IAPP.CIPT.v2023-07-15.q110

Exam Code:	CIPT
Exam Name:	Certified Information Privacy Technologist (CIPT)
Certification Provider:	IAPP
Free Question Number:	110
Version:	v2023-07-15
# of views:	1631
# of Questions views:	1100
https://www.exam-tests.com/CIPT-exam/IAPP.CIPT.v2023-07-15.q110.html	

NEW QUESTION: 1
SCENARIO
Wesley Energy has finally made its move, acquiring the venerable oil and gas exploration firm Lancelot from its long-time owner David Wilson. As a member of the transition team, you have come to realize that Wilson's quirky nature affected even Lancelot's data practices, which are maddeningly inconsistent. "The old man hired and fired IT people like he was changing his necktie," one of Wilson's seasoned lieutenants tells you, as you identify the traces of initiatives left half complete.
For instance, while some proprietary data and personal information on clients and employees is encrypted, other sensitive information, including health information from surveillance testing of employees for toxic exposures, remains unencrypted, particularly when included within longer records with less-sensitive dat a. You also find that data is scattered across applications, servers and facilities in a manner that at first glance seems almost random.
Among your preliminary findings of the condition of data at Lancelot are the following:
Cloud technology is supplied by vendors around the world, including firms that you have not heard of. You are told by a former Lancelot employee that these vendors operate with divergent security requirements and protocols.
The company's proprietary recovery process for shale oil is stored on servers among a variety of less-sensitive information that can be accessed not only by scientists, but by personnel of all types at most company locations.
DES is the strongest encryption algorithm currently used for any file.
Several company facilities lack physical security controls, beyond visitor check-in, which familiar vendors often bypass.
Fixing all of this will take work, but first you need to grasp the scope of the mess and formulate a plan of action to address it.
Which is true regarding the type of encryption Lancelot uses?
A. It employs the data scrambling technique known as obfuscation.

B. Its decryption key is derived from its encryption key.
C. It uses a single key for encryption and decryption.
D. It is a data masking methodology.
Answer: (SHOW ANSWER)
It uses a single key for encryption and decryption. In the scenario, it is mentioned that Lancelot uses symmetric encryption to protect its data. Symmetric encryption uses a single key for both encryption and decryption.

NEW QUESTION: 2
A key principle of an effective privacy policy is that it should be?
A. Made general enough to maximize flexibility in its application.
B. Presented with external parties as the intended audience.
C. Written in enough detail to cover the majority of likely scenarios.
D. Designed primarily by the organization's lawyers.
Answer: (SHOW ANSWER)

NEW QUESTION: 3
How should the sharing of information within an organization be documented?
A. With a data flow diagram.
B. With a memorandum of agreement.
C. With a binding contract.
D. With a disclosure statement.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 4
Which of the following techniques describes the use of encryption where encryption keys are divided into parts that can then be used to recover a full encryption key?
A. Homomorphic encryption.
B. Asymmetric cryptography.
C. Cryptographic hashing.
D. Secret sharing.
Answer: D (LEAVE A REPLY)
the technique that describes the use of encryption where encryption keys are divided into parts that can then be used to recover a full encryption key is called secret sharing.

NEW QUESTION: 5
Granting data subjects the right to have data corrected, amended, or deleted describes?
A. Use limitation.
B. Accountability.
C. Individual participation
D. A security safeguard

Answer: (SHOW ANSWER)

NEW QUESTION: 6
SCENARIO
Kyle is a new security compliance manager who will be responsible for coordinating and executing controls to ensure compliance with the company's information security policy and industry standards. Kyle is also new to the company, where collaboration is a core value. On his first day of new-hire orientation, Kyle's schedule included participating in meetings and observing work in the IT and compliance departments.
Kyle spent the morning in the IT department, where the CIO welcomed him and explained that her department was responsible for IT governance. The CIO and Kyle engaged in a conversation about the importance of identifying meaningful IT governance metrics. Following their conversation, the CIO introduced Kyle to Ted and Barney. Ted is implementing a plan to encrypt data at the transportation level of the organization's wireless network. Kyle would need to get up to speed on the project and suggest ways to monitor effectiveness once the implementation was complete. Barney explained that his short-term goals are to establish rules governing where data can be placed and to minimize the use of offline data storage.
Kyle spent the afternoon with Jill, a compliance specialist, and learned that she was exploring an initiative for a compliance program to follow self-regulatory privacy principles. Thanks to a recent internship, Kyle had some experience in this area and knew where Jill could find some support. Jill also shared results of the company's privacy risk assessment, noting that the secondary use of personal information was considered a high risk.
By the end of the day, Kyle was very excited about his new job and his new company. In fact, he learned about an open position for someone with strong qualifications and experience with access privileges, project standards board approval processes, and application-level obligations, and couldn't wait to recommend his friend Ben who would be perfect for the job.
Which of the following should Kyle recommend to Jill as the best source of support for her initiative?
A. Investors.
B. Regulators.
C. Industry groups.
D. Corporate researchers.
Answer: C (LEAVE A REPLY)
Jill is leading an initiative to develop a new industry standard for data privacy and security. Kyle should recommend that Jill seek support from industry groups as they are likely to have a vested interest in the development of such a standard and may be able to provide valuable input and resources.

NEW QUESTION: 7
What term describes two re-identifiable data sets that both come from the same unidentified individual?

A. Aggregated data.
B. Imprecise data.
C. Anonymous data.
D. Pseudonymous data.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 8
SCENARIO
Clean-Q is a company that offers house-hold and office cleaning services. The company receives requests from consumers via their website and telephone, to book cleaning services. Based on the type and size of service, Clean-Q then contracts individuals that are registered on its resource database - currently managed in- house by Clean-Q IT Support. Because of Clean-Q's business model, resources are contracted as needed instead of permanently employed.
The table below indicates some of the personal information Clean-Q requires as part of its business operations:

Category	Types of Personal Information
Customers	Name, address (location), contact information, billing information
Resources (contracted)	Name, contact information, banking details, address

Clean-Q has an internal employee base of about 30 people. A recent privacy compliance exercise has been conducted to align employee data management and human resource functions with applicable data protection regulation. Therefore, the Clean-Q permanent employee base is not included as part of this scenario.
With an increase in construction work and housing developments, Clean-Q has had an influx of requests for cleaning services. The demand has overwhelmed Clean-Q's traditional supply and demand system that has caused some overlapping bookings.
Ina business strategy session held by senior management recently, Clear-Q invited vendors to present potential solutions to their current operational issues. These vendors included Application developers and Cloud-Q's solution providers, presenting their proposed solutions and platforms.
The Managing Director opted to initiate the process to integrate Clean-Q's operations with a cloud solution (LeadOps) that will provide the following solution one single online platform: A web interface that Clean-Q accesses for the purposes of resource and customer management. This would entail uploading resource and customer information.
* A customer facing web interface that enables customers to register, manage and submit cleaning service requests online.
* A resource facing web interface that enables resources to apply and manage their assigned jobs.
* An online payment facility for customers to pay for services.
Which question would you most likely ask to gain more insight about LeadOps and provide practical privacy recommendations?
A. Does LeadOps practice agile development and maintenance of their system?

B. What is LeadOps' annual turnover?
C. How big is LeadOps' employee base?
D. Where are LeadOps' operations and hosting services located?
Answer: A (LEAVE A REPLY)

NEW QUESTION: 9
Which of the following most embodies the principle of Data Protection by Default?
A. A messaging app for high school students that uses HTTPS to communicate with the server.
B. An electronic teddy bear with built-in voice recognition that only responds to its owner's voice.
C. An internet forum for victims of domestic violence that allows anonymous posts without registration.
D. A website that has an opt-in form for marketing emails when registering to download a whitepaper.
Answer: D (LEAVE A REPLY)
Explanation

NEW QUESTION: 10
SCENARIO
Clean-Q is a company that offers house-hold and office cleaning services. The company receives requests from consumers via their website and telephone, to book cleaning services. Based on the type and size of service, Clean-Q then contracts individuals that are registered on its resource database - currently managed in-house by Clean-Q IT Support. Because of Clean-Q's business model, resources are contracted as needed instead of permanently employed.
The table below indicates some of the personal information Clean-Q requires as part of its business operations:

Category	Types of Personal Information
Customers	Name, address (location), contact information, billing information
Resources (contracted)	Name, contact information, banking details, address

Clean-Q has an internal employee base of about 30 people. A recent privacy compliance exercise has been conducted to align employee data management and human resource functions with applicable data protection regulation. Therefore, the Clean-Q permanent employee base is not included as part of this scenario.
With an increase in construction work and housing developments, Clean-Q has had an influx of requests for cleaning services. The demand has overwhelmed Clean-Q's traditional supply and demand system that has caused some overlapping bookings.

Ina business strategy session held by senior management recently, Clear-Q invited vendors to present potential solutions to their current operational issues. These vendors included Application developers and Cloud-Q's solution providers, presenting their proposed solutions and platforms. The Managing Director opted to initiate the process to integrate Clean-Q's operations with a cloud solution (LeadOps) that will provide the following solution one single online platform: A web interface that Clean-Q accesses for the purposes of resource and customer management. This would entail uploading resource and customer information.
A customer facing web interface that enables customers to register, manage and submit cleaning service requests online.
A resource facing web interface that enables resources to apply and manage their assigned jobs.
An online payment facility for customers to pay for services.
Which question would you most likely ask to gain more insight about LeadOps and provide practical privacy recommendations?
A. What is LeadOps' annual turnover?
B. How big is LeadOps' employee base?
C. Where are LeadOps' operations and hosting services located?
D. Does LeadOps practice agile development and maintenance of their system?
Answer: C (LEAVE A REPLY)
The location of LeadOps' operations and hosting services is important information for Clean-Q to consider when assessing LeadOps' appropriateness as a service provider. This is because different countries have different data protection laws and regulations that may impact how personal information can be processed and stored. Knowing where LeadOps' operations and hosting services are located will help Clean-Q make informed decisions about how to protect the personal information it entrusts to LeadOps.

NEW QUESTION: 11
During a transport layer security (TLS) session, what happens immediately after the web browser creates a random PreMasterSecret?
A. The web browser opens a TLS connection to the PremasterSecret.
B. The server decrypts the PremasterSecret.
C. The server and client use the same algorithm to convert the PremasterSecret into an encryption key.
D. The web browser encrypts the PremasterSecret with the server's public key.
Answer: (SHOW ANSWER)

NEW QUESTION: 12
Under the Family Educational Rights and Privacy Act (FERPA), releasing personally identifiable information from a student's educational record requires written permission from the parent or eligible student in order for information to be?
A. Released to a prospective employer.
B. Released to schools to which a student is transferring.

C. Released to specific individuals for audit or evaluation purposes.
D. Released in response to a judicial order or lawfully ordered subpoena.
Answer: C (LEAVE A REPLY)
Explanation/Reference: https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

NEW QUESTION: 13
What must be done to destroy data stored on "write once read many" (WORM) media?
A. The data must be made inaccessible by encryption.
B. The erase function must be used to remove all data.
C. The media must be physically destroyed.
D. The media must be reformatted.
Answer: C (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 14
After stringent testing an organization has launched a new web-facing ordering system for its consumer medical products. As the medical products could provide indicators of health conditions, the organization could further strengthen its privacy controls by deploying?
A. Run time behavior monitoring.
B. A content delivery network.
C. Context aware computing.
D. Differential identifiability.
Answer: D (LEAVE A REPLY)
after launching a new web-facing ordering system for its consumer medical products, an organization could further strengthen its privacy controls by deploying differential identifiability. Differential identifiability involves adding noise or randomness to data in order to preserve privacy while still allowing for statistical analysis.

NEW QUESTION: 15
A valid argument against data minimization is that it?
A. Can have an adverse effect on data quality.
B. Increases the chance that someone can be identified from data.
C. Decreases the speed of data transfers.
D. Can limit business opportunities.
Answer: (SHOW ANSWER)

NEW QUESTION: 16
A user who owns a resource wants to give other individuals access to the resource. What control would apply?
A. Mandatory access control.
B. Role-based access controls.

C. Discretionary access control.
D. Context of authority controls.
Answer: B (LEAVE A REPLY)
Explanation/Reference: https://docs.microsoft.com/bs-latn-ba/azure/role-based-access-control/overview

NEW QUESTION: 17
What is an example of a just-in-time notice?
A. A warning that a website may be unsafe.
B. A full organizational privacy notice publicly available on a website
C. A credit card company calling a user to verify a purchase before itis authorized
D. Privacy information given to a user when he attempts to comment on an online article.
Answer: (SHOW ANSWER)
Explanation/Reference: https://www.clarip.com/data-privacy/just-time-notices/

NEW QUESTION: 18
What is a main benefit of data aggregation?
A. It is a good way to perform analysis without needing a statistician.
B. It applies two or more layers of protection to a single data record.
C. It allows one to draw valid conclusions from small data samples.
D. It is a good way to achieve de-identification and unlinkabilty.
Answer: C (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 19
SCENARIO
WebTracker Limited is a cloud-based online marketing service located in London. Last year, WebTracker migrated its IT infrastructure to the cloud provider AmaZure, which provides SQL Databases and Artificial Intelligence services to WebTracker. The roles and responsibilities between the two companies have been formalized in a standard contract, which includes allocating the role of data controller to WebTracker.

