SOPHOS

simple + secure

The State of Data Security

Defending Against New Risks and Staying Compliant

Table of Contents

The State of Data Security

Defending Against New Risks and Staying Compliant

Report Abstract: What You'll Learn in this Paper

Today's IT and business managers must take a hard look at the risks and costs of potential data loss. Creating a proactive data security plan arms you with the knowledge you need to manage the risk and helps you to stay compliant with data protection rules and regulations. We all know that data breaches are constantly in the news—in fact security breaches compromised more than 500 million U.S. records since 2005. Plus, lost data due to human error or negligence is just as much of a threat. Fortunately, it's much less expensive to prevent a breach or other data loss incident, than it's to respond to one and resolve it after the fact.

Recognize how your data can become vulnerable, including the latest issues stemming from unprotected data on mobile devices and social media sites. Understand the compliance issues involved, and identify data protection strategies you can use to keep your company's information both safe and compliant.

What Does Data Protection Mean to my Organization?

Today's IT and business managers must take a hard look at the risks and costs of associated with potential data loss and have a plan in place to manage those risks. At the same time, you need to stay compliant with data protection rules and regulations.

Questions abound: Where is all my data? What data in my network today is sensitive? Who can access it? How can I keep track of it? What do I need to know to keep my company's data protected from harm and loss?

Data issues exist for small and medium-sized businesses as well as for large enterprises. As an IT practitioner, you first need to discover and control data. Then, you can put an effective data protection strategy in place. Recognize how your data can become vulnerable, including the latest issues stemming from unprotected data on mobile devices and social media sites.

According to the Identity Theft Resource Center, at least 662 data breaches in the U.S.occurred in 2010, which exposed more than 16 million records. Nearly two-thirds of breaches exposed Social Security numbers, and 26% involved credit card or debit card data. The majority of these attacks were malicious hacks or insider theft.

Data breaches are constantly in the news. According to the Privacy Rights Clearinghouse, security breaches compromised more than 500 million U.S. records since 2005, and those are just the reported breaches. Lost data due to human error or negligence is just as much of a threat. Fortunately, it's much less expensive to prevent a breach or other data loss incident than to respond to one and resolve it after the fact.

Compliance regulations aim to help keep your data secure and your customers safe. But, it often seems that compliance can be one big headache. Staying on top of changes in compliance regulations, proving compliance and avoiding fines are additional challenges.

So, how can you protect your company's information, remain compliant and still stay sane?

Create a proactive data security plan to arm yourself with the knowledge you need to manage the risks, while staying compliant with data protection rules and regulations.

Why Every Organization Needs to Protect Personal Information

Data can leave your network and your control in many ways, including through unprotected servers, desktop computers, laptops, mobile devices and email messages. And, cybercriminals may use malware to get into your network to destroy or steal your company's valuable information. This is why protecting sensitive and personal information is essential.

CSO magazine's 2011 CyberSecurity Watch Survey found that 81% of respondents' organizations experienced a security event during the past 12 months, compared with 60% in 2010. Twenty-eight percent of respondents saw an increase in the number of security events as compared with the prior 12 months.

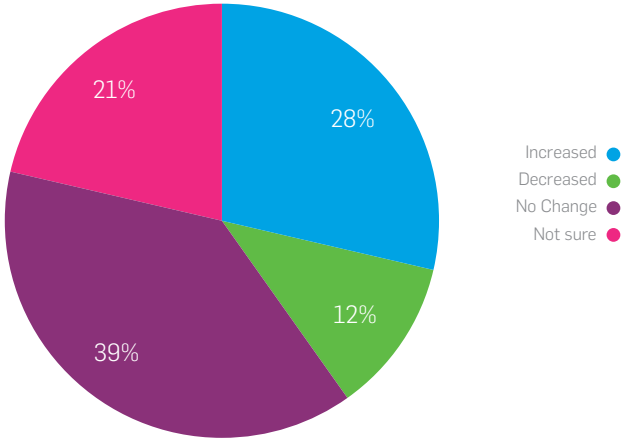
Today's connected world makes it easier than ever to let companies collect personal information, often for completely legitimate reasons. Personal information is any information that someone can use to uniquely identify, contact, or locate a single person, or use with other sources to uniquely identify a single individual. This information typically must be protected by law. Credit card numbers from a retail sale, Social Security numbers on tax forms, bank account information for online bill payment, medical details from a doctor's visit, and names, email addresses and birthdates entered on any Internet site registration—this data all resides in the databases of various companies, who often share it with third party vendors to perform a wide array of outsourced activities.

These bits and bytes of data let organizations contact their customers or prospects and provide them with offers and services. However, if cybercriminals illegally obtain this same information, they can easily exploit it for the purposes of identity theft or other crimes. Identity theft and, consequently, credit card theft have major financial and reputation consequences for both the individual whose identity is stolen and the company from which the thieves obtained the data. Beyond cybercrime, the corporate sharing of personal information with third parties violates compliance with a large number of laws and regulations if it happens without the individual's consent.

Number of Security Events During the Past 12 Months vs. the Prior 12 Months

81%

of respondents' organizations have experienced a security event during the past 12 months, compared to 60% in 2010.



