North America Community Meeting 2024

All Hail the Defenders: Cyber Incident Response for PCI…and Everyone Else

Incident Response, Incident Reporting, and PCI DSS v4.0

Harley Geiger, Venable LLP
Sabeen Malik, Rapid7

Who We Are

Harley Geiger

Counsel
Venable LLP

Sabeen Malik

Vice President of Global Government Affairs and Public Policy

Rapid7

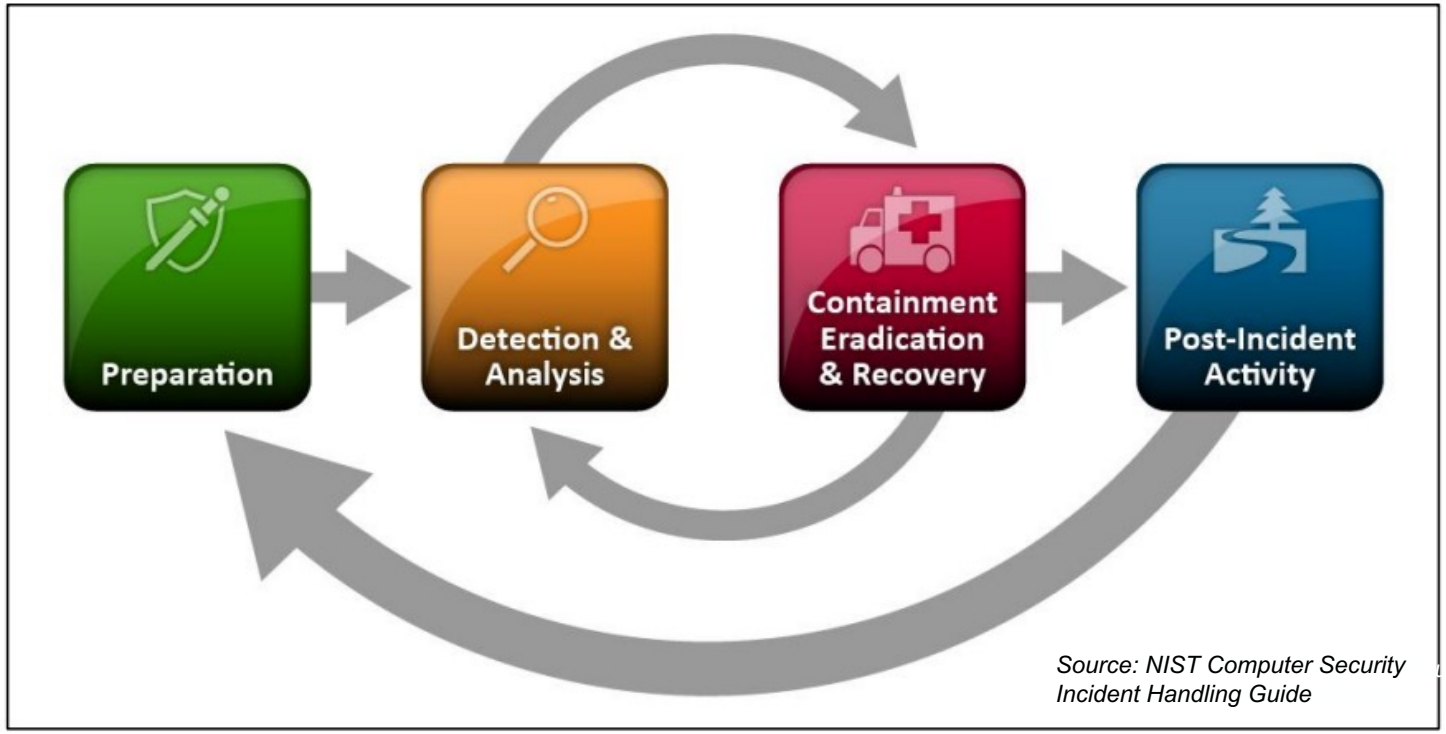
PCI Security Standards Council®

Agenda

1. Incident Response Overview
2. Incident Response Components
3. Incident Reporting Plans
4. Incident Response Requirements
    I. PCI DSS v4.0
    II. GLBA
    III. SEC / SOX
    IV. NYDFS
5. Practical takeaways

PCI Security Standards Council®

Incident Response Overview



Source: NIST Computer Security Incident Handling Guide

- Any organization can fall victim to a cyber attack.
- Incident response is a critical component of any organization's cybersecurity strategy. It involves a coordinated effort between various teams and departments to detect, analyze, and respond to security incidents.
- The goal of incident response is to minimize the impact of an incident and prevent it from happening again.

