IAPP.CIPM.v2024-11-08.q125

Exam Code:	CIPM
Exam Name:	Certified Information Privacy Manager (CIPM)
Certification Provider:	IAPP
Free Question Number:	125
Version:	v2024-11-08
# of views:	2207
# of Questions views:	1250
https://www.freeqas.com/qa/IAPP/CIPM/IAPP.CIPM.v2024-11-08.q125.html	

NEW QUESTION: 1
An executive for a multinational online retail company in the United States is looking for guidance in developing her company's privacy program beyond what is specifically required by law.
What would be the most effective resource for the executive to consult?
A. Breach notifications from competitors.
B. Industry frameworks.
C. Oversight organizations.
D. Internal auditors.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 2
SCENARIO
Please use the following to answer the next QUESTION:
Martin Briseno is the director of human resources at the Canyon City location of the U.S. hotel chain Pacific Suites. In 1998, Briseno decided to change the hotel's on-the-job mentoring model to a standardized training program for employees who were progressing from line positions into supervisory positions. He developed a curriculum comprising a series of lessons, scenarios, and assessments, which was delivered in-person to small groups. Interest in the training increased, leading Briseno to work with corporate HR specialists and software engineers to offer the program in an online format. The online program saved the cost of a trainer and allowed participants to work through the material at their own pace.
Upon hearing about the success of Briseno's program, Pacific Suites corporate Vice President Maryanne Silva-Hayes expanded the training and offered it company-wide. Employees who completed the program received certification as a Pacific Suites Hospitality Supervisor. By 2001, the program had grown to provide industry-wide training. Personnel at hotels across the country could sign up and pay to take the course online.
As the program became increasingly profitable, Pacific Suites developed an offshoot business, Pacific Hospitality Training (PHT). The sole focus of PHT was developing and marketing a variety of online courses and course progressions providing a number of professional certifications in the hospitality industry.

By setting up a user account with PHT, course participants could access an information library, sign up for courses, and take end-of-course certification tests. When a user opened a new account, all information was saved by default, including the user's name, date of birth, contact information, credit card information, employer, and job title. The registration page offered an opt-out choice that users could click to not have their credit card numbers saved. Once a user name and password were established, users could return to check their course status, review and reprint their certifications, and sign up and pay for new courses. Between 2002 and 2008, PHT issued more than 700,000 professional certifications.

PHT's profits declined in 2009 and 2010, the victim of industry downsizing and increased competition from e-learning providers. By 2011, Pacific Suites was out of the online certification business and PHT was dissolved. The training program's systems and records remained in Pacific Suites' digital archives, un-accessed and unused. Briseno and Silva-Hayes moved on to work for other companies, and there was no plan for handling the archived data after the program ended. After PHT was dissolved, Pacific Suites executives turned their attention to crucial day-to-day operations. They planned to deal with the PHT materials once resources allowed.

In 2012, the Pacific Suites computer network was hacked. Malware installed on the online reservation system exposed the credit card information of hundreds of hotel guests. While targeting the financial data on the reservation site, hackers also discovered the archived training course data and registration accounts of Pacific Hospitality Training's customers. The result of the hack was the exfiltration of the credit card numbers of recent hotel guests and the exfiltration of the PHT database with all its contents.

A Pacific Suites systems analyst discovered the information security breach in a routine scan of activity reports. Pacific Suites quickly notified credit card companies and recent hotel guests of the breach, attempting to prevent serious harm. Technical security engineers faced a challenge in dealing with the PHT data.

PHT course administrators and the IT engineers did not have a system for tracking, cataloguing, and storing information. Pacific Suites has procedures in place for data access and storage, but those procedures were not implemented when PHT was formed. When the PHT database was acquired by Pacific Suites, it had no owner or oversight. By the time technical security engineers determined what private information was compromised, at least 8,000 credit card holders were potential victims of fraudulent activity.

What key mistake set the company up to be vulnerable to a security breach?

A. Neglecting to make a backup copy of archived electronic files

B. Overlooking the need to organize and categorize data

C. Collecting too much information and keeping it for too long

D. Failing to outsource training and data management to professionals

Answer: (SHOW ANSWER)

NEW QUESTION: 3

What is the main purpose of a privacy program audit?

A. To mitigate the effects of a privacy breach.

B. To make decisions on privacy staff roles and responsibilities.

C. To justify a privacy department budget increase.

D. To ensure the adequacy of data protection procedures.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 4
What is least likely to be achieved by implementing a Data Lifecycle Management (DLM) program?
A. Reducing storage costs.
B. Ensuring data is kept for no longer than necessary.
C. Crafting policies which ensure minimal data is collected.
D. Increasing awareness of the importance of confidentiality.
Answer: (SHOW ANSWER)
Explanation
Crafting policies which ensure minimal data is collected is least likely to be achieved by implementing a Data Lifecycle Management (DLM) program, as it is more related to the data collection stage, not the data management stage. A DLM program focuses on how to handle the data after it has been collected, such as how to store, use, share, and dispose of it. The other options are more likely to be achieved by implementing a DLM program, as they help to optimize the data storage costs, comply with the data retention obligations, and protect the data confidentiality. References: CIPM Body of Knowledge, Domain III: Privacy Program Management Activities, Task 1: Manage data inventory.

NEW QUESTION: 5
What is the name for the privacy strategy model that describes delegated decision making?
A. De-centralized.
B. De-functionalized.
C. Hybrid.
D. Matrix.
Answer: D (LEAVE A REPLY)
Explanation
A matrix is a type of organizational structure that involves delegated decision making. In a matrix structure, employees report to more than one manager or leader, usually based on different functions or projects. For example, a software developer may report to both a product manager and a technical manager. A matrix structure allows for more flexibility, collaboration, and innovation in complex and dynamic environments.
The other options are not examples of delegated decision making structures. A de-centralized structure involves distributing decision making authority across different levels or units of the organization, rather than concentrating it at the top. A de-functionalized structure involves breaking down functional silos and creating cross-functional teams or processes. A hybrid structure involves combining elements of different types of structures, such as functional, divisional, or matrix.

NEW QUESTION: 6
SCENARIO
Please use the following to answer the next QUESTION:
Ben works in the IT department of IgNight, Inc., a company that designs lighting solutions for its clients.

Although IgNight's customer base consists primarily of offices in the US, some individuals have been so impressed by the unique aesthetic and energy-saving design of the light fixtures that they have requested IgNight's installations in their homes across the globe.

One Sunday morning, while using his work laptop to purchase tickets for an upcoming music festival, Ben happens to notice some unusual user activity on company files. From a cursory review, all the data still appears to be where it is meant to be but he can't shake off the feeling that something is not right. He knows that it is a possibility that this could be a colleague performing unscheduled maintenance, but he recalls an email from his company's security team reminding employees to be on alert for attacks from a known group of malicious actors specifically targeting the industry.

Ben is a diligent employee and wants to make sure that he protects the company but he does not want to bother his hard-working colleagues on the weekend. He is going to discuss the matter with this manager first thing in the morning but wants to be prepared so he can demonstrate his knowledge in this area and plead his case for a promotion.

To determine the steps to follow, what would be the most appropriate internal guide for Ben to review?

A. Incident Response Plan.

B. Code of Business Conduct.

C. IT Systems and Operations Handbook.

D. Business Continuity and Disaster Recovery Plan.

Answer: (SHOW ANSWER)

Explanation

The most appropriate internal guide for Ben to review is the Incident Response Plan. An Incident Response Plan is a document that outlines how an organization will respond to a security incident, such as a data breach, a cyberattack, or a malware infection. An Incident Response Plan typically includes:

* The roles and responsibilities of the incident response team and other stakeholders
* The procedures and protocols for detecting, containing, analyzing, and resolving incidents
* The communication and escalation channels for reporting and notifying incidents
* The tools and resources for conducting incident response activities
* The criteria and methods for evaluating and improving the incident response process An Incident Response Plan helps an organization prepare for and deal with security incidents in an effective and efficient manner. It also helps an organization minimize the impact and damage of security incidents, comply with legal and regulatory obligations, and restore normal operations as soon as possible.

The other options are not as relevant or useful as the Incident Response Plan for Ben's situation. The Code of Business Conduct is a document that defines the ethical standards and expectations for the organization's employees and stakeholders. It may include some general principles or policies related to security, but it does not provide specific guidance on how to handle security incidents. The IT Systems and Operations Handbook is a document that describes the technical aspects and functions of the organization's IT systems and infrastructure. It may include some information on security controls and configurations, but it does not provide detailed instructions on how to perform incident response tasks. The Business Continuity and Disaster Recovery Plan is a document that outlines how an organization will continue its critical functions and operations in the event of a disruption or disaster, such as a natural disaster, a power outage, or a fire. It may

include some measures to protect or recover data and systems, but it does not focus on security incidents or threats. References: What Is an Incident Response Plan for IT?; Incident Response Plan (IRP) Basics

NEW QUESTION: 7
An online retailer detects an incident involving customer shopping history but no keys have been compromised. The Privacy Offce is most concerned when it also involves?
A. Internal unique personal identifiers.
B. Plain text personal identifiers.
C. Hashed mobile identifiers.
D. No personal identifiers.
Answer: B (LEAVE A REPLY)
Explanation
An online retailer detects an incident involving customer shopping history but no keys have been compromised. The Privacy Office is most concerned when it also involves plain text personal identifiers. Plain text personal identifiers are data elements that can directly identify an individual, such as name, email address, phone number, or social security number. Plain text means that the data is not encrypted or otherwise protected from unauthorized access or disclosure. If an incident involves plain text personal identifiers, it poses a high risk to the privacy and security of the customers, as their personal data could be exposed, stolen, misused, or manipulated by malicious actors. The Privacy Office should take immediate steps to contain, assess, notify, evaluate, and prevent such incidents, . References: [CIPM - International Association of Privacy Professionals], [Free CIPM Study Guide - International Association of Privacy Professionals]

NEW QUESTION: 8
An organization is establishing a mission statement for its privacy program. Which of the following statements would be the best to use?
A. In the next 20 years, our privacy program should be able to eliminate 80% of our current breaches. To do this, everyone in our organization must complete our annual privacy training course and all personally identifiable information must be inventoried.
B. Our organization was founded in 2054 to reduce the chance of a future disaster like the one that occurred ten years ago. All individuals from our area of the country should be concerned about a future disaster. However, with our privacy program, they should not be concerned about the misuse of their information.
C. This privacy program encourages cross-organizational collaboration which will stop all data breaches
D. The goal of the privacy program is to protect the privacy of all individuals who support our organization. To meet this goal, we must work to comply with all applicable privacy laws.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 9
What is the function of the privacy operational life cycle?
A. It establishes initial plans for privacy protection and implementation
B. It allows the organization to respond to ever-changing privacy demands

C. It ensures that outdated privacy policies are retired on a set schedule
D. It allows privacy policies to mature to a fixed form
Answer: B (LEAVE A REPLY)
Explanation
The privacy operational life cycle is a process that allows the organization to respond to ever-changing privacy demands by continuously monitoring and improving the privacy program. It consists of four phases: assess, protect, sustain, and respond. Each phase involves different activities and outputs that help the organization identify and manage privacy risks and opportunities. References: IAPP CIPM Study Guide, page 14.

NEW QUESTION: 10
Which is NOT an influence on the privacy environment external to an organization?
A. Technological advances
B. Regulations
C. Consumer demand
D. Management team priorities
Answer: (SHOW ANSWER)

NEW QUESTION: 11
When devising effective employee policies to address a particular issue, which of the following should be included in the first draft?
A. Rationale for the policy.
B. Explanation of how the policy is applied within the organization.
C. Points of contact for the employee.
D. Roles and responsibilities of the different groups of individuals.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 12
SCENARIO
Please use the following to answer the next question:
Paul Daniels, with years of experience as a CEO, is worried about his son Carlton's successful venture, Gadgo.
A technological innovator in the communication industry that quickly became profitable, Gadgo has moved beyond its startup phase. While it has retained its vibrant energy, Paul fears that under Carlton's direction, the company may not be taking its risks or obligations as seriously as it needs to. Paul has hired you, a privacy Consultant, to assess the company and report to both father and son. "Carlton won't listen to me," Paul says, "but he may pay attention to an expert."
Gadgo's workplace is a clubhouse for innovation, with games, toys, snacks, espresso machines, giant fish tanks and even an iguana who regards you with little interest. Carlton, too, seems bored as he describes to you the company's procedures and technologies for data protection. It's a loose assemblage of controls, lacking consistency and with plenty of weaknesses. "This is a technology company," Carlton says. "We

create. We innovate. I don't want unnecessary measures that will only slow people down and clutter their thoughts." The meeting lasts until early evening. Upon leaving, you walk through the office. It looks as if a strong windstorm has recently blown through, with papers scattered across desks and tables and even the floor. A
"cleaning crew" of one teenager is emptying the trash bins. A few computers have been left on for the night; others are missing. Carlton takes note of your attention to this: "Most of my people take their laptops home with them, or use their own tablets or phones. I want them to use whatever helps them to think and be ready day or night for that great insight. It may only come once!" What would be the best kind of audit to recommend for Gadgo?
A. A third-party audit
B. A supplier audit
C. An internal audit
D. A self-certification
Answer: A (LEAVE A REPLY)

NEW QUESTION: 13
Why were the nongovernmental privacy organizations, Electronic Frontier Foundation (EFF) and Electronic Privacy Information Center (EPIC), established?
A. To promote security on the Internet through strong encryption.
B. To promote consumer confidence in the Internet industry.
C. To improve the user experience during online shopping.
D. To protect civil liberties and raise consumer awareness.
Answer: (SHOW ANSWER)

NEW QUESTION: 14
SCENARIO
Please use the following to answer the next QUESTION:
Penny has recently joined Ace Space, a company that sells homeware accessories online, as its new privacy officer. The company is based in California but thanks to some great publicity from a social media influencer last year, the company has received an influx of sales from the EU and has set up a regional office in Ireland to support this expansion. To become familiar with Ace Space's practices and assess what her privacy priorities will be, Penny has set up meetings with a number of colleagues to hear about the work that they have been doing and their compliance efforts.
Penny's colleague in Marketing is excited by the new sales and the company's plans, but is also concerned that Penny may curtail some of the growth opportunities he has planned. He tells her "I heard someone in the breakroom talking about some new privacy laws but I really don't think it affects us. We're just a small company. I mean we just sell accessories online, so what's the real risk?" He has also told her that he works with a number of small companies that help him get projects completed in a hurry. "We've got to meet our deadlines otherwise we lose money. I just sign the contracts and get Jim in finance to push through the payment. Reviewing the contracts takes time that we just don't have." In her meeting with a member of the IT team, Penny has learned that although Ace Space has taken a number of precautions to protect its website

from malicious activity, it has not taken the same level of care of its physical files or internal infrastructure. Penny's colleague in IT has told her that a former employee lost an encrypted USB key with financial data on it when he left. The company nearly lost access to their customer database last year after they fell victim to a phishing attack. Penny is told by her IT colleague that the IT team
"didn't know what to do or who should do what. We hadn't been trained on it but we're a small team though, so it worked out OK in the end." Penny is concerned that these issues will compromise Ace Space's privacy and data protection.
Penny is aware that the company has solid plans to grow its international sales and will be working closely with the CEO to give the organization a data "shake up". Her mission is to cultivate a strong privacy culture within the company.
Penny has a meeting with Ace Space's CEO today and has been asked to give her first impressions and an overview of her next steps.
What information will be LEAST crucial from a privacy perspective in Penny's review of vendor contracts?
A. Audit rights
B. Liability for a data breach
C. Pricing for data security protections
D. The data a vendor will have access to
Answer: C (LEAVE A REPLY)
Explanation
The information that will be least crucial from a privacy perspective in Penny's review of vendor contracts is the pricing for data security protections . This is because the pricing for data security protections is a business decision that does not directly affect the privacy rights and obligations of Ace Space and its customers. The pricing for data security protections may be relevant for budgeting and negotiating purposes, but it does not determine the level or adequacy of data security measures that the vendor must provide to protect personal data.
The other options are more crucial from a privacy perspective in Penny's review of vendor contracts. Audit rights (A) are important to ensure that Ace Space can monitor and verify the vendor's compliance with the contract terms and the applicable privacy laws and regulations. Audit rights allow Ace Space to access the vendor's records, systems, policies and procedures related to personal data processing and to conduct inspections or assessments as needed. Liability for a data breach (B) is important to allocate the responsibility and consequences of a data breach involving personal data that the vendor processes on behalf of Ace Space.
Liability for a data breach may include indemnification, compensation, notification, remediation and termination clauses that protect Ace Space's interests and obligations in the event of a data breach. The data a vendor will have access to (D) is important to define the scope, purpose, duration and conditions of the personal data processing that the vendor will perform for Ace Space. The data a vendor will have access to may include the categories, types, sources, recipients and retention periods of personal data that the vendor will collect, store, use or share on behalf of Ace Space.
References:
* CIPM Body of Knowledge Domain II: Privacy Program Operational Life Cycle - Task 3: Implement
* privacy program components - Subtask 3: Establish third-party processor management program

* CIPM Study Guide - Chapter 4: Privacy Program Operational Life Cycle - Section 4.3: Third-Party Processor Management

NEW QUESTION: 15
SCENARIO
Please use the following to answer the next QUESTION:
It's just what you were afraid of. Without consulting you, the information technology director at your organization launched a new initiative to encourage employees to use personal devices for conducting business. The initiative made purchasing a new, high-specification laptop computer an attractive option, with discounted laptops paid for as a payroll deduction spread over a year of paychecks. The organization is also paying the sales taxes. It's a great deal, and after a month, more than half the organization's employees have signed on and acquired new laptops. Walking through the facility, you see them happily customizing and comparing notes on their new computers, and at the end of the day, most take their laptops with them, potentially carrying personal data to their homes or other unknown locations. It's enough to give you data-protection nightmares, and you've pointed out to the information technology Director and many others in the organization the potential hazards of this new practice, including the inevitability of eventual data loss or theft.
Today you have in your office a representative of the organization's marketing department who shares with you, reluctantly, a story with potentially serious consequences. The night before, straight from work, with laptop in hand, he went to the Bull and Horn Pub to play billiards with his friends. A fine night of sport and socializing began, with the laptop "safely" tucked on a bench, beneath his jacket. Later that night, when it was time to depart, he retrieved the jacket, but the laptop was gone. It was not beneath the bench or on another bench nearby. The waitstaff had not seen it. His friends were not playing a joke on him. After a sleepless night, he confirmed it this morning, stopping by the pub to talk to the cleanup crew. They had not found it. The laptop was missing. Stolen, it seems. He looks at you, embarrassed and upset.
You ask him if the laptop contains any personal data from clients, and, sadly, he nods his head, yes. He believes it contains files on about 100 clients, including names, addresses and governmental identification numbers. He sighs and places his head in his hands in despair.
From a business standpoint, what is the most productive way to view employee use of personal equipment for work-related tasks?
A. The use of personal equipment must be reduced as it leads to inevitable security risks.
B. The use of personal equipment is a cost-effective measure that leads to no greater security risks than are always present in a modern organization.
C. Any computer or other equipment is company property whenever it is used for company business.
D. While the company may not own the equipment, it is required to protect the business-related data on any equipment used by its employees.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 16
What does it mean to "rationalize" data protection requirements?
A. Look for overlaps in laws and regulations from which a common solution can be developed
B. Address the less stringent laws and regulations, and inform stakeholders why they are applicable

C. Evaluate the costs and risks of applicable laws and regulations and address those that have the greatest penalties
D. Determine where laws and regulations are redundant in order to eliminate some from requiring compliance
Answer: (SHOW ANSWER)

NEW QUESTION: 17
SCENARIO
Please use the following to answer the next QUESTION:
Henry Home Furnishings has built high-end furniture for nearly forty years. However, the new owner, Anton, has found some degree of disorganization after touring the company headquarters. His uncle Henry had always focused on production - not data processing - and Anton is concerned. In several storage rooms, he has found paper files, disks, and old computers that appear to contain the personal data of current and former employees and customers. Anton knows that a single break-in could irrevocably damage the company's relationship with its loyal customers. He intends to set a goal of guaranteed zero loss of personal information.
To this end, Anton originally planned to place restrictions on who was admitted to the physical premises of the company. However, Kenneth - his uncle's vice president and longtime confidante - wants to hold off on Anton's idea in favor of converting any paper records held at the company to electronic storage. Kenneth believes this process would only take one or two years. Anton likes this idea; he envisions a password-protected system that only he and Kenneth can access.
Anton also plans to divest the company of most of its subsidiaries. Not only will this make his job easier, but it will simplify the management of the stored data. The heads of subsidiaries like the art gallery and kitchenware store down the street will be responsible for their own information management. Then, any unneeded subsidiary data still in Anton's possession can be destroyed within the next few years.
After learning of a recent security incident, Anton realizes that another crucial step will be notifying customers. Kenneth insists that two lost hard drives in Question are not cause for concern; all of the data was encrypted and not sensitive in nature. Anton does not want to take any chances, however. He intends on sending notice letters to all employees and customers to be safe.
Anton must also check for compliance with all legislative, regulatory, and market requirements related to privacy protection. Kenneth oversaw the development of the company's online presence about ten years ago, but Anton is not confident about his understanding of recent online marketing laws. Anton is assigning another trusted employee with a law background the task of the compliance assessment. After a thorough analysis, Anton knows the company should be safe for another five years, at which time he can order another check.

Documentation of this analysis will show auditors due diligence.
Anton has started down a long road toward improved management of the company, but he knows the effort is worth it. Anton wants his uncle's legacy to continue for many years to come.
In terms of compliance with regulatory and legislative changes, Anton has a misconception regarding?
A. The timeline for monitoring.
B. The method of recordkeeping.
C. The use of internal employees.
D. The type of required qualifications.
Answer: A (LEAVE A REPLY)
Explanation
In terms of compliance with regulatory and legislative changes, Anton has a misconception regarding the timeline for monitoring. He believes that the company should be safe for another five years after conducting a compliance assessment and documenting the analysis. However, this is a risky and unrealistic assumption that could expose the company to legal liabilities and penalties. Regulatory and legislative changes are dynamic and frequent in today's business environment. They can affect various aspects of the company's operations, such as data protection, online marketing, consumer rights, labor laws, tax laws, environmental laws, etc5 Therefore, the company needs to monitor these changes continuously and proactively to ensure compliance at all times. Waiting for five years to check for compliance again could result in missing important updates or requirements that could impact the company's business practices or obligations. Moreover, compliance monitoring is not only a one-time activity but an ongoing process that involves evaluating the effectiveness of the company's policies and procedures in meeting the regulatory standards and expectations6 Compliance monitoring also helps to identify any gaps or weaknesses in the company's compliance program and take corrective actions to improve it. Therefore, Anton should revise his timeline for monitoring regulatory and legislative changes and adopt a more regular and systematic approach that aligns with the company's risk profile and regulatory environment. References: 5: Regulatory Change Management: How To Keep Up With Regulatory Changes; 6: Compliance Monitoring - What Is It?

NEW QUESTION: 18
SCENARIO
Please use the following to answer the next QUESTION:
Amira is thrilled about the sudden expansion of NatGen. As the joint Chief Executive Officer (CEO) with her long-time business partner Sadie, Amira has watched the company grow into a major competitor in the green energy market. The current line of products includes wind turbines, solar energy panels, and equipment for geothermal systems. A talented team of developers means that NatGen's line of products will only continue to grow.
With the expansion, Amira and Sadie have received advice from new senior staff members brought on to help manage the company's growth. One recent suggestion has been to combine the legal and security functions of the company to ensure observance of privacy laws and the company's own privacy policy. This sounds overly complicated to Amira, who wants departments to be able to use, collect, store, and dispose of customer data in ways that will best suit their needs. She does not want administrative oversight and complex structuring to get in the way of people doing innovative work.

Sadie has a similar outlook. The new Chief Information Officer (CIO) has proposed what Sadie believes is an unnecessarily long timetable for designing a new privacy program. She has assured him that NatGen will use the best possible equipment for electronic storage of customer and employee dat a. She simply needs a list of equipment and an estimate of its cost. But the CIO insists that many issues are necessary to consider before the company gets to that stage.

Regardless, Sadie and Amira insist on giving employees space to do their jobs. Both CEOs want to entrust the monitoring of employee policy compliance to low-level managers. Amira and Sadie believe these managers can adjust the company privacy policy according to what works best for their particular departments. NatGen's CEOs know that flexible interpretations of the privacy policy in the name of promoting green energy would be highly unlikely to raise any concerns with their customer base, as long as the data is always used in course of normal business activities.

Perhaps what has been most perplexing to Sadie and Amira has been the CIO's recommendation to institute a privacy compliance hotline. Sadie and Amira have relented on this point, but they hope to compromise by allowing employees to take turns handling reports of privacy policy violations. The implementation will be easy because the employees need no special preparation. They will simply have to document any concerns they hear.

Sadie and Amira are aware that it will be challenging to stay true to their principles and guard against corporate culture strangling creativity and employee morale. They hope that all senior staff will see the benefit of trying a unique approach.

If Amira and Sadie's ideas about adherence to the company's privacy policy go unchecked, the Federal Communications Commission (FCC) could potentially take action against NatGen for what?

A. Failing to institute the hotline.

B. Negligence in consistent training.

C. Failure to notify of processing.

D. Deceptive practices.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 19

When conducting due diligence during an acquisition, what should a privacy professional avoid?

