

cyber_for_counties {guidebook} v1.0



NACO *National Association of Counties*

Content is copyright protected and provided for personal use only - not for reproduction or retransmission.
For reprints please contact the Publisher.

NATIONAL ASSOCIATION OF COUNTIES

Cyber for Counties Guidebook

Preventing, Detecting and Defending against Cyber-attacks

A publication of the National Association of Counties

Sponsored by AT&T



at&t



Special thanks to the Center for Internet Security for
their participation in the development of this Guidebook



**CENTER FOR
INTERNET SECURITY®**

foreword: some context for elected officials and IT executives

By Sebron K. Partridge
Chief Information Security Officer
Riverside County, California

After spending the past 30 years of my career in the private and public sector information technology (IT) fields, from help-desk support to the position I hold today as the Chief Information Security Officer for California's fourth-largest county, I have come to realize that IT is not about technology for technology's sake. The most successful organizations that I have worked in understood that IT is only a foundation to provide the organization with the ability to be more successful in providing its core product or service.

Each of the organizations in which I worked understood that healthy partnerships between the business and IT departments result in a much-improved ability to serve customers. How well an IT organization understands and aligns itself with the business units within an organization will be reflected directly in the return on investment (ROI) for each IT service that supports those business units. This ROI can be tracked over time to determine if the business and IT staff are in both tactical and strategic alignment.

In the following document you will find a strong rationale for county officials and business personnel to work together in support of cybersecurity initiatives, along with detailed recommendations that IT professionals can reference in their discourse with business-focused colleagues. We hope this information will provide valuable insight into each of the organizations, with important elements that you can use as you develop, enhance or validate a security program in your organization.

Commitment by elected officials, business professionals, and IT professionals to collaborate on any program is essential for organizational success. This is particularly so for initiatives as complex and rapidly evolving as cybersecurity. Resolve to finding common ground for discussion and understanding each other's culture as you venture forward. The reward for that commitment will be a safer and more agile business in which you, the county, and your constituents will benefit.

*Healthy partnerships
between business and IT
result in a much-improved
ability to serve customers.*

table of contents

foreword: some context for elected officials and IT executives	03
introduction	06
policy and governance best practices	12
[risk management]	
[cybersecurity training]	
[train.reinforce.repeat often.]	
[new technologies change the landscape]	
[measurement and reporting]	
[policy and governance/checklist]	
industry standard security control references	24
[critical security controls case studies]	
{the city of portland/oregon}	
{bankia}	
[industry standard security control references/checklist]	

operational_best_practices	36
[authentication authorization and access]	
[email security]	
[website and social networking best practices]	
[network infrastructure and security]	
[storage/data loss prevention]	
[cloud and storage security]	
[mobility]	
[measurement and reporting—logs]	
[application security]	
[incident response plan and program]	
[operational best practices/checklist]	
the road ahead	58
appendix 1: acknowledgements	65
appendix 2: additional resources for counties	64

cyber_for_counties

{guidebook} v1.0

introduction

cyber_for_counties {guidebook} v1.0





-VIDEO
-MUSIC
-FILM
-CONTACTS
-MESSAGES

-EUROPE
-AMERICA
-ASIA
-AFRICA

-CULTURE
-ECONOMIC
-FINANCE
-BUSINESS
-MEDIA
-PEOPLE
-CREATIVE
-TECHNOLOGY
-INVESTMENT
-NETWORKING

-VIDEO
-MUSIC
-FILM
-CONTACTS
-MESSAGES

-PEOPLE
-FORUMS
-CHAT
-SHOP
-BUY
-SALE

NEWS

120101110101010010010101010101
1101011100101011110101002010101
1111010110101011101010101010101
1010110001010111101010101010101
11110101010101010101010101010101
11110101010101010101010101010101

1201011101010100
1101011101010101
1111010110101011
1010110001010111
1010110101010101
1111101010101010

introduction

It's no longer a question of if, but when. Cyber threats are real, they're growing, and your county and every other organization is at risk.

How can you be sure? Take a look around. The most recent Norton Cybercrime report found that 1.5 million adults become victims of cybercrime every day – that's 18 per second and 556 million per year for a total financial loss of \$118 billion.¹ Businesses last year reported a 42 percent increase in cyber-attacks.² Government offices are also

under attack, and it's widely perceived that cyber-threats against them have become more common, more sophisticated, and more dangerous.

Information is power.

There's no telling what kind of information you can obtain from government networks.

– Mafiaboy, former hacker

Many assaults against government entities take place in the form of Advanced Persistent Threats (APT), a long-term pattern of targeted sneak attacks that are usually designed to steal data.

Government agencies reported 268 data breaches between 2009 and 2012,³ which exposed more than 94 million records containing personally identifiable information– twice as many breaches, and triple the number of records disclosed as were identified in the previous year. The average cost for each record lost or breached is \$194, a figure that quickly becomes overwhelming considering the massive numbers of records that each county maintains.

Counties store a wealth of information of interest to cyber attackers: financial accounts, personal information like Social Security and payment card numbers, health records and much more. Counties also play an important role in Homeland Security, making them attractive targets for an attack that could shut down airports, water systems, electrical grids and other vital systems for which counties are responsible. As the former hacker Mafiaboy explained, "Information is power. There is no telling what kind of information you can obtain from government networks."⁴

1 Symantec, Inc., "2012 Norton Cybercrime Report." Sept. 5, 2012.

Accessed at http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf

2 Ponemon Institute. "2012 U.S. Cost of Cyber Crime Study." October, 2012.

Accessed at www.ponemon.org/local/upload/file/2012_US_Cost_of_Cyber_Crime_Study_FINAL6%20.pdf

3 Rapid 7. "Data Breaches in the Government Sector." Sept 6, 2012. Accessed at www.rapid7.com/docs/data-breach-report.pdf

4 Mulholland, Jessica. "Ex-Hacker Mafiaboy Discusses Local Government Security." Government Technology, Jan. 30, 2012.

Accessed at www.govtech.com/security/Ex-Hacker-Mafiaboy-Discusses-Local-Government-Web-Security-.html

Here are just a few examples of the assaults on county governments that occurred within the last year:

- ⚠ Thieves stole five laptops from a county office in North Carolina but ended up with something much more valuable than the hardware – the personal information, including partial Social Security numbers, of 71,000 registered voters.
- ⚠ Intruders accessed the online banking system of a county in New Jersey through the server that supports its messaging applications and transferred \$19,000 to a California bank account.
- ⚠ Hackers used a computer program to try to fraudulently obtain thousands of absentee ballots from a Florida county, in an apparent attempt to steal the state senate election.
- ⚠ Turkish attackers shut down a Tennessee sheriff's department website; although it appears that nothing was stolen, the sheriff believes that hackers could have attempted to change prisoners' release dates or unleash a dangerous virus that could destroy county records.



This video was released on February 5, 2013 via naco.org. The video features former DHS Secretary, Janet Napolitano delivering a video message about the importance of Cyber Security and the ongoing partnership with DHS and NACo.

But here's the good news: there's a lot you can do to safeguard your information assets. The bad guys don't have to win. Currently, 97 percent of data breaches could have been avoided if the attacked organizations had put in place simple or intermediate controls.⁵

Counties should take every precaution in efforts to prevent and mitigate the effects of cyber-attacks. While this is a multilayered process, it can be summed up in three words: assessment, patching and training.



🔒 **Assessment** – ongoing analysis of your networks, processes to check for weaknesses, and classification of assets by criticality

🔒 **Patching** – regularly updating software to fix vulnerabilities

🔒 **Training** – educating staff, elected officials and all others who access your networks about the risks of cyber-attacks and what each person can do to keep your network safe.

In other words, Assessment, Patching & Training – APT – represents your best defense against APT – Advanced Persistent Threats.

These preventive measures offer counties protection, but it's important to remember that most networks are vulnerable in some way. Counties must therefore plan to respond to catastrophic cyber-events in the same way they would act in response to blizzards, epidemics and other emergencies: identify which assets are at risk and their worth to the county, and implement security controls to protect those assets.

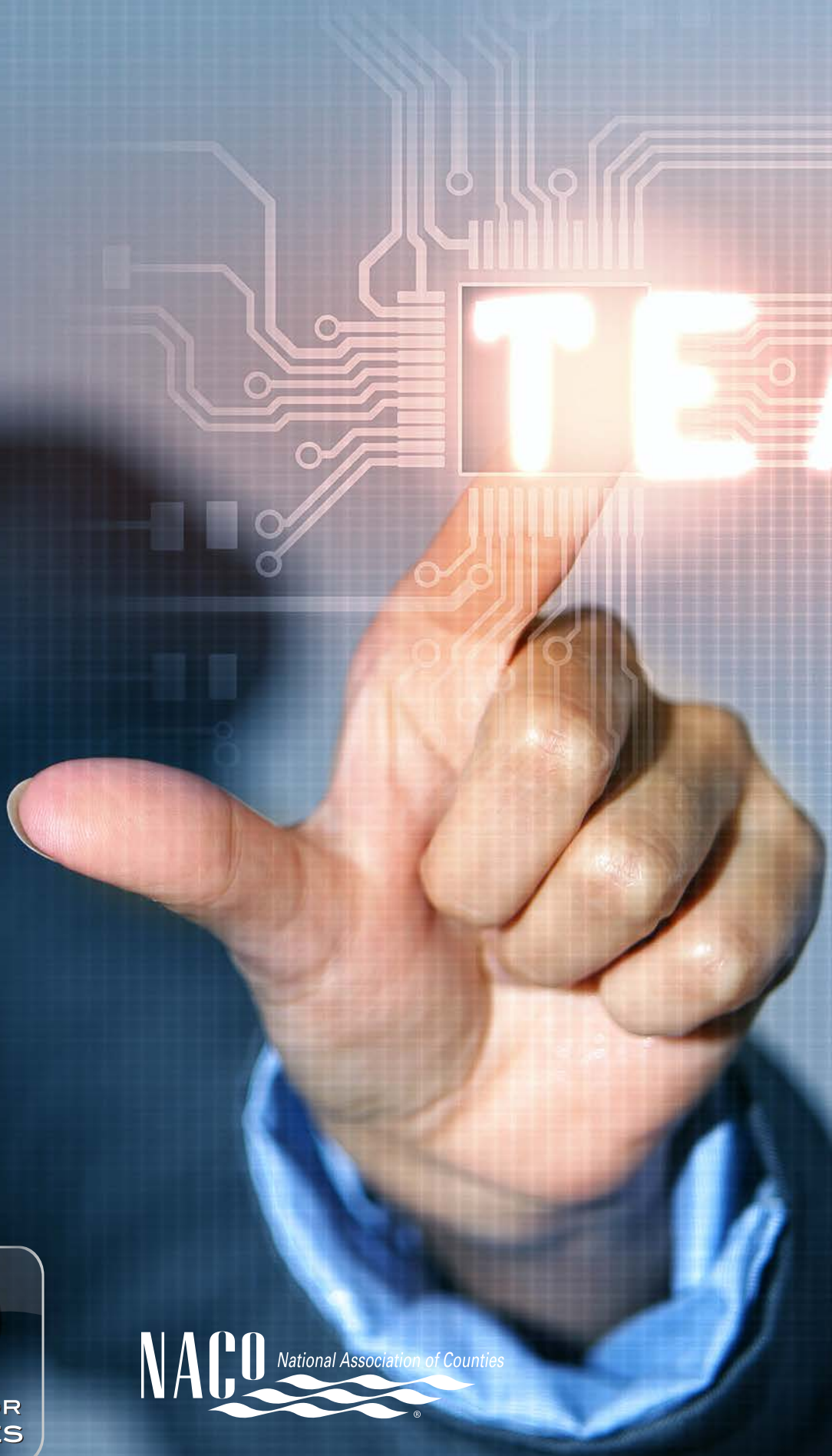
⁵ Verizon, Inc. 2012 Data Breach Investigations Report. March 22, 2012.
Accessed at www.wired.com/images_blogs/threatlevel/2012/03/Verizon-Data-Breach-Report-2012.pdf

You're not alone. NACo and experts from government and private industry are available to assist you in the ongoing process of protecting your assets. NACo has published this guidebook as a practical guide to safeguarding your county's information by preventing, detecting, and responding to cyber-attacks. It outlines the basic components of cybersecurity strategy and suggests a number of resources to assist counties at every stage of development.

It's not a question of if, but when. Your county will be attacked. Therefore it's important that your county is prepared, and that your computers and operating systems are safeguarded.

