

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, American organizations feel the impact of both external and internal breaches that could have been avoided. In May 2012, a passerby found a dumpster overflowing with files in a parking lot outside an LA Fitness¹. While the papers were those of ex-gym members, the files contained private

¹ <http://www.kpho.com/story/18362022/passersby-finds-hundreds-of-documents-with-personal-info-in-dumpster>



SECURING THE FUTURE

information, including names, addresses, social security numbers and credit card data. The attorney for Fitness 1, the gym that had been located at the same place before LA Fitness, claimed that it sold the location along with some memberships to LA Fitness, which had likely stored the contracts there. This case demonstrates the importance of securely shredding important documents before disposing of them. Companies owe it to their customers to ensure that their personal and billing information remains confidential.

American organizations have also felt the impact of internal breaches. It was revealed in 2012 that a woman stole confidential files from the psychiatric hospital where she was formerly employed². She sent six letters to patients between 2011 and 2012, threatening to expose confidential psychiatric information about them. She also forged some letters, writing that the patients' treatment didn't work and that lobotomy was suggested. She claimed that these acts were meant to embarrass the hospital for firing her. This shows that organizations need to properly secure information, even within their network of employees. Unauthorized employees should not gain access to confidential information about patients because it could potentially cause a great deal of harm.

Both of these cases have different people at fault and varying motives, but they both show the importance of having security procedures in place at organizations. Companies should be aware that data security breaches can occur because of various people and causes, ultimately impacting both the company and their customers. Proper security measures should be established in advance to prevent these breaches from occurring.

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 revealed that 36 per cent of large and small businesses surveyed in the U.S. 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://chicago.cbslocal.com/2012/08/22/ex-hospital-employee-accused-of-stealing-patient-files-harassing-patients/>



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 Tracker³ asked businesses how regularly their staff was trained in regards to their company's information security procedures or protocols. It was revealed that 30 per cent of U.S. companies, large and small, never train their staff, with 64 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 million⁴. 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

3 <http://shredit.com/Shred-it-Security-Tracker-2012>

4 http://www2.idexperts.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.

800.697.4733 | shredit.com



Making sure
it's secure.™