A. Discussing with the acquired company the type and scope of their data processing.

B. Allowing legal in both companies to handle the privacy laws and compliance.

C. Planning for impacts on the data processing operations post-acquisition.

D. Benchmarking the two Companies privacy policies against one another.

Answer: B (LEAVE A REPLY)

Explanation

When conducting due diligence during an acquisition, a privacy professional should avoid allowing legal in both companies to handle the privacy laws and compliance. This is because privacy is not only a legal issue, but also a business, technical, and operational issue that requires cross-functional collaboration and expertise.

A privacy professional should be involved in the due diligence process to assess the privacy risks and opportunities of the acquisition, such as the type and scope of data processing, the data protection policies

and practices, the data transfer mechanisms and agreements, the data breach history and response plans, and the impacts on the data processing operations post-acquisition. A privacy professional should also benchmark the two companies' privacy policies against one another to identify any gaps or inconsistencies that need to be addressed before or after the acquisition, . References: [CIPM - International Association of Privacy Professionals], [Free CIPM Study Guide - International Association of Privacy Professionals]

NEW QUESTION: 20
In which situation would a Privacy Impact Assessment (PIA) be the least likely to be required?
A. If a company created a credit-scoring platform five years ago.
B. If a health-care professional or lawyer processed personal data from a patient's file.
C. If a social media company created a new product compiling personal data to generate user profiles.
D. If an after-school club processed children's data to determine which children might have food allergies.
Answer: (SHOW ANSWER)
Explanation
A Privacy Impact Assessment (PIA) is a process that helps to identify and mitigate the privacy risks of a project or activity that involves personal data. A PIA is usually required when there is a new or significant change in the way personal data is collected, used, or disclosed. Therefore, a PIA would be the least likely to be required if a company created a credit-scoring platform five years ago, as this would not be a new or significant change. The other situations involve new or changed processing of personal data that could have privacy impacts, such as sensitive data (health or children's data), profiling data (user profiles), or large-scale data (patient's file). References: CIPM Study Guide, page 30; Guide to undertaking privacy impact assessments.

NEW QUESTION: 21
SCENARIO
Please use the following to answer the next question:
Edufox has hosted an annual convention of users of its famous e-learning software platform, and over time, it has become a grand event. It fills one of the large downtown conference hotels and overflows into the others, with several thousand attendees enjoying three days of presentations, panel discussions and networking. The convention is the centerpiece of the company's product rollout schedule and a great training opportunity for current users. The sales force also encourages prospective clients to attend to get a better sense of the ways in which the system can be customized to meet diverse needs and understand that when they buy into this system, they are joining a community that feels like family.
This year's conference is only three weeks away, and you have just heard news of a new initiative supporting it:
a smartphone app for attendees. The app will support late registration, highlight the featured presentations and provide a mobile version of the conference program. It also links to a restaurant reservation system with the best cuisine in the areas featured. "It's going to be great," the developer, Deidre Hoffman, tells you, "if, that is, we actually get it working!" She laughs nervously but explains that because of the tight time frame she'd been given to build the app, she outsourced the job to a local firm. "It's just three young people," she says, "but they do great work." She describes some of the other apps they have built. When asked how they

were selected for this job, Deidre shrugs. "They do good work, so I chose them." Deidre is a terrific employee with a strong track record. That's why she's been charged to deliver this rushed project. You're sure she has the best interests of the company at heart, and you don't doubt that she's under pressure to meet a deadline that cannot be pushed back. However, you have concerns about the app's handling of personal data and its security safeguards. Over lunch in the break room, you start to talk to her about it, but she quickly tries to reassure you, "I'm sure with your help we can fix any security issues if we have to, but I doubt there'll be any. These people build apps for a living, and they know what they're doing. You worry too much, but that's why you're so good at your job!" Which is the best first step in understanding the data security practices of a potential vendor?

A. Examining investigation records of any breaches the vendor has experienced.

B. Conducting a physical audit of the vendor's facilities.

C. Conducting a penetration test of the vendor's data security structure.

D. Requiring the vendor to complete a questionnaire assessing International Organization for Standardization (ISO) 27001 compliance.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 22

SCENARIO

Please use the following to answer the next QUESTION:

As they company's new chief executive officer, Thomas Goddard wants to be known as a leader in data protection. Goddard recently served as the chief financial officer of Hoopy.com, a pioneer in online video viewing with millions of users around the world. Unfortunately, Hoopy is infamous within privacy protection circles for its ethically Questionable practices, including unauthorized sales of personal data to marketers. Hoopy also was the target of credit card data theft that made headlines around the world, as at least two million credit card numbers were thought to have been pilfered despite the company's claims that "appropriate" data protection safeguards were in place. The scandal affected the company's business as competitors were quick to market an increased level of protection while offering similar entertainment and media content. Within three weeks after the scandal broke, Hoopy founder and CEO Maxwell Martin, Goddard's mentor, was forced to step down.

Goddard, however, seems to have landed on his feet, securing the CEO position at your company, Medialite, which is just emerging from its start-up phase. He sold the company's board and investors on his vision of Medialite building its brand partly on the basis of industry-leading data protection standards and procedures. He may have been a key part of a lapsed or even rogue organization in matters of privacy but now he claims to be reformed and a true believer in privacy protection. In his first week on the job, he calls you into his office and explains that your primary work responsibility is to bring his vision for privacy to life. But you also detect some reservations. "We want Medialite to have absolutely the highest standards," he says. "In fact, I want us to be able to say that we are the clear industry leader in privacy and data protection. However, I also need to be a responsible steward of the company's finances. So, while I want the best solutions across the board, they also need to be cost effective." You are told to report back in a week's time with your recommendations. Charged with this ambiguous mission, you depart the executive suite, already considering your next steps.

The CEO likes what he's seen of the company's improved privacy program, but wants additional assurance that it is fully compliant with industry standards and reflects emerging best practices. What would best help accomplish this goal?

A. An external audit conducted by a panel of industry experts

B. An internal audit team accountable to upper management

C. Creation of a self-certification framework based on company policies

D. Revision of the strategic plan to provide a system of technical controls

Answer: A (LEAVE A REPLY)

Explanation

This approach provides an independent, unbiased review of the company's privacy program. External experts can assess the company's processes and controls against industry standards, benchmarks, and emerging best practices. This will not only provide the desired assurance but also potentially enhance the company's credibility in the eyes of stakeholders, as it shows a willingness to be transparent and undergo external scrutiny.

NEW QUESTION: 23

What should be the first major goal of a company developing a new privacy program?

A. To schedule conversations with executives of affected departments.

B. To create Data Lifecycle Management policies and procedures to limit data collection.

C. To survey potential funding sources for privacy team resources.

D. To identify potential third-party processors of the organization's information.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 24

Which of the following controls does the PCI DSS framework NOT require?

A. Implement strong asset control protocols.

B. Implement strong access control measures.

C. Maintain an information security policy.

D. Maintain a vulnerability management program.

Answer: A (LEAVE A REPLY)

Explanation

The PCI DSS framework does not require implementing strong asset control protocols. Asset control protocols are policies and procedures that govern how an organization manages its physical and digital assets, such as inventory, equipment, software, data, etc. Asset control protocols may include aspects such as identification, classification, valuation, tracking, maintenance, disposal, etc. Asset control protocols are important for ensuring the security and integrity of an organization's assets, but they are not part of the PCI DSS framework.

NEW QUESTION: 25

Which is the best way to view an organization's privacy framework?

A. As an industry benchmark that can apply to many organizations

B. As a fixed structure that directs changes in the organization
C. As an aspirational goal that improves the organization
D. As a living structure that aligns to changes in the organization
Answer: D (LEAVE A REPLY)
Explanation
The best way to view an organization's privacy framework is as a living structure that aligns to changes in the organization, such as business goals, stakeholder expectations, legal requirements, and technological developments. A privacy framework should be flexible and adaptable to support the organization's privacy strategy and vision. It should also be compatible with other frameworks, such as the cybersecurity framework, that the organization may use. References: IAPP CIPM Study Guide, page 16.

NEW QUESTION: 26
SCENARIO
Please use the following to answer the next QUESTION:
Natalia, CFO of the Nationwide Grill restaurant chain, had never seen her fellow executives so anxious. Last week, a data processing firm used by the company reported that its system may have been hacked, and customer data such as names, addresses, and birthdays may have been compromised. Although the attempt was proven unsuccessful, the scare has prompted several Nationwide Grill executives to Question the company's privacy program at today's meeting.
Alice, a vice president, said that the incident could have opened the door to lawsuits, potentially damaging Nationwide Grill's market position. The Chief Information Officer (CIO), Brendan, tried to assure her that even if there had been an actual breach, the chances of a successful suit against the company were slim. But Alice remained unconvinced.
Spencer - a former CEO and currently a senior advisor - said that he had always warned against the use of contractors for data processing. At the very least, he argued, they should be held contractually liable for telling customers about any security incidents. In his view, Nationwide Grill should not be forced to soil the company name for a problem it did not cause.
One of the business development (BD) executives, Haley, then spoke, imploring everyone to see reason. "Breaches can happen, despite organizations' best efforts," she remarked. "Reasonable preparedness is key." She reminded everyone of the incident seven years ago when the large grocery chain Tinkerton's had its financial information compromised after a large order of Nationwide Grill frozen dinners. As a long-time BD executive with a solid understanding of Tinkerton's's corporate culture, built up through many years of cultivating relationships, Haley was able to successfully manage the company's incident response.
Spencer replied that acting with reason means allowing security to be handled by the security functions within the company - not BD staff. In a similar way, he said, Human Resources (HR) needs to do a better job training employees to prevent incidents. He pointed out that Nationwide Grill employees are overwhelmed with posters, emails, and memos from both HR and the ethics department related to the company's privacy program. Both the volume and the duplication of information means that it is often ignored altogether.
Spencer said, "The company needs to dedicate itself to its privacy program and set regular in-person trainings for all staff once a month." Alice responded that the suggestion, while well-meaning, is not practical.

With many locations, local HR departments need to have flexibility with their training schedules. Silently, Natalia agreed.
What is the most realistic step the organization can take to help diminish liability in the event of another incident?
A. Specifying mandatory data protection practices in vendor contracts.
B. Obtaining customer consent for any third-party processing of personal data.
C. Requiring the vendor to perform periodic internal audits.
D. Keeping the majority of processing activities within the organization.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 27
What is one obligation that the General Data Protection Regulation (GDPR) imposes on data processors?
A. To inform data subjects about the identity and contact details of the controller
B. To carry out data protection impact assessments in cases where processing is likely to result in high risk to the rights and freedoms of individuals
C. To honor all data access requests from data subjects
D. To implement appropriate technical and organizational measures that ensure an appropriate level of security
Answer: B (LEAVE A REPLY)

NEW QUESTION: 28
Formosa International operates in 20 different countries including the United States and France.
What organizational approach would make complying with a number of different regulations easier?
A. Data mapping.
B. Fair Information Practices.
C. Decentralized privacy management.
D. Rationalizing requirements.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 29
Which statement is FALSE regarding the use of technical security controls?
A. Most privacy legislation lists the types of technical security controls that must be implemented.
B. A person with security knowledge should be involved with the deployment of technical security controls.
C. Technical security controls are part of a data governance strategy.
D. Technical security controls deployed for one jurisdiction often satisfy another jurisdiction.
Answer: (SHOW ANSWER)

NEW QUESTION: 30
In a sample metric template, what does "target" mean?
A. The frequency at which the data is sampled
B. The suggested volume of data to collect

C. The threshold for a satisfactory rating
D. The percentage of completion
Answer: B (LEAVE A REPLY)

NEW QUESTION: 31
SCENARIO
Please use the following to answer the next question
You were recently hired by InStyte Date Corp as a privacy manager to help InStyle Data Corp become compliant with a new data protection law The law mandates that businesses have reasonable and appropriate security measures in place to protect personal data. Violations of that mandate are heavily fined and the legislators have stated that they will aggressively pursue companies that don t comply with the new law You are paved with a security manager and tasked with reviewing InStyle Data Corp s current state and advising the business how it can meet the "reasonable and appropriate security" requirement InStyle Data Corp has grown rapidly and has not kept a data inventory or completed a data mapping InStyte Data Corp has also developed security-related policies ad hoc and many have never been implemented The various teams involved in the creation and testing of InStyle Data Corp s products experience significant turnover and do not have well defined roles There's little documentation addressing what personal data is processed by which product and for what purpose Work needs to begin on this project immediately so that InStyle Data Corp can become compliant by the time the law goes into effect. You and you partner discover that InStyle Data Corp regularly sends files containing sensitive personal data back to its customers through email sometimes using InStyle Data Corp employees personal email accounts. You also team that InStyle Data Corp s privacy and information security teams are not informed of new personal data flows, new products developed by InStyte Data Corp that process personal data, or updates to existing InStyle Data Corp products that may change what or how the personal data is processed until after the product or update has gone have.
Through a review of InStyle Date Corp's test and development environment logs, you discover InStyle Data Corp sometimes gives login credentials to any InStyle Data Corp employee or contractor who requests them. The test environment only contains dummy data but the development environment contains personal data including Social Security Numbers, hearth ^formation and financial information All credentialed InStyle Data Corp employees and contractors have the ability to after and delete personal data in both environments regardless of their role or what project they are working on.
You and your partner provide a gap assessment citing the issues you spotted, along with recommended remedial actions and a method to measure implementation InStyle Data Corp implements all of the recommended security controls You review the processes roles, controls and measures taken to appropriately protect the personal data at every stop However, you realize there is no plan for monitoring and nothing in place addressing sanctions for violations of the updated policies and procedures InStyle Data Corp pushes back, stating they do not have the resources for such monitoring.
What aspect of the data management life cycle will still be unaddressed it you cannot find the resources to become compliant?
A. Auditability.
B. Enforcement
C. Irretrievability

D. Access management

Answer: (SHOW ANSWER)

Explanation

The aspect of the data management life cycle that will still be unaddressed if you cannot find the resources to become compliant is enforcement. Enforcement means ensuring that the data policies and procedures are followed by all data users and stakeholders, and that any violations or deviations are detected, reported, and corrected. Enforcement also involves imposing sanctions or penalties for non-compliance, such as revoking access rights, issuing warnings, or terminating contracts. Without enforcement, the data security measures that you implemented may not be effective or sustainable, as there would be no accountability or deterrence for data misuse or abuse1, 2.

To address the enforcement aspect of the data management life cycle, you should try to convince InStyle Data Corp of the importance and benefits of monitoring and sanctioning data activities. You should explain that monitoring can help identify and prevent data breaches, errors, or inefficiencies, as well as demonstrate compliance with the new data protection law. You should also explain that sanctioning can help enforce data discipline and responsibility, as well as deter potential violators or malicious actors. You should also propose some possible ways to allocate or optimize the resources for monitoring and sanctioning, such as automating some processes, outsourcing some tasks, or prioritizing some data types or sources1, 2.

References: Data Lifecycle Management: A 2023 Guide for Your Business - Cloudwards, 6 Data Lifecycle Stages: Data Cycle Management Guide

NEW QUESTION: 32

Read the following steps:

* Perform frequent data back-ups.
* Perform test restorations to verify integrity of backed-up data.
* Maintain backed-up data offline or on separate servers.

These steps can help an organization recover from what?

A. Phishing attacks

B. Authorization errors

C. Ransomware attacks

D. Stolen encryption keys

Answer: C (LEAVE A REPLY)

Explanation

NEW QUESTION: 33
SCENARIO
Please use the following to answer the next QUESTION:
Natalia, CFO of the Nationwide Grill restaurant chain, had never seen her fellow executives so anxious. Last week, a data processing firm used by the company reported that its system may have been hacked, and customer data such as names, addresses, and birthdays may have been compromised. Although the attempt was proven unsuccessful, the scare has prompted several Nationwide Grill executives to Question the company's privacy program at today's meeting.
Alice, a vice president, said that the incident could have opened the door to lawsuits, potentially damaging Nationwide Grill's market position. The Chief Information Officer (CIO), Brendan, tried to assure her that even if there had been an actual breach, the chances of a successful suit against the company were slim. But Alice remained unconvinced.
Spencer - a former CEO and currently a senior advisor - said that he had always warned against the use of contractors for data processing. At the very least, he argued, they should be held contractually liable for telling customers about any security incidents. In his view, Nationwide Grill should not be forced to soil the company name for a problem it did not cause.
One of the business development (BD) executives, Haley, then spoke, imploring everyone to see reason. "Breaches can happen, despite organizations' best efforts," she remarked. "Reasonable preparedness is key." She reminded everyone of the incident seven years ago when the large grocery chain Tinkerton's had its financial information compromised after a large order of Nationwide Grill frozen dinners. As a long-time BD executive with a solid understanding of Tinkerton's's corporate culture, built up through many years of cultivating relationships, Haley was able to successfully manage the company's incident response.
Spencer replied that acting with reason means allowing security to be handled by the security functions within the company - not BD staff. In a similar way, he said, Human Resources (HR) needs to do a better job training employees to prevent incidents. He pointed out that Nationwide Grill employees are overwhelmed with posters, emails, and memos from both HR and the ethics department related to the company's privacy program. Both the volume and the duplication of information means that it is often ignored altogether.
Spencer said, "The company needs to dedicate itself to its privacy program and set regular in-person trainings for all staff once a month." Alice responded that the suggestion, while well-meaning, is not practical. With many locations, local HR departments need to have flexibility with their training schedules. Silently, Natalia agreed.
How could the objection to Spencer's training suggestion be addressed?
A. By requiring training only on an as-needed basis.
B. By offering alternative delivery methods for trainings.
C. By customizing training based on length of employee tenure.
D. By introducing a system of periodic refresher trainings.
Answer: (SHOW ANSWER)

NEW QUESTION: 34
SCENARIO
Please use the following to answer the next question:

Perhaps Jack Kelly should have stayed in the U.S. He enjoys a formidable reputation inside the company, Special Handling Shipping, for his work in reforming certain "rogue" offices. Last year, news broke that a police sting operation had revealed a drug ring operating in the Providence, Rhode Island office in the United States.
Video from the office's video surveillance cameras leaked to news operations showed a drug exchange between Special Handling staff and undercover officers.
In the wake of this incident, Kelly had been sent to Providence to change the "hands off" culture that upper management believed had let the criminal elements conduct their illicit transactions. After a few weeks under Kelly's direction, the office became a model of efficiency and customer service. Kelly monitored his workers' activities using the same cameras that had recorded the illegal conduct of their former co-workers.
Now Kelly has been charged with turning around the office in Cork, Ireland, another trouble spot. The company has received numerous reports of the staff leaving the office unattended. When Kelly arrived, he found that even when present, the staff often spent their days socializing or conducting personal business on their mobile phones. Again, he observed their behaviors using surveillance cameras. He issued written reprimands to six staff members based on the first day of video alone.
Much to Kelly's surprise and chagrin, he and the company are now under investigation by the Data Protection Commissioner of Ireland for allegedly violating the privacy rights of employees. Kelly was told that the company's license for the cameras listed facility security as their main use, but he does not know why this matters. He has pointed out to his superiors that the company's training programs on privacy protection and data collection mention nothing about surveillance video.
You are a privacy protection consultant, hired by the company to assess this incident, report on the legal and compliance issues, and recommend next steps.
What should you advise this company regarding the status of security cameras at their offices in the United States?
A. Add security cameras at facilities that are now without them.
B. Set policies about the purpose and use of the security cameras.
C. Restrict access to surveillance video taken by the security cameras and destroy the recordings after a designated period of time.
D. Reduce the number of security cameras located inside the building.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 35
What have experts identified as an important trend in privacy program development?
A. The movement beyond crisis management to proactive prevention.
B. The narrowing of regulatory definitions of personal information.
C. The rollback of ambitious programs due to budgetary restraints.
D. The stabilization of programs as the pace of new legal mandates slows.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 36
An organization's internal audit team should do all of the following EXCEPT?

A. Verify that technical measures are in place.
B. Review how operations work in practice.
C. Ensure policies are being adhered to.
D. Implement processes to correct audit failures.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 37
What is the key factor that lays the foundation for all other elements of a privacy program?
A. A privacy mission statement
B. A responsible internal stakeholder
C. The structure of a privacy team
D. The applicable privacy regulations
Answer: D (LEAVE A REPLY)

NEW QUESTION: 38
You would like to better understand how your organization can demonstrate compliance with international privacy standards and identify gaps for remediation. What steps could you take to achieve this objective?
A. Carry out a second-party audit.
B. Consult your local privacy regulator.
C. Conduct an annual self assessment.
D. Engage a third-party to conduct an audit.
Answer: D (LEAVE A REPLY)
Explanation
Engaging a third-party to conduct an audit is the best way to ensure that your organization is compliant with international privacy standards and identify any gaps that need to be remediated. An audit should include a review of your organization's data processing activities, as well as its policies, procedures, and internal controls. Additionally, it should include an analysis of the applicable privacy laws and regulations. This audit will provide you with an objective third-party assessment of your organization's compliance with international privacy standards and identify any areas of non-compliance that need to be addressed

NEW QUESTION: 39
SCENARIO
Please use the following to answer the next QUESTION:
Manasa is a product manager at Omnipresent Omnimedia, where she is responsible for leading the development of the company's flagship product, the Handy Helper. The Handy Helper is an application that can be used in the home to manage family calendars, do online shopping, and schedule doctor appointments. After having had a successful launch in the United States, the Handy Helper is about to be made available for purchase worldwide.
The packaging and user guide for the Handy Helper indicate that it is a "privacy friendly" product suitable for the whole family, including children, but does not provide any further detail or privacy notice. In order to use the application, a family creates a single account, and the primary user has access to all information about the

other users. Upon start up, the primary user must check a box consenting to receive marketing emails from Omnipresent Omnimedia and selected marketing partners in order to be able to use the application.
Sanjay, the head of privacy at Omnipresent Omnimedia, was working on an agreement with a European distributor of Handy Helper when he fielded many Questions about the product from the distributor. Sanjay needed to look more closely at the product in order to be able to answer the Questions as he was not involved in the product development process.
In speaking with the product team, he learned that the Handy Helper collected and stored all of a user's sensitive medical information for the medical appointment scheduler. In fact, all of the user's information is stored by Handy Helper for the additional purpose of creating additional products and to analyze usage of the product. This data is all stored in the cloud and is encrypted both during transmission and at rest.
Consistent with the CEO's philosophy that great new product ideas can come from anyone, all Omnipresent Omnimedia employees have access to user data under a program called Eurek a. Omnipresent Omnimedia is hoping that at some point in the future, the data will reveal insights that could be used to create a fully automated application that runs on artificial intelligence, but as of yet, Eureka is not well-defined and is considered a long-term goal.
What can Sanjay do to minimize the risks of offering the product in Europe?
A. Sanjay should advise the distributor that Omnipresent Omnimedia has certified to the Privacy Shield Framework and there should be no issues.
B. Sanjay should document the data life cycle of the data collected by the Handy Helper.
C. Sanjay should write a privacy policy to include with the Handy Helper user guide.
D. Sanjay should work with Manasa to review and remediate the Handy Helper as a gating item before it is released.
Answer: (SHOW ANSWER)

NEW QUESTION: 40
SCENARIO
Please use the following to answer the next question:
For 15 years, Albert has worked at Treasure Box - a mail order company in the United States (U.S.) that used to sell decorative candles around the world, but has recently decided to limit its shipments to customers in the 48 contiguous states. Despite his years of experience, Albert is often overlooked for managerial positions. His frustration about not being promoted, coupled with his recent interest in issues of privacy protection, have motivated Albert to be an agent of positive change.
He will soon interview for a newly advertised position, and during the interview, Albert plans on making executives aware of lapses in the company's privacy program. He feels certain he will be rewarded with a promotion for preventing negative consequences resulting from the company's outdated policies and procedures.
For example, Albert has learned about the AICPA (American Institute of Certified Public Accountans)/CICA (Canadian Institute of Chartered Accountants) Privacy Maturity Model (PMM). Albert thinks the model is a useful way to measure Treasure Box's ability to protect personal data. Albert has noticed that Treasure Box fails to meet the requirements of the highest level of maturity of this model; at his interview, Albert will pledge

to assist the company with meeting this level in order to provide customers with the most rigorous security available.
Albert does want to show a positive outlook during his interview. He intends to praise the company's commitment to the security of customer and employee personal data against external threats. However, Albert worries about the high turnover rate within the company, particularly in the area of direct phone marketing. He sees many unfamiliar faces every day who are hired to do the marketing, and he often hears complaints in the lunch room regarding long hours and low pay, as well as what seems to be flagrant disregard for company procedures.
In addition, Treasure Box has had two recent security incidents. The company has responded to the incidents with internal audits and updates to security safeguards. However, profits still seem to be affected and anecdotal evidence indicates that many people still harbor mistrust. Albert wants to help the company recover.
He knows there is at least one incident the public in unaware of, although Albert does not know the details. He believes the company's insistence on keeping the incident a secret could be a further detriment to its reputation. One further way that Albert wants to help Treasure Box regain its stature is by creating a toll-free number for customers, as well as a more efficient procedure for responding to customer concerns by postal mail.
In addition to his suggestions for improvement, Albert believes that his knowledge of the company's recent business maneuvers will also impress the interviewers. For example, Albert is aware of the company's intention to acquire a medical supply company in the coming weeks.
With his forward thinking, Albert hopes to convince the managers who will be interviewing him that he is right for the job.
The company may start to earn back the trust of its customer base by following Albert's suggestion regarding which handling procedure?
A. Access
B. Escalation
C. Correction
D. Data Integrity
Answer: D (LEAVE A REPLY)

NEW QUESTION: 41
Which of the following is NOT typically a function of a Privacy Officer?
A. Responding to information access requests from the public.
B. Serving as an interdepartmental liaison for privacy concerns.
C. Managing an organization's information security infrastructure.
D. Monitoring an organization's compliance with privacy laws.
Answer: (SHOW ANSWER)

NEW QUESTION: 42
SCENARIO
Please use the following to answer the next QUESTION:

For 15 years, Albert has worked at Treasure Box - a mail order company in the United States (U.S.) that used to sell decorative candles around the world, but has recently decided to limit its shipments to customers in the 48 contiguous states. Despite his years of experience, Albert is often overlooked for managerial positions. His frustration about not being promoted, coupled with his recent interest in issues of privacy protection, have motivated Albert to be an agent of positive change.