In the January 14, 2013 edition of NACo's County News, NACo took an in depth look at all aspects of cybersecurity and how it impacts counties. Whether it is mitigating threats, responding to cyber-attacks or training a workforce of skilled IT professionals, this issue contains an enormous amount of tools and resources for local elected policy makers and IT professionals.





Content is copyright protected and provided for personal use only - not for reproduction or retransmission.
For reprints please contact the Publisher.



NETWORK

policy and
governance
best practices

cyber_for_counties
{guidebook} v1.0

Content is copyright protected and provided for personal use only - not for reproduction or retransmission.
For reprints please contact the Publisher.

policy and governance best practices

Cybersecurity – the way you protect your network, your assets, and your organization from attacks – is part of the toll all organizations pay for accessing the information highway. The threats are real and pervasive – from criminals who want to steal your cash or your citizens' identities to hackers with a political or social agenda who want to shut down your websites or destroy the county's data.

Advanced Persistent Threats (APTs), a long-term pattern of targeted hacking attacks, endanger any organization because they are often difficult to anticipate, detect, and

prevent. APT attackers are often more skilled and more patient than other hackers, and therefore more likely to succeed.⁶ They target specific organizations, using subversive means to steal or compromise the safety of assets.

Even if you have a good first line of defense against APTs and other attacks, that is only one layer of protection. Weak perimeter security contributes to your vulnerability. In fact, a common entry point for many attackers is a staff member who unknowingly

opens a malicious email that lets loose a virus or opens a connection that gives cyber-criminals access to your entire network. Training and reinforcement are two of your best weapons against cyber-attacks. Anyone with a need to access your devices or county network including staff, elected officials, or others – should receive training in order to earn such access.

Cybersecurity requires a plan and a commitment from staff members at all levels of the organization to work collaboratively, use common sense, and act thoughtfully and strategically to protect the county's assets. This means counties must create strong policy and governance standards, communicate them clearly to all stakeholders, monitor compliance, and develop ongoing communication strategies remind everyone of the importance of thwarting cyber-attacks.

Counties have to create strong policy and governance standards, communicate them clearly to all stakeholders and develop ongoing ways to reinforce the importance of thwarting cyber-attacks.

⁶ Schwartz, Matthew J. "Advanced Persistent Threats Get More Respect." Information Week Security. Feb. 9, 2012. Accessed at www.informationweek.com/security/cybercrime/advanced-persistent-threats-get-more-res/232600562

[risk management]

Many counties use a risk management approach to securing their networks. At the most basic level this consists of:

- 🔒 identifying your assets
- 🔒 classifying those assets based on importance
- 🔒 considering potential threats,
- 🔒 and determining what impact an attack could have on the county.

Organizational policies and processes that focus on hackers and other outside threats are missing another danger that could come from the next cubicle.

So what's at risk? Financial accounts, certainly. Handling banking and other financial tasks online is routine in almost every county. What if your CFO logged on one day to find that someone had transferred all the county's money to an offshore account? This is a very real possibility – it's happened to other government offices. Thieves would love to get at all the personally identifiable information that your county maintains, and there are potentially thousands of ways that criminals could benefit from stealing or changing the information in county files, such as property tax records to parole eligibility dates.

As you embark on bolstering your county's security, it's good policy to:

- 🔒 involve other stakeholders (government and private sector) in identifying which assets are at risk,
- 🔒 ensure staff, elected officials and related parties take cyber-threats more personally.

Indeed, intentionally engaging stakeholders opens the dialogue and generates more thoughtful and holistic preparation toward protecting the county's assets. Where are the threats? It's not too presumptuous to assume that threats are everywhere, and that the types of threats as well as their origins can vary significantly. Organizations need to protect against malicious code, spyware, hackers, zero-day attacks, denial of service attacks, data interception and theft, and identify theft.⁷

Some threats are intentional, as when intruders break into your systems and embed malware to damage or destroy data. Indeed, millions of new strains of malicious code are discovered every year, many of them are destructive programs that can disrupt a computer, steal data, deny a website's operation or shut down an entire network.⁸ Outsider attacks can also arise opportunistically – a software bug can create a vulnerability in your network that may leave it open to an attack.

⁷ Cisco. "What is Network Security?"

Accessed at www.cisco.com/cisco/web/solutions/small_business/resource_center/articles/secure_my_business/what_is_network_security/index.html

⁸ Panda Labs. "A Look Back at Cybersecurity in 2012." Accessed at <http://pandalabs.pandasecurity.com/a-look-back-at-cyber-security-in-2012/>



Most of us recognize the dangers that hackers and cybercriminals present – but network, security, and risk management professionals agree that many of the most significant threats originate from within an organization. Two thirds of IT executives surveyed said they worry most about staff accidentally causing a data breach or security problem, malicious insiders such as disgruntled employees and unsecured or non-compliant employee devices.⁹

That said, organizational policies and processes that focus solely on hackers and related outside threats fail to address a less obvious, but bigger dangers that originate from within the organization. Therefore, effective risk management demands network security policies that address internal and external threats. Equally important, the county must enforce its network security policies. Forgetting to block network access when an employee leaves the organization, neglecting to make other updates and apply patches, or making other updates throughout the network leave the organization vulnerable to serious damage to county assets, which may include:

- ⚠ viruses erasing an entire operating system
- ⚠ an intruder altering files
- ⚠ hackers using county/municipal computers to attack other networks and
- ⚠ thieves stealing county or personal information such as Social Security and credit card numbers.¹⁰

[cybersecurity training]

Information systems today provide high levels of security when properly configured and monitored. Employees are often among the weakest links in network security. They expose protected information by losing a laptop or by opening an email and then clicking infected attached files, HTML messages and embedded scripts, thereby unleashing a virus into the system. It takes just one person to engage with malware in this manner to give hackers access to that employee's computer and potentially your entire network.

⁹ AlgoSec, Inc. "The State of Network Security 2013: Attitudes and Opinions."

Accessed at www.algosec.com/resources/files/Specials/Survey%20files/State%20of%20Network%20Security%202013_Final%20Report.pdf

¹⁰ United States Computer Emergency Readiness Team. Accessed at www.us-cert.gov/

Counties today must engineer network security policies, communicate them clearly, and provide ongoing education so staff and other stakeholders understand their role in protecting the county's data and network assets. Provide thorough cybersecurity training to all your stakeholders, followed by continuing education to keep everyone aware of potential and evolving threats.

Training will be more effective if a users' manual is provided that clearly outlines stakeholders' responsibilities. A good example is "Information Assurance: What you Need to Stay Safe and Help Protect the County's Assets¹¹," written by Ralph Johnson, Chief Information Security and Privacy Officer of the King County (Washington) Department of Information Technology. The book, excerpts of which appear in Section V. of this guide-book, features clearly stated, easily understandable policies on enterprise information security, information privacy, password management, protected electronic information, acceptable use of information assets, employee and third party access, encryption standards, telecommuting, least restrictive access, and termination.

As technology becomes increasingly more sophisticated, the demand for an experienced and qualified workforce to protect our nation's networks and information systems has never been higher. The National Institute for Cybersecurity Careers & Studies (NICCS) serves as a national resource for cybersecurity awareness, education, training, and career opportunities. NICCS is the implementation of the National Initiative for Cybersecurity Education (NICE), whose goal is to establish an operational, sustainable and continually improving cybersecurity education program for the nation to use sound cyber practices that will enhance the nation's security. NICE is a nationally-coordinated effort that focuses on cybersecurity awareness, education, workforce structure, and training/professional development. NICCS takes the information developed by NICE and makes it available to the public. Visit www.niccs.us-cert.gov to learn more.

Counties today must engineer network security policies, communicate them clearly to provide ongoing education so staff and other stakeholders understand their role in protecting the county's data and network assets.



11 Johnson, Ralph. "Information Assurance: What you Need to Stay Safe and Help Protect the County's Assets." July 26, 2012

Accessed at www.naco.org/newsroom/countynews/Current%20Issue/1-14-13/Pages/Policies-Counties-Should-Have-to-Protect-Information-Assets.aspx

[train. reinforce. repeat often.]

It's also imperative to find ongoing ways to remind stakeholders how important they are in keeping your network and other assets safe. The Center for Internet Security (CIS) offers lots of useful resources on cybersecurity to help effectively communicate this issue with your staff and elected officials. Other excellent resources include the Protect Your Workplace Campaign from the U.S. Computer Emergency Readiness Team (US-CERT), available at www.uscert.gov/readingroom/distributable.html; and the website OnGuardOnline, published by a consortium of the Department of Justice, Federal Trade Commission, Department of Homeland Security, U.S. Postal Service, and Securities and Exchange Commission, available at www.onguardonline.gov.



train



reinforce



repeat often

Issuing regular reminders is a small step but an important and effective one. Properly educating and communicating with your staff is considered an excellent first line of defense against cyber intruders.

[new technologies change the landscape]

In the past, county networks consisted of a fixed number of locations – often just one building. Today, a county's network may extend across towns and across the country, expanding to accommodate employees who work from home or on the road, in patrol cars, and at satellite locations. Securing these off-site locations as well as the home base is a challenge, as is accommodating the variety of devices employees use to access the county network.






Making this challenge more complicated is the growing use of mobile devices for work-related purposes. This has contributed to a wave of attacks targeting cellphones and tablets. Every new mobile device provides another opportunity for a cyber-attack. In an effort to protect their networks, some organizations have banned the use of personal cellphones, personal laptops and storage devices like flash drives in the workplace.

Conversely, some organizations not only allow but encourage employees to "Bring Your Own Device" (BYOD) into the workplace, thereby potentially reducing a county's hardware expenses but multiplying its security risks. If you plan to permit employees to use their own devices, you need a policy that governs who can bring a device, which devices are acceptable and which digital resources the employees are permitted to use. If you allow staff to access county networks or store county information on personal devices, there should be a policy in place that gives IT governing control over the devices in case they are lost, stolen or misused. If staff use county devices to work at home, your policies should specify when and how they're permitted to access the county network and the public Internet with the devices.

If you plan to permit employees to bring their own devices, you need a policy that governs who can bring a device, which devices are acceptable and which digital resources the employees are permitted to use.

In addition, new capabilities such as Near Field Communication (NFC) will increase the opportunities for cyber criminals to exploit weaknesses. NFC enables smartphones to communicate with each other by simply touching two devices together or bringing them into close proximity. This technology facilitates credit card purchases and lets users see advertisements or coupons for nearby retailers. Risks with using NFC include intercepted transmission of credit card numbers and other data, and transferring viruses or other malware from one NFC-enabled device to another.

As each new technology is introduced, criminals search for ways to exploit any weaknesses for their own gain. You can help fend off attacks by using smart cybersecurity practices such as these:

-  Enable encryption and password features on your smart phones and other mobile devices.
-  Use strong passwords that combine upper and lower case letters, numbers, and special characters, and do not share them with anyone. Use a separate password for every account. In particular, do not use the same password for your work account on any other system.
-  Disable wireless, Bluetooth, and NFC when not in use.
-  Properly configure and patch operating systems, browsers, and other software programs. This should be done not only on workstations and servers, but mobile devices as well.
-  Use and regularly update firewalls, anti-virus, and anti-spyware programs. Do not use your work email address as a "User Name" on non-work related sites or systems.

- 🔒 Be cautious regarding all communications; think before you click. Use common sense when communicating with users you know and those you don't know. Do not open email or related attachments unless you absolutely trust the source.
- 🔒 Don't reveal too much information about yourself online. Revealing information could make you the target of identity or property theft.
- 🔒 Be careful with whom you communicate or provide information on social media sites. Those "friends" or games might be looking to steal your information.
- 🔒 Allow access to systems and data only to those who need it and protect those access credentials.
- 🔒 If the device is used for work purposes, do not share that device with friends or family.
- 🔒 Follow your organization's cybersecurity policies and report violations and issues immediately.¹²



12 Multi-State Information Sharing & Analysis Center. "Emerging Trends and Threats for 2013." Accessed at <http://msisac.cisecurity.org/newsletters/2013-01.cfm>

[measurement and reporting]

Your county may build most policy and governance standards from the ground up, through trial and error and consensus. When it comes to information security standards, however, few organizations have the expertise, resources, and time to develop their own. The Benchmarks Division of the Center for Internet Security creates and maintains a wide range of security configuration benchmarks (currently for over 70 systems, applications and devices covering 14 different technologies) to help organizations improve security by reducing vulnerabilities to information assets. The benchmarks include specific and actionable hardening procedures for IT systems and assets, which are defined through a consensus-development process including security professionals from around the globe.