PCI Security Standards Council

Incident Response Components

- Incident management
- Enterprise incident investigation
- Technical analysis
- Incident scoping
- Crisis communications
- Legal and regulatory concerns
- Executive decision making
- Reporting and remediation

PCI Security Standards Council®

Incident Response Plans

- Details the steps that must be taken
- Establishes roles and responsibilities
- Helps prevent slow responses
- Coordinates multiple workstreams
- Helps ensure thorough decision-making

PCI Security Standards Council®

Incident Response Requirements

- For PCI compliant organizations (i.e, merchants, processors, acquirers, issuers, and other service providers) there are numerous frameworks and requirements that incorporate cyber incident response.

- Key regulations and standards include:
  - **PCI DSS v4.0**
  - **GLBA**
  - **HIPAA**
  - **State laws**
  - **GDPR**

…and more.

PCI Security Standards Council

PCI DSS v4.0 – 12.10.2

Requirements and Testing Procedures		Guidance
12.10 Suspected and confirmed security incidents that could impact the CDE are responded to immediately.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
12.10.1 An incident response plan exists and is ready to be activated in the event of a suspected or confirmed security incident. The plan includes, but is not limited to: • Roles, responsibilities, and communication and contact strategies in the event of a suspected or confirmed security incident, including notification of payment brands and acquirers, at a minimum. • Incident response procedures with specific containment and mitigation activities for different types of incidents. • Business recovery and continuity procedures. • Data backup processes. • Analysis of legal requirements for reporting compromises. • Coverage and responses of all critical system components. • Reference or inclusion of incident response procedures from the payment brands.	**12.10.1.a** Examine the incident response plan to verify that the plan exists and includes at least the elements specified in this requirement. **12.10.1.b** Interview personnel and examine documentation from previously reported incidents or alerts to verify that the documented incident response plan and procedures were followed.	Without a comprehensive incident response plan that is properly disseminated, read, and understood by the parties responsible, confusion and lack of a unified response could create further downtime for the business, unnecessary public media exposure, as well as risk of financial and/or reputational loss and legal liabilities. **Good Practice** The incident response plan should be thorough and contain all the key elements for stakeholders (for example, legal, communications) to allow the entity to respond effectively in the event of a breach that could impact account data. It is important to keep the plan up to date with current contact information of all individuals designated as having a role in incident response. Other relevant parties for notifications may include customers, financial institutions (acquirers and issuers), and business partners. Entities should consider how to address all compromises of data within the CDE in their incident response plans, including compromises to account data, wireless encryption keys, encryption keys used for transmission and storage or account data or cardholder data, etc. *(continued on next page)*
Customized Approach Objective		
A comprehensive incident response plan that meets card brand expectations is maintained.		

PCI DSS v4.0 – 12.10.2

Requirements and Testing Procedures		Guidance
12.10.1 *(continued)*		**Examples** Legal requirements for reporting compromises include those in most US states, the EU General Data Protection Regulation (GDPR), and the Personal Data Protection Act (Singapore). **Further Information** For more information, refer to the *NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide*.
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Proper testing of the security incident response plan can identify broken business processes and ensure key steps are not missed, which could result in increased exposure during an incident. Periodic testing of the plan ensures that the processes remain viable, as well as ensuring that all relevant personnel in the organization are familiar with the plan. **Good Practice** The test of the incident response plan can include simulated incidents and the corresponding responses in the form of a "table-top exercise" that includes participation by relevant personnel. A review of the incident and the quality of the response can provide entities with the assurance that all required elements are included in the plan.
12.10.2 At least once every 12 months, the security incident response plan is: • Reviewed and the content is updated as needed. • Tested, including all elements listed in Requirement 12.10.1.	**12.10.2** Interview personnel and review documentation to verify that, at least once every 12 months, the security incident response plan is: • Reviewed and updated as needed. • Tested, including all elements listed in Requirement 12.10.1.	
Customized Approach Objective		
The incident response plan is kept current and tested periodically.		