He will soon interview for a newly advertised position, and during the interview, Albert plans on making executives aware of lapses in the company's privacy program. He feels certain he will be rewarded with a promotion for preventing negative consequences resulting from the company's outdated policies and procedures.

For example, Albert has learned about the AICPA (American Institute of Certified Public Accountans)/CICA (Canadian Institute of Chartered Accountants) Privacy Maturity Model (PMM). Albert thinks the model is a useful way to measure Treasure Box's ability to protect personal dat a. Albert has noticed that Treasure Box fails to meet the requirements of the highest level of maturity of this model; at his interview, Albert will pledge to assist the company with meeting this level in order to provide customers with the most rigorous security available.

Albert does want to show a positive outlook during his interview. He intends to praise the company's commitment to the security of customer and employee personal data against external threats. However, Albert worries about the high turnover rate within the company, particularly in the area of direct phone marketing. He sees many unfamiliar faces every day who are hired to do the marketing, and he often hears complaints in the lunch room regarding long hours and low pay, as well as what seems to be flagrant disregard for company procedures.

In addition, Treasure Box has had two recent security incidents. The company has responded to the incidents with internal audits and updates to security safeguards. However, profits still seem to be affected and anecdotal evidence indicates that many people still harbor mistrust. Albert wants to help the company recover. He knows there is at least one incident the public in unaware of, although Albert does not know the details. He believes the company's insistence on keeping the incident a secret could be a further detriment to its reputation. One further way that Albert wants to help Treasure Box regain its stature is by creating a toll-free number for customers, as well as a more efficient procedure for responding to customer concerns by postal mail.

In addition to his suggestions for improvement, Albert believes that his knowledge of the company's recent business maneuvers will also impress the interviewers. For example, Albert is aware of the company's intention to acquire a medical supply company in the coming weeks.

With his forward thinking, Albert hopes to convince the managers who will be interviewing him that he is right for the job.

What is one important factor that Albert fails to consider regarding Treasure Box's response to their recent security incident?

A. How data at the company is collected

B. How long data at the company is kept

C. Who has access to the data

D. What the nature of the data is

Answer: B (LEAVE A REPLY)

NEW QUESTION: 43

SCENARIO

Please use the following to answer the next question:

Martin Briseno is the director of human resources at the Canyon City location of the U.S. hotel chain Pacific Suites. In 1998, Briseno decided to change the hotel's on-the-job mentoring model to a standardized training program for employees who were progressing from line positions into supervisory positions. He developed a curriculum comprising a series of lessons, scenarios, and assessments, which was delivered in-person to small groups. Interest in the training increased, leading Briseno to work with corporate HR specialists and software engineers to offer the program in an online format. The online program saved the cost of a trainer and allowed participants to work through the material at their own pace.

Upon hearing about the success of Briseno's program, Pacific Suites corporate Vice President Maryanne Silva-Hayes expanded the training and offered it company-wide. Employees who completed the program received certification as a Pacific Suites Hospitality Supervisor. By 2001, the program had grown to provide industry-wide training. Personnel at hotels across the country could sign up and pay to take the course online.

As the program became increasingly profitable, Pacific Suites developed an offshoot business, Pacific Hospitality Training (PHT). The sole focus of PHT was developing and marketing a variety of online courses and course progressions providing a number of professional certifications in the hospitality industry.

By setting up a user account with PHT, course participants could access an information library, sign up for courses, and take end-of-course certification tests. When a user opened a new account, all information was saved by default, including the user's name, date of birth, contact information, credit card information, employer, and job title. The registration page offered an opt-out choice that users could click to not have their credit card numbers saved. Once a user name and password were established, users could return to check their course status, review and reprint their certifications, and sign up and pay for new courses. Between 2002 and

2008, PHT issued more than 700,000 professional certifications.

PHT's profits declined in 2009 and 2010, the victim of industry downsizing and increased competition from e-learning providers. By 2011, Pacific Suites was out of the online certification business and PHT was dissolved.

The training program's systems and records remained in Pacific Suites' digital archives, un-accessed and unused. Briseno and Silva-Hayes moved on to work for other companies, and there was no plan for handling the archived data after the program ended. After PHT was dissolved, Pacific Suites executives turned their attention to crucial day-to-day operations. They planned to deal with the PHT materials once resources allowed.

In 2012, the Pacific Suites computer network was hacked. Malware installed on the online reservation system exposed the credit card information of hundreds of hotel guests. While targeting the financial data on the reservation site, hackers also discovered the archived training course data and registration accounts of Pacific Hospitality Training's customers. The result of the hack was the exfiltration of the credit card numbers of recent hotel guests and the exfiltration of the PHT database with all its contents.

A Pacific Suites systems analyst discovered the information security breach in a routine scan of activity reports. Pacific Suites quickly notified credit card companies and recent hotel guests of the breach, attempting to prevent serious harm. Technical security engineers faced a challenge in dealing with the PHT data.
PHT course administrators and the IT engineers did not have a system for tracking, cataloguing, and storing information. Pacific Suites has procedures in place for data access and storage, but those procedures were not implemented when PHT was formed. When the PHT database was acquired by Pacific Suites, it had no owner or oversight. By the time technical security engineers determined what private information was compromised, at least 8,000 credit card holders were potential victims of fraudulent activity.
In the Information Technology engineers had originally set the default for customer credit card information to "Do Not Save," this action would have been in line with what concept?
A. Reactive risk management
B. Use limitation
C. Harm minimization
D. Privacy by Design
Answer: D (LEAVE A REPLY)

NEW QUESTION: 44
SCENARIO
Please use the following to answer the next QUESTION:
Manasa is a product manager at Omnipresent Omnimedia, where she is responsible for leading the development of the company's flagship product, the Handy Helper. The Handy Helper is an application that can be used in the home to manage family calendars, do online shopping, and schedule doctor appointments. After having had a successful launch in the United States, the Handy Helper is about to be made available for purchase worldwide.
The packaging and user guide for the Handy Helper indicate that it is a "privacy friendly" product suitable for the whole family, including children, but does not provide any further detail or privacy notice. In order to use the application, a family creates a single account, and the primary user has access to all information about the other users. Upon start up, the primary user must check a box consenting to receive marketing emails from Omnipresent Omnimedia and selected marketing partners in order to be able to use the application.
Sanjay, the head of privacy at Omnipresent Omnimedia, was working on an agreement with a European distributor of Handy Helper when he fielded many Questions about the product from the distributor. Sanjay needed to look more closely at the product in order to be able to answer the Questions as he was not involved in the product development process.
In speaking with the product team, he learned that the Handy Helper collected and stored all of a user's sensitive medical information for the medical appointment scheduler. In fact, all of the user's information is stored by Handy Helper for the additional purpose of creating additional products and to analyze usage of the product. This data is all stored in the cloud and is encrypted both during transmission and at rest.
Consistent with the CEO's philosophy that great new product ideas can come from anyone, all Omnipresent Omnimedia employees have access to user data under a program called Eureka. Omnipresent Omnimedia is hoping that at some point in the future, the data will reveal insights that could be used to create a fully

automated application that runs on artificial intelligence, but as of yet, Eureka is not well-defined and is considered a long-term goal.
What administrative safeguards should be implemented to protect the collected data while in use by Manasa and her product management team?
A. Document the data flows for the collected data.
B. Conduct a Privacy Impact Assessment (PIA) to evaluate the risks involved.
C. Implement a policy restricting data access on a "need to know" basis.
D. Limit data transfers to the US by keeping data collected in Europe within a local data center.
Answer: C (LEAVE A REPLY)
Explanation
An administrative safeguard that should be implemented to protect the collected data while in use by Manasa and her product management team is a policy restricting data access on a "need to know" basis. This means that only authorized personnel who have a legitimate business purpose for accessing the data should be able to do so3 This would help to prevent unauthorized or unnecessary access, use, or disclosure of sensitive or personal data by internal or external parties. It would also reduce the risk of data breaches, theft, or loss that could compromise the confidentiality, integrity, and availability of the data4 References: 3: HIPAA Security Series #2 - Administrative Safeguards - HHS.gov; 4: Administrative Safeguards of the Security Rule: What Are They?

NEW QUESTION: 45
SCENARIO
Please use the following to answer the next QUESTION:
Amira is thrilled about the sudden expansion of NatGen. As the joint Chief Executive Officer (CEO) with her long-time business partner Sadie, Amira has watched the company grow into a major competitor in the green energy market. The current line of products includes wind turbines, solar energy panels, and equipment for geothermal systems. A talented team of developers means that NatGen's line of products will only continue to grow.
With the expansion, Amira and Sadie have received advice from new senior staff members brought on to help manage the company's growth. One recent suggestion has been to combine the legal and security functions of the company to ensure observance of privacy laws and the company's own privacy policy. This sounds overly complicated to Amira, who wants departments to be able to use, collect, store, and dispose of customer data in ways that will best suit their needs. She does not want administrative oversight and complex structuring to get in the way of people doing innovative work.
Sadie has a similar outlook. The new Chief Information Officer (CIO) has proposed what Sadie believes is an unnecessarily long timetable for designing a new privacy program. She has assured him that NatGen will use the best possible equipment for electronic storage of customer and employee data. She simply needs a list of equipment and an estimate of its cost. But the CIO insists that many issues are necessary to consider before the company gets to that stage.
Regardless, Sadie and Amira insist on giving employees space to do their jobs. Both CEOs want to entrust the monitoring of employee policy compliance to low-level managers. Amira and Sadie believe these managers can adjust the company privacy policy according to what works best for their particular

departments. NatGen's CEOs know that flexible interpretations of the privacy policy in the name of promoting green energy would be highly unlikely to raise any concerns with their customer base, as long as the data is always used in course of normal business activities.
Perhaps what has been most perplexing to Sadie and Amira has been the CIO's recommendation to institute a privacy compliance hotline. Sadie and Amira have relented on this point, but they hope to compromise by allowing employees to take turns handling reports of privacy policy violations. The implementation will be easy because the employees need no special preparation. They will simply have to document any concerns they hear.
Sadie and Amira are aware that it will be challenging to stay true to their principles and guard against corporate culture strangling creativity and employee morale. They hope that all senior staff will see the benefit of trying a unique approach.
What Data Lifecycle Management (DLM) principle should the company follow if they end up allowing departments to interpret the privacy policy differently?
A. Create categories to reflect degrees of data importance.
B. Adequately document reasons for inconsistencies.
C. Prove the authenticity of the company's records.
D. Arrange for official credentials for staff members.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 46
When conducting due diligence during an acquisition, what should a privacy professional avoid?
A. Discussing with the acquired company the type and scope of their data processing.
B. Allowing legal in both companies to handle the privacy laws and compliance.
C. Planning for impacts on the data processing operations post-acquisition.
D. Benchmarking the two Companies privacy policies against one another.
Answer: B (LEAVE A REPLY)
Explanation
When conducting due diligence during an acquisition, a privacy professional should avoid allowing legal in both companies to handle the privacy laws and compliance. This is because legal teams may not have the expertise or the resources to address all the privacy issues and risks that may arise from the acquisition. A privacy professional should be involved in the due diligence process to ensure that the privacy policies, practices, and obligations of both companies are aligned and compliant with the applicable laws and regulations. The other options are not things that a privacy professional should avoid, but rather things that they should do as part of the due diligence process. References: CIPM Body of Knowledge, Domain V: Privacy Program Management, Section A: Privacy Program Administration, Subsection 3: Due Diligence.

NEW QUESTION: 47
SCENARIO
Please use the following to answer the next QUESTION:
Ben works in the IT department of IgNight, Inc., a company that designs lighting solutions for its clients. Although IgNight's customer base consists primarily of offices in the US, some individuals have been so impressed by the unique aesthetic and energy-saving design of the light fixtures that they have requested IgNight's installations in their homes across the globe.
One Sunday morning, while using his work laptop to purchase tickets for an upcoming music festival, Ben happens to notice some unusual user activity on company files. From a cursory review, all the data still appears to be where it is meant to be but he can't shake off the feeling that something is not right. He knows that it is a possibility that this could be a colleague performing unscheduled maintenance, but he recalls an email from his company's security team reminding employees to be on alert for attacks from a known group of malicious actors specifically targeting the industry.
Ben is a diligent employee and wants to make sure that he protects the company but he does not want to bother his hard-working colleagues on the weekend. He is going to discuss the matter with this manager first thing in the morning but wants to be prepared so he can demonstrate his knowledge in this area and plead his case for a promotion.
To determine the steps to follow, what would be the most appropriate internal guide for Ben to review?
A. Business Continuity and Disaster Recovery Plan.
B. Code of Business Conduct.
C. IT Systems and Operations Handbook.
D. Incident Response Plan.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 48
SCENARIO
Please use the following to answer the next question:
Paul Daniels, with years of experience as a CEO, is worried about his son Carlton's successful venture, Gadgo.
A technological innovator in the communication industry that quickly became profitable, Gadgo has moved beyond its startup phase. While it has retained its vibrant energy, Paul fears that under Carlton's direction, the company may not be taking its risks or obligations as seriously as it needs to. Paul has hired you, a privacy Consultant, to assess the company and report to both father and son. "Carlton won't listen to me," Paul says, "but he may pay attention to an expert." Gadgo's workplace is a clubhouse for innovation, with games, toys, snacks, espresso machines, giant fish tanks and even an iguana who regards you with little interest. Carlton, too, seems bored as he describes to you the company's procedures and technologies for data protection. It's a loose assemblage of controls, lacking consistency and with plenty of weaknesses. "This is a technology company," Carlton says. "We create. We innovate. I don't want unnecessary measures that will only slow

people down and clutter their thoughts." The meeting lasts until early evening. Upon leaving, you walk through the office. It looks as if a strong windstorm has recently blown through, with papers scattered across desks and tables and even the floor. A
"cleaning crew" of one teenager is emptying the trash bins. A few computers have been left on for the night; others are missing. Carlton takes note of your attention to this: "Most of my people take their laptops home with them, or use their own tablets or phones. I want them to use whatever helps them to think and be ready day or night for that great insight. It may only come once!" What phase in the Privacy Maturity Model (PMM) does Gadgo's privacy program best exhibit?
A. Repeatable
B. Managed
C. Ad hoc
D. Defined
Answer: C (LEAVE A REPLY)

NEW QUESTION: 49
SCENARIO
Please use the following to answer the next QUESTION:
Edufox has hosted an annual convention of users of its famous e-learning software platform, and over time, it has become a grand event. It fills one of the large downtown conference hotels and overflows into the others, with several thousand attendees enjoying three days of presentations, panel discussions and networking. The convention is the centerpiece of the company's product rollout schedule and a great training opportunity for current users. The sales force also encourages prospective clients to attend to get a better sense of the ways in which the system can be customized to meet diverse needs and understand that when they buy into this system, they are joining a community that feels like family.
This year's conference is only three weeks away, and you have just heard news of a new initiative supporting it: a smartphone app for attendees. The app will support late registration, highlight the featured presentations and provide a mobile version of the conference program. It also links to a restaurant reservation system with the best cuisine in the areas featured. "It's going to be great," the developer, Deidre Hoffman, tells you, "if, that is, we actually get it working!" She laughs nervously but explains that because of the tight time frame she'd been given to build the app, she outsourced the job to a local firm. "It's just three young people," she says, "but they do great work." She describes some of the other apps they have built. When asked how they were selected for this job, Deidre shrugs. "They do good work, so I chose them." Deidre is a terrific employee with a strong track record. That's why she's been charged to deliver this rushed project. You're sure she has the best interests of the company at heart, and you don't doubt that she's under pressure to meet a deadline that cannot be pushed back. However, you have concerns about the app's handling of personal data and its security safeguards. Over lunch in the break room, you start to talk to her about it, but she quickly tries to reassure you, "I'm sure with your help we can fix any security issues if we have to, but I doubt there'll be any. These people build apps for a living, and they know what they're doing. You worry too much, but that's why you're so good at your job!" Which is the best first step in understanding the data security practices of a potential vendor?

A. Requiring the vendor to complete a questionnaire assessing International Organization for Standardization (ISO) 27001 compliance.
B. Conducting a physical audit of the vendor's facilities.
C. Conducting a penetration test of the vendor's data security structure.
D. Examining investigation records of any breaches the vendor has experienced.
Answer: (SHOW ANSWER)
Explanation
This answer is the best first step in understanding the data security practices of a potential vendor, as it can provide a quick and easy way to evaluate the vendor's alignment with a widely recognized and respected standard for information security management systems (ISMS). Requiring the vendor to complete a questionnaire assessing ISO 27001 compliance can help you to obtain relevant and consistent information about the vendor's data security policies, objectives, risks, controls, processes and performance. The questionnaire can also help you to compare different vendors based on their level of compliance and identify any areas that need further clarification or verification. References: IAPP CIPM Study Guide, page 82; ISO/IEC 27002:2013, section 15.1.2

NEW QUESTION: 50
When building a data privacy program, what is a good starting point to understand the scope of privacy program needs?
A. Perform Data Protection Impact Assessments (DPIAs).
B. Perform Risk Assessments
C. Complete a Data Inventory.
D. Review Audits.
Answer: (SHOW ANSWER)
Explanation
A data inventory is a good starting point to understand the scope of privacy program needs, as it provides a comprehensive overview of what personal data is collected, processed, stored, shared, and disposed of by the organization. A data inventory can help identify the legal obligations, risks, and gaps in the privacy program, as well as the opportunities for improvement and optimization. The other options are also important components of a privacy program, but they are more effective when based on a data inventory. References: CIPM Body of Knowledge, Domain II: Privacy Program Operational Life Cycle, Task
1: Assess the current state of the privacy program.

NEW QUESTION: 51
SCENARIO
Please use the following to answer the next QUESTION:
Manasa is a product manager at Omnipresent Omnimedia, where she is responsible for leading the development of the company's flagship product, the Handy Helper. The Handy Helper is an application that can be used in the home to manage family calendars, do online shopping, and schedule doctor appointments. After having had a successful launch in the United States, the Handy Helper is about to be made available for purchase worldwide.

The packaging and user guide for the Handy Helper indicate that it is a "privacy friendly" product suitable for the whole family, including children, but does not provide any further detail or privacy notice. In order to use the application, a family creates a single account, and the primary user has access to all information about the other users. Upon start up, the primary user must check a box consenting to receive marketing emails from Omnipresent Omnimedia and selected marketing partners in order to be able to use the application.
Sanjay, the head of privacy at Omnipresent Omnimedia, was working on an agreement with a European distributor of Handy Helper when he fielded many Questions about the product from the distributor. Sanjay needed to look more closely at the product in order to be able to answer the Questions as he was not involved in the product development process.
In speaking with the product team, he learned that the Handy Helper collected and stored all of a user's sensitive medical information for the medical appointment scheduler. In fact, all of the user's information is stored by Handy Helper for the additional purpose of creating additional products and to analyze usage of the product. This data is all stored in the cloud and is encrypted both during transmission and at rest.
Consistent with the CEO's philosophy that great new product ideas can come from anyone, all Omnipresent Omnimedia employees have access to user data under a program called Eureka. Omnipresent Omnimedia is hoping that at some point in the future, the data will reveal insights that could be used to create a fully automated application that runs on artificial intelligence, but as of yet, Eureka is not well-defined and is considered a long-term goal.
What element of the Privacy by Design (PbD) framework might the Handy Helper violate?
A. Failure to obtain opt-in consent to marketing.
B. Failure to observe data localization requirements.
C. Failure to implement the least privilege access standard.
D. Failure to integrate privacy throughout the system development life cycle.
Answer: (SHOW ANSWER)
Explanation
The Handy Helper might violate the element of the Privacy by Design (PbD) framework that requires integrating privacy throughout the system development life cycle. According to the PbD framework, privacy should be embedded into the design and architecture of IT systems and business practices, not added as an afterthought1 This means that privacy should be considered at every stage of the system development life cycle, from planning to analysis to design to development to implementation to maintenance2 However, the Handy Helper seems to have been developed without involving Sanjay, the head of privacy, or conducting a privacy impact assessment (PIA) to identify and mitigate potential privacy risks3 The product also lacks a clear and transparent privacy notice that informs users about what data is collected, how it is used, where it is stored, who has access to it, and what choices they have4 These issues could expose the product to legal and reputational challenges, especially in regions with strict data protection regulations, such as Europe.
References: 1: Privacy by Design - The LIFE Institute; 2: System Development Life Cycle - GeeksforGeeks; 3: [Privacy Impact Assessment (PIA) | NZ Digital government]; 4: [Privacy Notices under EU Data Protection Law | Privacy International]

NEW QUESTION: 52
SCENARIO

Please use the following to answer the next QUESTION:
As the Director of data protection for Consolidated Records Corporation, you are justifiably pleased with your accomplishments so far. Your hiring was precipitated by warnings from regulatory agencies following a series of relatively minor data breaches that could easily have been worse. However, you have not had a reportable incident for the three years that you have been with the company. In fact, you consider your program a model that others in the data storage industry may note in their own program development.
You started the program at Consolidated from a jumbled mix of policies and procedures and worked toward coherence across departments and throughout operations. You were aided along the way by the program's sponsor, the vice president of operations, as well as by a Privacy Team that started from a clear understanding of the need for change.
Initially, your work was greeted with little confidence or enthusiasm by the company's "old guard" among both the executive team and frontline personnel working with data and interfacing with clients. Through the use of metrics that showed the costs not only of the breaches that had occurred, but also projections of the costs that easily could occur given the current state of operations, you soon had the leaders and key decision-makers largely on your side. Many of the other employees were more resistant, but face-to-face meetings with each department and the development of a baseline privacy training program achieved sufficient "buy-in" to begin putting the proper procedures into place.
Now, privacy protection is an accepted component of all current operations involving personal or protected data and must be part of the end product of any process of technological development. While your approach is not systematic, it is fairly effective.
You are left contemplating:
What must be done to maintain the program and develop it beyond just a data breach prevention program?
How can you build on your success?
What are the next action steps?
What process could most effectively be used to add privacy protections to a new, comprehensive program being developed at Consolidated?
A. Privacy by Design.
B. Innovation Privacy Standards.
C. Information Security Planning.
D. Privacy Step Assessment.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 53
SCENARIO
Please use the following to answer the next QUESTION:
Martin Briseno is the director of human resources at the Canyon City location of the U.S. hotel chain Pacific Suites. In 1998, Briseno decided to change the hotel's on-the-job mentoring model to a standardized training program for employees who were progressing from line positions into supervisory positions. He developed a curriculum comprising a series of lessons, scenarios, and assessments, which was delivered in-person to small groups. Interest in the training increased, leading Briseno to work with corporate HR specialists and

software engineers to offer the program in an online format. The online program saved the cost of a trainer and allowed participants to work through the material at their own pace.

Upon hearing about the success of Briseno's program, Pacific Suites corporate Vice President Maryanne Silva-Hayes expanded the training and offered it company-wide. Employees who completed the program received certification as a Pacific Suites Hospitality Supervisor. By 2001, the program had grown to provide industry-wide training. Personnel at hotels across the country could sign up and pay to take the course online.

As the program became increasingly profitable, Pacific Suites developed an offshoot business, Pacific Hospitality Training (PHT). The sole focus of PHT was developing and marketing a variety of online courses and course progressions providing a number of professional certifications in the hospitality industry.

By setting up a user account with PHT, course participants could access an information library, sign up for courses, and take end-of-course certification tests. When a user opened a new account, all information was saved by default, including the user's name, date of birth, contact information, credit card information, employer, and job title. The registration page offered an opt-out choice that users could click to not have their credit card numbers saved. Once a user name and password were established, users could return to check their course status, review and reprint their certifications, and sign up and pay for new courses. Between 2002 and

2008, PHT issued more than 700,000 professional certifications.

PHT's profits declined in 2009 and 2010, the victim of industry downsizing and increased competition from e-learning providers. By 2011, Pacific Suites was out of the online certification business and PHT was dissolved.

The training program's systems and records remained in Pacific Suites' digital archives, un-accessed and unused. Briseno and Silva-Hayes moved on to work for other companies, and there was no plan for handling the archived data after the program ended. After PHT was dissolved, Pacific Suites executives turned their attention to crucial day-to-day operations. They planned to deal with the PHT materials once resources allowed.

In 2012, the Pacific Suites computer network was hacked. Malware installed on the online reservation system exposed the credit card information of hundreds of hotel guests. While targeting the financial data on the reservation site, hackers also discovered the archived training course data and registration accounts of Pacific Hospitality Training's customers. The result of the hack was the exfiltration of the credit card numbers of recent hotel guests and the exfiltration of the PHT database with all its contents.

A Pacific Suites systems analyst discovered the information security breach in a routine scan of activity reports. Pacific Suites quickly notified credit card companies and recent hotel guests of the breach, attempting to prevent serious harm. Technical security engineers faced a challenge in dealing with the PHT data.

PHT course administrators and the IT engineers did not have a system for tracking, cataloguing, and storing information. Pacific Suites has procedures in place for data access and storage, but those procedures were not implemented when PHT was formed. When the PHT database was acquired by Pacific Suites, it had no owner or oversight. By the time technical security engineers determined what private information was compromised, at least 8,000 credit card holders were potential victims of fraudulent activity.

