Best Practices in Business: Electronic Threat Prevention

Shred Nations | @ShredNations

Table of Contents

Introduction

Since the later part of the 20th century, electronic information and technologies have been implemented in company document management systems with increasing speeds.

Hailed for being an answer to age-old requests for a cost-efficient way to help increase the efficiency of day-to-day tasks, the benefits to electronic data and documents stretch onward—ranging from cutting storage costs to boosting employee productivity and time management.

Despite this, with the number of information security risks—including fraud and corporate espionage—now being joined with newly adapted electronic threats to target digital information and devices, it's more important than ever that businesses take their security seriously if they want to truly benefit from the advantages of electronic information.

In order to better target electronic information, identity thieves, fraudsters, and criminals of all kinds are updating their tactics to better prey on their unsuspecting victims.

Without the proper preparation and protection, their next victim could be you—but at Shred Nations, it's our goal and priority to keep that from happening.

With this in-depth white paper, we take you through the full process of protecting your information from electronic threats, providing information ranging from the most common threats today to the information you need to protect—as well as how to do it using services like hard drive shredding and electronic media destruction.

Assessing Your Risk: Common Electronic Threats

While there are many benefits to efficiency and productivity in a world that is constantly gravitating closer toward electronics and away from traditional paper, a change of this significance does still come with some new drawbacks—or in this case, threats.

Information security risks have long been an issue for individuals and businesses alike to grapple with, however by today's technological standards, age-old threats like corporate espionage, fraud, and identity theft have taken a new shape.

Here is an overview of just a few of the newly-evolving electronic threats to businesses today:

Identity Theft

Much as its name implies, identity theft involves someone assuming the identity of another person in order to access their accounts, obtain credit, or collect other benefits in that individual's name.

Identity thieves usually target the personally identifiable information (PII) of their targets, which includes:

- Full Name
- Home Address
- Email Address
- Credit Card Numbers
- Social Security Number
- Biometric Information (fingerprints, etc.)
- Driver's License Number
- Vehicle Registration
- Date of Birth
- Phone Number

Although the PII of victims has always been the objective of identity thieves, improving electronic technologies has unfortunately made the potential accessibility of this confidential information even greater.

With the amount of information stored online today, it only takes a single data breach to potentially expose a wealth of personally identifiable information.

In 2016 for instance, social-networking platform LinkedIn lost a whopping 167 million account credentials in a data breach after a hacker compromised their site—drawing attention to the importance for businesses to ensure that their electronic information is securely managed from the time it is created and stored all the way up through its eventual destruction.

Fraud

With a history extending long before electronic information and documents were commonplace in the business world, fraud has been used to deceive, gain unlawful or unfair advantage, or to induce unknowing individuals to part with some valuable items or surrender a legal right.

Although traditional forms of fraud were made up by classics like scam telemarketers and Nigerian letter fraud, today electronic fraud attempts have adapted and evolved to keep up with technology.

After personally identifiable information like an individual's phone number has been leaked in a data breach like LinkedIn's in 2016 or Facebook's similar fate in 2012, fraudsters will now call a person's home or cell phone using software to mask their caller ID and help them appear more recognizable to victims.

Besides just updating traditional forms of fraud to meet current technological standards however, attackers have also adopted new strategies for coercing unwary individuals into forking over their information.

While modern electronic technologies have been rapidly developed and introduced into American business and everyday life, the speed with which users have embraced technology has moved somewhat slower.

As a result, fraudsters are also able to fool their victims by mimicking many of the everyday websites or applications people use. By creating a mirror image of sites like Facebook, the attacker can trick the individual into entering their login information into the fake site, where they will then take this sensitive information and use it for other malicious purposes.

Corporate Espionage

"Can you tell me what the competition is planning in the next quarter?"

Although it isn't quite the same sort of surveillance that James Bond used, corporate espionage still does involve some degree of spy tactics.

Rather than targeting the PII of individual victims, corporate espionage entails the oftentimes illegal act of companies using surveillance to steal trade secrets and gain leverage over other business competitors.