These are the only consensus-based, best-practice security configuration guides available that are both developed and leveraged by government, business, industry and academia. PDF versions of the benchmarks available at no cost are downloaded hundreds of thousands of times every year. You can obtain them from the Center for Internet Security website at: <https://benchmarks.cisecurity.org/downloads/multiform/index.cfm>.

Incident response has become an important component of cybersecurity programs. Because performing incident response effectively is a complex undertaking, establishing a successful incident response capability requires substantial planning and resources. The National Institute of Standards and Technologies (NIST) published a Computer Incident Reporting Guide to assist organizations in establishing computer security incident response capabilities and handling incidents efficiently and effectively. This publication provides guidelines for incident handling, particularly for analyzing incident-related data and determining the appropriate response to each incident. The guidelines, which can be followed independently of particular hardware platforms, operating systems, protocols, or applications, are available at <http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf>.

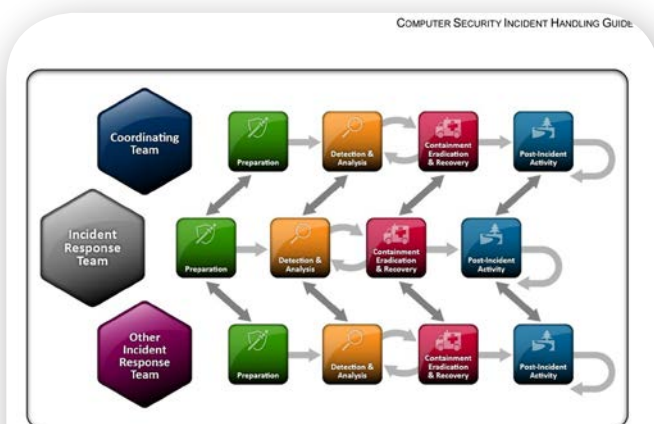


Figure 4-1. Incident Response Coordination

4.1.1 Coordination Relationships

An incident response team within an organization may participate in different types of coordination arrangements, depending on the type of organization with which it is coordinating. For example, the team members responsible for the technical details of incident response may coordinate with operational colleagues at partner organizations to share strategies for mitigating an attack spanning multiple organizations. Alternatively, during the same incident, the incident response team manager may coordinate with ISACs to satisfy necessary reporting requirements and seek advice and additional resources for successfully responding to the incident. Table 4-1 provides some examples of coordination relationships that may exist when collaborating with outside organizations.



policy and governance/checklist

- ☐ Does your security policy enable your security team the flexibility to mature the security program at the speed of today's business?
- ☐ Does your security policy enable your security team to accurately define what risk means to your enterprise?
- ☐ Does your security team meet regularly with your business and risk management groups to keep the risk definitions current?
- ☐ Is the identified risk easily illustrated and explained?
- ☐ Do all of your employees receive annual security training appropriate to their job responsibilities?
- ☐ Is your security policy in strategic alignment with your business initiatives and goals?
- ☐ Does your security team work with the business and risk management groups to ensure that security governance, policy, and risk are maintained at an equitable level across every location?
- ☐ Does your security policy enable your security team to manage the security of your enterprise programmatically and systematically?
- ☐ As new technologies or changes in technologies are implemented, does your security team do a risk assessment to ensure that the risks do not exceed accepted norms?
- ☐ Does your security team have the ability to quickly evaluate the security controls and risk factors within your enterprise?

If you could not check 2 or more of these items, now would be a great time to sit down with your security team and make the necessary changes. If you could not check 4 or more of these items now would be a great time to have an impartial third party do a gap analysis on your security program and provide a list of a remediation activities to reach an acceptable level of compliance.

*This tool was developed by Sebron K. Partridge,
NACo member and Chief Information Security Officer of Riverside County, California.*

industry standard security control references

cyber_for_counties
{guidebook} v1.0



**CYBER FOR
COUNTIES**

Content is copyright protected and provided for personal use only - not for reproduction or retransmission.
For reprints please contact the Publisher.



industry standard security control references

A few years ago thieves broke into the home of a Veterans Administration analyst and stole a laptop and external hard drive that contained an unencrypted database of names, birthdates, Social Security numbers, and disability ratings for 26.5 million active duty military personnel, veterans, and their spouses. The VA estimated it would cost \$100 million to \$500 million to prevent and cover possible losses from the theft. Fortunately, the stolen items were returned a month after they were taken.¹³

The state of South Carolina wasn't as fortunate. Last year, international hackers stole 3.6 million Social Security numbers and 387,000 payment card numbers from state income tax records.

Most cybercrimes pale in comparison with what could happen if the any of the vital services provided by counties and other agencies were attacked.

The attack, the largest ever against a state agency, put 75 percent of the state's population at risk for identity fraud and compromised information belonging to more than 650,000 businesses. State officials blamed outdated computers and security flaws at its Department of Revenue for enabling the hackers to access the tax records. The state is paying up to \$12 million to provide a free year of credit monitoring and identity theft protection to anyone affected.¹⁴

As disturbing as these cyber-crimes are, they pale in comparison with what could happen if any of the vital services provided by counties and other government agencies were attacked. In a story reported in *County News*, Seattle's Chief Information Security Officer Mike Hamilton put the issue in perspective: "All of the news that you read is all about loss of records, and 'wow, it's a bummer to lose those Social Security numbers,' and 'wow, it's expensive to comply with data-breach reporting statutes,'" he said. "On the other hand, if the control systems that move clean water in and sewage out for treatment stop working for 48 hours, there will be absolute mayhem in the streets."¹⁵

Already, there are documented cases of attackers accessing industrial control systems. The FBI confirmed a report that hackers recently took over remote control of a New Jersey company's HVAC system; no harm was done, but some cybersecurity experts note that a system so easily breached could attract terrorists intent on committing sabotage.¹⁶

13 "Top 5 Data Thefts." The Christian Science Monitor. May 4, 2011.

Accessed at www.csmonitor.com/Business/2011/0504/Data-theft-Top-5-most-expensive-data-breaches/5.-US-Veterans-Affairs-25-30-million

14 Accessed at www.nytimes.com/2012/11/21/us/more-details-of-south-carolina-hacking-episode.html?_r=0

15 Taylor, Charles. "Cybersecurity Threats Abound, and Not Just to your Data." NACo County News, Vol. 45, No. 1, Jan. 14, 2013.

Accessed at www.naco.org/newsroom/countynews/Current%20Issue/1-14-13/Pages/Cybersecurity-threats-abound,-and-not-just-to-your-data.aspx

In the sections that follow are experts' recommendations for securing your networks, and information about the Critical Security Controls, a detailed network security plan designed by the National Security Agency and a consortium of public and private entities to help organizations prioritize efforts and strengthen their defense against cyber-attacks.

[the 20 critical security controls]

Many countries have found that the 20 Critical Security Controls is an effective blueprint for enterprise computer security. The document prescribes how to block or mitigate known attacks; provides guidance on network and endpoint devices, their applications and the vulnerabilities; and covers malware defense, controlled access and recovery, and data protection.¹⁷

The core tenet of these controls is that many organizations can add new technologies and practices and automate and integrate Controls already in place to make their data networks more resistant and resilient to attack. The Controls focus on automation to provide cost efficiency, measurable results, scalability, and reliability. According to SANS, the five critical tenets of an effective cyber defense system as reflected in the Critical Controls include:

-  **Offense informs defense:** Use knowledge of actual attacks that have compromised systems to provide the foundation to build effective, practical defenses. Include only those controls that can be shown to stop known real-world attacks.
-  **Prioritization:** Invest first in controls that will provide the greatest risk reduction and protection against the most dangerous threat actors, and that can be feasibly implemented in your computing environment.
-  **Metrics:** Establish common metrics to provide a shared language for executives, IT specialists, auditors, and security officials to measure the effectiveness of security measures within an organization so that required adjustments can be identified and implemented quickly.
-  **Continuous monitoring:** Carry out continuous monitoring to test and validate the effectiveness of current security measures.
-  **Automation:** Automate defenses so that organizations can achieve reliable, scalable, and continuous measurements of their adherence to the controls and related metrics.

¹⁷ Hietala, Jim D. "Implementing the Critical Security Controls." April 2013. Sans Institute.

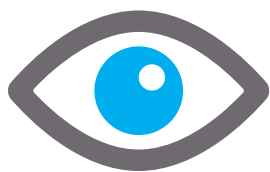
Accessed at www.sans.org/reading_room/analysts_program/implementing-critical-security-controls.pdf

Few organizations have the financial and human resources to implement all 20 Controls at once. Some experts recommend implementing as many as possible and making a schedule to add the remaining Controls over the next few years. The case studies that follow show how two organizations introduced the Controls by focusing on the areas in which they most needed to improve the security. This strategy was more affordable, easier for the organization's IT departments to manage, and resulted in quick wins that significantly increased their security.

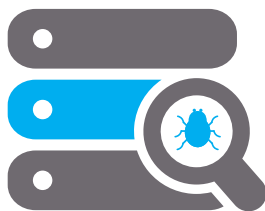
The two case studies that follow are shortened versions of Critical Security Controls Case Studies included in the SANS Institute's "Implementing the Critical Security Controls," written by Jim D. Hietala. For the full case studies see:

www.sans.org/reading_room/analysts_program/implementing-critical-security-controls.pdf.

In both of these case studies, organizations with limited budgets with which to tackle new security projects were able to leverage existing investments in security and IT systems management tools. They were able to make improvements in coverage, operational guidance, metrics, and measurement to fully realize the security benefits of each control. The organizations also faced common challenges in obtaining commitments from the business to provide the human resources needed to operate new security projects.



monitor



detect



prevent

20 critical security controls: V4.1

Critical Control 1:

Inventory of Authorized and Unauthorized Devices

Critical Control 2:

Inventory of Authorized and Unauthorized Software

Critical Control 3:

Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

Critical Control 4:

Continuous Vulnerability Assessment and Remediation

Critical Control 5:

Malware Defenses

Critical Control 6:

Application Software Security

Critical Control 7:

Wireless Device Control

Critical Control 8:

Data Recovery Capability

Critical Control 9:

Security Skills Assessment and Appropriate Training to Fill Gaps

Critical Control 10:

Secure Configurations for Network Devices such as Firewalls, Routers, and Switches

Critical Control 11:

Limitation and Control of Network Ports, Protocols, and Services

Critical Control 12:

Controlled Use of Administrative Privileges

Critical Control 13:

Boundary Defense

Critical Control 14:

Maintenance, Monitoring, and Analysis of Audit Logs

Critical Control 15:

Controlled Access Based on the Need to Know

Critical Control 16:

Account Monitoring and Control

Critical Control 17:

Data Loss Prevention

Critical Control 18:

Incident Response and Management

Critical Control 19:

Secure Network Engineering

Critical Control 20:

Penetration Tests and Red Team Exercises

critical security controls case study {the city of portland/oregon}

regulatory compliance is a key driver in adopting controls in stages

Organization: The City of Portland, Oregon's IT Security Bureau provides central IT services for 20 city departments, including police, fire, and housing. It also manages the firewalls, VPNs (Virtual Private Networks), configuration management and more, supporting more than 6,000 employees, 6,000 endpoints and 350 servers.

Challenges: Handling numerous responsibilities meant Portland's small IT Security team – just a director and four engineer/analysts – had little time for security planning, which made the city's approach reactive rather than strategic. Developing a long-term network security framework was further complicated by the fact that many city departments were required by law or policy to comply with a variety of IT security standards, including the Payment Card Industry Data Security Standard (PCI DSS) and the Health Insurance Portability and Accountability Act (HIPAA). Budget constraints and a scarcity of qualified candidates for the city's hiring pool further limited Portland's options.

Solution: When the city approved IT expenditures for a few projects necessary to meet regulatory requirements, its IT Security Bureau saw a chance to strengthen security across the network. After considering other possibilities, the team chose the 20 Critical Security Controls (CSCs), a framework judged by experts from both government and the private sector as vital in preventing cyber-attacks.

Implementation: The CSCs provided the IT team with a structure for defining benefits, which enabled them to show city officials how the benefits would offset costs and add value over time. The team determined that the savings in capital and human resources could fund implementation of two new controls per year.

