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 organization assess how susceptible they are to a breach.

When it comes to information security breaches, many organizations 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." 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 organizations to examine their information security policies and procedures. But how can organizations ensure they are protected, both internally and externally?

External and internal breaches: what can we learn?

Every year, Canadian organizations feel the impact of both external and internal breaches that could have been avoided. In March 2012, a Toronto man was charged with fraud when he stole nearly 30,000 x-rays from clinics and hospitals across Ontario[1]. The man posed as an employee of a recycling firm that picks up x-rays when they are ready to be disposed of by wearing one of the recycling company's uniforms. X-rays can store a large amount of sensitive information and in sectors such as health care,

1 http://ottawa.ctvnews.ca/ottawa-police-charge-toronto-man-after-thousands-of-x-rays-stolen-1.778085

where data is particularly sensitive, this story was very concerning to the public. Organizations must be aware of any external company or individual entering their premises as it can impact their risk of a breach. Even if a familiar company or individual requests entry into an office, it is important to always check identification and request that they sign-in and sign-out during every visit. No matter the level of familiarity, employees must remain vigilant in their protection of sensitive information. This case reaffirms the importance of having clearly understood protocols, as breaches can come from many sources outside of an organization.

Canadian organizations have also felt the impact of an internal oversight in 2012. In July, it was revealed that Elections Ontario lost the personal data of 2.4 million voters when USB sticks housing the data were stolen[2]. The USB sticks were found to lack proper encryption and many staff admitted to not understanding the data encryption procedure. What's more concerning is staff continued to place sensitive data on unsecured USB sticks even after the theft occurred. This incident has resulted in a loss of public trust from both government officials and Ontario residents. Ann Cavoukian, Ontario's Information and Privacy Commissioner, is holding Elections Ontario managers accountable for not training staff on proper security procedures. This case 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 may help to safeguard against breaches.

Though both cases have different culprits and causes, they both have a similar lesson: *it is essential to have well-established, communicated and understood information security procedures in every organization.* Organizations need to be aware that information security breaches can come from many sources and all need to be taken into consideration when organizations evaluate their risk levels.

What steps should businesses take?

One of the first steps in determining an organization's level of risk is to gauge employee awareness of security protocols. If an organization does not effectively communicate its protocols to employees, this can increase the organization's overall susceptibility to a loss of sensitive data. The Shred-it 2012 Information Security Tracker[3] revealed that 38 per cent of large and small businesses surveyed in Canada 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 organization to acquire information – it could also lead to a loss of data due to internal oversight.

2 http://www.theglobeandmail.com/news/national/privacy-commissioner-blasts-elections-ontario-over-missing-voter-data/article4452259/
3 http://shredit.com/Shred-it-Security-Tracker-2012

SECURING THE FUTURE

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 2012 Shred-it Information Security Tracker asked businesses how regularly their staff was trained in regards to their company's information security procedures or protocols. It was revealed that 28 per cent of Canadian companies, large and small, never train their staff, with 45 per cent admitting to training only on an as-needed basis. If employees are not fully trained in effective document destruction practices and information security procedures, the organization could be a target of both internal and external breaches that could be avoided.

Being the victim of a data breach, whether it originates from within an organization or outside of one, can have lasting consequences on organizations from all sectors. A recent study from the Ponemon Institute revealed that when healthcare organizations suffered a data breach, the average economic impact of the breach was $2.2 million[4]. For smaller organizations, this can be a potentially devastating financial setback, or may even result in a loss of an entire business. However, large organizations may not just suffer considerable financial repercussions – they could also experience a loss of trust from their stakeholders and irreversible reputational damage.

Best practices to prevent data loss

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

- Develop a comprehensive information security policy that is clearly communicated to all staff
- Regularly train staff in proper information and document security protocols
- Enact a shred-all policy by having staff put unneeded documents in a locked console to ensure sensitive data is not accessible
- Ensure unused or obsolete hard drives are fully crushed, as deleting, degaussing or wiping hard drives 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 sensitive information

4 http://www2.idexpertscorp.com/assets/uploads/PDFs/2011_Ponemon_ID_Experts_Study.pdf

SECURING THE FUTURE

Your FREE Security Consultation

Shred-it has developed an online survey to help businesses better understand security gaps. To conduct your own security self-assessment, visit the following link:
www.shredit.com/Shredding-Service/Risk-Assessment-Survey.aspx

To learn more about Shred-it services or to book your FREE security assessment, visit: www.shredit.com

For more details on the 2012 Shred-it Information Security Tracker, please visit:
www.shredit.com/Shred-it-Security-Tracker-2012

You can also visit Shred-it on Facebook, LinkedIn or follow us on Twitter at @Shredit.

About Shred-it

Shred-it is a world-leading information security company providing document destruction services that ensure the security and integrity of our customers' private information. The company operates 140 branches in 16 countries worldwide, servicing over 150,000 global, national and local businesses, including the world's top intelligence and security agencies, more than 500 police forces, 1,500 hospitals, 8,500 bank branches and 1,200 universities and colleges.