Here is a list of some of the information most commonly targeted by corporate espionage:

- **Intellectual Property** – Including Ideas, Techniques, Processes, Recipes, Formulas, and Industrial Manufacturing Practices.
- **Proprietary and Operational Information** – Such as Customer Datasets, Changing Compositions / Production Locations, Pricing, Planning & Marketing Strategies, Policies, and Research.

In order to acquire this confidential information from targeted businesses, companies using corporate espionage tactics have updated their methods to hone in on increasing volumes of electronic information.

For one particularly serious example of modern corporate espionage, in 2015 the security vendor Kaspersky Lab's systems were infiltrated and compromised by the Duqu 2 espionage malware.

What made this specific espionage attack so worrying to experts was the fact that it was a direct attack against a private security company from a nation-state attacker.

According to intelligence analysts from the security firm Symantec, the conclusion to be drawn from this is that corporate espionage is no longer just being used for the purposes of personal gain—it is now being used to illegally undermine and gain insight on the electronic securities currently in place to protect internet users and customers.

Consequently, this unfortunate development for corporate espionage and other electronic threats means that for businesses, the importance of keeping up-to-date on current security trends and technologies is all the more critical if they hope to keep themselves from falling victim to these threats themselves.

Information Needing Protection—and How to Do It

Regardless of the type of electronic threat you are trying to combat, fraud, identity theft, and corporate espionage attacks will typically target either the personally identifiable information of an individual or the confidential and potentially proprietary information of a business.

In order to protect this important information that is intrinsic to daily lives and business operations alike, companies are strongly encouraged to take all preventative steps possible so that they are prepared ***before*** disaster has the chance to strike.

The following are some of the best strategies for protecting yourself from external threats both externally and internally:

Protecting Electronic Information from External Risks

Because one of the largest contributing factors to data breaches and other electronic threats is documents being stolen or improperly disposed, it’s important that businesses try to close all gaps in their securities in order to keep external threats outside where they belong.

When hiring new employees, be sure to take all steps necessary to ensure that potential candidates have a clean background. Although no one can foresee the future without a crystal ball, you can still use this opportunity to look for any and all signs that may indicate an employee would abuse company information.

Also, when setting up accessibility and authorizations for individual employees in the company, try to limit access to sensitive information as much as possible without limiting efficiency. This is always a good backup plan to keep in place, as the less people who have access, the less likely the information can be stolen or misused.

For a final precaution, a business can also take the steps to encrypt their electronic information. This way, no matter whether your documents are misplaced or fall into the wrong hands, they are still rendered useless to anyone without the proper authorization and decryption key.

Protecting Electronic Information from Internal Threats

As the saying goes, knowledge equals power, and the same is true when it comes to safeguarding against electronic threats to your company's sensitive documents.

Although internal risks to electronic information can be the result of employees abusing their access to company information, by and large the majority of internal electronic threats stem from accidents caused by employees unintentionally exposing information to outside threats.

For instance, in 2013 a Minnesota health insurance exchange employee working for MNsure inadvertently disclosed the personal information of 2,400 individuals in an unencrypted email attachment.

The data breach's cause was accidental, but despite this information, security experts still draw attention to the privacy training policies in America.

While no amount of training can stop the reality that accidents happen, by keeping employees up to-date on information security best practices and the most recent victims of data breaches, you can help your own business to sidestep these potential roadblocks down the road.

Defending Against Data Breaches and Electronic Threats

Besides just being aware of risks like fraud and identity theft that threaten your electronic information today, businesses can also proactively take steps to help minimize the potential impact that these electronic threats pose.

Whether your electronic information and devices are ready for disposal and needing safe retirement, or they are still in use and could use a brush-up on their security, here are few handy tips for shoring up your electronic defenses:

Electronic Media Destruction and Equipment Retirement or Disposal

When it comes time to retire or dispose of your hard drives or other devices containing electronic media, it’s important that your business is aware of the best practices in disposing electronic information, as they tend to vary slightly from traditional paper document disposal.

Contrary to what you might initially think, simply deleting the information on an electronic device does not remove this information permanently.

Using sophisticated software, hackers and identity thieves are able to restore and recover previously deleted information to electronic devices, meaning that the only way to truly guarantee that the sensitive documents they contain has been safely removed is via absolute destruction.

