Internet Security Essentials for Business 2.0

THE SPIRIT OF ENTERPRISE
U.S. CHAMBER OF COMMERCE
1912–2012

Bank of America

Microsoft

splunk>

VISA

STOP | THINK | CONNECT™

The STOP. THINK. CONNECT. messaging convention is a public-private partnership established in 2009. It is led by the Anti-Phishing Working Group (APWG) and the National Cyber Security Alliance (NCSA) to develop and support a national cybersecurity awareness campaign. The Department of Homeland Security (DHS) provides the federal government's leadership for the campaign. Industry, government, nonprofits, and education institutions participate in STOP. THINK. CONNECT. Learn how to get involved at the STOP. THINK. CONNECT. Facebook page at **www.facebook.com/STOPTHINKCONNECT**, on Twitter at **@STOPTHNKCONNECT**, and on the campaign website at **www.stopthinkconnect.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.

TABLE OF CONTENTS

INTRODUCTION:
STRONG SECURITY IS SMART FOR

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.[1] 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 *National Broadband Plan* estimates that 97% of small businesses use email and 74% have a company website.[2] 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.[3]

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 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.[4]

BUSINESS AND THE NATION

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 help improve the security of information, computers, and networks as well as bolster a company's resilience.
- Give businesses of all sizes simple steps necessary to help 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 games. The United States' competitiveness and security depend on it.

COMMON THREATS TO BUSINESS

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 company, employee, and customer data, money, or intellectual property from businesses are increasing in scope and sophistication. Some businesses are good at changing their approaches 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 common weaknesses in an application or operating system software to gain unauthorized access.

The use of the word "hacking" has a lengthy history. The word "hacker" once meant "computer nerd"—a relatively benign connotation. Today, "good" hackers are sought after by governments and companies to employ their skills to root out security flaws in computer programs and to counter cyberattacks by "bad" hackers, or cybercriminals.[5]

Malware, such as self-replicating email 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 the target of cybercriminals.[6]

INFORMATION

Security experts suggest that the number of websites infected by malicious software installed by hackers nearly doubled between 2009 and 2010, when this guidebook was first published. In three months of surfing the Web, the average computer user has a 95% chance of visiting a malware-infected site.[7]

Lost or Stolen Physical Storage Media

Equally important as hacking and malware, devices such as laptops, Universal Serial Bus (USB) flash drives, smart phones, hard drives, and CDs/DVDs fall into this category.[8] They can carry a lot of information, so ensure that they do not get lost or misplaced. Also, take additional security measures, including setting passwords to access the device and using encryption to secure stored data. 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—has not gone away. 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.[9]

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 emailing sensitive information to the wrong person or to someone who has forged an email account, employees lacking awareness of good cybersecurity practices can give hackers easy access to a system. Fraudsters may seek to gain access to your organization's sensitive information or access your systems by abusing the trust of an unsuspecting employee—a tactic known as "social engineering."

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.[10] 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 ON THE RISE

Cybercrime in the United States is on the rise at troubling rates. As the personal and professional lives of individuals are more and more interwoven with the Internet and cyberspace, thieves have logically followed the action online.

It is not easy to get a complete picture of Internet crime. However, organizations such as the Internet Crime Complaint Center (IC3), a partnership established in 2000 between the FBI and the National White Collar Crime Center, provide a window into a concerning trend.

According to the latest IC3 *Internet Crime Report,* 2011 marked the third year in a row that the IC3 received more than 300,000 complaints. The 314,246 complaints represent a 3.4% increase over 2010. Today, IC3 accepts more complaints in a single month (approximately 26,000) than it received in its first six months. The reported dollar loss in 2011 was $485.3 million—a significant jump from $17.8 million in 2001. The most common victim complaints included FBI-related scams, identity theft, and advance fee fraud.[11]

As more Internet crimes are reported by individuals and businesses, IC3 can better assist law enforcement in apprehending and prosecuting those responsible. Gordon M. Snow, assistant director of the FBI's Cyber Division, encourages people to report Internet crime through the IC3 Web portal (**www.ic3.gov/default.aspx**). It is a unique resource for federal, state, and local law enforcement officials to accept cases efficiently, identify patterns in what otherwise appear to be isolated incidents, and combine multiple smaller crime reports into larger, higher priority cases.[12]

A Snapshot of Cybercrime in the United States

Year	Complaints received	Dollar loss (in millions)
2011	314, 246	$485.3
2010	303,809	NA
2009	336,655	559.7
2008	275,284	264.6
2007	206,884	239.1
2006	207,492	198.4
2005	231,493	183.1
2004	207,449	68.1
2003	124,515	125.6
2002	75,064	54.0
2001	50,412	17.8

Anyone who uses the Internet is susceptible to offenses such as payment card fraud or identity theft scams. The cost of attack is relatively low for criminals, and the payoff can be high. Businesses need to raise the sophistication of their cybersecurity practices to increase the price of success for adversaries. Some of the top crimes are listed at left, along with links to preventative measures (too lengthy to cover here in detail) for conducting transactions more securely over the Internet. All of the Internet crime prevention tips are available online at **www.ic3.gov/preventiontips.aspx**.

- Auction Fraud
- Counterfeit Cashier's Check
- Credit Card Fraud
- Debt Elimination
- DHL/UPS
- Employment/Business Opportunities
- Escrow Services Fraud
- Identity Theft
- Internet Extortion
- Investment Fraud
- Lotteries
- Nigerian Letter or "419"
- Phishing/Spoofing
- Ponzi/Pyramid
- Reshipping
- Spam
- Third-Party Receiver of Funds

INTERNET SAFETY AND SECURITY FUNDAMENTALS

Every desktop computer, 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 about a dozen that many experts tend to emphasize and have packaged them under four broad categories: set up a secure system, protect business data, train your workforce, and be prepared to respond to an incident.[13]

Set Up a Secure System

1. 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.[14]
- Is aware of regulatory requirements and guidance documents regarding data security and reviews the Federal Trade Commission's (FTC) guide for protecting personal information at **www.ftc.gov/infosecurity**.

Examples of Common Cybersecurity and Data Security Requirements and Standards[15]

SEC Cybersecurity Disclosure Guidance—In October 2011, the SEC's Division of Corporation Finance issued guidance for public companies about disclosure obligations relating to cybersecurity risks and cyber incidents (deliberate attacks or unintentional events). The guidance does not modify or create new SEC rules or regulations; it discusses how companies, both domestic and foreign, may consider cybersecurity matters when preparing disclosures in periodic SEC reports and registration statements. The guidance also highlights potential financial statement implications (e.g., known and potential costs of cyberattacks).[16]

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.[17]

Gramm-Leach-Bliley Act (GLBA)—Also known as GLBA, this law applies to financial institutions, broadly defined. It applies to businesses such as 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 like 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.[18]

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 use to ensure the confidentiality, integrity, and availability of electronic protected health information.[19]

Health Information Technology for Economic and Clinical Health (HITECH) Act—Linked to HIPAA, HITECH creates a federal breach notification requirement for health information that is not encrypted or otherwise made indecipherable. It requires that individuals be notified if there is an unauthorized disclosure or use of their health information.[20]

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.[21]

2. 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, business owners should install a firewall with strong access controls. These important safeguards will help protect your businesses' network from malware, viruses, and other Internet threats. Once you've created a system or network administrator account (which will help you function as the "traffic cop" of your network), you will need to take the following five important steps:

- Implement a firewall. A firewall allows you to control who has access to your network. Once implemented, configure the firewall settings to "deny all" for both inbound and outbound traffic and only allow access to trusted ports and services. (Certain firewalls may have "allow all" as a default setting, which will leave your network vulnerable to employees navigating to potentially harmful sites.)
- Establish what is known as a proxy server, which allows you to control and limit Internet access that is not required for business purposes.
- Have the system or network administrator assign strong passwords and access controls to users and devices on the network.
- Audit your network's connections regularly and eliminate unnecessary or outdated ones.
- Keep your operating systems and software current by installing updates and patches.

