SECURING THE FUTURE

In this Issue

American Businesses are Deprioritizing Information Security

In this issue, we will discuss how American organizations continue to be complacent about information security.

It's no secret that the improper disclosure of confidential information is risky and can cause damage to corporate reputations. In today's business climate, savvy business leaders know it simply makes good business sense to arm employees with tools and resources to safely manage information.

Shred-it's 4th Annual Information Security Tracker shows business leaders are taking little to no action to make information security a priority. In fact, the study shows that in some instances, information security policies have actually decreased. Considering the fact that Americans are more aware of their information security risks than ever before, it's clear more needs to be done to motivate business leaders to take action.

According to the annual study conducted by Ipsos Reid:

- Only 47 percent of US small business owners have an information security protocol that is strictly adhered to by all employees, and 31 percent admit to having no protocol in place at all.
- It's not only small business owners. One in five c-suite executives reported they have never performed a security audit and 15 percent admit to never training their staff on information security, a number which has risen significantly since last year.

SECURING THE FUTURE

When you consider that the average cost of a data breach is nearly $6 million, there is plenty of cause for concern. Organizations need to take more responsibility in safeguarding confidential information not only for their stakeholders, but also for their corporate livelihoods.

Are you doing enough?
To take control and properly manage your confidential data, keep the following suggestions in mind:

- Demonstrate a top-down commitment from management to the total security of your business and customer information.
- Implement formal information security policies; train your employees to know the policies and strictly follow them.
- Eliminate potential risk by introducing a "shred-all" policy; remove the decision-making process regarding what is and isn't confidential.
- Conduct a periodic information security audit.
- Introduce special locked containers instead of traditional recycling bins for disposing of confidential documents.
- Don't overlook hard drives on computers or photocopiers. 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.

Data breaches like the one that recently affected Target, compromising up to 70 million credit and debit cards, show that today, more than ever before, organizations need to prioritize information security and implement protocols to help protect confidential documents and hardware.[1]

Mind the gap

The gap between policy and practice leads to weakness in information security.

Imagine what would happen to your organization if you lost customer information, including credit and debit card numbers for millions of Americans? For Home Depot that scenario has become reality as security experts are reporting a massive theft of confidential information that may be linked to the retail giant.[2]

1 Target Corporate 2014, Data breach FAQ
2 Krebs on Security 2014, Banks: Credit Card Breach at Home Depot

SECURING THE FUTURE

According to investigators, customer data may have been stolen from nearly all of Home Depot's 2,200 stores in the United States. While authorities have yet to confirm or deny that Home Depot is the responsible party, the company has since moved quickly to calm customers' worries by offering credit monitoring services to those potentially affected by the breach.[3]

Quick corrective measures, such as the ones taken by Home Depot, are appropriate considering the issue at hand. When you consider that companies are digitally attacked an average of 16,856 times a year, it should be no surprise to smart business leaders that they need to take proactive steps to prevent breaches from occurring in the first place.[4]

Online attacks are not the only threat to an organization's information security. Businesses must ensure all data is secure, including hard drives and physical documents. As recently as June of this year, an employee at a Georgian law firm lost a hard drive containing names, social security numbers and other personal information when it was stolen from the trunk of his car.[5] While details of this data loss were not shared publicly, one can well imagine the impact to the firm's reputation and revenue.

Shred-it's 4th Annual Security Tracker revealed that 60 percent of US small business owners and 30 percent of c-suite executives have no policy in place for destroying digital assets. The study also revealed that almost half of the small business owners surveyed had never disposed of hardware containing confidential information. It is clear more needs to be done. American businesses need to prioritize information security, and they need to start as soon as possible.[6]

Three simple workplace guidelines are designed to safeguard hard drives:

- Perform a regular cleaning of storage facilities and avoid stockpiling unused hard drives.
- Destroy all unused hard drives using a third-party provider who has a secure chain of custody to help give you peace of mind and ensure your data is being kept out of the hands of fraudsters.
- Regularly review your organization's information security policy to incorporate new and emerging forms of electronic media.

3 Reuters 2014, Home Depot in contact with Secret Service over alleged breach: source
4 IBM 2014, 1.5 million Monitored cyber attacks in the United States in 2013
5 OAG.ca.gov 2014, Imhoff & Associates theft letter
6 Ipsos Reid, 2014 Security Information Tracker

SECURING THE FUTURE

What types of electronic media can be destroyed?

- Hard Drive (any kind of laptop, desktop, PATA, SATA and many more).
- Backup Magnetic Tapes (any kind of DLT, mini cartridges and many more).
- Floppy Disk (3.5 inch disk, 5.25 inch disks, and many more).
- Zip Disk (100 MB, 250 MB, and other large disks).
- Optical Media (CDs, DVDs, Blue Ray, and HD DVD).

What should your company do in the wake of a data breach?

If your organization experiences a data breach, there are a few important steps that should be taken immediately:

- Seek expert legal assistance and advice.
- Take inventory of the data that has been impacted.
- Develop a targeted plan of action that includes clearly-defined steps.
- Carefully manage the flow of information related to the breach.
- Be prepared to communicate effectively to all stakeholders, including customers, partners, vendors, employees and the media.

Quick corrective measures are essential, but it is also critical for companies to take proactive steps to prevent further breaches from occurring.

Contact Shred-it for a FREE security consultation

For more information on successfully implementing an information security program in your organization, 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.