SECURING THE FUTURE

In this Issue

- Businesses should avoid making these common mistakes
- Staying aware of scams
- Data breach roundup
- Customer connections

Businesses Should Avoid Making These Common Mistakes

The first step in improving information security is conducting a thorough assessment of the vulnerabilities in your business. However, according to the 2014 Shred-it Information Security Tracker, **one in five organizations in the United States** have never audited their company's protocols for storing and disposing of confidential information.[1]

Take a close look at your organization's current information security procedures so you can identify any potential mistakes and take concrete action to lower your risk.

Here are the top ten mistakes businesses make:

1. **Allow non-secure recycling bins and wastepaper baskets:** Disposing of information 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 of what is and isn't confidential from the process and ensures that employees don't accidentally leave confidential information in unsecure bins.

SECURING THE FUTURE

2. **Allow employees to leave documents on their desks or in unlocked filing cabinets:** Without a clear desk policy or lockable storage units for employees to protect confidential information, any paperwork is vulnerable to snooping and data theft, and available to outside staff such as cleaners and building maintenance.

3. **Don't secure 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. Also, businesses often overlook physically destroying hard drives on printers at the end of their use, not realizing that the information that's been printed is stored in the printer's memory.

4. **Allow employees to remove confidential information from the office:** With an increasingly mobile workplace, people take their work home with them. 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.

5. **Allow employees to use personal smartphones without reviewing security measures:** Smartphones allow employees to work from almost anywhere. They also allow another point of access to potentially confidential material. If your company doesn't require the use of passwords (at a minimum) or encryption as part of your cyber security plan, the risk of a data breach increases.

6. **Don't properly manage IT devices:** 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.

7. **Use whiteboards for team projects without clearing them:** A collaborative workplace can result in increased productivity and innovative thinking. However confidential information left on whiteboards can increase an organization's security risks as the information is available in common areas for any passerby to see. It's important to ensure policies extend to the clearing of whiteboards to ensure information doesn't fall into the wrong hands.

8. **Allow password sharing on shared accounts without clear transition policies:** Using a shared online account between multiple employees is convenient and can limit the number of accounts in use. However, using a common password that multiple people know increases vulnerability, especially when an employee leaves the company.

9. **Don't train your employees:** The best information security policy is the one that employees follow. If employees don't understand how or why to follow a policy, it's pretty much dead on arrival. By investing the time in helping employees follow the rules, your company is investing in real security.

10. **Revisit and assess existing policies:** As organizations change and grow, so do their information security risks. While many business leaders will include risk assessments of new programs at the onset of implementation, it is important to regularly revisit security policies and procedures to ensure they reflect the realities of a constantly changing business.

SECURING THE FUTURE

Staying Aware of Scams

Every year Americans lose billions of dollars to online, mail, door-to-door and telephone scams.[2] This type of fraud can cause devastating damage to businesses. It's important to stay informed so you can recognize these scams and protect confidential information.

Small businesses are often targeted by unauthorized directory listings or advertising fraud in an attempt to bill the organization for an advertisement or directory listing which does not exist. The organization is deceived by a fake quote based on a genuine entry or advertisement the business has had in a different publication or directory.

As a small business owner you can protect yourself by:

- Ensuring that employees processing invoices or answering calls are aware of these scams.
- Always checking that goods or services were both ordered and delivered before paying an invoice.
- Never giving out or updating any information about your business unless you know what the information will be used for.
- Not agreeing to a business proposal over the phone – always ask for an offer in writing.
- Limiting the number of employees who have access to funds and have the authority to approve purchases.

Data Breach Roundup

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

This quarter we're highlighting:

Book2Park.com:

Book2Park.com is an online parking reservation service for airports across the United States. According to sources, they appear to be the latest victim of the cybercriminal group who stole more than a 100 million credit and debit cards from Target and Home Depot. Book2park.com is the third online parking service since December 2014 to fall victim to this group.

What you can do:

Cybercrime continues to be one of the biggest threats to businesses, however according to the 4th Annual Shred-it Security Tracker, 57 percent of American organizations reported having no cyber security policy in place. It is important for business leaders to ensure their information security protocols extend to include cyber security and the disposal of e-media and hard drives. Erasing hard drives does not mean data is destroyed. Physical hard drive destruction is proven to be the only 100 percent secure way to destroy data from hard drives.

SECURING THE FUTURE

Customer Connections

Shred-it's most important relationship is with its customers, which is why Shred-it Partners are trained to provide top level customer service and expertise. In each edition we highlight a Shred-it Partner that went above and beyond to provide exceptional customer service.

Celso Cantu
Customer Security Representative, Tampa, Florida

For Celso Cantu being a Customer Security Representative means more than securely destroying documents, it means being dedicated to helping customers maintain their overall information security practices.

Celso demonstrates this commitment by being available on each customer visit to answer any questions they may have and always keeps an eye out for hard drives, CDs or other old electronic devices that need to be destroyed. Before leaving his small business customers, Celso takes the time to touch base with each employee, helping them check their recycling bins to make sure they have no additional confidential documents which need to be destroyed.

> *"Celso is not only professional, but also courteous when he services our account. He is never disruptive and everyone in the office loves him."*

Shred-it would like to commend Celso for going above and beyond for his customers by taking an active role in helping decrease their exposure to fraud.

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 follow us on Twitter at @Shredit

1 Ipsos Reid, 2014 Security Information Tracker
2 Yahoo News 2014, Phone scams cost Americans $8.6 billion last year – here's how to protect yourself