At Shred Nations, our hard drive shredding and electronic media destruction services are available to help ensure that the confidential information your hard drives, CDs, DVDs, and other electronic media contains has been completely and safely destroyed.

Our trucks are equipped with top-of-the-line hard drive shredders and will conveniently make the trip to your curbside to securely dispose of any and all of your devices containing electronic information.

Once the service is complete, your shredder will provide you with a formal certificate of destruction—guaranteeing your electronic media destruction was compliant with all applicable laws and regulations.

Securing Your Network

For electronic information or equipment that is still in use, there are still steps that businesses can take to better secure themselves and protect from electronic threats.

Besides ensuring that your employees are well informed of common security threats and keeping a network firewall active to help keep malware or virus attacks at bay, companies are strongly encouraged to implement encryption technologies to additionally secure electronic information.

Although encryption will not necessarily prevent your electronic information and devices from falling into the wrong hands, encrypting this information before it is compromised renders it inaccessible and virtually useless to data thieves hoping to prey on potentially unsecured personally identifiable information.

Conclusion: Best Practices in Electronic Threat Prevention

When it comes to managing the electronic threats that endanger the sensitive information your business depends on, the best rule of thumb a company can go by is to be prepared.

No matter the cost of the precautions your business takes, the logic can be narrowed down to simply this: with the average cost of a data breach at approximately $3.8 million, implementing virtually every safeguard combined will still not compare to the price a company pays for succumbing to electronic threats.

Here are a few final guidelines and best practices to keep in mind for keeping your company protected:

- **Implement Employee Security Training –** One of the most common electronic threats from internal sources stems from a lack of employee awareness on proper security practices. From accidentally sending private or protected information to getting snared by a scam login page, it's critical to ensure your employees negotiate these threats safely.
- **Manage Accessibility to Sensitive Information –** Although there may be some red flags to warn you of an employee with potentially malicious intentions, there is no truly guaranteed way to ensure that an employee may not try to steal or misuse information. As a result, businesses are urged to stay one step ahead of potential disaster by limiting the accessibility of this information from the get-go.
- **Safely Dispose of All Electronic Information and Devices –** Another common way that businesses fall victim to electronic threats without even realizing is via identity thieves dumpster-diving for electronic devices and restoring the sensitive information they contain. To be sure that your tracks are covered all the way through the lifespan of your electronic information, it's imperative that you make use of hard drive shredding and electronic media destruction services.

Get Free, No-Obligation Quotes on Hard Drive Shredding and Electronic Media Destruction Services Near You

When managing the protections and securities your business puts in place to help safeguard information from electronic threats, there are a host of new and ever-evolving risks in a rapidly-advancing and digitally-based world.

At Shred Nations, we partner with a nationwide network of hard drive shredding and electronic media destruction specialists who are experts in helping companies to protect their information from electronic threats like malware, fraud, and identity theft. Let us help you to ensure that your company is prepared to handle these threats before disaster has the chance to strike.

For more information or to get started scheduling an electronic media destruction service for preventing electronic threats to your information, **just give Shred Nations a call at (800) 747-3365, or simply fill out the form to your right to request free hard drive shredding and electronic media destruction quotes today!**

Additional Electronic Media Destruction and Hard Drive Shredding Resources

Protecting Your Company Against Fraud and Theft

Although electronic information and technologies have brought with them a host of new threats to the sensitive documents of both individuals and businesses, it's important to not forget about the traditional risks that hard-copy documents and information have long-faced. With this in-depth white paper, we explore not just the top risks to be on the lookout for, but strategies for protecting yourself as well.

A Guide to Proper Data & Document Destruction

One of the best ways a business can go about shoring-up on its securities is by studying what *not* to do. In this guide to data and document strategies, we cover several examples of improper document destruction policies, highlighting the information that poses greatest security risks as well as providing best practices and guidelines to properly shredding and disposing of these sensitive documents.

How to Avoid a Data Breach

The threat of a data breach is an ever-growing fear for business leaders to be aware of, and in this article, we zero-in on the subject of data breaches, breaking down many of the important considerations executives are keeping in mind such as cost factors, breach causes, and most importantly, strategies for preventing a disaster striking your company.