

Internet Security Essentials for Business





STOP | THINK | CONNECT™

Stop. Think. Connect. is a new public-private awareness and education campaign to help people stay safer and more secure online. This includes learning how to spot phishing scams and using strong passwords for your computer and commercial logins. **Stop. Think. Connect.** seeks to achieve for online safety and security awareness what Smokey Bear does to prevent wildfires and Click It or Ticket does for seatbelt safety. Visit **Stop. Think. Connect.** at www.stophinkconnect.org.



The U.S. Chamber of Commerce is the world's largest business federation representing the interests of more than 3 million businesses of all sizes, sectors, and regions, as well as state and local chambers and industry associations.

The U.S. Chamber of Commerce does not endorse any of the products or services contained in this guide.

Internet Security Essentials for Business

table of contents

2

INTRODUCTION:
SMART SECURITY IS GOOD FOR BUSINESS AND THE NATION

4

COMMON THREATS TO BUSINESS INFORMATION

4

Hacking and Malware

5

Lost or Stolen Physical Storage Media

5

Insider Threat and Human Error

5

Accidents and Natural Disasters

6

CYBERCRIME IS ON THE RISE

7

A Snapshot of Cybercrime in America

8

INTERNET SECURITY FUNDAMENTALS

8

Workforce

16

Policies and Problems

22

Prevention and Preparedness

27

CYBER INCIDENT AND COMPLAINT REPORTING ORGANIZATIONS

28

CONCLUSION:
ADD BUSINESS VALUE THROUGH INFORMATION SECURITY

29

INTERNET RESOURCES

30

CYBERSECURITY: NATIONAL AND SECTOR PERSPECTIVES

30

Banking and Financial Services

31

Chemical

32

Communications

32

Electric

33

Information Technology

35

ACKNOWLEDGEMENTS

36

ENDNOTES

INTRODUCTION

SMART SECURITY IS GOOD FOR BUSINESS AND THE NATION



Several U.S. presidents have said that protecting our nation's digital infrastructure is a top economic and national security issue. While extensive public and private sector efforts have been ongoing for years, President Obama articulated in May 2009 the need for wider public participation in protecting America's communication and information technology (IT) infrastructure, or cyberspace. He called for a national public awareness and education initiative to promote Internet security. "It's the great irony of our Information Age—the very technologies that empower us to create and to build also empower those who would disrupt and destroy," the president said.¹

The strength of our free enterprise system is directly tied to the prosperity and security of our interconnected world. The Internet is responsible for roughly \$10 trillion in annual online transactions and is a bulwark of the global economy.² Businesses and households conduct an increasing amount of their daily activities—from paying bills to shopping to texting friends and communicating with colleagues—online. The new *National Broadband Plan* estimates that 97% of small businesses use e-mail and 74% have a company website.³ Small businesses, which make up more than 99% of all businesses in the United States, play a critical role in enhancing our country's Internet security. They employ about half of all private sector workers and have been responsible for more than 60% of net new jobs over the past decade.⁴

Smart cybersecurity practices have positive implications for strong U.S. communities and national competitiveness. By managing their companies' cybersecurity, owners and managers not only help protect their crucial business and customer information but also help protect the Internet. Digital devices are so common in our daily lives that we often take them for granted, and yet sound day-to-day Internet security practices are much less ubiquitous.


However, there's some good news. A May 2010 poll conducted by the National Cyber Security Alliance (NCSA) and the Anti-Phishing Working Group (APWG), two leading Internet security education and awareness organizations, found that the vast majority of Americans are willing to practice good Internet safety and security habits given the right resources. Americans feel that doing their part to help keep the Internet safe benefits their homes and businesses as well as our national and economic security.⁵

The U.S. Chamber urges businesses to adopt essential Internet security practices to reduce network weaknesses to make life more difficult for the bad guys.

With this guide, we aim to do the following:

- Educate businesses about the common threats that they could become victim to online, particularly cybercrime. Just like the general public, most business owners, managers, and employees are not IT experts. This guide is ultimately about business preparedness.
- Provide simple recommendations to help businesses manage cyber risks. Perfect online security is unattainable, even for large businesses. But there are inexpensive practices that can be implemented to improve the security of information, computers, and networks as well as bolster a company's resilience.
- Give businesses simple steps necessary to protect their data and how and to whom to report cyber incidents.
- Stress that cybersecurity is a team sport. Taking the actions recommended in this guide will have positive consequences for the security of businesses, communities, and the country. The interconnectedness of computers and networks in cyberspace means that the public and private sectors share responsibility in raising their game. U.S. competitiveness and security depend on it.

COMMON THREATS TO BUSINESS INFORMATION



Barely a day goes by that news headlines aren't reporting the breach of an organization's network or the loss of a laptop. Making matters worse, the tools that nefarious actors—individual hackers, organized criminals, among others—use to steal data, money, or intellectual property (IP) from businesses are increasing in scope and sophistication. Some businesses are good at changing their approach to fit a changing security landscape, but criminals are good at adapting too. For businesses trying to avoid becoming victims, an obvious question arises about what kinds of threats are most commonly faced.

Hacking and Malware

According to studies, hacking, or gaining access into any computer system or network without the permission of the owner, is a leading cause of intrusions into a business' information system. Hackers have a number of techniques at their disposal to take advantage of poorly protected records or credentials, but many intrusions exploit weaknesses in an application or operating system software to gain unauthorized access.

Malware, such as self-replicating e-mail viruses and network worms, is commonly installed on a compromised system remotely. Hackers and organized criminals seek to minimize the chances of being detected to maximize the amount of data that they can steal. In recent years, malware has become innovative and stealthy to avoid revealing the attacker. Large and remotely accessible stores of online data remain a key target of cybercriminals.⁶



COMMON THREATS TO BUSINESS INFORMATION

Lost or Stolen Physical Storage Media

Equally important as hacking and malware, devices such as laptops, Universal Serial Bus (USB) flash drives (sometimes called thumb drives because of their size), smart phones, hard drives, and CDs/DVDs fall into this category.⁷ They can carry a lot of information, so ensure that they do not get lost or misplaced. Not all information that is compromised is accessed and abused by bad actors, but it should be considered data at risk.

Insider Threat and Human Error


Research suggests that the vast majority of data breaches originate from external sources. However, the “insider threat”—threats originating from within an organization—contributes to a significant number of data breaches that businesses suffer. An example is a trusted employee stealing the proprietary information of his or her employer. Insider threats, which involve the misuse of authorized privileges, have long presented serious problems for government and private sector computer systems. In addition to having access to company networks, insiders understand how things work, know what data are available, where data reside, and can wait for an opportune time to exploit a system, introduce malicious programs, or otherwise disrupt the systems.⁸

Not all insider threats are from employees looking to steal information or cripple a system. Human error can easily create a threat to information security. Whether an employee is opening spam mail, downloading, or installing programs or documents from untrustworthy sources, or simply e-mailing sensitive information to the wrong person or to someone who has forged an e-mail account, employees lacking awareness of good cybersecurity practices can give hackers easy access to a system. People with malicious intent may seek to gain access to your organization’s confidential documents or may attempt to alter, delete, or prevent your organization from using its data. Human error helps hackers turn valued, trusted employees into a potential threat to your enterprise.