The CEO of WebTracker, Mr. Bond, would like to assess the effectiveness of AmaZure's privacy controls, and he recently decided to hire you as an independent auditor. The scope of the engagement is limited only to the marketing services provided by WebTracker, you will not be evaluating any internal data processing activity, such as HR or Payroll.
This ad-hoc audit was triggered due to a future partnership between WebTracker and SmartHome - a partnership that will not require any data sharing. SmartHome is based in the USA, and most recently has dedicated substantial resources to developing smart refrigerators that can suggest the recommended daily calorie intake based on DNA information. This and other personal data is collected by WebTracker.
To get an idea of the scope of work involved, you have decided to start reviewing the company's documentation and interviewing key staff to understand potential privacy risks.
The results of this initial work include the following notes:
* There are several typos in the current privacy notice of WebTracker, and you were not able to find the privacy notice for SmartHome.
* You were unable to identify all the sub-processors working for SmartHome. No subcontractor is indicated in the cloud agreement with AmaZure, which is responsible for the support and maintenance of the cloud infrastructure.
* There are data flows representing personal data being collected from the internal employees of WebTracker, including an interface from the HR system.
* Part of the DNA data collected by WebTracker was from employees, as this was a prototype approved by the CEO of WebTracker.
* All the WebTracker and SmartHome customers are based in USA and Canada.
Based on the initial assessment and review of the available data flows, which of the following would be the most important privacy risk you should investigate first?
A. Verify that WebTracker's HR and Payroll systems implement the current privacy notice (after the typos are fixed).
B. Review the list of subcontractors employed by AmaZure and ensure these are included in the formal agreement with WebTracker.
C. Confirm whether the data transfer from London to the USA has been fully approved by AmaZure and the appropriate institutions in the USA and the European Union.
D. Evaluate and review the basis for processing employees' personal data in the context of the prototype created by WebTracker and approved by the CEO.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 20
SCENARIO
Clean-Q is a company that offers house-hold and office cleaning services. The company receives requests from consumers via their website and telephone, to book cleaning services. Based on the type and size of service, Clean-Q then contracts individuals that are registered on its resource database - currently managed in-house by Clean-Q IT Support. Because of Clean-Q's business model, resources are contracted as needed instead of permanently employed.

The table below indicates some of the personal information Clean-Q requires as part of its business operations:

Category	Types of Personal Information
Customers	Name, address (location), contact information, billing information
Resources (contracted)	Name, contact information, banking details, address

Clean-Q has an internal employee base of about 30 people. A recent privacy compliance exercise has been conducted to align employee data management and human resource functions with applicable data protection regulation. Therefore, the Clean-Q permanent employee base is not included as part of this scenario.

With an increase in construction work and housing developments, Clean-Q has had an influx of requests for cleaning services. The demand has overwhelmed Clean-Q's traditional supply and demand system that has caused some overlapping bookings.

Ina business strategy session held by senior management recently, Clear-Q invited vendors to present potential solutions to their current operational issues. These vendors included Application developers and Cloud-Q's solution providers, presenting their proposed solutions and platforms.

The Managing Director opted to initiate the process to integrate Clean-Q's operations with a cloud solution (LeadOps) that will provide the following solution one single online platform: A web interface that Clean-Q accesses for the purposes of resource and customer management. This would entail uploading resource and customer information.

* A customer facing web interface that enables customers to register, manage and submit cleaning service requests online.
* A resource facing web interface that enables resources to apply and manage their assigned jobs.
* An online payment facility for customers to pay for services.

Which question would you most likely ask to gain more insight about LeadOps and provide practical privacy recommendations?

A. How big is LeadOps' employee base?

B. Where are LeadOps' operations and hosting services located?

C. What is LeadOps' annual turnover?

D. Does LeadOps practice agile development and maintenance of their system?

Answer: D (LEAVE A REPLY)

NEW QUESTION: 21

After committing to a Privacy by Design program, which activity should take place first?

A. Create a privacy standard that applies to all projects and services.

B. Perform privacy reviews on new projects.

C. Establish a retention policy for all data being collected.

D. Implement easy to use privacy settings for users.
Answer: (SHOW ANSWER)

NEW QUESTION: 22
SCENARIO
Please use the following to answer the next questions:
Your company is launching a new track and trace health app during the outbreak of a virus pandemic in the US. The developers claim the app is based on privacy by design because personal data collected was considered to ensure only necessary data is captured, users are presented with a privacy notice, and they are asked to give consent before data is shared. Users can update their consent after logging into an account, through a dedicated privacy and consent hub. This is accessible through the 'Settings' icon from any app page, then clicking 'My Preferences', and selecting 'Information Sharing and Consent' where the following choices are displayed:
* "I consent to receive notifications and infection alerts";
* "I consent to receive information on additional features or services, and new products";
* "I consent to sharing only my risk result and location information, for exposure and contact tracing purposes";
* "I consent to share my data for medical research purposes"; and
* "I consent to share my data with healthcare providers affiliated to the company".
For each choice, an ON* or OFF tab is available The default setting is ON for all Users purchase a virus screening service for USS29 99 for themselves or others using the app The virus screening service works as follows:
* Step 1 A photo of the user's face is taken.
* Step 2 The user measures their temperature and adds the reading in the app
* Step 3 The user is asked to read sentences so that a voice analysis can detect symptoms
* Step 4 The user is asked to answer questions on known symptoms
* Step 5 The user can input information on family members (name date of birth, citizenship, home address, phone number, email and relationship).) The results are displayed as one of the following risk status "Low. "Medium" or "High" if the user is deemed at "Medium " or "High" risk an alert may be sent to other users and the user is Invited to seek a medical consultation and diagnostic from a healthcare provider.
A user's risk status also feeds a world map for contact tracing purposes, where users are able to check if they have been or are in dose proximity of an infected person If a user has come in contact with another individual classified as "medium' or 'high' risk an instant notification also alerts the user of this. The app collects location trails of every user to monitor locations visited by an infected individual Location is collected using the phone's GPS functionary, whether the app is in use or not however, the exact location of the user is "blurred' for privacy reasons Users can only see on the map circles Which technology is best suited for the contact tracing feature of the app1?
A. Bluetooth

B. Deep learning
C. Near Field Communication (NFC)
D. Radio-Frequency Identification (RFID)
Answer: A (LEAVE A REPLY)
Bluetooth technology can enable devices to communicate with each other over short distances. This makes it well-suited for contact tracing applications where proximity between individuals needs to be detected. Deep learning (option B), Near Field Communication (NFC) (option C), and Radio-Frequency Identification (RFID) (option D) are technologies that could also have potential uses in a contact tracing app but may not be as well-suited as Bluetooth.

NEW QUESTION: 23
SCENARIO - Please use the following to answer the next question:
Clean-Q is a company that offers house-hold and office cleaning services. The company receives requests from consumers via their website and telephor, to book cleaning services. Based on the type and size of service, Clean-Q then contracts individuals that are registered on its resource database - currently managed in-house by Clean-Q IT Support. Because of Clean-Q:s business. model, resources are contracted as needed instead of permanently employed.
The table below indicates some of the personal information Clean-Q requires as part of its business operations:

Category	Types of Personal Information
Customers	Name, address (location), contact information, billing information
Resources (contracted)	Name, contact information, banking details, address

Clean-Q has an internal employee base of about 30 people. A recent privacy compliance exercise has been conducted to align employee data management and human resource functions with applicable data protection regulation.
Therefore, the Clean-Q permanent employee base is not included as part of this scenario.
With an increase in construction work and housing developments, Clean-Q has had an influx of requests for cleaning services. The demand has overwhelmed Clean-Q:s traditional supply and demand system that has caused some overlapping bookings.
In a business statrategy session held by senior management recently, Clearning invited vendors to present potential solutions to their current operational issues. These vendors includes included Application development and Cloud solution providers, presenting their proposed solution and platforms.
The Managing Direct opted to initiate the process to integrate Clean-Q's operations with a cloud solution (LeadOps) that will provide the following solution one single online platform. A web interface that Clean-Q accesses for the purposes of resource and customer management. This would entail uploading resource and customer information.
A customer facing web interface that enables customers to register, manage and submit cleaning service requests online.
A resource facing web interface that enables resources to apply and manage their assigned jobs.

An online payment facility for customer to pay for services.
What is a key consideration for assessing external service providers like LeadOps, which will conduct personal information processing operations on Clean-Q:s behalf?
A. Recognizing the value of LeadOps website holding a verified security certificate.
B. Understanding LeadOps costing model.
C. Establishing a relationship with the Managing Director of LeadOps.
D. Obtaining knowledge of LeadOps information handling practices and information security environment.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 24
What is the best way to protect privacy on a geographic information system (GIS)?
A. Using a firewall.
B. Using a wireless encryption protocol.
C. Scrambling location information.
D. Limiting the data provided to the system.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 25
SCENARIO
Please use the following to answer next question:
EnsureClaim is developing a mobile app platform for managing data used for assessing car accident insurance claims. Individuals use the app to take pictures at the crash site, eliminating the need for a built-in vehicle camer a. EnsureClaim uses a third-party hosting provider to store data collected by the app. EnsureClaim customer service employees also receive and review app data before sharing with insurance claim adjusters.
The app collects the following information:
First and last name
Date of birth (DOB)
Mailing address
Email address
Car VIN number
Car model
License plate
Insurance card number
Photo
Vehicle diagnostics
Geolocation
The app is designed to collect and transmit geolocation data. How can data collection best be limited to the necessary minimum?
A. Allow user to opt-out geolocation data collection at any time.

B. Allow access and sharing of geolocation data only after an accident occurs.
C. Present a clear and explicit explanation about need for the geolocation data.
D. Obtain consent and capture geolocation data at all times after consent is received.
Answer: C (LEAVE A REPLY)
By providing users with a clear and explicit explanation about why geolocation data is needed and how it will be used, the app can help ensure that only the minimum amount of data necessary is collected. This can also help build trust with users and increase transparency.

NEW QUESTION: 26
Which activity would best support the principle of data quality?
A. Providing notice to the data subject regarding any change in the purpose for collecting such data.
B. Delivering information in a format that the data subject understands.
C. Ensuring that the number of teams processing personal information is limited.
D. Ensuring that information remains accurate.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 27
Which concept related to privacy choice is demonstrated by highlighting and bolding the "accept" button on a cookies notice while maintaining standard text format for other options?
A. Illuminating
B. Nudging
C. Suppression
D. Tagging
Answer: B (LEAVE A REPLY)
highlighting and bolding the "accept" button on a cookies notice while maintaining standard text format for other options is an example of nudging. Nudging is a concept related to privacy choice that involves subtly influencing individuals' decisions through the design of choice architecture.

NEW QUESTION: 28
SCENARIO
Carol was a U.S.-based glassmaker who sold her work at art festivals. She kept things simple by only accepting cash and personal checks.
As business grew, Carol couldn't keep up with demand, and traveling to festivals became burdensome. Carol opened a small boutique and hired Sam to run it while she worked in the studio. Sam was a natural salesperson, and business doubled. Carol told Sam, "I don't know what you are doing, but keep doing it!" But months later, the gift shop was in chaos. Carol realized that Sam needed help so she hired Jane, who had business expertise and could handle the back-office tasks. Sam would continue to focus on sales. Carol gave Jane a few weeks to get acquainted with the artisan craft business, and then scheduled a meeting for the three of them to discuss Jane's first impressions.

At the meeting, Carol could not wait to hear Jane's thoughts, but she was unprepared for what Jane had to say. "Carol, I know that he doesn't realize it, but some of Sam's efforts to increase sales have put you in a vulnerable position. You are not protecting customers' personal information like you should." Sam said, "I am protecting our information. I keep it in the safe with our bank deposit. It's only a list of customers' names, addresses and phone numbers that I get from their checks before I deposit them. I contact them when you finish a piece that I think they would like. That's the only information I have! The only other thing I do is post photos and information about your work on the photo sharing site that I use with family and friends. I provide my email address and people send me their information if they want to see more of your work. Posting online really helps sales, Carol. In fact, the only complaint I hear is about having to come into the shop to make a purchase." Carol replied, "Jane, that doesn't sound so bad. Could you just fix things and help us to post even more online?"
'I can," said Jane. "But it's not quite that simple. I need to set up a new program to make sure that we follow the best practices in data management. And I am concerned for our customers. They should be able to manage how we use their personal information. We also should develop a social media strategy." Sam and Jane worked hard during the following year. One of the decisions they made was to contract with an outside vendor to manage online sales. At the end of the year, Carol shared some exciting news. "Sam and Jane, you have done such a great job that one of the biggest names in the glass business wants to buy us out! And Jane, they want to talk to you about merging all of our customer and vendor information with theirs beforehand." Which regulator has jurisdiction over the shop's data management practices?
A. The Federal Trade Commission.
B. The Department of Commerce.
C. The Data Protection Authority.
D. The Federal Communications Commission.
Answer: C (LEAVE A REPLY)
The Data Protection Authority is a regulatory body responsible for enforcing data protection laws and ensuring that organizations comply with their obligations to protect personal data. The Federal Trade Commission (FTC) is an independent agency of the United States government whose primary mission is to promote consumer protection and prevent anti-competitive business practices.