Source: CSO magazine's 2011 CyberSecurity Watch survey

Risks arise when personal information is leaked, is improperly discarded or gets into the wrong hands. How organizations handle, use and safeguard personal information determines the magnitude of those risks. Consumers are becoming more aware of this issue as well: in a survey of 1,000 people in the U.K., 94% ranked "protecting personal information" as their top concern, equal to their concerns about crime, according to *The Telegraph*.

Businesses in every industry need to pay attention to myriad of legal requirements involving personal information security and related policies. And, if your company deals with financial, government, healthcare, education, energy or retail data, you're likely to face even more stringent regulations.

A series of legislative measures exist today to limit the distribution and accessibility of personal information. From the Gramm-Leach-Bliley Act (GLBA), to the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule and Security Rule, to the Health Information Technology for Economic and Clinical Health Act (HITECH) Act, to the Federal Information Security Management Act (FISMA), every industry has its own "alphabet soup" of regulations, guidelines, and standards to keep information safe.

How can you navigate through these regulations, make sure your company is in compliance and ensure that your customer data is secure? How can your company avoid data loss incidents that damage customer trust, cause corporate embarrassment and have a negative impact on the bottom line?

It's all about managing information risks.

Identity theft, and consequently credit card theft, has major financial and reputation consequences for both the individual whose identity is stolen and the company from which the data was obtained.

Manage Information Risks, and Compliance Will Follow

We recommend that you manage the information risks first, and as a result, compliance will become a much easier problem to tackle. There are many different legal requirements—and, yes, you do have to keep track of them and comply with these requirements. But, according to security expert Rebecca Herold, you'll cover roughly 85 to 90% of compliance regulations if you practice effective data protection.

Herold states, "At the heart of most data protection regulations is the requirement to address risks appropriately within the organization. The regulations then typically list some specifics, most of which are found within widely accepted information security standards, such as ISO/IEC 27001, ISO/IEC 27002 and multiple National Institute of Standards and Technology (NIST) documents."

"Many commonly used risk assessments use these standards," she continues. "So it makes sense, that if organizations identify their information security risks, and then work to mitigate them, the major burden of their compliance issues will have already been tackled."

The remaining requirements are typically very detailed activities that address specific industries. Here are some overarching strategies for managing information risk:

Know what you have: Define "personal information" as it applies to your organization, taking into account all the types of personal information that fall under your applicable legal requirements for information protection. Establish an inventory, and make sure to maintain it.

Know what your employees have, and also what they access: (including mobile technology, social media and emerging technologies). Identify who collects, processes, stores or accesses personal information. Determine who is, or should be, responsible for these activities.

Know where valuable data is kept: Identify storage locations, including mobile endpoints. Also include third parties you trust to store information.

Know what to collect, and what to keep and not to keep: Create policies to limit what you and your marketing teams collect for data. Are you really using what you have? If not, don't collect it. Follow data retention requirements. Incorporate this into your inventory information, or use a completely separate system to manage. Be sure to dispose of data securely and irreversibly.

Limit access: Restrict access to only those who have a business need to access the information for business purposes. Don't give access beyond the purposes for which you collected the information.

Put in place appropriate safeguards: Do a risk assessment, and then implement effective safeguards to appropriately mitigate the risks, following your policies and procedures. Be sure you communicate information about how to do this through regular training and ongoing awareness communications.

These strategies need to be supported with the appropriate technology tools and strong control processes, which we'll discuss later in this report. But first, let's look at what happens when there's a breach.

Recent Breaches: The Takeaways

About 85% of all U.S. companies have experienced one or more data breaches, according to the Ponemon Institute, but the figure may be even larger because many companies don't have the ability to detect exposed information. In the following brief case studies, we'll highlight how data security incidents can have a serious effect on organizations, and how the cost of these data breaches continues to rise.

Massachusetts General Hospital

Massachusetts General Hospital, the oldest and largest hospital in New England, drew a $1 million fine from the U.S. Department of Health and Human Services (HHS) for losing 192 patient medical records. An employee had left these hard-copy files on the subway—purely a human mistake. But this violation of the HIPAA Privacy Rule cost the hospital approximately $15,000 per patient file, proving the value of data protection.

If these were electronic files and the data was strongly encrypted using standards from the National Institute of Standards and Technology, the hospital wouldn't even have had to even notify HHS or patients of the incident. The Safe Harbor clause of the HITECH Act states that if you can prove the information was encrypted, no disclosure is required—a strong argument for encrypting your data.

BP

In another incident involving human error, a BP employee lost a laptop containing data on 13,000 oil spill claimants during "routine" business travel. The laptop included unencrypted names, Social Security numbers, addresses, phone numbers and birthdates of people who had filed claims related to the Deepwater Horizon accident.

And laptops are easy to lose: About 12,000 laptops are lost every week at U.S. airports alone, or approximately one every 50 seconds.

The Safe Harbor clause of the HITECH Act states that if you can prove the information was encrypted, no disclosure is required—a strong argument for encrypting your data.

Epsilon

Marketing services provider Epsilon fell victim to a massive data breach, which compromised email address data belonging to many of the world's biggest brands. Epsilon is the largest provider of permission-based email marketing and sends more than 40 billion emails a year on behalf of 2,500 brands, including Kroger, Marriott Rewards and Ritz Carlton Rewards.

With just names and email address data, hackers can launch targeted attacks against customers who expect to receive communication from these brands. These spearphishing emails may request personal or sensitive information, or include attachments that can launch a virus and expose the victim to further data theft. They also give criminals a window into the shopping habits and lives of those whose email addresses they possess.

