CYBER-SECURITY

A RESEARCH REPORT FROM
THE CENTER FOR DIGITAL GOVERNMENT

INSIDE:

NEW THREATS, NEW TACTICS

Maj. Gen. J. Kevin McLaughlin is the commander of the 24th Air Force, one of two component numbered air forces under Air Force Space Command, and Air Forces Cyber (AFCYBER), the Air Force component of U.S. Cyber Command.

e.Republic SMART MEDIA FOR PUBLIC SECTOR INNOVATION

100 BLUE RAVINE ROAD, FOLSOM, CA 95630
916.932.1300 PHONE | 916.932.1470 FAX

COVER PHOTO BY DENNIS BURNETT

THE END OF BUSINESS AS USUAL

One doesn't have to dig very deep to find the examples. In late October 2012, a large-scale attack at the South Carolina Department of Revenue exposed 4.2 million Social Security numbers, cost the state a reported $14 million (and counting) and led to the resignation of Director Jim Etter.[1] A similar incident earlier in 2012 claimed the job of highly respected CIO Stephen Fletcher after the health and Medicaid data of 800,000 Utah residents was stolen.[2] Additionally, a breach at the University of Nebraska exposed the personal information of over 650,000 students, parents and alumni.[3]

Cyber crimes, cyber thievery and cyber warfare have become an everyday reality in the 21st century. In fact, security breaches are so prevalent that, according to a new study from the National Cyber Security Alliance and a private sector firm, 26 percent of Americans have been the victims of a data breach in the past 12 months alone.[4] Another recent study reported that the federal government has (unintentionally) exposed more than 94 million records containing personally identifiable information in the last three years.[5]

Not only do breaches reduce citizens' trust in government to protect their confidential data, they also cost government agencies a significant amount of money that they can't afford to spend. The direct costs of the Utah breach, shouldered by the state itself, were estimated to be roughly $9 million. But according to a new study, the total costs could be much more: The impact on the government, the affected individuals and their financial institutions is expected to exceed $406 million.[6]

For most chief information officers (CIOs), chief information security officers (CISOs) and other government keepers of data, these examples prompt one immediate question — "Can this happen to us?" — followed by inquiries of where the threat is coming from, how bad it really is and how bad it can get. And finally, "How do we protect our systems and our people?"

The answer to the first question is yes. It probably already has to some degree. The follow-up questions are trickier.

This Special Report on Cybersecurity will look at the ever-evolving digital threats that are impacting federal, state and local governments, and identify some of the key players who are initiating cyber crimes. Data included from research conducted by the Center for Digital Government (CDG) will help leaders evaluate how their cybersecurity efforts compare to other government agencies across the nation. Most importantly, the content of the report will focus on solutions — proven practices and innovative thinking to combat cyber threats through awareness, training and technological innovations.

Today's Threats

SOURCE: DATA BREACH INVESTIGATIONS REPORT, 2013

UNDERSTANDING THE THREAT: IDENTIFYING THE KEY PLAYERS

Assessing Your Environment

The trend towards the "professionalization" of bad actors continues to unfold, and it has dire consequences for public sector organizations. According to the Data Breach Investigations Report for 2013, 75 percent of attacks worldwide are driven by financial motives.[7]

Another trend, particularly for the public sector, is the rise in threats from nation states and their proxies. Just as competing generals would fight for "air superiority," or control of the skies in wartime, nations are seeking to assert a sort of "cyber superiority" in the event that a formal conflict breaks out between nations. Competing nations aren't employing teenagers trying to hack their way to free long-distance phone calls; on the contrary, they are developing increasingly sophisticated espionage operations to map the public and private networks of their adversaries. Nations want the ability to take down entire computer-supported systems — and keep them down. In 2012, state-affiliated actors were responsible for 19 percent of all successful data breaches — and the number is rising at an astonishing rate.[8]