NEW QUESTION: 29
Which of the following suggests the greatest degree of transparency?
A. A privacy disclosure statement clearly articulates general purposes for collection
B. The data subject has multiple opportunities to opt-out after collection has occurred.
C. After reading the privacy notice, a data subject confidently infers how her information will be used.
D. A privacy notice accommodates broadly defined future collections for new products.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 30
What is the most important requirement to fulfill when transferring data out of an organization?
A. Ensuring the organization sending the data controls how the data is tagged by the receiver.
B. Ensuring the organization receiving the data performs a privacy impact assessment.
C. Ensuring the commitments made to the data owner are followed.
D. Extending the data retention schedule as needed.
Answer: (SHOW ANSWER)
The most important requirement to fulfill when transferring data out of an organization is ensuring the commitments made to the data owner are followed. The data owner is the person who has provided their personal data to an organization for a specific purpose or consented to its collection. When transferring data out of an organization, such as sharing it with another entity or moving it across borders, it is essential that the organization respects the rights and expectations of the data owner and complies with any applicable laws or regulations. The other options are not requirements for transferring data out of an organization, but rather possible measures or considerations that may be relevant depending on the context or nature of the transfer.

NEW QUESTION: 31
SCENARIO
Tom looked forward to starting his new position with a U.S -based automobile leasing company (New Company), now operating in 32 states. New Company was recently formed through the merger of two prominent players, one from the eastern region (East Company) and one from the western region (West Company). Tom, a Certified Information Privacy Technologist (CIPT), is New Company's first Information Privacy and Security Officer. He met today with Dick from East Company, and Harry, from West Company.
Dick and Harry are veteran senior information privacy and security professionals at their respective companies, and continue to lead the east and west divisions of New Company. The purpose of the meeting was to conduct a SWOT (strengths/weaknesses/opportunities/threats) analysis for New Company. Their SWOT analysis conclusions are summarized below.
Dick was enthusiastic about an opportunity for the New Company to reduce costs and increase computing power and flexibility through cloud services. East Company had been contemplating moving to the cloud, but West Company already had a vendor that was providing it with software-as-a-service (SaaS). Dick was looking forward to extending this service to the eastern region. Harry noted that this was a threat as well, because West Company had to rely on the third party to protect its data.
Tom mentioned that neither of the legacy companies had sufficient data storage space to meet the projected growth of New Company, which he saw as a weakness. Tom stated that one of the team's first projects would be to construct a consolidated New Company data warehouse. Tom would personally lead this project and would be held accountable if information was modified during transmission to or during storage in the new data warehouse.
Tom, Dick and Harry agreed that employee network access could be considered both a strength and a weakness. East Company and West Company had strong performance records in this

regard; both had robust network access controls that were working as designed. However, during a projected year-long transition period, New Company employees would need to be able to connect to a New Company network while retaining access to the East Company and West Company networks.
When employees are working remotely, they usually connect to a Wi-Fi network. What should Harry advise for maintaining company security in this situation?
A. Hiding wireless service set identifiers (SSID).
B. Retaining the password assigned by the network.
C. Employing Wired Equivalent Privacy (WEP) encryption.
D. Using tokens sent through HTTP sites to verify user identity.
Answer: A (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 32
Which is NOT a suitable method for assuring the quality of data collected by a third-party company?
A. Verifying the accuracy of the data by contacting users.
B. Validating the company's data collection procedures.
C. Introducing erroneous data to see if its detected.
D. Tracking changes to data through auditing.
Answer: (SHOW ANSWER)
Introducing erroneous data to see if it's detected is not a suitable method for assuring the quality of data collected by a third-party company1. This method could compromise the integrity and reliability of the data and cause confusion or harm to the users or the business1. The other options are suitable methods for assuring the quality of data collected by a third-party company1. Verifying the accuracy of the data by contacting users can help identify and correct any errors or inconsistencies in the data1. Validating the company's data collection procedures can help ensure that they follow best practices and standards for collecting, storing, and processing personal information1. Tracking changes to data through auditing can help monitor and document any modifications or deletions made to the data1.
https://www.isaca.org/resources/news-and-trends/industry-news/2021/data-minimization-a-practical-approach

NEW QUESTION: 33
To meet data protection and privacy legal requirements that may require personal data to be disposed of or deleted when no longer necessary for the use it was collected, what is the best privacy-enhancing solution a privacy technologist should recommend be implemented in application design to meet this requirement?
A. Implement a process to delete personal data on demand and maintain records on deletion requests.
B. Implement automated deletion of off-site backup of personal data based on annual risk assessments.
C. Develop application logic to validate and purge personal data according to legal hold status or retention schedule.
D. Securely archive personal data not accessed or used in the last 6 months. Automate a quarterly review to delete data
Answer: A (LEAVE A REPLY)
from archive once no longer needed.
Explanation:
to meet data protection and privacy legal requirements that may require personal data to be disposed of or deleted when no longer necessary for the use it was collected for, a privacy technologist should recommend implementing a process to delete personal data on demand and maintain records on deletion requests. This allows individuals to exercise their right to have their personal data deleted and provides a record of compliance with legal requirements.

NEW QUESTION: 34
Which of the following best describes the basic concept of "Privacy by Design?"
A. The adoption of privacy enhancing technologies.
B. The integration of a privacy program with all lines of business.
C. The implementation of privacy protection through system architecture.
D. The introduction of business process to identify and assess privacy gaps.
Answer: (SHOW ANSWER)
the basic concept of "Privacy by Design" is the implementation of privacy protection through system architecture.

NEW QUESTION: 35
SCENARIO
It should be the most secure location housing data in all of Europe, if not the world. The Global Finance Data Collective (GFDC) stores financial information and other types of client data from large banks, insurance companies, multinational corporations and governmental agencies. After a long climb on a mountain road that leads only to the facility, you arrive at the security booth. Your credentials are checked and checked again by the guard to visually verify that you are the person pictured on your passport and national identification card. You are led down a long corridor with

server rooms on each side, secured by combination locks built into the doors. You climb a flight of stairs and are led into an office that is lighted brilliantly by skylights where the GFDC Director of Security, Dr. Monique Batch, greets you. On the far wall you notice a bank of video screens showing different rooms in the facility. At the far end, several screens show different sections of the road up the mountain Dr. Batch explains once again your mission. As a data security auditor and consultant, it is a dream assignment: The GFDC does not want simply adequate controls, but the best and most effective security that current technologies allow.
"We were hacked twice last year," Dr. Batch says, "and although only a small number of records were stolen, the bad press impacted our business. Our clients count on us to provide security that is nothing short of impenetrable and to do so quietly. We hope to never make the news again." She notes that it is also essential that the facility is in compliance with all relevant security regulations and standards.
You have been asked to verify compliance as well as to evaluate all current security controls and security measures, including data encryption methods, authentication controls and the safest methods for transferring data into and out of the facility. As you prepare to begin your analysis, you find yourself considering an intriguing question: Can these people be sure that I am who I say I am?
You are shown to the office made available to you and are provided with system login information, including the name of the wireless network and a wireless key. Still pondering, you attempt to pull up the facility's wireless network, but no networks appear in the wireless list. When you search for the wireless network by name, however it is readily found.
What measures can protect client information stored at GFDC?
A. Server-side controls.
B. Data pruning
C. De-linking of data into client-specific packets.
D. Cloud-based applications.
Answer: (SHOW ANSWER)

NEW QUESTION: 36
SCENARIO - Please use the following to answer the next question:
WebTracker Limited is a cloud-based online marketing service located in London. Last year, WebTracker migrated its IT infrastructure to the cloud provider AmaZure, which provides SQL Databases and Artificial Intelligence services to WebTracker. The roles and responsibilities between the two companies have been formalized in a standard contract, which includes allocating the role of data controller to WebTracker.
The CEO of WebTracker, Mr. Bond, would like to assess the effectiveness of AmaZure s privacy controls, and he recently decided to hire you as an independent auditor. The scope of the engagement is limited only to the marketing service! Provided by WebTracker, you will not be evaluating any internal data processing activity, such as HR or Payroll.
This ad-hoc audit was triggered due to a future partnership between WebTracker and SmartHome-a partnership that will not require any data sharing. SmartHome is based in the USA,

and most recently has dedicated substantial resources to developing smart refrigerators that can suggest the recommended daily calorie intake based on DNA information. This and other personal data is collected by WebTracker.
To get an idea of the scope of work involved, you have decided to start reviewing the company s documentation and interviewing key staff to understand potential privacy risks. The results of this initial work include the following notes:
To get an idea of the scope of work involved, you have decided to start reviewing the company s documentation and interviewing key staff to understand potential privacy risks. The results of this initial work include the following notes:
o There are several typos in the current privacy notice of WebTracker. and you were not able to find the privacy notice for SmartHome.
o You were unable to identify all the sub-processors working for SmartHome. No subcontractor is indicated in the cloud agreement with AmaZure. which is responsible for the support and maintenance of the cloud infrastructure.
o There are data flows representing personal data being collected from the internal employees of WebTracker, including an interface from the HR system.
o Part of the DNA data collected by WebTracker was from employees, as this was a prototype approved by the CEO of WebTracker.
o All the WebTracker and SmartHome customers are based in USA and Canada Which of the following issues is most likely to require an investigation by the Chief Privacy Officer (CPO) of WebTracker?
A. AmaZure sends newsletter to WebTracker customers, as approved by the Marketing Manager
B. File Integrity Monitoring is being deployed in SQL servers, as indicated by the IT Architect Manager.
C. Data flows use encryption for data at rest, as defined by the IT manager.
D. Employees personal data are being stored in a cloud HR system, as approved by the HR Manager.
Answer: (SHOW ANSWER)

NEW QUESTION: 37
To comply with the Sarbanes-Oxley Act (SOX), public companies in the United States are required to annually report on the effectiveness of the auditing controls of their financial reporting systems. These controls must be implemented to prevent unauthorized use, disclosure, modification, and damage or loss of financial data.
Why do these controls ensure both the privacy and security of data?
A. Damage or loss of data are aspects of privacy; disclosure, unauthorized use, and modification of data are aspects of privacy.
B. Modification of data is an aspect of privacy; unauthorized use, disclosure, and damage or loss of data are aspects of security.
C. Unauthorized use of data is an aspect of privacy; disclosure, modification, and damage or loss of data are aspects of security.

D. Disclosure of data is an aspect of privacy; unauthorized use, modification, and damage or loss of data are aspects of security.
Answer: (SHOW ANSWER)

NEW QUESTION: 38
Value sensitive design focuses on which of the following?
A. Quality and benefit.
B. Ethics and morality.
C. Confidentiality and integrity.
D. Consent and human rights.
Answer: B (LEAVE A REPLY)
Value sensitive design (VSD) is a theoretically grounded approach to the design of technology that accounts for human values in a principled and comprehensive manner1. It brings human values to the forefront of the technical design process2.

NEW QUESTION: 39
A developer is designing a new system that allows an organization's helpdesk to remotely connect into the device of the individual to provide support Which of the following will be a privacy technologist's primary concern"?
A. Geolocation
B. Geofencing
C. Geo-tracking
D. Geo-tagging
Answer: A (LEAVE A REPLY)
a privacy technologist's primary concern when designing a new system that allows an organization's helpdesk to remotely connect into the device of the individual to provide support would be geolocation.

NEW QUESTION: 40
Which of the following functionalities can meet some of the General Data Protection Regulation's (GDPR's) Data Portability requirements for a social networking app designed for users in the EU?
A. Allow users to download the content they have provided the app.
B. Allow users to get a time-stamped list of what they have provided the app.
C. Allow users to delete the content they provided the app.
D. Allow users to modify the data they provided the app.
Answer: (SHOW ANSWER)

NEW QUESTION: 41
In order to prevent others from identifying an individual within a data set, privacy engineers use a cryptographically-secure hashing algorithm. Use of hashes in this way illustrates the privacy tactic known as what?