How would a strong data life cycle management policy have helped prevent the breach?

A. Information would have been categorized and assigned a deadline for destruction

B. The most sensitive information would have been immediately erased and destroyed

C. The most important information would have been regularly assessed and tested for security
D. Information would have been ranked according to importance and stored in separate locations
Answer: A (LEAVE A REPLY)

NEW QUESTION: 54
SCENARIO
Please use the following to answer the next QUESTION:
It's just what you were afraid of. Without consulting you, the information technology director at your organization launched a new initiative to encourage employees to use personal devices for conducting business. The initiative made purchasing a new, high-specification laptop computer an attractive option, with discounted laptops paid for as a payroll deduction spread over a year of paychecks. The organization is also paying the sales taxes. It's a great deal, and after a month, more than half the organization's employees have signed on and acquired new laptops. Walking through the facility, you see them happily customizing and comparing notes on their new computers, and at the end of the day, most take their laptops with them, potentially carrying personal data to their homes or other unknown locations. It's enough to give you data-protection nightmares, and you've pointed out to the information technology Director and many others in the organization the potential hazards of this new practice, including the inevitability of eventual data loss or theft.
Today you have in your office a representative of the organization's marketing department who shares with you, reluctantly, a story with potentially serious consequences. The night before, straight from work, with laptop in hand, he went to the Bull and Horn Pub to play billiards with his friends. A fine night of sport and socializing began, with the laptop "safely" tucked on a bench, beneath his jacket. Later that night, when it was time to depart, he retrieved the jacket, but the laptop was gone. It was not beneath the bench or on another bench nearby. The waitstaff had not seen it. His friends were not playing a joke on him. After a sleepless night, he confirmed it this morning, stopping by the pub to talk to the cleanup crew. They had not found it. The laptop was missing. Stolen, it seems. He looks at you, embarrassed and upset.
You ask him if the laptop contains any personal data from clients, and, sadly, he nods his head, yes. He believes it contains files on about 100 clients, including names, addresses and governmental identification numbers. He sighs and places his head in his hands in despair.
In order to determine the best course of action, how should this incident most productively be viewed?
A. As the accidental loss of personal property containing data that must be restored.
B. As a potential compromise of personal information through unauthorized access.
C. As an incident that requires the abrupt initiation of a notification campaign.
D. As the premeditated theft of company data, until shown otherwise.
Answer: B (LEAVE A REPLY)
Explanation
This answer recognizes the risk of data breach that may result from the loss of the laptop, as it may expose the personal information of the clients to unauthorized or unlawful processing. A data breach is defined as a security incident that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed. A data breach may have serious consequences for the individuals whose data is compromised, such as identity theft, fraud, discrimination, financial loss or reputational damage. Therefore, it is important to view this incident as a potential compromise

of personal information and take appropriate measures to contain, assess and mitigate the impact of the breach. References: IAPP CIPM Study Guide, page 86; ISO/IEC 27002:2013, section 16.1.1

NEW QUESTION: 55
While trying to e-mail her manager, an employee has e-mailed a list of all the company's customers, including their bank details, to an employee with the same name at a different company. Which of the following would be the first stage in the incident response plan under the General Data Protection Regulation (GDPR)?
A. Notification to data subjects.
B. Containment of impact of breach.
C. Remediation offers to data subjects.
D. Notification to the Information Commissioner's Office (ICO).
Answer: (SHOW ANSWER)
Explanation
The first stage in the incident response plan under the General Data Protection Regulation (GDPR) for this scenario would be to contain the impact of the breach. This means taking immediate action to stop the unauthorized access or disclosure of personal data, and to prevent it from happening again in the future. This could involve revoking access to the data, notifying the employee who mistakenly sent the data, and implementing security measures to prevent similar breaches from occurring in the future.
References:
* https://gdpr-info.eu/art-33-gdpr/
* https://gdpr-info.eu/art-34-gdpr/

NEW QUESTION: 56
Rationalizing requirements in order to comply with the various privacy requirements required by applicable law and regulation does NOT include which of the following?
A. Implementing a solution that significantly addresses shared obligations and privacy rights.
B. Harmonizing shared obligations and privacy rights across varying legislation and/or regulators.
C. Addressing requirements that fall outside the common obligations and rights (outliers) on a case-by-case basis.
D. Applying the strictest standard for obligations and privacy rights that doesn't violate privacy laws elsewhere.
Answer: (SHOW ANSWER)

NEW QUESTION: 57
SCENARIO
Please use the following to answer the next QUESTION:
As the Director of data protection for Consolidated Records Corporation, you are justifiably pleased with your accomplishments so far. Your hiring was precipitated by warnings from regulatory agencies following a series of relatively minor data breaches that could easily have been worse. However, you have not had a reportable incident for the three years that you have been with the company. In fact, you consider your program a model that others in the data storage industry may note in their own program development.

You started the program at Consolidated from a jumbled mix of policies and procedures and worked toward coherence across departments and throughout operations. You were aided along the way by the program's sponsor, the vice president of operations, as well as by a Privacy Team that started from a clear understanding of the need for change.
Initially, your work was greeted with little confidence or enthusiasm by the company's "old guard" among both the executive team and frontline personnel working with data and interfacing with clients. Through the use of metrics that showed the costs not only of the breaches that had occurred, but also projections of the costs that easily could occur given the current state of operations, you soon had the leaders and key decision-makers largely on your side. Many of the other employees were more resistant, but face-to-face meetings with each department and the development of a baseline privacy training program achieved sufficient "buy-in" to begin putting the proper procedures into place.
Now, privacy protection is an accepted component of all current operations involving personal or protected data and must be part of the end product of any process of technological development. While your approach is not systematic, it is fairly effective.
You are left contemplating:
What must be done to maintain the program and develop it beyond just a data breach prevention program?
How can you build on your success?
What are the next action steps?
What process could most effectively be used to add privacy protections to a new, comprehensive program being developed at Consolidated?
A. Privacy by Design.
B. Privacy Step Assessment.
C. Information Security Planning.
D. Innovation Privacy Standards.
Answer: A (LEAVE A REPLY)
Explanation
This is a process that embeds privacy protections into the design and development of new technologies, systems, products or services that involve personal data. It ensures that privacy is considered at every stage of the development process, from conception to completion, and that the privacy principles are integrated into the core functionality of the program.

NEW QUESTION: 58
SCENARIO
Please use the following to answer the next QUESTION:
Perhaps Jack Kelly should have stayed in the U.S. He enjoys a formidable reputation inside the company, Special Handling Shipping, for his work in reforming certain "rogue" offices. Last year, news broke that a police sting operation had revealed a drug ring operating in the Providence, Rhode Island office in the United States. Video from the office's video surveillance cameras leaked to news operations showed a drug exchange between Special Handling staff and undercover officers.
In the wake of this incident, Kelly had been sent to Providence to change the "hands off" culture that upper management believed had let the criminal elements conduct their illicit transactions. After a few weeks under

Kelly's direction, the office became a model of efficiency and customer service. Kelly monitored his workers' activities using the same cameras that had recorded the illegal conduct of their former co-workers.
Now Kelly has been charged with turning around the office in Cork, Ireland, another trouble spot. The company has received numerous reports of the staff leaving the office unattended. When Kelly arrived, he found that even when present, the staff often spent their days socializing or conducting personal business on their mobile phones. Again, he observed their behaviors using surveillance cameras. He issued written reprimands to six staff members based on the first day of video alone.
Much to Kelly's surprise and chagrin, he and the company are now under investigation by the Data Protection Commissioner of Ireland for allegedly violating the privacy rights of employees. Kelly was told that the company's license for the cameras listed facility security as their main use, but he does not know why this matters. He has pointed out to his superiors that the company's training programs on privacy protection and data collection mention nothing about surveillance video.
You are a privacy protection consultant, hired by the company to assess this incident, report on the legal and compliance issues, and recommend next steps.
What does this example best illustrate about training requirements for privacy protection?
A. Training needs must be weighed against financial costs.
B. Training on local laws must be implemented for all personnel.
C. Training must be repeated frequently to respond to new legislation.
D. Training must include assessments to verify that the material is mastered.
Answer: B (LEAVE A REPLY)
Explanation
This answer is the best way to illustrate the training requirements for privacy protection, as it shows the importance of understanding and complying with the different legal and regulatory frameworks that apply to the organization's data processing activities in different jurisdictions. Training on local laws must be implemented for all personnel who are involved in or responsible for collecting, using, disclosing, storing or transferring personal data across borders, as they may face different obligations and restrictions depending on the nature and location of the data and the data subjects. Training on local laws can help to prevent or mitigate the risks of violating the privacy rights of individuals, facing legal actions, fines, sanctions or investigations from authorities, or losing trust and reputation among customers, partners and stakeholders.
References: IAPP CIPM Study Guide, page 901; ISO/IEC 27002:2013, section 7.2.2

NEW QUESTION: 59
Which of the following is NOT a type of privacy program metric?
A. Business enablement metrics.
B. Data enhancement metrics.
C. Value creation metrics.
D. Risk-reduction metrics.
Answer: B (LEAVE A REPLY)
Explanation
Data enhancement metrics are not a type of privacy program metric because they do not measure the performance, value, or risk of the privacy program. Data enhancement metrics are related to the quality,

accuracy, and completeness of the data collected and processed by the organization, which are not directly linked to the privacy program objectives. References: CIPM Body of Knowledge, Domain II: Privacy Program Governance, Section B: Establishing a Privacy Program Framework, Subsection 2: Privacy Program Metrics.

NEW QUESTION: 60
Which of the following is NOT a type of privacy program metric?
A. Data enhancement metrics.
B. Value creation metrics.
C. Business enablement metrics.
D. Risk-reduction metrics.
Answer: (SHOW ANSWER)

NEW QUESTION: 61
Which of the following actions is NOT required during a data privacy diligence process for Merger & Acquisition (M&A) deals?
A. Revise inventory of applications that house personal data and data mapping.
B. Perform a privacy readiness assessment before the deal.
C. Update business processes to handle Data Subject Requests (DSRs).
D. Compare the original use of personal data to post-merger use.
Answer: (SHOW ANSWER)

NEW QUESTION: 62
SCENARIO
Please use the following to answer the next QUESTION:
Amira is thrilled about the sudden expansion of NatGen. As the joint Chief Executive Officer (CEO) with her long-time business partner Sadie, Amira has watched the company grow into a major competitor in the green energy market. The current line of products includes wind turbines, solar energy panels, and equipment for geothermal systems. A talented team of developers means that NatGen's line of products will only continue to grow.
With the expansion, Amira and Sadie have received advice from new senior staff members brought on to help manage the company's growth. One recent suggestion has been to combine the legal and security functions of the company to ensure observance of privacy laws and the company's own privacy policy. This sounds overly complicated to Amira, who wants departments to be able to use, collect, store, and dispose of

customer data in ways that will best suit their needs. She does not want administrative oversight and complex structuring to get in the way of people doing innovative work.
Sadie has a similar outlook. The new Chief Information Officer (CIO) has proposed what Sadie believes is an unnecessarily long timetable for designing a new privacy program. She has assured him that NatGen will use the best possible equipment for electronic storage of customer and employee data. She simply needs a list of equipment and an estimate of its cost. But the CIO insists that many issues are necessary to consider before the company gets to that stage.
Regardless, Sadie and Amira insist on giving employees space to do their jobs. Both CEOs want to entrust the monitoring of employee policy compliance to low-level managers. Amira and Sadie believe these managers can adjust the company privacy policy according to what works best for their particular departments. NatGen's CEOs know that flexible interpretations of the privacy policy in the name of promoting green energy would be highly unlikely to raise any concerns with their customer base, as long as the data is always used in course of normal business activities.
Perhaps what has been most perplexing to Sadie and Amira has been the CIO's recommendation to institute a privacy compliance hotline. Sadie and Amira have relented on this point, but they hope to compromise by allowing employees to take turns handling reports of privacy policy violations. The implementation will be easy because the employees need no special preparation. They will simply have to document any concerns they hear.
Sadie and Amira are aware that it will be challenging to stay true to their principles and guard against corporate culture strangling creativity and employee morale. They hope that all senior staff will see the benefit of trying a unique approach.
What is the most likely reason the Chief Information Officer (CIO) believes that generating a list of needed IT equipment is NOT adequate?
A. Senior staff members need to first commit to adopting a minimum number of Privacy Enhancing Technologies (PETs).
B. The company needs to have policies and procedures in place to guide the purchasing decisions.
C. Staff members across departments need time to review technical information concerning any new databases.
D. The privacy notice for customers and the Business Continuity Plan (BCP) still need to be reviewed.
Answer: (SHOW ANSWER)

NEW QUESTION: 63
SCENARIO
Please use the following to answer the next QUESTION:
As the Director of data protection for Consolidated Records Corporation, you are justifiably pleased with your accomplishments so far. Your hiring was precipitated by warnings from regulatory agencies following a series of relatively minor data breaches that could easily have been worse. However, you have not had a reportable incident for the three years that you have been with the company. In fact, you consider your program a model that others in the data storage industry may note in their own program development.
You started the program at Consolidated from a jumbled mix of policies and procedures and worked toward coherence across departments and throughout operations. You were aided along the way by the program's

sponsor, the vice president of operations, as well as by a Privacy Team that started from a clear understanding of the need for change.
Initially, your work was greeted with little confidence or enthusiasm by the company's "old guard" among both the executive team and frontline personnel working with data and interfacing with clients. Through the use of metrics that showed the costs not only of the breaches that had occurred, but also projections of the costs that easily could occur given the current state of operations, you soon had the leaders and key decision-makers largely on your side. Many of the other employees were more resistant, but face-to-face meetings with each department and the development of a baseline privacy training program achieved sufficient "buy-in" to begin putting the proper procedures into place.
Now, privacy protection is an accepted component of all current operations involving personal or protected data and must be part of the end product of any process of technological development. While your approach is not systematic, it is fairly effective.
You are left contemplating:
What must be done to maintain the program and develop it beyond just a data breach prevention program?
How can you build on your success?
What are the next action steps?
What stage of the privacy operational life cycle best describes Consolidated's current privacy program?
A. Protect.
B. Sustain.
C. Respond.
D. Assess.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 64
SCENARIO
Please use the following to answer the next QUESTION:
Penny has recently joined Ace Space, a company that sells homeware accessories online, as its new privacy officer. The company is based in California but thanks to some great publicity from a social media influencer last year, the company has received an influx of sales from the EU and has set up a regional office in Ireland to support this expansion. To become familiar with Ace Space's practices and assess what her privacy priorities will be, Penny has set up meetings with a number of colleagues to hear about the work that they have been doing and their compliance efforts.
Penny's colleague in Marketing is excited by the new sales and the company's plans, but is also concerned that Penny may curtail some of the growth opportunities he has planned. He tells her "I heard someone in the breakroom talking about some new privacy laws but I really don't think it affects us. We're just a small company. I mean we just sell accessories online, so what's the real risk?" He has also told her that he works with a number of small companies that help him get projects completed in a hurry. "We've got to meet our deadlines otherwise we lose money. I just sign the contracts and get Jim in finance to push through the payment. Reviewing the contracts takes time that we just don't have." In her meeting with a member of the IT team, Penny has learned that although Ace Space has taken a number of precautions to protect its website from malicious activity, it has not taken the same level of care of its physical files or internal infrastructure.

Penny's colleague in IT has told her that a former employee lost an encrypted USB key with financial data on it when he left. The company nearly lost access to their customer database last year after they fell victim to a phishing attack. Penny is told by her IT colleague that the IT team
"didn't know what to do or who should do what. We hadn't been trained on it but we're a small team though, so it worked out OK in the end." Penny is concerned that these issues will compromise Ace Space's privacy and data protection.
Penny is aware that the company has solid plans to grow its international sales and will be working closely with the CEO to give the organization a data "shake up". Her mission is to cultivate a strong privacy culture within the company.
Penny has a meeting with Ace Space's CEO today and has been asked to give her first impressions and an overview of her next steps.
To establish the current baseline of Ace Space's privacy maturity, Penny should consider all of the following factors EXCEPT?
A. Ace Space's documented procedures
B. Ace Space's employee training program
C. Ace Space's vendor engagement protocols
D. Ace Space's content sharing practices on social media
Answer: D (LEAVE A REPLY)
Explanation
The factor that Penny should not consider to establish the current baseline of Ace Space's privacy maturity is Ace Space's content sharing practices on social media. This is because this factor is not directly related to the privacy program elements that Penny should assess, such as leadership and organization, privacy risk management, engineering and information security, incident response, individual participation, transparency and redress, privacy training and awareness, and accountability1. The other factors are relevant to these elements and can help Penny measure the current state of Ace Space's privacy program against a recognized maturity model, such as the Privacy Capability Maturity Model (PCMM) developed by the Association of Corporate Counsel2. For example:
* Ace Space's documented procedures can help Penny evaluate the level of formalization and
* standardization of the privacy policies and practices across the organization, as well as the alignment with the applicable legal and regulatory requirements1, 2.
* Ace Space's employee training program can help Penny assess the level of awareness and competence of the staff on privacy issues and responsibilities, as well as the effectiveness and frequency of the training delivery and evaluation1, 2.
* Ace Space's vendor engagement protocols can help Penny determine the level of due diligence and oversight of the third parties that process personal data on behalf of Ace Space, as well as the contractual and technical safeguards that are in place to protect the data1, 2.

NEW QUESTION: 65
SCENARIO
Please use the following to answer the next QUESTION:

For 15 years, Albert has worked at Treasure Box - a mail order company in the United States (U.S.) that used to sell decorative candles around the world, but has recently decided to limit its shipments to customers in the 48 contiguous states. Despite his years of experience, Albert is often overlooked for managerial positions. His frustration about not being promoted, coupled with his recent interest in issues of privacy protection, have motivated Albert to be an agent of positive change.

He will soon interview for a newly advertised position, and during the interview, Albert plans on making executives aware of lapses in the company's privacy program. He feels certain he will be rewarded with a promotion for preventing negative consequences resulting from the company's outdated policies and procedures.

For example, Albert has learned about the AICPA (American Institute of Certified Public Accountans)/CICA (Canadian Institute of Chartered Accountants) Privacy Maturity Model (PMM). Albert thinks the model is a useful way to measure Treasure Box's ability to protect personal dat a. Albert has noticed that Treasure Box fails to meet the requirements of the highest level of maturity of this model; at his interview, Albert will pledge to assist the company with meeting this level in order to provide customers with the most rigorous security available.

Albert does want to show a positive outlook during his interview. He intends to praise the company's commitment to the security of customer and employee personal data against external threats. However, Albert worries about the high turnover rate within the company, particularly in the area of direct phone marketing. He sees many unfamiliar faces every day who are hired to do the marketing, and he often hears complaints in the lunch room regarding long hours and low pay, as well as what seems to be flagrant disregard for company procedures.

In addition, Treasure Box has had two recent security incidents. The company has responded to the incidents with internal audits and updates to security safeguards. However, profits still seem to be affected and anecdotal evidence indicates that many people still harbor mistrust. Albert wants to help the company recover. He knows there is at least one incident the public in unaware of, although Albert does not know the details. He believes the company's insistence on keeping the incident a secret could be a further detriment to its reputation. One further way that Albert wants to help Treasure Box regain its stature is by creating a toll-free number for customers, as well as a more efficient procedure for responding to customer concerns by postal mail.

In addition to his suggestions for improvement, Albert believes that his knowledge of the company's recent business maneuvers will also impress the interviewers. For example, Albert is aware of the company's intention to acquire a medical supply company in the coming weeks.

With his forward thinking, Albert hopes to convince the managers who will be interviewing him that he is right for the job.

Based on Albert's observations regarding recent security incidents, which of the following should he suggest as a priority for Treasure Box?

A. Appointing an internal ombudsman to address employee complaints regarding hours and pay.

B. Using a third-party auditor to address privacy protection issues not recognized by the prior internal audits.

C. Evaluating the company's ability to handle personal health information if the plan to acquire the medical supply company goes forward

D. Working with the Human Resources department to make screening procedures for potential employees more rigorous.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 66
SCENARIO
Please use the following to answer the next question:
As the director of data protection for Consolidated Records Corporation, you are justifiably pleased with your accomplishments so far. Your hiring was precipitated by warnings from regulatory agencies following a series of relatively minor data breaches that could easily have been worse. However, you have not had a reportable incident for the three years that you have been with the company. In fact, you consider your program a model that others in the data storage industry may note in their own program development.
You started the program at Consolidated from a jumbled mix of policies and procedures and worked toward coherence across departments and throughout operations. You were aided along the way by the program's sponsor, the vice president of operations, as well as by a Privacy Team that started from a clear understanding of the need for change.
Initially, your work was greeted with little confidence or enthusiasm by the company's "old guard" among both the executive team and frontline personnel working with data and interfacing with clients. Through the use of metrics that showed the costs not only of the breaches that had occurred, but also projections of the costs that easily could occur given the current state of operations, you soon had the leaders and key decision-makers largely on your side. Many of the other employees were more resistant, but face-to-face meetings with each department and the development of a baseline privacy training program achieved sufficient "buy-in" to begin putting the proper procedures into place.
Now, privacy protection is an accepted component of all current operations involving personal or protected data and must be part of the end product of any process of technological development. While your approach is not systematic, it is fairly effective.
You are left contemplating: What must be done to maintain the program and develop it beyond just a data breach prevention program? How can you build on your success? What are the next action steps?
What practice would afford the Director the most rigorous way to check on the program's compliance with laws, regulations and industry best practices?
A. Assessment
B. Forensics
C. Monitoring
D. Auditing
Answer: C (LEAVE A REPLY)

NEW QUESTION: 67
Formosa International operates in 20 different countries including the United States and France. What organizational approach would make complying with a number of different regulations easier?
A. Fair Information Practices.
B. Rationalizing requirements.

C. Data mapping.
D. Decentralized privacy management.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 68
What should a privacy professional keep in mind when selecting which metrics to collect?
A. Metrics should be reported to the public.
B. The number of metrics should be limited at first.
C. Metrics should reveal strategies for increasing company earnings.
D. A variety of metrics should be collected before determining their specific functions.
Answer: B (LEAVE A REPLY)
Explanation
A privacy professional should keep in mind that the number of metrics should be limited at first when selecting which metrics to collect. Metrics are quantitative measures that help evaluate the performance and effectiveness of a privacy program. However, collecting too many metrics can be overwhelming, confusing, and costly. Therefore, a privacy professional should start with a few key metrics that are relevant, meaningful, actionable, and aligned with the organization's privacy goals and priorities. These metrics can be refined and expanded over time as the privacy program matures and evolves. References: [Privacy Metrics], [Measuring Privacy Program Effectiveness]

NEW QUESTION: 69
SCENARIO
Please use the following to answer the next QUESTION:
Richard McAdams recently graduated law school and decided to return to the small town of Lexington, Virginia to help run his aging grandfather's law practice. The elder McAdams desired a limited, lighter role in the practice, with the hope that his grandson would eventually take over when he fully retires. In addition to hiring Richard, Mr. McAdams employs two paralegals, an administrative assistant, and a part-time IT specialist who handles all of their basic networking needs. He plans to hire more employees once Richard gets settled and assesses the office's strategies for growth.
Immediately upon arrival, Richard was amazed at the amount of work that needed to done in order to modernize the office, mostly in regard to the handling of clients' personal data. His first goal is to digitize all the records kept in file cabinets, as many of the documents contain personally identifiable financial and medical data. Also, Richard has noticed the massive amount of copying by the administrative assistant throughout the day, a practice that not only adds daily to the number of files in the file cabinets, but may create security issues unless a formal policy is firmly in place Richard is also concerned with the overuse of the communal copier/ printer located in plain view of clients who frequent the building. Yet another area of concern is the use of the same fax machine by all of the employees. Richard hopes to reduce its use dramatically in order to ensure that personal data receives the utmost security and protection, and eventually move toward a strict Internet faxing policy by the year's end.
Richard expressed his concerns to his grandfather, who agreed, that updating data storage, data security, and an overall approach to increasing the protection of personal data in all facets is necessary Mr. McAdams

granted him the freedom and authority to do so. Now Richard is not only beginning a career as an attorney, but also functioning as the privacy officer of the small firm. Richard plans to meet with the IT employee the following day, to get insight into how the office computer system is currently set-up and managed.
Richard needs to closely monitor the vendor in charge of creating the firm's database mainly because of what?
A. The vendor will be required to report any privacy violations to the appropriate authorities.
B. The vendor may not be aware of the privacy implications involved in the project.
C. The vendor may not be forthcoming about the vulnerabilities of the database.
D. The vendor will be in direct contact with all of the law firm's personal data.
Answer: D (LEAVE A REPLY)
Explanation
The main reason why Richard needs to closely monitor the vendor in charge of creating the firm's database is that the vendor will be in direct contact with all of the law firm's personal data. This means that the vendor will have access to sensitive and confidential information about the law firm's clients, such as their financial and medical data, which could expose them to identity theft, fraud, or other harms if mishandled or breached. Therefore, Richard needs to ensure that the vendor follows the best practices of data protection and security, such as:
* Signing a data processing agreement that specifies the scope, purpose, duration, and terms of the data processing activities, as well as the rights and obligations of both parties.
* Implementing appropriate technical and organizational measures to protect the data from unauthorized or unlawful access, use, disclosure, alteration, or destruction, such as encryption, access control, backup and recovery, logging and monitoring, etc.
* Complying with the relevant laws and regulations that govern the collection, use, transfer, and retention of personal data, such as the GDPR or other local privacy laws.
* Reporting any data breaches or incidents to the law firm and the relevant authorities as soon as possible and taking corrective actions to mitigate the impact and prevent recurrence.
* Deleting or returning the data to the law firm after the completion of the project or upon request.