Nationwide Building Society

Nationwide Building Society is one of the UK's largest financial service companies. The Financial Services Authority (FSA) fined the company nearly £1m in fines for lax security procedures and controls which led to the exposure of the personal details when a company laptop containing confidential records for nearly 11 million customers was stolen.

The laptop was stolen from an employee's home during a burglary, and authorities believe the thief was only looking to steal the laptop itself, not the data. However, the company was still hit with a very substantial fine, plus the cost of notifying the millions of people whose records were stolen.

The Cost of Data Breaches

As these examples show, data breaches can not only harm the consumer whose data is lost, but also pose significant costs to the organization.

The Ponemon Institute's most recent U.S. Cost of a Data Breach report shows that costs continue to rise. In 2010, the costs of a data breach reached $214 per compromised record and averaged $7.2 million per data breach event.

It's not only direct costs of a data breach—such as notification and legal defense costs—that impact the bottom line for companies, but also indirect costs like loss of trust and lost customer business.

A recent OnePoll survey demonstrates the impact of indirect costs. The survey found that about two-thirds of U.K. consumers would try to avoid interacting with firms that they knew lost confidential information. The Ponemon Institute adds that the potential expense of losing customers to a security breach is prompting U.S. companies to spend more on bolstering protection for their systems.

This only makes sense: you need to find the right balance between what it costs to protect your company's data and what you stand to lose.

Ironically, the Ponemon Institute reports that companies that respond quickly to data breaches pay more than companies that take longer to respond—in 2010, they paid 54% more. So, why does it cost more to "do the right thing" as soon as possible?

"The survey found that around two-thirds of U.K. consumers would try to avoid interacting with firms which are known to have lost confidential information."

ONEPOLL

The Ponemon Institute speculates that compliance with regulations like HIPAA, the HITECH Act and the numerous state data breach notification laws is fueling this rush to notify customers. Unfortunately, these companies are in such a hurry to notify victims that they end up over notifying and notify everyone, even customers whose data was never lost or stolen. Dr. Larry Ponemon concludes, "Companies that take a more surgical approach and spend the time on forensics to detect which customers are actually at risk and require notification ultimately spend less on data breaches."

Furthermore, the costs of data breaches are increasing as individual states pass a patchwork of laws requiring companies disclose whenever customers' personal information is exposed. So far, at least 46 U.S. states have passed such measures, but definitions of a breach and of personal information vary, as along with differing deadlines for notifying customers and punishments for failing to comply. To simplify this mishmash of state-based regulations, many data security experts are calling for national legislation on this issue across the board, similar to the healthcare industry's HITECH Act.

The U.S. House of Representatives passed a bill in 2009 that would set a unified standard for responding to breaches and require consumer notification. The Senate introduced a version of the legislation in various bills over the past five years, but that has yet to advance.

Since your goal is to prevent a data loss incident before it happens, let's explore how data become vulnerable in the first place.

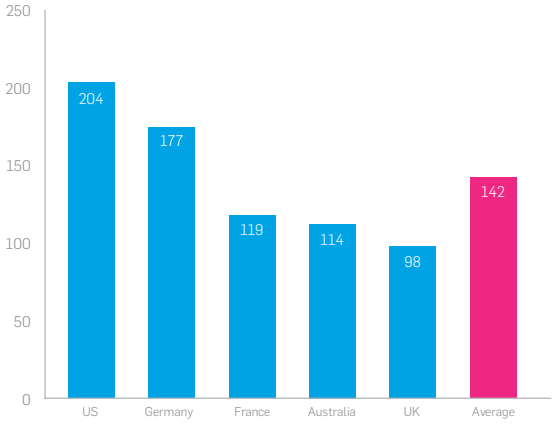
Are There Global Differences?

The Ponemon Institute also researched the global costs of a data breach, with a consolidated analysis of five national "cost of data breach" studies covering the United States, the United Kingdom, Germany, France and Australia. To maintain consistency, it limited the size the analyzed data breach incidents, excluding catastrophic breach incidents, to avoid skewing overall findings (which explains why the U.S. cost is slightly lower than stated earlier).

The U.S. had the highest cost per compromised record at $204, followed by Germany at $177, France at $119, Australia at $114 and the U.K. at $98.

Per capita cost

Converted to $US dollars



Source: Ponemon Institute

New Ways Data become Vulnerable

So, how does data become exposed and leave company networks? A number of factors can make your organization's data vulnerable to loss or theft. Simple human mistakes, malicious cybertheft, technology failures and emerging technologies all contribute to the problem. The use of mobile technologies and the blending of at-home and at-work technologies—the so-called "Consumerization of IT"—are some of the newer causes of data vulnerability.