A. Stripping.
B. Isolation.
C. Obfuscation.
D. Perturbation.
Answer: (SHOW ANSWER)

NEW QUESTION: 42
Which Organization for Economic Co-operation and Development (OECD) privacy protection principle encourages an organization to obtain an individual s consent before transferring personal information?
A. Individual participation.
B. Purpose specification.
C. Collection limitation.
D. Accountability.
Answer: A (LEAVE A REPLY)
The individual participation principle encourages an organization to obtain an individual's consent before transferring personal information1. According to this principle, an individual should have the right to obtain from a data controller confirmation of whether or not the data controller has data relating to him; to have communicated to him such data within a reasonable time; to be given reasons if a request made under subparagraphs (a) and (b) is denied by the data controller; and to challenge such denial; and to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended1. The other options are not principles that encourage an organization to obtain an individual's consent before transferring personal information.
http://www.oecdprivacy.org/

NEW QUESTION: 43
SCENARIO
Clean-Q is a company that offers house-hold and office cleaning services. The company receives requests from consumers via their website and telephone, to book cleaning services. Based on the type and size of service, Clean-Q then contracts individuals that are registered on its resource database - currently managed in-house by Clean-Q IT Support. Because of Clean-Q's business model, resources are contracted as needed instead of permanently employed.
The table below indicates some of the personal information Clean-Q requires as part of its business operations:

Category	Types of Personal Information
Customers	Name, address (location), contact information, billing information
Resources (contracted)	Name, contact information, banking details, address

Clean-Q has an internal employee base of about 30 people. A recent privacy compliance exercise has been conducted to align employee data management and human resource functions with applicable data protection regulation. Therefore, the Clean-Q permanent employee base is not included as part of this scenario.

With an increase in construction work and housing developments, Clean-Q has had an influx of requests for cleaning services. The demand has overwhelmed Clean-Q's traditional supply and demand system that has caused some overlapping bookings.

Ina business strategy session held by senior management recently, Clear-Q invited vendors to present potential solutions to their current operational issues. These vendors included Application developers and Cloud-Q's solution providers, presenting their proposed solutions and platforms.

The Managing Director opted to initiate the process to integrate Clean-Q's operations with a cloud solution (LeadOps) that will provide the following solution one single online platform: A web interface that Clean-Q accesses for the purposes of resource and customer management. This would entail uploading resource and customer information.

A customer facing web interface that enables customers to register, manage and submit cleaning service requests online.

A resource facing web interface that enables resources to apply and manage their assigned jobs.

An online payment facility for customers to pay for services.

What is a key consideration for assessing external service providers like LeadOps, which will conduct personal information processing operations on Clean-Q's behalf?

A. Understanding LeadOps' costing model.

B. Establishing a relationship with the Managing Director of LeadOps.

C. Recognizing the value of LeadOps' website holding a verified security certificate.

D. Obtaining knowledge of LeadOps' information handling practices and information security environment.

Answer: (SHOW ANSWER)

When engaging an external service provider to process personal information on its behalf, it is important for Clean-Q to have a good understanding of the service provider's information handling practices and information security environment. This will help Clean-Q assess whether or not the service provider has appropriate measures in place to protect the personal information it entrusts to them.

NEW QUESTION: 44

SCENARIO - Please use the following to answer the next question:

Kyle is a new security compliance manager who will be responsible for coordinating and executing controls to ensure compliance with the company s information security policy and industry standards. Kyle is also-new to the company, where collaboration is a core value. On his first day of new-hire orientation, Kyle s schedule included participating in meetings and observing work in the IT and compliance departments.
Kyle spent the morning in the IT department, where the CIO welcomed him and explained that her department was responsible for IT governance. The CIO and Kyle engaged in a conversation about the importance of identifying meaningful IT governance metrics. Following their conversation, the CIO introduced Kyle to Ted and Barney. Ted is implementing a plan to encrypt data at the transportation level of the organization s wireless network. Kyle would need to get up to speed on the project and suggest ways to monitor effectiveness once the implementation was complete. Barney explained that his short-term goals are to establish rules governing where data can be placed and to minimize the use of offline data storage.
Kyle spent the afternoon with Jill, a compliance specialist, and learned that she was exploring an initiative for a compliance program to follow self-regulatory privacy principles. Thanks to a recent internship, Kyle had some experience in this area and knew where Jill could find some support. Jill also shared results of the company s privacy risk assessment, noting that the secondary use of personal information was considered a high risk.
By the end of the day, Kyle was very excited about his new job and his new company. In fact, he learned about an open position for someone with strong qualifications and experience with access privileges, project standards board approval processes, and application-level obligations, and couldn t wait to recommend his friend Ren who would be nerfert for the job Teds implementation is most likely a response to what incident?
A. Encryption keys were previously unavailable to the organization s cloud storage host.
B. Confidential information discussed during a strategic teleconference was intercepted by the organization stop competitor.
C. Signatureless advanced malware was detected at multiple points on the organization s networks.
D. Cyber criminals accessed proprietary data by running automated authentication attacks on the organization s network.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 45
Which Organisation for Economic Co-operation and Development (OECD) privacy protection principle encourages an organization to obtain an individual s consent before transferring personal information?
A. Accountability.
B. Purpose specification.
C. Individual participation.
D. Collection limitation.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 46
SCENARIO - Please use the following to answer the next question:
It should be the most secure location housing data in all of Europe, if not the world. The Global Finance Data Collective (GFDC) stores financial information and other types of client data from large banks, insurance companies, multinational corporations and governmental agencies. After a long climb on a mountain road that leads only to the facility, you arrive at the security booth. Your credentials are checked and checked again by the guard to visually verify that you are the person pictured on your passport and national identification card.
You are led down a long corridor with server rooms on each side, secured by combination locks built into the doors. You climb a flight of stairs and are led into an office that is lighted brilliantly by skylights where the GFDC Director of Security, Dr. Monique Batch, greets you. On the far wall you notice a bank of video screens showing different rooms in the facility. At the far end, several screens show different sections of the road up the mountain.
Dr. Batch explains once again your mission. As a data security auditor and consultant, it is a dream assignment: The GFDC does not want simply adequate controls, but the best and most effective security that current technologies allow.
!'We were hacked twice last year," Dr. Batch says, :'and although only a small number of records were stolen, the bad press impacted our business. Our clients count on us to provide security that is nothing short of impenetrable and to do so quietly. We hope to never make the news again."
She notes that it is also essential that the facility is in compliance with all relevant security regulations and standards.
You have been asked to verify compliance as well as to evaluate all current security controls and security measures, including data encryption methods, authentication controls and the safest methods for transferring data into and out of the facility. As you prepare to begin your analysis, you find yourself considering an intriguing question: Can these people be sure that I am who I say I am?
You are shown to the office made available to you and are provided with system login information, including the name of the wireless network and a wireless key. Still pondering, you attempt to pull up the facility s wireless network, but no networks appear in the wireless list. When you search for the wireless network by name, however it is readily found What measures can protect client information stored at GFDC?
A. Cloud-based applications.
B. De-linking of data into client-specific packets.
C. Server-side controls.
D. Data pruning.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 47
What is the best way to protect privacy on a geographic information system?
A. Scrambling location information.
B. Limiting the data provided to the system.
C. Using a firewall.
D. Using a wireless encryption protocol.
Answer: (SHOW ANSWER)

NEW QUESTION: 48
What logs should an application server retain in order to prevent phishing attacks while minimizing data retention?
A. Limited-retention, de-identified logs including only metadata.
B. Limited-retention logs including the links clicked in messages, the identity of parties sending and receiving them, as well as metadata.
C. Limited-retention, de-identified logs including the links clicked in messages as well as metadata.
D. Limited-retention logs including the identity of parties sending and receiving messages as well as metadata.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 49
SCENARIO
Please use the following to answer the next question:
Jordan just joined a fitness-tracker start-up based in California, USA, as its first Information Privacy and Security Officer. The company is quickly growing its business but does not sell any of the fitness trackers itself. Instead, it relies on a distribution network of third-party retailers in all major countries. Despite not having any stores, the company has a 78% market share in the EU. It has a website presenting the company and products, and a member section where customers can access their information. Only the email address and physical address need to be provided as part of the registration process in order to customize the site to the user's region and country. There is also a newsletter sent every month to all members featuring fitness tips, nutrition advice, product spotlights from partner companies based on user behavior and preferences.

Jordan says the General Data Protection Regulation (GDPR) does not apply to the company. He says the company is not established in the EU, nor does it have a processor in the region. Furthermore, it does not do any "offering goods or services" in the EU since it does not do any marketing there, nor sell to consumers directly. Jordan argues that it is the customers who chose to buy the products on their own initiative and there is no "offering" from the company.
The fitness trackers incorporate advanced features such as sleep tracking, GPS tracking, heart rate monitoring. wireless syncing, calorie-counting and step-tracking. The watch must be paired with either a smartphone or a computer in order to collect data on sleep levels, heart rates, etc. All information from the device must be sent to the company's servers in order to be processed, and then the results are sent to the smartphone or computer. Jordan argues that there is no personal information involved since the company does not collect banking or social security information.
Why is Jordan's claim that the company does not collect personal information as identified by the GDPR inaccurate?
A. The website collects the customers' and users' region and country information.
B. The fitness trackers capture sleep and heart rate data to monitor an individual's behavior.
C. The customers must pair their fitness trackers to either smartphones or computers.
D. The potential customers must browse for products online.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 50
What must be done to destroy data stored on "write once read many" (WORM) media?
A. The media must be reformatted.
B. The media must be physically destroyed.
C. The data must be made inaccessible by encryption.
D. The erase function must be used to remove all data.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 51
What tactic does pharming use to achieve its goal?
A. It modifies the user's Hosts file.
B. It encrypts files on a user's computer.
C. It creates a false display advertisement.
D. It generates a malicious instant message.
Answer: (SHOW ANSWER)
Explanation/Reference: https://inspiredelearning.com/blog/phishing-vs-pharming-whats-difference/

NEW QUESTION: 52

Organizations understand there are aggregation risks associated with the way the process their customer's dat a. They typically include the details of this aggregation risk in a privacy notice and ask that all customers acknowledge they understand these risks and consent to the processing. What type of risk response does this notice and consent represent?

A. Risk mitigation.

B. Risk transfer.

C. Risk avoidance.

D. Risk acceptance.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 53

If you are asked to advise on privacy concerns regarding paid advertisements, which is the most important aspect to cover?

A. Unseen web beacons that combine information on multiple users.

B. Personal information collected by cookies linked to the advertising network.

C. Latent keys that trigger malware when an advertisement is selected.

D. Sensitive information from Structured Query Language (SQL) commands that may be exposed.

Answer: (SHOW ANSWER)

NEW QUESTION: 54

SCENARIO - Please use the following to answer the next question:

Carol was a US-based glassmaker who sold her work at art festivals. She kept things simple by only accepting cash and personal checks.

As business grew, Carol couldn't keep up with demand, and traveling to festivals became burdensome. Carol opened a small boutique and hired Sam to run it while she worked in the studio. Sam was a natural salesperson, and business doubled. Carol told Sam, :'I don't know what you are doing, but keep doing it; But months later, the gift shop was in chaos. Carol realized that Sam needed help so she hired Jane, who had business expertise and could handle the back-office tasks. Sam would continue to focus on sales. Carol gave Jane a few weeks to get acquainted with the artisan craft business, and then scheduled a meeting for the three of them to discuss Jane s first impressions.

At the meeting, Carol could not wait to hear Jane s thoughts, but she was unprepared for what Jane had to say.

"Carol. I know that he doesn't realize it, but some of Sam s efforts to increase sales have put you in a vulnerable position. You are not protecting customers personal information like you should." Sam said, :'I am protecting our information. I keep it in the safe with our bank deposit. It's only a list of customers names, addresses and phone numbers that I get from their checks before I deposit them. I contact them when you finish a piece that I think they would like. That's the only information I have! The only other thing I do is post photos and information about your work on the photo sharing site that I use with family and friends. I provide my email address and people

send me their information if they want to see more of your work. Posting online really helps sales, Carol. In fact, the only complaint I hear is about having to come into the shop to make a purchase." Carol replied, "Jane, that doesn't sound so bad. Could you just fix things and help us to post even more online?"
"I can," said Jane. "But it's not quite that simple. I need to set up a new program to make sure that we follow the best practices in data management. And I am concerned for our customers. They should be able to manage how we use their personal information. We also should develop a social media strategy" Sam and Jane worked hard during the following year. One of the decisions they made was to contract with an outside vendor to manage online sales. At the end of the year Carol shared some exciting news. "Sam and Jane, you have done such a great job that one of the biggest names in the glass business wants to buy us out!
And Jane, they want to talk to you about merging all of our customer and vendor information with theirs beforehand " When initially collecting personal information from customers, what should Jane be guided by?
A. Vendor management principles.
B. Digital rights management.
C. Data minimization principles.
D. Digital rights management.
E. Vendor management principles.
When initially collecting personal information from customers, what should Jane be guided by?
F. Onward transfer rules.
G. Onward transfer rules.
H. Data minimization principles.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 55
SCENARIO
Please use the following to answer the next question:
Light Blue Health (LBH) is a healthcare technology company developing a new web and mobile application that collects personal health information from electronic patient health records. The application will use machine learning to recommend potential medical treatments and medications based on information collected from anonymized electronic health records. Patient users may also share health data collected from other mobile apps with the LBH app.
The application requires consent from the patient before importing electronic health records into the application and sharing it with their authorized physicians or healthcare provider. The patient can then review and share the recommended treatments with their physicians securely through the app. The patient user may also share location data and upload photos in the app. The patient user may also share location data and upload photos in the app for a healthcare provider to review along with the health record. The patient may also delegate access to the app.