NEW QUESTION: 70
What is least likely to be achieved by implementing a Data Lifecycle Management (DLM) program?
A. Reducing storage costs.
B. Increasing awareness of the importance of confidentiality.
C. Ensuring data is kept for no longer than necessary.
D. Crafting policies which ensure minimal data is collected.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 71
SCENARIO
Please use the following to answer the next question:
You lead the privacy office for a company that handles information from individuals living in several countries throughout Europe and the Americas. You begin that morning's privacy review when a contracts officer sends

you a message asking for a phone call. The message lacks clarity and detail, but you presume that data was lost.

When you contact the contracts officer, he tells you that he received a letter in the mail from a vendor stating that the vendor improperly shared information about your customers. He called the vendor and confirmed that your company recently surveyed exactly 2000 individuals about their most recent healthcare experience and sent those surveys to the vendor to transcribe it into a database, but the vendor forgot to encrypt the database as promised in the contract. As a result, the vendor has lost control of the data.

The vendor is extremely apologetic and offers to take responsibility for sending out the notifications. They tell you they set aside 2000 stamped postcards because that should reduce the time it takes to get the notice in the mail. One side is limited to their logo, but the other side is blank and they will accept whatever you want to write. You put their offer on hold and begin to develop the text around the space constraints. You are content to let the vendor's logo be associated with the notification.

The notification explains that your company recently hired a vendor to store information about their most recent experience at St. Sebastian Hospital's Clinic for Infectious Diseases. The vendor did not encrypt the information and no longer has control of it. All 2000 affected individuals are invited to sign-up for email notifications about their information. They simply need to go to your company's website and watch a quick advertisement, then provide their name, email address, and month and year of birth.

You email the incident-response council for their buy-in before 9 a.m. If anything goes wrong in this situation, you want to diffuse the blame across your colleagues. Over the next eight hours, everyone emails their comments back and forth. The consultant who leads the incident-response team notes that it is his first day with the company, but he has been in other industries for 45 years and will do his best. One of the three lawyers on the council causes the conversation to veer off course, but it eventually gets back on track. At the end of the day, they vote to proceed with the notification you wrote and use the vendor's postcards.

Shortly after the vendor mails the postcards, you learn the data was on a server that was stolen, and make the decision to have your company offer credit monitoring services. A quick internet search finds a credit monitoring company with a convincing name: Credit Under Lock and Key (CRUDLOK). Your sales rep has never handled a contract for 2000 people, but develops a proposal in about a day which says CRUDLOK will:

1.Send an enrollment invitation to everyone the day after the contract is signed.
2.Enroll someone with just their first name and the last-4 of their national identifier.
3.Monitor each enrollee's credit for two years from the date of enrollment.
4.Send a monthly email with their credit rating and offers for credit-related services at market rates.
5.Charge your company 20% of the cost of any credit restoration.

You execute the contract and the enrollment invitations are emailed to the 2000 individuals. Three days later you sit down and document all that went well and all that could have gone better. You put it in a file to reference the next time an incident occurs.

Which of the following elements of the incident did you adequately determine?

A. The likelihood the incident may lead to harm
B. The likelihood that the information is accessible and usable
C. The number of individuals whose information was affected
D. The nature of the data elements impacted

Answer: A (LEAVE A REPLY)

NEW QUESTION: 72
SCENARIO
Please use the following to answer the next question:
Edufox has hosted an annual convention of users of its famous e-learning software platform, and over time, it has become a grand event. It fills one of the large downtown conference hotels and overflows into the others, with several thousand attendees enjoying three days of presentations, panel discussions and networking. The convention is the centerpiece of the company's product rollout schedule and a great training opportunity for current users. The sales force also encourages prospective clients to attend to get a better sense of the ways in which the system can be customized to meet diverse needs and understand that when they buy into this system, they are joining a community that feels like family.
This year's conference is only three weeks away, and you have just heard news of a new initiative supporting it: a smartphone app for attendees. The app will support late registration, highlight the featured presentations and provide a mobile version of the conference program. It also links to a restaurant reservation system with the best cuisine in the areas featured. "It's going to be great," the developer, Deidre Hoffman, tells you, "if, that is, we actually get it working!" She laughs nervously but explains that because of the tight time frame she'd been given to build the app, she outsourced the job to a local firm. "It's just three young people," she says, "but they do great work." She describes some of the other apps they have built. When asked how they were selected for this job, Deidre shrugs. "They do good work, so I chose them." Deidre is a terrific employee with a strong track record. That's why she's been charged to deliver this rushed project. You're sure she has the best interests of the company at heart, and you don't doubt that she's under pressure to meet a deadline that cannot be pushed back. However, you have concerns about the app's handling of personal data and its security safeguards. Over lunch in the break room, you start to talk to her about it, but she quickly tries to reassure you, "I'm sure with your help we can fix any security issues if we have to, but I doubt there'll be any. These people build apps for a living, and they know what they're doing. You worry too much, but that's why you're so good at your job!" You see evidence that company employees routinely circumvent the privacy officer in developing new initiatives. How can you best draw attention to the scope of this problem?
A. Develop a metric showing the number of initiatives launched without consultation and include it in reports, presentations, and consultation.
B. Insist upon one-on-one consultation with each person who works around the privacy officer.
C. Take your concerns straight to the Chief Executive Officer.
D. Hold discussions with the department head of anyone who fails to consult with the privacy officer.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 73
SCENARIO
Please use the following to answer the next QUESTION:
Penny has recently joined Ace Space, a company that sells homeware accessories online, as its new privacy officer. The company is based in California but thanks to some great publicity from a social media influencer last year, the company has received an influx of sales from the EU and has set up a regional office in Ireland to support this expansion. To become familiar with Ace Space's practices and assess what her privacy

priorities will be, Penny has set up meetings with a number of colleagues to hear about the work that they have been doing and their compliance efforts.
Penny's colleague in Marketing is excited by the new sales and the company's plans, but is also concerned that Penny may curtail some of the growth opportunities he has planned. He tells her "I heard someone in the breakroom talking about some new privacy laws but I really don't think it affects us. We're just a small company. I mean we just sell accessories online, so what's the real risk?" He has also told her that he works with a number of small companies that help him get projects completed in a hurry. "We've got to meet our deadlines otherwise we lose money. I just sign the contracts and get Jim in finance to push through the payment. Reviewing the contracts takes time that we just don't have." In her meeting with a member of the IT team, Penny has learned that although Ace Space has taken a number of precautions to protect its website from malicious activity, it has not taken the same level of care of its physical files or internal infrastructure.
Penny's colleague in IT has told her that a former employee lost an encrypted USB key with financial data on it when he left. The company nearly lost access to their customer database last year after they fell victim to a phishing attack. Penny is told by her IT colleague that the IT team "didn't know what to do or who should do what. We hadn't been trained on it but we're a small team though, so it worked out OK in the end." Penny is concerned that these issues will compromise Ace Space's privacy and data protection.
Penny is aware that the company has solid plans to grow its international sales and will be working closely with the CEO to give the organization a data "shake up". Her mission is to cultivate a strong privacy culture within the company.
Penny has a meeting with Ace Space's CEO today and has been asked to give her first impressions and an overview of her next steps.
To establish the current baseline of Ace Space's privacy maturity, Penny should consider all of the following factors EXCEPT?
A. Ace Space's content sharing practices on social media
B. Ace Space's employee training program
C. Ace Space's documented procedures
D. Ace Space's vendor engagement protocols
Answer: C (LEAVE A REPLY)

NEW QUESTION: 74
If done correctly, how can a Data Protection Impact Assessment (DPIA) create a win/win scenario for organizations and individuals?
A. By quickly identifying potentially problematic data attributes and reducing the risk exposure.
B. By allowing Data Controllers to solicit feedback from individuals about how they feel about the potential data processing.
C. By enabling Data Controllers to be proactive in their analysis of processing activities and ensuring compliance with the law.
D. By better informing about the risks associated with the processing activity and improving the organization's transparency with individuals.
Answer: D (LEAVE A REPLY)

A Data Protection Impact Assessment (DPIA) is a process that organizations use to evaluate the potential risks associated with a specific data processing activity, and to identify and implement measures to mitigate those risks. By conducting a DPIA, organizations can proactively identify and address potential privacy concerns before they become a problem, and ensure compliance with data protection laws and regulations. When organizations are transparent about their data processing activities and the risks associated with them, individuals are better informed about how their personal data is being used and can make more informed decisions about whether or not to provide their personal data. This creates a win/win scenario for organizations and individuals, as organizations are able to continue processing personal data in a compliant and transparent manner, while individuals are able to trust that their personal data is being used responsibly. Additionally, by engaging with individuals in the DPIA process and soliciting their feedback, organizations can better understand the potential impact of their data processing activities on individuals and take steps to mitigate any negative impacts.
Reference:
-https://ec.europa.eu/info/publications/data-protection-impact-assessment-dpia-guidelines_en -https://gdpr-info.eu/art-35-gdpr/

NEW QUESTION: 75
An organization's privacy officer was just notified by the benefits manager that she accidentally sent out the retirement enrollment report of all employees to a wrong vendor. Which of the following actions should the privacy officer take FIRST?
A. Send firm-wide email notification to employees
B. Contact the recipient to delete the email
C. Report the incident to law enforcement
D. Perform a risk of harm analysis
Answer: D (LEAVE A REPLY)

NEW QUESTION: 76
SCENARIO
Please use the following to answer the next QUESTION:
Perhaps Jack Kelly should have stayed in the U.S. He enjoys a formidable reputation inside the company, Special Handling Shipping, for his work in reforming certain "rogue" offices. Last year, news broke that a police sting operation had revealed a drug ring operating in the Providence, Rhode Island office in the United States. Video from the office's video surveillance cameras leaked to news operations showed a drug exchange between Special Handling staff and undercover officers.
In the wake of this incident, Kelly had been sent to Providence to change the "hands off" culture that upper management believed had let the criminal elements conduct their illicit transactions. After a few weeks under Kelly's direction, the office became a model of efficiency and customer service. Kelly monitored his workers' activities using the same cameras that had recorded the illegal conduct of their former co-workers.
Now Kelly has been charged with turning around the office in Cork, Ireland, another trouble spot. The company has received numerous reports of the staff leaving the office unattended. When Kelly arrived, he found that even when present, the staff often spent their days socializing or conducting personal business on

their mobile phones. Again, he observed their behaviors using surveillance cameras. He issued written reprimands to six staff members based on the first day of video alone.
Much to Kelly's surprise and chagrin, he and the company are now under investigation by the Data Protection Commissioner of Ireland for allegedly violating the privacy rights of employees. Kelly was told that the company's license for the cameras listed facility security as their main use, but he does not know why this matters. He has pointed out to his superiors that the company's training programs on privacy protection and data collection mention nothing about surveillance video.
You are a privacy protection consultant, hired by the company to assess this incident, report on the legal and compliance issues, and recommend next steps.
What does this example best illustrate about training requirements for privacy protection?
A. Training needs must be weighed against financial costs.
B. Training must include assessments to verify that the material is mastered.
C. Training must be repeated frequently to respond to new legislation.
D. Training on local laws must be implemented for all personnel.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 77
Under the General Data Protection Regulation (GDPR), what must be included in a written agreement between the controller and processor in relation to processing conducted on the controller's behalf?
A. An obligation on the processor to assist the controller in complying with the controller's obligations to notify the supervisory authority about personal data breaches.
B. An obligation on both parties to report any serious personal data breach to the supervisory authority.
C. An obligation on both parties to agree to a termination of the agreement if the other party is responsible for a personal data breach.
D. An obligation on the processor to report any personal data breach to the controller within 72 hours.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 78
SCENARIO
Please use the following to answer the next question:
Henry Home Furnishings has built high-end furniture for nearly forty years. However, the new owner, Anton, has found some degree of disorganization after touring the company headquarters. His uncle Henry has always focused on production - not data processing - and Anton is concerned. In several storage rooms, he

has found paper files, disks, and old computers that appear to contain the personal data of current and former employees and customers. Anton knows that a single break-in could irrevocably damage the company's relationship with its loyal customers. He intends to set a goal of guaranteed zero loss of personal information. To this end, Anton originally planned to place restrictions on who was admitted to the physical premises of the company. However, Kenneth - his uncle's vice president and longtime confidante - wants to hold off on Anton's idea in favor of converting any paper records held at the company to electronic storage. Kenneth believes this process would only take one or two years. Anton likes this idea; he envisions a password-protected system that only he and Kenneth can access.

Anton also plans to divest the company of most of its subsidiaries. Not only will this make his job easier, but it will simplify the management of the stored data. The heads of subsidiaries like the art gallery and kitchenware store down the street will be responsible for their own information management. Then, any unneeded subsidiary data still in Anton's possession can be destroyed within the next few years.

After learning of a recent security incident, Anton realizes that another crucial step will be notifying customers. Kenneth insists that two lost hard drives in Question not cause for concern; all of the data was encrypted and not sensitive in nature. Anton does not want to take any chances, however. He intends on sending notice letters to all employees and customers to be safe.

Anton must also check for compliance with all legislative, regulatory, and market requirements related to privacy protection. Kenneth oversaw the development of the company's online presence about ten years ago, but Anton is not confident about his understanding of recent online marketing laws. Anton is assigning another trusted employee with a law background the task of the compliance assessment. After a thorough analysis, Anton knows the company should be safe for another five years, at which time he can order another check.

Documentation of this analysis will show auditors due diligence.

Anton has started down a long road toward improved management of the company, but he knows the effort is worth it. Anton wants his uncle's legacy to continue for many years to come.

What would the company's legal team most likely recommend to Anton regarding his planned communication with customers?

A. To consider under what circumstances communication is necessary

B. To shift to electronic communication

C. To send consistent communication

D. To delay communications until local authorities are informed

Answer: A (LEAVE A REPLY)

NEW QUESTION: 79

How do privacy audits differ from privacy assessments?

A. They are conducted by external parties.

B. They are non-binding.

C. They are based on standards.

D. They are evidence-based.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 80
SCENARIO
Please use the following to answer the next QUESTION:
Amira is thrilled about the sudden expansion of NatGen. As the joint Chief Executive Officer (CEO) with her long-time business partner Sadie, Amira has watched the company grow into a major competitor in the green energy market. The current line of products includes wind turbines, solar energy panels, and equipment for geothermal systems. A talented team of developers means that NatGen's line of products will only continue to grow.
With the expansion, Amira and Sadie have received advice from new senior staff members brought on to help manage the company's growth. One recent suggestion has been to combine the legal and security functions of the company to ensure observance of privacy laws and the company's own privacy policy. This sounds overly complicated to Amira, who wants departments to be able to use, collect, store, and dispose of customer data in ways that will best suit their needs. She does not want administrative oversight and complex structuring to get in the way of people doing innovative work.
Sadie has a similar outlook. The new Chief Information Officer (CIO) has proposed what Sadie believes is an unnecessarily long timetable for designing a new privacy program. She has assured him that NatGen will use the best possible equipment for electronic storage of customer and employee data. She simply needs a list of equipment and an estimate of its cost. But the CIO insists that many issues are necessary to consider before the company gets to that stage.
Regardless, Sadie and Amira insist on giving employees space to do their jobs. Both CEOs want to entrust the monitoring of employee policy compliance to low-level managers. Amira and Sadie believe these managers can adjust the company privacy policy according to what works best for their particular departments. NatGen's CEOs know that flexible interpretations of the privacy policy in the name of promoting green energy would be highly unlikely to raise any concerns with their customer base, as long as the data is always used in course of normal business activities.
Perhaps what has been most perplexing to Sadie and Amira has been the CIO's recommendation to institute a privacy compliance hotline. Sadie and Amira have relented on this point, but they hope to compromise by allowing employees to take turns handling reports of privacy policy violations. The implementation will be easy because the employees need no special preparation. They will simply have to document any concerns they hear.
Sadie and Amira are aware that it will be challenging to stay true to their principles and guard against corporate culture strangling creativity and employee morale. They hope that all senior staff will see the benefit of trying a unique approach.
What is the most likely reason the Chief Information Officer (CIO) believes that generating a list of needed IT equipment is NOT adequate?
A. The company needs to have policies and procedures in place to guide the purchasing decisions.
B. The privacy notice for customers and the Business Continuity Plan (BCP) still need to be reviewed.
C. Staff members across departments need time to review technical information concerning any new databases.
D. Senior staff members need to first commit to adopting a minimum number of Privacy Enhancing Technologies (PETs).

Answer: A (LEAVE A REPLY)

Explanation

The most likely reason the Chief Information Officer (CIO) believes that generating a list of needed IT equipment is not adequate is that the company needs to have policies and procedures in place to guide the purchasing decisions. Policies and procedures are essential for ensuring that the IT equipment meets the business needs and objectives, as well as the legal and regulatory requirements for data protection and security6 Policies and procedures can help the company to:

* Define the roles and responsibilities of the IT staff and other stakeholders involved in the purchasing process.
* Establish the criteria and standards for selecting and evaluating the IT equipment vendors and products.
* Determine the budget and timeline for acquiring and deploying the IT equipment.
* Implement the best practices for installing, configuring, testing, maintaining, and disposing of the IT equipment.
* Monitor and measure the performance and effectiveness of the IT equipment.

Without policies and procedures in place, the company may face risks such as:

* Wasting time and money on unnecessary or inappropriate IT equipment.
* Exposing sensitive data to unauthorized access or loss due to inadequate or incompatible IT equipment.
* Failing to comply with data protection laws or industry standards due to non-compliant or outdated IT equipment.
* Facing legal or reputational consequences due to data breaches or incidents caused by faulty or insecure IT equipment.

Therefore, generating a list of needed IT equipment is not adequate without having policies and procedures in place to guide the purchasing decisions. References: 6: IT Policies & Procedures: A Quick Guide - ProjectManager; 7: IT Policies & Procedures: A Quick Guide - ProjectManager

NEW QUESTION: 81

SCENARIO

Please use the following to answer the next question:

As the director of data protection for Consolidated Records Corporation, you are justifiably pleased with your accomplishments so far. Your hiring was precipitated by warnings from regulatory agencies following a series of relatively minor data breaches that could easily have been worse. However, you have not had a reportable incident for the three years that you have been with the company. In fact, you consider your program a model that others in the data storage industry may note in their own program development.

You started the program at Consolidated from a jumbled mix of policies and procedures and worked toward coherence across departments and throughout operations. You were aided along the way by the program's sponsor, the vice president of operations, as well as by a Privacy Team that started from a clear understanding of the need for change.

Initially, your work was greeted with little confidence or enthusiasm by the company's "old guard" among both the executive team and frontline personnel working with data and interfacing with clients. Through the use of metrics that showed the costs not only of the breaches that had occurred, but also projections of the costs that easily could occur given the current state of operations, you soon had the leaders and key decision-

makers largely on your side. Many of the other employees were more resistant, but face-to-face meetings with each department and the development of a baseline privacy training program achieved sufficient "buy-in" to begin putting the proper procedures into place.
Now, privacy protection is an accepted component of all current operations involving personal or protected data and must be part of the end product of any process of technological development. While your approach is not systematic, it is fairly effective.
You are left contemplating: What must be done to maintain the program and develop it beyond just a data breach prevention program? How can you build on your success? What are the next action steps?
How can Consolidated's privacy training program best be further developed?
A. By using industry standard off-the-shelf programs
B. By adopting e-learning to reduce the need for instructors
C. Through a review of recent data breaches
D. Through targeted curricula designed for specific departments
Answer: (SHOW ANSWER)

NEW QUESTION: 82
SCENARIO
Please use the following to answer the next QUESTION:
Your organization, the Chicago (U.S.)-based Society for Urban Greenspace, has used the same vendor to operate all aspects of an online store for several years. As a small nonprofit, the Society cannot afford the higher-priced options, but you have been relatively satisfied with this budget vendor, Shopping Cart Saver (SCS). Yes, there have been some issues. Twice, people who purchased items from the store have had their credit card information used fraudulently subsequent to transactions on your site, but in neither case did the investigation reveal with certainty that the Society's store had been hacked. The thefts could have been employee-related.
Just as disconcerting was an incident where the organization discovered that SCS had sold information it had collected from customers to third parties. However, as Jason Roland, your SCS account representative, points out, it took only a phone call from you to clarify expectations and the "misunderstanding" has not occurred again.
As an information-technology program manager with the Society, the role of the privacy professional is only one of many you play. In all matters, however, you must consider the financial bottom line. While these problems with privacy protection have been significant, the additional revenues of sales of items such as shirts and coffee cups from the store have been significant. The Society's operating budget is slim, and all sources of revenue are essential.
Now a new challenge has arisen. Jason called to say that starting in two weeks, the customer data from the store would now be stored on a data cloud. "The good news," he says, "is that we have found a low-cost provider in Finland, where the data would also be held. So, while there may be a small charge to pass through to you, it won't be exorbitant, especially considering the advantages of a cloud." Lately, you have been hearing about cloud computing and you know it's fast becoming the new paradigm for various applications. However, you have heard mixed reviews about the potential impacts on privacy protection. You begin to research and discover that a number of the leading cloud service providers have signed a letter of

intent to work together on shared conventions and technologies for privacy protection. You make a note to find out if Jason's Finnish provider is signing on.
What is the best way to prevent the Finnish vendor from transferring data to another party?
A. Restrict the vendor to using company security controls
B. Offer company resources to assist with the processing
C. Include transfer prohibitions in the vendor contract
D. Lock the data down in its current location
Answer: C (LEAVE A REPLY)
Explanation
This answer is the best way to prevent the Finnish vendor from transferring data to another party, as it can establish clear and binding terms and conditions for both parties regarding their roles and responsibilities for data processing activities. Including transfer prohibitions in the vendor contract can help to define the scope, purpose, duration and type of data processing, as well as the rights and obligations of both parties. The contract can also specify that the vendor is not allowed to share, disclose or transfer the data to any third party without the prior consent or authorization of the organization, and that any breach of this clause may result in legal actions, penalties or termination of the contract.

NEW QUESTION: 83
SCENARIO
Please use the following to answer the next QUESTION:
For 15 years, Albert has worked at Treasure Box - a mail order company in the United States (U.S.) that used to sell decorative candles around the world, but has recently decided to limit its shipments to customers in the 48 contiguous states. Despite his years of experience, Albert is often overlooked for managerial positions. His frustration about not being promoted, coupled with his recent interest in issues of privacy protection, have motivated Albert to be an agent of positive change.
He will soon interview for a newly advertised position, and during the interview, Albert plans on making executives aware of lapses in the company's privacy program. He feels certain he will be rewarded with a promotion for preventing negative consequences resulting from the company's outdated policies and procedures.
For example, Albert has learned about the AICPA (American Institute of Certified Public Accountans)/CICA (Canadian Institute of Chartered Accountants) Privacy Maturity Model (PMM). Albert thinks the model is a useful way to measure Treasure Box's ability to protect personal data. Albert has noticed that Treasure Box fails to meet the requirements of the highest level of maturity of this model; at his interview, Albert will pledge to assist the company with meeting this level in order to provide customers with the most rigorous security available.
Albert does want to show a positive outlook during his interview. He intends to praise the company's commitment to the security of customer and employee personal data against external threats. However, Albert worries about the high turnover rate within the company, particularly in the area of direct phone marketing. He sees many unfamiliar faces every day who are hired to do the marketing, and he often hears complaints in the lunch room regarding long hours and low pay, as well as what seems to be flagrant disregard for company procedures.

In addition, Treasure Box has had two recent security incidents. The company has responded to the incidents with internal audits and updates to security safeguards. However, profits still seem to be affected and anecdotal evidence indicates that many people still harbor mistrust. Albert wants to help the company recover.
He knows there is at least one incident the public in unaware of, although Albert does not know the details. He believes the company's insistence on keeping the incident a secret could be a further detriment to its reputation. One further way that Albert wants to help Treasure Box regain its stature is by creating a toll-free number for customers, as well as a more efficient procedure for responding to customer concerns by postal mail.
In addition to his suggestions for improvement, Albert believes that his knowledge of the company's recent business maneuvers will also impress the interviewers. For example, Albert is aware of the company's intention to acquire a medical supply company in the coming weeks.
With his forward thinking, Albert hopes to convince the managers who will be interviewing him that he is right for the job.
What is one important factor that Albert fails to consider regarding Treasure Box's response to their recent security incident?
A. Who has access to the data
B. How data at the company is collected
C. How long data at the company is kept
D. What the nature of the data is
Answer: (SHOW ANSWER)

NEW QUESTION: 84
SCENARIO
Please use the following to answer the next question:
For 15 years, Albert has worked at Treasure Box - a mail order company in the United States (U.S.) that used to sell decorative candles around the world, but has recently decided to limit its shipments to customers in the 48 contiguous states. Despite his years of experience, Albert is often overlooked for managerial positions. His frustration about not being promoted, coupled with his recent interest in issues of privacy protection, have motivated Albert to be an agent of positive change.
He will soon interview for a newly advertised position, and during the interview, Albert plans on making executives aware of lapses in the company's privacy program. He feels certain he will be rewarded with a promotion for preventing negative consequences resulting from the company's outdated policies and procedures.
For example, Albert has learned about the AICPA (American Institute of Certified Public Accountans)/CICA (Canadian Institute of Chartered Accountants) Privacy Maturity Model (PMM). Albert thinks the model is a useful way to measure Treasure Box's ability to protect personal data. Albert has noticed that Treasure Box fails to meet the requirements of the highest level of maturity of this model; at his interview, Albert will pledge to assist the company with meeting this level in order to provide customers with the most rigorous security available.