PCI DSS v4.0 – 12.10.3

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** An incident could occur at any time, therefore if a person who is trained in incident response and familiar with the entity's plan is available when an incident is detected, the entity's ability to correctly respond to the incident is increased. **Good Practice** Often, specific personnel are designated to be part of a security incident response team, with the team having overall responsibility for responding to incidents (perhaps on a rotating schedule basis) and managing those incidents in accordance with the plan. The incident response team can consist of core members who are permanently assigned or "on-demand" personnel who may be called up as necessary, depending on their expertise and the specifics of the incident. Having available resources to respond quickly to incidents minimizes disruption to the organization. Examples of types of activity the team or individuals should respond to include any evidence of unauthorized activity, detection of unauthorized wireless access points, critical IDS alerts, and reports of unauthorized critical system or content file changes.
12.10.3 Specific personnel are designated to be available on a 24/7 basis to respond to suspected or confirmed security incidents.	**12.10.3** Examine documentation and interview responsible personnel occupying designated roles to verify that specific personnel are designated to be available on a 24/7 basis to respond to security incidents.	
Customized Approach Objective		
Incidents are responded to immediately where appropriate.		

PCI DSS v4.0 – 12.10.4

Requirements and Testing Procedures		Guidance
Defined Approach Requirements **12.10.4** Personnel responsible for responding to suspected and confirmed security incidents are appropriately and periodically trained on their incident response responsibilities.	**Defined Approach Testing Procedures** **12.10.4** Examine training documentation and interview incident response personnel to verify that personnel are appropriately and periodically trained on their incident response responsibilities.	**Purpose** Without a trained and readily available incident response team, extended damage to the network could occur, and critical data and systems may become "polluted" by inappropriate handling of the targeted systems. This can hinder the success of a post-incident investigation. **Good Practice** It is important that all personnel involved in incident response are trained and knowledgeable about managing evidence for forensics and investigations.
Customized Approach Objective Personnel are knowledgeable about their role and responsibilities in incident response and are able to access assistance and guidance when required.		
Defined Approach Requirements **12.10.4.1** The frequency of periodic training for incident response personnel is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1.	**Defined Approach Testing Procedures** **12.10.4.1.a** Examine the entity's targeted risk analysis for the frequency of training for incident response personnel to verify the risk analysis was performed in accordance with all elements specified in Requirement 12.3.1. **12.10.4.1.b** Examine documented results of periodic training of incident response personnel and interview personnel to verify training is performed at the frequency defined in the entity's targeted risk analysis performed for this requirement.	**Purpose** Each entity's environment and incident response plan are different, and the approach will depend on a number of factors, including the size and complexity of the entity, the degree of change in the environment, the size of the incident response team, and the turnover in personnel. Performing a risk analysis will allow the entity to determine the optimum frequency for training personnel with incident response responsibilities.
Customized Approach Objective Incident response personnel are trained at a frequency that addresses the entity's risk.		
Applicability Notes *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*		

PCI Security Standards Council

PCI DSS v4.0 – 12.10.5

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
12.10.5 The security incident response plan includes monitoring and responding to alerts from security monitoring systems, including but not limited to: • Intrusion-detection and intrusion-prevention systems. • Network security controls. • Change-detection mechanisms for critical files. • The change-and tamper-detection mechanism for payment pages. *This bullet is a best practice until its effective date; refer to Applicability Notes below for details.* • Detection of unauthorized wireless access points.	**12.10.5** Examine documentation and observe incident response processes to verify that monitoring and responding to alerts from security monitoring systems are covered in the security incident response plan, including but not limited to the systems specified in this requirement.	Responding to alerts generated by security monitoring systems that are explicitly designed to focus on potential risk to data is critical to prevent a breach and therefore, this must be included in the incident-response processes.
Customized Approach Objective		
Alerts generated by monitoring and detection technologies are responded to in a structured, repeatable manner.		
Applicability Notes		
The bullet above (for monitoring and responding to alerts from a change- and tamper-detection mechanism for payment pages) is a best practice until 31 March 2025, after which it will be required as part of Requirement 12.10.5 and must be fully considered during a PCI DSS assessment.		