Maj. Gen. J. Kevin McLaughlin is the commander of the 24th Air Force, one of two component numbered air forces under Air Force Space Command, and Air Forces Cyber (AFCYBER), the Air Force component of U.S. Cyber Command. "The incredibly capable Airmen of 24th Air Force and AFCYBER, both military and civilian, extend, maintain and defend the Air Force portion of the Department of Defense global network. Our command provides U.S. Cyber Command with trained and ready cyber forces to plan and conduct cyberspace operations in support of combatant commanders. These Airmen provide full spectrum capabilities in cyberspace, giving joint warfighters and the nation's leaders freedom of action in this domain," says McLaughlin.[9] McLaughlin works out of the organization's headquarters at Joint Base San Antonio - Lackland, Texas. In this role, he has a unique perspective to comment about the threats from nation states and their proxies.

"Some articles in the media may overstate the specter of 'cyber war,' while others may downplay threats in the domain; however, as with most things, the truth lies somewhere in the middle," says McLaughlin. "We do know the threat is very real. Malicious activity in cyberspace is on the rise, requiring advanced skills and persistent efforts to defend our nation."

McLaughlin says that because traditional borders delineating where allies and adversaries operate from are less relevant in cyberspace, agencies must work closely with their allies to share information.

"We must also adopt the mindset of protecting our most important assets and worry less about incursions that do not cause harm to systems or missions. We need to apply our resources efficiently and effectively to ensure we can accomplish our mission," says McLaughlin. He is quick to note, however, that this mindset is not valuable solely to military organizations like his own. In his estimation, "this concept applies across the spectrum of public and private organizations."

"We are working to protect our key cyber terrain through focused, deliberate operations," says McLaughlin. "Working together with our sister services and other partners is the only way to get the full picture of our adversaries' activities, thus the only way to posture ourselves ahead of those malicious efforts."

While everyone expects that large federal agencies like the Department of Defense or Department of Homeland Security would be targeted, the comparatively smaller size of state and local government entities is no protection. "Lesson one is that the 'I'm too small to be a target' argument doesn't hold water," notes the Data Breach Investigations Report. While most targets of cyber espionage tend to be in the manufacturing, transportation and professional industry segments, public sector entities are high-value targets themselves.[10]

Thinking About the Insider Threat

New data has shed light on the true nature of the insider threat — in other words, the security dangers caused by an organization's own employees or trusted partners. Insiders are commonly considered to be the highest-risk population, and insider threats — when they materialize — often involve the greatest damage to the organization. This can lead to a misconception, however, regarding the number of attacks that result from insiders. One global study revealed that only 14 percent of successful breaches were actually perpetrated by insiders.[11] This comparatively small number is cold comfort, however, to those stung by the severity of insider breaches.

Unfortunately for government, it's also becoming easier for hackers with little technical skill to get into the game. The long derided "script kiddies" — a derogatory term among hackers for unskilled people who use pre-packaged programs to attack a target — are coming into their own.

A huge number of effective, downloadable and potentially devastating computer programs are available on the Web. Many of them are offered for free, although some charge a fee for their use. Many script kiddies fit the old-fashioned conception of a hacker as a bored teenager looking for mischief. But these pre-packaged tools are increasingly being used for financial gain. While pre-packaged hackware often targets known or common vulnerabilities, it is still effective. This is especially true for government organizations — many of whom lack the resources to stay current on patches, upgrades and security fixes in the systems that they manage.

24TH AIR FORCE MEDIA GALLERY

The 24th Air Force and AFCYBER extend, maintain and defend the Air Force portion of the Department of Defense global network. The command provides U.S. Cyber Command with trained and ready cyber forces to plan and conduct cyberspace operations in support of combatant commanders.

DEFENSE MECHANISMS: FORTIFYING YOUR SYSTEMS

As noted previously, the threats faced by government are changing all the time. A prudent government security practitioner needs to constantly ask: How do my current defense tactics stack up? Can I defend against attacks from a hostile nation state trying to probe my systems? Against a for-profit criminal enterprise? Against a script kiddie with off-the-shelf hackware?

