SECURING THE FUTURE

In this Issue

Small Actions for Big Wins – The Information Security Checklist

It's no secret that in today's economic environment businesses have to be selective with their operational investments. Often times it seems that if a program isn't able to show an immediate increase in revenue, it's the first to be cut. This was certainly apparent when reviewing results from Shred-it's 2014 Information Security Tracker.

This year's Security Tracker suggests that more than a quarter of American businesses have no protocols for storing and disposing data. This number is alarming, especially considering new stats show the cost of a data breach is pushing the $6 million mark[1].

Overlooking information security won't save money in the long run. Often, the costs incurred from regulatory fines, litigation, fraud and most importantly, the reputational damage that can result from a data breach, far exceed the cost of implementing a simple information security protocol.

1 2014 Cost of Data Breach Study: Global Analysis, Ponemon Institute, May 2014.

SECURING THE FUTURE

For these reasons, check out the Small Actions for Big Wins Information Security Checklist. The checklist outlines the most commonly overlooked information security practices to help businesses easily and affordably protect themselves from information theft and fraud.

You can download the Small Actions for Big Wins Information Security Checklist here.

Fight Fraud by Focusing on Your Office's Most Vulnerable Areas

Many business leaders don't know that one of the biggest sources of fraud comes from within the business itself. As a result, they often overlook key areas of vulnerability.

This year, to mark International Fraud Week, we've identified the top five most vulnerable areas within an office. The goal being to set business leaders up for success, so they can easily protect themselves and their customers.

The top five most vulnerable areas include:

1) **Printers:** Many offices do not require employees to use a security code to complete a print job, which means that confidential information is frequently printed and left at printing stations. In order to mitigate this danger, businesses should mandate that employees secure their print jobs by using a security code or allow employees printing confidential information to use a printer in their own office workspace.

2) **Non-Secure Recycling Bins and Wastepaper Baskets:** Disposing data in an unsecure bin is just as risky as leaving it at a printer or on a desk. A shred-all policy eliminates the guesswork from the process and ensures that employees don't accidentally leave confidential information in unsecure locations. What's more, shredded material is still recycled when using a third party provider, but securely.

3) **Messy Desks:** Messy desks with loose paperwork are vulnerable to snooping and data theft. They also expose confidential information to external staff, such as cleaners, who have access to the office place. Consider implementing a clean desk policy and provide lockable storage units so employees can protect confidential information.

4) **IT Device Storage:** Electronic storage devices are very convenient when you can't access the company network, but they also raise the risk of fraud. Businesses can reduce the risk of fraud by requiring that storage devices be signed out and ensuring that they are securely destroyed when they reach the end of their use.

5) **Car/Homes/Hotels:** In the past, employees generally worked at the office and rested at home. With an increasingly mobile workplace, people can now access all their files remotely in many locations. While convenient, that means that confidential information may be left in areas that are unsecure. Companies should caution employees to only take or print confidential information outside the workplace when absolutely necessary and instruct them on proper secure disposal.

As Workforces Go Mobile, Data Breach Risks Increase

As businesses move to improve employee satisfaction, productivity and work-life balance, there has been a significant shift towards remote working arrangements. In fact, over 30 million Americans work from a home office at least once a week[2].

While many employers recognize the positive effects of a flexible work program, business leaders should be aware that this trend could have adverse effects on information security. Organizations need to be wary of allowing confidential information to leave the workplace and ensure all staff are mindful of data security risks when working from home.

Implementing preventative measures specifically for remote workers will help to safeguard an organization's physical and digital assets. A well-understood information security policy, which includes remote working requirements, helps companies to address the extra risks associated with mobile working by ensuring that their information security protocol extends beyond company walls.

From encouraging staff to return confidential documents to the office for safe and secure disposal, to outlining best practice with respect to handling corporate devices such as laptops and mobiles, businesses need to provide clear rules to help employees maximize their productivity while also protecting sensitive information.

2 Telework Research Network, www.globalworkplaceanalytics.com

SECURING THE FUTURE

For tips on the mobile workforce, please visit the Shred-it Resource Center for more information. You can also stay informed with Shred-it on Facebook and LinkedIn or follow us on Twitter @Shredit.

Data Breach Roundup

Our pick of recent high profile data breaches and their impacts:

Staples – Staples recently confirmed that the retailer is investigating a potential breach, but no details are available as to how many stores have been impacted. According to reports, multiple banks had identified a pattern of credit and debit card fraud, suggesting that several Staples locations were experiencing a data breach.[3]

Sourcebooks – In an ironic turn of events, Brian Krebs reported that Sourcebook, the publisher for his upcoming book on cybercrime, Spam Nation, suffered a data breach. According to the publisher disclosure letter on the California Attorney General's website, the breach occurred through a vulnerability in the company's shopping cart software. April through June 2014, the credit card numbers, billing information, and some account passwords were compromised for more than 5,000 shoppers.[4]

Penn Highlands Brookville – A Pennsylvania hospital has confirmed that approximately 4,500 patients may have been impacted in a potential data breach. A third party vendor, which held the patient records, was hacked. As a result, patient names, addresses, dates of birth, driver's license numbers, social security numbers, phone numbers, insurance information, medical information, and gender may have been compromised. As a precaution, the hospital is notifying patients of the recent hack until they can confirm the extent of the breach.[5]

About Shred-it

Shred-it is a world-leading information security company providing information destruction services that ensure the security and integrity of our clients' private information. The company operates in 170 markets throughout 18 countries worldwide, servicing more than 300,000 global, national and local businesses. For more information, please visit shredit.com

3,4 & 5 Kate Vinton, "Data Breach Bulletin: Staples, NeedMyTranscript, iCloud, Sourcebooks", October 2014, www.forbes.com