PCI – Sharing the burden of risk

Cyber risks are often thought to be the responsibility of the IT department. IT security is a 'point in time' issue, and so the repercussions of a cyber breach are not the primary responsibility of the IT department.

Erica Constance reports

As the internet has become a critical component of our daily lives, personally and in business, more than ever, companies need to ensure the security of their networks and data. Evolving technology is allowing money to flow between accounts in innovative ways. With new technologies come new vulnerabilities; these need to be constantly monitored and managed. Payment card data is extremely attractive to financially motivated actors. Therefore, having this data passing through or stored within the network, makes a company a natural target.

The educated customer is looking to only transact with those companies that can demonstrate at least a level of adequate security in place to mitigate cyber risks. As much as PCI compliance strengthens the brand of a company, a PCI breach can have an adverse effect and weaken it.

Cyber risks are often incorrectly or naively thought to be the responsibility of the IT department. These teams work hard to keep the network secure whilst balancing a need to ensure the network is available in real-time for all employees to carry out the business operations. Their role is vital to the success of the company and is a challenging ongoing project.

However, IT security is a 'point in time' issue, and so the repercussions of a cyber breach such as customer churn, loss of profits, breach of PCI contracts, breach of data protection regulations, damage to reputation, are not the primary responsibility of the IT department.

The IT department could make the network 100% secure – remove all access from the external world, create a closed network where no information can be sent out or inputted by mobile devices. This is simply not practical, so cyber risks must be managed more widely across organisations, involving the many various stakeholders who are responsible for different elements to provide a comprehensive defence (see Table 1).

In managing cyber risks, there is the potential for conflict between different parts of the business. Those in operations do not always make it easy for the IT department to achieve their goal of locking down the network from intruders or internal cyber breaches.

Table 1

Cyber risk stakeholders	Cyber role	Cyber risk responsibility
IT Department	Manage and maintain a secure IT network	Implement strong perimeter defences to keep hackers out, and internal controls limiting the potential for human error. Creating and owning the Incidence Response Plan
Legal	PCI, IT outsourcer and NDA contract reviews	Ensuring contractual liabilities, warranties and terms are acceptable
Chief Privacy Officer	Understand what confidential data is held within the organisation and which Privacy Regulations apply	Ensure that sensitive data is adequately collected, stored and disposed
Risk & Audit	Identify cyber risks and ensure the risks are either mitigated or managed effectively throughout the organisation	Ensure controls and checks are in place and report the cyber risks to the board
HR and Compliance	Implementing training, controls and procedures to minimise cyber risks	Ensuring awareness of cyber risks are raised and mitigated throughout the organisation
Finance	Managing budgets and investment in cyber risk prevention and risk transfer	Ensuring cash is available in the event of a cyber breach, possibly through purchasing insurance
Security	Effectively control all physical perimeters	Ensuring zero unauthorised physical access to IT networks and sensitive information
Chief Executive Officer	To mitigate cyber risks negatively affecting the company	Ultimately is responsible for all cyber risks within the organisation