sysnet global solutions

Data Breach:

Prepare your Business

How should I prepare for a breach?

Have an incident response plan

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

Your incident response 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 to any suspected incident, 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
- Be available to all in the event of a breach
- Be regularly tested

You can make use of this Security Incident Response Plan Template (https://sysnetgs.com/wp-content/uploads/2016/08/Security-Incident-Response-Plan-1.dotx) to help you fully define and document your Incident Response Plan.

Test your plan

Do not underestimate the value of testing your incident response plan. A walkthrough test or practical simulation of a data breach 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.

Testing your incident response plan will make sure you and your third party service providers are ready and able to respond to a real security incident in a timely and effective manner. This in turn will help you to maintain business continuity, quickly recover normal business operations and thereby minimise the impact of the breach on your customers and your business.

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:

- Unauthorised or unusual user account activity on your computer systems or network, such as excessive or unusual log-in behaviour
- Excessive or unusual remote access activity into your business. In particular, watch out for suspicious activities linked to third party vendor or service provider accounts used for remote access into your business systems
- The presence of new or unauthorised wireless networks (Wi-Fi) accessible from or otherwise connected to your business network
- Detection of malware (viruses, Trojans or other unauthorised executables or programs) on your network or systems
- The presence of, or unusual activity in relation to, new/unapproved software and programs on your business systems
- Critical alerts from your firewall, intrusion detection systems, web application firewall or other security monitoring and protection systems
- Malicious attacks against your Internet-facing computer systems as well as suspicious or unusual activity on, or behaviour of, your internet-facing systems
- Evidence of tampering with Point-of-Sale (POS) payment devices, payment terminals, chip & PIN/signature devices or dip/swipe card readers, as well as of your computer and networking equipment
- Any card-skimming devices found in your business
- Hardware or software key-loggers found connected to or installed on your systems
- 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 merchant receipts or any other records that display the full payment card number or card security code (the 3- or 4-digit number printed on the card) or other evidence of unauthorised physical intrusion
- Lost or stolen computer equipment and media (computers, laptops, mobile devices, removable media, etc.) which may have had access to or contained payment card data or other sensitive data

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

How should I respond to a breach?

Your Incident Response Plan must outline the steps to be taken to protect your business and react to a security incident. In summary those steps are:

1. Immediately report the breach, security incident or suspicious security event (i.e. to the Incident Response Lead named in your Security Incident Response Plan)
2. Investigate the incident and initiate the actions laid out in the Security Incident Response Plan
3. 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 your network or unplugging any network cables and do not switch them off
    - If using a wireless network, change the SSID (Service Set Identifier) on the wireless access point and on systems that may be using this wireless network (but not on any systems believed to be compromised).
    - 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

4. Record details of the breach and all actions taken, when and by whom
5. Stay alert for further signs of compromise or suspicious activity
6. Notify all necessary parties:

    - Internal parties with incident response responsibilities, such as senior management, personnel responsible for communications / PR
    - Your acquirer
    - Local law enforcement
    - Parties affected by the compromise such as customers, business partners or suppliers

7. 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
8. 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 (the 'accounts at risk').