Accidents and Natural Disasters

Natural disasters (e.g., fires, floods, and tornados), accidental deletions, hardware failures, and computer crashes can permanently cripple your business. Unlike cyberattacks, disasters and emergencies are nonmalicious but need to be taken equally seriously. According to the Red Cross, 15%–40% of businesses fail following a natural or man-made disaster.⁹ From the U.S. Chamber’s perspective, good security goes hand in hand with good preparedness, whether the threat arises online or from a weather event, a terrorist attack, or a pandemic.

CYBERCRIME IS ON THE RISE



At a congressional hearing, a cybersecurity expert gave an account of a small wooden furniture company that had been successfully hacked, resulting in the loss of data containing its valued designs. The witness suggested that the alleged offender(s) was able to commandeer the company's IP to rush new furniture to market and at cheaper prices.

The thieves didn't need to physically break into the company—that would be too risky and unnecessary. All they needed to do was steal the data with a few key strokes. How pervasive are cyber intrusions like this one, the witness asked rhetorically, if bad actors are hacking into the information system of a seemingly innocuous small business for commercial gain?¹⁰ The Bureau of Justice Statistics' National Computer Security Survey says that many cyberattacks against businesses go unreported to law enforcement authorities, but various indicators suggest that cybercrime is growing rapidly in scope and sophistication.¹¹ The Obama administration's *Cyberspace Policy Review* states that industry losses from IP theft were as high as \$1 trillion in 2008, which is a staggering figure.¹²

Cybercrime in the United States is on the rise at troubling rates. While it is difficult to get a complete picture of the entire problem, organizations such as the Internet Crime Complaint Center (IC3), a joint operation between the FBI and the National White Collar Crime Center, provides a window into a growing trend.

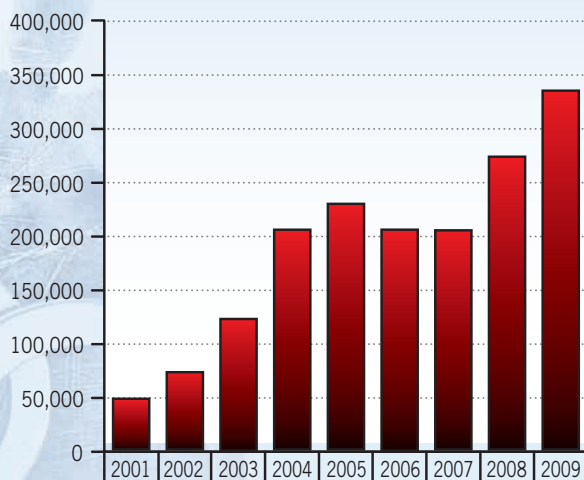
According to the IC3's *2009 Internet Crime Report*, annual crime complaints reported to IC3 have increased nearly 668% when compared with data from its 2001 annual report. Complaint submissions for 2009 were 336,655, a 22% increase from 275,284 in 2008, and a 63% increase from 206,884 complaints in 2007.

CYBERCRIME IS ON THE RISE

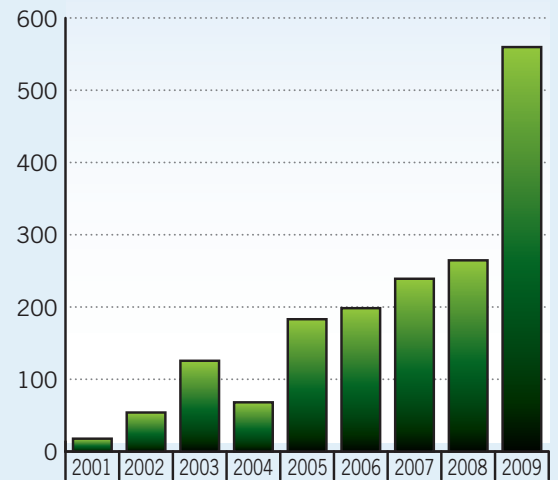
This total of criminal complaints includes many different types, including both fraudulent and nonfraudulent crimes. Yet research indicates that only one in seven incidents of fraud ever makes its way to the attention of enforcement or regulatory agencies. The dollar loss from all cases of crime referred to law enforcement totaled \$559.7 million, a 112% increase from \$264.6 million in 2008.¹³

A Snapshot of Cybercrime in America¹⁴

Complaints Received



Dollar Loss (in millions)



Anyone who uses the Internet is susceptible to offenses such as credit card fraud or the theft of IP. The cost of attack is relatively low for criminals, and the payoff is high. The goal for businesses is to raise the sophistication of your cybersecurity practices to increase the price of success for your adversaries.

INTERNET SECURITY FUNDAMENTALS



Every desktop PC, laptop, or handheld digital device can be vulnerable to attack. The consequences of such an attack can range from simple inconvenience to financial catastrophe. The U.S. Chamber suggests that owners, managers, and employees take a number of actions described in this guide to improve the cybersecurity of their companies. Of the many points that a guide could cover, we've selected a dozen that many experts tend to emphasize and have packaged them under three buckets: workforce, policies and problems, and prevention and preparedness.^{15, 16}

Workforce

Educate your workforce

Employee education is job number one—technology alone will not secure your organization and its information assets. The security of your computers and data is crucial for your employees as well as your company. Lost or stolen information can reveal company secrets or expose your confidential or personal information. Raise Internet security awareness through a brown-bag lunch, employee newsletters, internal e-mails, or your company's Intranet. Here are some top points to stress:

- Think before you share sensitive business or customer information.
- Look for signs that a webpage is safe before you enter sensitive data—e.g., a web address with [https](https://) (“s” for secure) and a closed padlock (🔒) beside it.

- Never give sensitive information in response to an e-mail or instant message (IM) request.
 - Think before you click on attachments or links in e-mail or IM. Confirm that you know the sender and are expecting the attachment.
 - Ensure that the link is legitimate by typing the official website address yourself, as e-mails can be forged.
- Be wary of clicking links or buttons in pop-up windows.
- Recognize e-mail hoaxes, such as phishing scams. Phishing scams entice e-mail recipients into clicking on a link that takes them to a bogus website, which may prompt them to provide Social Security, bank account, or credit card numbers, or it may download malicious software onto their computers. Both the link and website may appear authentic. However, they are not legitimate.
- Look out for alarmist messages, misspellings, deals that sound too good to be true, requests for sensitive information such as account numbers, and other signs of a scam.¹⁷
- Turn on pop-up blockers that help warn you of suspicious websites.

Download Free Internet Safety Toolkit



Microsoft's Internet Safety at Work toolkit teaches employees how to protect company information, customer data, and their own personal information. You can download the toolkit at www.uschamber.com/cybersecurity.

For printed copies of these resources, e-mail saferweb@microsoft.com. The Internet Safety at Work toolkit contains the following resources:



Internet Safety Toolkit Instructions

A guide to using the resources in the toolkit.



Internet Safety at Work PowerPoint Presentation

20-slide presentation with speaker notes.



Tip Cards: Top Tips for Internet Safety at Work Presentation

Information condensed into a printable, double-sided card.



Video: "Stay Sharp on Internet Safety at Work"

Presentation information condensed into a 3-minute video.



