SECURING THE FUTURE

In this Issue

The Future of Data and Document Security: What you need to know today, to plan for the future

In this issue we will discuss business security trends for 2013, and in light of these trends, how businesses can protect themselves from data breaches.With every passing year the traditional office continues to evolve, and so do business security issues. As we start a new year, now is the time to look at some of the latest business security trend predictions for 2013.

In this issue you will find suggestions on how you can do a better job at protecting your confidential information and reputation.

Trend #1: Cyber Crimes will grow

Hacking. Phishing. Worms. Malware. Botnets. Viruses. Cyberstalking. Identity Theft. Computer crimes are here to stay, and will continue to be a 'growth industry' for 2013 and beyond. Not only can businesses be impacted financially if attacked, but their brand image can suffer, consumer trust can diminish and they can be held liable for leaked data. For instance, the Ponemon Institute issued their 2012 Cost of Cyber Crime Study which revealed that the median annualized cost of cybercrime is $8.9 million per year[1]. In 2011 the cost was $8.4 million, representing an increase of 6% in year-over-year. It goes without saying that the year 2013 may see a rise in high-profile hacking of businesses and government organizations along with spyware and malware mutations targeting smartphones and tablets.

1 http://www.ponemon.org/local/upload/file/2012_US_Cost_of_Cyber_Crime_Study_FINAL6%20.pdf

SECURING THE FUTURE

With technology moving forward at breakneck speed, companies are constantly upgrading their computer hardware and devices and recycling, selling, donating or simply discarding hardware that is considered to be obsolete. Because of this trend, the proper disposal of aging and obsolete hardware is of both national and global concern. When hardware is not properly disposed of and confidential company/client information is left vulnerable to recovery, the company's reputation is put in jeopardy, business bottom lines are at risk and inevitably IT professionals' jobs are put in danger.

Businesses and IT managers need to know that erasing, reformatting, wiping and degaussing (or erasure) of electronics documents from a hard drive or a USB stick doesn't mean information is gone forever – in the end corporate data can still be recovered. The only 100% secure way to erase information is to safely and securely destroy the hardware/media itself. The best way to ensure that no one can restore confidential data and essentially hack into private client and company information is to physically destroy any obsolete eMedia by crushing it, rendering such things as old hard drives, memory sticks and photocopier memories completely useless and beyond repair.

Back to the Top

SECURING THE FUTURE

Trend #2: Cloud Computing Security Yet to be Proven

As more companies move their private data into the cloud, security issues may arise namely around data privacy and security.

Many countries have specific laws that state data on citizens must be held domestically. With cloud computing, that data could reside anywhere and the customer might not have any idea where, in a geographical sense, that actually is. In the U.S., companies can choose to adhere to the Safe Harbor Principles, a directive designed to harmonize with the European Union Directive 95/46/EC to protect consumer data. However, because this is not a mandate set forth by the government, and companies decide for themselves if they wish to opt in, businesses need to take care to protect both their employees and their customers' data.

On the security front, businesses are understand-ably concerned about the risks associated with corporate data being housed in the cloud. When control over data security is relinquished to a third party, it can be difficult to ensure data is managed properly. It can also be a challenge to fully know who has access to the servers and if your company's obsolete electronic data is being properly destroyed. It's critical that business practices and risk management policies are not ignored when working with third-party vendors for cloud storage and database management requirements.

According to a recent study by the Ponemon Institute, 39% of business and IT managers believe cloud adoption has decreased their companies' security posture[2]. Before considering cloud computing, business leaders and IT managers need to ask tough questions and consider getting a security assessment from a neutral third party before committing to a cloud vendor.

Back to the Top

2 http://www.ponemon.org/local/upload/file/Encryption_in_the_Cloud%20FINAL_6_2.pdf

SECURING THE FUTURE

Trend # 3 – A Growing Mobile Workforce Means an Increase in Security Threats

The advent of new technologies is making it easier for employees to be located just about anywhere. In fact, according to a recent IDC study, it is estimated that the worldwide mobile worker population will grow to 1.3 billion in 2015, accounting for 37.2% of the workforce[3].

Unfortunately for IT professionals, an increase in the mobile worker population means an increase in security threats. While devices like smartphones and tablets enable employees to access information on the go, these portable devices are also more susceptible to viruses and can fall into the wrong hands while workers are on the move, thus placing the company at risk of an electronic data breach. Furthermore, the concept of a paperless office (mobile or not) is not part of the reality of the working world.

With mobility rapidly evolving, the U.S. government has yet to institute any regulations around the secure transmission of data via mobile technologies. Thus, mobile workers are still printing out confidential documents and may not necessarily be abiding by their company's secure document destruction policies once these documents are no longer needed, putting the company at risk of a breach.

As the trend of an untethered office continues to grow, companies need to update and adapt both their electronic data and paper document security and destruction policies. As best practices go, here are some protocols to consider for both electronic data and paper document security:

3 http://cdn.idc.asia/files/5a8911ab-4c6d-47b3-8a04-01147c3ce06d.pdf

SECURING THE FUTURE

To protect the mobile worker from an electronic breach, practice the following:

- Ensure laptops are regularly scanned for infections and equipped with up-to-date security levels.
- Ensure acceptable usage policies are being implemented by blocking inappropriate content, excessive downloads and risky web sites.
- Protect electronic interactions including email, web communications, and instant messaging.
- Secure interactions regardless of whether employees are accessing company resources from Wi-Fi hotspots, their homes or anywhere else.
- Ensure that obsolete mobile devices (whether laptops, smartphones or tablets) are properly disposed of so that confidential information cannot be recovered. Erasing hard drives does not mean that data is gone. Physical hard drive destruction is only proven to be the only 100% secure way to destroy data from hard drives.

To stop mobile workers from intentionally or unintentionally facilitating a paper document breach, practice the following:

- Introduce a "shred-all" policy. That means all unneeded documents are fully destroyed on a regular basis.
- Train your employees on your security policies. Implementing policies and procedures is one thing, but it is also important that all employees are aware of the information destruction procedures and trained on a regular basis.
- Continue to assess your company's level of risk. Conduct a periodic information security audit of your mobile workers' habits and practices of storing and destroying information.
- Hire a reliable vendor that is well-informed and keeps you compliant with pertinent legislation, training requirements etc. Make this vendor's services available to your mobile workforce. Finding a vendor that provides you with a certificate of destruction upon completion is ideal.

By taking such steps and regularly reviewing security policies, organizations with a mobile workforce can protect themselves from the significant long-term impact of a data breach. If staff are not aware that there are policies and procedures in place, mistakes may occur, which could prove potentially fatal to the future of the business.

Back to the Top

SECURING THE FUTURE

Your FREE Security Consultation

Shred-it has developed an online survey to help businesses better understand security gaps, conduct your own security self-assessment

Learn more about Shred-it services or book your FREE security assessment

You can also visit Shred-it on LinkedIn, Facebook or follow us on Twitter.

Back to the Top

About Shred-it

Shred-it is a world-leading information security company providing document destruction services that ensure the security and integrity of our customers' private information. The company operates 140 branches in 16 countries worldwide, servicing over 150,000 global, national and local businesses, including the world's top intelligence and security agencies, more than 500 police forces, 1,500 hospitals, 8,500 bank branches and 1,200 universities and colleges.