PCI DSS v4.0 – 12.10.6

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Incorporating lessons learned into the incident response plan after an incident occurs and in-step with industry developments, helps keep the plan current and able to react to emerging threats and security trends. **Good Practice** The lessons-learned exercise should include all levels of personnel. Although it is often included as part of the review of the entire incident, it should focus on how the entity's response to the incident could be improved. It is important to not just consider elements of the response that did not have the planned outcomes but also to understand what worked well and whether lessons from those elements that worked well can be applied to areas of the plan that did not. Another way to optimize an entity's incident response plan is to understand the attacks made against other organizations and use that information to fine-tune the entity's detection, containment, mitigation, or recovery procedures.
12.10.6 The security incident response plan is modified and evolved according to lessons learned and to incorporate industry developments.	**12.10.6.a** Examine policies and procedures to verify that processes are defined to modify and evolve the security incident response plan according to lessons learned and to incorporate industry developments.	
	12.10.6.b Examine the security incident response plan and interview responsible personnel to verify that the incident response plan is modified and evolved according to lessons learned and to incorporate industry developments.	
Customized Approach Objective		
The effectiveness and accuracy of the incident response plan is reviewed and updated after each invocation.		

PCI DSS v4.0 – 12.10.7

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
12.10.7 Incident response procedures are in place, to be initiated upon the detection of stored PAN anywhere it is not expected, and include: • Determining what to do if PAN is discovered outside the CDE, including its retrieval, secure deletion, and/or migration into the currently defined CDE, as applicable. • Identifying whether sensitive authentication data is stored with PAN. • Determining where the account data came from and how it ended up where it was not expected. • Remediating data leaks or process gaps that resulted in the account data being where it was not expected.	**12.10.7.a** Examine documented incident response procedures to verify that procedures for responding to the detection of stored PAN anywhere it is not expected to exist, ready to be initiated, and include all elements specified in this requirement. **12.10.7.b** Interview personnel and examine records of response actions to verify that incident response procedures are performed upon detection of stored PAN anywhere it is not expected.	Having documented incident response procedures that are followed in the event that stored PAN is found anywhere it is not expected to be, helps to identify the necessary remediation actions and prevent future leaks. **Good Practice** If PAN was found outside the CDE, analysis should be performed to 1) determine whether it was saved independently of other data or with sensitive authentication data, 2) identify the source of the data, and 3) identify the control gaps that resulted in the data being outside the CDE. Entities should consider whether there are contributory factors, such as business processes, user behavior, improper system configurations, etc. that caused the PAN to be stored in an unexpected location. If such contributory factors are present, they should be addressed per this Requirement to prevent recurrence.
Customized Approach Objective		
Processes are in place to quickly respond, analyze, and address situations in the event that cleartext PAN is detected where it is not expected.		
Applicability Notes		
This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.		

GLBA - FTC Safeguards Rule

Who it Applies To:

Non-banking financial institutions, such as mortgage brokers, motor vehicle dealers, and payday lenders

Incident Response Requirements:

Establish a written incident response plan designed to promptly respond to, and recover from, any security event materially affecting the confidentiality, integrity, or availability of customer information in your control.

(1) The goals of the incident response plan;
(2) The internal processes for responding to a security event;
(3) The definition of clear roles, responsibilities, and levels of decision-making authority;
(4) External and internal communications and information sharing;
(5) Identification of requirements for the remediation of any identified weaknesses in information systems and associated controls;
(6) Documentation and reporting regarding security events and related incident response activities; and
(7) The evaluation and revision as necessary of the incident response plan following a security event.

SEC / SOX

Who it Applies To:

U.S. reporting issuers and foreign private issuers, including all companies with stock traded on U.S. exchanges (public companies).

Incident Response Requirements:

Maintain effective controls and procedures that enable timely disclosures of material cybersecurity incidents.

Reporting Requirements:

Disclose material cybersecurity incidents on Form 8-K within four business days of determining the incident is material, and disclose any material updates on an ongoing basis

NYDFS Cybersecurity Regulation

Who it Applies To:
New York insurance companies, banks, and other regulated financial services institutions—including agencies and branches of non-US banks licensed in the state of New York.

Incident Response Requirements:
Develop and implement an incident response plan.

Maintain business continuity and disaster recovery plan requirements that are tested annually.

Reporting Requirements:
Requires notice of all cybersecurity incidents within 72 hours after determining that the event has occurred.

Requires notice and explanation of extortion payments made in connection with cybersecurity events involving the covered entity within 24 hours of the payment.