Quiz: Test Your Internet Safety IQ

Printable 10-question quiz to help spread awareness among your employees.

INTERNET SECURITY FUNDAMENTALS

Designate a person to handle security and preparedness

This role may be part time or full time depending on the scope and complexity of your business operations. The person in this position performs a number of functions:

- Determines which information assets require protection, maintains an inventory of the computer equipment needed to fulfill critical business functions in case of a disaster, and develops a plan for responding to cybersecurity incidents.¹⁸
- Is aware of regulatory requirements and guidance documents regarding data security and reviews the Federal Trade Commission's (FTC's) guide for protecting personal information at www.ftc.gov/infosecurity.

Learn to Spot Phishing Scams—Don't Get Hooked

- ➔ Phishing attacks are perpetrated through Internet-connected devices like PCs and handheld computers. The Anti-Phishing Working Group, an industry and law enforcement association focused on eliminating the fraud and identity theft that result from phishing and related scams, offers educational materials at www.antiphishing.org.
- ➔ Various consumer alerts, tips, and fraud trends can be accessed at www.lookstoogoodtobetrue.com, a website developed to equip people with information so that they do not fall victim to Internet scam artists.

Use strong passwords

Passwords provide the first line of defense against unauthorized access to your computer. Weak passwords make it easier for attackers to access your computers and network. Strong passwords are considerably harder to crack, even with the latest password-cracking software.

- Strong passwords have the following characteristics:
 - Have at least eight characters.
 - Do not contain your user name, real name, Social Security number, company name, or a complete dictionary word.
 - Contain upper and lower case letters, numbers, and symbols (!, @, #, \$, %, etc.).
 - Are not used for multiple accounts or computers.
- Keep passwords and PINs secret. Don't disclose them to co-workers or businesses (e.g., an Internet cafe operator), and don't get tricked into giving them away.
- Change your computer and banking logins and other important passwords at regular intervals, such as every 90 days.
- Set your computer to hibernate or go into sleep mode, requiring a password to unlock it, when you step away for more than a few minutes.
- Implement an employee departure checklist for those who are no longer employed by your business to ensure that account termination is performed quickly and efficiently on laptops, mobile phones, and other digital devices.

Take a Quiz. Are These Passwords Strong or Weak?

	WEAK	STRONG
(1) 555.12.999	<input type="checkbox"/>	<input type="checkbox"/>
(2) 06/04/79	<input type="checkbox"/>	<input type="checkbox"/>
(3) Exp3d!ti0us	<input type="checkbox"/>	<input type="checkbox"/>
(4) Amb!anc3	<input type="checkbox"/>	<input type="checkbox"/>
(5) 135781113	<input type="checkbox"/>	<input type="checkbox"/>
(6) MdAw3yoiN	<input type="checkbox"/>	<input type="checkbox"/>

ANSWERS

- (1) **WEAK.** Only numbers, possibly a Social Security number, which criminals can easily find online.
- (2) **WEAK.** A date—birth or anniversary date, for example—can be found by a criminal.
- (3) **WEAK.** Don't use words that you can find in a dictionary in any language (expeditious). Criminals will not be fooled by common look-alike replacements such as "3" for "e."
- (4) **STRONG.** Letters, symbols, numbers, not a word found in the dictionary.
- (5) **WEAK.** Only numbers. Avoid sequences, or repeated numbers, such as 22222222.
- (6) **STRONG.** A sentence that's easy to remember but difficult for others to guess.

- ➔ Eight characters or longer.
- ➔ Take the first letters of this sentence: My daughter Annabelle was 3-years-old in November.
- ➔ Add complexity by mixing upper and lower case letters, symbols, and numbers.



Drop the Data


In 2008, the U.S. Chamber and Visa, along with participating local chambers of commerce, spearheaded Drop the Data—a nationwide tour in multiple cities designed to make businesses aware of the risks of retaining prohibited cardholder data and educating them on actionable steps that they can take to avoid storing such data.²⁴ Resources for this campaign are available on a number of websites and answer a number of questions such as, “I’m a merchant, where can I get basic information? What steps do I need to take?” While small businesses often lack in-house support for securing their customers’ private information, there are many online resources available to help.



For information on Visa’s Data Security Compliance Program, visit www.visa.com/cisp.



The Payment Card Industry (PCI) Security Standards Council provides a global forum for the ongoing development, enhancement, storage, dissemination, and implementation of security standards for account data protection. To learn more and see how your business can contribute, visit www.pcisecuritystandards.org.



For a list of point-of-sale payment applications compliant with the Payment Application Data Security Standard (PA-DSS), go to www.pcisecuritystandards.org/security_standards/vpa.



See the Resources for Merchants & Service Providers link at www.pcisecuritystandards.org.

PASSWORD



Some Examples of Data Security Requirements and Standards¹⁹

→ **Fair Credit Reporting Act (FCRA)**—This law is designed primarily to protect the privacy of what it calls “consumer report” information—the details in a consumer’s credit report. In your files, you may have consumer reports on your employees if you’ve done background checks or you’ve needed to look into customers’ credit histories. You have a legal obligation to keep this information secure when it’s in your possession.

But what happens when you no longer have a legitimate business need to keep this consumer report information or want to pitch files? The FTC has issued a rule—called the Disposal Rule—requiring companies to exercise care when pitching consumer reports or information. The rule requires businesses that have information covered by the FCRA to take reasonable measures when they dispose of it.

→ **State data breach notification laws**—As concerns over identity theft and data security have increased, 46 states, the District of Columbia, Puerto Rico, and the Virgin Islands have enacted legislation requiring notification of security breaches involving personal information.²⁰

→ **Gramm-Leach-Bliley Act (GLBA)**—Also known as GLB, this law applies to financial institutions, broadly defined. It applies to businesses, including car dealers, tax preparers, and even courier services, engaged in a wide range of financial activities. Businesses that are financial institutions and are not regulated by other agencies such as the Federal Deposit Insurance Corporation may fall within the FTC’s Safeguards Rule. This rule requires businesses to have reasonable policies and procedures to ensure the security and confidentiality of customer information.²¹

→ **Health Insurance Portability and Accountability Act (HIPAA)**—HIPAA applies to health data. The HIPAA Security Rule specifies a series of administrative, physical, and technical safeguards for covered entities, such as health care plans, providers, and clearinghouses to ensure the confidentiality, integrity, and availability of electronic protected health information.²²

→ **Payment Card Industry Data Security Standards (PCI DSS)**—The PCI DSS is a set of comprehensive requirements for enhancing payment account data security. It was developed by the founding payment brands of the PCI Security Standards Council, including Visa, to help facilitate the broad adoption of consistent data security measures globally.²³




Control network access

One of the best and easiest ways to protect your network is to limit the sites that employees can visit and what they can download and install onto a system. To decrease the chance of an employee navigating to a malicious site or downloading a virus-laden program, consider creating a system administrator account. This account allows you to do the following:

- Take control of your network. Create a system administrator account with administrative privileges that only you or your system administrator has access to. This enables you to operate as the “traffic cop” of your network, where you can monitor all Internet traffic and control who has access to your network. You can also manage any media downloaded or installed onto your computer(s).
- The system administrator account is used to determine the rules for your network. Once set up and configured, the account only needs to be accessed for updates and new software installation. The account is not meant to be used for day-to-day transactions.
- Go to www.microsoft.com/windowsxp/using/setup/winxp/accounts.mspx for guidance on creating and customizing user accounts.




