By Megan Evans

Avoiding Corporate Theft and Protecting Electronic Data

One of a company's most important assets is its electronic data. The success of a business is directly tied to the security of its intellectual property, customer lists, and account information. In today's tech savvy world where everyone carries a mini computer in their pocket, a company's electronic data is also its most vulnerable asset. Life is so inundated with data, that we actually have unlimited data at our finger tips. While this technology makes life easier, it also makes it easier for criminals to steal your company's private data.

A company does not have to look farther than its own break room to identify possible threats. Employees are copying, transferring, and using corporate data in inappropriate and illegal ways. Sophisticated hackers are also wreaking havoc by stealing intellectual property and customer data at alarming rates. A new large-scale data breach is reported almost every week. These thefts by employees and hackers cost companies hundreds of millions of dollars and permanently damage company reputations and relationships with consumers.

How can a company avoid becoming the next victim of electronic data theft? It can begin by understanding legal requirements for storing electronic data, increasing awareness of the various threats and costs, and learning about preventive measures. No one should feel immune to corporate data theft. And while there are no simple solutions, there are many steps a company can take to decrease the likelihood of a data theft.

Where Do the Threats Come From?

A company must protect its electronic data from all angles. The most obvious threats are the most sinister: the cyber criminals and hackers seeking financial gain. These cyber-criminals utilize countless methods to invade private databases looking for customer lists, trade secrets, bank account information, and consumers' identities and credit card numbers. The years 2013 and 2014 saw a huge increase in data breaches involving millions of credit card numbers or other private customer data. The less obvious, but just as problematic, threats are employees. Employees have access to vast amounts of private corporate data, and are saving and sharing this data with competitors on a daily basis. Companies must be armed to prevent thefts from both insiders and outsiders.

▪ Megan Evans is a member of the Michigan Bar and joined Rincon Law Group in El Paso, Texas, in April 2014. Her practice is principally focused on federal court practice and she is involved in the defense of a broad range of commercial and tort claims. Ms. Evans is a member of DRI, the Federal Bar Association, and the Military Spouse J.D. Network.

Internal Threats: Employees

Employee theft is not a new phenomenon. While not all employees are as resourceful as the disgruntled programmers from the popular movie *Office Space*, a 2013 survey conducted by a forensic accounting firm, Kessler, found that 95 percent of employees steal from their employers, up from only 79 percent in 1999. That number should be alarming to even the most cynical employers. The surveyed employees admitted to falsifying their time records, pilfering office supplies, products, and services, and stealing corporate intelligence.

While employee theft is common place, electronic data theft is now easier and more prevalent than ever. Half of the companies responding to Carnegie Mellon University's Software Engineering Institution annual survey have reported at least one data security breach by an insider every year since 2004.

Employee data theft is gaining prevalence because they simply have more access to corporate information than they used to because most data is stored on networks. Companies have also taken advantage of new technology like the elusive "Cloud". The Cloud allows companies to store vast amounts of data and software easily, effectively, and in one place. While this technology has revolutionized computing, it also increased the risk of data theft. Anyone who can gain access to the Cloud has access to much more information than if the data was disbursed between different systems.

Employees also have many more options for transmitting that information to the outside world. Employees bring smartphones, iPads, flash drives, and other portable electronic devices into the workplace on a daily basis. These personal devices have immense capacities and can quickly transfer data from company devices. Employees can even snap photos of confidential data, leaving no trace of a data transfer or file share.

While some employers may encourage the use of personal devices to enable remote work, they must weigh the risks with the potential benefits. Because of constant access to personal devices, employees are stealing confidential electronic data at increasing rates. In 2013, Symantec, a cyber-security software corporation, reported that over half of employees email business documents from their workplace to personal email accounts. Forty-one percent also download the company's intellectual property to personally owned devices, and 37 percent transfer data using file sharing applications, like Google Docs, without their employers' permission.

Half of the companies responding to Carnegie Mellon University's Software Engineering Institution annual survey have reported at least one data security breach by an insider every year since 2004.

What are employees doing with this stolen data? According to the 2013 Symantec report, 40 percent of employees planned to use the stolen confidential data in their new jobs. Corporations are not only losing control of their valuable data, but it is being placed directly in the hands of their competitors. The ramifications are difficult to calculate, especially because most employee data theft isn't immediately discovered.