NOTE If you use Windows, Microsoft offers guidance on creating user accounts:

For Windows 7:
http://windows.microsoft.com/en-IN/windows7/Create-a-user-account

For Windows Vista:
http://windows.microsoft.com/en-US/windows-vista/Create-a-user-account

For Windows XP:
http://support.microsoft.com/kb/279783

3. Defend company computers

Running a small business can leave little time for practicing good cybersecurity. However, relatively simple actions can help you strengthen your business' systems and devices.

- Keep all software current, including your operating system and Web browser. Take time to install security updates and patches if they cannot be done automatically. For those businesses using Microsoft products, Microsoft Update (**http://update.microsoft.com**) provides downloads for Windows, Office, and other Microsoft applications all in one place.[22]
- Never turn off the firewall on any company computer. (A firewall is on by default in Windows.) A firewall is not a substitute for antivirus 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).[23]
- Install antivirus and antispyware software and keep it up to date. Microsoft offers free protection in Microsoft Security Essentials for small businesses: **http://windows.microsoft.com/en-US/windows/products/security-essentials**. Go to **www.microsoft.com/security/pc-security/protect-pc.aspx** for free computer protection.
- 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." Regardless of your stance on P2P file sharing, it is important as a company to have one and to 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**.

NOTE To learn eight simple ways to help maintain your computer and devices at work, go to **www.microsoft.com/atwork/maintenance/maintain.aspx#fbid=v8auoxLHOxd**.

Protect Business Data

4. Organize business data and assess risk

Most organizations view cybersecurity as an IT problem that can only be handled by the organization's IT department.[24] 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 cyberattack by minimizing its vulnerabilities and deterring adversaries through basic risk management.[25] Businesses need to recognize the importance of online security and build it into the culture of their organizations.

- 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 do not need protecting. Small businesses have an array of information—personnel records, blueprints, tax forms, customer orders, credit reports, and customer payment records—that require protection.
- 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.[26]

Example of a Risk Assessment Table[27]

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

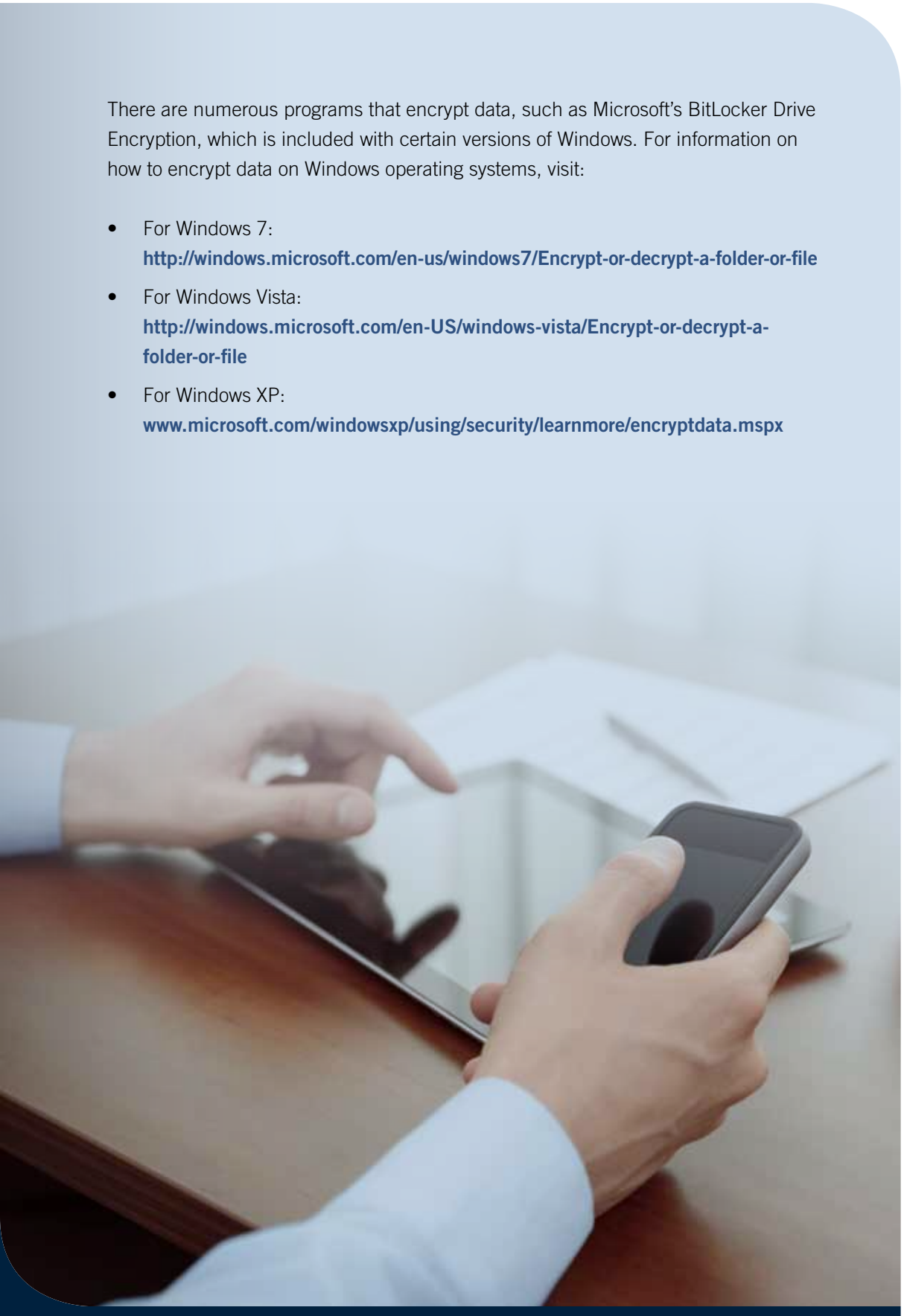
5. Manage the security of business data

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.

- 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**.[28]
- Implement an employee departure checklist for those who are no longer employed by the business to ensure that account termination is performed quickly and efficiently on laptops, mobile phones, and other digital devices.
- Assess how mobile your workforce is. Risks may rise as your workforce becomes more mobile or is increasingly accessing wireless (Wi-Fi) hot spots.[29]
- Ask your Internet service provider (ISP) if it offers a cost-effective suite of services that will enhance the cybersecurity of your business.
- For the most sensitive transactions—such as Automated Clearing House (ACH) payments and payroll processes—consider a dedicated computer that is not used for email or web browsing.
- To help prevent unauthorized access of your data—say, if your computer is lost or stolen—encrypt sensitive data on all computers and storage devices, particularly removable storage devices and drives.[30] Encrypting folders and files can protect them from unwanted access.