LBH's privacy team meets with the Application development and Security teams, as well as key business stakeholders on a periodic basis. LBH also implements Privacy by Design (PbD) into the application development process.
The Privacy Team is conducting a Privacy Impact Assessment (PIA) to evaluate privacy risks during development of the application. The team must assess whether the application is collecting descriptive, demographic or any other user related data from the electronic health records that are not needed for the purposes of the application. The team is also reviewing whether the application may collect additional personal data for purposes for which the user did not provide consent.
What is the best way to minimize the risk of an exposure violation through the use of the app?
A. Create a policy to prevent combining data with external data sources.
B. Dissociate the patient health data from the personal data.
C. Prevent the downloading of photos stored in the app.
D. Exclude the collection of personal information from the health record.
Answer: (SHOW ANSWER)

NEW QUESTION: 56
An organization based in California, USA is implementing a new online helpdesk solution for recording customer call information. The organization considers the capture of personal data on the online helpdesk solution to be in the interest of the company in best servicing customer calls. Before implementation, a privacy technologist should conduct which of the following?
A. A privacy risk and impact assessment to evaluate potential risks from the proposed processing operations.
B. A Data Protection Impact Assessment (DPIA) and consultation with the appropriate regulator to ensure legal compliance.
C. A security assessment of the help desk solution and provider to assess if the technology was developed with a security by design approach.
D. A Legitimate Interest Assessment (LIA) to ensure that the processing is proportionate and does not override the privacy, rights and freedoms of the customers.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 57
SCENARIO
Tom looked forward to starting his new position with a U.S -based automobile leasing company (New Company), now operating in 32 states. New Company was recently formed through the merger of two prominent players, one from the eastern region (East Company) and one from the western region (West Company). Tom, a Certified Information Privacy Technologist (CIPT), is New Company's first Information Privacy and Security Officer. He met today with Dick from East Company, and Harry, from West Company. Dick and Harry are veteran senior information privacy and security professionals at their respective companies, and continue to lead the east and west divisions of New Company. The purpose of the meeting was to conduct a SWOT

(strengths/weaknesses/opportunities/threats) analysis for New Company. Their SWOT analysis conclusions are summarized below.
Dick was enthusiastic about an opportunity for the New Company to reduce costs and increase computing power and flexibility through cloud services. East Company had been contemplating moving to the cloud, but West Company already had a vendor that was providing it with software-as-a-service (SaaS). Dick was looking forward to extending this service to the eastern region. Harry noted that this was a threat as well, because West Company had to rely on the third party to protect its data.
Tom mentioned that neither of the legacy companies had sufficient data storage space to meet the projected growth of New Company, which he saw as a weakness. Tom stated that one of the team's first projects would be to construct a consolidated New Company data warehouse. Tom would personally lead this project and would be held accountable if information was modified during transmission to or during storage in the new data warehouse.
Tom, Dick and Harry agreed that employee network access could be considered both a strength and a weakness. East Company and West Company had strong performance records in this regard; both had robust network access controls that were working as designed. However, during a projected year-long transition period, New Company employees would need to be able to connect to a New Company network while retaining access to the East Company and West Company networks.
Which statement is correct about addressing New Company stakeholders' expectations for privacy?
A. New Company's commitment to stakeholders ends when the stakeholders' data leaves New Company.
B. New Company should expect consumers to read the company's privacy policy.
C. New Company should manage stakeholder expectations for privacy even when the stakeholders' data is not held by New Company.
D. New Company would best meet consumer expectations for privacy by adhering to legal requirements.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 58
SCENARIO
Please use the following to answer the next questions:
Your company is launching a new track and trace health app during the outbreak of a virus pandemic in the US. The developers claim the app is based on privacy by design because personal data collected was considered to ensure only necessary data is captured, users are presented with a privacy notice, and they are asked to give consent before data is shared. Users can update their consent after logging into an account, through a dedicated privacy and consent hub. This is accessible through the 'Settings' icon from any app page, then clicking 'My Preferences', and selecting 'Information Sharing and Consent' where the following choices are displayed:

* "I consent to receive notifications and infection alerts";
* "I consent to receive information on additional features or services, and new products";
* "I consent to sharing only my risk result and location information, for exposure and contact tracing purposes";
* "I consent to share my data for medical research purposes"; and
* "I consent to share my data with healthcare providers affiliated to the company".

For each choice, an ON* or OFF tab is available The default setting is ON for all Users purchase a virus screening service for USS29 99 for themselves or others using the app The virus screening service works as follows:

* Step 1 A photo of the user's face is taken.
* Step 2 The user measures their temperature and adds the reading in the app
* Step 3 The user is asked to read sentences so that a voice analysis can detect symptoms
* Step 4 The user is asked to answer questions on known symptoms
* Step 5 The user can input information on family members (name date of birth, citizenship, home address, phone number, email and relationship).) The results are displayed as one of the following risk status "Low. "Medium" or "High" if the user is deemed at "Medium " or "High" risk an alert may be sent to other users and the user is Invited to seek a medical consultation and diagnostic from a healthcare provider.

A user's risk status also feeds a world map for contact tracing purposes, where users are able to check if they have been or are in dose proximity of an infected person If a user has come in contact with another individual classified as "medium' or 'high' risk an instant notification also alerts the user of this. The app collects location trails of every user to monitor locations visited by an infected individual Location is collected using the phone's GPS functionary, whether the app is in use or not however, the exact location of the user is "blurred' for privacy reasons Users can only see on the map circles Which of the following pieces of information collected is the LEAST likely to be justified tor the purposes of the app?

A. Relationship of family member
B. Phone number
C. Dale of birth
D. Citizenship

Answer: D (LEAVE A REPLY)

Of the pieces of information collected by the app described in the scenario provided in the exhibit you shared, citizenship (option D) is LEAST likely to be justified for the purposes of the app. Citizenship may not be necessary for providing health recommendations or contact tracing services. Collecting this type of personal information could raise privacy concerns if it is not necessary for fulfilling the primary purpose of the app.

NEW QUESTION: 59

Under the Family Educational Rights and Privacy Act (FERPA), releasing personally identifiable information from a student s educational record requires written permission from the parent or eligible student in order for information to be?

A. Released to schools to which a student is transferring.
B. Released to specific individuals for audit or evaluation purposes.
C. Released to a prospective employer.
D. Released in response to a judicial order or lawfully ordered subpoena.
Answer: (SHOW ANSWER)

NEW QUESTION: 60
SCENARIO
WebTracker Limited is a cloud-based online marketing service located in London. Last year, WebTracker migrated its IT infrastructure to the cloud provider AmaZure, which provides SQL Databases and Artificial Intelligence services to WebTracker. The roles and responsibilities between the two companies have been formalized in a standard contract, which includes allocating the role of data controller to WebTracker.
The CEO of WebTracker, Mr. Bond, would like to assess the effectiveness of AmaZure's privacy controls, and he recently decided to hire you as an independent auditor. The scope of the engagement is limited only to the marketing services provided by WebTracker, you will not be evaluating any internal data processing activity, such as HR or Payroll.
This ad-hoc audit was triggered due to a future partnership between WebTracker and SmartHome - a partnership that will not require any data sharing. SmartHome is based in the USA, and most recently has dedicated substantial resources to developing smart refrigerators that can suggest the recommended daily calorie intake based on DNA information. This and other personal data is collected by WebTracker.
To get an idea of the scope of work involved, you have decided to start reviewing the company's documentation and interviewing key staff to understand potential privacy risks.
The results of this initial work include the following notes:
* There are several typos in the current privacy notice of WebTracker, and you were not able to find the privacy notice for SmartHome.
* You were unable to identify all the sub-processors working for SmartHome. No subcontractor is indicated in the cloud agreement with AmaZure, which is responsible for the support and maintenance
* of the cloud infrastructure.
* There are data flows representing personal data being collected from the internal employees of WebTracker, including an interface from the HR system.
* Part of the DNA data collected by WebTracker was from employees, as this was a prototype approved by the CEO of WebTracker.
* All the WebTracker and SmartHome customers are based in USA and Canada.
Based on the initial assessment and review of the available data flows, which of the following would be the most important privacy risk you should investigate first?
A. Evaluate and review the basis for processing employees' personal data in the context of the prototype created by WebTracker and approved by the CEO.

B. Review the list of subcontractors employed by AmaZure and ensure these are included in the formal agreement with WebTracker.
C. Confirm whether the data transfer from London to the USA has been fully approved by AmaZure and the appropriate institutions in the USA and the European Union.
D. Verify that WebTracker's HR and Payroll systems implement the current privacy notice (after the typos are fixed).
Answer: A (LEAVE A REPLY)

NEW QUESTION: 61
Which of the following is an example of the privacy risks associated with the Internet of Things (IoT)?
A. An insurance company raises a person's rates based on driving habits gathered from a connected car.
B. A water district fines an individual after a meter reading reveals excess water use during drought conditions.
C. A group of hackers infiltrate a power grid and cause a major blackout.
D. A website stores a cookie on a user's hard drive so the website can recognize the user on subsequent visits.
Answer: (SHOW ANSWER)

NEW QUESTION: 62
A user who owns a resource wants to give other individuals access to the resource. What control would apply?
A. Mandatory access control.
B. Context of authority controls.
C. Role-based access controls.
D. Discretionary access control.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 63
SCENARIO
Please use the following to answer the next questions:

Your company is launching a new track and trace health app during the outbreak of a virus pandemic in the US. The developers claim the app is based on privacy by design because personal data collected was considered to ensure only necessary data is captured, users are presented with a privacy notice, and they are asked to give consent before data is shared. Users can update their consent after logging into an account, through a dedicated privacy and consent hub. This is accessible through the 'Settings' icon from any app page, then clicking 'My Preferences', and selecting 'Information Sharing and Consent' where the following choices are displayed:
* "I consent to receive notifications and infection alerts";
* "I consent to receive information on additional features or services, and new products";
* "I consent to sharing only my risk result and location information, for exposure and contact tracing purposes";
* "I consent to share my data for medical research purposes"; and
* "I consent to share my data with healthcare providers affiliated to the company".
For each choice, an ON* or OFF tab is available The default setting is ON for all Users purchase a virus screening service for USS29 99 for themselves or others using the app The virus screening service works as follows:
* Step 1 A photo of the user's face is taken.
* Step 2 The user measures their temperature and adds the reading in the app
* Step 3 The user is asked to read sentences so that a voice analysis can detect symptoms
* Step 4 The user is asked to answer questions on known symptoms
* Step 5 The user can input information on family members (name date of birth, citizenship, home address, phone number, email and relationship).) The results are displayed as one of the following risk status "Low. "Medium" or "High" if the user is deemed at "Medium " or "High" risk an alert may be sent to other users and the user is Invited to seek a medical consultation and diagnostic from a healthcare provider.
A user's risk status also feeds a world map for contact tracing purposes, where users are able to check if they have been or are in dose proximity of an infected person If a user has come in contact with another individual classified as "medium' or 'high' risk an instant notification also alerts the user of this. The app collects location trails of every user to monitor locations visited by an infected individual Location is collected using the phone's GPS functionary, whether the app is in use or not however, the exact location of the user is "blurred' for privacy reasons Users can only see on the map circles The location data collected and displayed on the map should be changed for which of the following reasons?
A. The blurriness does not allow users to know how close they are to an infected person
B. The radius used for location data exceeds official social distancing rules
C. The location data has not been pseudonymized
D. The location data is loo precise
Answer: (SHOW ANSWER)
Location data that is too precise can reveal sensitive information about an individual's movements and activities. This could raise privacy concerns if this detailed location data is shared with third

parties or used for purposes other than contact tracing. Pseudonymizing location data (option C) could also help protect user privacy but may not address concerns about overly precise location data.

NEW QUESTION: 64
Granting data subjects the right to have data corrected, amended, or deleted describes?
A. Use limitation.
B. Accountability.
C. A security safeguard
D. Individual participation
Answer: D (LEAVE A REPLY)
Reference:
Granting data subjects the right to have data corrected, amended, or deleted describes individual participation1. As explained above, the individual participation principle gives individuals certain rights over their personal data held by a data controller1. One of these rights is to challenge data relating to them and, if the challenge is successful, to have the data erased, rectified, completed or amended1. The other options are not principles that describe granting data subjects this right.