Symptoms of an Infected Computer




A computer may have been compromised if it exhibits any of the following characteristics or signs:

- Is slow or nonresponsive.
- Shows signs of a high level of activity on the hard drive that is not the result of anything you initiated.
- Displays messages on your screen that you haven't seen before.
- Is unable to run a program because you don't have enough memory.
- Crashes constantly.



Your business may be experiencing a cybersecurity incident if it shows any of the following:

- Finding e-mail refused (bouncing back).
- No longer receiving any e-mail for visitors to your website.
- Receiving complaints from users that their passwords don't work anymore.
- Getting complaints from the users that the network has slow response time.²⁵



Ask your Internet service provider if it provides a cost-effective suite of services that will enhance your business' cybersecurity.



Policies and Problems

Identify and prioritize your business' information

Most organizations view cybersecurity as an IT problem that can only be handled by the organization's IT Department. A view of cybersecurity solely as an IT function keeps it from being recognized and treated as an issue impacting an entire organization. Cyber risks cannot be eliminated totally, but a business can substantially reduce the negative consequences of a successful cyber incident by minimizing its vulnerabilities and deterring adversaries through basic risk management.²⁶ Businesses need to recognize the importance of online security and build it into the culture of their organization.

- Small businesses should organize the information they keep, know where it is stored, and prioritize by level of importance—think of this process as information security triage.
- Define “information type” in any way that makes sense to your business. Sometimes small business owners or managers say, “We don’t have any sensitive stuff to protect,” which is more a function of feeling busy, rather than truly believing that their data are adequately safe and secure. Small businesses have an array of information—personnel records, blueprints, tax forms, customer orders, credit reports, and customer payment records—that require protection.



Example of a Risk Assessment Table²⁷

Information type	Personnel records
Media type or storage location(s)	Desktop
Value (high, medium, low)	High
Risk level (high, medium, low)	High (identity theft)
Put data on a stand-alone computer?	Under consideration
Notes (explain major risks and costs)	Have a high value to the business for reporting, payroll, etc.

- Identify the digital and physical locations of business data. Being aware of the information that's present within your business, which employees have access to it, where it goes, and whether it is connected to the Internet—which increases its chances of being stolen or corrupted—is critical to its protection.
- Consider what data can be separated or segmented on the network or put on a stand-alone computer so that it's not immediately and easily accessible to bad actors.
- Create a simple table for all your business information types. List the information asset and where it's stored. Assess its value and chance for loss.²⁸



Defend company computers

Running a small business can leave little time for practicing good cybersecurity. Wherever possible, set your computer to automatically check for updates. Ensure that all software is current, including your web browser. Take time to install security updates from all vendors if they cannot be done automatically.

- Keep *all* software current. For those businesses using Microsoft products, Microsoft Update (<http://update.microsoft.com/microsoftupdate>) provides downloads for Windows, Office, and other Microsoft applications all in one place.²⁹
- Activate the firewall on all company computers—a firewall is not a substitute for anti-virus software. A beginner's guide to firewalls can be found at www.msisac.org, compliments of the Multi-State Information Sharing and Analysis Center (MS-ISAC).³⁰
- Establish an acceptable use policy for the use of information resources and IT systems. For example, confidential or sensitive business information should not be posted by employees on social networking sites such as Facebook or MySpace. An Internet and acceptable use template to help business and office managers craft their own policies can be found at www.msisac.org.³¹

- The FTC warns that peer-to-peer (P2P) file sharing can pose serious risks to your company's information infrastructure. If business owners or managers are asked, "What's your company's policy on P2P file sharing?" the only wrong answer is, "We don't have one." Whether you decide to ban P2P file sharing, it's important to create a policy and take the necessary steps to implement and enforce it. A primer on P2P file sharing can be found at <http://ftc.gov/bcp/edu/pubs/business/idtheft/bus46.pdf>.

Dispose of media safely and securely

Hard drives and other disposable computer equipment may contain saved information even if that information has been "deleted." Information that is deleted from a computer may be retrieved by using forensics or other recovery tools. As new computers are purchased, older computers may be redeployed or discarded. It must be assumed that at some point sensitive information may have been stored and is still retrievable from all electronic storage media, such as computer and network hard drives, external hard drives, CDs, DVDs, floppy disks, tapes, thumb drives, and mobile phones.

- Run a utility program that can overwrite, or wipe, the hard drive so that data are no longer recoverable. The Center for Magnetic Recording Research (CMRR), affiliated with the University of California, San Diego, provides free software known as Secure Erase (<http://cmrr.ucsd.edu/people/Hughes/SecureErase.shtml>) that should be suitable for some basic data destruction needs. Secure Erase has been approved by the National Institute for Standards and Technology (NIST). CMRR does not provide technical support for this program.
- If you have data that require more "lethal" methods, seek help from organizations that offer demagnetization (a.k.a. degaussing) or physical destruction.
- Be sure to get rid of computer data in a way that follows best practices and is consistent with legal requirements. A nontechnical guide on erasing information and disposing of electronic media can be accessed at www.msisac.org.³²



Have a plan to address cyber incidents

Has your system been compromised? How did it happen? What do you do? At some point, your business may experience an information security incident if it hasn't already, and the incident may jeopardize your computer security. Fast and efficient responses can lead to quick recovery, minimize damage, and help prevent future incidents. All end users should be familiar with symptoms that may indicate an incident and need to know what to do.

- Take infected or compromised equipment out of service as soon as practical to prevent further harm.
- Tell management and other users, as appropriate, based on your organization's cybersecurity policy.
- Fix the problem and restore the compromised equipment to service. If you don't have an IT contractor, take your device to a local IT merchant for servicing. Consult your local chamber of commerce for recommendations.
- Consider notifying your partners with whom you connect.
- Reassess your security policy and practices to determine what lessons can be learned from the cybersecurity incident to help you strengthen your cybersecurity practices.

- Contact your local law enforcement authorities if you suspect a crime has been committed. Similarly, work with law enforcement authorities who contact you because they suspect nefarious activity on your network. Cybercrime is not “somebody else’s problem.” Threats on the computers of one business can easily spill over to yours and vice versa.
- Learn more about what to do if you suspect your computer has been hacked or infected by a virus at www.staysafeonline.org, made available by the National Cyber Security Alliance. Also, a model cyber security incident response guide can be accessed at www.msisac.org.³³ It describes how businesses can recover from an incident in a timely and secure manner and minimize consequences on your organization and business partners.

Know the Information That Goes Into a Complaint or Incident Report

Incident reporting organizations such as the Internet Crime Complaint Center (IC3) accept online Internet crime complaints from either the person who believes that he or she was defrauded or from a third party to the complainant. The IC3 requests that you provide the following information when filing a complaint:

- Your name.
- Your mailing address.
- Your telephone number.
- The name, address, telephone number, and web address, if available, of the individual or organization you believe defrauded you.
- Specific details on how, why, and when you believe you were defrauded.
- Other relevant information necessary to support your complaint.