The Portland IT bureau recognized that the CSCs could be deployed individually, allowing the city to target areas most in need of improved security and leverage quick wins with minimal effort and expenditure. They initially focused on low-hanging fruit, controls that had a low cost and

"low drag" in terms of human resources, but that provided real risk reduction. This approach built on several areas in which some tools were already in use. Portland's early wins included:

- 🔒 Revoking local administrator privileges where practical and making it standard for staff to have ordinary user privileges (Critical Control #12)
- 🔒 Deploying standard configurations from gold master images (Critical Control #3)
- 🔒 Implementing regular and frequent patching for all core applications, and extending patching to include Adobe Reader, Adobe Flash and Java. (Critical Control #3)
- 🔒 Centralized antivirus protection for all endpoint devices. (Critical Control #5)

Benefits: The city's IT security posture has measurably improved since the initial adoption of the Critical Security Controls framework. The advantages so far:

- 🔒 The biggest benefits of adopting the Controls came in the form of additional structure for the information security program and a framework for planning additional projects and measuring progress.
- 🔒 A subtler benefit has been the acceptance of a common vocabulary throughout the IT organization.
- 🔒 As the security vocabulary is accepted, operations and business groups are more readily embracing security enhancements. Staff can understand the goals of each of the Controls and how security will improve when they are adopted.
- 🔒 The security team members saw fewer endpoint infections, which they attribute to administrative privileges and better patching.
- 🔒 Fewer trouble tickets were issued for configuration issues, thanks the city's using standard images for desktops and servers and ensuring policy conformance through the directory service; this enabled the IT bureau to focus on higher-value tasks, such as improving the security posture.

critical security controls case study {bankia}

how a financial conglomerate used the controls to support a merger

Government agency: Bankia is government-owned financial conglomerate headquartered in Madrid that was formed in 2011 from a merger of seven Spanish banks, including Spain's oldest bank, CajaMadrid. Two years earlier, CajaMadrid had begun implementing the Open Information Security Management Maturity Model (O-ISM3) and started developing a new approach to information security management.

When CajaMadrid became part of Bankia, the IT projects continued: rather than build an entirely new information security management system, Bankia IT staff opted for a bottom-up approach, starting with vulnerability management. O-ISM3 provided the initial framework for measuring the vulnerability of the bank's web applications and remediation of any weaknesses, and for focusing web application development managers on the goal of continuous improvement. Originally a private institution, Bankia was nationalized by Spain in 2012 after the bank required the largest bailout in the country's history.

Challenges: Prior to the O-ISM3 implementation, Bankia attempted to test new applications before putting them into production, relying on subsequent scans performed at irregular intervals to detect flaws – but no success criteria had been defined for these vulnerability assessment or remediation efforts. The bank didn't capture metrics, and so had no way to continuously improve its vulnerability management program. It also lacked a consistent terminology for the security program, specifically in the area of vulnerability management.

Solution: O-ISM3 provided the initial framework that helped Bankia accomplish several important tasks:

-  establish goals & objectives
-  measure activity
-  define success criteria, and
-  manage vulnerability scanning and remediation towards continuous improvement.

As Bankia's approach developed, its IT group added the Critical Security Controls, focusing initially on CC #4, Continuous Vulnerability Assessment and Remediation. It soon became clear that the how-to guidance the CSCs provided added valuable practitioner detail to the knowledge management aspects of the bank's vulnerability management program. The guidance in Critical Control #4 also brought about some quick wins; its metrics for success supplied all the detail that the bank required for its measurement and continuous improvement functions.

The team started with its web applications, which the bank considers to be highly critical for customer business and because web applications have become a primary attack vector. For these applications, vulnerability management represented low-hanging fruit from which the bank would get the most return on its security improvement investment.

Benefits: Bankia was able to add the additional guidance and metrics from Critical Control #4 to the existing O-ISM3-based vulnerability management program, with impressive results in outcomes:

- 🔒 significantly more vulnerabilities were discovered and fixed
- 🔒 web app checks now occur much more frequently
- 🔒 staff hours spent manually scanning applications are significantly reduced
- 🔒 there's a lower cost in dealing with vulnerabilities
- 🔒 vulnerability repair is streamlined
- 🔒 there's less cost and overhead in managing web apps and
- 🔒 more apps are repaired, reducing the attack service dramatically.

Conclusion: Large IT organizations have to respond to many departmental needs and business requirements. Security is a critical requirement, but it is far from being the only important issue that IT organizations have to deal with, or even the most important one. In the real world where Chief Information Officers (CIOs) operate, budgets are limited and other obstacles to change have to be managed.



industry standard security control references/checklist

do your security controls provide the following?

- ☐ CC1 Identification of the relationship between IT assets and business processes for a clear understanding of business impact arising from the loss or unavailability of an IT asset.
- ☐ CC1/CC2 Identification of the relationship between employees and the equipment and software they support for a clear understanding of business impact resulting from the loss or unavailability of an employee.
- ☐ CC1/CC2 Linking IT assets, employee resources, and business processes provides both the business and IT staff clear insight into the ongoing IT budget required to sustain that process.
- ☐ CC4 Automated monitoring and reporting of software patch status.
- ☐ CC4/CC5 Automated monitoring and reporting of the antivirus protection on all end points at a central location.
- ☐ CC5 Automated monitoring and reporting of suspicious network traffic.
- ☐ CC6 Ensures that your software development lifecycle includes oversight by a software developer with security experience and collaboration with an expert from your security team on any homegrown or third-party software.
- ☐ CC7 Mobile device network registration and authentication processes.
- ☐ CC8 Data classified so that your ability to recover data to support specific business processes meets the business expectations for IT systems recovery.
- ☐ CC9 Training processes that support easily updating the training materials.
- ☐ CC9 Training that is easily accessible to all employees and contractors that will be accessing your information.

These are just touch points that you can use as you assess your network security – they are NOT comprehensive. There are many more individual facets of these 20 security controls that your organization must develop to ensure that your security program continues to evolve to meet the ever-changing threat landscape that counties face on a daily basis.

- ❑ CC9 Training that has automated monitoring and reporting for ease of tracking compliance.
- ❑ CC10/11 Access to configuration backups and configuration documentation for devices on your network.
- ❑ CC12 Separation of duties of IT administrators to ensure no individual administrator that has the ability to add/change/delete privileges or data can also edit the logging of those same systems.
- ❑ CC13 Clear documentation of the expected network traffic between your network segments and between your network and the internet.
- ❑ CC13 Automated alerting to notify your network operations center of any traffic that has not been previously documented.
- ❑ CC14 Time allotted to operational staff to review logs on a daily basis.
- ❑ CC15 Information categorized and aligned with the business process to ensure that only those business personnel and customers who need access are provided access rights to that information.
- ❑ CC16 IT system logging configured to automatically log successful and failed information access attempts.
- ❑ CC17 The ability to track information as it is saved to, copied to, cut and pasted to, and emailed to locations other than the original location.
- ❑ CC18 Event escalation process and procedure to ensure consistent response and escalation of events from event to incident through resolution and remediation.
- ❑ CC18 Training that ensures everyone in your organization is capable of responding to and successfully working through an incident to its successful remediation.
- ❑ CC19 Minimizes access to only the access required by the users, equipment and applications that are known and validated in your environment.
- ❑ CC20 Schedule independent security analysts to do penetration when there are any significant changes to your IT environment or at a minimum on an annual basis.

*This tool was developed by Sebron K. Partridge,
NACo member and Chief Information Security Officer of Riverside County, California.*



Electronic content provided for personal use only - not for reproduction or retransmission. For more information please contact the Publisher.

operational best practices

cyber_for_counties
{guidebook} v1.0



operational best practices

The data each county collects and stores is extremely valuable to thieves – bank and credit card accounts, personal financial data, Social Security numbers, health records and much more is at stake. Here are some practical suggestions for protecting your essential data.

[authentication, authorization and access]

Authentication is any process by which you verify that someone trying to access your network is who they claim to be. At the most basic level, this means inputting a username and password. Many government agencies have begun requiring more stringent, two-factor authentications. This requires users to present another form of identification such as a temporary access code delivered to a smartphone.¹⁸



authentication



authorization



access

Organizations , including county governments, that access the Criminal Justice Information System (CJIS) database must adhere to a higher standard- multi-factor authentication; besides a login ID and password, CJIS requires biometric identifiers such as a fingerprint, user-based public key infrastructure, smart cards, software token or hardware token.¹⁹

Authorization is the mechanism that determines what level of access to resources each authenticated user should have. County health department employees, for instance, need to access medical files to complete their work responsibilities, but staff from the engineering office should not be authorized to see these files. Authorization strategies may be set up to give employees the ability to see but not make changes to some files, but permit others to make changes. Restricting file access to authorized personnel is especially important when it comes to data protected by regulations or laws such as the Health Insurance Portability and Accountability Act (HIPAA).

¹⁸ Peterson, Tommy. "The Growing Wave of Two-Factor Authentication in Local Government." StateTech. January 10, 2013.

Accessed at www.statetechmagazine.com/article/2013/01/growing-wave-two-factor-authentication-local-government




¹⁹ Criminal Justice Information System Mandate. 2013. Accessed at www.cjismandate.com/

Finally, access refers to controlling one's ability to get to an online resource. Access can be granted or denied based on a wide variety of criteria, such as the network address of the client, the time of day, or the browser that the visitor is using. Access control is analogous to locking the gate at closing time; it's controlling entrance by some arbitrary condition which may or may not have anything to do with the attributes of the particular visitor.²⁰

[email security]

By Ralph Johnson, *CISSP, HISP, CISM, CIPP/US*, Chief Information Security and Privacy Officer of the King County (Washington) Department of Information Technology

Mr. Johnson wrote the handbook, "Information Assurance: What You Need to Stay Safe and Help Protect the County's Assets." This email policy and the Web Security section that follows are excerpted from that book.

-  ***Do not open an email attachment or file unless you know who it's from.*** Save attachments to your hard drive to allow the antivirus program to scan them before opening.
-  ***Do not click on an embedded link unless you know who sent it.***
-  ***Keep antivirus software up to date.*** If you think your computer is not updating automatically, contact your county's IT support center.
-  ***Do not forward any type of security, informational, or virus warnings. Report them to your IT support center.***
-  ***Know how to deal with email spam and hoaxes.*** If you receive an email message that you believe is a hoax, take the time to check the facts. Delete the message and notify your IT director. For hoax information, visit: <http://vil.nai.com/vil/hoaxes.aspx>.
-  ***Beware of spoof email claiming to be from a company you trust asking for personal information.*** This is called phishing. The email may inform you that there is a problem with your account/password. There may be a link to click. Forward any of these emails to the company it claims to be sent from (each organization usually provides an "abuse" email address on their webpage). Reputable organizations like Yahoo!, MSN, Gmail or your bank will never ask you for your email password. Don't fall for it.
-  ***Make sure to disable Outlook attachment previews.*** Attachment previews takes away your ability to decide whether or not to open an attachment.²¹

20 Drexel University. "Authentication, Authorization, and Access Control." Accessed at <http://cluster.cis.drexel.edu/manual/howto/auth.html>

21 Johnson, Ralph. "Information Assurance: What you Need to Stay Safe and help protect the County's Assets." July 26, 2012.

Accessed at www.naco.org/newsroom/countynews/Current%20Issue/1-14-13/Pages/Policies-Counties-Should-Have-to-Protect-Information-Assets.aspx

[website and social networking best practices]

The Internet has a wealth of information and resources but it also is a source for malicious software. Some examples of non-business sites, which if visited could lead to malware infection include any that contain:

- ⚠ adult content
- ⚠ gambling oriented messages
- ⚠ personal chat rooms.

When signing up for, installing or agreeing to anything, read the fine print. If you do not want to receive junk mail or get put on a telemarketer list, look for a box usually near the bottom of the page that asks if you want to receive information and offers – this is called “opting out.” Most companies assume you want to “opt in,” so the box will likely be checked. Read the information carefully and select what’s appropriate for you. The best sites will have a privacy policy regarding your information and what they do with it. Some sites require you to give all your information to get the product or service they are offering. Provide only the information marked “required.”

