SECURING THE FUTURE

In this Issue

- External and internal breaches: what can we learn?
- What steps should businesses take?
- Best practices to prevent data loss
- Request your free security consultation

Inside job versus outside hack – How to determine if you're at risk

In this issue, we will discuss how to evaluate internal and external information security protocols to help an organisation assess how susceptible they are to a breach.

When it comes to information security breaches, many organisations may be tempted to focus their efforts on protecting themselves from a faceless, inconspicuous culprit. However, security breaches not only occur as the result of malicious intent from an outside source; they can also be accidental, resulting from an internal error, or an "inside job" perpetrated by a rogue employee. Technology has made everything more accessible for both employees and outsiders, making it more difficult to control the flow of information. That's why it has never been more crucial for organisations to examine their information security policies and procedures. But how can organisations ensure they are protected, both internally and externally?

External and internal breaches: what can we learn?

Every year, UK organisations feel the impact of both external and internal breaches that could have been avoided.

In 2013 a City Council in Scotland was fined £150,000 by the Information Commissioner's Office (ICO) for the loss of two unencrypted laptops, one of which contained personal details of more than

SECURING THE FUTURE

20,000 people (including bank account details of over 6,000 individuals). The laptops were stolen from council premises that were insecure as they were being refurbished — there had already been complaints of theft and a lack of security at the site that had gone unheeded. The ICO investigation discovered that a further 74 unencrypted laptops were missing, six of which were known to be stolen. It found that, despite its previous warning and in breach of its own policy, the council had issued a number of its staff with unencrypted laptops after encountering problems with the encryption software. The fact that these laptops have never been recovered, and no record was made of the information stored on them, means the true extent of the breach will most likely never be known.

The Council had been issued with an enforcement notice previously, in 2010, after a similar incident where an unencrypted memory stick was lost. The fact that poor information security practices persisted, even after the initial intervention and subsequent sanctions from the ICO, demonstrates the consequences of not having a clearly understood policy that is reflected in the everyday practices of employees. Further, it indicates that regular, effective training is essential in helping to safeguard against breaches and highlights the fact that breaches can come from sources outside of an organisation, so employees must remain vigilant in their protection of sensitive information.[1]

UK organisations have also felt the impact of an internal oversight. In 2012, a council worker at a County Council just outside London sent personal and financial data of 400 people in care to an unauthorised recipient. The data allegedly contained addresses and financial information about citizens in "substantial" and "critical" need of care and was sent from the Adults Health and Community Wellbeing Department to an external computer outside of the council. Following the breach, a council staff member was sacked and the incident reported to Essex Police as well as the ICO.[2] This case once again demonstrates the significance of ensuring that employees are all trained in proper information and document security protocols.

Overall, both cases demonstrate a similar lesson: it is essential to have well-established, communicated and understood information security procedures in every organisation. Organisations need to be aware that information security breaches can come from many sources and all need to be taken into consideration when evaluating their risk levels.

1 BBC, www.bbc.co.uk/news/uk-scotland-glasgow-west-22807593
2 ITPRO, www.itpro.co.uk/642367/data-breach-in-essex-exposes-details-of-400-people

SECURING THE FUTURE

What steps should businesses take?

One of the first steps in determining an organisation's level of risk is to gauge employee awareness of security protocols. If an organisation does not effectively communicate its protocols to employees, this can increase their overall susceptibility to a loss of sensitive data. The Shred-it 2014 Information Security Tracker revealed that nearly a quarter (23%) of large and just under a third (31%) of small businesses surveyed in the UK did not have a known and understood protocol in place for storing and disposing of confidential data. If there is no clear protocol in place, this not only makes it easier for someone outside of the organisation to acquire information — it could also lead to a loss of data due to internal oversight or malicious intent.

Though employee awareness of existing policies and procedures around document destruction and information security is vital, there must be reinforcement through proper employee training. The 2014 Security Tracker asked businesses how regularly their staff were trained in regards to their company's information security procedures or protocols. Over half (52%) of large organisations and more than two thirds (70%) of SMEs do not provide regular training on information security. However, if employees are not fully trained in effective document destruction practices and information security procedures, the organisation could be a target of both internal and external breaches that could easily be avoided.

Being the victim of a data breach, whether it originates from within an organisation or outside of it, can have lasting consequences on organisations from all sectors. A recent study from the Ponemon Institute revealed that the average cost incurred by organisations who suffered a data security breach has now risen to a staggering £2.21 million.[3] For smaller companies, this can be a potentially devastating financial setback, or may even result in the loss of an entire business. However, large organisations may not just suffer considerable financial repercussions – they could also experience a loss of trust from their stakeholders and irreversible reputational damage, the consequences of which can be far-reaching and long term.

Best practices to prevent data loss

When examining your organisation's information security policies and procedures, consider these best practices which could help minimise the risk of both an internal and external breach:

- Develop a comprehensive information security policy that is clearly communicated to all staff

3 Ponemon Institute, 2014 Cost of Data Breach Global Analysis, www.ponemon.org

SECURING THE FUTURE

- Regularly train staff in proper information and document security protocols
- Ensure unused or obsolete hard drives are completely destroyed, as deleting, degaussing or wiping them does not guarantee the information cannot be recovered
- Configure passwords to protect wireless networks and use unique passwords for secure sites
- Be diligent about who has access to your office workspace and any sensitive information within it
- Implement a shred-all policy by having staff put all unwanted documents in a locked console and then securely shredded and recycled to ensure sensitive data cannot accidentally end up in unsecure waste or recycling streams

Your FREE Security Consultation

To conduct your own information security self-assessment, Shred-it has developed an online survey to help businesses better understand security gaps. You can access it via the following link: shredit.co.uk/information-security-best-practices-and-checklist

To learn more about Shred-it services or to book your FREE data security risk assessment, visit shredit.co.uk

You can also visit Shred-it on Facebook and Linkedin or follow us on Twitter @Shredit_UK.