SECURING THE FUTURE

In this Issue

- Why does information security matter?
- Businesses and organisations need to take more proactive measures
- How to start creating a culture of security and trust
- Request your free security consultation

It's all about trust: How to establish and maintain trust by developing a culture of security

In this issue, we will discuss how implementing and enforcing document security protocols can help an organisation maintain trust with both internal and external stakeholders.

Reputation is an important asset — a powerful, yet intangible and fragile one that serves as a magnet, attracting attention and often new business. While most businesses work hard to build and maintain a positive reputation with stakeholders, many underestimate how severely a data breach could undermine these efforts, potentially causing the public to lose trust in the organisation and long-term damage to the brand. With this in mind, the protection of business, employee and customer information should be of vital concern to all organisations.

Why does information security matter?

Case Study

In June 2012, an NHS Trust in the south-east of England was given the highest fine issued to date by the Information Commissioner's Office for a data breach. The breach occurred when hard drives — containing highly sensitive personal data belonging to tens of thousands of patients and staff — which were scheduled to be destroyed, ended up for sale on an internet auction site. The drives had not been destroyed and instead, information including national insurance numbers, home addresses, ward and hospital IDs, and information referring to criminal convictions and suspected offences, ended up in the public domain. The NHS Trust was fined £325,000 and is still unable

SECURING THE FUTURE

to provide regulators with a full account of how at least 252 of the approximate 1,000 hard drives they were supposed to destroy ended up for sale.[1]

Since that incident another NHS Trust, also in the South East of England, was fined £200,000 in July 2013 for a similar breach resulting in hard drives full of sensitive data being found for sale to the highest bidder on the internet.

It may be shocking in today's privacy-conscious climate that documents and data are still being disposed of carelessly. This newsletter sheds light on the lack of understanding among many employees around the importance of secure information destruction and the need to instill regulated practices to protect sensitive data. According to the Ponemon Institute, 40 per cent of data breaches occur as a result of negligence, making it the leading cause. These incidents, like many others, brought negative attention and scrutiny to the organisations involved, with police investigations and media coverage, all of which could have been prevented with greater employee awareness around information security.[2]

Businesses and organisations need to take more proactive measures

Implementing proper information destruction protocols that are understood and adhered to by all employees is essential in protecting against fraud, identity theft and the reputation damage that can result from a security breach. Yet the results from the 2014 Shred-it Information Security Tracker show that regardless of size, organisations are not doing enough to make document security part of their business culture. In particular, almost a third of larger companies (32%) said their employees either didn't have a protocol to refer to, they had one but not all staff were aware of it or they were not aware that one existed. Furthermore, nearly a third of SMEs (30%) said they did not have anyone in their business who was specifically responsible for managing data security issues.

There is also a worrying gap between the management discipline of putting people and protocols in place and actually making sure information is secure. In the UK, nearly a quarter of SMEs (24%) surveyed for the 2014 Shred-it Information Security Tracker admitted that they never audit their information security procedures and protocols. The equivalent figure for larger organisations was, perhaps even more surprisingly, not much better at 23 per cent. In addition, of the larger companies surveyed, less than half (48%) say they provide information security training to staff on an annual or

1 BBC, www.bbc.co.uk/news/uk-england-sussex-18293565
2 Ponemon Institue, 2014 Cost of Data Breach Global Analysis, www.ponemon.org

more frequent basis and 10 per cent provide no training at all! And there's not much improvement when it comes to document destruction processes — 24 per cent of large organisations and 41 per cent of SMEs still do not provide any secure places for sensitive documents to be stored before being put through an in-house shredding machine.

Data theft can occur when employees leave documents or electronic devices — such as old computers or memory sticks — unsecured, or dispose of them via non-secure recycling or general waste streams. Fraudsters have become increasingly determined and will retrieve confidential data through means such as looking into dustbins (often referred to as 'bin raiding') or hacking 'wiped' hard drives. This means that companies need to make sure that not only are they safely storing data, but that they are educating their employees on how best to securely dispose of it as well.

With identity theft and security breaches making headlines regularly, consumers are keenly aware of how easily personal information can be compromised and have the expectation that the organisations entrusted with their information are taking proactive measures to protect their confidential data.

How to start creating a culture of security and trust

The bulk of data breaches, whether malicious or accidental, happen internally within an organisation. As such, an information security policy is only as strong as the employees that adhere to it. As fraud and data theft continue to be a reality in today's business world, it is crucial for organisations to take proactive measures against these threats in order to maintain stakeholder trust.

When assessing whether it has effectively cultivated a culture of security within the organisation, a business should ask itself the following questions:

- Does my organisation have the facilities and resources necessary to ensure that confidential information is protected?
- Do we use a method of document and data destruction that is safe and secure?
- Are information security policies clear, easy-to-understand and effectively communicated to all employees?
- Does the company have an employee that manages information security issues and ensures that all policies are strictly followed — including regular audits?
- Are employees regularly and thoroughly trained on all data protection regulations and the importance of protecting sensitive information?
- Does the company have a shred-all policy for documents that don't need to be retained?

SECURING THE FUTURE

If the answer to any of these questions is 'no', there is a very real danger that employees will fail to understand the importance of following information security protocols, putting the businesses and their customers at serious risk of data breaches and fraud. It is the responsibility of every organisation, large and small, to take proactive steps to ensure that client and company information is adequately safeguarded. In doing so, a business protects not only its clients but also its reputation — and potentially even its very existence.

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.