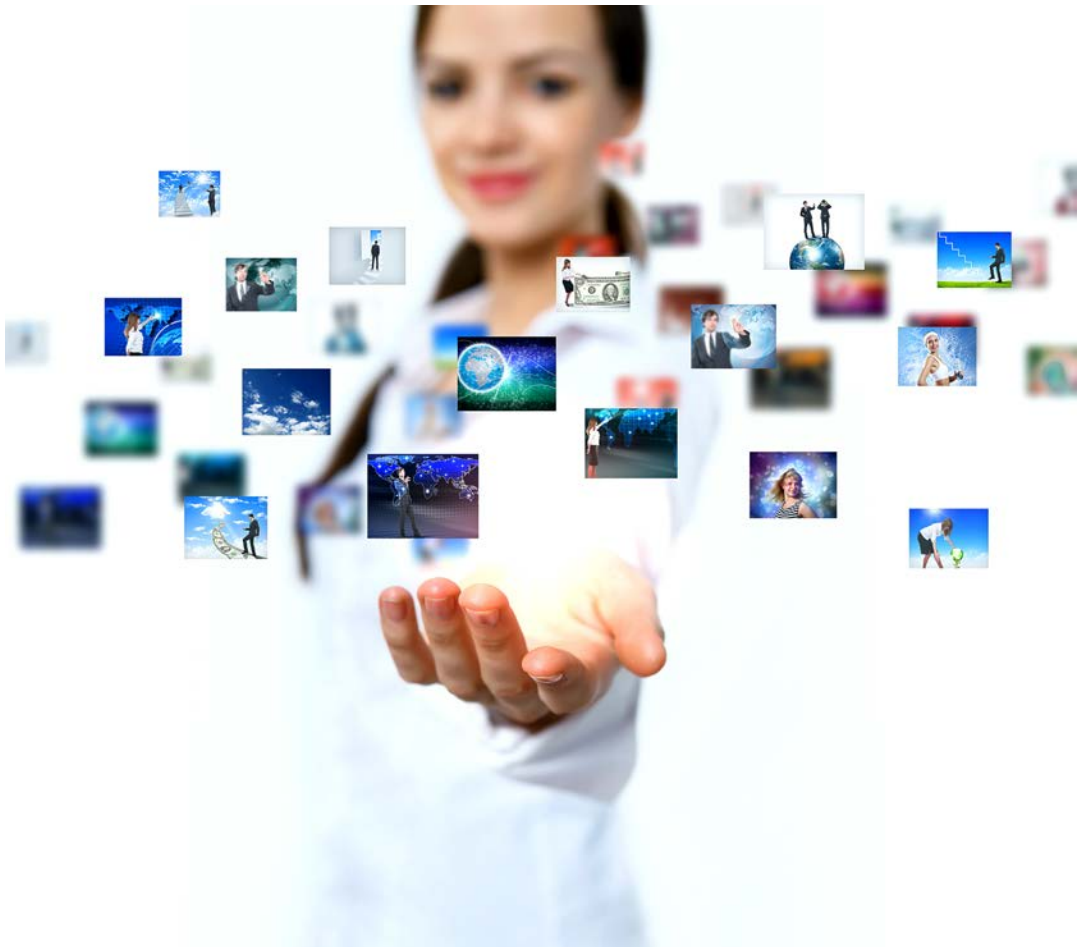
Do not give out your full name, address, or phone number to anyone online that you don’t trust or know personally. This is especially important in chat rooms. Beware of mass distribution letters (i.e. very general emails that don’t actually address you personally), anyone who wants to negotiate a wire transfer, and anyone who wants to work out a business arrangement while they’re abroad, including your friends.

Social Networks – Social networking is everywhere. With social networks people across the world have access to tools and options that were previously non-existent. However, with these opportunities to connect with others come potential dangers. Social networking has opened up many new doorways for cybercrime, and with all the people on social networks who are new to technology, it is more important than ever to make sure you are aware of the risks.

Phishing/Scams – There are a number of scammers on social networks who may try to steal or use your personal information – information that can potentially be used for crimes such as identity theft or fraud. Once someone has your password they can use it to destroy your profile or send out spam messages and viruses, which could do irreparable damage to your online reputation, not to mention your financial one. Always make sure you are at the right website when you enter your credentials. You can do this by double checking the address bar and making sure you are in the right place before you log in.

Employment – One thing we often forget while having fun on social networks is that almost anybody can see what we are doing. While we are tagging photos of what we did on the weekends or tweeting our thoughts it can be easy to forget that someone at work or potential employers may see this.

Acceptable Use of the Internet: Never download or install software unless you get specific approval ahead of time. Do not visit chat rooms using county resources.²²



operational best practices 41

Content is copyright protected and provided for personal use only - not for reproduction or retransmission.
For reprints please contact the Publisher.

[network infrastructure and security]

The following suggestions provide guidance on ways to secure your infrastructure and systems.

Passwords: Use strong passwords to secure your information. Passwords should have at least eight characters and include uppercase and lowercase letters, numerals and special characters. It is important to keep different passwords for different accounts. This will reduce the chances that if one password fails your other accounts will be vulnerable as well. Do not use the same passwords for accessing work systems on any other accounts.

If your computer is not updated, you are leaving it open to attack via these vulnerabilities. Set programs and systems to auto-update to avoid missing a critical update.

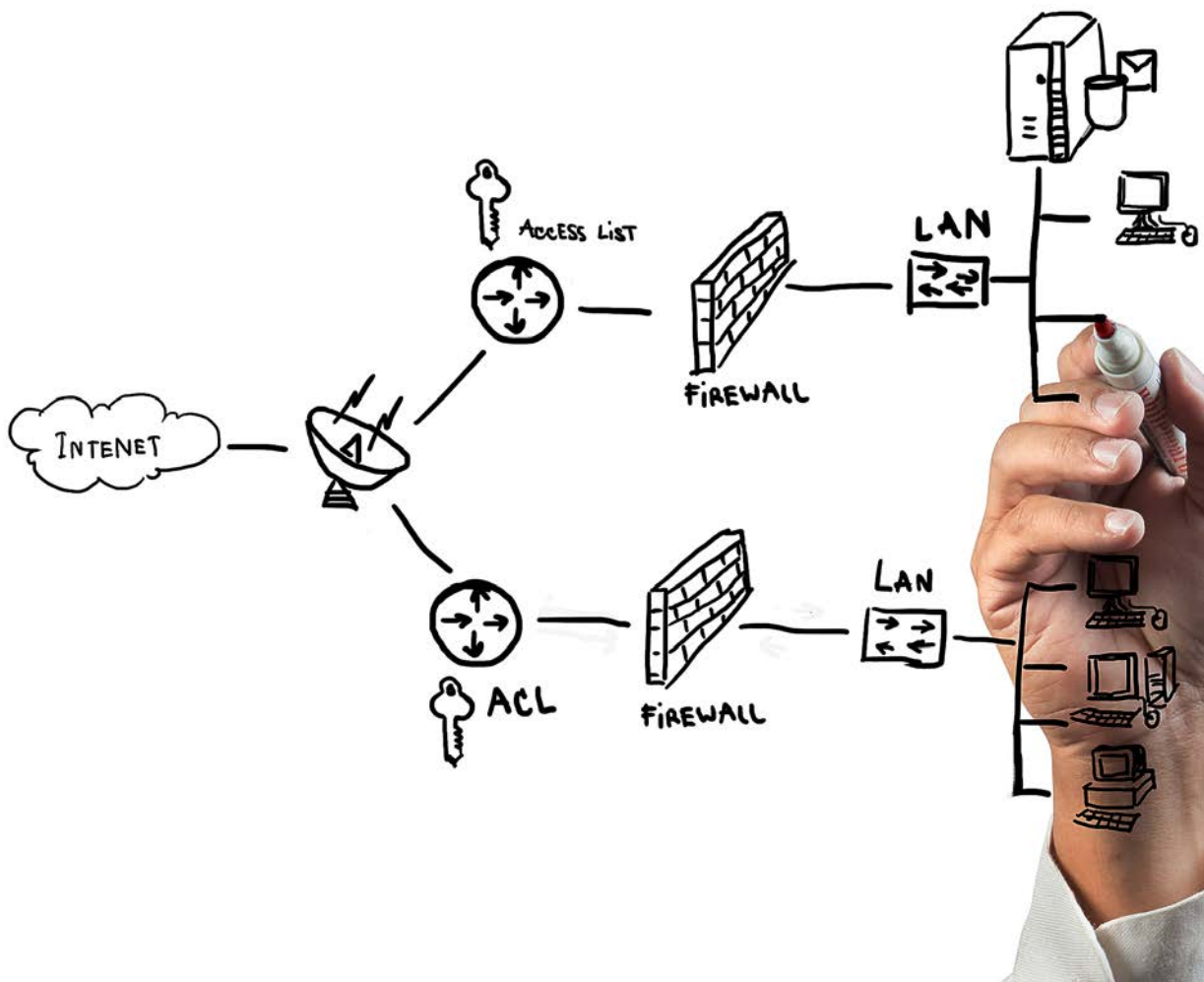
External Devices: Many organizations have policies that limit the use of external devices (computers or devices such as thumb drives, smartphones and mobile devices that are not the property of the organization). These policies are intended to protect the overall system.

Admin vs. Non-Admin accounts: Administrator or "Admin" accounts have more control over programs and settings for your computer. Hackers can potentially take control of your computer by accessing these accounts. Non-Administrator accounts, or guest accounts can still use programs, but limit the ability to make changes that hackers need to harm your computer. It is important to change the default password on your Admin accounts and to always run your computer as a non-administrator or non-admin unless otherwise needed.

Systems and software updates: It is important to keep your systems and software up-to-date. System and software vendors often find vulnerabilities that they fix in the latest update. If your computer is not updated, then you are leaving it open to attack via these vulnerabilities. Set programs and systems to auto-update to avoid missing a critical update. This includes your operating system, business applications, media players, browsers, and other programs that can access the Internet.

Mobile devices: It is important to make sure you secure your portable devices to protect both the device and the information contained on the device. Establish a password and enable screen lock or auto lock on all devices. If your device has Bluetooth functionality and it's not used, check to be sure this setting is disabled. Some devices have Bluetooth-enabled by default. If the Bluetooth functionality is used, be sure to change the default password for connecting to a Bluetooth enabled device. Encrypt data and data transmissions whenever possible.

Firewalls: A firewall is a software program or hardware device that filters the inbound and outbound traffic between your network or computer and the Internet. A firewall is a very valuable tool to protect your data and your computers. Firewalls can block intruders and unwanted traffic from getting into your computer. Make sure your firewall is enabled.



Anti-virus and anti-spyware programs: Anti-virus programs can stop viruses, worms, and other malware. Anti-spyware programs can stop malware that perform certain behaviors such as pop-up advertising, collecting personal information, or changing the configuration of your computer. It is important to keep these up-to-date by keeping the license active and the program set to auto-update.

Wireless networks: Wireless networks are not as secure as the traditional “wired” networks, but you can minimize the risk on your wireless network by enabling encryption, changing the default password, changing the Service Set Identifier (SSID) name (which is the name of your network) as well as turning off SSID broadcasting and using the MAC filtering feature, which allows you to designate and restrict which computers can connect to your wireless network.²³

As cybersecurity is our shared responsibility it is important that everyone keeps informed of the latest threats, and the best ways to stay safe online.

23 Multi-State Information Sharing and Analysis Center. “Cybersecurity and You – Top Ten Tips.” MS-ISAC Cybersecurity Tips Newsletter. Vol. 26, Issue 1, October 2011. Accessed at <http://msisac.cisecurity.org/newsletters/2011-10.cfm>

[storage/data loss prevention]

Counties are struggling to keep up with dramatic increases in the volume of data within their own networks and across government agencies at all levels – and the problem is only going to get worse. In just the next two years government agencies are expected to add a petabyte of new data – roughly the amount contained in 20 million four-drawer filing cabinets filled with text.²⁴

Making the leap to the cloud can be especially challenging for government agencies, which often require higher levels of security.

Complicating the storage of this data are conflicting principles of openness and privacy. Much of the data maintained by counties is public and so must be accessible to citizens. But increasing amounts of data, including personally identifiable information like Social Security numbers and payment card records, are protected by privacy laws and regulations, requiring

counties to perform a difficult balancing act as they make sure the information is both available and secure.

Data loss prevention software protects information while it's in transit by encrypting it, and prevents employees from sending sensitive data outside the county network.

Identify the data within your county that requires protection, and determine which employees need to access the data. Just because an employee has a high rank or has a need to access some sensitive data doesn't mean he or she should be able to see all restricted data.

[cloud and storage security]

Cloud storage has become a popular option for organizations looking to contain costs and increase network scalability and availability. Cloud solutions provide on-demand network access to a shared pool of computing resources such as networks, servers, storage and applications. There are a number of advantages, but also some challenges, since network traffic can bypass the usual inspection points. Additionally, as the number of applications available in the cloud grows, policy controls for web applications and cloud services will also need to evolve.²⁵

Making the leap to the cloud can be especially challenging for government agencies, which often require higher levels of security. Here are some areas that the Center for Internet Security suggests investigating before you make any decisions:

24 MeriTalk. "Government Agencies Adding a Petabyte of New Data in the Next Two Years." May 7, 2012.

Accessed at www.meritalk.com/pdfs/big-data/MeriTalk_Big_Data_Gap_Press_Release.pdf

25 Multi-State Information Sharing and Analysis Center "Cloud Computing." Cybersecurity Tips Newsletter. April 2010.

Accessed at <http://msisac.cisecurity.org/newsletters/2010-04.cfm>

Vendor Security: Cloud computing customers rely on providers to implement appropriate security measures to protect the confidentiality, integrity, and availability of data. Be wary of providers who are reluctant to share details of their security architecture/practices with customers.