There are numerous programs that encrypt data, such as Microsoft's BitLocker Drive Encryption, which is included with certain versions of Windows. For information on how to encrypt data on Windows operating systems, visit:

- For Windows 7:
  http://windows.microsoft.com/en-us/windows7/Encrypt-or-decrypt-a-folder-or-file
- For Windows Vista:
  http://windows.microsoft.com/en-US/windows-vista/Encrypt-or-decrypt-a-folder-or-file
- For Windows XP:
  www.microsoft.com/windowsxp/using/security/learnmore/encryptdata.mspx



Data Security Basics

Nothing is more crucial to a business than its customers. It's a relationship that relies on trust, which is difficult to earn and easy to lose. New gains in technology can allow hackers to steal data from anywhere in the world. Protecting your business and customer information is more critical than ever. If your business accepts payment cards, it is important to have security steps in place to ensure that your customers' information is kept safe. Every business is different, but there are a number of common best practices that companies can adopt to protect payment data. Here are five top tips from Visa:

- Don't store any cardholder data that is not needed to run your business. Ask your merchant processor if you can use alternative data such as transaction IDs or tokens, rather than the full cardholder account number to respond to chargebacks and other customer inquiries.
- Ensure that all printed copies containing full cardholder account number (e.g., paper receipts, orders, and invoices) are physically secure.
- Know who has access to your business computers, including any vendors who may need to connect to them remotely for maintenance purposes. If you use vendors that have access to your customers' data, make sure they are protecting that information.
- Destroy any physical or electronic records containing full cardholder account numbers when they are no longer needed for business purposes. Take the necessary steps to destroy it responsibly. (This topic is addressed on page 20.)
- If you use a computer at your business to handle cardholder data or to facilitate payment card transactions, make sure that you install an antivirus program and update it regularly. If your business has an outward-facing Internet protocol address (these are Internet-facing entry points to your network), it is also essential to implement a firewall. If possible, do not use your business computer for any function that is not business-related to minimize your network's exposure to viruses and malware.

Securing Payment Information—Online Resources

Visa has worked with the U.S. Chamber of Commerce for many years to educate small businesses in cities across America. The multicity Drop the Data tour is one example of joint educational outreach to help make small businesses aware of the risks associated with retaining prohibited cardholder data. Learn more at **www.visa.com/dropthedata/index.html**. While small businesses often lack in-house support for securing their customers' payment information, there are a number of online resources that can help:

- The PCI Security Standards Council provides a global forum for the ongoing development, enhancement, storage, dissemination, and implementation of security standards for payment data protection: **www.pcisecuritystandards.org**
- Visa's PCI DSS Data Security Compliance Program: **www.visa.com/cisp**
- Businesses that outsource payment card processing or other card functions to third parties should review Visa's Global Registry of Service Providers—PCI DSS Validated Entities: **http://usa.visa.com/merchants/risk_management/cisp_service_providers.html**
- Data Security Guide for Small Businesses: **http://usa.visa.com/download/merchants/data-security-tips-for-small-business.pdf**
- Visa's Fraud News blog with information on the latest payment card scams and tips to help stay safe for consumers and small businesses: **www.visasecuritysense.com/en_US/fraud-news.jsp**
- Visa's Interactive Business Guide to Data Security: **http://usa.visa.com/merchants/risk_management/data_security_demo/popup.html**

6. Back up data regularly

Our computers contain vast amounts of data in a variety of forms—from business memos and negotiation documents 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.

Data backup is a simple, three-step process: Making copies of the data on your computer(s); selecting the appropriate hardware to store the backup data; and safely storing the backup device that holds your copied files.

- For guidance on conducting these steps, refer to "Back It up" at **http://staysafeonline.org/stay-safe-online/protect-your-personal-information/back-it-up**.
- 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.
- Protect computer equipment from natural hazards and security threats. 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 **http://disastersafety.org/open-for-business**.[31]

NOTE Look for additional how-to suggestions on backing up data at **www.msisac.org**.[32] If you are using Windows 7, consult **www.microsoft.com/windows/windows-7/features/backup-and-restore.aspx**.

Looking to the 'Clouds'

Cloud computing is receiving a great deal of buzz. It is a subscription-based service where you can obtain network storage space and computer resources. The cloud enables you to access your information from anywhere at any time, assuming that you have an Internet connection. Your cloud provider can both own and house the hardware and software necessary to run your business applications.

If you are considering using the cloud, identify the information you will be putting out in the cloud, who will have access to that information, and what you will need to ensure that it is protected. Additionally, know what type of cloud will be best for your needs, what type of provider will be most useful to you, and the reputation and responsibilities of the provider you are considering before you sign up. A good primer on cloud technologies is provided by Carnegie Mellon University and the Department of Homeland Security at **www.us-cert.gov/reading_room/USCERT-CloudComputingHuthCebula.pdf**.

7. Dispose of data and 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 through recovery tools. As new computers are purchased, older computers with their data may be redeployed or discarded.

Assume 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, flash drives, and mobile phones.

- 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**.[33]
- 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 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 (aka degaussing) or physical destruction.

Train Your Workforce

Technology alone will not secure your organization and its information assets—employee education is essential to help protect company information, customer data, and employees' own personal information at work. Raise Internet security awareness through a brown-bag lunch, employee newsletter, internal email, or your company's Intranet.

8. Defend your computer

The security of your computers and data is crucial for your employees as well as for your company. Lost or stolen information can reveal company secrets or expose your confidential or personal information.

- Strengthen your computer's defenses by keeping all software (including your Web browser) current with automatic updating and following the direction of IT staff. Install legitimate antivirus and antispyware software. Protect your company's wireless router with strong passwords or phrases.
- Don't be tricked into downloading malicious software. Think carefully before opening attachments or clicking links in unusual email or instant messages (IM) on a social network or in random pop-up windows. If you're unsure if a message is genuine—even from a co-worker—contact the sender to confirm, using a different channel.

Download Free Internet Security At Work Toolkit

Microsoft offers the free Internet Security at Work Toolkit to help teach employees how to protect company, customer, and employee information. It includes the following resources with instructions on how to use them:

- **Tip Card: Top Tips for Internet Security at Work**
  Information condensed into a printable, double-sided card.
- **Presentation: Internet Security at Work PowerPoint**
  30-minute slide presentation with speaker's notes.
- **Video: "Stay Sharp on Internet Safety at Work"**
  Presentation information condensed into a 3-minute video.
- **Quiz: Test Your Internet Security IQ**
  Printable 10-question quiz to help spread awareness among your employees.
- **Poster: Internet Security Begins With You**
  Let employees know about the presentation.

NOTE You can download the toolkit at **www.uschamber.com/cybersecurity**. For a version on a thumb drive, email **saferweb@microsoft.com**.

9. Protect sensitive business data—and watch out for scams

Don't put sensitive and confidential information in email or instant or text messages; they may not be secure.