Employees also have nonchalant attitudes regarding data theft. According to the 2013 Symantec survey, most employees do not believe it is wrong to transfer confidential corporate data to their personal devices. Over half of the employees also do not believe that using confidential data taken from a previous employer is a crime. In fact, the top reasons employees believe it is acceptable to take corporate data include: (1) it doesn't harm the company; (2) the company doesn't strictly enforce its policies; (3) the information is generally available and not secured; and (4) the employee won't receive economic gain.

Fortunately, the 2013 Symantec report also found that most employees don't want to harm the company. Instead, employees reportedly feel a sense of ownership to any corporate data they helped create. For example, 42 percent of survey takers felt that the conduct of a software developer who re-uses source code he or she created for another company is acceptable because that employee shares ownership of the work. Most employees are just not aware of how damaging the theft of corporate data can be. To combat employee theft, companies must increase awareness that the documents employees create legally belong to their employer.

External Threats: Sophisticated Hackers

For most companies, electronic data breaches by cyber criminals are the more obvious threat, and for good reason. According to the Identity Theft Resource Center, hacking remains the top method for stealing data, accounting for more than 25 percent of all data breaches in 2013. The number of targeted hackings has even increased in recent years. According to a 2013 Symantec report, the number of targeted hackings increased 62 percent in 2013 compared to 2012, dubbing 2013 the Year of the Mega Breach.

Who are these hackers and what do they want? Most obviously, a large number of hackers steal data for their own financial gain. Others are a part of more sophisticated espionage, with ties to a foreign country, seeking to wreak havoc on the American economy and American businesses. American companies are vulnerable to both threats.

In recent years, hackers have targeted American consumers' personal financial information. A 2012 survey by the Aite Group and ACI Worldwide reported that 42 percent of Americans had experienced some kind of card fraud in the last five years. America is home to more credit cards than any other region. In 2013, there were 1.2 billion payment cards in America, nearly five cards per adult. A significant percentage of data breaches involve payment card information. According to a 2013 Identify Theft Research Center report, 15.6 percent of data breaches exposed credit or debit card information.

Where are the hackers getting this private information? Hackers are targeting American companies to gain access to their customers' identities, credit card numbers, social security numbers, and bank account information to sell on black markets. As a result, countless large American retailers have experienced major credit card breaches in the last few years, exposing millions of customers' identities and credit card numbers.

Target's 2013 holiday season credit card breach was one of the first breaches to rattle American consumers because it was the biggest retail hack in history. A group with possible ties to Russia hacked into Target's payment system, installing malware designed to steal credit card numbers from any customer shopping with a card during the busy holiday season. The stolen data was sent to a hacked server in the United States, and then forwarded to Moscow. After some investigation, Target reported in March 2014 that 40 million card numbers were stolen and an additional 70 million customers' personal information, including phone numbers and emails, was taken.

Target is far from alone. In January 2014, Neiman Marcus announced that hackers installed card stealing software in their systems, exposing around 350,000 credit card numbers. In June 2014, P.F. Chang's China Bistro reported that 33 of its restaurants' credit card processing systems were compromised. Home Depot is a more recent victim of a major credit card breach. In September 2014, Home Depot reported that 56 million credit cards may have been compromised in an attack on its payment systems, making this a larger breach than Target's.

Banks have also been targeted by hackers. In October 2014, J.P. Morgan Chase announced that 76 million households were affected by its previously disclosed summer breach, making it one of the largest breaches of 2014. So far, J.P. Morgan has concluded that the hackers did not obtain account data, but only customer contact information that can be used to send fake emails intended to lure customers into logging into imposter accounts set up by the hackers. Countless other credit card breaches affected American businesses in 2014, with no end in sight.

Large retail corporations and banks are not the only companies at risk. Hackers target companies of all sizes. Specifically, there has been a large increase in cyber-attacks against small businesses—those with fewer than 250 employees—in the last few years. According to a 2012 Symantec survey, small businesses were targeted in 31 percent of cyber-attacks, a three-fold increase since 2011. In particular, manufacturing companies have been increasingly targeted by hackers in recent years. The 2013 Symantec report found that manufacturing companies in the supply chain are hackers' new favorite targets. Contractors and subcontractors are especially vulnerable because their systems are less secure, but rife with valuable data about the larger companies that employ them. All small businesses must remember that their corporate data is just as valuable to hackers, and is often easier to access because they take fewer cyber security measures.

According to the 2013 Symantec report, 40 percent of employees planned to use the stolen confidential data in their new jobs.