Isolation/Segregation: Users access cloud computing resources via a virtual machine hosted on an unknown physical machine. The physical machine may be shared with other users. Providers must ensure that multiple customers do not interfere with each other, maliciously or unintentionally.

Data Location: Providers may have data centers located in other countries. Be sure your vendor contract stipulates any restrictions you may have on the physical location of where your data is stored.

Management Interface: Customers access the cloud management interface via the Internet, thus increasing exposure to potential attack.

Reputation Sharing: Bad behavior by one cloud customer may impact others using the cloud. For example, a customer engaging in spamming may cause a common cloud IP address to be blacklisted.

Provider Viability: What happens to your organization's applications and data in the event that the provider goes out of business?



Compliance: Placement of data in the cloud does not eliminate an organization's need to meet legal and regulatory requirements such as payment card industry standards and HIPAA. Organizations will need timely assistance from cloud computing providers to fulfill investigation/audit requirements.²⁶

Finally, industry analysts recommend that government organizations choose a cloud computing vendor capable of providing these important capabilities and features:

- 🔒 Service Level Agreements (SLAs) that ensure high availability, disaster recovery and incident handling;
- 🔒 data handling guidelines;
- 🔒 security best practices such as separate cages, adherence to ISO 27001 and SSAE 16 information management standards;
- 🔒 regular third-party assessments;
- 🔒 migration capability and integration experience;
- 🔒 compliance with government security standards, including Federal Information Security Management Act (FISMA);
- 🔒 fully owned and operated integrated solution covering network, data center and cloud platform; and
- 🔒 the capability to accurately track and bill consumption.²⁷

[mobility]

Although mobile devices have become commonplace in organizations, a recent SANS mobile device survey²⁸ found that organizations are not prepared to safely accommodate the devices. Fully 61 percent of the 650 survey respondents allow personal devices to connect to protected network resources, yet only 9 percent said they understood what those devices were and what they were accessing. Half said they either did not have policies or depended on the user to comply with corporate security policies.

Companies that don't have BYOD policies rely on Virtual Private Networks, authentication and network firewalls. "Without security policies, allowing employee-owned devices to access company resources makes our protected IT networks sitting ducks," the SANS

26 Multi-State Information Sharing and Analysis Center "Cloud Computing." Cybersecurity Tips Newsletter. April 2010.

Accessed at <http://msisac.cisecurity.org/newsletters/2010-04.cfm>

27 Chandrasekaran, Arun & Mayank Kapoor. "State of Cloud Computing in the Public Sector." Frost & Sullivan, 2011.

Accessed at www.frost.com/prod/servlet/cfp/232651119

28 Johnson, Kevin & Tony LaGrange. "SANS Survey on Mobility/BYOD Security Policies and Practices." Sans Institute. October 2012.

Accessed at www.sans.org/reading_room/analysts_program/SANS-survey-mobility.pdf

Institute survey found. The survey stressed the importance of creating and enforcing mobility security policies before mobile users are permitted to access your networks.²⁹

The *IT Manager Daily* technology news website recommends three things for organizations planning to let employees use smartphones and other personal devices in the office:

- 🔒 a software application for managing the devices
- 🔒 a written policy outlining the responsibilities of both the employer and the users, and
- 🔒 an agreement users must sign, acknowledging that they have read and understand the policy.³⁰

IT Manager Daily offers a free BYOD policy template at www.itmanagerdaily.com/byod-policy-template/.

In addition, the White House Digital Government website provides a free toolkit to help government agencies implement BYOD programs at www.whitehouse.gov/digitalgov/bring-your-own-device.



29 Johnson, Kevin & Tony LaGrange. "SANS Survey on Mobility/BYOD Security Policies and Practices." Sans Institute. October 2012. Accessed at www.sans.org/reading_room/analysts_program/SANS-survey-mobility.pdf

30 Berry, Megan. "Bring Your Own Device Policy Template." IT Manager Daily. Accessed at www.itmanagerdaily.com/byod-policy-template/

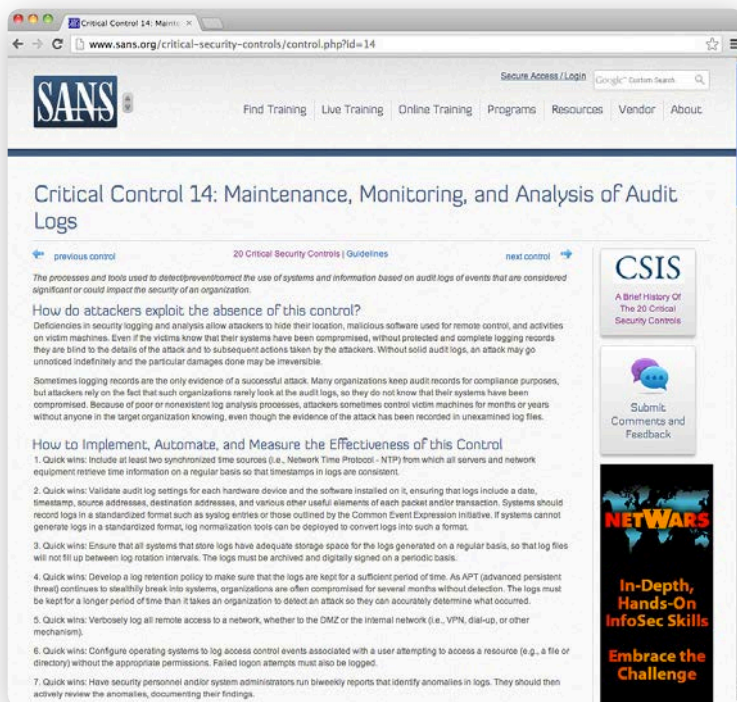
[measurement and reporting logs]

Audit logs maintain a record of system activity both by system and application processes and by user activity of systems and applications.³¹ They're very useful in detecting security violations, performance problems, and flaws in applications. Sometimes an organization doesn't even know it's been breached until someone analyzes the log. Make it a priority to collect your logs.

According to the *SANS guideline for Critical Control #14: Maintenance, Monitoring and Analysis of Audit Logs*, deficiencies in security logging and analysis allow attackers to hide their location, malicious software used for remote control, and activities on victims' machines. Even if the victims know that their systems have been compromised, without protected and complete logging records they are blind to the details of the attack and to subsequent actions taken by the attackers. Without solid audit logs, an attack may go unnoticed indefinitely and the particular damages done may be irreversible.

Sometimes logging records are the only evidence of a successful attack. Many organizations keep audit records for compliance purposes, but attackers rely on the fact that such organizations rarely look at the audit logs, so they won't know that their systems

have been compromised. Because of poor or nonexistent log analysis processes, attackers sometimes control victims' machines for months or years without anyone in the target organization knowing, even though the evidence of the attack has been recorded in unexamined log files.³²



31 Audit Trails. NIST Special Publication 800-12, Introduction to Computer Security: The NIST Handbook. Accessed at: <http://csrc.nist.gov/publications/nistpubs/800-12/800-12.html/chapter18.html>

32 Sans Institute. Critical Control 14: Maintenance, Monitoring, and Analysis of Audit Logs. SANS Institute. Accessed at www.sans.org/critical-security-controls/control.php?id=14

[application security]

_intrusion detection prevention

Intrusion detection and prevention systems (IDPS) have become a necessary component of network architecture. The concept is simple but important – intrusion detection monitors networks for any sign of attack or violation of the organization's security or acceptable use policies. Intrusion prevention goes a step further, attempting to stop incidents. Organizations also use IDPSs to identify problems with security policies, document existing threats, and deter individuals from violating security policies.³³

There are four primary types of IDPS technologies—network-based, wireless, Network Based Analysis, and host-based. Each offers different advantages. Experts recommend using multiple types of IDPS technologies to achieve more comprehensive and accurate detection and prevention of malicious activity.³⁴ Correlating with multiple logs such as firewall, proxy server, web server, and system logs creates the capacity for a more comprehensive and accurate detection and prevention of malicious activity.



Cyber-attacks can be costly if not resolved quickly. The average time to resolve a cyber-attack is 24 days, but it can take up to 50 days, according to the U.S. Cost of Cybercrime study. The average cost incurred during this 24-day period was \$591,780, representing a 42 percent increase over last year's estimated average cost of \$415,748 during an 18-day average resolution period.³⁵

The potential for downtime and associated monetary losses makes the cost of IDPS seem reasonable. According to a paper by the SANS Institute, companies that weigh the potential damages from attacks are more inclined to introduce protective measures like IDPS technologies. The paper recommends using a combination of IPS and IDS technologies to raise the level of visibility and control for networks.³⁶

33 Scarfone, Karen & Peter Mell. "Guide to Intrusion Detection and Prevention Systems." NIST Special Publication 800-94. February, 29967. Accessed at <http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf>

34 Scarfone, Karen & Peter Mell. "Guide to Intrusion Detection and Prevention Systems." NIST Special Publication 800-94. February, 29967. Accessed at <http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf>

35 Ponemon Institute. "2012 U.S. Cost of Cyber Crime Study." October, 2012. Accessed at www.sans.org/reading_room/whitepapers/detection/understanding-ips-ids-ips-ids-defense-in-depth_1381

36 Lyne, James. "Eight Trends that are Changing Network Security." Sophos. Undated. Accessed at www.sophos.com/en-us/security-news-trends/security-trends/network-security-top-trends.aspx

_application firewalls

Application firewalls protect against attacks by identifying unexpected sequences of commands that often originate from buffer overflow attacks, denial of service attacks, malware, and other forms of attack carried out within application protocols such as HTTP.³⁷



These firewalls monitor traffic before it reaches the web application, so they can analyze requests before passing them on. This gives them an advantage over intrusion prevention systems, which interrogate all network traffic and therefore can't analyze the application layer as thoroughly.

Another advantage is their ability to detect and prevent new types of attacks. By watching for unusual or unexpected patterns, in the traffic firewalls, they can alert and defend against unknown attacks. If an application firewall detects that the application is returning much more than data expected, it can block it and alert someone. These firewalls augment intrusion detection and prevention systems, providing an additional layer of protection.³⁸

_penetration testing

Penetration testing is security testing in which assessors mimic real-world attacks to identify methods for circumventing the security features of an application, system, or network. It often involves launching real attacks on real systems and data that use tools and techniques commonly used by attackers. Most penetration tests involve looking for combinations of vulnerabilities on one or more systems that can be used to gain more access than could be achieved through a single vulnerability. Penetration testing can also be useful for determining:

- 🔒 how well the system tolerates real world-style attack patterns
- 🔒 the likely level of sophistication an attacker needs to successfully compromise the system
- 🔒 additional countermeasures that could mitigate threats against the system
- 🔒 defenders' ability to detect attacks and respond appropriately.

37 Scarfone, Karen and Paul Hoffman. "Guidelines on Firewalls and Firewall Policy." NIST. September, 2009.

Accessed at <http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf>

38 McMillan, Jim. "Intrusion Detection FAQ: What is the difference between an IPS and a Web Application Firewall?" SANS Institute. November 2009.

Accessed at www.sans.org/security-resources/idaq/ips-web-app-firewall.php

Penetration testing can be invaluable, but it is labor-intensive and requires great expertise to minimize the risk to targeted systems. Systems may be damaged or otherwise rendered inoperable during the course of penetration testing, even though the organization benefits in knowing how a system could be rendered inoperable by an intruder. Although experienced penetration testers can mitigate this risk, it can never be fully eliminated.³⁹

The biggest mistake most organizations make when it comes to cybersecurity is failing to factor in the cost of securing the network when they're building it.

vulnerability and threat management

Unless an event has occurred or risk is clearly understood, some organizations are unlikely to build adequate security into their networks.

A recent report by the National Association of State Chief Information Officers (NASCIO) found that 50 percent of states reported spending less than 3 percent of their IT budget on security. The private sector spends 5 percent or more. And state spending on cybersecurity is actually trending downward, according to NASCIO. Local governments are likely to show similar spending trends.⁴⁰

The biggest mistake many organizations make when it comes to cybersecurity is failing to factor in the cost of security at the beginning of a project, such as network rollout. Security is an essential component of networks, as integral as the hardware, access points and operating systems.

