CountyNews
Hot Topics
SPECIAL EDITION
January 14, 2013

INSIDE

Hackers, phishers and malware, oh my!
Why cybersecurity matters to you

Cybersecurity threats abound, and not just to your data

By Charles Taylor
SENIOR STAFF WRITER

Organized crime, a rogue nation-state and the person in the office next to you all have something in common: Each can pose a risk to your county's computer networks and cybersecurity.

Recent news headlines tell only part of the story. In Colorado, Washington and South Carolina, government data systems have been breached or attacked at the county, city and state levels, respectively.

• "Former Fort Collins Resident Indicted for Denial of Service Attack on Larimer County Government" — FBI

• "Burlington city bank account hacked, $400k stolen" — *KOMOnews.com*

• "3.6 million Social Security numbers hacked in South Carolina — Tax returns, personal data compromised in 'massive' breach" — *The State*

In this Hot Topics special report, *County News* takes a look at cybersecurity from the inside out: the threats counties are facing, what they're doing to protect themselves and what role each individual can play in securing cyber assets.

How Big Is the Problem?

Though figures vary — and many cybercrime-cost studies have been sponsored by software and computer companies — the impact is considerable. The 2012 Cost of Cyber Crime Study, conducted by the Ponemon Institute and sponsored by HP, found that cybercrime cost U.S. businesses $8.9 million on average. It also reported a 42 percent increase in cyberattacks, with organizations experiencing an average of 102 successful attacks per week.

Roberta G. Stempfley is the U.S. Department of Homeland Security's (DHS) deputy assistant secretary of cybersecurity. "The cybersecurity threats that local governments see are in part because we're all a part of this interconnected network," she said. "And so we're all vulnerable in some ways to the threat environment that comes with that interconnectivity."

President Barack Obama has called cybersecurity "a matter of public safety and national security."

It's Everyone's Job

Just whose responsibility is cybersecurity? The federal government, states, localities? Individuals?

All of the above.

By and large, county commissioners aren't cybersecurity experts. So, counties hire top-notch information security people and IT professionals — if they can afford them — to operate, protect and maintain their computer infrastructure. That should be enough, right?

"I think we depend on them, but then it becomes the issue of how educated are we that we even know what to we're supposed ask or look for?" said Mary Ann Borgeson, a Douglas County, Neb. commissioner, who chairs NACo's Cybersecurity Task Force. "We may not have all the intricate details as the technology people would, but we're the ones who are forming policies."

Ed Sherman is in charge of cybersecurity for Kitsap County, Wash., where the IT department reports to the County Board. "More and more,

See **SECURITY** *page 7*

Cybersecurity FAQs

Q: What can personal or business computer users do to remain safe online?

The most important thing is that you be aware of dangers that exist on the Internet and how to recognize them. Factors to keep in mind include:

• Be aware of performance changes like slow file loading in the computer and run an antivirus scan such as Norton scan

• If on your county's network, report all suspicious events like a "phishing" email to a system administrator

• When possible, perform personal and financial transactions on only trusted computers and networks. Avoid using public wireless networks and never use public computers.

Computers today have a many components that should be activated to improve security. Some of these features include:

• Reputable antivirus, anti-spyware and anti-spam software with automatic updates

Well-configured system updates that run automatically to perform timely security patches.

Q: If our computer system is severely compromised, how can we make sure that business continues without loss of data or functionality?

Disaster recovery and business continuity are very important in any organization. Though somewhat different in their technical meaning, these terms ultimately refer to an organization's ability to keep running and to recover from a destructive incident. This can include a natural disaster like an earthquake or flood, or human activity like hacking or sabotage.

The key to recovering from an incident like this is pre-planning. Some of the information technology considerations in planning for disasters include:

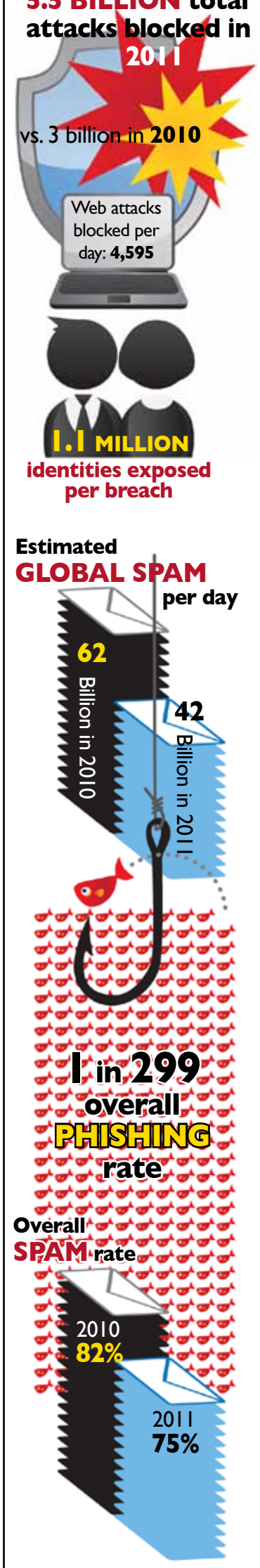
• Making sure your IT staff has drafted a backup plan to both continue operating and also to recover systems to their original state. It should include where data is backed up, how soon it can be made available, who is charged with executing the plan and what other staff are assigned as back-ups

• Deciding where employees should report to work in the event of a natural or man-made disaster and which technology may be available

• Testing the plan for effectiveness on regular intervals

See **CYBER FAQs** *page 3*

Cyber Threat Numbers



Data from Symantec 2011 Internet Security Threat Report • www.symantec.com

Policies Counties Should Have to Protect Information Assets

By Ralph Johnson
KING COUNTY, WASH.

When thinking about policies to protect county information, it's important to understand their purpose. Policies are essentially the "rules" of an organization. They set a baseline of expectations of behavior for the workforce. Through policies, employees and others gain an understanding of what is expected of them; in this case, how to protect the information that is in their county's possession.

The goal of information security in developing policies is to provide guidance and direction to protect the information from unauthorized access, modification or destruction.

Your county probably already has a number of policies related to information security in place. Before developing further policies it is critical to consider the laws and regulations that govern your specific jurisdiction, such as HIPAA (Health Insurance Portability and Accountability Act), COPPA (Children's Online Privacy Protection Act) or CJIS (Criminal Justice Information Services) policy.

By doing this, guidance can be developed to determine what information to protect and in some cases, how it must be protected. This method also places focus on the information, not the technology.

If policy development is focused on the technology rather than the information, the selection and implementation of specific technologies may not provide adequate protections for that information.

In addition to laws and regulations it is important to know any contractual obligations that already exist between the county, its vendors and other service providers that contain security requirements. Often these contracts have obligations to maintain certain levels of security, generally on the part of the service provider but frequently the county also retains some obligations.