Some hackers have direct ties to foreign countries, like China. The intelligence community has been warning companies for years that Chinese hackers want to steal American corporations' trade secrets, and they know what they are doing. Eric Schmidt, the executive chairman of Google, labels Chinese hackers the "most sophisticated and prolific" hackers of foreign companies. The Economist, *Smoking gun*, February 23, 2013 (print edition), http://www.economist.com/node/21572228/print. In fact, 90 percent of firms compromised by Chinese hackers in 2012 didn't even know it. The Economist, *Can you keep a secret?*, March 16, 2013 (print edition), http://www.economist.com/node/21573580/print. Fortunately, not all Chinese hackers remain undiscovered. Since 2008, 44 percent of all Economic Espionage Act (EEA) prosecutions have had a connection to China. *Id.* But, China isn't the only country looking to steal America's secrets. Hackers with ties to Russia have also been behind some of the biggest hacks of in recent years. Both the Target 2013 breach and more recent J.P. Morgan 2014 hackers may have had ties to Russia or Eastern Europe.

The Cost of Electronic Data Theft

Electronic data theft costs American companies hundreds of billions of dollars each year. The annual value of stolen corporate intellectual property in America is $300 billion, according to a survey by ASIS International (security-industry body). Other surveys estimated the loss was $1 trillion worldwide.

Large retailers have spent millions responding to credit card breaches. For example, Target spent at least $61 million dollars within two months after the breach. That number jumped to $148 million in Target's second quarter after the breach, with costs still rising. Some of the cost comes from alerting consumers of the breach, public relations damage control, legal fees, and handling potential fraud. Target set up a customer response operation and attempted to regain the trust of its customers by promising they wouldn't have to pay for fraudulent charges stemming from the breach. Target also offered a year of free credit monitoring to any customer who believed their data was compromised. Similarly, Neiman Marcus, which also experienced a breach, reported $147.2 million in net losses in its end of fiscal year report, and attributed some of those losses to the data breach.

The cost of electronic data theft cannot be measured only in the direct costs of responding to the breach. A company's reputation and relationship with its customers is invaluable, and can be severely damaged by a data breach. Resentful customers may shop elsewhere when they feel their personal and financial information is at risk. Even with millions of loyal customers, Target reported a 46 percent loss in profits compared to the previous holiday shopping period, which is the biggest decline the store had reported. Target customers took the breach very seriously, and Target's fourth quarter report reflected the hit to its reputation.

Exposure to Lawsuits and Government Actions

Data breaches also expose companies to lawsuits from customers whose data was stolen, banks, and card issuers looking to recoup costs for fraudulent charges and issuing new cards. These individual or class actions for negligent protection of data are common after a data breach. Depending on the situation, plaintiffs may also have claims for breach of contract, intentional infliction of emotion distress, deceptive trade practices, or consumer protection claims under state laws.

Well over 100 lawsuits were filed against Target by banks and customers seeking compensatory damages, which could run into the billions. Some of the federal class action negligence lawsuits allege Target did not respond quickly enough to the breach to prevent further loss, did not implement reasonable security procedures, and that the duty to detect and prevent loss of private customer information was breached. These class actions also allege violations of relevant state laws involving privacy or consumer sales practices, bailment and conversion claims, invasion of privacy and public distribution of private facts claims, and misappropriation of identity claims. Fighting negligence lawsuits can be risky for defendant companies like Target because this area of the law is still developing.

Directors and corporate officers may also be subject to shareholder derivative lawsuits looking to hold corporate leaders accountable for any failure to address cyber threats risk, loss of income, and loss of business reputation. For example, shareholders of TJX Companies, Inc. brought a 2010 derivative suit after a significant 2007 data breach where cyber criminals stole 45 million credit or debit card numbers. The lawsuit settled in 2010. After the December 2013 breach, Target shareholders also filed similar derivative actions against the directors and officers and the company itself. The shareholder lawsuits alleged breach of fiduciary duty, waste of corporate assets, gross mismanagement, and abuse of control.