For this reason, it's vital to educate everyone – county officials, your staff, and taxpayers – about what's at stake. Taxpayers and county officials have to understand what kind of data the county is storing, and the consequences if intruders were able to steal or compromise it. Your employees need to understand how their actions can put county assets in jeopardy or help keep the network secure.

39 Scarfone, Karen, et al. Technical Guide to Information Security Testing and Assessment. NIST Guide 800-115. September 2008.

Accessed at <http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf>

40 Newcombe, Todd. "Cybercrime Hits Small Towns." Governing. December 2011.

Accessed at www.governing.com/topics/technology/cybercrime-hits-small-towns.html

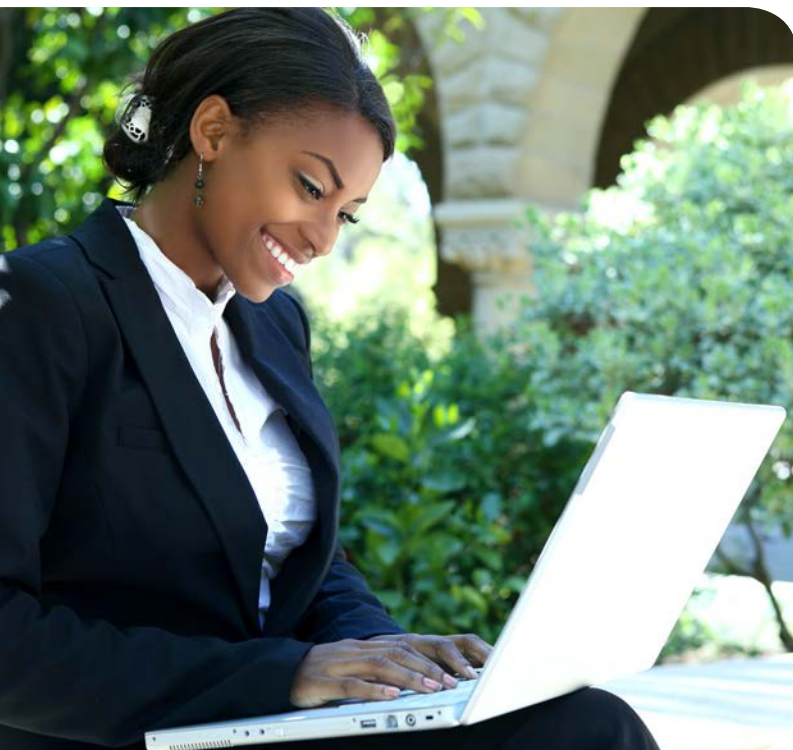
_endpoint security

Every time staff access your network remotely, they create a potential entry point for intruders. Endpoint security, which provides an increasingly important protection, usually involves software installed on the server and on the individual devices staff use to access your network. Many organizations, however, fail to monitor employee devices to be sure all the latest

Even protected devices have been known to permit malicious downloads, which can cause major problems before they're discovered – and intruders have broadened their attacks to include smartphones and other wireless devices.

malware defense applications have been downloaded, leaving the organization vulnerable to new malware. Additionally, even protected devices have been known to permit malicious downloads, which can cause major problems before they're discovered. And intruders today have broadened their attacks to include smartphones and other wireless devices.

Endpoint solutions that capture and analyze data in real time are becoming a necessity, especially as criminals get smarter about attacking networks. These tools can give you a picture of all processes running on endpoints at any given time, identify processes often used in malware, and alert you to specific processes that deviate from the usual.



Real-time endpoint forensic data capture and analysis replaces traditional forensic processes that were usually put in place following a data breach.⁴¹ Heading off an attack before it can cause trouble will save the county time and money, and provide better security for your data and network infrastructure.




41 Oltsik, John. "Endpoint Forensics Will Become a Mainstream Cybersecurity Technology." Network World. May 22, 2013. Accessed at www.networkworld.com/community/blog/endpoint-forensics-will-become-mainstream-cybersecurity-technology

_patch management

The National Institute of Standards and Technology (NIST) defines patch management as the process for identifying, acquiring, installing, and verifying patches for products and systems. Applying patches to eliminate software vulnerabilities significantly reduces the opportunities for exploitation. Patch management is required by various security compliance mandates such as the Payment Card Industry (PCI) Data Security Standard (DSS), which requires that the latest patches be installed and sets a maximum timeframe for installing the most critical patches.⁴²

Patches serve other purposes than just fixing software flaws; they can also add new features to software and firmware, including security capabilities. According to the NIST *Guide to Enterprise Patch Management Technologies*, many major attacks in the past few years have targeted known vulnerabilities for which patches existed before the breaches. Timely patching of security issues is generally recognized as critical to maintaining the operational availability, confidentiality, and integrity of information technology (IT) systems.⁴³

All organizations should have a systematic, accountable, and documented process for managing exposure to vulnerabilities through the timely deployment of patches. NIST recommends implementation of the following recommendations to assist in patch and vulnerability management:

-  deploy enterprise patch management tools using a phased approach,
-  reduce the risks associated with enterprise patch management tools by applying standard security techniques that should be used when deploying any enterprise-wide application, and
-  balance security needs with their usability and availability needs.⁴⁴

NIST published its *Guide to Enterprise Patch Management Technologies* for security managers, engineers, administrators and others responsible for working with security patches as well as auditors who need to assess system security. It explains the importance of patch management and examines the challenges inherent in performing patch management. The guide provides an overview of enterprise patch management technologies and briefly discusses metrics for measuring the technologies' effectiveness and for comparing the relative importance of patches. You can download the Guide to Enterprise Patch Management Technologies, NIST Special Publication 800-40 Revision 3, at <http://csrc.nist.gov/publications/drafts/800-40/draft-sp800-40rev3.pdf>.

42 Souppaya, Murugiah and Karen Scarfone. "Guide to Enterprise Patch Management Technologies." NIST Special Publication 800-40 Revision 3. September 2012. Accessed at <http://csrc.nist.gov/publications/drafts/800-40/draft-sp800-40rev3.pdf>

43 Souppaya, Murugiah and Karen Scarfone. "Guide to Enterprise Patch Management Technologies." NIST Special Publication 800-40 Revision 3. September 2012. Accessed at <http://csrc.nist.gov/publications/drafts/800-40/draft-sp800-40rev3.pdf>

44 Souppaya, Murugiah and Karen Scarfone. "Guide to Enterprise Patch Management Technologies." NIST Special Publication 800-40 Revision 3. September 2012. Accessed at <http://csrc.nist.gov/publications/drafts/800-40/draft-sp800-40rev3.pdf>

[incident response plan and program]

The National Institute of Standards and Technology Incident Response Plan⁴⁵ lists 11 major steps that should be performed when a technical professional believes that a serious incident has occurred and the organization does not have an incident response capability available.

1. Document everything. This effort includes every action that is performed, every piece of evidence, and every conversation with users, system owners, and others regarding the incident.
2. Find a coworker who can provide assistance. Handling the incident will be much easier if two or more people work together. For example, one person can perform actions while the other documents them.
3. Analyze the evidence to confirm that an incident has occurred. Perform additional research as necessary (e.g., Internet search engines, software documentation) to better understand the evidence. Reach out to other technical professionals within the organization for additional help.
4. Notify the appropriate people within the organization. This should include the chief information officer (CIO), the head of information security, and the local security manager. Use discretion when discussing details of an incident with others; tell only the people who need to know and use communication mechanisms that are reasonably secure. (If the attacker has compromised email services, do not send emails about the incident.)
5. Notify US-CERT and/or other external organizations for assistance in dealing with the incident.
6. Stop the incident if it is still in progress. The most common way to do this is to disconnect affected systems from the network. In some cases, firewall and router configurations may need to be modified to stop network traffic that is part of an incident, such as a denial of service (DoS) attack.
7. Preserve evidence from the incident. Make backups (preferably disk image backups, not file system backups) of affected systems. Make copies of log files that contain evidence related to the incident.
8. Wipe out all effects of the incident. This effort includes malware infections, inappropriate materials (e.g., pirated software), Trojan horse files, and any other changes made to systems by incidents. If a system has been fully compromised, rebuild it from scratch or restore it from a known good backup.

⁴⁵ Cichonski, Paul, Tom Millar, Tim Grance, and Karen Scarfone. "Computer Security Incident Handling Guide." NIST Special Publication 800-61 Revision 2. August 2012. Accessed at <http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf>



9. Identify and mitigate all vulnerabilities that were exploited. The incident may have occurred by taking advantage of vulnerabilities in operating systems or applications. It is critical to identify such vulnerabilities and eliminate or otherwise mitigate them so that the incident does not recur.
10. Confirm that operations have been restored to normal. Make sure that data, applications, and other services affected by the incident have been returned to normal operations.
11. Create a final report. This report should detail the incident handling process. It also should provide an executive summary of what happened and how a formal incident response capability would have helped to handle the situation, mitigate the risk, and limit the damage more quickly.⁴⁶

⁴⁶ Cichonski, Paul, Tom Millar, Tim Grance, and Karen Scarfone. "Computer Security Incident Handling Guide." NIST Special Publication 800-61 Revision 2. August 2012. Accessed at <http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf>



operational best practices/checklist

did you know?

- ☐ Email is one of the easiest ways to dupe your employees into giving their user ID and password up to a stranger.
- ☐ Your endpoint anti-virus solution can catch a significant number of emails that have malicious software that could infect your network.
- ☐ Patching your desktops is an integral part of a strategy to prevent malicious software sent via email from affecting your network.
- ☐ Many malicious Internet attacks come in the form of email from companies that you normally do business with, from people you may indirectly know or using the promise of prizes or money to tempt you to open a malicious piece of software or Internet link.
- ☐ It's not a matter of if, but when, you will have to respond to an incident.
- ☐ Without cooperation and preplanning across IT, business and executive management your incident response plan will fall short.
- ☐ You can require the companies that respond to network equipment requests for proposal/quote/information (RFP/Q/I) provide you with a review of your existing environment and a configuration for the new device to work securely in your environment.
- ☐ Employees will have diverse types of devices that will still require central management tools.

It may seem as if creating a security program within your organization is complex. Actually, it's a development process with simple foundational elements you can use as reference points, which may make you feel much more comfortable moving forward. You have probably made some mistakes and will probably continue to make mistakes in the future. Your organization can benefit greatly if you can learn from these mistakes and incorporate what you learn into your security program.

- ❑ Understanding your business workflows will provide you with the best indicators on how to manage data across your IT systems.
- ❑ Gartner predicts that half of employers will require employees to supply their own device for work purposes by 2017. www.gartner.com/newsroom/id/2466615
- ❑ Many IT organizations fail to incorporate an upgrade of the logging capabilities when adding new systems or increasing the network connectivity between internal networks or their enterprise and the Internet.
- ❑ Many organizations avoid doing penetration testing for the fear that it will "break" some critical internal IT system.
- ❑ Only by understanding your IT infrastructure as a whole can you truly have an enterprise view of your vulnerabilities. Then and only then can you begin to compare the incoming threat data against those vulnerabilities to clearly discern your enterprise risk.
- ❑ The combination of antivirus, patching and encryption of each endpoint is great progress for an organization but it is not everything your security organization has to have in place to keep your organization secure.
- ❑ Websites that contain explicit material, allow gambling, or the download of illegal software, etc. are in a great many cases carrying or are linked to malware.
- ❑ Any link on any site has the potential to infect you with malicious software or bring you to a malicious website. You can place your cursor over the link without clicking to preview where the link will actually take you.
- ❑ Incident response plan development is not as onerous as some of your staff may think. You can start simple and as you practice those involved will naturally fill in the gaps as part of their incident remediation plan.

*This tool was developed by Sebron K. Partridge,
NACo member and Chief Information Security Officer of Riverside County, California.*

the road ahead

cyber_for_counties {guidebook} v1.0



Copyright protected and provided for personal use only - not for reproduction or retransmission.
For reprints please contact the Publisher.



the road ahead

By Chris Rodgers

Commissioner of Douglas County, Nebraska

Immediate Past President, National Association of Counties

“*For many years, America's counties have prepared for floods, hurricanes, tornadoes, wild fires, and other traditional disasters, but not until recently have we given adequate attention to the destruction that can happen in our “the cyber ecosystem.”*

Cybersecurity is one of the top issues of the next century and NACo is proud to be the first of the government trade organizations to elevate the subject to a level of adequate prominence. Whether it is information from drivers licenses, medical records or criminal investigations, counties are responsible for some of the most sensitive information an individual possesses and with that in mind, we are positioning our organization and membership for the long haul when it comes to cybersecurity importance in today's society.