One note about public disclosure; I am often asked, "If all of our information is public why do we need to protect it?" The answer is simple; first not all of the information in the possession of any governmental organization is publicly available: examples include employee Social Security numbers, personnel records, criminal histories and health records.

Second, we are responsible to maintain the integrity of the information that is publicly available. In other words even if information is readily available to the public, it is the responsibility of the organization to ensure that it is neither altered nor destroyed by unauthorized means.

Photo courtesy of King County, Wash.

Ralph Johnson, chief information security and privacy officer.

Determine Acceptable Risk Levels

The organization must determine what risks of exposure can be absorbed. For example, the organization should consider the risks associated with the use of unencrypted laptops containing information that might trigger a breach-notification requirement. This should be balanced against the costs of encrypting all or some of the organization's laptops in relation to the likelihood that laptops might be lost and the subsequent cost of notifying affected parties that their personal information may have been exposed.

Types of Policies Needed

Now, what policies should a county consider? There is no one-size-fits-all answer to this question. It depends upon the issues already discussed above, size and complexity of the organization and, in some cases, the technology already in place. There are, however, a number of policies that every organization should have. This applies whether the organization is a government, private enterprise, nonprofit or multinational corporation. All of these policies should be developed at a high level, and provide concepts and definitions that other, more specific technology-based policies can be based on.

Information Security Policy: This policy defines what information security is, sets a clear direction and demonstrates support for, and commitment to, information security. This policy can also include guidance related to what is considered an acceptable risk level relative to the loss or unauthorized access, modification or destruction of information. It is imperative that this policy be endorsed at the highest levels of county government with potential consideration given to enacting an ordinance codifying these concepts.

Information Privacy Policy: This policy defines privacy of information and what type of

See **POLICIES** *page 5*

Best Practices for Securing Your County's Cybersecurity

One of the parts of any cybersecurity program is to get buy-in from county employees on the security measures implemented. Below are some best-practices programs for engaging county employees in the importance of county security measures.

Maricopa County, Ariz.

The Maricopa County Internal Audit Department developed a unique and fun training program for county staff. The department created Web-based videos to increase organizational awareness of the importance of security issues. All scripting, casting, filming and editing of the videos were performed by the internal audit staff to save external production costs.

Overall, these videos provide an inexpensive and entertaining way to train employees on appropriate responses to workplace situations where fraud or abuse could occur and to avoid actions that prevent organizations from accomplishing their goals.

You can view the videos at *www.maricopa.gov/internal_audit/controls.aspx*

Fairfax County, Va.

Protecting the data of Fairfax County's more than one million residents, 11,000 employees, and thousands of vendors who sell goods and services to the county is an important task. To encourage good cybersecurity habits, Fairfax County's IT Department sponsors an annual Security Awareness Day for all employees.

The annual Security Awareness Day balances technical and non-technical sessions that offer the range of issues that are important for anyone using the organization's technology systems and electronic information.

Topics include business, employer and personal use of the Internet; new policies affecting use of IT resources; and special considerations for protecting children and e-commerce. With the growing number of employees who telecommute, the program also highlights the specific issues with accessing the government's system from home computers.

Johnson County, Kan.

The Johnson County Security Awareness Campaign is specifically designed to reach the county's nearly

See **BEST PRACTICES** *page 4*

The Federal Government, Congress and Combating Cyber Threats

By Dalen A. Harris
ASSOCIATE LEGISLATIVE DIRECTOR

For more than a decade and as the information age continues to evolve, various experts have expressed concerns about the vulnerability of information systems — often referred to as cybersecurity — in the United States and aboard. The frequency, impact, and sophistication of attacks on various information systems have grown and added urgency to how best to protect these critical parts of our nation's vital infrastructure.

The federal role in addressing this ongoing threat is complex and emerging, and Congress and the president have spent several years introducing a number of proposals and initiatives to better secure the nation's information systems. However, no major cybersecurity legislation has been enacted since 2002, but many proposals could undoubtedly impact county governments.

Thus far, legislative proposals have focused largely on issues in 10 broad areas, including:

- strengthening the national strategy and the role of federal government and agencies
- reform of the Federal Information Security Management Act (FISMA)
- enhanced protection of critical infrastructure; improved information sharing and cross-sector coordination
- combating breaches resulting in theft or exposure of personal data
- cyber crime
- protecting electronic commerce and privacy
- international efforts
- research and development, and
- readying the cyber workforce.

Although none of the current legislative proposals have been passed, the administration and Congress have proposed a number of reforms that local leaders should start to monitor closely.

Building on President George W. Bush's National Security Presidential Directive 16 (NSPD-16), President Obama's Comprehensive National Cybersecurity Legislative Initiative "seeks to ensure an organized and unified response to future cyber incidents; strengthen public/private partnerships to find technology solutions that ensure U.S. security and prosperity; invest in the cutting-edge research and development necessary for the innovation and discovery to meet the digital challenges of our time; and begin a campaign to promote cybersecurity awareness" in collaboration with key stakeholders including state and local governments, and the private sector.

Within this overarching framework, the president has proposed providing increased technical assistance and enhanced information sharing for states, local governments and the private sector to better combat cyber intrusions. Additionally, the president's comprehensive framework calls on Congress and industries to develop a plan to protect the nation's critical infrastructure such as the electricity grid, financial sector and other essential services.

Meanwhile some noteworthy legislative proposals that would have impacted counties included H.R. 1292. They sought to amend Title I of the Omnibus Crime Control and Safe Streets Act of 1968 to establish a program of law enforcement grants to state and local criminal justice agencies and relevant nonprofit agencies to combat "white-collar crime," including cyber crime. However, the legislation was never reported out to the House floor by the Committee on the Judiciary.

Additionally, throughout the 112th Congress, the Cybersecurity Act of 2012 received considerable attention. This comprehensive legislation proposed a number of changes consistent with President Obama's Comprehensive National Cybersecurity Legislative Initiative, but largely strengthened federal agencies' response to cyber threats. It would have also provided incentives for industry to adopt voluntary cybersecurity practices; authorized the government to provide security clearances to companies with a need to receive classified information to protect their networks; created a public-private partnership to combat cyber threats; strengthened the cybersecurity workforce; and coordinated cybersecurity research and development. The legislation was never enacted, however, and advocacy efforts to urge the president to issue an Executive Order consistent with many proposals in the bill stalled.

Cyber laws are on the books

The federal role is complex, and focuses on securing systems managed by the federal government and respective agencies; and determining what the appropriate federal role in protecting non-federal systems is. While there is no all-encompassing federal legislation in place yet, many statutes address various aspects of cybersecurity. Among them are:

- the Communications Assistance for Law Enforcement Act of 1994 (P.L. 103-414, 108 Stat. 4279)
- the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 (P.L. 98-473, 98 Stat. 2190)
- the Electronic Communications Privacy Act of 1986 (P.L. 99-508, 100 Stat. 1848)
- the Computer Security Act of 1987 (P.L. 100-235. 101 Stat. 1724)
- the Homeland Security Act of 2002 (P.L. 107-296, Titles II and III, Stat. 2135) and
- FISMA (P.L. 107-296, Title X) Stat. 2259 and P.L. 107-347, Title III, Stat 2946).