Data breaches also expose companies to government enforcement action. In recent years, the Federal Trade Commission (FTC) has brought over 40 legal actions against companies for violating §5 of the Federal Trade Commission Act, which prohibits unfair or deceptive practices and acts that affect commerce. It also brought actions for violations of customer privacy under various other privacy laws. Most companies settle quickly, rather than prolong expensive fights with regulators over what actually constitutes negligent action in cybersecurity. Joshua Brustein, *Is Target To Blame for Its Data Breach? Let The Lawsuits Begin.* Bloomberg BusinessWeek, December 26, 2013, http://www.businessweek.com/articles/2013-12-26/is-target-to-blame-for-its-data-breach-let-the-lawsuits-begin.

> Hackers are targeting American companies to gain access to their customers' identities, credit card numbers, social security numbers, and bank account information to sell on black markets.

The Federal Communications Commission (FCC) has also initiated actions against communications companies. The FCC recently announced its intent to fine two telecommunications companies that failed to protect customer information by storing it on unprotected internet servers in violation of their duties under the Communications Act. Jason C. Gavejian, *FCC Issues First Data Security Fine - Federal Communications Commission*, The National Law Review, October 28, 2014, http://www.natlawreview.com/article/fcc-issues-first-data-security-fine-federal-communications-commission. The fines could reach 10 million. *Id.*

Applicable Laws and Guidelines

Data Breach Disclosure and Notification Laws

Data breaches were seldom in the news before the mid-2000s, when states began to enact breach disclosure and notification laws. California was the first state to enact the Database Protection Act in 2003, and now 46 states and the District of Columbia have similar laws requiring consumer notification when personal information is disclosed or compromised. Violations of these state laws are enforced by state attorney general action, private actions, or administrative fines depending on the state.

State notification and breach disclosure laws are similar, but vary in the details regarding the type of personal information covered, the events triggering notification obligations, and the timing and type of notification required. Some state laws require notification only to affected consumers, while others may require notification to the state attorney general. Laws also differ on method of notification, with some now requiring emails or telephone calls instead of regular mail. The state laws also define the triggering breach differently, with some requiring notification and disclosure when data is merely accessed. Others require notification only if there is a likelihood of identity theft, fraud, or economic harm. Many in the cybersecurity world have argued that a uniformly applicable federal law would help standardize the notification process, especially when it is difficult to determine which state law would apply. Congress has yet to pass a similar federal statute, though many have been proposed over the years.

While there is no equivalent federal law, in 2011, the Securities and Exchange Commission (SEC) released guidelines for public companies registered with the SEC that experience a material cyber-attack. Generally, the SEC guidelines consider the interests of investors and require disclosure of expected or incurred remediation costs, cost of increased cybersecurity measures to prevent future breaches, loss in revenue stemming from reputational damage, litigation information, and possibly information that would make investment in the company risky. Securities and Exchange Commission, Cyber Security Disclosure Guidelines, http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm. Companies must be aware of their legal obligations after a data breach.

Privacy Laws

There are countless privacy laws that protect information or impose requirements for information sharing. These privacy laws usually target specific industries. For example, the Gramm-Leach-Bliley Act (GLBA) requires financial intuitions to keep private data secure and to explain information sharing practices to their customers. Along with the GLBA, the FTC issued the Safeguards Rule, which requires financial institutions to have procedures in place to secure customer data, based on the size of the company, the nature and extent of its activities, and the type of sensitive information used. Security and disclosure of personal health information is governed by the Health Insurance Portability and Accountability Act. With the advent of electronic medical records and patient portals, health information privacy laws are more important than ever.

Other privacy laws apply generally, such as the Fair and Accurate Credit Transactions Act (FACTA) which regulates all consumer credit transactions. FACTA was designed to protect consumers from identity theft by creating requirements for information privacy, accuracy, disposal, and limits the ways consumer credit information can be shared. In part, FACTA requires free credit reports, allowance for alert messages when a consumer believes he is a victim of fraud, fraud alert notices to be clear and conspicuous, mandates truncation of credit card and debit card numbers, allowing the printing of no more than the last five digits, and also truncation of personal account numbers.

Loss Recovery and Criminal Laws for Victims of a Data Breach

The Computer Fraud and Abuse Act (CFAA) (18 U.S.C. §1030) is the most frequently used law for combating computer fraud and hacking because it criminalizes a broad range of fraudulent activities and hacking. Under the CFAA, computer fraud can include computer hacking, theft of data, theft of money, breach of data security and privacy, distribution of viruses, malware, and other denial of service attacks. Specifically, the CFAA prohibits unauthorized access of a computer, which includes any payment system or device used to store data, and obtaining financial information which causes damage and loss. 18 U.S.C. §1030(a)(2). The CFAA also prohibits transmitting codes that damage computer systems as well as conspiracies to commit computer fraud and abuse, as well as attempts to commit such conduct. 18 U.S.C. §1030(a)(5); 18 U.S.C. §1030(b). Limited civil action is also available under the CFAA if certain factors are met including a loss in any one-year period aggregating at least $ 5,000. Most recent retail hack victims would easily meet that threshold and could attempt to recover their extensive losses. However, this first requires locating the alleged hackers, which may prove difficult.