I want to thank everyone who made this possible and ask for your continued support as we work to establish a public/private partnership that prepares our counties and our country to thrive and advance in this technology centered society.

— Chris Rodgers

During his term as NACo President, Commissioner Rodgers made cybersecurity a priority. This guidebook is one result of his vision to educate NACo members about the scope of the problem and provide them with resources, information, and programming to address the emerging threat.

We at NACo hope that you find this guidebook useful as you continue the important work of securing your county's networks. In addition to case studies and recommendations provided herein, we also encourage you to review the recommendations of the Deloitte-National Association of State Chief Information Officers (NASCIO) Cybersecurity Study. The study was conducted by NASCIO and the consulting firm of Deloitte LLP to assess the security of state digital data and cyber assets administered by states. It highlights the challenges that states and chief information officers and information security officers face in protecting states' critically important systems and data, which are many of the same challenges facing counties today. The survey calls for greater collaboration among government IT staff, business staff, executive staff and elected officials when it comes to protecting digital data and cyber assets.⁴⁷



⁴⁷ Deloitte-NASCIO Cybersecurity Study. Oct. 26, 2012.

Accessed at www.deloitte.com/view/en_US/us/Services/audit-enterprise-risk-services/Security-Privacy-Services/23eac2887a97a310VgnVCM2000003356f70aRCRD.htm



the 2012 Deloitte-NASCIO cybersecurity study recommendations

- Assess and communicate security risks: Adopt a uniform security framework such as the Federal NIST standard, perform regular compliance assessments against the framework across agencies, and communicate risks to relevant business stakeholders.
- Better articulate risks and audit findings with business stakeholders: Routine reporting of cybersecurity threats, projects, and status is essential to building support for security and privacy initiatives.
- Explore creative paths to improve cybersecurity effectiveness within states' current federated governance models: Create cybersecurity competency centers or pursue a shared services model to maximize the use of scarce qualified personnel resources, technology, and dollars to avoid duplication of effort across agencies and departments.
- Focus on audit and continuous monitoring of third-party compliance: With greater use of outsourcing, more needs to be done to manage the growing shared risk. States must communicate cybersecurity policies and practices to partners, including local governments, and regularly use specific metrics to assess how well these protective measures are being followed.
- Raise stakeholder awareness to combat accidental data breaches: Better, more effective user education is a huge opportunity—because the number one cause of security breaches is user error. Balance the cost of education and the disruption to individuals against the benefit of keeping the state out of the headlines—and it's clear the investment is a sound one.
- Aggressively explore alternative funding sources including collaboration with other entities: Leave no stone unturned in the hunt for additional funding for security and privacy initiatives. Identify agency initiatives with federal funding and help make sure cybersecurity requirements are considered and addressed. Use what's learned to benefit state agencies and their partners.
- Make better security an enabler of the use of emerging technologies: Leverage the strong motivation of business leaders to embrace new technology to improve program effectiveness by building effective security measures and using them as an enabler. Identify and agree on a core security services taxonomy to serve as a common vocabulary for describing services that must be provided to meet the requirements of security standards frameworks defined by the federal government and various standards bodies.⁴⁸

48 www.deloitte.com/assets/Dcom-UnitedStates/Local%20Assets/Documents/AERS/us_aers_nascio%20Cybersecurity%20Study_10192012.pdf

appendix 1: acknowledgements

NACo is grateful to numerous individuals who contributed to the publication of this guidebook.

AT&T

Jodi Chapin
Lisa Young
James Knopka
Steve Hurst
Kim Bilderback
Chris Boyer

NACo Cyber for Counties Task Force

Mary Ann Borgeson
Chris Rodgers
Sebron K. Partridge
Ralph Johnson

NACo Professional Development, Education and Training Division

Karon Harden
Emily Star
Dan Gillison
Matt Chase

Center for Internet Security/MS-ISAC

Kristin Judge
Rich Comeau
Tom Duffy
Krista Montie
Laura Iwan
Adnan Baykal

Department of Homeland Security

Kelvin Coleman
Erin Meehan
Janet Quist
Taylor Price

appendix 2: additional resources for counties

The U.S. Department of Homeland Security (DHS) Office of Cybersecurity and Communications (CS&C) partners with the public and private sectors to improve the cybersecurity of the nation's critical infrastructures by facilitating risk management activities that reduce cyber vulnerabilities and minimize cyber-attacks. Within CS&C, the State, Local, Tribal, and Territorial (SLTT) Cybersecurity Engagement Program fosters the relationships that protect the country's critical infrastructures.

{partnership opportunities}

- 📡 The [Critical Infrastructure Partnership Advisory Council \(CIPAC\)](#) is a partnership between government and critical infrastructure owners and operators, which provides a forum to engage in a broad spectrum of critical infrastructure protection activities like the [Cross-Sector Cybersecurity Working Group](#). To learn more, [email cipac@dhs.gov](mailto:cipac@dhs.gov).
- 📡 The [Information Technology-Government Coordinating Council \(IT-GCC\)](#) brings together diverse federal, state, local, and tribal interests to identify and develop collaborative strategies that advance IT critical infrastructure protection. The IT-GCC serves as a counterpart to the IT Sector Coordinating Council (IT-SCC).
- 📡 The [Multi-State Information Sharing and Analysis Center \(MS-ISAC\)](#), a division of the not-for-profit Center for Internet Security, is a collaborative effort based on a strong partnership with DHS and the SLTT Cybersecurity Engagement program. The MS-ISAC has been designated by DHS as the key resource for cyber threat prevention, protection, response and recovery for the Nation's SLTT governments. Through its state-of-the-art 24/7 Security Operations Center, the MS-ISAC serves as a central resource for situational awareness and incident response for SLTT governments, at no cost to its members. In partnership with DHS and the (SLTT) Cybersecurity Engagement Program, MS-ISAC provides cybersecurity support and services to SLTT governments. For more information, visit the MS-ISAC at www.msisac.org or contact them at info@msisac.org.

{cyber assessments evaluations and reviews}

- 📡 The [Cyber Resilience Review \(CRR\)](#) is provided by DHS to SLTT governments as a free service and involves a one-day, onsite interview that examines the overall practice, integration and health of an organization's cybersecurity program. The CRR is based on the [CERT Resilience Management Model \(CERT-RMM\)](#) (<http://cert.org/resilience/rmm.html>). For additional information or to request a CRR, email CSE@hq.dhs.gov.
- 📡 The [Cybersecurity Evaluation Tool \(CSET®\)](#) is a self-contained software tool which runs on a desktop or laptop computer. It evaluates the cybersecurity of an automated, industrial control or business system using a hybrid risk and standards-based approach, and provides relevant recommendations for improvement. For all information regarding CSET Assessments please visit, <http://ics-cert.us-cert.gov/Assessments>. This site will give you an overview of the assessment tool, purpose, key benefits, and how to obtain CSET.
- 📡 The DHS [Cybersecurity Assessment and Risk Management Approach \(CARMA\)](#) is a flexible, repeatable, and reusable cyber risk management approach to help state and local governments, CIKR sectors, and other public and private sector organizations manage cyber critical infrastructure risk. CARMA helps public and private sector partners assess, prioritize and manage cyber infrastructure risk by providing a picture of sector-wide risks for different categories of cyber critical infrastructure. For more information, email CS&C_IER@hq.dhs.gov.

{software assurance assistance}

- 📡 The [Software Assurance Forum](#) brings together members of government, industry and academia with vested interests in software assurance, semi-annually, to discuss and promote integrity, security and reliability in software. For more information, visit: <https://buildsecurityin.us-cert.gov/swa/forums-and-working-groups>.
- 📡 "Building Security In" (BSI) is a collaborative effort to provide tools, guidelines and other resources, which software developers, architects and security practitioners can use to build security into software in every phase of development. For information, visit: <https://buildsecurityin.us-cert.gov/swa> or email software.assurance@dhs.gov.
- 📡 [Cyber Exercises](#) – directly supports state, local, tribal, and territorial cyber exercise, design, development, and execution. Cyber exercises familiarize SLTT cyber stakeholders with the roles, responsibilities, policies, plans, and procedures related to cyber incidents. DHS provides direct cyber exercise support to SLTT organizations upon request. For more information, contact CEP@dhs.gov.

{cyber incident and emergency response}

- 📡 The [National Cybersecurity Communications Integration Center \(NCCIC\)](#), is a 24x7 cyber monitoring, analysis, incident response, and management center that is the national nexus of cyber and communications incident integration for the federal domain, intelligence networks, law enforcement, the private sector, State, local, tribal, and territorial governments, and international partners. The NCCIC organizationally encompasses the US-CERT and ICS-CERT cyber emergency response capabilities, detailed below. For more information, visit: www.dhs.gov/about-national-cybersecurity-communications-integration-center.
- 📡 The [United States Computer Emergency Readiness Team \(US-CERT\)](#) brings advanced network and digital media analysis expertise to bear on malicious activity targeting our nation's networks. US-CERT develops timely and actionable information for distribution to federal departments and agencies, state and local governments, private sector organizations, and international partners. In addition, US-CERT operates the National Cybersecurity Protection System (NCPS), which provides intrusion detection and prevention capabilities to covered federal departments and agencies. The US-CERT's **National Cyber Alert System (NCAS)** delivers timely and actionable information and threat products including alerts, bulletins and tips for users of all technical levels. Visit www.us-cert.gov/cas/signup.html to subscribe or visit, www.us-cert.gov for more information.
- 📡 [Industrial Control Systems Cyber Emergency Response Team \(ICS-CERT\)](#) reduces risk to the Nation's critical infrastructure by strengthening control systems security through public-private partnerships. ICS-CERT has four focus areas: situational awareness for CIKR stakeholders; control systems incident response and technical analysis; control systems vulnerability coordination; and strengthening cybersecurity partnerships with government departments and agencies. To report suspicious cyber activity affecting ICS, visit, <http://ics-cert.us-cert.gov>, call the ICS-CERT Watch Floor at 877.776.7585 or [email ics-cert@dhs.gov](mailto:ics-cert@dhs.gov).
- 📡 [MS-ISAC Reporting](#) If you would like to leverage the MS-ISAC for malware analysis, computer forensics, network forensics, incident response or onsite response, please contact our 7x24 Security Operation Center by calling 1-866-787-4722 or emailing soc@msisac.org.

{outreach and awareness}

- 📡 [National Cyber Security Awareness Month \(NCSAM\)](#), held during the month of October each year, proactively advances preparedness through increased awareness and information sharing. Since inception in 2004, NCSAM has been formally recognized by Congress, federal, state and local governments, as well as leaders from industry and academia. The SLTT Cybersecurity Engagement Program collaborates with state and local governments to sponsor events and activities throughout the country and disseminate Awareness Month messages. For more information, contact SLTTCyber@hq.dhs.gov.
- 📡 The [Stop.Think.Connect. Cyber Awareness Coalition](#) provides SLTT governments with the opportunity to demonstrate leadership on cybersecurity by working directly with DHS and the Stop.Think.Connect. Campaign to promote awareness about cyber threats and online safety practices both within their organizations and to the general public. For more information, email stopthinkconnect@dhs.gov or visit www.dhs.gov/stopthinkconnect.

{additional resources}

- 📡 [Securing our eCity Foundation](#): The Securing Our eCity Organization provides awareness of potential cyber security risks and offers free information, resources and education on protecting your family, business, the aging population and youths in a rapidly changing technology-driven environment. For information, visit: <http://securingoureconomy.org>.
- 📡 The [AT&T Cyber Security Essentials for State and Local Governments](#) provides a guide that shares best practices for policy and governance, operations and worst-case scenarios. For information, visit: www.corp.att.com/stateandlocal/docs/cyber_security_essentials.pdf.
- 📡 The [Top 10 Vulnerabilities Inside the Network](#) article from the Nov. 8, 2010 online publication, *Network World*, lists the top 10 ways a computer network can be attacked from inside and what an IT staff can do to guard against cyber intrusions. For information, visit: www.networkworld.com/news/tech/2010/110810-network-vulnerabilities.html.



NACo | PDET

PROFESSIONAL DEVELOPMENT,
EDUCATION AND TRAINING



@NACoDC



@NACoTweets



@NACoVideo



@in/NACoDC