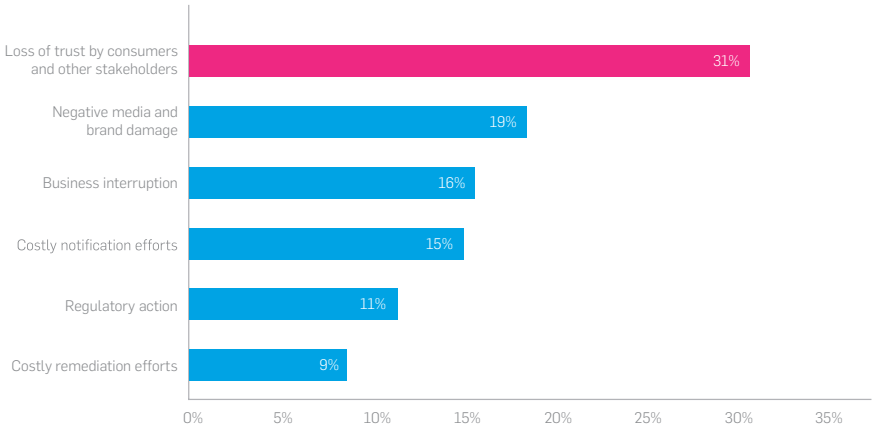
To top it all off, when your employees are not aware of the issues around data security, or trained on how to protect the data they use, your company's risk increases. We'll explore each of these risks in greater detail:

Human Mistakes

In *An Essay on Criticism* in 1711, English poet Alexander Pope wrote, "To err is human." And, as we see with so many of the data breaches today, information is lost due to simple human error. A laptop left on a plane or train, a BlackBerry or iPhone that slips out of a pocket at dinner, a USB memory stick dropped at a trade show—all of these are simple mistakes that can have disastrous consequences. Pope also stated that "to forgive is divine"; unfortunately IT professionals can't afford to be very forgiving when it comes to data loss.

The most susceptible time to lose a laptop is during travel, according to a Ponemon Institute study. Study participants reported that the most common locations where employees lost their laptops were hotels, airports and rental cars, and at conferences. Employees are often careless or circumvent security procedures, and as a result, confidential and sensitive data can be at great risk. The greatest employee-related threats include failing to use proper authentication or passwords, transferring files on USB memory sticks and neglecting to protect laptops when traveling.

If your organization had a lost or stolen laptop computer, which of the following possible consequences would have the most negative impact?



Source: Ponemon Institute

USB memory sticks, CDs and DVDs can also contain unauthorized software that puts your network at risk. Malware like the Conficker worm is becoming a major issue, as these devices can help spread it. Users can also copy sensitive data onto these portable media, which might then be lost or shared with outsiders. Therefore, you may want to disable the ability for these devices to run automatically when plugged in, or consider restricting where they're used. If your business depends on removable media, scan them regularly for malware and sensitive data.

Employees need to be aware of how detrimental a lost laptop, mobile device or portable media can be and learn simple ways to prevent loss, as well as the proper procedures for immediately reporting a data loss. According to statistics from the Privacy Rights Clearinghouse in the U.S., about 30 of the 144 data breaches announced in Q1 2011 involved mobile data-bearing devices.

Security analysts recommend encryption as one of the most effective ways to protect data on mobile devices against these sorts of breaches, and they specifically recommend full-disk encryption for laptops. "There really is no excuse for not encrypting laptops," says Avivah Litan, Vice President and Distinguished Analyst at Gartner. "Enterprises that are not putting in laptop encryption are just being lazy." Unfortunately, many companies continue to ignore this advice, due to the cost and the perceived complexity involved with encryption. Herold adds, "Most organizations believe encryption is too expensive, so they don't implement it as a way to 'save' money." Regrettably, this is an extremely shortsighted view.

IIn addition to mistakes by in-house employees, you should also think carefully about data security when using outsourced services, and safeguard against improper access to information. For example, the HITECH Act extends HIPAA compliance to all business associates who work with protected health information (PHI) data. In turn, any subcontractors also need to safeguard information to the same level—even if their business is not in the healthcare industry. To collaborate with outside vendors and business associates, it's important to put the appropriate security measures in place to comply with regulations, such as protecting patient privacy.

Automated controls can help minimize human error—in essence, taking the end user out of the decision tree. Although automation can't remove the human factor completely, it can certainly limit it. Implementing data protection shouldn't be a hassle for the user or require extra steps. When the process can be automated—such as automatically encrypting email messages or attachments—users don't have to worry about being a part of the security implementation process.

"There really is no excuse for not encrypting laptops. Enterprises that are not putting in laptop encryption are just being lazy."

AVIVAH LITAN
Vice President and Distinguished Analyst, Gartner

Malicious Intent

Another type of human risk is the nonaccidental type—it's born of malicious intent. External hackers look to gain access to valuable data; disgruntled employees try to damage something within their company or steal information for personal gain.

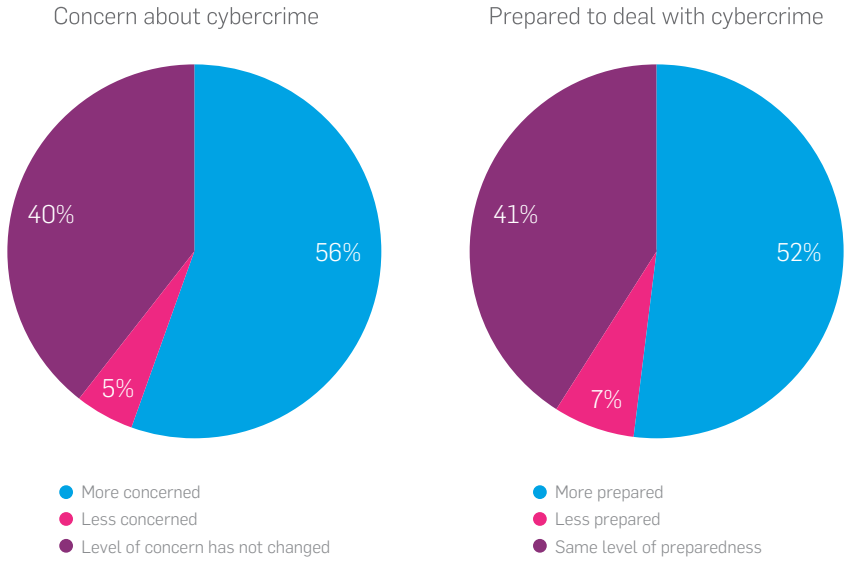
Malicious intent is also at play in the theft of laptops or other devices that contain company information. And, attacks get more sophisticated all the time—the recent malicious attack on RSA demonstrates that even professional security firms are in the crosshairs today.