NEW QUESTION: 65
SCENARIO
Clean-Q is a company that offers house-hold and office cleaning services. The company receives requests from consumers via their website and telephone, to book cleaning services. Based on the type and size of service, Clean-Q then contracts individuals that are registered on its resource database - currently managed in- house by Clean-Q IT Support. Because of Clean-Q's business model, resources are contracted as needed instead of permanently employed.
The table below indicates some of the personal information Clean-Q requires as part of its business operations:

Category	Types of Personal Information
Customers	Name, address (location), contact information, billing information
Resources (contracted)	Name, contact information, banking details, address

Clean-Q has an internal employee base of about 30 people. A recent privacy compliance exercise has been conducted to align employee data management and human resource functions with applicable data protection regulation. Therefore, the Clean-Q permanent employee base is not included as part of this scenario.
With an increase in construction work and housing developments, Clean-Q has had an influx of requests for cleaning services. The demand has overwhelmed Clean-Q's traditional supply and demand system that has caused some overlapping bookings.
Ina business strategy session held by senior management recently, Clear-Q invited vendors to present potential solutions to their current operational issues. These vendors included Application developers and Cloud-Q's solution providers, presenting their proposed solutions and platforms.

The Managing Director opted to initiate the process to integrate Clean-Q's operations with a cloud solution (LeadOps) that will provide the following solution one single online platform: A web interface that Clean-Q accesses for the purposes of resource and customer management. This would entail uploading resource and customer information.
* A customer facing web interface that enables customers to register, manage and submit cleaning service requests online.
* A resource facing web interface that enables resources to apply and manage their assigned jobs.
* An online payment facility for customers to pay for services.
Considering that LeadOps will host/process personal information on behalf of Clean-Q remotely, what is an appropriate next step for Clean-Q senior management to assess LeadOps' appropriateness?
A. Nothing at this stage as the Managing Director has made a decision.
B. Determine if any Clean-Q competitors currently use LeadOps as a solution.
C. Obtain a legal opinion from an external law firm on contracts management.
D. Involve the Information Security team to understand in more detail the types of services and solutions LeadOps is proposing.
Answer: D (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 66
A valid argument against data minimization is that it?
A. Can limit business opportunities.
B. Decreases the speed of data transfers.
C. Can have an adverse effect on data quality.
D. Increases the chance that someone can be identified from data.
Answer: A (LEAVE A REPLY)
A valid argument against data minimization is that it can limit business opportunities23. Data minimization refers to limiting the collection, storage, and processing of personal information to only what is strictly necessary for business operations3. While this practice can help protect privacy and security, it can also restrict the potential uses and benefits of data for innovation, research, marketing, analytics etc.23. The other options are not valid arguments against data minimization, but rather arguments in favor of it23.
https://www.manageengine.com/data-security/what-is/data-minimization.html

NEW QUESTION: 67
A sensitive biometrics authentication system is particularly susceptible to?
A. Theft of finely individualized personal data.
B. False positives.
C. Slow recognition speeds.
D. False negatives.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 68
Machine-learning based solutions present a privacy risk because?
A. Training data used during the training phase is compromised.
B. The solution may contain inherent bias from the developers.
C. The decision-making process used by the solution is not documented.
D. Machine-learning solutions introduce more vulnerabilities than other software.
Answer: B (LEAVE A REPLY)
machine-learning based solutions present a privacy risk because they may contain inherent bias from the developers. Bias can be introduced into machine learning models through biased training data or through biased decision-making processes used by the solution.

NEW QUESTION: 69
When writing security policies, the most important consideration is to?
A. Require all employees to read and acknowledge their understanding.
B. Ensure they are based on the organization's risk profile.
C. Ensure they cover enough details for common situations.
D. Follow industry best practices.
Answer: (SHOW ANSWER)
the most important consideration when writing security policies is to ensure they are based on the organization's risk profile. This means that the policies should be tailored to address the specific risks faced by the organization.

NEW QUESTION: 70
Which of the following became a foundation for privacy principles and practices of countries and organizations across the globe?
A. The Code of Fair Information Practices.
B. The Organization for Economic Co-operation and Development (OECD) Privacy Principles.
C. The EU Data Protection Directive.
D. The Personal Data Ordinance.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 71
SCENARIO
Clean-Q is a company that offers house-hold and office cleaning services. The company receives requests from consumers via their website and telephone, to book cleaning services. Based on the type and size of service, Clean-Q then contracts individuals that are registered on its resource database - currently managed in-house by Clean-Q IT Support. Because of Clean-Q's business model, resources are contracted as needed instead of permanently employed.

The table below indicates some of the personal information Clean-Q requires as part of its business operations:

Category	Types of Personal Information
Customers	Name, address (location), contact information, billing information
Resources (contracted)	Name, contact information, banking details, address

Clean-Q has an internal employee base of about 30 people. A recent privacy compliance exercise has been conducted to align employee data management and human resource functions with applicable data protection regulation. Therefore, the Clean-Q permanent employee base is not included as part of this scenario.

With an increase in construction work and housing developments, Clean-Q has had an influx of requests for cleaning services. The demand has overwhelmed Clean-Q's traditional supply and demand system that has caused some overlapping bookings.

Ina business strategy session held by senior management recently, Clear-Q invited vendors to present potential solutions to their current operational issues. These vendors included Application developers and Cloud-Q's solution providers, presenting their proposed solutions and platforms.

The Managing Director opted to initiate the process to integrate Clean-Q's operations with a cloud solution (LeadOps) that will provide the following solution one single online platform: A web interface that Clean-Q accesses for the purposes of resource and customer management. This would entail uploading resource and customer information.

* A customer facing web interface that enables customers to register, manage and submit cleaning service requests online.
* A resource facing web interface that enables resources to apply and manage their assigned jobs.
* An online payment facility for customers to pay for services.

What is a key consideration for assessing external service providers like LeadOps, which will conduct personal information processing operations on Clean-Q's behalf?

A. Recognizing the value of LeadOps' website holding a verified security certificate.
B. Establishing a relationship with the Managing Director of LeadOps.
C. Understanding LeadOps' costing model.
D. Obtaining knowledge of LeadOps' information handling practices and information security environment.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 72

When should code audits be concluded?

A. Before launch after all code for a feature is complete.
B. While code is being sent to production.
C. At code check-in time.

D. At engineering design time.
Answer: (SHOW ANSWER)

NEW QUESTION: 73
A BaaS provider backs up the corporate data and stores it in an outsider provider under contract with the organization. A researcher notifies the organization that he found unsecured data in the cloud. The organization looked into the issue and realized $ne of its backups was misconfigured on the outside provider's cloud and the data fully exposed to the open internet. They quickly secured the backup. Which is the best next step the organization should take?
A. Review the content of the data exposed.
B. Review its contract with the outside provider.
C. Investigate how the researcher discovered the unsecured data.
D. Investigate using alternate BaaS providers or on-premise backup systems.
Answer: B (LEAVE A REPLY)
The best next step the organization should take is to review its contract with the outside provider. This will help the organization to identify the responsibilities of the outside provider and the organization in the event of a data breach.

NEW QUESTION: 74
SCENARIO
Kyle is a new security compliance manager who will be responsible for coordinating and executing controls to ensure compliance with the company's information security policy and industry standards. Kyle is also new to the company, where collaboration is a core value. On his first day of new-hire orientation, Kyle's schedule included participating in meetings and observing work in the IT and compliance departments.
Kyle spent the morning in the IT department, where the CIO welcomed him and explained that her department was responsible for IT governance. The CIO and Kyle engaged in a conversation about the importance of identifying meaningful IT governance metrics. Following their conversation, the CIO introduced Kyle to Ted and Barney. Ted is implementing a plan to encrypt data at the transportation level of the organization's wireless network. Kyle would need to get up to speed on the project and suggest ways to monitor effectiveness once the implementation was complete. Barney explained that his short-term goals are to establish rules governing where data can be placed and to minimize the use of offline data storage.
Kyle spent the afternoon with Jill, a compliance specialist, and learned that she was exploring an initiative for a compliance program to follow self-regulatory privacy principles. Thanks to a recent internship, Kyle had some experience in this area and knew where Jill could find some support. Jill also shared results of the company's privacy risk assessment, noting that the secondary use of personal information was considered a high risk.
By the end of the day, Kyle was very excited about his new job and his new company. In fact, he learned about an open position for someone with strong qualifications and experience with

access privileges, project standards board approval processes, and application-level obligations, and couldn't wait to recommend his friend Ben who would be perfect for the job.
Which data practice is Barney most likely focused on improving?
A. Deletion
B. Inventory.
C. Retention.
D. Sharing
Answer: (SHOW ANSWER)

NEW QUESTION: 75
SCENARIO
You have just been hired by Ancillary.com, a seller of accessories for everything under the sun, including waterproof stickers for pool floats and decorative bands and cases for sunglasses. The company sells cell phone cases, e-cigarette cases, wine spouts, hanging air fresheners for homes and automobiles, book ends, kitchen implements, visors and shields for computer screens, passport holders, gardening tools and lawn ornaments, and catalogs full of health and beauty products. The list seems endless. As the CEO likes to say, Ancillary offers, without doubt, the widest assortment of low-price consumer products from a single company anywhere.
Ancillary's operations are similarly diverse. The company originated with a team of sales consultants selling home and beauty products at small parties in the homes of customers, and this base business is still thriving.
However, the company now sells online through retail sites designated for industries and demographics, sites such as "My Cool Ride" for automobile-related products or "Zoomer" for gear aimed toward young adults.
The company organization includes a plethora of divisions, units and outrigger operations, as Ancillary has been built along a decentered model rewarding individual initiative and flexibility, while also acquiring key assets. The retail sites seem to all function differently, and you wonder about their compliance with regulations and industry standards. Providing tech support to these sites is also a challenge, partly due to a variety of logins and authentication protocols.
You have been asked to lead three important new projects at Ancillary:
The first is the personal data management and security component of a multi-faceted initiative to unify the company's culture. For this project, you are considering using a series of third- party servers to provide company data and approved applications to employees.
The second project involves providing point of sales technology for the home sales force, allowing them to move beyond paper checks and manual credit card imprinting.
Finally, you are charged with developing privacy protections for a single web store housing all the company's product lines as well as products from affiliates. This new omnibus site will be known, aptly, as "Under the Sun." The Director of Marketing wants the site not only to sell Ancillary's products, but to link to additional products from other retailers through paid advertisements. You need to brief the executive team of security concerns posed by this approach.
What technology is under consideration in the first project in this scenario?

A. Cloud computing
B. Data on demand
C. MAC filtering
D. Server driven controls.
Answer: (SHOW ANSWER)

NEW QUESTION: 76
When designing a new system, which of the following is a privacy threat that the privacy technologist should consider?
A. Encryption.
B. Social distancing.
C. Social engineering.
D. Identity and Access Management.
Answer: C (LEAVE A REPLY)
Social engineering is a privacy threat that the privacy technologist should consider when designing a new system.

NEW QUESTION: 77
An organization must terminate their cloud vendor agreement immediately. What is the most secure way to delete the encrypted data stored in the cloud?
A. Transfer the data to another location.
B. Invoke the appropriate deletion clause in the cloud terms and conditions.
C. Obtain a destruction certificate from the cloud vendor.
D. Destroy all encryption keys associated with the data.
Answer: D (LEAVE A REPLY)
Destroying all encryption keys associated with encrypted data stored on a cloud server would make that encrypted data inaccessible even if it still exists on that server 4.

NEW QUESTION: 78
Which of the following is a privacy consideration for NOT sending large-scale SPAM type emails to a database of email addresses?
A. Poor user experience.

B. Emails are unsolicited.
C. Data breach notification.
D. Reduction in email deliverability score.
Answer: (SHOW ANSWER)
a privacy consideration for NOT sending large-scale SPAM type emails to a database of email addresses is that the emails are unsolicited. Sending unsolicited emails can violate individuals' privacy rights and may also be illegal under certain anti-spam laws.

NEW QUESTION: 79
Aadhaar is a unique-identity number of 12 digits issued to all Indian residents based on their biometric and demographic data. The data is collected by the Unique Identification Authority of India. The Aadhaar database contains the Aadhaar number, name, date of birth, gender and address of over 1 billion individuals. Which of the following datasets derived from that data would be considered the most de-identified?
A. A count of the day of birth and hash of the person s first initial of their first name.
B. A count of the years of birth and hash of the person s gender.
C. A count of the century of birth and hash of the last 3 digits of the person s Aadhaar number.
D. A count of the month of birth and hash of the person s first name.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 80
Which is NOT a suitable action to apply to data when the retention period ends?
A. Aggregation.
B. De-identification.
C. Deletion.
D. Retagging.
Answer: D (LEAVE A REPLY)
Retagging is not a suitable action to apply to data when the retention period ends2. Retagging means changing the classification or label of data based on its sensitivity or value2. Retagging does not reduce the risk of unauthorized access or disclosure of personal data that is no longer needed by the organization2. The other options are suitable actions to apply to data when the retention period ends, as they either remove or anonymize personal data2.

NEW QUESTION: 81
SCENARIO
Wesley Energy has finally made its move, acquiring the venerable oil and gas exploration firm Lancelot from its long-time owner David Wilson. As a member of the transition team, you have come to realize that Wilson's quirky nature affected even Lancelot's data practices, which are maddeningly inconsistent. "The old man hired and fired IT people like he was changing his necktie," one of Wilson's seasoned lieutenants tells you, as you identify the traces of initiatives left half complete.