Prevention and Preparedness

Defend your data on the go

- Assess how mobile your workforce is. Risks may rise as your workforce becomes more mobile or is increasingly accessing wireless (Wi-Fi) hot spots.³⁴
- Do not expect privacy in Internet cafes, hotels, offices, or public places when traveling.
- Information that you send electronically can be intercepted. Wireless devices are particularly vulnerable. When your employees use public Wi-Fi, consider requiring them to choose the most secure option even if it comes with a cost; it should include password protection and encryption.
- Confirm the exact spelling of the wireless network you're connecting to. Be aware of clever (slightly misspelled) fakes.
- It sounds like common sense, but keep an eye on your electronic devices when going through airport screening. Research suggests that 10% of laptop thefts occur in airports. Avoid transporting devices in checked baggage.³⁵
- Tips from the National Counterintelligence Executive, which is part of the Office of the Director of National Intelligence, on traveling securely overseas with your mobile phones, laptops, and other electronic devices are available at www.ncix.gov/publications/reports/traveltips.pdf.

Encrypt business sensitive information

You keep valuable and sensitive data on your computer. You may have sensitive information about your company or clients or your personal bank statements on a laptop you use at home and at work. Encrypting folders and files can protect them from unwanted access. To help keep unauthorized people from accessing your data—even if your computer is lost or stolen—you should encrypt all sensitive data. We recommend that you encrypt data on all computers and storage devices, including removable storage devices and drives.³⁶

- Ensure that business sensitive information, whether it's located on a laptop or flash drive, is properly encrypted.
- There are numerous programs that encrypt data, such as Microsoft's BitLocker Data Encryption, which is included with certain versions of Windows.
- For information on how to encrypt data on a Windows operating system, visit <http://windows.microsoft.com/en-us> and select the corresponding version of Windows.³⁷





Back up your computer data regularly

Our computers contain vast amounts of data in a variety of forms—from family photos and music collections to several years' worth of financial records and personal contacts. There are many risks to our data, such as hardware or software malfunctions, natural disasters, emergencies, floods, hurricanes, tornadoes, house fires, and theft. But viruses, spyware, and cyberattacks are also externally launched events that can lead to data loss and can either destroy your computer or render it useless. Not only large events cause data loss. Important files can be lost by accidental deletion too.

- Protect yourself against data loss by making electronic copies of important files, commonly referred to as a backup. Data backup is a simple, three-step process:
 - (1) Make copies of the data on your computer(s).
 - (2) Select the appropriate hardware to store the backup data.
 - (3) Safely store the backup device that holds your copied files.
- For guidance on conducting these steps, click on “Backup important files” at www.staysafeonline.org.
- Train your staff to perform regular backups of files, applications, or entire computer systems at least daily; test the backup and recovery process periodically to be sure it works.

INTERNET SECURITY FUNDAMENTALS



- Computer equipment needs to be physically protected from both security threats and natural hazards. Complete a list of the computer equipment, hardware, and software that you will need to fulfill your critical business functions in case of an emergency, ranging from an accidental storeroom flood to a tornado. A helpful guide, compliments of the Institute for Business & Home Safety, is available at www.disastersafety.org/business_protection.³⁸
- Additional how-to suggestions for backing up data can be found at www.msiscac.org³⁹ and at www.microsoft.com/windows/windows-7/features/backup-and-restore.aspx.

NATIONAL CYBERSECURITY AWARENESS MONTH

OUR SHARED RESPONSIBILITY
OCTOBER 2010



StaySafeOnline.org



Participate in National Cybersecurity Awareness Month

- Read more about National Cybersecurity Awareness Month and top tips to enhance your online security at www.staysafeonline.org.
- Subscribe to trusted newsletters or sign up to receive free and timely alerts from organizations on new threats and how to protect your section of cyberspace.⁴⁰
- Get to know information security officials and organizations in your community and state. Turn a negative into a positive. Cyber incidents can be opportunities for small organizations to enter into trusted partnerships with local organizations and government officials. For example, you may want to join a local chapter of InfraGard (www.infragard.net). The FBI launched InfraGard nearly 15 years ago to reduce cyber threats to the nation's critical infrastructure. InfraGard is an association of businesses, academic institutions, and state and local law enforcement agencies dedicated to sharing information and intelligence to prevent hostile acts against the United States.

CYBER INCIDENT AND COMPLAINT REPORTING ORGANIZATIONS

OnGuard Online (www.onguardonline.gov; www.alertaenlinea.gov in Spanish)

OnGuard Online offers practical tips on how to protect yourself against Internet fraud, secure your computers, and guard personal information. The site is sponsored by both government, with FTC in the lead, and private sector entities.

- File a complaint with OnGuard Online at www.onguardonline.gov/file-complaint.aspx.

Internet Crime Complaint Center (IC3) (www.ic3.gov)

IC3 was established to receive Internet-related criminal complaints and to research, develop, and refer the criminal complaints to federal, state, local, international law enforcement, or regulatory agencies for further investigation. Since its inception, IC3, a partnership between the FBI and the National White Collar Crime Center (NW3C), has received complaints crossing the spectrum of cybercrime matters, including IP rights matters, computer intrusions (hacking), economic espionage (theft of trade secrets), online extortion, international money laundering, identity theft, and a growing list of Internet-facilitated crimes.

- File a complaint with IC3 at www.ic3.gov/complaint/default.aspx.

United States Computer Emergency Readiness Team (US-CERT) (www.us-cert.gov)

US-CERT is the operational arm of the Department of Homeland Security's (DHS's) National Cyber Security Division (NCSA), which leads a public-private partnership to protect and defend the nation's cyber infrastructure. Partners include industry, academia, federal agencies, information sharing and analysis centers, state and local governments, and international organizations. NCSA was established by DHS to serve as the federal government's cornerstone for cybersecurity coordination and preparedness.

- File an incident report with US-CERT at <https://forms.us-cert.gov/report>.

CONCLUSION: ADD BUSINESS VALUE THROUGH INFORMATION SECURITY



Unlike larger enterprises, which often have specialists, such as a chief information officer or a chief security officer, to manage an array of risks facing businesses, small businesses generally do not have the people and resources for a formal information security program. In today's challenging economy, small businesses are looking for creative ways to make ends meet. Still, regardless of size and resources, the obligation for dealing with threats to a business' information security rests with each person—from CEOs to frontline workers.

Business owners and managers can add value to their enterprises by implementing the suggestions highlighted in this guide, many of which are relatively easy and inexpensive to employ. It's far less expensive to invest in better Internet security than to lose trusted customers and business partners, get enmeshed in legal actions, or face the possible consequences of a security breach.