In 2010, malicious attacks were the root cause of 31% of the data breaches studied, according to the Ponemon Institute. That's up from 24% in 2009 and 12% in 2008. Hostile breaches cost more, on average, than incidents stemming from negligence. Malicious attacks create greater costs because they are harder to detect, the investigation is more involved and they are more difficult to contain and remediate. Another reason malicious attacks are so expensive is because malicious activity generally centers on monetary gain, or on gaining personal information that thieves can sell.

A new breed of malicious intent seems focused on nation-sponsored attacks with a bent toward political activism and even terrorism. From sites such as WikiLeaks, which was created specifically to leak information to reveal government communications to distributed denial of service (DDoS) attacks that disable certain websites to make a point, these "hacktivist" groups pose a new type of threat.

Interestingly, according to the 2011 CyberSecurity Watch survey, organizations are more concerned about cybercrime, as compared to last year, but they also feel that they are more prepared. The survey also shows that security spending is on the rise.

More Concerned, More Prepared



Source: CSOmagazine's 2011 CyberSecurity Watch survey

Technology failures or glitches

Sometimes people are not to blame. For instance, if an automated service fails or if data is stored on the Web inappropriately, an unintentional leak of proprietary data can occur. In addition, new or updated technologies may have undiscovered weaknesses, allowing malicious attacks through these vulnerabilities—a good reason to keep up with regular security patches.

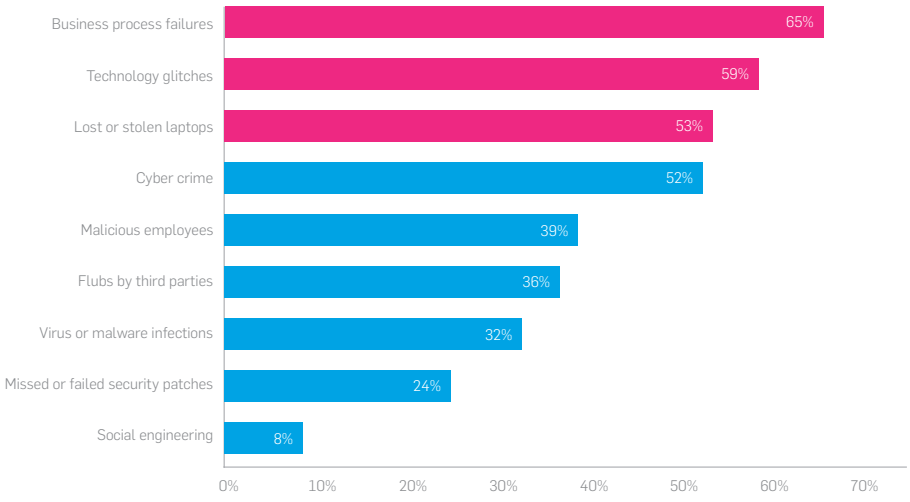
A recent technology glitch at the National Australia Bank (NAB) threw the bank's transaction system into chaos, causing millions of transactions to be delayed, duplicated or not posted. At Commonwealth Bank, also in Australia, up to 40 ATMs started spewing cash as a result of a database maintenance glitch.

Often, the form of data you have makes it difficult to secure. Unstructured data—such as Microsoft Excel spreadsheets and PowerPoint documents—are not built to allow you to easily control and keep track of any sensitive data within a document.

When the Ponemon Institute asked 714 IT and IT security practitioners in the U.S. about the top three security threats facing their organization, they listed business process failures and technology glitches as the two biggest threats, followed by lost or stolen laptops.

Rank order of the threat of a lost or stolen laptop with other known security threats

Each bar defines the percentage of 1+2 (highest risk) on a nine-point scale



Source: Ponemon Institute

Emerging Technologies

Emerging technologies—and new ways of using technology—are challenges that are keeping IT managers up at night. The Consumerization of IT, mobile technologies, social media, virtualization and cloud computing ... the list of issues goes on and on.

Consumerization of IT: With an ever-diminishing distinction between work and home, personal and portable devices are creeping onto company networks. Employees are using personal devices such as laptops, tablets and smartphones for work and are accessing sensitive corporate information from their home computers. Traditional enterprise IT organizations tried to keep work-related technology separate from personal, consumer-based technology, but the two inevitably blended.

"As the borders of traditional networks start to blur, IT managers need to think about how to secure information, rather than how to secure just the network," states Herold. "Your networks now have living endpoints, and as a result you need to think beyond the physical facility."