> While there is no equivalent federal law, in 2011, the Securities and Exchange Commission (SEC) released guidelines for public companies registered with the SEC that experience a material cyber-attack.

Other relevant statutes would include:

The Electronic Communications Privacy Act (ECPA) (18 U.S.C. §§2510-2521, 2701-2710) and the Wire Tap Act (WTA) (18 U.S.C. §2511) criminalize unlawful interception and disclosures or use of any wire communications including cell phones, voicemails, emails or other data sent online. These statutes would mostly apply if corporate data was specifically stolen from communications, and not just off a general server or database.

The Economic Espionage Act (EEA) (18 U.S.C. §1831-32) prosecutes both domestic and international hacking by prohibiting foreign espionage and theft of trade secrets to benefit a foreign government or entity. Section 1332 of the EEA makes it a federal crime to steal any trade secrets regardless of who benefits. The EEA is most often used to prosecute Chinese hackers, and others with ties to foreign governments.

The Identity Theft and Assumption Deterrence Act (ITADA)(18 U.S.C. §1028(a)(7)) criminalizes identity theft and prosecutes "whoever knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or otherwise promote, carry on, or facilitate any unlawful activity that constitutes a violation of federal law." 18 U.S.C. §1028. Similar to the CFAA, the ITADA also prohibits conspiracy and attempts to carry out the conduct criminalized by the Act. Retail and bank hackers who make off with names, social security numbers, bank account information, and credit card numbers can be prosecuted under this section. However, the ITADA does not create a private remedy, thus victims do not have standing to bring an action under the ITADA.

Additionally, each state has enacted some form of computer crime laws to prohibit a variety of actions that interfere with computer systems, including hacking, unauthorized access, introducing viruses and malware, and other activities that harm businesses and individuals. However, these state laws are limited and cannot address the extraterritoriality of computer crimes.

While many cyber criminals are never found or prosecuted, some serve actual time. TJX, Inc. hacker, Albert Gonzalez, was sentenced to 20 years in prison for leading a group of cybercriminals that stole more than 90 million payment card numbers from TJX and other retailers. After a long investigation, in 2014, the United States began prosecuting Russian hacker, Sasha Panin for conspiracy, computer hacking, wire and bank fraud, and money laundering. Panin is the creator of sophisticated malware software, named SpyEye, which was purchased and used by hackers all over the world to collect personal and financial information. Similar software is used in large retail hacks. If caught, cyber criminals like Gonzalez and Panin face decades in prison.

How to Detect and Prevent Data Theft: Solutions and Strategies for Companies of All Sizes

The most effective manner for companies to reduce the cost of data breaches by employees or sophisticated hackers is to prevent them. Spending time and money upfront can save millions in the long run. But, there is no magic bullet. Prevention must occur in steps and through layers of security. There is no quick fix or one-size-fits-all solution. While not all companies have extensive resources, there are strategies for companies of all sizes to effectively detect and prevent data breaches.

Prioritize Protection: After a company decides to implement information security measures, it should first identify the data that need the most protection. Companies often focus on protecting all data, instead of strategically prioritizing protection of the most sensitive information. Companies should instead focus on more protection for the most important data to get the best return on their cybersecurity investment.

Continuous Monitoring: The best way to detect and deter internal and external threats is by regular database monitoring. Data loss prevention or content management software is often the best way to track who is accessing which databases. This software can also flag unusual activity or alert employers to increased access to certain databases. It can even track when certain files or folders are opened. Some new networks' forensics software can even record digital traffic and look for suspicious patterns. These different software options can help detect leaks when they happen and discourage employees from taking unnecessary risks by sharing corporate data. This software will not alone solve all problems, but will help reduce the possibility of breaches.

Employ a Chief Information Security Officer: Assigning a trusted and well-vetted employee extra information security responsibilities is necessary. Someone must lead the charge and give other employees someone to look to for questions and concerns about information security.