INTERNET RESOURCES



www.uschamber.com/cybersecurity > U.S. Chamber cybersecurity information

www.visa.com/cisp > Visa Cardholder Information Security Program

www.microsoft.com/security > Microsoft Security—products, updates, tools, and news

www.stopthinkconnect.org > Stop. Think. Connect.—online safety and security education and awareness campaign

www.staysafeonline.org > National Cyber Security Alliance—tools and resources for business and home users

www.msisac.org > Multi-State Information Sharing and Analysis Center (MS-ISAC)—cybersecurity guides, toolkits, and newsletters

www.ftc.gov/infosecurity; <http://business.ftc.gov> > Federal Trade Commission's *Protecting Personal Information: A Guide for Business*; Bureau of Consumer Protection Business Center

<http://csrc.nist.gov/groups/SMA/sbc/index.html> > National Institute of Standards and Technology (NIST), Computer Security Division, Small Business Corner

www.dhs.gov/cyber > U.S. Department of Homeland Security (DHS) National Cybersecurity Awareness Month resources


www.us-cert.gov/cas/tips > United States Computer Emergency Readiness Team (US-CERT) cybersecurity tips

www.justice.gov/criminal/cybercrime > U.S. Department of Justice Computer Crime and Intellectual Property Security Section—links to report Internet-related and intellectual property crime

www.secretservice.gov/ectf.shtml > U.S. Secret Service Electronic Crimes Task Force (ECTF)—links to more than 20 state and local ECTFs

www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf > The White House, *Cyberspace Policy Review: Assuring a Resilient and Trusted Information and Communications Infrastructure*

National and Sector Perspectives



This Internet security guide has focused on small businesses, which drive the U.S. economy. For a complete picture, it's important to take a step back and look at the digital ecosystem from a national perspective, which involves larger businesses, entire sectors, and government players. Too often, the media focus on negative stories—the proverbial car crash during rush hour—to the exclusion of what's positive. Such stories form a significant part of raising public awareness. However, they can easily overlook much of the positive work that various sectors of the economy are undertaking to enhance the computer and network security of the nation's critical infrastructure.

Included here are brief descriptions of the initiatives of a few sectors to guard businesses from interruption, prevent the loss of capital or IP, and protect public safety.

Banking and Financial Services

The banking and financial services sector is complex and diverse—ranging from small community banks and credit unions to large institutions. The sector is estimated to have assets of more than \$60 trillion and accounted for 8.3% of U.S. gross domestic product (GDP) in 2009.⁴¹ While diverse, a unifying goal of the banking and financial services sector is to maintain its operations in the wake of a natural hazard or man-made threats, such as a cyberattack. Industry leaders understand that it is imperative that the sector's information infrastructure be well protected and resilient, enabling customers to entrust their assets to financial institutions and have access to credit.⁴²

CYBERSECURITY: NATIONAL AND SECTOR PERSPECTIVES

Working through public-private partnerships, organizations like the Financial Services Information Sharing and Analysis Center (FS-ISAC) serve to protect the financial services community against an array of risks. The FS-ISAC acts as a trusted third party, allowing members to submit threat, vulnerability, and incident information in a nonattributable manner so that information can be shared for the benefit of the sector and the nation. The sector also undertakes exercises to assess and improve its own capabilities.⁴³ For example, the Chamber helped promote the FS-ISAC's Cyber Attack against Payment Process exercise in February 2010, which tested the financial services industry's ability to respond to different types of cyberattacks. The exercise demonstrated multiple areas in which enterprises could improve their security and reduce their operational risk.⁴⁴

Chemical

The chemical sector is an integral component of the U.S. economy, converting various raw materials into more than 70,000 diverse products, employing nearly 1 million people, and earning revenues of roughly \$664 billion per year. Industry members are highly dependent on IT for their communications and operations. The chemical sector has been a leader in developing methods and processes to address safety and reduce risk. The sector has long recognized its vulnerability to cyberattacks and has viewed cybersecurity as an essential aspect of risk reduction. Industry activities have included development of guides and standards to help improve operational safety and reliability.

In close partnership with DHS officials, the chemical sector has developed a roadmap that describes what is required to improve the cybersecurity of industrial control systems. These control systems were often designed to operate without a connection to a wide area network. However, they are increasingly becoming linked to corporate or business networks, making them potentially vulnerable to common cyberattacks. Several companies have taken voluntary steps to guard their control systems; the roadmap provides a means of sharing these measures across the sector. Implementation of the roadmap by the sector will be coordinated with DHS as well as with those working on similar programs in other critical infrastructure sectors.⁴⁵


Communications

The communications industry, an integral part of the U.S. economy, includes wireline, wireless, satellite, cable, and broadcasting providers. Its infrastructure underlies the operations of businesses, public safety organizations, and government. Over the last 25 years, the communications industry has evolved from a predominantly voice-centric service into a diverse, competitive, and interconnected industry that supports the Internet and other key information delivery systems. Commercial carriers devote considerable resources and expertise toward identifying and mitigating threats on the Internet as they are emerging. They take actions 24/7, as allowed by law, to address spam, phishing, and other malicious activity that threaten to disrupt their own networks or their customers' use of it.

Businesses invest heavily in threat detection and mitigation technologies; they also make strategic research and development investments to tackle emerging and future threats. Furthermore, the communications industry works closely with the government on national security and emergency preparedness issues through partnerships, including providing the president with policy advice through the National Security Telecommunications Advisory Committee⁴⁶ as well as operational support through the National Coordinating Center for Telecommunications (NCC)⁴⁷ and the Communications Information Sharing and Analysis Center (C-ISAC). In addition, the Communications Sector Coordinating Council (CSCC),⁴⁸ established in 2005, acts as the principal entity for coordinating with the government in implementing national infrastructure protection and response plans.

Electric

The use of electricity in the United States is ubiquitous, spanning all sectors of the economy. The electric power industry represents about 3% of U.S. economic output and employs nearly 400,000 American workers. More than 70% of electricity customers are served by shareholder-owned electric companies, which are highly regulated.⁴⁹ In 2009, electric power accounted for nearly 40% of all energy consumed in the United States.^{50, 51} Electric sector owners and operators routinely strive to strengthen the security of their cyber systems and identify and mitigate any network vulnerability.



Protecting the power grid from cyberattacks requires a coordinated effort among industry stakeholders and federal officials. Electric companies work closely with the North American Electric Reliability Corporation, an industry self-regulatory body, and federal agencies to enhance the cybersecurity of the bulk power system. This includes coordinating with the Federal Energy Regulatory Commission,⁵² DHS, and the Department of Energy. A signature public-private effort includes the development of the *Roadmap to Secure Control Systems in the Energy Sector* to help focus and make actionable various security initiatives.⁵³ In addition, the electric industry has contributed to the *Smart Grid Cyber Security Strategy and Requirements* framework to ensure that cybersecurity protections are incorporated into both the grid architecture and the new smart grid technologies.⁵⁴

Information Technology

The IT sector accounts for roughly 7% of U.S. GDP. The industry is made up of companies that provide the key functions—including IT products and services, Internet routing and switching, Internet-based content, domain name resolution, identity management, and incident response—that enable the efficient operation of today's information-based society. For example, facilitated by IT systems, more than \$3 trillion worth of economic activity flow over secure federal financial networks daily. Threats to the IT industry are complex and varied, ranging from natural hazards, such as destructive storms, to man-made threats, such as individual hackers, criminal syndicates, or politically motivated actors.⁵⁵

For more than a decade, the IT sector has worked with public sector security partners to maximize the security and resilience of the global information infrastructure. In August 2009, IT sector professionals and government officials produced a baseline assessment of the myriad risks that the industry faces daily to inform owners and operators about resource allocation and various protective measures.⁵⁶ IT sectors members, along with those of other critical infrastructure