- Think carefully before you open attachments or click links in unusual messages, on a social network or in random pop-up windows. Instead, look up the company's official website address yourself, as links embedded within an email may take you to a fake website. If you're unsure if a message is genuine—even from a co-worker—contact the sender using a different device or account.
- Never give sensitive information, such as a user name or password, in response to a phone call, an email, or other online request (even from a co-worker).
- Look for alarmist messages, misspellings, deals that sound too good to be true, requests for sensitive information (e.g., account numbers), and other signs of a scam.[34]
- Look for signs that a Web page is secure before you enter sensitive data—a Web address with https ("s" for secure) and a closed padlock (🔒) beside it. (Note, however, that these signs of security can also be fake, so don't rely on them completely.)

Learn to Spot Phishing Scams—Don't Get Hooked

Email "phishing" scams aren't just targeted toward consumers; merchants can become victims too. These scams utilize fraudulent emails that appear to originate from legitimate financial institutions, transaction processors, or other business entities that routinely conduct business with merchants. Through these email scams, criminals try to convince merchants to provide sensitive information such as merchant account information, passwords, login credentials, or other payment transaction information, which can be used by criminals to commit fraud.

In most of these email phishing cases, the merchant is asked to click on an Internet hyperlink embedded in the email. This link connects to the criminal's fraudulent website or computer server and may lead to the installation of malware on the merchant's computer.

Merchants and acquirers are encouraged to review both the example phishing email message and the list of phishing scam indicators in the links provided below. Together, these tips can help merchants identify and report suspicious emails.

- "Visa Security Alert About Merchant Email Phishing Scams": **http://usa.visa.com/download/merchants/alert-phishing-120910.pdf**
- Visa's "How to Catch a Phish": **www.visasecuritysense.com/en_US/phishing-attack.jsp**
- Get more information to avoid falling victim to Internet scam artists at **www.lookstoogoodtobetrue.com**. 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 **http://education.apwg.org**.

10. Create strong passwords and keep them secret

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. Lock devices, screensavers, files, and online accounts with passwords, passphrases[35] or a personal identification number (PIN).

Strong passwords and passphrases have the following characteristics:

- Using a unique password or passphrase on each account or device containing personal or business data, and change them regularly.
  - Use at least eight characters.
  - Don't include your real name, Social Security number, company name, or a complete dictionary word in your password or passphrase. Common brand names are also not recommended.
  - Utilize upper and lower case letters, numbers, and symbols (!, @, #, $, %, etc.).
- Not enabling any options to save or remember passwords.
- Never disclosing passwords and PINs to co-workers.
- Changing your computer, banking, and other important passwords at regular intervals, such as every 90 days.
- Setting 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.

Take a Quiz.
Are These Passwords Strong or Weak?

(1) 555.12.999

(2) 06/04/79

(3) Exp3d!ti0us

(4) Ambl!anc3

(5) 135781113

(6) MdHwb7yoiO

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. Add complexity by mixing upper and lower case letters, symbols, and numbers. For instance: Take the first letters of this sentence: My dog Hannibal will be 7 years old in October.

11. Guard your data when on the go

Treat all public Wi-Fi as a security risk. Do not expect privacy in Internet cafes, hotels, offices, or public places when traveling.

- When connecting to a public wireless network, it's a best practice to choose the most secure option, even if you have to pay for it. Some wireless networks offer a network key or certificate that encrypts (or scrambles) data as they travel between your laptop and the router.
- Confirm the exact spelling of the wireless network you're connecting to. Beware of clever (slightly misspelled) fakes—**www.uschmber.com**, for example.
- Never make financial or other sensitive transactions on any device over public Wi-Fi.
- Encrypt all confidential data on smart phones, flash drives, laptops, or other portable devices in case they're lost or stolen.
- 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 putting devices in checked baggage.[36]

NOTE Get tips on traveling securely overseas with mobile devices from the National Counterintelligence Executive (part of the Office of the Director of National Intelligence) at **www.ncix.gov/publications/reports/docs/traveltips.pdf**.

12. Use flash drives carefully

Minimize the chance that you'll infect your company network with malware:

- Don't put any unknown flash (or USB) drive into your computer.
- To block malware, hold down the Shift key when you insert a flash drive into your computer.
- Don't open files on your flash drive that are not familiar.

Be Prepared

13. Log monitoring

Security professionals and law enforcement officials commonly say that there are only two kinds of businesses: those that have been hacked and know it, and those that have been hacked and don't know it (yet).

Small businesses may believe that they are diligent about changing passwords and patching software to help prevent cybersecurity incidents, but they cannot be sure if they seldom if ever review their computer security logs.

What is a log? A log is a record of an event occurring due to a human-to-machine or machine-to-machine interaction with an organization's IT systems and networks. Facility access systems, HVAC systems, firewalls, servers, and applications create log data. Log data can be thought of as the "exhaust gas" of system and network activity. The data are the definitive and searchable record of user transactions, customer behavior, machine behavior, security threats, fraudulent activity, and more.

Conventional goals associated with log management include proactive maintenance of information system resources for reliability and resilience, security investigation, and regulatory compliance reporting. Many organizations are required by federal laws and regulations (e.g., HIPAA/HITECH, SOX, GLBA, and PCI DSS) to store and analyze log data for specific lengths of time. (Examples of data security requirements are found on page 10.)

More and more, cybersecurity experts are recommending that businesses leverage their log data to detect possible cyberattacks—basically being more aware of "normal" versus "abnormal" network traffic and system activity to support after-the-fact investigations of security incidents.

Small organizations typically do not have the awareness, expertise, or funding to perform log monitoring on par with the sophistication of the threats they face. However, log monitoring should not be overlooked. According to the *Verizon 2012 Data Breach Investigations Report* (DBIR), roughly 72% of the 855 data breaches analyzed in the report were at companies of 100 or fewer employees—up from 63% of the 761 data breaches Verizon analyzed in 2010.[37] The 2012 DBIR report also indicated that less than 1% of data breaches were discovered through log analysis.

When it comes to collecting and analyzing log data, there are at least three key challenges that small business typically face:

- Logs come in all shapes, sizes, and formats. Many solutions for the collection and analysis require you to change log data to fit them into a specific format for a database. This can force you to leave out information that may prove valuable for investigations.
- Attackers and malicious insiders count on the likelihood that businesses with limited resources do not continuously monitor their log data for cyber threats and abnormal behaviors.
- Small business owners have organizations to run, so information security cannot be allowed to consume all or most of their time. However, log monitoring needs to be an increasing part of their thinking and regular routines.

Continuous Monitoring

Splunk advises that companies continuously monitor their log data. It recommends using indexing technologies in lieu of a database to help collect, analyze, and correlate logs so that they are usable. Indexing solutions don't require preformatting of data at collection time. These technologies include search capabilities, the ability to automate searches, statistical analysis capabilities, and data visualization capabilities. Machine data can be collected and indexed in real time, and users can interact with their data using a familiar interface for searching through structured and unstructured log data to identify and highlight abnormal activities.

Whether your business is large or small, the keys to good security are the same: fostering employee awareness, having internal security policies, and utilizing technologies to help make sense of what is happening on your business' networks. Splunk advises owners and managers to continuously monitor and review the following activities, among others, that could require logging and analysis:

- Successful and unsuccessful logons and logoffs.
- Use of privileged accounts.
- Successful and unsuccessful attempts to access sensitive data, including customer data, intellectually property, and credit card data.
- System software updates and installations.
- Unauthorized configuration changes.
- Unsuccessful usage of user identification or authentication mechanisms.
- Changes to or deletion of log files.
- Activities that modify, bypass, or negate system security controls.
- Correlations of data indicating that an event happened at the wrong time by the wrong person from the wrong place.