Albert does want to show a positive outlook during his interview. He intends to praise the company's commitment to the security of customer and employee personal data against external threats. However, Albert worries about the high turnover rate within the company, particularly in the area of direct phone marketing. He sees many unfamiliar faces every day who are hired to do the marketing, and he often hears complaints in the lunch room regarding long hours and low pay, as well as what seems to be flagrant disregard for company procedures.

In addition, Treasure Box has had two recent security incidents. The company has responded to the incidents with internal audits and updates to security safeguards. However, profits still seem to be affected and anecdotal evidence indicates that many people still harbor mistrust. Albert wants to help the company recover.

He knows there is at least one incident the public in unaware of, although Albert does not know the details. He believes the company's insistence on keeping the incident a secret could be a further detriment to its reputation. One further way that Albert wants to help Treasure Box regain its stature is by creating a toll-free number for customers, as well as a more efficient procedure for responding to customer concerns by postal mail.

In addition to his suggestions for improvement, Albert believes that his knowledge of the company's recent business maneuvers will also impress the interviewers. For example, Albert is aware of the company's intention to acquire a medical supply company in the coming weeks.

With his forward thinking, Albert hopes to convince the managers who will be interviewing him that he is right for the job.

Based on Albert's observations regarding recent security incidents, which of the following should he suggest as a priority for Treasure Box?

A. Appointing an internal ombudsman to address employee complaints regarding hours and pay.

B. Working with the Human Resources department to make screening procedures for potential employees more rigorous.

C. Evaluating the company's ability to handle personal health information if the plan to acquire the medical supply company goes forward

D. Using a third-party auditor to address privacy protection issues not recognized by the prior internal audits.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 85

SCENARIO

Please use the following to answer the next QUESTION:

As the Director of data protection for Consolidated Records Corporation, you are justifiably pleased with your accomplishments so far. Your hiring was precipitated by warnings from regulatory agencies following a series of relatively minor data breaches that could easily have been worse. However, you have not had a reportable incident for the three years that you have been with the company. In fact, you consider your program a model that others in the data storage industry may note in their own program development.

You started the program at Consolidated from a jumbled mix of policies and procedures and worked toward coherence across departments and throughout operations. You were aided along the way by the program's

sponsor, the vice president of operations, as well as by a Privacy Team that started from a clear understanding of the need for change.
Initially, your work was greeted with little confidence or enthusiasm by the company's "old guard" among both the executive team and frontline personnel working with data and interfacing with clients. Through the use of metrics that showed the costs not only of the breaches that had occurred, but also projections of the costs that easily could occur given the current state of operations, you soon had the leaders and key decision-makers largely on your side. Many of the other employees were more resistant, but face-to-face meetings with each department and the development of a baseline privacy training program achieved sufficient "buy-in" to begin putting the proper procedures into place.
Now, privacy protection is an accepted component of all current operations involving personal or protected data and must be part of the end product of any process of technological development. While your approach is not systematic, it is fairly effective.
You are left contemplating:
What must be done to maintain the program and develop it beyond just a data breach prevention program?
How can you build on your success?
What are the next action steps?
What practice would afford the Director the most rigorous way to check on the program's compliance with laws, regulations and industry best practices?
A. Auditing.
B. Monitoring.
C. Assessment.
D. Forensics.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 86
Which of the following helps build trust with customers and stakeholders?
A. Enable customers to view and change their own personal information within a dedicated portal.
B. Provide a dedicated privacy space with the privacy policy, explanatory documents and operation frameworks.
C. Only publish what is legally necessary to reduce your liability.
D. Publish your privacy policy using broad language to ensure all of your organization's activities are captured.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 87
SCENARIO
Please use the following to answer the next question:
As they company's new chief executive officer, Thomas Goddard wants to be known as a leader in data protection. Goddard recently served as the chief financial officer of Hoopy.com, a pioneer in online video viewing with millions of users around the world. Unfortunately, Hoopy is infamous within privacy protection circles for its ethically Questionable practices, including unauthorized sales of personal data to marketers.

Hoopy also was the target of credit card data theft that made headlines around the world, as at least two million credit card numbers were thought to have been pilfered despite the company's claims that "appropriate" data protection safeguards were in place. The scandal affected the company's business as competitors were quick to market an increased level of protection while offering similar entertainment and media content. Within three weeks after the scandal broke, Hoopy founder and CEO Maxwell Martin, Goddard's mentor, was forced to step down.
Goddard, however, seems to have landed on his feet, securing the CEO position at your company, Medialite, which is just emerging from its start-up phase. He sold the company's board and investors on his vision of Medialite building its brand partly on the basis of industry-leading data protection standards and procedures. He may have been a key part of a lapsed or even rogue organization in matters of privacy but now he claims to be reformed and a true believer in privacy protection. In his first week on the job, he calls you into his office and explains that your primary work responsibility is to bring his vision for privacy to life. But you also detect some reservations. "We want Medialite to have absolutely the highest standards," he says. "In fact, I want us to be able to say that we are the clear industry leader in privacy and data protection. However, I also need to be a responsible steward of the company's finances. So, while I want the best solutions across the board, they also need to be cost effective." You are told to report back in a week's time with your recommendations. Charged with this ambiguous mission, you depart the executive suite, already considering your next steps.
What metric can Goddard use to assess whether costs associated with implementing new privacy protections are justified?
A. Cost-effective mean
B. Return on investment
C. Implementation measure
D. Compliance ratio
Answer: B (LEAVE A REPLY)

NEW QUESTION: 88
Integrating privacy requirements into functional areas across the organization happens at which stage of the privacy operational life cycle?
A. Assessing data.
B. Protecting personal data.
C. Sustaining program performance.
D. Responding to requests and incidents.
Answer: (SHOW ANSWER)
Explanation
Integrating privacy requirements into functional areas across the organization happens at the "protect" stage of the privacy operational life cycle. This stage involves implementing privacy policies, procedures, and controls to ensure that personal data is processed in a lawful, fair, and transparent manner. The other stages of the privacy operational life cycle are "assess", "align", "respond", and "sustain". References: CIPM Body of Knowledge, Domain III: Privacy Program Operational Life Cycle, Section B: Protect.

NEW QUESTION: 89

SCENARIO

Please use the following to answer the next question:

Henry Home Furnishings has built high-end furniture for nearly forty years. However, the new owner, Anton, has found some degree of disorganization after touring the company headquarters. His uncle Henry has always focused on production - not data processing - and Anton is concerned. In several storage rooms, he has found paper files, disks, and old computers that appear to contain the personal data of current and former employees and customers. Anton knows that a single break-in could irrevocably damage the company's relationship with its loyal customers. He intends to set a goal of guaranteed zero loss of personal information.

To this end, Anton originally planned to place restrictions on who was admitted to the physical premises of the company. However, Kenneth - his uncle's vice president and longtime confidante - wants to hold off on Anton's idea in favor of converting any paper records held at the company to electronic storage. Kenneth believes this process would only take one or two years. Anton likes this idea; he envisions a password-protected system that only he and Kenneth can access.

Anton also plans to divest the company of most of its subsidiaries. Not only will this make his job easier, but it will simplify the management of the stored data. The heads of subsidiaries like the art gallery and kitchenware store down the street will be responsible for their own information management. Then, any unneeded subsidiary data still in Anton's possession can be destroyed within the next few years.

After learning of a recent security incident, Anton realizes that another crucial step will be notifying customers. Kenneth insists that two lost hard drives in Question not cause for concern; all of the data was encrypted and not sensitive in nature. Anton does not want to take any chances, however. He intends on sending notice letters to all employees and customers to be safe.

Anton must also check for compliance with all legislative, regulatory, and market requirements related to privacy protection. Kenneth oversaw the development of the company's online presence about ten years ago, but Anton is not confident about his understanding of recent online marketing laws. Anton is assigning another trusted employee with a law background the task of the compliance assessment. After a thorough analysis, Anton knows the company should be safe for another five years, at which time he can order another check.

Documentation of this analysis will show auditors due diligence.

Anton has started down a long road toward improved management of the company, but he knows the effort is worth it. Anton wants his uncle's legacy to continue for many years to come.

Which of Anton's plans for improving the data management of the company is most unachievable?

A. His initiative to achieve regulatory compliance

B. His objective for zero loss of personal information

C. His intention to send notice letters to customers and employees

D. His intention to transition to electronic storage

Answer: A (LEAVE A REPLY)

NEW QUESTION: 90

Which of the following is NOT recommended for effective Identity Access Management?

A. Demographics.

B. Unique user IDs.

C. User responsibility.
D. Credentials (e.g.. password).
Answer: A (LEAVE A REPLY)
Identity and Access Management (IAM) is a process that helps organizations secure their systems and data by controlling who has access to them and what they can do with that access. Effective IAM includes a number of best practices, such as:
Unique user IDs: Each user should have a unique ID that is used to identify them across all systems and applications.
Credentials: Users should be required to provide authentication credentials, such as a password or biometric data, in order to access systems and data.
User responsibility: Users should be made aware of their responsibilities when it comes to security, such as the need to keep their passwords secret and the importance of reporting suspicious activity.
Demographics refers to the statistical characteristics of a population, such as age, gender, income, etc. While demographic data may be collected and used for various purposes, it is not a recommended practice for effective IAM. Demographic data is not a reliable method of identification or authentication, and it is not used to provide access to systems and data.
Reference:
https://aws.amazon.com/iam/
https://en.wikipedia.org/wiki/Identity_and_access_management
https://en.wikipedia.org/wiki/Demographics

NEW QUESTION: 91
In privacy protection, what is a "covered entity"?
A. Personal data collected by a privacy organization.
B. An organization subject to the privacy provisions of HIPAA.
C. A privacy office or team fully responsible for protecting personal information.
D. Hidden gaps in privacy protection that may go unnoticed without expert analysis.
Answer: B (LEAVE A REPLY)
Explanation
A covered entity is an organization that is subject to the privacy provisions of the Health Insurance Portability and Accountability Act (HIPAA) of 1996. HIPAA regulates how covered entities use and disclose protected health information (PHI) of individuals. Covered entities include health plans, health care clearinghouses, and health care providers that transmit health information electronically. References: [HIPAA for Professionals], [What is a Covered Entity?]

NEW QUESTION: 92
Which of the following best supports implementing controls to bring privacy policies into effect?
A. The Chief Information Officer as part of the Senior Management Team creating enterprise privacy policies to ensure controls are available.
B. The information technology (IT) group supporting and enhancing the privacy program and privacy policy by developing processes and controls.
C. The legal department or outside counsel conducting a thorough review of the privacy program and policies.
D. The internal audit department establishing the audit controls which test for policy effectiveness.
Answer: (SHOW ANSWER)

NEW QUESTION: 93
SCENARIO
Please use the following to answer the next question:
You lead the privacy office for a company that handles information from individuals living in several countries throughout Europe and the Americas. You begin that morning's privacy review when a contracts officer sends you a message asking for a phone call. The message lacks clarity and detail, but you presume that data was lost.
When you contact the contracts officer, he tells you that he received a letter in the mail from a vendor stating that the vendor improperly shared information about your customers. He called the vendor and confirmed that your company recently surveyed exactly 2000 individuals about their most recent healthcare experience and sent those surveys to the vendor to transcribe it into a database, but the vendor forgot to encrypt the database as promised in the contract. As a result, the vendor has lost control of the data.
The vendor is extremely apologetic and offers to take responsibility for sending out the notifications. They tell you they set aside 2000 stamped postcards because that should reduce the time it takes to get the notice in the mail. One side is limited to their logo, but the other side is blank and they will accept whatever you want to write. You put their offer on hold and begin to develop the text around the space constraints. You are content to let the vendor's logo be associated with the notification.
The notification explains that your company recently hired a vendor to store information about their most recent experience at St. Sebastian Hospital's Clinic for Infectious Diseases. The vendor did not encrypt the information and no longer has control of it. All 2000 affected individuals are invited to sign-up for email notifications about their information. They simply need to go to your company's website and watch a quick advertisement, then provide their name, email address, and month and year of birth.
You email the incident-response council for their buy-in before 9 a.m. If anything goes wrong in this situation, you want to diffuse the blame across your colleagues. Over the next eight hours, everyone emails their comments back and forth. The consultant who leads the incident-response team notes that it is his first day with the company, but he has been in other industries for 45 years and will do his best. One of the three lawyers on the council causes the conversation to veer off course, but it eventually gets back on track. At the end of the day, they vote to proceed with the notification you wrote and use the vendor's postcards.

Shortly after the vendor mails the postcards, you learn the data was on a server that was stolen, and make the decision to have your company offer credit monitoring services. A quick internet search finds a credit monitoring company with a convincing name: Credit Under Lock and Key (CRUDLOK). Your sales rep has never handled a contract for 2000 people, but develops a proposal in about a day which says CRUDLOK will:
1. Send an enrollment invitation to everyone the day after the contract is signed.
2. Enroll someone with just their first name and the last-4 of their national identifier.
3. Monitor each enrollee's credit for two years from the date of enrollment.
4. Send a monthly email with their credit rating and offers for credit-related services at market rates.
5. Charge your company 20% of the cost of any credit restoration.
You execute the contract and the enrollment invitations are emailed to the 2000 individuals. Three days later you sit down and document all that went well and all that could have gone better. You put it in a file to reference the next time an incident occurs.
Which of the following was done CORRECTLY during the above incident?
A. Finding a vendor who will offer the affected individuals additional services
B. The process by which affected individuals sign up for email notifications
C. Your assessment of which credit monitoring company you should hire
D. The speed at which you sat down to reflect and document the incident
Answer: D (LEAVE A REPLY)

NEW QUESTION: 94
SCENARIO
Please use the following to answer the next QUESTION:
Edufox has hosted an annual convention of users of its famous e-learning software platform, and over time, it has become a grand event. It fills one of the large downtown conference hotels and overflows into the others, with several thousand attendees enjoying three days of presentations, panel discussions and networking. The convention is the centerpiece of the company's product rollout schedule and a great training opportunity for current users. The sales force also encourages prospective clients to attend to get a better sense of the ways in which the system can be customized to meet diverse needs and understand that when they buy into this system, they are joining a community that feels like family.
This year's conference is only three weeks away, and you have just heard news of a new initiative supporting it: a smartphone app for attendees. The app will support late registration, highlight the featured presentations and provide a mobile version of the conference program. It also links to a restaurant reservation system with the best cuisine in the areas featured. "It's going to be great," the developer, Deidre Hoffman, tells you, "if, that is, we actually get it working!" She laughs nervously but explains that because of the tight time frame she'd been given to build the app, she outsourced the job to a local firm. "It's just three young people," she says, "but they do great work." She describes some of the other apps they have built. When asked how they were selected for this job, Deidre shrugs. "They do good work, so I chose them." Deidre is a terrific employee with a strong track record. That's why she's been charged to deliver this rushed project. You're sure she has the best interests of the company at heart, and you don't doubt that she's under pressure to meet a deadline that cannot be pushed back. However, you have concerns about the app's handling of personal data and its security safeguards. Over lunch in the break room, you start to talk to her about it, but she quickly tries to

reassure you, "I'm sure with your help we can fix any security issues if we have to, but I doubt there'll be any. These people build apps for a living, and they know what they're doing.
You worry too much, but that's why you're so good at your job!"
What safeguard can most efficiently ensure that privacy protection is a dimension of relationships with vendors?
A. Include appropriate language about privacy protection in vendor contracts.
B. Perform a privacy audit on any vendor under consideration.
C. Require that a person trained in privacy protection be part of all vendor selection teams.
D. Do business only with vendors who are members of privacy trade associations.
Answer: A (LEAVE A REPLY)
Explanation
This answer is the best way to ensure that privacy protection is a dimension of relationships with vendors, as it can establish clear and binding terms and conditions for both parties regarding their roles and responsibilities for data processing activities. Including appropriate language about privacy protection in vendor contracts can help to define the scope, purpose, duration and type of data processing, as well as the rights and obligations of both parties. The contracts can also specify the technical and organizational measures that the vendor must implement to protect the data from unauthorized or unlawful access, use, disclosure, alteration or destruction, and to notify the organization of any security incidents or breaches. The contracts can also allow the organization to monitor, audit or inspect the vendor's performance and compliance with the contract terms and applicable laws and regulations. References: IAPP CIPM Study Guide, page 82; ISO/IEC 27002:2013, section
15.1.2

NEW QUESTION: 95
SCENARIO
Please use the following to answer the next QUESTION:
You lead the privacy office for a company that handles information from individuals living in several countries throughout Europe and the Americas. You begin that morning's privacy review when a contracts officer sends you a message asking for a phone call. The message lacks clarity and detail, but you presume that data was lost.
When you contact the contracts officer, he tells you that he received a letter in the mail from a vendor stating that the vendor improperly shared information about your customers. He called the vendor and confirmed that your company recently surveyed exactly 2000 individuals about their most recent healthcare experience and sent those surveys to the vendor to transcribe it into a database, but the vendor forgot to encrypt the database as promised in the contract. As a result, the vendor has lost control of the data.
The vendor is extremely apologetic and offers to take responsibility for sending out the notifications. They tell you they set aside 2000 stamped postcards because that should reduce the time it takes to get the notice in the mail. One side is limited to their logo, but the other side is blank and they will accept whatever you want to write. You put their offer on hold and begin to develop the text around the space constraints. You are content to let the vendor's logo be associated with the notification.

The notification explains that your company recently hired a vendor to store information about their most recent experience at St. Sebastian Hospital's Clinic for Infectious Diseases. The vendor did not encrypt the information and no longer has control of it. All 2000 affected individuals are invited to sign-up for email notifications about their information. They simply need to go to your company's website and watch a quick advertisement, then provide their name, email address, and month and year of birth.
You email the incident-response council for their buy-in before 9 a.m. If anything goes wrong in this situation, you want to diffuse the blame across your colleagues. Over the next eight hours, everyone emails their comments back and forth. The consultant who leads the incident-response team notes that it is his first day with the company, but he has been in other industries for 45 years and will do his best. One of the three lawyers on the council causes the conversation to veer off course, but it eventually gets back on track. At the end of the day, they vote to proceed with the notification you wrote and use the vendor's postcards.
Shortly after the vendor mails the postcards, you learn the data was on a server that was stolen, and make the decision to have your company offer credit monitoring services. A quick internet search finds a credit monitoring company with a convincing name: Credit Under Lock and Key (CRUDLOK). Your sales rep has never handled a contract for 2000 people, but develops a proposal in about a day which says CRUDLOK will:
1.Send an enrollment invitation to everyone the day after the contract is signed.
2.Enroll someone with just their first name and the last-4 of their national identifier.
3.Monitor each enrollee's credit for two years from the date of enrollment.
4.Send a monthly email with their credit rating and offers for credit-related services at market rates.
5.Charge your company 20% of the cost of any credit restoration.
You execute the contract and the enrollment invitations are emailed to the 2000 individuals. Three days later you sit down and document all that went well and all that could have gone better. You put it in a file to reference the next time an incident occurs.
Which of the following was done CORRECTLY during the above incident?
A. The process by which affected individuals sign up for email notifications
B. Your assessment of which credit monitoring company you should hire
C. The speed at which you sat down to reflect and document the incident
D. Finding a vendor who will offer the affected individuals additional services
Answer: C (LEAVE A REPLY)
Explanation
This answer is the only thing that was done correctly during the incident, as it shows a good practice of learning from and improving on the incident response process. The speed at which you sat down to reflect and document the incident means that you did not delay or postpone this important step, which can help you to capture and analyze what went well and what could have gone better during the incident, as well as to identify any lessons learned, best practices or recommendations for future incidents. Documenting and reflecting on the incident can also help you to update and improve your privacy policies, procedures and safeguards, as well as to demonstrate your accountability and compliance with any legal or contractual obligations.

NEW QUESTION: 96
SCENARIO

Please use the following to answer the next QUESTION:
Your organization, the Chicago (U.S.)-based Society for Urban Greenspace, has used the same vendor to operate all aspects of an online store for several years. As a small nonprofit, the Society cannot afford the higher-priced options, but you have been relatively satisfied with this budget vendor, Shopping Cart Saver (SCS). Yes, there have been some issues. Twice, people who purchased items from the store have had their credit card information used fraudulently subsequent to transactions on your site, but in neither case did the investigation reveal with certainty that the Society's store had been hacked. The thefts could have been employee-related.
Just as disconcerting was an incident where the organization discovered that SCS had sold information it had collected from customers to third parties. However, as Jason Roland, your SCS account representative, points out, it took only a phone call from you to clarify expectations and the "misunderstanding" has not occurred again.
As an information-technology program manager with the Society, the role of the privacy professional is only one of many you play. In all matters, however, you must consider the financial bottom line. While these problems with privacy protection have been significant, the additional revenues of sales of items such as shirts and coffee cups from the store have been significant. The Society's operating budget is slim, and all sources of revenue are essential.
Now a new challenge has arisen. Jason called to say that starting in two weeks, the customer data from the store would now be stored on a data cloud. "The good news," he says, "is that we have found a low-cost provider in Finland, where the data would also be held. So, while there may be a small charge to pass through to you, it won't be exorbitant, especially considering the advantages of a cloud." Lately, you have been hearing about cloud computing and you know it's fast becoming the new paradigm for various applications. However, you have heard mixed reviews about the potential impacts on privacy protection. You begin to research and discover that a number of the leading cloud service providers have signed a letter of intent to work together on shared conventions and technologies for privacy protection. You make a note to find out if Jason's Finnish provider is signing on.
What process can best answer your Questions about the vendor's data security safeguards?
A. A public records search for earlier legal violations
B. A second-party of supplier audit
C. A table top demonstration of a potential threat
D. A reference check with other clients
Answer: (SHOW ANSWER)

NEW QUESTION: 97
SCENARIO
Please use the following to answer the next QUESTION:
Ben works in the IT department of IgNight, Inc., a company that designs lighting solutions for its clients. Although IgNight's customer base consists primarily of offices in the US, some individuals have been so impressed by the unique aesthetic and energy-saving design of the light fixtures that they have requested IgNight's installations in their homes across the globe.

One Sunday morning, while using his work laptop to purchase tickets for an upcoming music festival, Ben happens to notice some unusual user activity on company files. From a cursory review, all the data still appears to be where it is meant to be but he can't shake off the feeling that something is not right. He knows that it is a possibility that this could be a colleague performing unscheduled maintenance, but he recalls an email from his company's security team reminding employees to be on alert for attacks from a known group of malicious actors specifically targeting the industry.

Ben is a diligent employee and wants to make sure that he protects the company but he does not want to bother his hard-working colleagues on the weekend. He is going to discuss the matter with this manager first thing in the morning but wants to be prepared so he can demonstrate his knowledge in this area and plead his case for a promotion.

If this were a data breach, how is it likely to be categorized?

A. Availability Breach.

B. Authenticity Breach.

C. Confidentiality Breach.

D. Integrity Breach.

Answer: C (LEAVE A REPLY)

Explanation

If this were a data breach, it is likely to be categorized as a confidentiality breach. A confidentiality breach is a type of data breach that involves unauthorized or accidental disclosure of or access to personal data. A confidentiality breach violates the principle of confidentiality, which requires that personal data is protected from unauthorized or unlawful use or disclosure. A confidentiality breach can occur when personal data is exposed to unauthorized parties, such as hackers, competitors, or third parties without consent. A confidentiality breach can also occur when personal data is sent to incorrect recipients, such as by email or mail.

The other options are not likely to be the correct category for this data breach. An availability breach is a type of data breach that involves accidental or unauthorized loss of access to or destruction of personal data. An availability breach violates the principle of availability, which requires that personal data is accessible and usable by authorized parties when needed. An availability breach can occur when personal data is deleted, corrupted, encrypted, or otherwise rendered inaccessible by malicious actors or technical errors. An authenticity breach is a type of data breach that involves unauthorized or accidental alteration of personal data.

An authenticity breach violates the principle of authenticity, which requires that personal data is accurate and up to date. An authenticity breach can occur when personal data is modified, tampered with, or falsified by malicious actors or human errors. An integrity breach is a type of data breach that involves unauthorized or accidental alteration of personal data that affects its quality or reliability. An integrity breach violates the principle of integrity, which requires that personal data is complete and consistent with its intended purpose. An integrity breach can occur when personal data is incomplete, inconsistent, outdated, or inaccurate due to malicious actors or human errors. References: Personal Data Breaches: A Guide; Guidance on the Categorisation and Notification of Personal Data Breaches

NEW QUESTION: 98

SCENARIO
Please use the following to answer the next QUESTION:
As the Director of data protection for Consolidated Records Corporation, you are justifiably pleased with your accomplishments so far. Your hiring was precipitated by warnings from regulatory agencies following a series of relatively minor data breaches that could easily have been worse. However, you have not had a reportable incident for the three years that you have been with the company. In fact, you consider your program a model that others in the data storage industry may note in their own program development.
You started the program at Consolidated from a jumbled mix of policies and procedures and worked toward coherence across departments and throughout operations. You were aided along the way by the program's sponsor, the vice president of operations, as well as by a Privacy Team that started from a clear understanding of the need for change.
Initially, your work was greeted with little confidence or enthusiasm by the company's "old guard" among both the executive team and frontline personnel working with data and interfacing with clients. Through the use of metrics that showed the costs not only of the breaches that had occurred, but also projections of the costs that easily could occur given the current state of operations, you soon had the leaders and key decision-makers largely on your side. Many of the other employees were more resistant, but face-to-face meetings with each department and the development of a baseline privacy training program achieved sufficient "buy-in" to begin putting the proper procedures into place.
Now, privacy protection is an accepted component of all current operations involving personal or protected data and must be part of the end product of any process of technological development. While your approach is not systematic, it is fairly effective.
You are left contemplating:
What must be done to maintain the program and develop it beyond just a data breach prevention program?
How can you build on your success?
What are the next action steps?
How can Consolidated's privacy training program best be further developed?
A. Through targeted curricula designed for specific departments.
B. By adopting e-learning to reduce the need for instructors.
C. By using industry standard off-the-shelf programs.
D. Through a review of recent data breaches.
Answer: A (LEAVE A REPLY)
Explanation
This would allow Consolidated to tailor the privacy training to the specific needs and risks of each department, and to ensure that the employees are aware of the relevant policies and procedures for their roles.