Also, more than 100 other laws or statutes have provisions relating to cybersecurity, and in the 111th and 112th Congresses, proposals to revise many of these current directives were debated, but ultimately were not enacted into public law.

What types of cyber threats do county employees face?

CYBER FAQs *from page 1*

Q: What security challenges are associated with the increasing numbers of private mobile devices accessing business networks?

Bring your own device (BYOD) is now a common part of today's business-computing environment. Users are allowed to connect to network resources with their personal smartphones, tablet computers and laptops that they bring into the office.

In most cases, network administrators have little control over these devices. As a result, malicious software (malware) or other dangers on these devices have a potential of infecting or otherwise compromising business or government networks. Compared to regular computers, these devices carry very little malware, but the numbers are growing rapidly.

Mobile antivirus and other security software are quickly coming onto the market to fill the need to protect these devices. IT departments are adopting many new technologies that allow for more control over these devices. Also, users are being forced to comply with new conditions, giving up more control of these devices to make sure they don't become harmful to networks.

Q: Does cloud computing pose a security risk to county information technology?

Cloud computing comes in many flavors and each brings a different level of risk. In public cloud computing, the client company's, or in this case, the county's in-house information technology staff retains a lot of control over the management and security of the cloud infrastructure. With public clouds, as well as with many semi-private configurations, servers are located in remote, third-party data centers.

In such situations, cloud-hosting vendors must be chosen very carefully to make sure they can meet the specific security needs of the client organization. This information must be documented very clearly, including the disposition of the data in the event that the vendor-hosting client relationship ends.

The client company is always the owner of the data and must bear the ultimate responsibility to make sure the data is properly secured to meet all fiduciary and regulatory requirements.

Q: The federal government is engaging counties to coordinate cybersecurity efforts. How does this help counties?

As the likelihood of cyber attacks increases at both national and local levels, the U.S. Department of Homeland Security (DHS) is using its deep knowledge of cybersecurity to work closely with counties. These are mutually beneficial engagements to secure the nation's infrastructure from attacks. Partnerships with county governments, first responders, utilities and local businesses help improve and strengthen the cybersecurity posture at all levels.

Counties get access to vast DHS cybersecurity resources, and DHS gets county partners to help spread the cybersecurity awareness message and local boots on the ground in case of a cyber attack.

On the Personal Level

Q: What are the dangers of social networking?

When posting information online, always consider whether the information can be harmful to you or your organization. Common information that users make public online is often the same information used for private financial transaction security. One must make sure that no confidential information is inadvertently disclosed. These often include:

- mother's maiden name
- last four digit's of social security number
- date of birth including year
- other security verification information that you provide to a financial institution

Additional dangers include disclosing your location and when you will be away from home. As with all computer-related accounts, passwords must be strong to prevent access to your data. Also, children are increasingly victimized by either their peers through cyber-bullying or are being targeted by pedophiles. Vulnerable children must be supervised online or kept off social networking.

Most cybersecurity insurance not ready for county market

By Charlie Ban
STAFF WRITER

Cybersecurity liability policies tend to encourage preventive measures

An ounce of prevention in fortifying county information systems is worth at least a pound of cybersecurity liability insurance, many county officials say.

Steve Acquario saw the headache that resulted from a cybersecurity breach in 2012, when the Desmond Hotel and Conference Center in Albany, N.Y. reported that credit card information for guests who had stayed there over an 11-month period may have been stolen when the hotel's computer system was hacked. Acquario is the executive director of the New York State Association of Counties, which had held its legislative conference at the hotel during that time.

Despite the headaches that arose from covering that fiasco, he said cybersecurity liability insurance is not yet a smart purchase for most counties.

"It's an emerging market," he said. "It's too early for it to be cost-effective because it's not clear exactly what they are covering. The price is still too high for that."

The U.S. Department of Homeland Security agrees with that assessment for the cybersecurity insurance market in general, opining that "while a sizable third-party market exists to cover losses suffered by a company's customers, first-party policies that address direct harms to companies themselves remain expensive, rare and largely unattractive."

Valuing damage from cyberattacks is also murky, because detecting one is not necessarily a given, and a lot of time may pass before one is uncovered.

Cynthia Stephenson, the risk management coordinator for the New Mexico Association of Counties said her members have not been flocking to the cybersecurity policy her association's insurance broker has offered, with only nine of the 28 insurance pool members opting in.

"We haven't had anyone asking us for it, beating down the doors demanding to have it," she said. "It has, though, given us an opportunity to do some education for our members to show them what threats are out there."

Acquario said rather than focusing on recovering after a cybersecurity breach, which he said may take time to even notice, counties should protect themselves by fortifying their systems.

The U.S. Department of Commerce Internet Policy Task Force considers insurance as "a potentially effective, market-driven way of increasing cybersecurity" because the policies promote an increase in preventative measures.

Among those measures, Acquario wants to see a multi-state cooperative database of threats so participants could be notified when one member county has a security breach. The greater diversity enhances the variety of information sources.

"Right now nobody's talking to each other, and Sullivan County, N.Y. doesn't know what kind of threats Middlesex County, Va. is facing," he said. "That could be valuable information in working on defenses."

Scott Moss underwrites policies for Citycounty Insurance Services, of which the Association of Oregon Counties is a member.

CIS's rates for cybersecurity liability coverage are lower than private insurers, ranging from $1,000 to $10,000, and provide up to $250,000 in coverage.

Rates are based on the budget a county offers for a policy, the number of records covered, the amount of sensitive information involved and the steps the county has taken to mitigate the risk of a security breach. Variables that influence liability include:

- number of credit-debit card transactions in a year
- number of personally identifiable information records stored
- whether mobile devices are encrypted, and
- whether a system had previously been hacked.

"Having a policy for safeguarding sensitive information helps," Moss said. "Limiting the number of unsuccessful access attempts, pre-authorization controls for users... The more steps a county takes to prevent a breach, the lower their liability."

Gus Wirth, the president of the Wisconsin Counties Association, said his counties are coming around to recognizing the threat cybersecurity breaches pose, but they aren't jumping for insurance policies.

"It's like fire insurance, nobody thinks they need it until it's too late," he said. "Some anticipate their existing policies cover losses from these problems, but they shouldn't be worried about cleaning up the messes. They need to make sure they're not a doorway to infecting other systems in other counties or the state, since everything's connected.

"I think it will be one of those situations where we'll have to be forceful to let the counties know this is a problem."

Ralph Johnson, who serves as King County, Wash.'s chief information security and privacy officer, said the nature of the digital information in which counties deal contrasts with private businesses.