CYBERSECURITY: NATIONAL AND SECTOR PERSPECTIVES

sectors, are contributing to the nation's National Cyber Incident Response Plan, which will guide how the nation responds to significant cyber incidents. This plan, tested in September 2010 as part of DHS's biennial national cyber exercise, Cyber Storm, will help the nation prepare for and respond to the effects of a major cyberattack.⁵⁷

The IT Sector Coordinating Council (IT SCC) brings together companies, associations, and other key IT participants on a regular basis to coordinate strategic activities and communicate sector member views on infrastructure protection, response, and recovery. The IT SCC also serves as the base of IT sector representation to the Partnership for Critical Infrastructure Security, which is formally recognized by the U.S. government as the Cross-Sector Council under the U.S. National Infrastructure Protection Plan. The IT SCC engages with its government partners to convey the perspectives of the private sector on a wide range of national cyber and physical infrastructure policy and operational issues.⁵⁸ Similarly, the IT-Information Sharing and Analysis Center draws upon the collective knowledge and capabilities of its members to identify threats and vulnerabilities to IT infrastructure, respond to incidents and attacks through real-time analysis, and provide timely recommendations for corrective actions.⁵⁹

ACKNOWLEDGEMENTS

The U.S. Chamber of Commerce would like to thank members of its National Security Task Force as well as the National Cyber Security Alliance and the Multi-State Information Sharing and Analysis Center for contributing to the content of this guide.

Gold Sponsor



Silver Sponsor



Bronze Sponsor



ENDNOTES

1. President Barack Obama, "Remarks by the President in Securing Our Nation's Cyber Infrastructure," May 29, 2009, www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure.
2. U.S. Department of Commerce Secretary Gary Locke, "Remarks at Cybersecurity Policy Review Meeting," July 14, 2010, at www.commerce.gov/news/secretary-speeches/2010/07/14/remarks-cybersecurity-policy-review-meeting.
3. Federal Communications Commission, *Connecting America: The National Broadband Plan* (2010); see www.broadband.gov/plan/3-current-state-of-the-ecosystem, or <http://download.broadband.gov/plan/national-broadband-plan-chapter-3-current-state-of-the-broadband-ecosystem.pdf>.
4. U.S. Small Business Administration, "Frequently Asked Questions," <http://web.sba.gov/faqs/faqindex.cfm?arealD=24>.
5. See Aug. 10, 2010, press release by the National Cyber Security Alliance and the Anti-Phishing Working Group. The release is available at <http://staysafeonline.mediaroom.com/index.php?s=43&item=62>. The poll was conducted as part of a public-private Smokey Bear-style national messaging convention to promote cybersecurity awareness among members of the general public.
6. The language on common threats to business derived from Verizon Business RISK Team's 2008, 2009, and 2010 data breach investigation reports, which can be accessed, respectively, at www.verizonbusiness.com/resources/security/databreachreport.pdf, www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf, and www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf.
7. The eighth volume of Microsoft's *Security Intelligent Report* covers trends in security breaches (www.microsoft.com/security/about/sir.aspx); see pp. 50–53.
8. Office of the National Counterintelligence Executive, *Networked Information Systems* booklet; see section on insider threat at www.ncix.gov/publications/booklets_brochures/booklet_NISprotect_product/booklet_NISprotect_p1.html.
9. Red Cross Ready Rating Program, "The Reality of Preparedness," www.readyrating.org/Join/TheRealityofPreparedness.aspx.
10. Example of the wood furniture company provided by Dr. James A. Lewis, Director and Senior Fellow, Technology and Public Policy Program, Center for Strategic and International Studies. See his testimony from a Feb. 23, 2010, Senate hearing on cybersecurity and critical infrastructure, available at http://commerce.senate.gov/public/index.cfm?p=Hearings&ContentRecord_id=a676548f-a2a7-40ff-a18d-889a7907801c&ContentType_id=14f995b9-dfa5-407a-9d35-56cc7152a7ed&Group_id=b06c39af-e033-4cba-9221-de668ca1978a&MonthDisplay=2&YearDisplay=2010. Also, in the

- Sept./Oct. 2010 issue of *Foreign Affairs*, a top Pentagon official writes that while “the threat to intellectual property is less dramatic than the threat to critical national infrastructure, it may be the most significant cyberthreat that the United States will face over the long term” (p. 100); see www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain.
11. Ramona R. Rantala, *Cybercrime against Business, 2005*, U.S. Department of Justice, Bureau of Justice Statistics, Sept. 17, 2008, <http://bjs.ojp.usdoj.gov/index.cfm?ty=pbdetail&iid=769>, p. 7.
 12. See *Cyberspace Policy Review*, p. 2.
 13. Internet Crime Complaint Center (IC3), *2009 Internet Crime Report*; see Mar. 12, 2010, IC3 press release and report, respectively, at www.ic3.gov/media/2010/100312.aspx; www.ic3.gov/media/annualreport/2009_IC3Report.pdf.
 14. *Ibid.*
 15. FEMA, Ready Business, “Improve Cyber Security,” www.ready.gov/business/protect/cybersecurity.html.
 16. A “getting started” guide on cybersecurity, from which this guide borrows many recommendations, is available from the Multi-State Information Sharing and Analysis Center (MS-ISAC) at www.msisac.org/awareness/documents/Getting%20Started%20Guide.pdf (*Getting Started*).
 17. The Internal Revenue Service (IRS) has warned the public about an Internet scam in which consumers receive an e-mail informing them of a tax refund. The e-mail, which claims to be from the IRS, directs the consumer to a link that requests personal information, such as Social Security number and credit card information. This scheme is an attempt to trick the e-mail recipients into disclosing their personal and financial data. The practice is called “phishing” for information. The information fraudulently obtained is then used to steal the taxpayer’s identity and financial assets. Generally, identity thieves use someone’s personal data to steal his or her financial accounts, run up charges on the victim’s existing credit cards, apply for new loans, credit cards, services, or benefits in the victim’s name and even file fraudulent tax returns. IRS information on phishing taken directly from www.irs.gov/newsroom/article/0,,id=151065,00.html.
 18. An MS-ISAC cyber incident response guide is available at www.msisac.org/localgov/documents/FINALIncidentResponseGuide.pdf. See, too, Karen Scarfone et al., *Computer Incident Response Handling Guide*, National Institute for Standards and Technology (NIST), Mar. 2008, at <http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf>.
 19. Language on data security requirements taken from Federal Trade Commission (FTC) webpages www.ftc.gov/bcp/edu/pubs/articles/art08.shtm and www.ftc.gov/bcp/menus/business/data.shtm.
 20. See list of security breach laws at www.ncsl.org/Default.aspx?TabId=13481, including recommended practices on breach notifications by California’s Office of Privacy Protection.