Mobile devices: Mobile devices by their very nature are harder to protect, and therefore can represent the weakest technology link in your network. According to the 2010 report on Gartner's Magic Quadrant for Mobile Data Protection, "Mobile data protection (MDP) systems and procedures are needed to protect data privacy and to comply with audit requirements, and every company must include MDP in its IT operations plan." Herold adds, "Employee training and awareness to rein in mobile computer risks are also part of the equation."

Some U.S. states are starting to enact legislation about data protection on mobile devices. For example, in September 2008, Massachusetts passed the Mass Data Protection Law—formally known as Mass 201 CMR 17.00—which requires companies to encrypt sensitive personal data stored on mobile devices. This regulation applies to all organizations "who own, license, store or maintain personal information about a resident of the Commonwealth of Massachusetts." Most provisions of this law went into effect in March 2010.

Social media: Workplace use of social media sites—such as Facebook or LinkedIn—exposes companies to risk, regardless of whether employees access the sites for personal or business use. Herold states, "Most people using social media sites don't know or care when they behave in a risky way, or put their privacy at risk. Most individuals are used to dealing with reputable companies protecting them, and their information. They believe that a promise made today, including those for privacy, will be kept tomorrow and forever. However, this isn't the case in our ever-evolving and widening digital world. Facebook is a prime example, with their almost monthly privacy changes and rearranges."

> "Mobile data protection (MDP) systems and procedures are needed to protect data privacy and to comply with audit requirements, and every company must include MDP in its IT operations plan."
>
> GARTNER

A good rule of thumb for social media site users is that if you don't pay for the service, then the site's security and access policies are most likely directed at protecting those who are: the advertisers. For the advertisers on social networking sites, access to you and your information is the reason they advertise.

Use of social networking sites can affect your business when employees log on to social media sites from work, provide detailed personal information that could lead to spearphishing email attacks, respond to online survey scams and use the same passwords as they do for business related applications. It's your weakest link that determines your level of security. There are also risks from vulnerabilities in Facebook's code, which could open the door to phishing, spam and even malicious attacks.

Virtualization: The case for server virtualization is so compelling that more than 50% of server licenses sold today are for virtual servers, not physical ones, according to market research firm IDC. In addition, organizations are now considering virtualizing their desktops. Since many organizations view virtualization technology as an increasingly important part of their network, it's important that they properly secure any investment in virtualization to prevent data security issues. Strategies for protecting virtual servers and desktops include implementing full endpoint security on your virtual computers, as well as updating and scanning, all while balancing protection with performance.

Outsourcing and cloud computing: Cloud computing uses the Internet to access, modify, use and store data. With cloud computing, someone other than the user owns and operates the application. Outsourcing to a cloud services provider can save money and reduce complexity, but can also increase risks, especially when personal or otherwise sensitive data is involved. Some security experts recommend that you keep your "trophy data," or most important data, on servers that you own, operate and control. The recent Epsilon data breach demonstrates the risks of cloud computing. Since Epsilon is a cloud provider of electronic direct marketing services, a breach of Epsilon's system is, effectively, a breach of all its customers' systems as well.

So when you outsource the handling, processing and storage of information, you need to make sure your cloud computing vendor has controls in place. For instance, if your company uses protected health information, then your business associates and outsourcing partners all need to comply with the HITECH Act. By documenting what you're doing to ensure your cloud provider uses appropriate controls, you demonstrate due diligence and create documentation that shows you're following a compliance strategy.

Lack of Training and Awareness

Employees' lack of awareness about IT security issues can often result in inadequate protection of valuable corporate information.

Employees need to know how to safeguard the information they work with on a daily basis to do their job successfully. In addition, states Herold, "there are a growing number of laws and regulations that include requirements for the covered entities to provide some type of information security and/or privacy awareness and training to not only their personnel, but also in some instances to their customers and consumers."

Implementing regular information security and privacy training can help organizations experience fewer data security incidents. Provide ongoing awareness communications to reinforce security and privacy requirements. Not only do well-informed personnel know how to protect personal information, but their training also makes them more accountable for their actions.

Are You Doing All You Can to Keep Your Data Safe and Compliant?

To take charge of information security, you'll need to look at it in manageable pieces. There are three components of an information security strategy: the things you're required to do by law; the operational processes and procedures you put into place; and the technology tools you use to get the job done.

It's useful to think of the technology tools in four categories, each one supporting a different facet of information security, yet building on one another for a layered approach to protection. Here's an overview of how Sophos provides layered protection:

Encryption: Sophos makes it easy to securely share data with proven full-disk, removable storage and email encryption. Our SafeGuard Enterprise solution enforces policy-based encryption for PCs and mobile devices across mixed environments.

Threat protection: You need a solution that proactively detects zero-day threats and reacts quickly to attacks. With Anti-virus, Live protection and Web protection, Sophos has you covered.

Data loss prevention: Sophos offers a unique and simple solution for data loss prevention (DLP). We integrate content scanning into the threat detection engine and include a comprehensive set of sensitive data-type definitions to enable immediate protection of your sensitive data.

Security controls: You can create a secure IT environment for your company by addressing the sources of infection and preventing incidents. Sophos provides network access control, application control, device control and file type control, which all help reduce threats.

Constant Monitoring for Effective and Compliant Data Protection

Effective data security and compliant data protection means you need to be constantly vigilant in monitoring the information your company generates and tracking where it goes as well as in implementing safeguards for that information.

Sophos can help you with technology tools and guidance. A good first step is the Sophos Roadmap to Data Security. Also visit our Security News and Trends site on an ongoing basis to get the latest news on data protection.