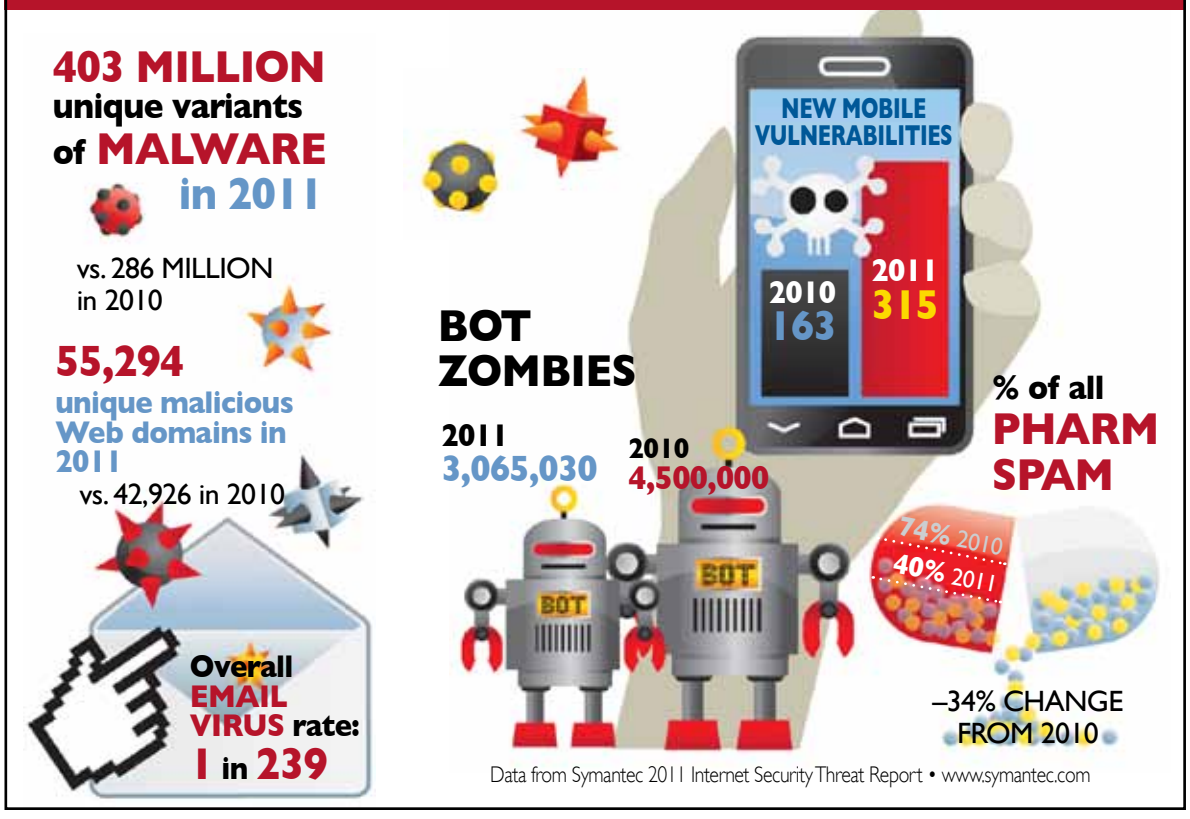
"We're putting out a lot of public information, so we're more concerned with keeping it accurate rather than keeping it hidden," he said. "Counties are still dealing with customers, when they pay taxes or fees online, but not as much as a retailer's website would."

Acquario recommends the Multi-State Information Sharing and Analysis Center as a resource for counties bolstering their information systems—*www.msisac.cisecurity.org*.

Moss suggests the Ponemon Institute—*www.ponemon.org*.

The Identity Theft Resource Center *www.idtheftcenter.org* tracks security breaches and releases alerts.

Cyber Threat Numbers



Online training keeps Wake County employees security-aware

BEST PRACTICES *from page 2*

3,700 employees and make them aware of their responsibility and role in cybersecurity matters.

One of the first steps to gain buy-in from employees was to hold a slogan contest for the program based on the mission statement of the program. The winning slogan was WISE PATH, an acronym based on the first letter of each of the following: Willing to lead; Incorporating best practices; Staying alert; Ensuring all data is secure; Protecting our resources; Accepting our responsibilities; Taking action; Help us succeed.

The program underscores the need for all to accept their security responsibilities, know how to properly use and protect the county's information technology resources, and incorporate security best practices, policies and procedures into their daily operations.

In addition to a one-day security conference about these topics, IT department members staffed booths in many of the county's main facilities to engage employees in discussions about security and answer questions about why security policies were put in place.

Wake County, N.C.

Wake County partnered with Inspired eLearning to provide online training to employees about security awareness. The program caters to the specific policies, platforms and procedures of the county and allows employees to take the training at a time convenient for them. The mandatory training for employees using IT resources lasts only about 30 minutes.

For any employees who need a refresher on any county IT policies, all policies are posted in one online portal for easy access and review. This includes not only the policies governing behavior of employees but also frequent questions such as how to access the county network remotely or how to connect to county WiFi.

You can view the county's online security portal here, *https://we.wakegov.com/is/policies/security/Pages/default.aspx*

You may also want to read:

Five tips for cybersecurity training your employees, published online in FCW: The Business of Federal Technology, 1/21/10

http://fcw.com/articles/2010/01/25/feat-cybersecurity-training-a-must.aspx

You may also want to subscribe to:

Security Awareness Tip of the Day, short, practical bits of advice and tales of caution, provided by the SANS Institute in Bethesda, Md.

www.sans.org/tip_of_the_day.php

Two things a chief information officer should do for your county

By Bert Jarreau
CHIEF INFORMATION OFFICER

The increase of Internet bandwidth has led to the growing adoption of social media to strengthen constituent relationships, the dissemination of less costly service delivery via cloud computing and changing consumer expectations for more self-services via the Internet.

Increased broadband capabilities have enabled the introduction of new mobile devices, which has opened up new possibilities for county governments to provide enhanced mobile service delivery. However, the open nature of the Internet provides an ever-growing list of cybersecurity risks that every county needs to address.

Cybersecurity risks typically include unauthorized website access, denial of service attacks, data privacy loss, identity theft, credit card fraud, repairs to county databases after system failures, services disruption, reputation impairment and failure to comply with the growing number of regulations on data privacy. Attacks have attracted national attention and chief information officers (CIO) who have not addressed these problems have been found wanting (as in "Career Is Over").

There are two things your county's CIO should do for you regarding cybersecurity: Maintain a strong cybersecurity team and raise awareness.

Maintain a Strong Cybersecurity Team

The county CIO's cybersecurity team is responsible for integrating technologies and practices that county governments use to protect their digital networks and resources from attack, damage or unauthorized access and use.

The cybersecurity team typically addresses the need for disciplined identity authentication, rigorous password utilization and management, disciplined change-management procedures, the development of backup resources and routines, and preparations for business continuity management.

