

SECURING THE FUTURE

In this Issue

- Trend #1: Cyber crimes will grow
- Trend #2: Cloud computing security yet to be proven
- Trend #3: A growing mobile workforce means an increase in security threats
- Request your free security consultation



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 2012, 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 2012. 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 2012 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. The year 2012 may see a rise in high-profile hacking of businesses and government organisations along with spyware and malware mutations targeting smartphones and tablets.

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. A recent survey estimated that British businesses and households are throwing away a staggering



SECURING THE FUTURE

15.1 million gigabytes of data a year on old computers. 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 per cent 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.



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.

For data privacy, many countries have specific laws that say 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.

On the security front, businesses are understandably concerned about the risks associated with corporate data being housed on 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, only one-third of IT security and compliance executives surveyed think cloud infrastructure environments are as secure as on-premise data centres. 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.

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 1.19 billion in 2013, accounting for 34.9 per cent of the workforce.

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. 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:



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 the only 100 per cent 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 with regard to storing and destroying information.
- Hire a reliable document destruction vendor that is well-informed and keeps you compliant with pertinent legislation and training requirements. 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, organisations 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.



SECURING THE FUTURE

Your FREE Security Consultation

Shred-it has recently launched a new mini guide to risk management in information security, disposal and compliance. Read the mini guide to [risk management](#) today.

Learn more about [Shred-it services](#) or book your [FREE security assessment](#).



About Shred-it

In the UK alone, Shred-it has 16 branches, employs over 400 people and operates over 120 shredding trucks, providing the most secure and trustworthy data destruction services possible for its customers. Shred-it UK has customers which span the sectors, from government agencies to financial and legal institutions, taking each customer's unique needs into account and bringing secure on site document destruction services direct to their door, thus ensuring total confidentiality in security and shredding. Shred-it is a world-leading document destruction company that ensures 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 and more than 500 police forces, 1,500 hospitals, 8,500 bank branches and 1,200 universities and colleges.

To learn more about Shred-it, contact us on 0800 197 1164 or visit our [website](#).