In summary, log management is needed to help protect businesses from cyberattacks and insider threats and to meet specific regulatory requirements. Log monitoring doesn't have to be onerous on a business. There are solutions on the market that can make this easy to do and won't break the bank. Log data can also be used to understand customer behavior to support marketing efforts and to monitor supply chains. Applying behavioral analysis to log data is another element in the growing fight against cyber threats.[38]

NOTE A brief video on monitoring for "known" and "unknown" cybersecurity threats and "thinking like a criminal" is available at **www.splunk.com/view/SP-CAAAGMN**.

14. Make 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.

Refer to the model cyber security incident response guide at **www.msisac.org**.[39] It describes how businesses can recover from an incident in a timely and secure manner and minimize consequences on your organization and business partners. Its advice includes the following:

- 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.

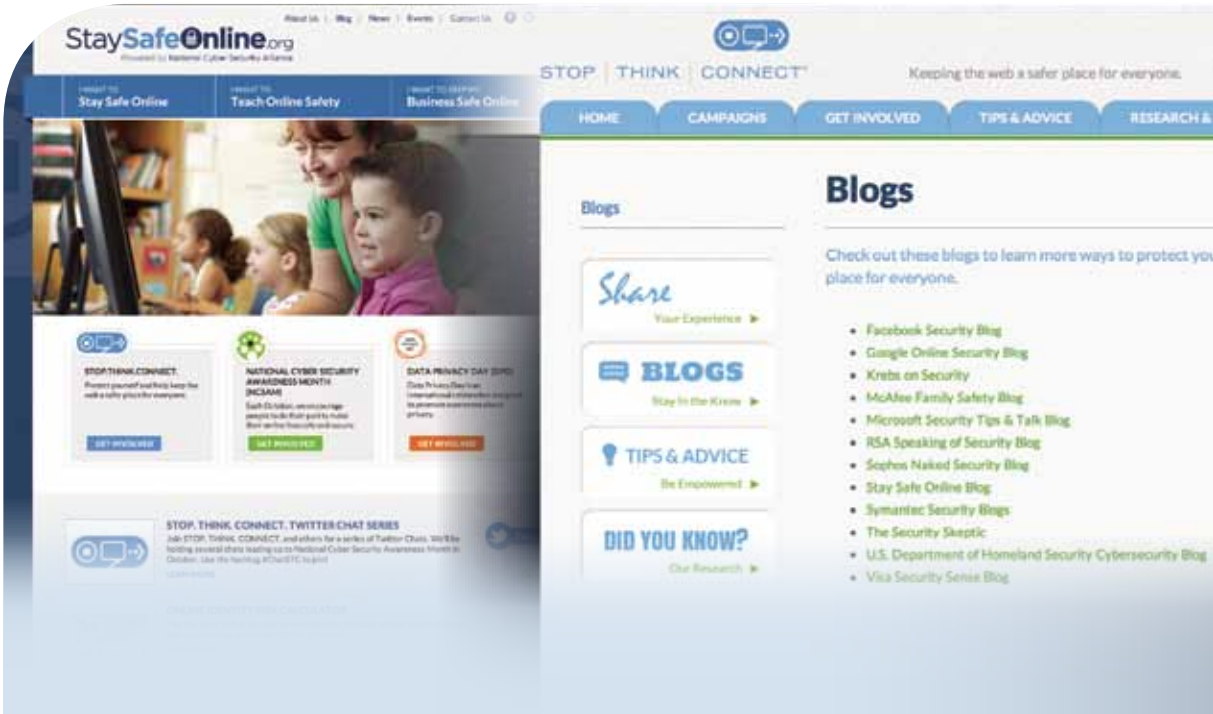
- Contact local law enforcement authorities if you suspect a crime has been committed. Similarly, work with law enforcement authorities who contact you because they suspect nefarious activity on your network. Cybercrime is not "somebody else's problem." Threats against your business computers can easily spill over to others' computers and vice versa.
- If you believe that payment information has been compromised, Visa's guide *What To Do If Compromised* provides information on what steps you should take and whom to contact. Access the guide at **http://usa.visa.com/download/merchants/cisp_what_to_do_if_compromised.pdf**.

Symptoms of an Infected Computer … and Troubleshooting Tips

- A computer may have been compromised if it exhibits any of the following characteristics or signs:
  - Is slow or nonresponsive.
  - Shows signs of high-level 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.

NOTE Microsoft can help you address common computer problems: **http://aka.ms/Troubleshooting_101**

- Your business may be experiencing a cybersecurity incident if it shows any of the following:
  - Finding email refused (bouncing back).
  - No longer receiving any email 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.[40]



15. 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. The STOP.THINK.CONNECT. campaign offers blogs to help individuals protect themselves and keep the Web a safer place for everyone. Go to **http://stopthinkconnect.org/blogs**.[41]

16. Help authorities fight cybercrime

- Report stolen finances or identities and other cybercrime to the Internet Crime Complaint Center (IC3) and to your local law enforcement entities as appropriate.
- 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.

Know the Information That Goes Into a Complaint or Incident Report

Incident reporting organizations, such as 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.

Cyber Incident and Complaint Reporting Organizations

OnGuard Online

OnGuard Online (**www.onguardonline.gov**; **www.alertaenlinea.gov** in Spanish) 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 **http://onguardonline.gov/filecomplaint**.

Internet Crime Complaint Center (IC3)

IC3 (**www.ic3.gov**) 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 intellectual property 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)

US-CERT (**www.us-cert.gov**) is the operational arm of the Department of Homeland Security's (DHS's) National Cyber Security Division (NCSD), 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. NCSD 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 of Commerce's *Internet Security Essentials for Business* 2.0 and other cybersecurity tips and tools

www.microsoft.com/security
Microsoft's website offering computer security, data privacy, and online safety updates, tools, free resources, and news

www.visa.com/cisp
Visa's Cardholder Information Security Program

www.visasecuritysense.com/en_US/for-retailers.jsp
Visa Security Sense: Information for Retailers

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.fcc.gov/cyberplanner
Federal Communication Commission (FCC) and partners' *Small Biz Cyber Planner*—an online resource to help small businesses create customized cybersecurity plans

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 (FTC) P*rotecting 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 of Technology (NIST), Computer Security Division, Small Business Corner

---

www.dhs.gov/cyber
U.S. Department of Homeland Security (DHS) Cybersecurity Awareness Month and related 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 (DOJ) 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*

CYBERSECURITY:
NATIONAL AND PRIVATE SECTOR

Since this guidebook was published in 2010, threats to businesses in cyberspace have grown in scope, seriousness, and sophistication. Unprecedented malware, such as Stuxnet and Flame, has captured the attention of security experts, business leaders, and policymakers.[42]

The administration and Congress are considering legislation to address disruptive or destructive threats to the nation by improving information sharing and by mandating the use of certain standards and best practices. The U.S. Chamber of Commerce has been engaged in shaping bills in the House and Senate.

The Chamber's public-policy advocacy goes hand in hand with its priority to educate members and the wider business community about cyber threats and network protection. The Chamber understands that the strength of our free enterprise system is directly tied to the prosperity and security of our interconnected world. Included here are brief descriptions of the initiatives of a few sectors to guard businesses from interruption, prevent the loss of capital or intellectual property, and protect public safety.