The relentless pace of technology evolution is fueling a huge and continually increasing demand for qualified cybersecurity expertise. One of your CIO's biggest challenges is dealing with the cybersecurity workforce shortage. The shortfall in cybersecurity skills is a critical weak point for emergency response teams trying to cope with escalating incidents and threats. CIOs are working to strengthen the

See **CIOs** *page 6*

Computer usage policies educate, set rules for county employees

POLICIES *from page 2*

information is deemed "private." Information privacy must be weighed against the public disclosure requirements within the jurisdiction. It will set forth guidance for employees relative to handling and dissemination of such information. It will also provide constituents assurances that such information about them in the possession of the county will be protected from disclosure within the bounds of the prevailing public disclosure legislation. This policy too must be endorsed at the highest levels of county government. As with the information security policy, codification should also be considered.

Information Classification Policy: Information classification defines the categories of sensitivity of information. This policy is essential in determining what to protect and how best to protect it. Classification levels should be easy to understand and apply with no more than four or five categories. Examples of classification levels include public, protected, sensitive and highly confidential.

Acceptable Use Policy: As guardians of the public trust, our employees must not abuse or misuse county assets. This policy outlines what workforce members are and are not allowed to do using the county's information and information systems.

Setting forth such expectations of behavior for employees and others shows our residents that we care about their trust. Be sure to coordinate this policy with any ethics policy or guidelines that exist in your jurisdiction.

Access Control Policy: Access control sets forth the rules that govern who can have access to what types of information, under what circumstances and when. This policy is where concepts such as "least privileges," "need to know" and "deny all except what is explicitly granted" are defined as well as how access to information and systems is granted and managed for employees, contractors, vendors and even residents.

Second-tier Policies

Once these are in place then the organization can focus on policies specific to its needs. The second tier of policies are based on the concepts set forward in the policies above. They focus more on the technologies inherent within the organization. Some examples of such policies may include:

- Firewall management
- Vulnerability and patch management
- Email and instant messaging
- Use of encryption
- Internet filtering
- Network interconnection
- Remote access
- Incident response
- Physical security of information assets
- Business continuity and disaster recovery
- Consumerization or BYOD (bring your own device)

In developing these documents, every policy should relate to an organizational objective. If you can't identify an objective, ask why do we need this policy? In other words, define the problem as clearly as possible before beginning to develop the policy.

For example, King County's strategic plan includes the objective: "Exercise sound financial management and build King County's long-term fiscal strength."

Our enterprise information security policy tracks back to this objective by stating that "information security controls should be cost-effective and proportionate to the risks associated with the information asset." This statement provides focus on the risks associated with specific information systems and balances the cost of controls against those risks.

The same strategic plan also states the objective of "Establish a culture of customer service and deliver services that are responsive to community needs." If we consider the county's privacy policy, it's all about serving our customers, residents and others. This policy contains statements such as "When Personally Identifiable information is collected directly from the individual, Organizations shall at the time of collection identify the purpose for collecting the information," and "Organizations shall allow an individual to review his/her Personally Identifiable Information and, upon request."

It is essential that, once a set of information security policies is established and approved, they are distributed to and made available to all workforce members. This ensures that all employees and contractors are aware of their expectations of behavior and that they will be judged, evaluated and even disciplined based on their adherence to these policies.

Also consider making policies available to residents on the Internet (use caution as not to publish information that is confidential, for example any policies that mention specifics related to technology in use and configurations). This provides evidence of due diligence and shows your citizens that you care about the protection of their information.

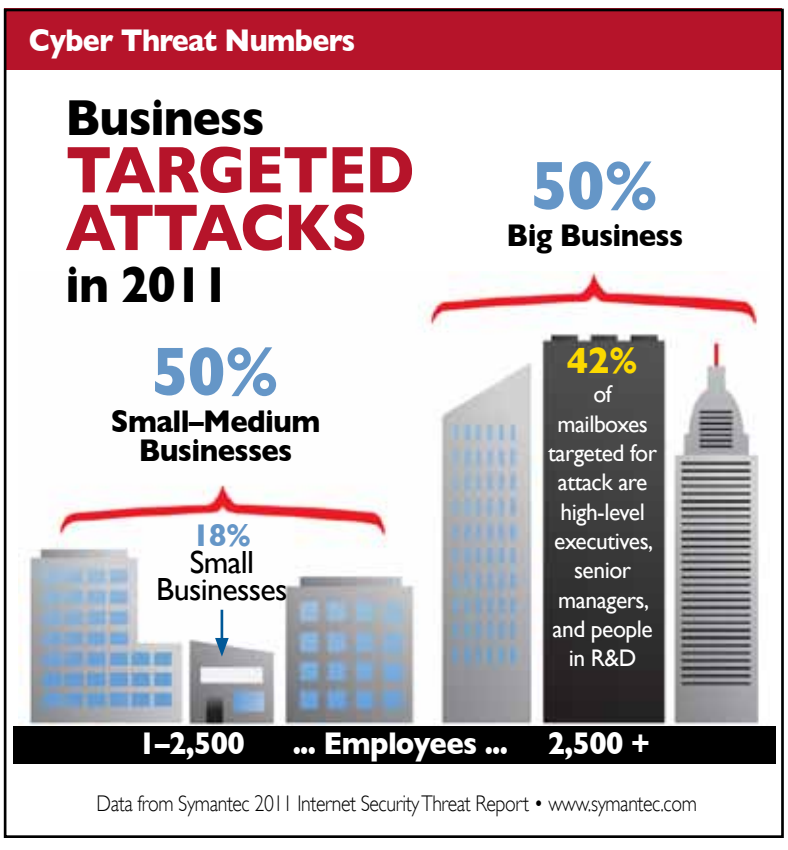
Policies are essential to establish expectations of behavior for workforce members. Nowhere in the organization are they more important than the area of information security.

By developing clear and concise policies in this area based on sound reasoning, you can provide your county with a solid base to ensure that the right things are done to protect the information about your residents, employees and vendors that is in your county's possession.

(Ralph Johnson, CISSP, CISM, CIPP/US, HISP is the chief information security and privacy officer for King County, Wash.)

Hear more from Ralph Johnson about protecting your information assets at a NACo's Legislative Conference workshop, "Cyber for Counties: What Elected Officials Need to Know," March 4.

Cyber Threat Numbers



Data from Symantec 2011 Internet Security Threat Report • www.symantec.com

Cybersecurity workshops offered at NACo Legislative Conference

CIOs *from page 5*

county cybersecurity workforce via improved recruitment, internships, fellowships, and job rotation and recognition opportunities.

Regardless of the technologies the cybersecurity team implements to protect your county digital network, a seemingly innocent action from your county staff can compromise your security. All it takes is one county staff member to unwittingly open a malicious email and click on an embedded link. Vigilance and education across the employee population help to control and contain such deceptions.