For instance, while some proprietary data and personal information on clients and employees is encrypted, other sensitive information, including health information from surveillance testing of employees for toxic exposures, remains unencrypted, particularly when included within longer records with less-sensitive data. You also find that data is scattered across applications, servers and facilities in a manner that at first glance seems almost random.
Among your preliminary findings of the condition of data at Lancelot are the following:
* Cloud technology is supplied by vendors around the world, including firms that you have not heard of. You are told by a former Lancelot employee that these vendors operate with divergent security requirements and protocols.
* The company's proprietary recovery process for shale oil is stored on servers among a variety of less- sensitive information that can be accessed not only by scientists, but by personnel of all types at most company locations.
* DES is the strongest encryption algorithm currently used for any file.
* Several company facilities lack physical security controls, beyond visitor check-in, which familiar vendors often bypass.
* Fixing all of this will take work, but first you need to grasp the scope of the mess and formulate a plan of action to address it.
Which procedure should be employed to identify the types and locations of data held by Wesley Energy?
A. Data classification.
B. Privacy audit.
C. Data inventory.
D. Log collection
Answer: (SHOW ANSWER)

NEW QUESTION: 82
Which of the following is one of the fundamental principles of information security?
A. Accountability.
B. Accessibility.
C. Confidentiality.
D. Connectivity.
Answer: (SHOW ANSWER)
confidentiality is one of the fundamental principles of information security. Confidentiality refers to protecting information from unauthorized access and disclosure.

NEW QUESTION: 83
An individual drives to the grocery store for dinner. When she arrives at the store, she receives several unsolicited notifications on her phone about discounts on items at the grocery store she is about to shop at. Which type of privacy problem does the represent?
A. Intrusion.
B. Surveillance.

C. Decisional Interference.
D. Exposure.
Answer: B (LEAVE A REPLY)
The individual receives unsolicited notifications on her phone about discounts on items at the grocery store she is about to shop at. This is an example of surveillance because the grocery store is tracking the individual's location and sending her unsolicited notifications.

NEW QUESTION: 84
Which of the following statements describes an acceptable disclosure practice?
A. Intermediaries processing sensitive data on behalf of an organization require stricter disclosure oversight than vendors.
B. With regard to limitation of use, internal disclosure policies override contractual agreements with third parties.
C. When an organization discloses data to a vendor, the terms of the vendor' privacy notice prevail over the organization' privacy notice.
D. An organization's privacy policy discloses how data will be used among groups within the organization itself.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 85
Which of the following are the mandatory pieces of information to be included in the documentation of records of processing activities for an organization that processes personal data on behalf of another organization?
A. Copies of the consent forms from each data subject.
B. Contact details of the processor and Data Protection Offer (DPO).
C. Time limits for erasure of different categories of data.
D. Descriptions of the processing activities and relevant data subjects.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 86
SCENARIO - Please use the following to answer the next question:
Kyle is a new security compliance manager who will be responsible for coordinating and executing controls to ensure compliance with the company s information security policy and industry standards. Kyle is also-new to the company, where collaboration is a core value. On his first day of new-hire orientation, Kyle s schedule included participating in meetings and observing work in the IT and compliance departments.
Kyle spent the morning in the IT department, where the CIO welcomed him and explained that her department was responsible for IT governance. The CIO and Kyle engaged in a conversation about the importance of identifying meaningful IT governance metrics. Following their conversation, the CIO introduced Kyle to Ted and Barney. Ted is implementing a plan to encrypt data at the transportation level of the organization s wireless network. Kyle would need to get up

to speed on the project and suggest ways to monitor effectiveness once the implementation was complete. Barney explained that his short-term goals are to establish rules governing where data can be placed and to minimize the use of offline data storage.
Kyle spent the afternoon with Jill, a compliance specialist, and learned that she was exploring an initiative for a compliance program to follow self-regulatory privacy principles. Thanks to a recent internship, Kyle had some experience in this area and knew where Jill could find some support. Jill also shared results of the company s privacy risk assessment, noting that the secondary use of personal information was considered a high risk.
By the end of the day, Kyle was very excited about his new job and his new company. In fact, he learned about an open position for someone with strong qualifications and experience with access privileges, project standards board approval processes, and application-level obligations, and couldn't wait to recommend his friend Ben who would be perfect for the job.
Which data practice is Barney most likely focused on improving?
A. Inventory.
B. Sharing.
C. Retention.
D. Deletion.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 87
SCENARIO
Looking back at your first two years as the Director of Personal Information Protection and Compliance for the Berry Country Regional Medical Center in Thorn Bay, Ontario, Canada, you see a parade of accomplishments, from developing state-of-the-art simulation based training for employees on privacy protection to establishing an interactive medical records system that is accessible by patients as well as by the medical personnel. Now, however, a question you have put off looms large: how do we manage all the data-not only records produced recently, but those still on hand from years ago? A data flow diagram generated last year shows multiple servers, databases, and work stations, many of which hold files that have not yet been incorporated into the new records system. While most of this data is encrypted, its persistence may pose security and compliance concerns. The situation is further complicated by several long-term studies being conducted by the medical staff using patient information. Having recently reviewed the major Canadian privacy regulations, you want to make certain that the medical center is observing them.
You also recall a recent visit to the Records Storage Section, often termed "The Dungeon" in the basement of the old hospital next to the modern facility, where you noticed a multitude of paper records. Some of these were in crates marked by years, medical condition or alphabetically by patient name, while others were in undifferentiated bundles on shelves and on the floor. The back shelves of the section housed data tapes and old hard drives that were often unlabeled but appeared to be years old. On your way out of the dungeon, you noticed just ahead of you a small

man in a lab coat who you did not recognize. He carried a batch of folders under his arm, apparently records he had removed from storage.
Which cryptographic standard would be most appropriate for protecting patient credit card information in the records system?
A. Obfuscation
B. Symmetric Encryption
C. Hashing
D. Asymmetric Encryption
Answer: D (LEAVE A REPLY)

NEW QUESTION: 88
What tactic does pharming use to achieve its goal?
A. It modifies the user s Hosts file.
B. It creates a false display advertisement.
C. It generates a malicious instant message.
D. It encrypts files on a user s computer.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 89
SCENARIO
Please use the following to answer the next question:
Jordan just joined a fitness-tracker start-up based in California, USA, as its first Information Privacy and Security Officer. The company is quickly growing its business but does not sell any of the fitness trackers itself. Instead, it relies on a distribution network of third-party retailers in all major countries. Despite not having any stores, the company has a 78% market share in the EU. It has a website presenting the company and products, and a member section where customers can access their information. Only the email address and physical address need to be provided as part of the registration process in order to customize the site to the user's region and country. There is also a newsletter sent every month to all members featuring fitness tips, nutrition advice, product spotlights from partner companies based on user behavior and preferences.
Jordan says the General Data Protection Regulation (GDPR) does not apply to the company. He says the company is not established in the EU, nor does it have a processor in the region. Furthermore, it does not do any "offering goods or services" in the EU since it does not do any marketing there, nor sell to consumers directly. Jordan argues that it is the customers who chose to buy the products on their own initiative and there is no "offering" from the company.
The fitness trackers incorporate advanced features such as sleep tracking, GPS tracking, heart rate monitoring. wireless syncing, calorie-counting and step-tracking. The watch must be paired with either a smartphone or a computer in order to collect data on sleep levels, heart rates, etc. All information from the device must be sent to the company's servers in order to be processed, and then the results are sent to the smartphone or computer. Jordan argues that there is no

personal information involved since the company does not collect banking or social security information.
Based on the current features of the fitness watch, what would you recommend be implemented into each device in order to most effectively ensure privacy?
A. Hashing.
B. A2DP Bluetooth profile.
C. Persistent unique identifier.
D. Randomized MAC address.
Answer: D (LEAVE A REPLY)
To most effectively ensure privacy in the fitness watch described in the scenario provided in the exhibit you shared, one feature that could be implemented into each device would be option D: Randomized MAC address.

NEW QUESTION: 90
SCENARIO - Please use the following to answer the next question:
Tom looked forward to starting his new position with a U.S.-based automobile leasing company (New Company), now operating in 32 states. New Company was recently formed through the merger of two prominent players, one from the eastern region (East Company) and one from the western region (West Company). Tom, a Certified Information Privacy Technologist (CIPT), is New Company s first Information Privacy and Security Officer. He met today with Dick from East Company, and Harry, from West Company.
Dick and Harry are veteran senior information privacy and security professionals at their respective companies, and continue to lead the east and west divisions of New Company. The purpose of the meeting was to conduct a SWOT (strengths/weaknesses/opportunities/threats) analysis for New Company. Their SWOT analysis conclusions are summarized below.
Dick was enthusiastic about an opportunity for the New Company to reduce costs and increase computing power and flexibility through cloud services. East Company had been contemplating moving to the cloud, but West Company already had a vendor that was providing it with software-as-a-service (SaaS). Dick was looking forward to extending this service to the eastern region. Harry noted that this was a threat as well, because West Company had to rely on the third party to protect its data.
Tom mentioned that neither of the legacy companies had sufficient data storage space to meet the projected growth of New Company, which he saw as a weakness. Tom stated that one of the team s first projects would be to construct a consolidated New Company data warehouse. Tom would personally lead this project and would be held accountable if information was modified during transmission to or during storage in the new data warehouse.
Tom, Dick and Harry agreed that employee network access could be considered both a strength and a weakness. East Company and West Company had strong performance records in this regard; both had robust network access controls that were working as designed. However, during a projected year-long transition period, New Company employees would need to be able to

connect to a New Company network while retaining access to the East Company and West Company networks.
Which statement is correct about addressing New Company stakeholders expectations for privacy?
A. New Company should expect consumers to read the company s privacy policy.
B. New Company s commitment to stakeholders ends when the stakeholders data leaves New Company.
C. New Company would best meet consumer expectations for privacy by adhering to legal requirements.
D. New Company should manage stakeholder expectations for privacy even when the stakeholders data is not held by New Company.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 91
SCENARIO
Wesley Energy has finally made its move, acquiring the venerable oil and gas exploration firm Lancelot from its long-time owner David Wilson. As a member of the transition team, you have come to realize that Wilson's quirky nature affected even Lancelot's data practices, which are maddeningly inconsistent. "The old man hired and fired IT people like he was changing his necktie," one of Wilson's seasoned lieutenants tells you, as you identify the traces of initiatives left half complete.
For instance, while some proprietary data and personal information on clients and employees is encrypted, other sensitive information, including health information from surveillance testing of employees for toxic exposures, remains unencrypted, particularly when included within longer records with less-sensitive data. You also find that data is scattered across applications, servers and facilities in a manner that at first glance seems almost random.
Among your preliminary findings of the condition of data at Lancelot are the following:
* Cloud technology is supplied by vendors around the world, including firms that you have not heard of. You are told by a former Lancelot employee that these vendors operate with divergent security requirements and protocols.
* The company's proprietary recovery process for shale oil is stored on servers among a variety of less- sensitive information that can be accessed not only by scientists, but by personnel of all types at most company locations.
* DES is the strongest encryption algorithm currently used for any file.
* Several company facilities lack physical security controls, beyond visitor check-in, which familiar vendors often bypass.
* Fixing all of this will take work, but first you need to grasp the scope of the mess and formulate a plan of action to address it.
Which is true regarding the type of encryption Lancelot uses?
A. It employs the data scrambling technique known as obfuscation.
B. Its decryption key is derived from its encryption key.

C. It uses a single key for encryption and decryption.
D. It is a data masking methodology.
Answer: (SHOW ANSWER)
Explanation/Reference: https://www.techopedia.com/definition/25015/data-obfuscation-do

NEW QUESTION: 92
A company configures their information system to have the following capabilities:
Allow for selective disclosure of attributes to certain parties, but not to others.
Permit the sharing of attribute references instead of attribute values - such as "I am over 21" instead of birthday date.
Allow for information to be altered or deleted as needed.
These capabilities help to achieve which privacy engineering objective?
A. Manageability.
B. Predictability.
C. Disassociability.
D. Integrity.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 93
What has been found to undermine the public key infrastructure system?
A. Man-in-the-middle attacks.
B. Browsers missing a copy of the certificate authority's public key.
C. Disreputable certificate authorities.
D. Inability to track abandoned keys.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 94
A clinical research organization is processing highly sensitive personal data, including numerical attributes, from medical trial results. The organization needs to manipulate the data without revealing the contents to data users. This can be achieved by utilizing?
A. k-anonymity.
B. Microdata sets.

C. Polymorphic encryption.
D. Homomorphic encryption.
Answer: (SHOW ANSWER)
Homomorphic encryption. Homomorphic encryption allows computations to be performed on encrypted data without revealing the contents of the data. This can be useful in situations where sensitive personal data needs to be processed without revealing its contents to data users.