Banking and Finance

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 $60.8 trillion in 2010 and accounted for 8.5% of U.S. GDP in 2010. The sector employed 5.8 million workers in 2011.[43] 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 cyber incident. 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.[44] Federal financial regulators have implemented a comprehensive regime that includes the supervision of the banking and financial services sector's operational, financial, and technological systems.[45]

PERSPECTIVES

The current system includes the Federal Financial Institutions Examination Council (FFIEC), whose members conduct regular and continuous examinations to assess the adequacy of institutional controls. These examinations focus on cyber and physical security as well as business continuity, vendor management, and other operational risks as identified in the FFIEC *Information Technology Handbook*.[46] Public sector entities, self-regulatory organizations, and rulemaking bodies provide additional industry oversight to respond to any gaps in cybersecurity practices.[47]

In addition, working through public-private partnerships, organizations like the Financial Services Sector Coordinating Council and the Financial Services Information Sharing and Analysis Center (FS-ISAC) serve to protect the financial services community against an array of risks. For example, 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, which the Chamber has promoted, to assess and improve its own capabilities and often works in partnership with the Treasury Department, federal financial regulators, the Department of Homeland Security (DHS), and law enforcement and national security agencies.[48]

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 1.3 million people, and earning revenues of roughly $700 billion per year. Industry members are dependent on IT for their communications and operations. The chemical sector has been a leader in developing methods and processes to address safety and manage risk. The sector has long recognized the need to view cybersecurity as an essential aspect of risk management. Industry activities have included development of guides and standards to help improve operational safety and reliability.

In close partnership with federal officials, the chemical sector has developed a dynamic roadmap (*Roadmap to Secure Control Systems in the Chemical Sector*) describing 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; they are increasingly becoming linked to corporate or business networks to increase market efficiencies and real-time information flows. However, industry has taken proactive steps to guard its control systems, and the roadmap provides a means of sharing smart and effective measures across the sector. Implementation of the roadmap by the sector is being coordinated by a DHS working group composed of representatives of government and industry. This group also interacts with those working on similar programs in other critical infrastructure sectors.[49]

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 action 24/7, as allowed by law, to address spam, phishing, and other malicious activity that threatens 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 through partnerships, such as providing the president with policy advice through the National Security Telecommunications Advisory Committee[50] as well as operational support through the National Coordinating Center for Telecommunications (NCC)[51] and the Communications Information Sharing and Analysis Center (C-ISAC). In addition, the Communications Sector Coordinating Council (CSCC),[52] established in 2005, acts as the principal entity for coordinating with the government in implementing national infrastructure protection and response plans.

The National Cybersecurity and Communications Integration Center (NCCIC) was launched in October 2009.[53] It unites the communications sector coordination of the NCC and the cyber protection efforts of the United States Computer Emergency Readiness Team (US-CERT). Industry partners are testing industry-to-industry information sharing to provide policy recommendations to the president and enhance NCCIC operations.[54]

Electric

The use of electricity in the United States is ubiquitous, spanning all sectors of the economy. More than 70% of electricity customers are served by shareholder-owned electric companies, which are highly regulated.[55] In 2009, electric power accounted for nearly 40% of all energy consumed in the United States.[56, 57] Electric sector owners and operators routinely strive to strengthen the security of their control systems and identify and mitigate any network vulnerability. Protecting the power grid from cyberattacks requires a coordinated effort and the exchange of timely and actionable cyber threat information between industry stakeholders and federal officials.

To maximize the cybersecurity of the bulk power system, electric utilities work closely with the North American Electric Reliability Corporation (NERC), an industry regulatory body empowered by statute and strictly supervised by the Federal Energy Regulatory Commission (FERC). The mandatory and enforceable critical infrastructure protection (CIP) standards resulting from this established regulatory model already require FERC-regulated utilities to implement numerous countermeasures against potential cyber and physical attacks on critical electric infrastructure. This regulatory regime also facilitates the coordination of cybersecurity protection measures and threat information between utilities, FERC, DHS, and the Department of Energy (DOE).[58]

Another 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.[59] 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's existing architecture and emerging smart grid technologies.[60] A significant variety of industry stakeholders also participate in the development and implementation of the DOE's Electricity Subsector Cybersecurity Risk Management Maturity Model,[61] a tool that allows electric utilities and grid operators to assess their cybersecurity capabilities and prioritize their actions and investments. On top of these multi-tiered efforts, most industry members voluntarily participate in the Transmission Forum, which administers numerous audits that focus on security and standards compliance at member utilities, while serving as a valuable information exchange between senior system operators and utility company senior operational executives.

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.[62]

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.[63] IT sector members, along with those of other critical infrastructure 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 as part of DHS' national cyber exercise, Cyber Storm, will help the nation prepare for and respond to the effects of a major cyberattack.[64]

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.[65] 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.[66]

Oil and Natural Gas

The oil and natural gas (ONG) industry features the exploration, production, storage, shipment, and delivery of crude oil and natural gas. Oil and natural gas are imported and produced domestically, stored throughout the United States, and transported over millions of miles via pipelines, waterways, railways, and highways. ONG company owners and operators recognize that their industry has crucial links to other critical infrastructure sectors (and vice versa) and is integral to the nation's energy supply.

Oil and natural gas are vital to the success of our nation's economy and energy security. More than 9 million Americans depend on the ONG industry for their jobs. In 2010, the production of oil and natural gas on federal lands brought $9.2 billion into the treasuries of federal and state governments and Indian tribes. Nearly $6.5 billion of that amount came from ONG production. Although the share of non-fossil fuels continues to grow, the ONG industry will continue to play a leading role in meeting U.S. energy needs. Today, oil and natural gas supply more than 60% of the nation's energy demand. According to the U.S. Energy Information Administration (EIA) forecasts, the ONG industry will continue to supply roughly 60% of the nation's energy needs through 2035.[67]

The ONG industry has worked in close partnership with government entities to identify cyber vulnerabilities and develop mitigation strategies. Through extensive coordination and the contribution of technical expertise, the ONG subsector and DOE developed the *Roadmap to Secure Control Systems in the Energy Sector* (2006),[68] which identifies concrete steps to secure control systems in the electric sector and ONG industry.

In addition, collaborative efforts to enhance U.S. cybersecurity are under way with the DHS Industrial Control System Cyber Emergency Response Team related to information sharing and training; with the Transportation Security Administration's (TSA) Transportation Systems Cyber Security Working Group for the development of cybersecurity risk assessment methodology; and with DHS and the Department of Defense to prioritize the security of cyber-dependent business functions. A long list of recommended practices, standards, and guidelines, including the TSA *Pipeline Security Guidelines* (2011), are employed by industry operators to bolster their cybersecurity posture and resilience in an all-hazards context.

ACKNOWLEDGEMENTS

The U.S. Chamber of Commerce thanks the members of its National Security Task Force, the National Cyber Security Alliance, the Multi-State Information Sharing and Analysis Center, as well as its sponsors—Bank of America, Microsoft, Splunk, and Visa—for contributing to the content of this guide.

