What happens if I am breached?

Natasja Bolton, Consulting Manager, Sysnet Global Solutions

How do I recognise a breach?

A breach is an intrusion into your computer systems or physical environment where unauthorised access, disclosure, modification, or destruction of data may have led to a compromise of cardholder data.

A number of activities and security events may indicate a breach has taken place or is underway. Indicators include:

- Detection of unauthorised or unusual activity on your computer systems or network, including the presence of unauthorised wireless access points or critical alerts from your intrusion detection system;
- Detection of malware (viruses, Trojans or other unauthorised executables or programmes) and / or unauthorised critical system or content file changes on your computer systems;
- Malicious attacks against your Internet-facing computer systems;
- Evidence of physical tampering with card readers, Point of Sale (POS) systems/ terminals or other computer equipment;
- Accidental or deliberate contravention of policies or processes relating to the handling of cardholder data, e.g. mistakenly including card data in an external communication, misplaced hard copy reports containing card data;
- Lost or stolen hard copy media containing cardholder data (paper receipts, reports, etc) or other evidence of unauthorised physical intrusion;
- Lost or stolen computer equipment and media (computers, laptops, mobile devices or removable media which may have had access to or contained cardholder data).

Any such unusual activities, security alerts or policy / process infringements may be indicative of a possible breach and should be investigated.

How should I be prepared for a breach?

The key to breach preparedness is having a plan; a detailed and thorough incident response plan that considers a variety of breach scenarios that may affect you or the third parties that store, process or transmit cardholder data on your behalf.

That plan must contain all the key elements to allow your company to react effectively. That is to investigate, contain, notify and respond in a timely manner thereby reducing the potential impact of a breach.

The plan must:

- Define and allocate incident response responsibilities;
- Ensure security events and indicators of potential compromise are recognised and reported;
- Ensure response actions are taken immediately to contain, respond to and recover from the breach;
- Define breach notification requirements and contact details;
- Be distributed to, read and understood by all responsible parties;

About Sysnet Global Solutions

Established in 1989, Sysnet Global Solutions provides payment card industry compliance services, specialising in PCI DSS compliance validation and merchant intelligence solutions Sysnet offers a range of services, including its proprietary web based compliance management and merchant intelligence solution SysnetAIR™, to a wide variety of businesses including acquirers, ISOs, international banks, payment service providers and merchants. Sysnet has more than 20 years experience in multiple IT environments and its expert engineering and consulting teams are certified to the highest standards. Headquartered in Dublin, Ireland, Sysnet has clients in over 35 countries worldwide.

- Be available to all in the event of a breach;
- Be regularly tested.

Do not underestimate the value of testing your incident response plan. A walkthrough test with all key parties present will highlight flaws, discrepancies or unknown dependencies. It is critical that personnel know who to contact, their responsibilities and the actions they should take in the event of a security event or system breach.

How should I respond to a breach?

1. Take action to contain the breach, to limit further exposure and minimise further loss of data:

- Do not access or alter compromised systems; don't logon or change passwords;
- Isolate affected systems by disconnecting them from the network and do not switch off;
- Collect and preserve logs and other electronic evidence to facilitate investigation:
  - Ensure logs are not overwritten as time progresses
  - Take a back-up of the affected systems to preserve a record of their current state;

2. Record details of the breach and all actions taken, when and by whom.

3. Immediately alert all necessary parties:

- Internal parties with incident response responsibilities, such as your incident response team or information security officer;
- Your acquirer;
- The card brands;
- Local law enforcement.

4. Identify the card data that may have been impacted (Primary Account Number, Full Track data, Sensitive Authentication Data, encrypted or plain text data) and the potentially compromised account numbers and report to your acquirer.

5. Follow your acquirer's incident investigation procedures which may include engaging with a PCI Forensic Investigator (PFI) to determine:

- The scope of the breach (locations and systems);
- The window of attack (or vulnerability);
- The attack vector;
- The cardholder data at risk of compromise;

Additional Sysnet PCI DSS Services

PCI DSS Trusted Advisor

- Information security strategy, policy & procedure development
- Remediation plan
- Solution compliance and compensating control validation
- Remediation project progress review

PCI DSS Annual Assessment

- Pre assessment
- Validation upgrade

PCI DSS Programme Management

- Web application vulnerability assessment
- Penetration testing
- Seal of approval
- Onsite assessment and PCI DSS validation

PCI DSS Readiness Assessment

- Documentation review
- Gap analysis
- Introductory workshop
- Training
- Compliance scope analysis
- Risk assessment
- Scanning worldwide
- Forensic services

For more information please call +44 (0) 207 643 1795 or email info@sysnetglobalsolutions.com

PCI FORENSIC INVESTIGATOR PROGRAM · APPROVED SCANNING VENDOR · QUALIFIED SECURITY ASSESSOR · ISO 27001

sysnet global solutions.