THE QI IQ TEST

Dealerhship IT and Cybersecurity Standards Guide by DealerEFX.

DealerEFX™

DealerEFX is a service offering of The Association of Dealership Compliance Officers. ADCO ASSOCIATION OF DEALERSHIP COMPLIANCE OFFICERS

KNOWLEDGE SECTION

IT Methods & Best Practices

1. **The effective implementation of a Simple Risk Management Framework (SRMF) includes which of the following steps?**
   a. Evaluating, implementing and distributing IT security assessments over time
   b. Ongoing and comprehensive IT system monitoring
   c. Conducting a thorough dealership risk assessment
   d. All of the above

2. **A dealership program to provide training and awareness about IT security to employees should include guidance on _____.**
   a. how to use security tools effectively
   b. how to ensure the IT security service provider selected has the human resources required to fulfill security objectives
   c. the importance of IT security
   d. how to report suspicious activity
   e. how to avoid email phishing and ransomware attacks
   f. All of the above
   g. All of the above, except b

3. **Important tools, best practices and methods for dealership risk management include _____.**
   a. conducting a thorough dealership risk assessment
   b. providing training and awareness about IT security, evaluating cybersecurity tool vendors and ensuring integration and compatibility of security tools
   c. implementing a robust 24/7/365 dealership IT infrastructure monitoring system
   d. conducting proof of concept (PoC) testing
   e. developing a comprehensive incident response plan
   f. All of the above
   g. All of the above, except d

4. **When selecting IT and cybersecurity tools and providers, a dealership should weigh the vendor's market reputation, cybersecurity track record, dealer customer service and response reviews, and the scope and breadth of the vendor's solutions. It is also advisable to conduct a proof of concept (PoC) to assess the effectiveness of the tool in the specific environment and across third-party DSPs.**
   a. True
   b. False

5. **As mandated by the FTC Safeguards Rule, the dealership must develop a comprehensive incident response plan that _____.**
   a. details the steps that will be taken in the event of a security breach
   b. includes the use of cyber remediation tools
   c. addresses possible negotiation consultants (provided by the cybersecurity insurance provider) in the event of a ransomware attack to mitigate the impact and restore normal operations as soon as possible
   d. All of the above
   e. a and b

Understanding System & Software Cybersecurity Threats and Vulnerabilities

1. Coursera, Udemy and edX are platforms that offer courses and tutorials on system and software security.
   a. True
   b. False

2. Some recommended books on system and software security threats and vulnerabilities include _____.
   a. The Web Application Hacker's Handbook by Dafydd Stuttard and Marcus Pinto
   b. Hacking: The Art of Exploitation by Jon Erickson
   c. The Tangled Web: A Guide to Securing Modern Web Applications by Michal Zalewski
   d. The Information by James Gleick
   e. a, b and c

3. Reputable cybersecurity blogs and websites that provide information on the latest security threats and vulnerabilities include _____.
   a. Open Web Application Security Project (OWASP)
   b. KrebsOnSecurity
   c. Schneier on Security
   d. All of the above
   e. a and c

4. Black Hat, DEF CON and RSA Conference are respected security conferences and events to attend for learning about system and software security.
   a. True
   b. False

5. Due to the constantly evolving nature of cybersecurity, a QI best practice is to follow reputable cybersecurity blogs and websites, attend security conferences and events, and participate in online courses and tutorials.
   a. True
   b. False

DSP Cyber Risk Management Practices

1. The purpose of the risk assessment is to identify potential threats and vulnerabilities that could compromise the security of the dealer's system and assess the potential impact of threats stemming from 3rd party DSP software.
   a. True
   b. False

2. Cybersecurity service providers typically implement which of the following measures to protect dealer systems from cyber threats and prevent software vulnerabilities?
   a. Firewalls
   b. Encryption
   c. Secure coding practices
   d. Evolving security technologies
   e. All of the above
   f. All of the above, except c

3. Regular audits and monitoring are important in detecting signs of a security breach in real time – including unusual activity that might otherwise go unnoticed – and allowing for immediate action if a breach has occurred.
   a. True
   b. False

4. Dealer IT and cybersecurity service provider employees are educated in preventing and detecting cyber threats, how to avoid them and how to respond in the event of a security breach.
   a. True
   b. False

Payment Card Industry Data Security Standard (PCI DSS)

1. The purpose of the PCI DSS is to ensure that companies that accept, process, store or transmit credit card information maintain a secure environment.
   a. True
   b. False

2. The PCI DSS is administered and managed by the _____.
   a. PCI SPC (Payment Card Industry Security Protocol Council)
   b. PCI SPA (Payment Card Industry Security Protocol Administration)
   c. PCI SSC (Payment Card Industry Security Standards Council)
   d. Federal Reserve Board
   e. Federal Trade Commission

3. Which of the following is not one of the six control objectives of the PCI DSS?
   a. Build and maintain a secure network and systems
   b. Protect cardholder data
   c. Maintain a vulnerability management program
   d. Implement strong access control measures
   e. Regularly monitor and test networks
   f. Maintain an information security policy
   g. Always require two-factor authentication

4. What actions should a QI take to comply with the "Build and Maintain a Secure Network and Systems" control objective?
   a. Install and maintain a firewall configuration to protect cardholder data
   b. Change vendor-supplied defaults for system passwords and other security parameters
   c. a and b
   d. None of the above