NATIONAL SECURITY AND EMERGENCY PREPAREDNESS DEPARTMENT

Established in 2003, the U.S. Chamber of Commerce's National Security and Emergency Preparedness Department is responsible for developing and implementing the Chamber's homeland and national security policies. The department works through the National Security Task Force, a policy committee composed of roughly 160 Chamber members representing a broad spectrum of the nation's economy. The Task Force's Cybersecurity Working Group identifies current and emerging issues, crafts policies and positions, and provides analysis and direct advocacy to government and business leaders.

The department champions members' views through outreach to congressional lawmakers and staff, regulatory filings with federal agencies, meetings with agency and department officials, communications with the media, and public forums with elected and appointed officials and members of the business community. The department offers positive solutions to Washington leaders on an array of homeland and national security challenges that impact the strength of the nation and the global economy.

To learn more about the National Security and Emergency Preparedness Department and the Cybersecurity Working Group, contact:

- Ann M. Beauchesne (**abeauchesne@uschamber.com**), Vice President
- Matthew J. Eggers (**meggers@uschamber.com**), Senior Director

ENDNOTES

1. U.S. Department of Commerce Secretary Gary Locke, "Remarks at Cybersecurity Policy Review Meeting," July 14, 2010; see also **www.commerce.gov/news/fact-sheets/2011/05/13/fact-sheet-digital-literacy#_edn1**, **www.nationaljournal.com/magazine/are-passwords-pass-not-just-yet-20110421**, or **www.freeenterprise.com/2011/04/how-do-you-protect-10-trillion**.

2. Federal Communications Commission (FCC), *Connecting America: The National Broadband Plan (2010)*, **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**.

3. U.S. Small Business Administration, "Frequently Asked Questions" (FAQs), **http://web.sba.gov/faqs/faqindex.cfm?areaID=24**.

4. See August 10, 2010, press release by the National Cyber Security Alliance and the Anti-Phishing Working Group. The release is available at **http://staysafeonline.org/about-us/news/details/?id=279**. 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.

5. Marcia Clemmitt, "Computer Hacking." *CQ Researcher*, September 16, 2011, vol. 21, no. 32, pp. 757–780, **http://library.cqpress.com/cqresearcher**.

6. The language on common threats to business derived, in part, from Verizon Business RISK Team's data breach investigation reports can be accessed at **www.verizonbusiness.com/Products/security/dbir**.

7. *CQ's* "Computer Hacking," p. 761.

8. The eighth volume (July–December 2009) of Microsoft's Security Intelligent Report covers trends in security breaches; see pp. 50–53, **www.microsoft.com/security/about/sir.aspx**.

9. ONCIX, Networked Information Systems (2000) booklet; see section on insider threat at www.h**sdl.org/?view&did=447415**.

10. Red Cross Ready Rating Program, "Preparedness Research Findings," **www.readyrating.org/HowItWorks/ReasonstoPrepare.aspx**.

11. Internet Crime Complaint Center (IC3), *2011 Internet Crime Report*, **www.ic3.gov/media/annualreport/2011_IC3Report.pdf**.

12. IC3 press release, "IC3 2010 Annual Report on Internet Crime Released," February 24, 2011, **www.ic3.gov/media/2011/110224.aspx**.

13. A beginner's guide on cybersecurity, from which this guide borrows many recommendations, is available from the Multi-State Information Sharing and Analysis Center (MS-ISAC) at **http://msisac.cisecurity.org/resources/guides/documents/Getting%20Started%20Guide.pd** (Getting Started) via **http://msisac.cisecurity.org/resources/guides**.

14. An MS-ISAC cyber incident response guide is available at **http://msisac.cisecurity.org/resources/guides/documents/Incident-Response-Guide.pdf**. See, too, Paul Cichonski et al., *Computer Incident Response Handling Guide* (Draft), National Institute for Standards and Technology (NIST), January 2012, **http://csrc.nist.gov/publications/drafts/800-61-rev2/draft-sp800-61rev2.pdf**.

15. Language on data security requirements taken from Federal Trade Commission (FTC) Web pages **www.ftc.gov/bcp/edu/pubs/articles/art08.shtm** and **http://business.ftc.gov/privacy-and-security**.

16. SEC Division of Corporation Finance, *CF Disclosure Guidance: Topic No. 2, Cybersecurity*, available at **www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm**; see KPMG newsletter, S*EC Staff Issues Cybersecurity Disclosure Guidance*, November 2011, available at **www.kpmg.com/CN/en/IssuesAndInsights/ArticlesPublications/Newsletters/Defining-Issues/Documents/Defining-Issues-O-1111-58.pdf**. See, also, "How Companies Can Apply the SEC's Cyber Security Disclosure Guidance," *The Wall Street Journal*, September 4, 2012, **http://deloitte.wsj.com/cio/2012/09/04/how-companies-can-apply-the-secs-cyber-security-disclosure-guidance**.

17. See list of security breach laws at **http://www.ncsl.org/issues-research/telecom/overview-security-breaches.aspx**, including recommended practices on breach notifications by California's Office of Privacy Protection.

18. See FTC Web pages **www.ftc.gov/privacy/privacyinitiatives/glbact.html**, **www.ftc.gov/bcp/edu/pubs/articles/art08.shtm**, and **www.ftc.gov/infosecurity**.

19. See U.S. Department of Health and Human Services Web pages 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**.

20. HITECH Breach Notification Interim Final Rule, **www.hhs.gov/news/press/2009pres/08/20090819f.html** and **www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html**.

21. The Payment Card Industry (PCI) Security Standards Council, **www.pcisecuritystandards.org**.

22. 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 that they receive timely security updates for Microsoft products.

23. MS-ISAC, *Beginners Guide to Firewalls*, **http://msisac.cisecurity.org/resources/guides/documents/FirewallGuide021108.pdf**.

24. The proliferation of personal devices (e.g., smart phones and tablets) in the workplace—commonly known as "bring your own device" (BYOD)—has complicated the job of the person who is managing information security. See, for example, Tony Bradley, "Pros and Cons of Bringing Your Own Device to Work," *PC World*, December 21, 2011, **www.pcworld.com/businesscenter/article/246760/pros_and_cons_of_bringing_your_own_device_to_work.html**.

25. See October 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://chsdemocrats.house.gov/SiteDocuments/20071031154853-26197.pdf** or **http://www.gpo.gov/fdsys/pkg/CHRG-110hhrg48977/pdf/CHRG-110hhrg48977.pdf**.

26. 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.

27. For additional information on risk-management essentials, see **http://msisac.cisecurity.org/resources/guides/documents/Risk-Management-Guide.pdf**.

28. MS-ISAC, Internet and Acceptable Use Policy Template, **http://msisac.cisecurity.org/resources/guides/documents/AcceptableUseGuide021108.pdf**.

29. See, for example, Mary K. Pratt, "Hot Spot Dangers: That Internet Cafe Could Cost You Way More Than a Cup of Coffee," *Computerworld*, April 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**.

30. 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**.

31. See, for example, Institute for Business & Home Safety's "Computer Equipment and Software" inventory form at **http://disastersafety.org/wp-content/uploads/10_Hardware_Software.pdf**.

32. MS-ISAC, *Guidelines for Backing Up Information*, **http://msisac.cisecurity.org/resources/guides/documents/Backing-Up-Information-Guide.pdf**.