Data Security Policies and Employee Training: Many companies may not have a formal policy outlining expectations for employees or anyone with access to corporate data, including contractors and subcontractors. Creating such a policy is a basic way to combat data theft. At a minimum, the policy should define expectations for the use of personal email and devices, file-sharing programs, corporate systems from remote locations, copying of data to personal devices, and any confidentiality requirements. The policy should also describe expectations for departing employees and clearly describe the types of information that should not be taken or shared by the employee.

While there is no guaranteed solution to electronic data theft, companies have many options to take control of the security of their valuable data.

Once in place, the policy must be carefully implemented by the company relative to training all employees. Employees can be the first line of defense against data theft; however the 2013 Symantec report revealed that most employees are uninformed about the ownership of corporate data. The company must explain the policy on corporate data and emphasize that it is a crime to take confidential data or use it while working for another company. This training may help thwart employees' nonchalant attitudes about data theft and decrease the chances of data theft by an insider. To be effective, the company must also be willing to enforce the policy and impose consequences against violators.

End Over-Entitlement: Employees have access to more corporate data than ever before, even if it is not essential to their jobs. Companies often give the same vast access to outsourced or temporary employees who have little loyalty to the company. A simple data theft prevention method is to tailor employees' access to their job duties. This may involve logistical changes and limiting Cloud storage, but strategically limiting access is a simple way to prevent or limit the effects of employee data theft. Companies can even purchase access control and management software that can classify data and define which employees have access.

Secure Cyber Insurance Coverage: Traditional CGL or other business interruption, employee dishonesty, or property coverage may not cover losses associated with electronic data theft by employees or hackers. Cyber insurance coverages are specifically designed to cover losses associated with responding to data theft or a data breach. Policies can cover defense costs for lawsuits arising out of the breach, regulatory investigation expenses, public relations work, computer forensics, credit monitoring, notification responses, crisis management, and media and privacy liability. Other more traditional policies like director and officers coverage or errors and omissions coverage can also be written to include data breaches.

Implement Chip and PIN Card Technology: The United States still relies on cards with magnetic strips, which are far easier targets for hackers. Other developed countries, including Britain and Canada, have adopted chip and PIN technology, which uses a personal code with a microchip, making it harder to steal data. To be most effective, this solution would need to be collectively adopted by American companies. Target's CFO has announced plans to switch to chip-and-PIN Target credit cards and payment devices. While this switch will cost Target around $100 million, it has the potential to drastically decrease the chances for a data breach.

Taking Action After a Data Breach: Detection software is not guaranteed to prevent theft. Even the best detection software won't prevent theft if the company does not act on the alerts. To minimize losses, a company must have a system in place to evaluate and respond to any detected threats. Target, for example, had installed a $1.6 million malware detection tool from the reputable computer security firm, FireEye, six months before the breach. Target also employed a team of security specialists monitoring its computer systems. Target's FireEye system detected the malware threats and set alerts off, but Target's security team did not respond. As a result, 40 million credit card numbers were stolen.

Conduct a Post Breach Investigation: Companies should conduct an investigation just as it would after the theft of physical property or money. An electronic forensics investigation can determine the cause of the breach and the extent of the damage. With no fingerprints left behind, special software can trace electronic evidence, and can examine databases, looking for foreign malware or viruses. The software can also back track the electronic activity of insiders to determine who had accessed the compromised data. While post-breach action cannot prevent the breach, it can mitigate the damages and prevent even greater costs to the company.

Visit the FTC Bureau of Consumer Protection Website: If your company would like to learn more about what it can do to protect corporate data, the FTC's Bureau of Consumer Protection offers free Guides for Businesses regarding data security. These guides offer specific issues practical tips for businesses looking to improve data security. *See* http://www.business.ftc.gov/privacy-and-security/data-security.

Conclusion

Ignoring the various threats to electronic corporate data is no longer an option. Cybercrime and electronic data theft is taking a large toll on corporations worldwide. Whether it is theft of intellectual property by employees or theft of payment card information by hackers, the costs of corporate theft truly fall on the affected company. Companies must learn to prevent the theft of their electronic data, or at least to mitigate the effects. While there is no guaranteed solution to electronic data theft, companies have many options to take control of the security of their valuable data. Taking proactive steps to prioritize protection, monitor systems, and effectively respond to breaches can lower the chances that your company will be the next big headline. Corporations have everything to lose by not effectively securing their electronic data. IDQ