ENDNOTES

21. See FTC webpages www.ftc.gov/privacy/privacyinitiatives/glbact.html, www.ftc.gov/bcp/edu/pubs/articles/art08.shtm, and www.ftc.gov/infosecurity.
22. See U.S. Department of Health and Human Services webpages on the Health Insurance Portability and Accountability Act at www.hhs.gov/ocr/privacy and www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html.
23. The Payment Card Industry (PCI) Security Standards Council, www.pcisecuritystandards.org.
24. Visa-U.S. Chamber of Commerce “Drop the Data” tour online resources, www.visa.com/droptheedata/index.html.
25. MS-ISAC, *Getting Started*, p. 8.
26. See Oct. 31, 2007, testimony of Sally Katzen, who addresses enterprise risk management principles in depth at a House hearing on cybersecurity and sector specific plans. Her written statement is available at <http://hsc.house.gov/hearings/index.asp?ID=100>.
27. For additional information on risk management essentials, see www.msisac.org/awareness/documents/Risk-Management-Guide.pdf, particularly pp. 3, 9.
28. Richard Kissel, *Small Business Information Security: The Fundamentals*, NIST, p. A-1, <http://csrc.nist.gov/publications/nistir/ir7621/nistir-7621.pdf>. Additional worksheets are included in the NIST report, such as one to help businesses estimate other costs (e.g., lost work time, computer repairs, and legal expenses) due to security incidents.
29. Users can opt in to the service when installing software offered through Microsoft Update or at the Microsoft Update website. Microsoft recommends configuring computers to use Microsoft Update instead of Windows Update to help ensure they receive timely security updates for Microsoft products.
30. MS-ISAC, *Beginners Guide to Firewalls*, www.msisac.org/awareness/documents/Firewall%20Guide.pdf.
31. MS-ISAC, *Internet and Acceptable Use Policy Template*, www.msisac.org/awareness/documents/Acceptable%20Use%20Guide.pdf.
32. MS-ISAC, *Erasing Information and Disposal of Electronic Media*, www.msisac.org/awareness/documents/Erasing%20and%20Disposal%20Guide.pdf.
33. MS-ISAC, *Cyber Incident Response Guide*, www.msisac.org/awareness/documents/Incident-Response-Guide.pdf.

34. See, for example, Mary K. Pratt, “Hot spot dangers: That Internet cafe could cost you way more than a cup of coffee,” *Computerworld*, Apr. 20, 2010, www.computerworld.com/s/article/9175780/Hot_spot_dangers_That_Internet_cafe_could_cost_you_way_more_than_a_cup_of_coffee?source=CTWNLE_nlt_security_2010-04-20.
35. Additional tips for increasing the security laptops while traveling are available at www.ftc.gov/bcp/edu/pubs/articles/art07.shtm; www.microsoft.com/atwork/security/laptopsecurity.aspx.
36. The Windows Security Compliance Toolkit (<http://go.microsoft.com/fwlink/?LinkId=160808>) contains step-by-step guidance for deploying BitLocker Drive Encryption and the Encrypting File System (EFS) in enterprise environments. Microsoft recommends using the Data Encryption Toolkit for Mobile PCs to effectively implement BitLocker and EFS for mobile PCs; see <http://technet.microsoft.com/en-us/library/cc500474.aspx>.
37. Learn how to encrypt a file in Windows 7, Windows Vista, and Windows XP, respectively, at <http://windows.microsoft.com/en-us/windows7/Encrypt-or-decrypt-a-folder-or-file>, <http://windows.microsoft.com/en-US/windows-vista/Encrypt-or-decrypt-a-folder-or-file>, and <http://www.microsoft.com/windowsxp/using/security/learnmore/encrypt-data.msp>.
38. See Institute for Business & Home Safety’s “Computer Equipment and Software” inventory form at www.disaster-safety.org/resource/resmgr/PDFs/10_-_Computer_Equipment___So.pdf.
39. MS-ISAC, *Guidelines for Backing Up Information*, www.msisac.org/awareness/documents/Backing-Up-Information-Guide.pdf.
40. For example, the MS-ISAC provides cybersecurity newsletters monthly. Sign up at www.msisac.org/awareness/news/. Business managers and IT professionals may want to sign up for Microsoft technical security notifications at <http://technet.microsoft.com/en-us/security/default.aspx> or <http://technet.microsoft.com/en-us/security/dd252948.aspx>.
41. See Insurance Information Institute, “Financial Services at a Glance,” <http://www2.iii.org/financial/fsataglance/ataglance>.
42. U.S. Departments of Homeland Security (DHS) and Treasury, *Banking and Finance Sector-Specific Plan*, May 2007, www.dhs.gov/xlibrary/assets/nipp-ssp-banking.pdf.
43. See Sept. 14, 2009, testimony of the Financial Services-Information Sharing and Analysis Center’s William Nelson from a Senate hearing on protecting industry from cyber threats, http://hsgac.senate.gov/public/index.cfm?FuseAction=Hearings.Hearing&Hearing_ID=c643f97a-0814-4770-8121-ba20ce4d90db.
44. A summary of the Cyber Attack against Payment Process exercise is available at www.fsisac.com/files/public/db/p243.pdf.

ENDNOTES

45. DHS, *Roadmap to Secure Control Systems in the Chemical Sector*, Sept. 2009. For an electronic copy of this document, send an e-mail request to ChemicalSector@dhs.gov.
46. National Communications System, www.ncs.gov/nstac/nstac.html.
47. National Coordinating Center for Telecommunications, www.ncs.gov/ncc.
48. U.S. Communications Sector Coordinating Council, www.commscc.org.
49. Edison Electric Institute, "About the Industry," www.eei.org/whoweare/AboutIndustry.
50. DHS and U.S. Department of Energy (DOE), *Energy Sector-Specific Plan*, May 2007, www.dhs.gov/xlibrary/assets/nipp-ssp-energy-redacted.pdf.
51. U.S. Energy Information Administration, *Annual Energy Review 2009*, Figure 2.1a, Energy Consumption by Sector Overview, www.eia.doe.gov/emeu/aer/pdf/pages/sec2_4.pdf.
52. In Jan. 2008, the Federal Energy Regulatory Commission approved eight Critical Infrastructure Protection standards, which were developed by the North American Electric Reliability Corporation, to require certain users, owners, and operators of the bulk power system to protect America's grid from cyberattacks and other reliability breaches. At the time of writing, an industry drafting team is working diligently on changes to strengthen these standards.
53. DOE, "Control Systems Security," www.oe.energy.gov/controlsecurity.htm.
54. See NIST, "Smart Grid Interoperability Standards Project," www.nist.gov/smartgrid/index.cfm or <http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7628>.
55. DHS et al., *Information Technology Sector-Specific Plan*, May 2007, www.dhs.gov/xlibrary/assets/nipp-ssp-information-tech.pdf.
56. DHS et al., *Information Technology Sector Baseline Risk Assessment*, Aug. 2009, www.dhs.gov/xlibrary/assets/nipp_it_baseline_risk_assessment.pdf.
57. DHS, "Cyber Storm: Securing Cyber Space," www.dhs.gov/files/training/gc_1204738275985.shtm.
58. For more information about the IT Sector Coordinating Council, visit www.it-scc.org.
59. For more information about the IT-Information Sharing and Analysis Center, visit www.it-isac.org.



Copyright © 2010 by the United States Chamber of Commerce. All rights reserved. No part of this publication may be reproduced or transmitted in any form—print, electronic, or otherwise—without the expressed written permission of the publisher.



U.S. CHAMBER OF COMMERCE
1615 H Street, NW, Washington, DC 20062
www.uschamber.com
cybersecurity@uschamber.com

Gold Sponsor



Silver Sponsor

Bronze Sponsor

