SECURING THE FUTURE

In this Issue

State of the Industry Report

Privacy and data breaches continue to dominate the headlines of major newspapers as organizations, big and small, fall victim to both malicious crimes and unfortunate mistakes. With a focus on protecting the confidential information of employees, customers and their organization, business leaders no longer consider information security policies and procedures a “should”, but rather a “must”.

As new threats to data security emerge, governments consistently revise and develop new regulations to protect personal information. With so much in flux, organizations can struggle to meet information security requirements, especially in tightly-regulated sectors such as healthcare and financial services, where privacy protection requirements are exceptionally stringent.

While the 2015 Shred-it Information Security Tracker survey found that more organizations are becoming aware of their current obligations and requirements to securely protect their data, it also saw that awareness does not always translate into action.

According to the Security Tracker, 90 percent of C-suite executives and 79 percent of small business owners are aware of the legal requirements for storing, keeping or disposing of confidential data in their industry.

SECURING THE FUTURE

However, a shocking 37 percent of small business owners reported having no protocol in place for the secure destruction of confidential information. The gap between large organizations and small businesses was even wider on cybersecurity policies with 85 percent of C-suites reporting having such a policy, while only 35 percent of small business owners do.

Without the proper information security protocols and policies in place, organizations are not only risking the personal and confidential information of their customers and employees, but increasing their chances of financial loss, reputational damage and legal repercussions. As such, organizations should develop comprehensive policies that are aligned with legislative requirements and aimed at protecting sensitive data in all forms, starting from collection through storage and into destruction.

To get the facts about current security views, risk factors and prevention strategies in this year's State of the Industry report please visit the Shred-it Resource Center to download the full report.

Small Businesses Risk Reputation by Ignoring Information Security Threats

Information security policies and procedures play an important part in protecting small businesses from the risk of a data breach, yet the most recent Shred-it Security Tracker shows that US small businesses lag behind in terms of taking action.

While 63 percent of C-suite executives say that they have protocols in place for the storage and disposal of data that are **strictly** adhered to by all employees, only 46 percent of small businesses say the same. Even more troubling is the fact that 37 percent of small business owners admit to having no protocol in place at all, and for those who do, 40 percent never train employees in correct implementation.

Planning and implementing a comprehensive information security protocol can be a challenge for businesses with limited resources — they often don't know how to protect their data or they think it's too expensive and time consuming to do so. But for small businesses the alternative is much worse.

According to the Ponemon Institute the average cost of a data breach is almost $6 million — far more than any small business is equipped to absorb.[1] Even if a breach doesn't end up being financially ruinous or legally damaging it can erode a business' reputation and the confidence of its customers. For small businesses, which are built on relationships and trust, one information security breach can drive consumers away.

Luckily for small businesses, there are some simple and easy-to-implement ways that will educate employees and help protect data in their organizations. Shred-it is helping small business

SECURING THE FUTURE

owners with convenient and executable tips for employees. To download Shred-it's Helpful Reminders please visit the Shred-it Resource Center:

- Printing Station: Confidential documents left at printing stations are vulnerable to snooping and can increase your security risks. Remind employees to ask themselves "Do you have all your printed material?"
- Unsecure Bins: Disposing information in unsecure bins increases your organization's risk of fraud. Securely shred all documents to eliminate guesswork and still ensure your paper is recycled. Remind employees "Stop! That should be shredded."
- Unused Hardware: Securely destroying hardware that has outlived its usefulness is the only way to ensure that the data on them is completely gone. Remind employees "Don't delete. Destroy!"
- Storage: Locking storage units and filing cabinets prevents unauthorized access to confidential information and helps decrease the risk of fraud. Remind employees "Don't forget to lock up."

Data Breach Roundup

The first step in fixing a problem is knowing that it exists. In each edition we feature a high profile data breach to show businesses how they can mitigate similar risks.

This quarter we're featuring Community Catalysts of California, Inc.

Community Catalysts of California, Inc., a not-for-profit organization who provides services and advocacy for people with disabilities and Veterans, learned that an unencrypted USB that may have contained client information was recently stolen from an employee's residence. It is suspected that the stolen USB included names, addresses, diagnoses, date of birth, age, gender and/or telephone numbers for numerous current and former clients. No driver's license, state identification, health insurance or financial account numbers were exposed.

What can you do: While USBs and other removable media, such as laptops or external hard drives, are convenient for their size and portability, they can create significant security risks if not managed properly. According to the 2015 Shred-it Security Tracker, 37 percent of US businesses surveyed have never disposed of hard drives, USBs and other hardware containing confidential information.[2] Considering how easily these portable devices can be lost or stolen, that translates into a lot of confidential data that could potentially fall into the wrong hands.

It is important that business leaders ensure their commitment to information security extends beyond printed material to include cyber security and the disposal of e-media and hard drives. As such, there are guidelines designed to safeguard the confidential information found on devices around the office:

- Perform regular clean-ups of storage facilities to avoid stockpiling unused hard drives.
- Sign out all electronic storage devices, especially if they contain confidential data, to ensure they are being tracked at all times and never left for a passer-by to easily pick up.
- Ensure employees lock their laptop to the desk and remember to lock their screen when they leave their desk.
- Engage a third-party provider to destroy all unused hard drives including old laptops, smartphones, tablets and USBs.
- Encrypt smartphones, tablets, external memory drives and laptops to ensure data remains secure even if the device is lost or stolen.

SECURING THE FUTURE

Customer Connections

In each edition we highlight a Shred-it Associate who went above and beyond to provide exceptional customer service.

Jerame Henderson, CISP
Customer Security Representative, Shred-it, Boise

Jerame Henderson has a reputation amongst his colleagues and customers for going above and beyond to provide not only high quality service but solution-driven results. Joining the Shred-it team over a year ago following the merger with Cintas, Jerame displays an uncanny ability to recognize risks to his customers' confidential data, including problematic placement of containers or improper storage of documents. With the goal of making his customers happy, Jerame provides strategic solutions and advice to highlight potential risk areas for fraud.

> *"When Jerame offers advice on a solution to his customers, they seem to jump to follow his lead. No CSR at my branch has more great comments from his customers for helping them add containers or increase security than Jerame!"*
>
> — Shaun Kirkham,
> Operations Manager, Shred-it Boise

Jerame credits the other CSRs and supervisors in his area for providing him the necessary resources to help his customers. "With open lines of communication, I know I can always call on my supervisors or other CSRs to advise me on the best solution for my customers."

Jerame's long-time knowledge of the document destruction industry has served him and his customers well. Shred-it commends him on his work ethic, drive to get the job done and his ability to speak to customers.

For more tips on improving information security, please visit the Shred-it Resource Center at shredit.com/resource-center

You can also stay informed with Shred-it on Facebook and LinkedIn or you can follow us on Twitter at @Shredit

---

1. Ponemon Institute LLC/IBM, 2015, *Cost of a Data Breach Study: United States*
2. Ipsos Public Affairs/Shred-it, 2015, *Shred-it's 5th Annual Security Tracker: C-Suite Executives Lead the Information Security Race in America*