Raise Awareness

Cybersecurity awareness provides protection from significant future losses from cyber crimes, such as financial fraud, stolen critical intellectual property, identity theft, or lawsuits and fines resulting from the unauthorized disclosure of personally identifiable information. You should offer training to all your county employees that raises their cybersecurity awareness.

There are many resources to raise cybersecurity awareness. For example, NACo is offering a series of workshops at the NACo Legislative Conference in March where county officials can learn about cybersecurity demands. In addition, the nonprofit organization, The SANS Institute, offers an online cybersecurity training program called Securing the Human (*www.securingthehuman.org*) that ensures your county is compliant and focuses on changing behaviors and reducing risk.

Cybersecurity Resources

There are a number of nonprofit and corporate publications that can help raise your employees' cybersecurity awareness:

Digital Communities Special Report (December 2012): *Cybersecurity Handbook for Cities and Counties* – Cyberthreats are increasing in number and severity, but an ounce of prevention goes a long way toward protecting systems and information. Visit *www.digitalcommunities.com/magazine/Digital-Communities-December-2012.html*.

2012 Deloitte-National Association of State Chief Information Officers (NASCIO) Cybersecurity Study: *State Governments at Risk: A Call for Collaboration and Compliance* – Documents the relative strengths and weaknesses of the security programs that protect state governments' vital systems and data. Visit *www.nascio.org/publications/index.cfm#157*.

2012 Verizon Data Breach Investigations Report – A study conducted by the Verizon Research Intelligence Solutions Knowledge (RISK) Team with cooperation from the Australian Federal Police, Dutch National High-Tech Crime Unit, Irish Reporting and Information Security Service, Police Central e-Crime Unit and U.S. Secret Service. See *www.verizonbusiness.com/about/events/2012dbir/*.

Symantec's *The Internet Security Threat Report (April 2012)* – Provides an overview and analysis of the year in global threat activity. The report is based on data from the Global Intelligence Network, which Symantec's analysts use to identify, analyze and provide commentary on emerging trends in attacks, malicious code activity, phishing and spam. Visit *www.symantec.com/threatreport/*.

IBM Institute for Business Value's *Managing Threats in the Digital Age (2011)* – Addresses security, risk and compliance in the C-suite. Visit *www-935.ibm.com/services/us/gbs/thoughtleadership/ibv-security-managing-threats.html*.

IBM Institute for Business Value's *Emerging Security Trends and Risks (2011)* – Highlights the importance of taking a holistic approach to cybersecurity that addresses both business challenges and technical issues. Visit *www-935.ibm.com/services/us/gbs/thoughtleadership/ibv-it-security-trends.html*.

Annotated Glossary of Cybersecurity Terms

The National Institute of Science and Technology's "Glossary of Information Security Terms" lists 1,393 entries. That's a lot of definitions. We won't subject you to quite that many, though. We reduced the list — a lot — so you can get a jump on understanding some of the common terms often used by information technology professionals when discussing cybersecurity today.

▶ **Backdoor** — In a computer system, a backdoor refers to an overlooked or hidden entry into a computer system. A backdoor allows a hacker or other unauthorized user to bypass a password requirement and to gain access to a computer.

▶ **BYOD (Bring Your Own Device)** — a term used to describe a policy allowing users to bring their own devices (smart phones, tablets and non-standard personal laptops) to interact with companies' network. IT departments have traditionally prohibited this in the past for security and control reason. However, the productivity and cost savings realized from BYOD have prompted companies to change their policies.

▶ **Cloud Computing** — A popular and overused term today, cloud computing broadly refers to computer resources that are off-site, available remotely and hosted by a third party. The security implication of being in a cloud world demands a clear understanding of the terms of engagement between the cloud provider and the client company, or county.

▶ **Denial of Service (DoS) Attacks** — Although the means to carry out, motives for, and targets of a DoS attack may vary, they generally consist of the efforts to temporarily or indefinitely interrupt or suspend services of a computer network connected to the Internet.

One common method of attack involves saturating the target machine (computer or server) with external communications requests so that it cannot respond to legitimate traffic, or responds so slowly as to be rendered essentially unavailable.

▶ **Firewalls** — Systems placed on a network that inspect all data coming in and out of the network. They work on a set of predefined technical rules to decide with pieces of data are able to pass through and which must be stopped. They are essentially the gatekeepers to determine what gets in and what gets out.

▶ **Firmware** — Software that is embedded into hardware. It can be found in electric components including computer chips and is usually created to manage very specific functions. Computers generally have several chips with built-in firmware. With time, errors or vulnerabilities can be discovered in firmware that can cause security risks to host computers.

▶ **Flash drives, Thumb Drives** — Very small, portable storage devices that can store very large quantities of information and can be attached to a USB or firewire port quickly and easily to transfer files.

▶ **Hacktivist Groups** — Ideologically motivated hackers who attack entities' networks to promote change or make a political statement. Tactics include Web defacements, redirects, denial of service, information theft, Web site parodies, virtual sit-ins, and virtual sabotage. Some groups are well organized and aim to conduct more malicious attacks to advance their views.

▶ **Malware** — A term that is used to describe malicious software, created solely for the purpose of bringing harm to computer systems. Also referred to as malicious code, malware comes in the form of viruses, worms, Trojans, spyware and other harmful programs. Malware damage can range from the merely annoying to severely destructive.

Some of the more common forms of malware include:

– **Viruses** are malicious computer codes attached to other computer files. They generally require action from the user to activate the code to perform their intended illicit function. They are most often spread by email and infected websites.

– **Worms** can be as dangerous as viruses. The main difference between them is that worms have the ability to replicate themselves from one computer to another within a network without any interaction with the user.

– **Trojans** are unique in that they trick users into believing they are installing legitimate software. When activated, they often create mechanisms for criminals to remotely harm or control the infected computer.

– **Spyware** is software that attaches to infected computer systems, then searches for personal information stored on the computer and forwards it to a remote location predetermined by cyber criminals

– **Adware** generally forces an infected computer to pop-up commercial advertising, often in an attempt to coerce the user into purchasing unneeded software to remove said adware.

▶ **Phishing** — A term used to describe attempts to lure users into disclosing personal, financial or other compromising information. They usually arrive in the form of pop-up windows or emails pretending to be from a familiar, trustworthy source. Providing the requested personal information can lead to financial exposure.

▶ **Social Engineering** — A euphemism for non-technical or low-technology means such as lies, impersonations, tricks, bribes, blackmail and threats used to gain access to and attack information systems.

▶ **Spoofing** — An email that arrives with a fake email address to fool the recipient into believing that the email is from a familiar or other reputable source. It is often used to help carry out a phishing scheme or some other nefarious task.

Can't get enough of cybersecurity terms? Overheard an expression you are unfamiliar with?
Try *www.whoswatchingcharlottesville.org/glossary.html* for more cyber word definitions.