NEW QUESTION: 99
SCENARIO
Please use the following to answer the next QUESTION:
Martin Briseno is the director of human resources at the Canyon City location of the U.S. hotel chain Pacific Suites. In 1998, Briseno decided to change the hotel's on-the-job mentoring model to a standardized training program for employees who were progressing from line positions into supervisory positions. He developed a

curriculum comprising a series of lessons, scenarios, and assessments, which was delivered in-person to small groups. Interest in the training increased, leading Briseno to work with corporate HR specialists and software engineers to offer the program in an online format. The online program saved the cost of a trainer and allowed participants to work through the material at their own pace.

Upon hearing about the success of Briseno's program, Pacific Suites corporate Vice President Maryanne Silva-Hayes expanded the training and offered it company-wide. Employees who completed the program received certification as a Pacific Suites Hospitality Supervisor. By 2001, the program had grown to provide industry-wide training. Personnel at hotels across the country could sign up and pay to take the course online.

As the program became increasingly profitable, Pacific Suites developed an offshoot business, Pacific Hospitality Training (PHT). The sole focus of PHT was developing and marketing a variety of online courses and course progressions providing a number of professional certifications in the hospitality industry.

By setting up a user account with PHT, course participants could access an information library, sign up for courses, and take end-of-course certification tests. When a user opened a new account, all information was saved by default, including the user's name, date of birth, contact information, credit card information, employer, and job title. The registration page offered an opt-out choice that users could click to not have their credit card numbers saved. Once a user name and password were established, users could return to check their course status, review and reprint their certifications, and sign up and pay for new courses. Between 2002 and

2008, PHT issued more than 700,000 professional certifications.

PHT's profits declined in 2009 and 2010, the victim of industry downsizing and increased competition from e-learning providers. By 2011, Pacific Suites was out of the online certification business and PHT was dissolved.

The training program's systems and records remained in Pacific Suites' digital archives, un-accessed and unused. Briseno and Silva-Hayes moved on to work for other companies, and there was no plan for handling the archived data after the program ended. After PHT was dissolved, Pacific Suites executives turned their attention to crucial day-to-day operations. They planned to deal with the PHT materials once resources allowed.

In 2012, the Pacific Suites computer network was hacked. Malware installed on the online reservation system exposed the credit card information of hundreds of hotel guests. While targeting the financial data on the reservation site, hackers also discovered the archived training course data and registration accounts of Pacific Hospitality Training's customers. The result of the hack was the exfiltration of the credit card numbers of recent hotel guests and the exfiltration of the PHT database with all its contents.

A Pacific Suites systems analyst discovered the information security breach in a routine scan of activity reports. Pacific Suites quickly notified credit card companies and recent hotel guests of the breach, attempting to prevent serious harm. Technical security engineers faced a challenge in dealing with the PHT data.

PHT course administrators and the IT engineers did not have a system for tracking, cataloguing, and storing information. Pacific Suites has procedures in place for data access and storage, but those procedures were not implemented when PHT was formed. When the PHT database was acquired by Pacific Suites, it had no owner or oversight. By the time technical security engineers determined what private information was compromised, at least 8,000 credit card holders were potential victims of fraudulent activity.

How was Pacific Suites responsible for protecting the sensitive information of its offshoot, PHT?

A. As the parent company, it should have performed an assessment of PHT's infrastructure and confirmed complete separation of the two networks.
B. As the parent company, it should have replaced PHT's electronic files with hard-copy documents stored securely on site.
C. As the parent company, it should have transferred personnel to oversee the secure handling of PHT's data.
D. As the parent company, it should have ensured its existing data access and storage procedures were integrated into PHT's system.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 100
Which of the following is an example of Privacy by Design (PbD)?
A. The information technology group uses privacy considerations to inform the development of new networking software.
B. A labor union insists that the details of employers' data protection methods be documented in a new contract.
C. The human resources group develops a training program from employees to become certified in privacy policy.
D. A company hires a professional to structure a privacy program that anticipates the increasing demands of new laws.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 101
SCENARIO
Please use the following to answer the next QUESTION:
Edufox has hosted an annual convention of users of its famous e-learning software platform, and over time, it has become a grand event. It fills one of the large downtown conference hotels and overflows into the others, with several thousand attendees enjoying three days of presentations, panel discussions and networking. The convention is the centerpiece of the company's product rollout schedule and a great training opportunity for current users. The sales force also encourages prospective clients to attend to get a better sense of the ways in which the system can be customized to meet diverse needs and understand that when they buy into this system, they are joining a community that feels like family.
This year's conference is only three weeks away, and you have just heard news of a new initiative supporting it: a smartphone app for attendees. The app will support late registration, highlight the featured presentations and provide a mobile version of the conference program. It also links to a restaurant reservation system with the best cuisine in the areas featured. "It's going to be great," the developer, Deidre Hoffman, tells you, "if, that is, we actually get it working!" She laughs nervously but explains that because of the tight time frame she'd been given to build the app, she outsourced the job to a local firm. "It's just three young people," she says, "but they do great work." She describes some of the other apps they have built. When asked how they were selected for this job, Deidre shrugs. "They do good work, so I chose them." Deidre is a terrific employee with a strong track record. That's why she's been charged to deliver this rushed project. You're sure she has

the best interests of the company at heart, and you don't doubt that she's under pressure to meet a deadline that cannot be pushed back. However, you have concerns about the app's handling of personal data and its security safeguards. Over lunch in the break room, you start to talk to her about it, but she quickly tries to reassure you, "I'm sure with your help we can fix any security issues if we have to, but I doubt there'll be any. These people build apps for a living, and they know what they're doing. You worry too much, but that's why you're so good at your job!" You see evidence that company employees routinely circumvent the privacy officer in developing new initiatives.

How can you best draw attention to the scope of this problem?

A. Develop a metric showing the number of initiatives launched without consultation and include it in reports, presentations, and consultation.

B. Take your concerns straight to the Chief Executive Officer.

C. Insist upon one-on-one consultation with each person who works around the privacy officer.

D. Hold discussions with the department head of anyone who fails to consult with the privacy officer.

Answer: (SHOW ANSWER)

NEW QUESTION: 102

SCENARIO

Please use the following to answer the next question:

Your organization, the Chicago (U.S.)-based Society for Urban Greenspace, has used the same vendor to operate all aspects of an online store for several years. As a small nonprofit, the Society cannot afford the higher-priced options, but you have been relatively satisfied with this budget vendor, Shopping Cart Saver (SCS). Yes, there have been some issues. Twice, people who purchased items from the store have had their credit card information used fraudulently subsequent to transactions on your site, but in neither case did the investigation reveal with certainty that the Society's store had been hacked. The thefts could have been employee-related.

Just as disconcerting was an incident where the organization discovered that SCS had sold information it had collected from customers to third parties. However, as Jason Roland, your SCS account representative, points out, it took only a phone call from you to clarify expectations and the "misunderstanding" has not occurred again.

As an information-technology program manager with the Society, the role of the privacy professional is only one of many you play. In all matters, however, you must consider the financial bottom line. While these problems with privacy protection have been significant, the additional revenues of sales of items such as shirts and coffee cups from the store have been significant. The Society's operating budget is slim, and all sources of revenue are essential.

Now a new challenge has arisen. Jason called to say that starting in two weeks, the customer data from the store would now be stored on a data cloud. "The good news," he says, "is that we have found a low-cost provider in Finland, where the data would also be held. So, while there may be a small charge to pass through to you, it won't be exorbitant, especially considering the advantages of a cloud." Lately, you have been hearing about cloud computing and you know it's fast becoming the new paradigm for various applications. However, you have heard mixed reviews about the potential impacts on privacy protection. You begin to research and discover that a number of the leading cloud service providers have signed a letter of

intent to work together on shared conventions and technologies for privacy protection. You make a note to find out if Jason's Finnish provider is signing on.
What is the best way to prevent the Finnish vendor from transferring data to another party?
A. Lock the data down in its current location
B. Restrict the vendor to using company security controls
C. Include transfer prohibitions in the vendor contract
D. Offer company resources to assist with the processing
Answer: C (LEAVE A REPLY)

NEW QUESTION: 103
What are you doing if you succumb to "overgeneralization" when analyzing data from metrics?
A. Using data that is too broad to capture specific meanings
B. Possessing too many types of data to perform a valid analysis
C. Using limited data in an attempt to support broad conclusions
D. Trying to use several measurements to gauge one aspect of a program
Answer: (SHOW ANSWER)
Explanation/Reference: https://www.researchgate.net/publication/226716755_The_Impact_of_Overfitting_and_Overgeneralization_on_the_Classification_Accuracy_in_Data_Mining

NEW QUESTION: 104
SCENARIO
Please use the following to answer the next QUESTION:
Paul Daniels, with years of experience as a CEO, is worried about his son Carlton's successful venture, Gadgo. A technological innovator in the communication industry that quickly became profitable, Gadgo has moved beyond its startup phase. While it has retained its vibrant energy, Paul fears that under Carlton's direction, the company may not be taking its risks or obligations as seriously as it needs to. Paul has hired you, a Privacy Consultant, to assess the company and report to both father and son. "Carlton won't listen to me," Paul says, "but he may pay attention to an expert." Gadgo's workplace is a clubhouse for innovation, with games, toys, snacks. espresso machines, giant fish tanks and even an iguana who regards you with little interest. Carlton, too, seems bored as he describes to you the company's procedures and technologies for data protection. It's a loose assemblage of controls, lacking consistency and with plenty of weaknesses. "This is a technology company," Carlton says. "We create. We innovate. I don't want unnecessary measures that will only slow people down and clutter their thoughts." The meeting lasts until early evening. Upon leaving, you walk through the office it looks as if a strong windstorm has recently blown through, with papers scattered across desks and tables and even the floor. A "cleaning crew" of one teenager is emptying the trash bins. A few computers have been left on for the night, others are missing. Carlton takes note of your attention to this: "Most of my people take their laptops home with them, or use their own tablets or phones. I want them to use whatever helps them to think and be ready day or night for that great insight. It may only come once!" What would be the best kind of audit to recommend for Gadgo?
A. An internal audit.

B. A supplier audit.
C. A third-party audit.
D. A self-certification.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 105
SCENARIO
Please use the following to answer the next QUESTION:
For 15 years, Albert has worked at Treasure Box - a mail order company in the United States (U.S.) that used to sell decorative candles around the world, but has recently decided to limit its shipments to customers in the 48 contiguous states. Despite his years of experience, Albert is often overlooked for managerial positions. His frustration about not being promoted, coupled with his recent interest in issues of privacy protection, have motivated Albert to be an agent of positive change.
He will soon interview for a newly advertised position, and during the interview, Albert plans on making executives aware of lapses in the company's privacy program. He feels certain he will be rewarded with a promotion for preventing negative consequences resulting from the company's outdated policies and procedures.
For example, Albert has learned about the AICPA (American Institute of Certified Public Accountans)/CICA (Canadian Institute of Chartered Accountants) Privacy Maturity Model (PMM). Albert thinks the model is a useful way to measure Treasure Box's ability to protect personal data. Albert has noticed that Treasure Box fails to meet the requirements of the highest level of maturity of this model; at his interview, Albert will pledge to assist the company with meeting this level in order to provide customers with the most rigorous security available.
Albert does want to show a positive outlook during his interview. He intends to praise the company's commitment to the security of customer and employee personal data against external threats. However, Albert worries about the high turnover rate within the company, particularly in the area of direct phone marketing. He sees many unfamiliar faces every day who are hired to do the marketing, and he often hears complaints in the lunch room regarding long hours and low pay, as well as what seems to be flagrant disregard for company procedures.
In addition, Treasure Box has had two recent security incidents. The company has responded to the incidents with internal audits and updates to security safeguards. However, profits still seem to be affected and anecdotal evidence indicates that many people still harbor mistrust. Albert wants to help the company recover.
He knows there is at least one incident the public in unaware of, although Albert does not know the details. He believes the company's insistence on keeping the incident a secret could be a further detriment to its reputation. One further way that Albert wants to help Treasure Box regain its stature is by creating a toll-free number for customers, as well as a more efficient procedure for responding to customer concerns by postal mail.
In addition to his suggestions for improvement, Albert believes that his knowledge of the company's recent business maneuvers will also impress the interviewers. For example, Albert is aware of the company's intention to acquire a medical supply company in the coming weeks.

With his forward thinking, Albert hopes to convince the managers who will be interviewing him that he is right for the job.
On which of the following topics does Albert most likely need additional knowledge?
A. The possibility of delegating responsibilities related to privacy
B. The requirements for a managerial position with privacy protection duties
C. The role of privacy in retail companies
D. The necessary maturity level of privacy programs
Answer: A (LEAVE A REPLY)

NEW QUESTION: 106
As a Data Protection Officer, one of your roles entails monitoring changes in laws and regulations and updating policies accordingly.
How would you most effectively execute this responsibility?
A. Consult an external lawyer.
B. Regularly engage regulators.
C. Attend workshops and interact with other professionals.
D. Subscribe to email list-serves that report on regulatory changes.
Answer: D (LEAVE A REPLY)
Explanation
As a Data Protection Officer (DPO), one of the most effective ways to execute your responsibility of monitoring changes in laws and regulations and updating policies accordingly is to subscribe to email list-serves that report on regulatory changes. Email list-serves are online mailing lists that allow subscribers to receive regular updates on topics or issues of interest via email7 By subscribing to email list-serves that report on regulatory changes, you can stay informed of the latest developments and trends in the regulatory environment that affect your organization and its data protection practices. You can also access relevant information and resources from reliable sources, such as regulatory agencies, law firms, industry associations, or experts8 This can help you to identify and analyze the impact of regulatory changes on your organization and its data processing activities, and to update your policies and procedures accordingly to ensure compliance8 Some examples of email list-serves that report on regulatory changes are:
* The ICO Newsletter: This is a monthly newsletter from the UK Information Commissioner's Office (ICO) that provides updates on data protection news, guidance, events, consultations, and enforcement actions9
* The Privacy Advisor: This is a monthly newsletter from the International Association of Privacy Professionals (IAPP) that covers global privacy news, analysis, and insights10
* The Privacy & Data Security Law Journal: This is a monthly journal from LexisNexis that provides articles and case notes on privacy and data security law issues from around the world11
* The Data Protection Report: This is a blog from Norton Rose Fulbright that provides updates and commentary on data protection and cybersecurity developments across various jurisdictions12 References: 7: What is a listserv?; 8: 5 Practical Ways to Keep Up with Regulatory Changes; 9: ICO Newsletter; 10: The Privacy Advisor; 11: Privacy & Data Security Law Journal; 12: Data Protection Report

NEW QUESTION: 107

SCENARIO

Please use the following to answer the next QUESTION:

Henry Home Furnishings has built high-end furniture for nearly forty years. However, the new owner, Anton, has found some degree of disorganization after touring the company headquarters. His uncle Henry had always focused on production - not data processing - and Anton is concerned. In several storage rooms, he has found paper files, disks, and old computers that appear to contain the personal data of current and former employees and customers. Anton knows that a single break-in could irrevocably damage the company's relationship with its loyal customers. He intends to set a goal of guaranteed zero loss of personal information.

To this end, Anton originally planned to place restrictions on who was admitted to the physical premises of the company. However, Kenneth - his uncle's vice president and longtime confidante - wants to hold off on Anton's idea in favor of converting any paper records held at the company to electronic storage. Kenneth believes this process would only take one or two years. Anton likes this idea; he envisions a password-protected system that only he and Kenneth can access.

Anton also plans to divest the company of most of its subsidiaries. Not only will this make his job easier, but it will simplify the management of the stored data. The heads of subsidiaries like the art gallery and kitchenware store down the street will be responsible for their own information management. Then, any unneeded subsidiary data still in Anton's possession can be destroyed within the next few years.

After learning of a recent security incident, Anton realizes that another crucial step will be notifying customers. Kenneth insists that two lost hard drives in Question are not cause for concern; all of the data was encrypted and not sensitive in nature. Anton does not want to take any chances, however. He intends on sending notice letters to all employees and customers to be safe.

Anton must also check for compliance with all legislative, regulatory, and market requirements related to privacy protection. Kenneth oversaw the development of the company's online presence about ten years ago, but Anton is not confident about his understanding of recent online marketing laws. Anton is assigning another trusted employee with a law background the task of the compliance assessment. After a thorough analysis, Anton knows the company should be safe for another five years, at which time he can order another check.

Documentation of this analysis will show auditors due diligence.

Anton has started down a long road toward improved management of the company, but he knows the effort is worth it. Anton wants his uncle's legacy to continue for many years to come.

What would the company's legal team most likely recommend to Anton regarding his planned communication with customers?

A. To shift to electronic communication.

B. To delay communications until local authorities are informed.
C. To consider under what circumstances communication is necessary.
D. To send consistent communication.
Answer: (SHOW ANSWER)

NEW QUESTION: 108
SCENARIO
Please use the following to answer the next question:
Edufox has hosted an annual convention of users of its famous e-learning software platform, and over time, it has become a grand event. It fills one of the large downtown conference hotels and overflows into the others, with several thousand attendees enjoying three days of presentations, panel discussions and networking. The convention is the centerpiece of the company's product rollout schedule and a great training opportunity for current users. The sales force also encourages prospective clients to attend to get a better sense of the ways in which the system can be customized to meet diverse needs and understand that when they buy into this system, they are joining a community that feels like family.
This year's conference is only three weeks away, and you have just heard news of a new initiative supporting it: a smartphone app for attendees. The app will support late registration, highlight the featured presentations and provide a mobile version of the conference program. It also links to a restaurant reservation system with the best cuisine in the areas featured. "It's going to be great," the developer, Deidre Hoffman, tells you, "if, that is, we actually get it working!" She laughs nervously but explains that because of the tight time frame she'd been given to build the app, she outsourced the job to a local firm. "It's just three young people," she says, "but they do great work." She describes some of the other apps they have built. When asked how they were selected for this job, Deidre shrugs. "They do good work, so I chose them." Deidre is a terrific employee with a strong track record. That's why she's been charged to deliver this rushed project. You're sure she has the best interests of the company at heart, and you don't doubt that she's under pressure to meet a deadline that cannot be pushed back. However, you have concerns about the app's handling of personal data and its security safeguards. Over lunch in the break room, you start to talk to her about it, but she quickly tries to reassure you, "I'm sure with your help we can fix any security issues if we have to, but I doubt there'll be any. These people build apps for a living, and they know what they're doing. You worry too much, but that's why you're so good at your job!" You want to point out that normal protocols have not been followed in this matter. Which process in particular has been neglected?
A. Forensic inquiry
B. Privacy breach prevention
C. Data mapping
D. Vendor due diligence or vetting
Answer: (SHOW ANSWER)

NEW QUESTION: 109
SCENARIO
Please use the following to answer the next question:

As the director of data protection for Consolidated Records Corporation, you are justifiably pleased with your accomplishments so far. Your hiring was precipitated by warnings from regulatory agencies following a series of relatively minor data breaches that could easily have been worse. However, you have not had a reportable incident for the three years that you have been with the company. In fact, you consider your program a model that others in the data storage industry may note in their own program development.
You started the program at Consolidated from a jumbled mix of policies and procedures and worked toward coherence across departments and throughout operations. You were aided along the way by the program's sponsor, the vice president of operations, as well as by a Privacy Team that started from a clear understanding of the need for change.
Initially, your work was greeted with little confidence or enthusiasm by the company's "old guard" among both the executive team and frontline personnel working with data and interfacing with clients. Through the use of metrics that showed the costs not only of the breaches that had occurred, but also projections of the costs that easily could occur given the current state of operations, you soon had the leaders and key decision-makers largely on your side. Many of the other employees were more resistant, but face-to-face meetings with each department and the development of a baseline privacy training program achieved sufficient "buy-in" to begin putting the proper procedures into place.
Now, privacy protection is an accepted component of all current operations involving personal or protected data and must be part of the end product of any process of technological development. While your approach is not systematic, it is fairly effective.
You are left contemplating: What must be done to maintain the program and develop it beyond just a data breach prevention program? How can you build on your success? What are the next action steps?
What stage of the privacy operational life cycle best describes Consolidated's current privacy program?
A. Protect
B. Sustain
C. Respond
D. Assess
Answer: B (LEAVE A REPLY)

NEW QUESTION: 110
SCENARIO
Please use the following to answer the next QUESTION:
John is the new privacy officer at the prestigious international law firm - A&M LLP. A&M LLP is very proud of its reputation in the practice areas of Trusts & Estates and Merger & Acquisition in both U.S. and Europe.
During lunch with a colleague from the Information Technology department, John heard that the Head of IT, Derrick, is about to outsource the firm's email continuity service to their existing email security vendor - MessageSafe. Being successful as an email hygiene vendor, MessageSafe is expanding its business by leasing cloud infrastructure from Cloud Inc. to host email continuity service for A&M LLP.
John is very concerned about this initiative. He recalled that MessageSafe was in the news six months ago due to a security breach. Immediately, John did a quick research of MessageSafe's previous breach and learned that the breach was caused by an unintentional mistake by an IT administrator. He scheduled a meeting with Derrick to address his concerns.

At the meeting, Derrick emphasized that email is the primary method for the firm's lawyers to communicate with clients, thus it is critical to have the email continuity service to avoid any possible email downtime. Derrick has been using the anti-spam service provided by MessageSafe for five years and is very happy with the quality of service provided by MessageSafe. In addition to the significant discount offered by MessageSafe, Derrick emphasized that he can also speed up the onboarding process since the firm already has a service contract in place with MessageSafe. The existing on-premises email continuity solution is about to reach its end of life very soon and he doesn't have the time or resource to look for another solution. Furthermore, the off-premises email continuity service will only be turned on when the email service at A&M LLP's primary and secondary data centers are both down, and the email messages stored at MessageSafe site for continuity service will be automatically deleted after 30 days.
Which of the following is the most effective control to enforce MessageSafe's implementation of appropriate technical countermeasures to protect the personal data received from A&M LLP?
A. MessageSafe must notify A&M LLP of a data breach.
B. MessageSafe must apply appropriate security controls on the cloud infrastructure.
C. MessageSafe must flow-down its data protection contract terms with A&M LLP to Cloud Inc.
D. MessageSafe must apply due diligence before trusting Cloud Inc. with the personal data received from A&M LLP.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 111
SCENARIO
Please use the following to answer the next QUESTION:
Natalia, CFO of the Nationwide Grill restaurant chain, had never seen her fellow executives so anxious. Last week, a data processing firm used by the company reported that its system may have been hacked, and customer data such as names, addresses, and birthdays may have been compromised. Although the attempt was proven unsuccessful, the scare has prompted several Nationwide Grill executives to Question the company's privacy program at today's meeting.
Alice, a vice president, said that the incident could have opened the door to lawsuits, potentially damaging Nationwide Grill's market position. The Chief Information Officer (CIO), Brendan, tried to assure her that even if there had been an actual breach, the chances of a successful suit against the company were slim. But Alice remained unconvinced.
Spencer - a former CEO and currently a senior advisor - said that he had always warned against the use of contractors for data processing. At the very least, he argued, they should be held contractually liable for telling customers about any security incidents. In his view, Nationwide Grill should not be forced to soil the company name for a problem it did not cause.
One of the business development (BD) executives, Haley, then spoke, imploring everyone to see reason. "Breaches can happen, despite organizations' best efforts," she remarked. "Reasonable preparedness is key." She reminded everyone of the incident seven years ago when the large grocery chain Tinkerton's had its financial information compromised after a large order of Nationwide Grill frozen dinners. As a long-time BD executive with a solid understanding of Tinkerton's's corporate culture, built up through many years of cultivating relationships, Haley was able to successfully manage the company's incident response.