5. Protecting stored cardholder data and encrypting transmission of cardholder data across open, public networks would support compliance with the PCI DSS objective of protecting cardholder data.
   a. True
   b. False

QI RESPONSIBILITIES AND CAPABILITIES SECTION

Developing Policy, Plans and Strategy for Compliance

1. The QI's first step in developing compliant policy, plans and strategy for auto dealership cyber-IT activities is to develop a working knowledge of the laws, regulations, policies and standards that apply to auto dealership cyber-IT activities in the United States.
   a. True
   b. False

2. Federal acts, regulations and rules that apply to auto dealership cyber-IT activities include _____.
   a. the Gramm-Leach-Bliley Act (GLBA)
   b. the Federal Trade Commission Act (FTCA)
   c. the Disposal Rule
   d. the Safeguards Rule
   e. the Magnuson-Moss Warranty Act
   f. All of the above
   g. All of the above, except e

3. Industry-specific standards that can be used as a reference for auto dealership cyber-IT policy, plans and strategy include the _____.
   a. Payment Card Industry Data Security Standard (PCI DSS) for dealerships
   b. National Institute of Standards and Technology (NIST) cybersecurity frameworks, such as the NIST Cybersecurity Framework (CSF) and the NIST Special Publication 800-53
   c. the Uniform Commercial Code (UCC)
   d. All of the above
   e. a and b

4. In developing the dealership's cybersecurity policies and procedures, the QI should address _____.
   a. data protection and access controls
   b. incident response
   c. employee training
   d. compliance with the applicable laws, regulations, policies and standards
   e. regular reviews and updates to policies and procedures to stay abreast of evolving threats
   f. All of the above
   g. All of the above, except c

Assessing and Forecasting IT Resources for the Dealership

1. Identifying internal IT "pain points" is the first step in assessing and forecasting IT resource requirements to meet dealership objectives. This means listening to and documenting the pain points of the dealership's tech users, quantifying the time and resources expended on manual cybersecurity tasks or existing dealership processes because your current technology does not support or allow for automation.
   a. True
   b. False

2 In the context of assessing IT resource requirements, "thinking outside the box" means _____.

a. looking beyond standard solutions and considering how technology can make your processes more efficient to support a “culture of compliance”

b. paying attention to the processes that require repetition or cause delays – and leveraging compliance and cybersecurity technology to minimize inefficiency and eliminate repetition

c. emphasizing software solutions over hardware

d. All of the above

e. a and b

3 Though changes in technology, software and cyber threats are constantly evolving, thinking long term is essential for establishing event milestones that will help identify criteria in your technology deployment timeline and cybersecurity lifecycle. This information will help determine the level of investment appropriate for the lifespan of the technology and the processes and compliance mandates that must be addressed.

a. True

b. False

Identifying External IT & Compliance Partners to Support Cybersecurity Operations

1 Best practices for identifying external IT and compliance partners to support auto dealership cybersecurity operations include _____.

a. researching reputable cybersecurity firms that specialize in the auto industry

b. looking for companies with a strong track record in providing IT, cybersecurity, PCI and FTC Saf guards Rule compliance services

c. consulting industry associations, such as the National Automobile Dealers Association (NADA), your state dealer association, and the Association of Dealership Compliance Officers (ADCO) – for their lists of trusted partners or venders

d. getting recommendations from trusted dealerships and dealer organizations in your 20Group or other professional peer group

e. All of the above

2 Reading reviews and testimonials from other auto dealerships that have worked with potential IT and compliance partners can provide insights into multiple performance factors – the potential partner’s level of expertise, customer service and the dealer’s overall satisfaction with the service – helping the QI make an informed decision.

a. True

b. False

3 To thoroughly vet potential IT and compliance partners, the QI should _____.

a. check their credentials, certifications and industry experience

b. schedule meetings or consultations with a few different companies to discuss the dealership’s specific needs and see which is the best fit

c. a and b

d. None of the above

Working Across Departments and Business Units

1. To implement a dealership's consumer data privacy principles and programs, the QI should understand the dealership's consumer data privacy "first principles," policies and guidelines in order to align them with the cybersecurity objectives. The QI should also command a knowledge of cybersecurity principles and best practices to align the two objectives.
   a. True
   b. False

2. Staying updated on the latest data privacy regulations and laws, such as the FTC Safeguards Rule and the California Consumer Privacy Act (CCPA), helps you implement data privacy principles effectively with the cybersecurity tools available to the QI and ensures continuing compliance with all relevant legislation.
   a. True
   b. False

3. In order to limit liability and help avoid fines, claims and litigation, a QI can show that a "good faith cyber-security compliance program" has been implemented via the systemic use of _____.
   a. data encryption
   b. access controls
   c. an incident response plan
   d. thorough documentation
   e. All of the above
   f. All of the above, except d

4. It's important for QIs to possess strong cross-functional communication skills in order to effectively collaborate with different teams and stakeholders. Methods to help Qis develop such skills include _____.
   a. building a contact list
   b. arranging meetings where the QI employs active listening
   c. learning how to explain complex concepts in a simple manner
   d. clearly articulating and documenting legislated mandates
   e. attending leadership skill-building sessions provided by industry associations
   f. All of the above

ADCO | ASSOCIATION OF DEALERSHIP COMPLIANCE OFFICERS

Dealer EFX™

DealerEFX is a service offering of The Association of Dealership Compliance Officers.
Learn more at www.dealerefx.com