Think your county is immune to cyber threats? Think again

SECURITY *from page 1*

the county depends on technology to function," he said, "whether it's someone at the front desk wanting to get a marriage license, or a cop on the street needing to get information on someone they've just pulled over. It's all technology-driven."

Threats to Data and Infrastructure

While theft of data, as in South Carolina, is headline-grabbing and not to be minimized, cybersecurity is more than keeping records secure. Counties have another key directive: to protect the lives, health and safety of their residents.

Mike Hamilton is Seattle's chief information security officer and has created a system — comprising the city, counties, municipal utilities and hospitals — to assess cyber-terrorism threats regionwide. "It's a neighborhood block watch, essentially," he says of the Public Regional Information Security Event Management system, PRISEM for short (see related story below).

"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."

Local government computers don't just store and process data, they also run and monitor systems, including water treatment plants, electric utilities, and the like. Already, there are documented cases of hackers accessing industrial control systems (ICS). Last month, the FBI confirmed a report that a New Jersey company had remote control of its HVAC system taken over by a hacker; no harm was done. Cybersecurity experts believe if it can be done, it will be done, next time perhaps with intent to sabotage.

In an October 2012 report, DHS' Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) warned of an increased interest in hacking industrial control systems by so-called "hacktivists" (hacker activists). These are ideologically motivated hackers who attack networks to promote change or make a political statement.

"Hacktivist groups are evolving and have demonstrated improved malicious skills," ICS-CERT wrote. "They are acquiring and using specialized search engines to identify Internet-facing control systems, taking advantage of the growing arsenal of exploitation tools developed specifically for control systems."

SHODAN is one such specialized search engine. Its freely accessible homepage (*www.shodanhq.com*) proclaims: "Expose Online Devices. Webcams. Routers. Power Plants. iPhones. Wind Turbines. Refrigerators. VoIP (voice over Internet) Phones."

Seattle's Hamilton said while counties need to be concerned about their "key information resources," control systems exist in every local jurisdiction in the United States.

"Everybody manages transportation; everybody moves water around. These are what we ought to be focusing on here," he said, "and this is where either the federal government needs to step in and provide some grant money for local jurisdictions to get after the business of securing this stuff, or regional innovations like the PRISEM system are going to have to step up and pick up the slack."

Whether protecting infrastructure or information, the biggest challenge for cybersecurity professionals is aiming at a moving target.

"Cybersecurity is a journey. There is no such thing as perfect security, and the weakest link is people," said John Lainhart, an IBM cybersecurity expert who is an industry representative on NACo's task force. This is true regardless of what protective systems are in place.

Gone 'Phishing'

Aside from the occasional inside job, most malicious threats to computer network security originate outside a county government center's walls. But many breaches — South Carolina's included — probably would not have been as successful for the intruders if it weren't for an employee's seemingly innocent mouse click on a link in a "phishing" email. Cybercriminals phish for information — usernames, passwords and financial account information, for example — by posing as a trusted entity.

In a report on the South Carolina incident, Mandiant, the company hired by the state to assess what happened, was able to determine that a malicious email was sent to several Department of Revenue employees last Aug. 12. At least one of them clicked on a link in the email, launching so-called malware (malicious software) that likely stole the person's username and password.

According to Microsoft, cybercriminals often use "social engineering" — appealing to a person's fears or emotions — to convince computer users to install malware or give up personal information under false pretenses. It could be via email or a phone call to convince you to download something from a website. Social engineering techniques can include threats of account suspension or the promise of something of value for free.

Federal Resources Available

The Department of Homeland Security's Stempfley said federal resources are available to help counties with cybersecurity. They include the Multi-State Information Sharing and Analysis Center (MS-ISAC) and the State, Local, Tribal, and Territorial (SLTT) Engagement Program (see Resources, page 8).

"Several of the programs that we're putting forward such as the continuous diagnostics and mitigation program for the federal government, we're procuring in a way that will enable state and local governments to procure off of it as well," she said, "thereby buying at a lower price point … because the federal government has helped to meet an initial bar for purchasing to get a volume discount."

Cyber threats come in many forms, as the previous examples have shown. A distributed denial of service (DDoS) attack, like the one that affected Larimer County, Colo., is one in which a network or website is flooded with incoming requests that overwhelm the system, making it unavailable to legitimate users. The September 2010 attack left county employees unable to access email or use the Internet for two days.

Sheriff Justin Smith said, "It had a significant impact on Larimer County both operationally and financially."

The attack didn't come from Kazakhstan. According to the FBI, it was launched by a 27-year-old former county resident who allegedly was retaliating for receiving a DUI citation from the sheriff's department.

Educating County Policymakers about Cybersecurity Threats

NACo President Chris Rodgers has made cybersecurity a key initiative of his term in office, hoping to get county policy makers engaged, educated and empowered to prepare them for this evolving, shape-shifting threat to their operations.

"For years, counties have been at the forefront of emergency management. We have prepared for floods, hurricanes, tornadoes, and more," Rodgers said. "But for one of the most destructive issues of our time — cybersecurity threats — we are ultimately vulnerable.

"County IT staffs have known about this for years, but the elected county policy makers are way behind."

In Pacific Northwest, counties participate in PRISEM system to identify cyber threats

By Charles Taylor
SENIOR STAFF WRITER

"There's strength in numbers" could be the mantra of counties and cities in the Seattle area that are collaborating to assess cyber threats regionally.

The Public Regional Information Security Event Management (PRISEM) system is led by the city of Seattle. It is equivalent to a private sector firm known as a managed security service provider, which reviews computer network event logs for unusual or unauthorized behavior.

King, Kitsap and Thurston counties are among its members, along with the Shonomish County Public Utility District (an electric and water utility), several cities, maritime ports and a local children's hospital.

"The real focus is protecting critical infrastructure," said Mike Hamilton, Seattle's chief information security officer, who led the effort. Each participant's logs are sent to a central entity for review to provide a regional view — look for patterns and irregularities — rather than just looking at each individual network. The data is analyzed for potential threats.

Individual incidents such as a compromised desktop communicating to Ukraine — a known center for cybercrime activity — typically would be handled by the targeted jurisdiction, he explained. But PRISEM can determine whether other participants are experiencing the same threat.

The project is being funded by grants — about $500,000 from the U.S. Department of Homeland Security — and state and port security grants, Hamilton said.

PRISEM has been able to show that a cybersecurity attack targeted at Seattle was actually trying to steal medical research data from the University of Washington. "Why would they attack the city of Seattle for that?" Hamilton asked. "Because we share networks; we have trust established between us, and so they're looking for the unlocked door to be able to get in."

Kitsap County's cybersecurity honcho, Ed Sherman, explained the system's value to his county. "If someone is trying to get into Snohomish County's system — it's just a few hits — it's not a big deal," he said. "But if Kitsap County or Thurston County or some of the other entities in the area are getting the same types of hits from the same locations, then all of a sudden it becomes much more visible as this is a valid and probably dangerous attack."