Spencer replied that acting with reason means allowing security to be handled by the security functions within the company - not BD staff. In a similar way, he said, Human Resources (HR) needs to do a better job training employees to prevent incidents. He pointed out that Nationwide Grill employees are overwhelmed with posters, emails, and memos from both HR and the ethics department related to the company's privacy program. Both the volume and the duplication of information means that it is often ignored altogether.
Spencer said, "The company needs to dedicate itself to its privacy program and set regular in-person trainings for all staff once a month." Alice responded that the suggestion, while well-meaning, is not practical. With many locations, local HR departments need to have flexibility with their training schedules. Silently, Natalia agreed.
Based on the scenario, Nationwide Grill needs to create better employee awareness of the company's privacy program by doing what?
A. Varying the modes of communication.
B. Communicating to the staff more often.
C. Improving inter-departmental cooperation.
D. Requiring acknowledgment of company memos.
Answer: A (LEAVE A REPLY)
Explanation
This answer is the best way to create better employee awareness of the company's privacy program, as it can increase the effectiveness and retention of the information by appealing to different learning styles and preferences. Varying the modes of communication can include using different formats and channels, such as posters, emails, memos, videos, webinars, podcasts, newsletters, quizzes, games or interactive modules. Varying the modes of communication can also help to avoid information overload or duplication, which may cause employees to ignore or disregard the privacy messages. References: IAPP CIPM Study Guide, page 90; ISO/IEC 27002:2013, section 7.2.2

NEW QUESTION: 112
SCENARIO
Please use the following to answer the next QUESTION:
Paul Daniels, with years of experience as a CEO, is worried about his son Carlton's successful venture, Gadgo. A technological innovator in the communication industry that quickly became profitable, Gadgo has moved beyond its startup phase. While it has retained its vibrant energy, Paul fears that under Carlton's direction, the company may not be taking its risks or obligations as seriously as it needs to. Paul has hired you, a Privacy Consultant, to assess the company and report to both father and son. "Carlton won't listen to me," Paul says, "but he may pay attention to an expert." Gadgo's workplace is a clubhouse for innovation, with games, toys, snacks. espresso machines, giant fish tanks and even an iguana who regards you with little interest. Carlton, too, seems bored as he describes to you the company's procedures and technologies for data protection. It's a loose assemblage of controls, lacking consistency and with plenty of weaknesses. "This is a technology company," Carlton says. "We create. We innovate. I don't want unnecessary measures that will only slow people down and clutter their thoughts." The meeting lasts until early evening. Upon leaving, you walk through the office it looks as if a strong windstorm has recently blown through, with papers scattered across desks and tables and even the floor. A "cleaning crew" of one teenager is emptying the trash bins. A

few computers have been left on for the night, others are missing. Carlton takes note of your attention to this: "Most of my people take their laptops home with them, or use their own tablets or phones. I want them to use whatever helps them to think and be ready day or night for that great insight. It may only come once!" What phase in the Privacy Maturity Model (PMM) does Gadgo's privacy program best exhibit?
A. Ad hoc.
B. Managed.
C. Defined.
D. Repeatable.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 113
What is the key factor that lays the foundation for all other elements of a privacy program?
A. The applicable privacy regulations
B. The structure of a privacy team
C. A privacy mission statement
D. A responsible internal stakeholder
Answer: D (LEAVE A REPLY)
Explanation
This answer is the key factor that lays the foundation for all other elements of a privacy program, as it can help to establish leadership, accountability and support for the privacy program within the organization. A responsible internal stakeholder is a person or group who has authority, influence or interest in the organization's data processing activities, such as senior management, board members, business units or departments. A responsible internal stakeholder can help to define and communicate the organization's vision, mission and goals for privacy protection, allocate resources and budget for the privacy program, approve and endorse privacy policies and procedures, monitor and evaluate privacy program performance and compliance, and resolve any issues or conflicts that may arise from data processing activities.

NEW QUESTION: 114
What United States federal law requires financial institutions to declare their personal data collection practices?
A. The Kennedy-Hatch Disclosure Act of 1997.
B. The Gramm-Leach-Bliley Act of 1999.
C. SUPCLA, or the federal Superprivacy Act of 2001.
D. The Financial Portability and Accountability Act of 2006.
Answer: B (LEAVE A REPLY)
Explanation
The United States federal law that requires financial institutions to declare their personal data collection practices is the Gramm-Leach-Bliley Act (GLBA) of 1999. The GLBA is also known as the Financial Services Modernization Act or the Financial Modernization Act10 The GLBA regulates how financial institutions collect, use, disclose, and protect the nonpublic personal information of their customers11 The GLBA requires financial institutions to provide a privacy notice to their customers that explains what kinds of information they

collect, how they use and share that information, and how they safeguard that information12 The GLBA also gives customers the right to opt out of certain information sharing practices with third parties13 The other options are not US federal laws that require financial institutions to declare their personal data collection practices. The Kennedy-Hatch Disclosure Act of 1997 is a proposed but not enacted legislation that would have required health insurers to disclose their policies and practices regarding the use and disclosure of genetic information14 SUPCLA, or the federal Superprivacy Act of 2001, is a fictional law that does not exist in reality. The Financial Portability and Accountability Act of 2006 is also a fictional law that does not exist in reality, although it may be confused with the Health Insurance Portability and Accountability Act (HIPAA) of 1996, which regulates the privacy and security of health information15 References: 10: Gramm-Leach-Bliley Act | Federal Trade Commission; 11: Financial Privacy | Federal Trade Commission; 12: Financial Privacy | Federal Trade Commission; 13: Financial Privacy | Federal Trade Commission; 14: S. 422 (105th): Genetic Information Nondiscrimination in Health Insurance Act of 1997; 15: Health Information Privacy | HHS.gov

NEW QUESTION: 115
Under which circumstances would people who work in human resources be considered a secondary audience for privacy metrics?
A. They do not interface with the financial office
B. They do not have privacy policy as their main task
C. They do not have frequent interactions with the public
D. They do not receive training on privacy issues
Answer: B (LEAVE A REPLY)

NEW QUESTION: 116
SCENARIO
Please use the following to answer the next QUESTION:
Natalia, CFO of the Nationwide Grill restaurant chain, had never seen her fellow executives so anxious. Last week, a data processing firm used by the company reported that its system may have been hacked, and customer data such as names, addresses, and birthdays may have been compromised. Although the attempt was proven unsuccessful, the scare has prompted several Nationwide Grill executives to Question the company's privacy program at today's meeting.
Alice, a vice president, said that the incident could have opened the door to lawsuits, potentially damaging Nationwide Grill's market position. The Chief Information Officer (CIO), Brendan, tried to assure her that even if there had been an actual breach, the chances of a successful suit against the company were slim. But Alice remained unconvinced.
Spencer - a former CEO and currently a senior advisor - said that he had always warned against the use of contractors for data processing. At the very least, he argued, they should be held contractually liable for telling customers about any security incidents. In his view, Nationwide Grill should not be forced to soil the company name for a problem it did not cause.
One of the business development (BD) executives, Haley, then spoke, imploring everyone to see reason. "Breaches can happen, despite organizations' best efforts," she remarked. "Reasonable preparedness is key." She reminded everyone of the incident seven years ago when the large grocery chain Tinkerton's had

its financial information compromised after a large order of Nationwide Grill frozen dinners. As a long-time BD executive with a solid understanding of Tinkerton's's corporate culture, built up through many years of cultivating relationships, Haley was able to successfully manage the company's incident response.
Spencer replied that acting with reason means allowing security to be handled by the security functions within the company - not BD staff. In a similar way, he said, Human Resources (HR) needs to do a better job training employees to prevent incidents. He pointed out that Nationwide Grill employees are overwhelmed with posters, emails, and memos from both HR and the ethics department related to the company's privacy program. Both the volume and the duplication of information means that it is often ignored altogether.
Spencer said, "The company needs to dedicate itself to its privacy program and set regular in-person trainings for all staff once a month." Alice responded that the suggestion, while well-meaning, is not practical. With many locations, local HR departments need to have flexibility with their training schedules. Silently, Natalia agreed.
Based on the scenario, Nationwide Grill needs to create better employee awareness of the company's privacy program by doing what?
A. Improving inter-departmental cooperation.
B. Communicating to the staff more often.
C. Requiring acknowledgment of company memos.
D. Varying the modes of communication.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 117
SCENARIO
Please use the following to answer the next QUESTION:
Perhaps Jack Kelly should have stayed in the U.S. He enjoys a formidable reputation inside the company, Special Handling Shipping, for his work in reforming certain "rogue" offices. Last year, news broke that a police sting operation had revealed a drug ring operating in the Providence, Rhode Island office in the United States. Video from the office's video surveillance cameras leaked to news operations showed a drug exchange between Special Handling staff and undercover officers.
In the wake of this incident, Kelly had been sent to Providence to change the "hands off" culture that upper management believed had let the criminal elements conduct their illicit transactions. After a few weeks under Kelly's direction, the office became a model of efficiency and customer service. Kelly monitored his workers' activities using the same cameras that had recorded the illegal conduct of their former co-workers.
Now Kelly has been charged with turning around the office in Cork, Ireland, another trouble spot. The company has received numerous reports of the staff leaving the office unattended. When Kelly arrived, he found that even when present, the staff often spent their days socializing or conducting personal business on their mobile phones. Again, he observed their behaviors using surveillance cameras. He issued written reprimands to six staff members based on the first day of video alone.
Much to Kelly's surprise and chagrin, he and the company are now under investigation by the Data Protection Commissioner of Ireland for allegedly violating the privacy rights of employees. Kelly was told that the company's license for the cameras listed facility security as their main use, but he does not know why this

matters. He has pointed out to his superiors that the company's training programs on privacy protection and data collection mention nothing about surveillance video.
You are a privacy protection consultant, hired by the company to assess this incident, report on the legal and compliance issues, and recommend next steps.
What should you advise this company regarding the status of security cameras at their offices in the United States?
A. Add security cameras at facilities that are now without them.
B. Reduce the number of security cameras located inside the building.
C. Restrict access to surveillance video taken by the security cameras and destroy the recordings after a designated period of time.
D. Set policies about the purpose and use of the security cameras.
Answer: (SHOW ANSWER)

NEW QUESTION: 118
Data retention and destruction policies should meet all of the following requirements EXCEPT?
A. Documentation related to audit controls (third-party or internal) should be saved in a non-permanent format by default.
B. Data destruction triggers and methods should be documented.
C. Personal information should be retained only for as long as necessary to perform its stated purpose.
D. The organization should be documenting and reviewing policies of its other functions to ensure alignment (e.g. HR, business development, finance, etc.).
Answer: A (LEAVE A REPLY)

NEW QUESTION: 119
The General Data Protection Regulation (GDPR) specifies fines that may be levied against data controllers for certain infringements. Which of the following will be subject to administrative fines of up to 10 000 000 EUR, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year?
A. Failure to demonstrate that consent was given by the data subject to the processing of their personal data where it is used as the basis for processing
B. Failure to implement technical and organizational measures to ensure data protection is enshrined by design and default
C. Failure to process personal information in a manner compatible with its original purpose
D. Failure to provide the means for a data subject to rectify inaccuracies in personal data
Answer: B (LEAVE A REPLY)
Explanation
The GDPR specifies fines that may be levied against data controllers for certain infringements. According to Article 83(4)(a) of the GDPR, failure to implement technical and organizational measures to ensure data protection is enshrined by design and default will be subject to administrative fines of up to 10 000 000 EUR, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher. Data protection by design and default is a principle that requires data controllers to

integrate data protection considerations into every stage of the processing activities, from the conception to the execution, and to adopt appropriate measures to safeguard the rights and interests of the data subjects by default, such as minimizing the amount and retention period of personal data, pseudonymizing or encrypting personal data, ensuring transparency and accountability, and enabling data subject rights.
References:
* CIPM Body of Knowledge (2021), Domain I: Privacy Program Governance, Section A: Privacy Governance Models, Subsection 2: Privacy by Design
* CIPM Study Guide (2021), Chapter 2: Privacy Governance Models, Section 2.2: Privacy by Design
* CIPM Textbook (2019), Chapter 2: Privacy Governance Models, Section 2.2: Privacy by Design
* CIPM Practice Exam (2021), Question 130
* GDPR Article 83(4)(a) and Article 25

NEW QUESTION: 120
SCENARIO
Please use the following to answer the next QUESTION:
Natalia, CFO of the Nationwide Grill restaurant chain, had never seen her fellow executives so anxious. Last week, a data processing firm used by the company reported that its system may have been hacked, and customer data such as names, addresses, and birthdays may have been compromised. Although the attempt was proven unsuccessful, the scare has prompted several Nationwide Grill executives to Question the company's privacy program at today's meeting.
Alice, a vice president, said that the incident could have opened the door to lawsuits, potentially damaging Nationwide Grill's market position. The Chief Information Officer (CIO), Brendan, tried to assure her that even if there had been an actual breach, the chances of a successful suit against the company were slim. But Alice remained unconvinced.
Spencer - a former CEO and currently a senior advisor - said that he had always warned against the use of contractors for data processing. At the very least, he argued, they should be held contractually liable for telling customers about any security incidents. In his view, Nationwide Grill should not be forced to soil the company name for a problem it did not cause.
One of the business development (BD) executives, Haley, then spoke, imploring everyone to see reason. "Breaches can happen, despite organizations' best efforts," she remarked. "Reasonable preparedness is key." She reminded everyone of the incident seven years ago when the large grocery chain Tinkerton's had its financial information compromised after a large order of Nationwide Grill frozen dinners. As a long-time BD executive with a solid understanding of Tinkerton's's corporate culture, built up through many years of cultivating relationships, Haley was able to successfully manage the company's incident response.
Spencer replied that acting with reason means allowing security to be handled by the security functions within the company - not BD staff. In a similar way, he said, Human Resources (HR) needs to do a better job training employees to prevent incidents. He pointed out that Nationwide Grill employees are overwhelmed with posters, emails, and memos from both HR and the ethics department related to the company's privacy program. Both the volume and the duplication of information means that it is often ignored altogether.
Spencer said, "The company needs to dedicate itself to its privacy program and set regular in-person trainings for all staff once a month." Alice responded that the suggestion, while well-meaning, is not practical.

With many locations, local HR departments need to have flexibility with their training schedules. Silently, Natalia agreed.
The senior advisor, Spencer, has a misconception regarding?
A. The amount of responsibility that a data controller retains.
B. The appropriate role of an organization's security department.
C. The degree to which training can lessen the number of security incidents.
D. The role of Human Resources employees in an organization's privacy program.
Answer: A (LEAVE A REPLY)
Explanation
Spencer has a misconception regarding the amount of responsibility that a data controller retains, as he suggests that the contractors should be held contractually liable for telling customers about any security incidents, and that Nationwide Grill should not be forced to soil the company name for a problem it did not cause. However, as a data controller, Nationwide Grill is ultimately responsible for ensuring that the personal data of its customers is processed in compliance with applicable laws and regulations, regardless of whether it uses contractors or not. Nationwide Grill cannot transfer or delegate its accountability or liability to the contractors, and it has a duty to inform the customers and the relevant authorities of any security incidents or breaches that may affect their data. Therefore, Spencer's view is unrealistic and risky, as it may expose Nationwide Grill to legal actions, fines, reputational damage and loss of trust.

NEW QUESTION: 121
Under the General Data Protection Regulation (GDPR), what are the obligations of a processor that engages a sub-processor?
A. The processor must give the controller prior written notice and perform a preliminary audit of the sub-processor.
B. The processor must Obtain the controllers specifiC written authorization and provide annual reports on the sub-processor'S performance.
C. The processor must receive a written agreement that the sub-processor will be fully liable to the controller for the performance of its obligations in relation to the personal data concerned.
D. The processor must obtain the consent of the controller and ensure the sub-processor complies with data processing obligations that are equivalent to those that apply to the processor.
Answer: D (LEAVE A REPLY)
Explanation
Under the General Data Protection Regulation (GDPR), the obligations of a processor that engages a sub-processor are to obtain the consent of the controller and ensure the sub-processor complies with data processing obligations that are equivalent to those that apply to the processor. The GDPR defines a processor as a natural or legal person, public authority, agency, or other body that processes personal data on behalf of the controller. A sub-processor is a third party that is engaged by the processor to carry out specific processing activities on behalf of the controller. The GDPR requires that the processor does not engage another processor without prior specific or general written authorization of the controller. In the case of general written authorization, the processor must inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such

changes. The processor must also ensure that the same data protection obligations as set out in the contract or other legal act between the controller and the processor are imposed on that other processor by way of a contract or other legal act under Union or Member State law, . References: [GDPR Article 28], [CIPM - International Association of Privacy Professionals]

NEW QUESTION: 122
SCENARIO
Please use the following to answer the next question:
As they company's new chief executive officer, Thomas Goddard wants to be known as a leader in data protection. Goddard recently served as the chief financial officer of Hoopy.com, a pioneer in online video viewing with millions of users around the world. Unfortunately, Hoopy is infamous within privacy protection circles for its ethically questionable practices, including unauthorized sales of personal data to marketers. Hoopy also was the target of credit card data theft that made headlines around the world, as at least two million credit card numbers were thought to have been pilfered despite the company's claims that "appropriate" data protection safeguards were in place. The scandal affected the company's business as competitors were quick to market an increased level of protection while offering similar entertainment and media content. Within three weeks after the scandal broke, Hoopy founder and CEO Maxwell Martin, Goddard's mentor, was forced to step down.
Goddard, however, seems to have landed on his feet, securing the CEO position at your company, Medialite, which is just emerging from its start-up phase. He sold the company's board and investors on his vision of Medialite building its brand partly on the basis of industry-leading data protection standards and procedures. He may have been a key part of a lapsed or even rogue organization in matters of privacy but now he claims to be reformed and a true believer in privacy protection. In his first week on the job, he calls you into his office and explains that your primary work responsibility is to bring his vision for privacy to life. But you also detect some reservations. "We want Medialite to have absolutely the highest standards," he says. "In fact, I want us to be able to say that we are the clear industry leader in privacy and data protection. However, I also need to be a responsible steward of the company's finances. So, while I want the best solutions across the board, they also need to be cost effective." You are told to report back in a week's time with your recommendations. Charged with this ambiguous mission, you depart the executive suite, already considering your next steps.
You are charged with making sure that privacy safeguards are in place for new products and initiatives. What is the best way to do this?
A. Conduct a gap analysis after deployment of new products, then mend any gaps that are revealed
B. Hold a meeting with stakeholders to create an interdepartmental protocol for new initiatives

C. Institute Privacy by Design principles and practices across the organization
D. Develop a plan for introducing privacy protections into the product development stage
Answer: D (LEAVE A REPLY)

NEW QUESTION: 123
An organization's business continuity plan or disaster recovery plan does NOT typically include what?
A. Statement of organizational responsibilities
B. Recovery time objectives
C. Emergency Response Guidelines
D. Retention schedule for storage and destruction of information
Answer: D (LEAVE A REPLY)

NEW QUESTION: 124
SCENARIO
Please use the following to answer the next QUESTION:
Penny has recently joined Ace Space, a company that sells homeware accessories online, as its new privacy officer. The company is based in California but thanks to some great publicity from a social media influencer last year, the company has received an influx of sales from the EU and has set up a regional office in Ireland to support this expansion. To become familiar with Ace Space's practices and assess what her privacy priorities will be, Penny has set up meetings with a number of colleagues to hear about the work that they have been doing and their compliance efforts.
Penny's colleague in Marketing is excited by the new sales and the company's plans, but is also concerned that Penny may curtail some of the growth opportunities he has planned. He tells her "I heard someone in the breakroom talking about some new privacy laws but I really don't think it affects us. We're just a small company. I mean we just sell accessories online, so what's the real risk?" He has also told her that he works with a number of small companies that help him get projects completed in a hurry. "We've got to meet our deadlines otherwise we lose money. I just sign the contracts and get Jim in finance to push through the payment. Reviewing the contracts takes time that we just don't have." In her meeting with a member of the IT team, Penny has learned that although Ace Space has taken a number of precautions to protect its website from malicious activity, it has not taken the same level of care of its physical files or internal infrastructure.
Penny's colleague in IT has told her that a former employee lost an encrypted USB key with financial data on it when he left. The company nearly lost access to their customer database last year after they fell victim to a phishing attack. Penny is told by her IT colleague that the IT team
"didn't know what to do or who should do what. We hadn't been trained on it but we're a small team though, so it worked out OK in the end." Penny is concerned that these issues will compromise Ace Space's privacy and data protection.
Penny is aware that the company has solid plans to grow its international sales and will be working closely with the CEO to give the organization a data "shake up". Her mission is to cultivate a strong privacy culture within the company.
Penny has a meeting with Ace Space's CEO today and has been asked to give her first impressions and an overview of her next steps.

What is the best way for Penny to understand the location, classification and processing purpose of the personal data Ace Space has?

A. Analyze the data inventory to map data flows

B. Audit all vendors' privacy practices and safeguards

C. Conduct a Privacy Impact Assessment for the company

D. Review all cloud contracts to identify the location of data servers used

Answer: A (LEAVE A REPLY)

Explanation

The best way for Penny to understand the location, classification and processing purpose of the personal data Ace Space has is to analyze the data inventory to map data flows. A data inventory is a comprehensive record of the personal data that an organization collects, stores, uses and shares. It helps to identify the sources, categories, locations, recipients and retention periods of personal data. A data flow map is a visual representation of how personal data flows within and outside an organization. It helps to identify the data transfers, processing activities, legal bases, risks and safeguards of personal data.

By analyzing the data inventory and mapping the data flows, Penny can gain a clear picture of the personal data lifecycle at Ace Space and identify any gaps or issues that need to be addressed. For example, she can determine whether Ace Space has a lawful basis for processing personal data of EU customers, whether it has adequate security measures to protect personal data from unauthorized access or loss, whether it has appropriate contracts with its vendors and cloud providers to ensure compliance with applicable laws and regulations, and whether it has mechanisms to respect the rights and preferences of its customers.

The other options are not the best way for Penny to understand the location, classification and processing purpose of the personal data Ace Space has. Auditing all vendors' privacy practices and safeguards (B) is an important step to ensure that Ace Space's third-party processors are complying with their contractual obligations and legal requirements, but it does not provide a comprehensive overview of Ace Space's own personal data processing activities. Conducting a Privacy Impact Assessment (PIA) for the company is a useful tool to assess the privacy risks and impacts of a specific project or initiative involving personal data, but it does not provide a baseline understanding of the existing personal data landscape at Ace Space. Reviewing all cloud contracts to identify the location of data servers used (D) is a relevant aspect of understanding the location of personal data, but it does not cover other aspects such as classification and processing purpose.

References:

* CIPM Body of Knowledge Domain I: Privacy Program Governance - Task 1: Establish privacy program vision and strategy - Subtask 1: Identify applicable privacy laws, regulations and standards
* CIPM Body of Knowledge Domain II: Privacy Program Operational Life Cycle - Task 1: Assess current state of privacy in an organization - Subtask 1: Conduct gap analysis
* CIPM Study Guide - Chapter 2: Privacy Program Governance - Section 2.1: Data Inventory
* CIPM Study Guide - Chapter 2: Privacy Program Governance - Section 2.2: Data Flow Mapping

NEW QUESTION: 125

SCENARIO

Please use the following to answer the next QUESTION:

Henry Home Furnishings has built high-end furniture for nearly forty years. However, the new owner, Anton, has found some degree of disorganization after touring the company headquarters. His uncle Henry had always focused on production - not data processing - and Anton is concerned. In several storage rooms, he has found paper files, disks, and old computers that appear to contain the personal data of current and former employees and customers. Anton knows that a single break-in could irrevocably damage the company's relationship with its loyal customers. He intends to set a goal of guaranteed zero loss of personal information. To this end, Anton originally planned to place restrictions on who was admitted to the physical premises of the company. However, Kenneth - his uncle's vice president and longtime confidante - wants to hold off on Anton's idea in favor of converting any paper records held at the company to electronic storage. Kenneth believes this process would only take one or two years. Anton likes this idea; he envisions a password-protected system that only he and Kenneth can access.

Anton also plans to divest the company of most of its subsidiaries. Not only will this make his job easier, but it will simplify the management of the stored data. The heads of subsidiaries like the art gallery and kitchenware store down the street will be responsible for their own information management. Then, any unneeded subsidiary data still in Anton's possession can be destroyed within the next few years.

After learning of a recent security incident, Anton realizes that another crucial step will be notifying customers. Kenneth insists that two lost hard drives in Question are not cause for concern; all of the data was encrypted and not sensitive in nature. Anton does not want to take any chances, however. He intends on sending notice letters to all employees and customers to be safe.

Anton must also check for compliance with all legislative, regulatory, and market requirements related to privacy protection. Kenneth oversaw the development of the company's online presence about ten years ago, but Anton is not confident about his understanding of recent online marketing laws. Anton is assigning another trusted employee with a law background the task of the compliance assessment. After a thorough analysis, Anton knows the company should be safe for another five years, at which time he can order another check.

Documentation of this analysis will show auditors due diligence.

Anton has started down a long road toward improved management of the company, but he knows the effort is worth it. Anton wants his uncle's legacy to continue for many years to come.

Which important principle of Data Lifecycle Management (DLM) will most likely be compromised if Anton executes his plan to limit data access to himself and Kenneth?

A. Practicing data minimalism.

B. Ensuring data retrievability.

C. Implementing clear policies.

D. Ensuring adequacy of infrastructure.

Answer: A (LEAVE A REPLY)

Explanation

The important principle of Data Lifecycle Management (DLM) that will most likely be compromised if Anton executes his plan to limit data access to himself and Kenneth is ensuring data retrievability. Data retrievability refers to the ability to access and use data when needed for business purposes or legal obligations1 It involves maintaining the availability, integrity, and usability of data throughout its lifecycle2 However, if Anton

restricts data access to only himself and Kenneth, he will create a single point of failure and a bottleneck for data retrieval. This could pose several risks and challenges for the company, such as:
* Losing data if Anton or Kenneth forgets the password or leaves the company without sharing it with others.
* Delaying data retrieval if Anton or Kenneth is unavailable or unresponsive when someone else needs the data urgently.
* Violating data protection laws or regulations that require data access by certain parties or authorities under certain circumstances.
* Reducing data quality or accuracy if Anton or Kenneth fails to update or maintain the data properly.
* Missing business opportunities or insights if Anton or Kenneth does not share the data with other relevant stakeholders or departments.
Therefore, Anton should reconsider his plan and adopt a more balanced and secure approach to data access management that follows the principle of least privilege. This means granting data access only to those who need it for their specific roles and responsibilities and revoking it when no longer needed3 He should also implement proper authentication, authorization, encryption, backup, and audit mechanisms to protect the data from unauthorized or unlawful access, use, disclosure, alteration, or destruction4 References: 1: Data Retrievability: What Is It?; 2: Data Lifecycle Management | IBM; 3: What is Least Privilege? Definition & Examples; 4: Technical Security Controls: Encryption, Firewalls & More