NEW QUESTION: 95
SCENARIO
You have just been hired by Ancillary.com, a seller of accessories for everything under the sun, including waterproof stickers for pool floats and decorative bands and cases for sunglasses. The company sells cell phone cases, e-cigarette cases, wine spouts, hanging air fresheners for homes and automobiles, book ends, kitchen implements, visors and shields for computer screens, passport holders, gardening tools and lawn ornaments, and catalogs full of health and beauty products. The list seems endless. As the CEO likes to say, Ancillary offers, without doubt, the widest assortment of low-price consumer products from a single company anywhere.
Ancillary's operations are similarly diverse. The company originated with a team of sales consultants selling home and beauty products at small parties in the homes of customers, and this base business is still thriving.
However, the company now sells online through retail sites designated for industries and demographics, sites such as "My Cool Ride" for automobile-related products or "Zoomer" for gear aimed toward young adults.
The company organization includes a plethora of divisions, units and outrigger operations, as Ancillary has been built along a decentered model rewarding individual initiative and flexibility, while also acquiring key assets. The retail sites seem to all function differently, and you wonder about their compliance with regulations and industry standards. Providing tech support to these sites is also a challenge, partly due to a variety of logins and authentication protocols.
You have been asked to lead three important new projects at Ancillary:
The first is the personal data management and security component of a multi-faceted initiative to unify the company's culture. For this project, you are considering using a series of third- party servers to provide company data and approved applications to employees.
The second project involves providing point of sales technology for the home sales force, allowing them to move beyond paper checks and manual credit card imprinting.
Finally, you are charged with developing privacy protections for a single web store housing all the company's product lines as well as products from affiliates. This new omnibus site will be known, aptly, as "Under the Sun." The Director of Marketing wants the site not only to sell Ancillary's products, but to link to additional products from other retailers through paid advertisements. You need to brief the executive team of security concerns posed by this approach.
If you are asked to advise on privacy concerns regarding paid advertisements, which is the most important aspect to cover?
A. Personal information collected by cookies linked to the advertising network.

B. Unseen web beacons that combine information on multiple users.
C. Sensitive information from Structured Query Language (SQL) commands that may be exposed.
D. Latent keys that trigger malware when an advertisement is selected.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 96
After downloading and loading a mobile app, the user is presented with an account registration page requesting the user to provide certain personal details. Two statements are also displayed on the same page along with a box for the user to check to indicate their confirmation:
Statement 1 reads: "Please check this box to confirm you have read and accept the terms and conditions of the end user license agreement" and includes a hyperlink to the terms and conditions.
Statement 2 reads: "Please check this box to confirm you have read and understood the privacy notice" and includes a hyperlink to the privacy notice.
Under the General Data Protection Regulation (GDPR), what lawful basis would you primarily except the privacy notice to refer to?
A. Legal obligation.
B. Legitimate interests.
C. Vital interests.
D. Consent.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 97
What is the goal of privacy enhancing technologies (PETS) like multiparty computation and differential privacy?
A. To facilitate audits of third party vendors.
B. To protect sensitive data while maintaining its utility.
C. To standardize privacy activities across organizational groups.
D. To protect the security perimeter and the data items themselves.
Answer: B (LEAVE A REPLY)
Explanation/Reference: https://royalsociety.org/-/media/policy/projects/privacy-enhancing-technologies/privacy-report- summary.pdf

NEW QUESTION: 98
Which is likely to reduce the types of access controls needed within an organization?
A. Regular data inventories.
B. Standardization of technology.
C. Increased number of remote employees.
D. Decentralization of data.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 99
SCENARIO
Looking back at your first two years as the Director of Personal Information Protection and Compliance for the Berry Country Regional Medical Center in Thorn Bay, Ontario, Canada, you see a parade of accomplishments, from developing state-of-the-art simulation based training for employees on privacy protection to establishing an interactive medical records system that is accessible by patients as well as by the medical personnel. Now, however, a question you have put off looms large: how do we manage all the data-not only records produced recently, but those still on hand from years ago? A data flow diagram generated last year shows multiple servers, databases, and work stations, many of which hold files that have not yet been incorporated into the new records system. While most of this data is encrypted, its persistence may pose security and compliance concerns. The situation is further complicated by several long-term studies being conducted by the medical staff using patient information. Having recently reviewed the major Canadian privacy regulations, you want to make certain that the medical center is observing them.
You also recall a recent visit to the Records Storage Section, often termed "The Dungeon" in the basement of the old hospital next to the modern facility, where you noticed a multitude of paper records. Some of these were in crates marked by years, medical condition or alphabetically by patient name, while others were in undifferentiated bundles on shelves and on the floor. The back shelves of the section housed data tapes and old hard drives that were often unlabeled but appeared to be years old. On your way out of the dungeon, you noticed just ahead of you a small man in a lab coat who you did not recognize. He carried a batch of folders under his arm, apparently records he had removed from storage.
Which regulation most likely applies to the data stored by Berry Country Regional Medical Center?
A. The Health Records Act 2001
B. Personal Information Protection and Electronic Documents Act
C. The European Union Directive 95/46/EC
D. Health Insurance Portability and Accountability Act
Answer: (SHOW ANSWER)

NEW QUESTION: 100
A credit card with the last few numbers visible is an example of what?
A. Masking data
B. Synthetic data
C. Sighting controls.
D. Partial encryption
Answer: A (LEAVE A REPLY)
Explanation/Reference: https://money.stackexchange.com/questions/98951/credit-card-number-masking-good-practices- rules-law-regulations

NEW QUESTION: 101
SCENARIO
Wesley Energy has finally made its move, acquiring the venerable oil and gas exploration firm Lancelot from its long-time owner David Wilson. As a member of the transition team, you have come to realize that Wilson's quirky nature affected even Lancelot's data practices, which are maddeningly inconsistent. "The old man hired and fired IT people like he was changing his necktie," one of Wilson's seasoned lieutenants tells you, as you identify the traces of initiatives left half complete.
For instance, while some proprietary data and personal information on clients and employees is encrypted, other sensitive information, including health information from surveillance testing of employees for toxic exposures, remains unencrypted, particularly when included within longer records with less-sensitive data.
You also find that data is scattered across applications, servers and facilities in a manner that at first glance seems almost random.
Among your preliminary findings of the condition of data at Lancelot are the following:
* Cloud technology is supplied by vendors around the world, including firms that you have not heard of.
You are told by a former Lancelot employee that these vendors operate with divergent security requirements and protocols.
* The company's proprietary recovery process for shale oil is stored on servers among a variety of less-sensitive information that can be accessed not only by scientists, but by personnel of all types at most company locations.
* DES is the strongest encryption algorithm currently used for any file.
* Several company facilities lack physical security controls, beyond visitor check-in, which familiar vendors often bypass.
* Fixing all of this will take work, but first you need to grasp the scope of the mess and formulate a plan of action to address it.
Which procedure should be employed to identify the types and locations of data held by Wesley Energy?
A. Log collection
B. Data classification.
C. Privacy audit.
D. Data inventory.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 102
After committing to a Privacy by Design program, which activity should take place first?
A. Perform privacy reviews on new projects.
B. Create a privacy standard that applies to all projects and services.
C. Establish a retention policy for all data being collected.

D. Implement easy to use privacy settings for users.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 103
Value Sensitive Design (VSD) focuses on which of the following?
A. Ethics and morality.
B. Principles and standards.
C. Privacy and human rights.
D. Quality and benefit.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 104
SCENARIO
Carol was a U.S.-based glassmaker who sold her work at art festivals. She kept things simple by only accepting cash and personal checks.
As business grew, Carol couldn't keep up with demand, and traveling to festivals became burdensome. Carol opened a small boutique and hired Sam to run it while she worked in the studio. Sam was a natural salesperson, and business doubled. Carol told Sam, "I don't know what you are doing, but keep doing it!" But months later, the gift shop was in chaos. Carol realized that Sam needed help so she hired Jane, who had business expertise and could handle the back-office tasks. Sam would continue to focus on sales. Carol gave Jane a few weeks to get acquainted with the artisan craft business, and then scheduled a meeting for the three of them to discuss Jane's first impressions.
At the meeting, Carol could not wait to hear Jane's thoughts, but she was unprepared for what Jane had to say.
"Carol, I know that he doesn't realize it, but some of Sam's efforts to increase sales have put you in a vulnerable position. You are not protecting customers' personal information like you should." Sam said, "I am protecting our information. I keep it in the safe with our bank deposit. It's only a list of customers' names, addresses and phone numbers that I get from their checks before I deposit them. I contact them when you finish a piece that I think they would like. That's the only information I have! The only other thing I do is post photos and information about your work on the photo sharing site that I use with family and friends. I provide my email address and people send me their information if they want to see more of your work. Posting online really helps sales, Carol. In fact, the only complaint I hear is about having to come into the shop to make a purchase." Carol replied, "Jane, that doesn't sound so bad. Could you just fix things and help us to post even more online?"
'I can," said Jane. "But it's not quite that simple. I need to set up a new program to make sure that we follow the best practices in data management. And I am concerned for our customers. They should be able to manage how we use their personal information. We also should develop a social media strategy." Sam and Jane worked hard during the following year. One of the decisions they made was to contract with an outside vendor to manage online sales. At the end of

the year, Carol shared some exciting news. "Sam and Jane, you have done such a great job that one of the biggest names in the glass business wants to buy us out!
And Jane, they want to talk to you about merging all of our customer and vendor information with theirs beforehand." What type of principles would be the best guide for Jane's ideas regarding a new data management program?
A. Fair Information Practice Principles
B. Collection limitation principles.
C. Incident preparedness principles.
D. Vendor management principles.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 105
What is the term for information provided to a social network by a member?
A. Identifier information.
B. Personal choice data.
C. Declared data.
D. Profile data.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 106
SCENARIO
Wesley Energy has finally made its move, acquiring the venerable oil and gas exploration firm Lancelot from its long-time owner David Wilson. As a member of the transition team, you have come to realize that Wilson's quirky nature affected even Lancelot's data practices, which are maddeningly inconsistent. "The old man hired and fired IT people like he was changing his necktie," one of Wilson's seasoned lieutenants tells you, as you identify the traces of initiatives left half complete.
For instance, while some proprietary data and personal information on clients and employees is encrypted, other sensitive information, including health information from surveillance testing of employees for toxic exposures, remains unencrypted, particularly when included within longer records with less-sensitive data. You also find that data is scattered across applications, servers and facilities in a manner that at first glance seems almost random.
Among your preliminary findings of the condition of data at Lancelot are the following:
* Cloud technology is supplied by vendors around the world, including firms that you have not heard of. You are told by a former Lancelot employee that these vendors operate with divergent security requirements and protocols.
* The company's proprietary recovery process for shale oil is stored on servers among a variety of less- sensitive information that can be accessed not only by scientists, but by personnel of all types at most company locations.
* DES is the strongest encryption algorithm currently used for any file.

* Several company facilities lack physical security controls, beyond visitor check-in, which familiar vendors often bypass.
* Fixing all of this will take work, but first you need to grasp the scope of the mess and formulate a plan of action to address it.
Which is true regarding the type of encryption Lancelot uses?
A. It is a data masking methodology.
B. It uses a single key for encryption and decryption.
C. It employs the data scrambling technique known as obfuscation.
D. Its decryption key is derived from its encryption key.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 107
How can a hacker gain control of a smartphone to perform remote audio and video surveillance?
A. By installing a roving bug on the phone.
B. By manipulating geographic information systems.
C. By performing cross-site scripting.
D. By accessing a phone's global positioning system satellite signal.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 108
What is the main reason the Do Not Track (DNT) header is not acknowledged by more companies?
A. Most web browsers incorporate the DNT feature.
B. It has been difficult to solve the technological challenges surrounding DNT
C. The financial penalties for violating DNT guidelines are too high.
D. There is a lack of consensus about what the DNT header should mean.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 109
What would be an example of an organization transferring the risks associated with a data breach?
A. Using a third-party service to process credit card transactions.

B. Encrypting sensitive personal data during collection and storage
C. Purchasing insurance to cover the organization in case of a breach.
D. Applying industry standard data handling practices to the organization' practices.
Answer: C (LEAVE A REPLY)
Explanation/Reference: http://www.hpso.com/Documents/pdfs/newsletters/firm09-rehabv1.pdf

NEW QUESTION: 110
In day to day interactions with technology, consumers are presented with privacy choices. Which of the following best represents the Privacy by Design (PbD) methodology of letting the user choose a non-zero-sum choice?
A. Using contexts, antecedent events, and other priming concepts to assist the user in making a better privacy choice.
B. Providing plain-language design choices that elicit privacy-related responses, helping users avoid errors and minimize the negative consequences of errors when they do occur.
C. Displaying the percentage of users that chose a particular option, thus enabling the user to choose the most preferred option.
D. Using images, words, and contexts to elicit positive feelings that result in proactive behavior, thus eliminating negativity and biases.
Answer: B (LEAVE A REPLY)