Hamilton said PRISEM also gives the region the ability to predict areas of vulnerability. "There are certain things that can occur as well that we need to tell the federal government about," he said, "and another one of our R&D projects is automating event escalation to the federal level.

"If you think about it, there could be events that we can predefine that are pretty easy to define, actually, like all of the energy utilities in the region are under attack by this threat actor in North Korea, whatever.

"We're going to have our problem to solve here, and we're going to have to fend that off. But that is something that the federal government needs to know, because they can push down that information elsewhere and give that situational awareness to utilities that might not have been aware of that problem, and they can raise their defenses," he said.

Cybersecurity Resources

Department of Homeland Security

The U.S. Department of Homeland Security (DHS) National Cyber Security Division (NCSD) 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 NCSD, the State, Local, Tribal, and Territorial (SLTT) Engagement Program fosters the relationships that protect the country's critical infrastructure.

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 Cyber Security Working Group**.

To learn more, email *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 **Cybersecurity Partner Local Access Plan (CPLAP)** is an initiative that leverages the existing capabilities of state fusion centers as platforms to facilitate classified cybersecurity information sharing to state cybersecurity officials. CPLAP provides states with valuable risk-management information on threat context, vulnerability identification and analysis, in addition to information on potential consequences of threats for Critical Infrastructure and Key Resources (CIKR) Sectors and local governments.

For more information, contact the SLTT program at *SLTTNCSD@dhs.gov.*

▶ The **Multi-State Information Sharing and Analysis Center (MS-ISAC)**, in partnership with DHS and the State, Local, Tribal, and Territorial (SLTT) Engagement Program, MS-ISAC provides cybersecurity support and services to SLTT governments. Currently, DHS grant funding to the MS-ISAC provides cybersecurity services for the networks and systems of 16 states and two local governments.

For more information, contact the SLTT program at *SLTTNCSD@dhs.gov.*

▶ The **SLTT Security Clearance Initiative** grants security clearances to state chief information officers (CIO) and chief information security officers (CISO). Clearances received through the initiative will enable SLTT CIOs and CISOs to receive high-value classified and sensitive information about current and recent cyber-attacks and threats, better informing their cybersecurity risk-management decisions.

For more information, contact the SLTT program at *SLTTNCSD@dhs.gov.*

Cyber Assessments, Evaulations and Reviews

▶ The **Cyber Security Evaluation Tool (CSET)** provides a systematic and repeatable approach to assess the cybersecurity posture of Integrated Computer Sharing (ICS) networks. CSET is a stand-alone software tool that enables users to assess their network and ICS security practices against industry and government standards, and it provides prioritized recommendations.

To request a CSET CD, email *cset@dhs.gov.* For all other questions, email *cssp@dhs.gov* or visit *www.us-cert.gov/control_systems/*.

▶ The **Cybersecurity Assessment and Risk Management Approach (CARMA)** assists 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 *NCSD_CIP-CS@dhs.gov*.

▶ **The Cyber Resilience Review (CRR)** is 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://www.cert.org/resilience/rmm.html.*

For additional information or to request a CRR email *CSE@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/bsi/events/1417-BSI.html*

▶ **"Build 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*.

Exercises and Training

▶ The **CyberStorm Exercise Series** focuses on simulated cyber-specific threat scenarios intended to highlight critical infrastructure interdependence and further integrate federal, state, international and private sector response and recovery efforts. The series helps participants assess their response and coordination capabilities specific to a cyber incident. Contact *CEP@dhs.gov* for more information.

Emergency Response and Readiness Teams

▶ The **United States Computer Emergency Readiness Team (US-CERT)** operates a "24x7x365" Operations Center; provides situational awareness reports and detection information regarding cyber threats and vulnerabilities and conducts cyber analysis; and provides on-site incident response capabilities to federal and state agencies. To report suspicious cyber activity, call US-CERT at 888.828.0870 or email *soc@us-cert.gov.*

The US-CERT's **National Cyber Alert System (NCAS)** delivers timely and actionable information and threat products, including alerts, bulletins and tips to users of all technical levels. Visit *www.us-cert.gov/cas/signup.html* to subscribe.

▶ **Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)** coordinates control systems-related security incidents and information sharing through use of **Fly-Away Teams** with federal, state and local agencies and organizations, the intelligence community, private sector constituents, and international and private sector CERTs. ICS-CERT also operates a **Malware Lab** to analyze vulnerabilities and malware threats to ICS equipment used in settings such as water, waste water or electricity plants.

To report suspicious cyber activity affecting ICS, call the ICS-CERT Watch Floor at 877.776.7585 or email *ics-cert@dhs.gov*

Outreach and Awareness

▶ DHS' National Cyber Security Division (NCSD) collaborates with its partners, including the National Cyber Security Alliance (NCSA) and the Multi-State Information Sharing and Analysis Center, to support public outreach and awareness activities, including **National Cyber Security Awareness Month** in October, **Stay Safe Online Campaign** and the **Stop. Think.Connect. Campaign**. The SLTT Engagement Program has been essential to the continued success of this annual event, helping to secure resolutions from all 50 states. In partnership with MS-ISAC and NCSD's Outreach and awareness program, the SLTT Engagement Program works to sponsor events and activities throughout the country and disseminate Awareness Month key messages to state and local partners.

To learn more or to book a speaker for an upcoming event, visit *www.dhs.gov/cyber* or *www.dhs.gov/stopthinkconnect.*

Additional Resources

▶ **Center for Internet Security (CIS):** CIS is a not-for-profit organization, focusing on cybersecurity readiness and response of public and private sector entities, with a commitment to collaboration. Through its three divisions — Security Benchmarks, Multi-State Information Sharing and Analysis Center and Trusted Purchasing Alliance — CIS serves as a central resource for high-quality products and services. *www.cisecurity.org*

▶ **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. *http://securingourecity.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. *www.corp.att.com/stateandlocal/docs/cyber_security_essentials.pdf*

▶ **Top 10 Vulnerabilities Inside the Network**

Article from 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. *www.networkworld.com/news/tech/2010/110810-network-vulnerabilities.html*

▶ **Mobile Attacks Top the List of 2013 Security Threats**

Article from Jan. 9, 2013 online publication, *CIO* lays out new threats on the horizon to securing your cyber space. *www.cio.com/article/725948/Mobile_Attacks_Top_the_List_of_2013_Security_Threats*

Hot Topics

Contributors

- **Charlie Ban,** staff writer
- **Katie Bess,** research assistant
- **Jerryl Guy,** information technology manager
- **Dalen Harris,** associate legislative director
- **Jack Hernandez,** senior graphic artist
- **Bert Jarreau,** CIO
- **Kathryn Murphy,** senior research associate
- **Beverly Schlotterbeck,** executive editor
- **Charles Taylor,** senior staff writer

Guest Writer

Ralph Johnson, King County, Wash.