33. MS-ISAC, *Erasing Information and Disposal of Electronic Media*, **http://msisac.cisecurity.org/resources/guides/documents/Erasing%20and%20Disposal%20Guide.pdf**.

34. The Internal Revenue Service (IRS) has issued several recent consumer warnings on the wrongful use of the IRS name or logo by fraudsters trying to gain access to consumers' financial information in order to steal their identity and assets, including phishing attacks; see **www.irs.gov/newsroom/article/0,,id=155682,00.html**.

35 A passphrase is new way of thinking about a much longer password. Dictionary words and names are no longer restricted. In fact, one of the very few restrictions is the length (i.e., 15 characters). Your passphrase can be a favorite song lyric; quote from a book, magazine, or movie; or something your kids said last week. Explanation adapted from **http://protect.iu.edu/cybersecurity/safeonline/passphrases**.

36. 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**.

37. Sarah E. Needleman, Cybercriminals Sniff Out Vulnerable Firms," *The Wall Street Journal*, July 5, 2012, **http://online.wsj.com/article/0,,SB10001424052702303933404577504790964060610,00.html?mod=vocus**.

38. Additional resources on log management representing federal and state perspectives can be found at **http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf** and **http://cybersecurity.alabama.gov/documents/Policy_677_Log_Management.pdf**.

39. MS-ISAC, *Cyber Incident Response Guide*, **http://msisac.cisecurity.org/resources/guides/documents/Incident-Response-Guide.pdf**.

40. MS-ISAC, *Getting Started*, p. 8.

41. For example, the MS-ISAC provides a cybersecurity newsletters monthly. Sign up at **www.msisac.org/awareness/news**. Business managers and IT professionals may want to sign up for Microsoft bulletins and technical security notifications at **http://technet.microsoft.com/en-us/security/default.aspx** or **http://technet.microsoft.com/en-us/security/dd252948.aspx**.

42. Hayley Tsukayama, "Newly Discovered Malware Linked to Stuxnet, Flame," *The Washington Post*, August 9, 2012, **www.washingtonpost.com/business/technology/newly-discovered-malware-linked-to-stuxnet-flame/2012/08/09/eef637b2-e23d-11e1-a25e-15067bb31849_story.html**; *The New York Times*, Times Topics: Cyberattacks on Iran—Stuxnet and Flame, **http://topics.nytimes.com/top/reference/timestopics/subjects/c/computer_malware/stuxnet/index.html**.

43. Insurance Information Institute (III), "Financial Services at a Glance," **http://www2.iii.org/financial-services-fact-book/financial-services-industry/financial-services-at-a-glance.html**; see, too, III and The Financial Services Roundtable, The Financial Services Fact Book 2012, **www.fsround.org/fsr/publications_and_research/files/2012FinancialFactBook.pdf**.

44. U.S. Department of Homeland Security (DHS) et al., *Banking and Finance Sector-Specific Plan*, May 2007, **www.dhs.gov/xlibrary/assets/nipp-ssp-banking.pdf**.

45. U.S. Government Accountability Office (GAO), C*ritical Infrastructure Protection: Cybersecurity Guidance Is Available, but More Can Be Done to Promote Its Use*, December, 2011, **www.gao.gov/assets/590/587529.pdf**.

46. The FFIEC is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the board of governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Consumer Financial Protection Bureau (CFPB) and to make recommendations to promote uniformity in the supervision of financial institutions.

47. For example, the Municipal Securities Rulemaking Board, the Financial Industry Regulatory Authority, the National Futures Association, the Payment Card Industry Security Standards Council, and exchanges, such as the Chicago Mercantile Exchange and the New York Stock Exchange.

48. See September 14, 2009, testimony of the Financial Services-Information Sharing and Analysis Center's (FS-ISAC's) William Nelson from a Senate hearing on protecting industry from cyber threats, via **www.hsgac.senate.gov/hearings/cyber-attacks-protecting-industry-against-growing-threats**.

49. DHS, *Roadmap to Secure Control Systems in the Chemical Sector*, September, 2009. For an electronic copy of this document, send an email request to **ChemicalSector@dhs.gov**.

50. National Communications System, **www.ncs.gov/nstac/nstac.html**.

51. National Coordinating Center for Telecommunications, **www.ncs.gov/ncc**.

52. U.S. Communications Sector Coordinating Council, **www.commscc.org**.

53. **http://www.dhs.gov/news/2009/10/30/new-national-cybersecurity-center-opened**.

54. **www.dhs.gov/about-national-cybersecurity-communications-integration-center-nccic**.

55. Edison Electric Institute, "About the Industry," **www.eei.org/whoweare/Aboutindustry/Pages/default.aspx**.

56. DHS et al., Energy Sector-Specific Plan (May 2007 version); 2010 version, **www.dhs.gov/xlibrary/assets/nipp-ssp-energy-2010.pdf**.

57. U.S. Energy Information Administration, *Annual Energy Review 2010*, Figure 2.1a, *Energy Consumption by Sector Overview*, **www.eia.gov/totalenergy/data/annual/pdf/sec2_4.pdf**.

58. In January 2008, the Federal Energy Regulatory Commission (FERC) 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.

59. U.S. Department of Energy (DOE), "Control Systems Security," **www.oe.energy.gov/controlsecurity.htm**.

60. See NIST, "Smart Grid Interoperability Standards Project," **www.nist.gov/smartgrid/index.cfm** or **http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7628**.

61. The Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2), which allows electric utilities and grid operators to assess their cybersecurity capabilities and prioritize their actions and investments to improve cybersecurity, combines elements from existing cybersecurity efforts into a common tool that can be used consistently across the industry. The ES-C2M2 was developed as part of a White House initiative led by the DOE in partnership with DHS and involved close collaboration with industry, other Federal agencies, and other stakeholders. See **http://energy.gov/oe/articles/doe-releases-electricity-subsector-cybersecurity-risk-management-process-rmp-guideline**; **http://energy.gov/oe/services/cybersecurity/electricity-subsector-cybersecurity-capability-maturity-model**.

62. DHS et al., *Information Technology Sector-Specific Plan*, 2010, **www.hsdl.org/?view&did=7899**.

63. DHS et al., *Information Technology Sector Baseline Risk Assessmen*t, August 2009, **www.dhs.gov/xlibrary/assets/nipp_it_baseline_risk_assessment.pdf**.

64. DHS, "Cyber Storm: Securing Cyber Space," **www.dhs.gov/files/training/gc_1204738275985.shtm**.

65. For more information about the IT Sector Coordinating Council, visit **www.it-scc.org**.

66. For more information about the IT-Information Sharing and Analysis Center, visit **www.it-isac.org**.

67. American Petroleum Institute, Energizing America, August 2012, **www.api.org/policy-and-issues/policy-items/jobs/~/media/Files/Policy/Jobs/Energizing-America/ENERGIZING_AMERICA_AUGUST_2012_MedRes.ashx**; see U.S. Energy Information Administration data at **www.eia.gov/forecasts/aeo/MT_energydemand.cfm#average** and **www.eia.gov/totalenergy/data/annual/diagram1.cfm**.

68. Also noteworthy is the *Roadmap to Achieve Energy Delivery Systems Cybersecurity* (September 2011), **http://energy.gov/oe/downloads/roadmap-achieve-energy-delivery-systems-cybersecurity-2011**.

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