At Sophos, it's our job to stay on top of the changing landscape of data security and compliance. We'll continue to monitor developments and report back on a regular basis.

APPENDIX A: Major Compliance Regulations, A Listing

Although a comprehensive set of all compliance laws and regulations isn't readily available online, here's a helpful list of resources on compliance regulations by geography, plus others that appear in this report:

Selected U.S. State Laws Related to Internet Privacy compiled by the National Conference of State Legislature (NCSL)

U.S. State Security Breach Notification Laws compiled by the National Conference of State Legislature (NCSL)

U.S. State Data Security Breach Laws compiled by law firm Mintz Levin

Western Hemisphere Data Protection Laws compiled by the U.S. Department of Commerce

Selected Asia and Oceania Data Protection Laws compiled by the U.S. Department of Commerce

Selected Country Reports compiled by Privacy International

Privacy Act Issues under Gramm-Leach-Bliley (GLBA), compiled by the Federal Deposit Insurance Corporation (FDIC)

Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule and Security Rule, compiled by the U.S. Department of Health and Human Services

Health Information Technology for Economic and Clinical Health (HITECH) Act, compiled by the U.S.Department of Health & Human Services

Federal Information Security Management Act (FISMA), compiled by the National Institute of Standards and Technology (NIST)

APPENDIX B: Proving Compliance and Why Effective Compliance Costs Less

Proving Compliance

At some point, the rubber needs to meet the road. This is where you put strategy into action, making it part of your daily life in securing your organization's data, ensuring compliance and, if needed, proving that compliance.

We've boiled it down to four key areas:

1. Responsibility: Every company must take the responsibility of protecting its data seriously—both the data it possesses as well as the data it entrusts to third parties for processing. There's a lot of talk about how companies need to be good corporate citizens and be socially responsible in their communities—but if you think about it, a first step in that responsibility is protecting the private and sensitive information of their customers.

One recent example of a company disregarding this responsibility is the case of Cignet Health. The U.S. Department of Health and Human Services issued the healthcare organization a $4.3 million fine for violations to the HIPAA Privacy Rule because Cignet failed to provide 41 patients with copies of their medical records, and then failed to respond to requests for information related to the complaints. Ultimately, HHS found that Cignet showed "willful neglect of its obligation."

2. Accountability: In order for your company as a whole to take compliance seriously, it must have someone who's accountable for the function. In some organizations, this may be a person who has the title of Compliance Officer, but more often than not, this function touches many departments—Legal, Records Management, IT, Finance, Operations— yet no one person seems to own it. Having a senior-level "point person" to drive compliance helps to demonstrate its importance in the organization and will help get things done. A recent Ponemon report shows that more organizations are putting Chief Information Security Officers (CISOs) in charge of data breach response, demonstrating the link between solid business practice and technology.

Personal accountability is also an increasingly important topic in the realm of privacy and personal data protection. Many experts seem to believe that users of online services have a responsibility to protect themselves by following a few basic rules.

3. Diligence: Compliance is not a "set it and forget it" type of function. Just because you've worked hard to protect your company's information and comply with industry regulations doesn't mean you can now move on and do something else. As a recent Focus Expert Roundtable pointed out, the business model needs to change to ask the questions, "What do we need to do to have ongoing compliance?" and "What do we need to change about how we do our work?"

To keep your data safe and stay compliant, you need to balance both operational and technical security issues. You need to document your company policies and procedures and make sure they are "living" documents that you can change and customize as necessary—and are understood by all employees and partners. Diligent compliance means taking a 360-degree view: Your employees need to understand their part, but you also need to be responsible for third-party business associates, such as outside services used for billing, collections, pre-employment screening and managed IT. To complete the picture, you should put

Compliance is not a "set it and forget it" type of function. Just because you've worked hard to protect your company's information and comply with industry regulations doesn't mean you can now move on and do something else.

training and awareness programs in place to make sure everyone involved understands their role.

4. Technical controls: In addition to responsibility, accountability and diligence, you need technical controls—tools to put in place on your network to protect your data and keep it safe and compliant. A layered approach to technical controls includes implementing encryption, threat protection, data loss prevention and security controls. And, the associated monitoring reports provide documentation to prove compliance in the event of an audit.

Effective Compliance Costs Less

The recent Ponemon Institute benchmark study titled "The True Cost of Compliance" supports managing information risk. This study shows that organizations with well-thought-out data security strategies and practices can reduce their financial risk and the costs of compliance.

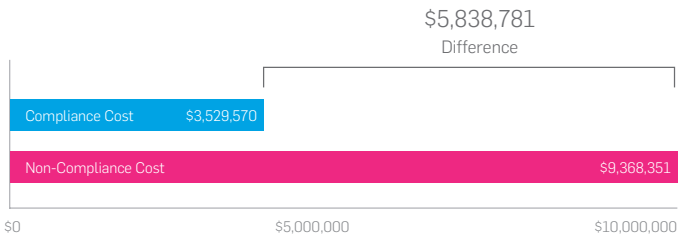
By avoiding costly data breaches in the first place, and minimizing the impact when breaches do occur, companies can actually save money.

The purpose of the study was to determine the financial impact to organizations that adopt and implement compliance-related activities, including processes, policies, people and technologies. Noncompliance costs included things like fines, legal fees and lost-opportunity costs. The study examined these activities for 46 multinational corporations and found that noncompliance costs for organizations are, on average, 2.65 times higher than compliance costs.

The study showed that companies with ongoing investments in compliance-related activities saved money compared with those organizations that fail to comply with various domestic and international security regulations. Of the companies studied, compliance costs averaged $3.5 million, while noncompliance costs averaged $9.3 million, meaning those organizations that invested $3.5 million in compliance saved $5.8 million.

Ponemon summarizes, "To reduce those compliance costs successfully, you need to focus on the right mix of technology, control processes, smart people and good governance."

The True Cost of Compliance



Source: Ponemon/Tripwire

APPENDIX C: Practical Advice for Managing Information Risk, A Checklist

Actions	Requirements and Deliverables
Get Executive Support	❑ Executives need to understand impact to business of legal non-compliance and privacy breaches ❑ Executive support must be active and visible to drive end user buy-in
Assign Responsibilities	❑ Identify corporate roles and responsibilities for information security and privacy ❑ Assign supporting roles and responsibilities throughout the enterprise
Identify Legal Requirements for Compliance	❑ PCI-DSS for credit card processing ❑ Applicable regulations: e.g. HIPAA/HITECH (healthcare); GLBA (financial); FERPA (education); FISMA (U.S. government); SOX (publicly traded companies) ❑ Applicable country, state and provincial laws ❑ Contractual requirements
Define and Document Information	❑ Define personal and sensitive information as it applies to your organization, customers, and employees ❑ Create data classifications and supporting procedures ❑ Document data storage locations, entry and exit points, how it is used, and those with access
Establish and Implement Policies and Procedures	❑ Consistent with all relevant legal requirements ❑ Around vulnerabilities identified from risk assessments ❑ Conduct a gap analysis of current policies, tools and controls
Identify Supporting Technical Controls	❑ Encryption ❑ Malware protection ❑ Data leak prevention ❑ Application & physical device controls ❑ Network & client firewalls ❑ Data backup ❑ Data integrity controls ❑ Authorization & identity management ❑ Logical & physical access controls ❑ Monitoring and reporting
Educate Personnel	❑ Identify and document education ❑ Implement regular training for target groups ❑ Institute ongoing awareness and communicationsand activities
Check out These Resources	❑ Read new Sophos Data Protection report every six months ❑ Sign up for RSS feed for Sophos Naked Security Blog at: http://nakedsecurity.sophos.com/ ❑ Check out our other Sophos reports and white papers at: http://www.sophos.com/en-us/security-news-trends/whitepapers.aspx ❑ Monitor breach list on: http://www.hhs.gov/ ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html ❑ Sophos-related products and tools: http://www.sophos.com/en-us/products.aspx

Sources

2011 CyberSecurity Watch Survey, a cooperative effort of *CSO* magazine, the U.S. Secret Service, the Software Engineering Institute CERT® Program at Carnegie Mellon University and Deloitte

BBC News, "Nationwide fine for stolen laptop," February 14, 2007

Bloomberg, "Security-breach costs climb 7% to $7.2 million per incident," by Kelly Riddell, March 8, 2011

Computerworld, "BP employee loses laptop containing data on 13,000 spill claimants" by Jikumar Vijayan, March 29, 2011

Computerworld, "Failure to encrypt portable devices inexcusable, say analysts" by Jikumar Vijayan, March 31, 2011

Focus IT Roundtable: The State of IT Compliance—What's Working and What's Not (with Rebecca Herold), March 3, 2011

Gartner Information Technology Resources

Gartner's Magic Quadrant report for 2010 Mobile Data Protection

Information Security and Privacy Training and Awareness, a Rebecca Herold video

International Association of Privacy Professionals (IAPP) website

Identity Theft Resource Center—Data Breaches in 2010

IT World, "Consumerization of IT—good, bad, or just the way things are now?" by Ryan Faas, February 24, 2011

"Managing an Information Security and Privacy Awareness and Training Program" by Rebecca Herold (2010, p.23), 2nd Edition, CRC Press, Boca Raton, Fla.

Ponemon Institute—Business Risk of a Lost Laptop

Ponemon Institute—"Compliance like a club," Dr. Ponemon's Blog

Ponemon Institute—"Cost of a data breach climbs higher," Dr. Ponemon's Blog

Privacy Rights Clearinghouse—Chronology of Data Breaches

SC Magazine UK, "TripAdvisor admits that its mailing list was compromised, with some email addresses stolen," by Dan Raywood, March 25, 2011

Sophos cloud computing podcast: download

Sophos Naked Security blog

Threatpost Newsletter, "HIPAA Bares Its Teeth: $4.3m Fine for Privacy Violation," by Paul Roberts, February 23, 2011

VentureBeat, "Epsilon data breach results in a huge loss of customer data," by Dean Takahashi, April 2, 2011

Wikipedia

ZDNet, Australian edition, "CommBank ATMs spew cash," by Darren Pauli, March 1, 2011

ZDNet, Australian edition, "NAB implicates vendor in transaction woes," by Suzanne Tindal, December 16, 2010

Additional Resources

Sophos Data Security Toolkit

Sophos Naked Security Blog

Sophos Roadmap to Data Security

What does Compliance Mean to You? a Sophos video (less than 5 minutes)

United Kingdom Sales:
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales:
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Boston, USA | Oxford, UK

Sophos Security Report 5.11v1.dNA

SOPHOS