Understanding Your "Attack Surface"

The array of potential defensive tactics can be bewildering. Before any organization can choose the right tactics, key leaders need to assess the threats and response options in a methodical way. One way to do that is to understand your "attack surface."

In software development, a particular program's attack surface can be defined as the parts of the system that could conceivably be "touched" by unauthorized users, even before a breach would happen. In a physical security context, this would be the outside of the building — the doors, windows and exterior walls. Understanding the "edge" of the system being protected is the beginning of protecting against unauthorized entry.

The greater the size of the attack surface, the greater the risk. This essential concept isn't just for software developers. In reality, it can be extended to all parts of the enterprise. To consider your own attack surface, you first need to consider the building blocks of the security stack, and how you are protecting them.

One powerful methodology for understanding your attack surface is the VERIS methodology, which stands for "Vocabulary for Event Recording and Incident Sharing." Available online at www.veriscommunity.net, the VERIS community is an open framework that aims to provide a comprehensive approach to incident tracking, impact assessment and threat classification. While VERIS was originally developed by the private sector, it has now been released as an open community to allow better collaboration with governments and other

> UNDERSTANDING THE "EDGE" OF THE SYSTEM BEING PROTECTED IS THE BEGINNING OF PROTECTING AGAINST UNAUTHORIZED ENTRY.

industry players. VERIS "is designed to provide a common language for describing security incidents in a structured and repeatable manner."[12] It is increasingly being adopted by governments to map out their attack surface and identify gaps in their current defenses.

How Solid is Your Security Foundation?

To consider your own attack surface, you first need to consider the building blocks of the security stack, and how you are protecting them. All of the layers in this graphic are critical to an organization's infrastructure, and all are vulnerable to attacks. How does your security foundation stack up?

A New Approach to Document Security

To encrypt or not to encrypt? That question has bedeviled security practitioners and users alike. Encrypting an entire hard drive helps when a device is lost, but it isn't much use when a document is emailed from that hard drive — in plain text — or copied onto a non-encrypted portable flash drive. Alternatively, full-document encryption can help protect data while it's in transit, but it hides the sensitive information along with all of the other content that doesn't need to be encrypted.

New approaches are surfacing to make data self-protecting — allowing only the sensitive portions of the document to be redacted. User roles can be defined that allow different levels of access. Add-on software allows portions of a document to be encrypted within the native file format. This approach is promising — it allows data to be secured while following the organization's normal document workflows and processes.

Likewise, several companies are investing in intelligent agents that can scan a network within an organization, and quickly identify data that could be sensitive, such as Social Security numbers or patient addresses. The approach could end up making it easier to protect information, regardless of where the data lands.

The Successful CISO's Toolbox

Familiarize yourself with these tools and solutions. They will help you protect and fend off looming cybersecurity threats to your organization's vital assets.

HOT TOPICS: NEW TRENDS IMPACTING SECURITY

The Mobile Threat Vector

It's no secret that government agencies and their employees are increasingly shifting to mobile platforms to get their work done. In a recent survey, CDG had government leaders identify their top reasons for going mobile.

Overwhelmingly, respondents to the survey cited the need for increased productivity as the reason they were moving their applications and services to a mobile platform. This meant mobility for government employees themselves — but also tapping into the increased mobility of the constituents that are served. One government agency CDG contacted — who asked to remain anonymous — noted that more than 40 percent of the traffic to its health and human services agency's online services was coming from mobile devices. Many of the underprivileged and at-risk populations served didn't have a traditional PC at home, but they did have access to a smartphone with Internet access.[13] Thus the mobile platform was not only a way to reach the avant-garde techies out there, but actually those on the margins of society as well.

For better or for worse, mobility has become somewhat synonymous with the notion of BYOD, or bring your own device. Forty-one percent of organizations surveyed by CDG had security concerns when it came to BYOD in their organizations. These organizations pointed to a number of important issues, including malware infection (45%), unauthorized access (45%), data leakage (36%), theft or loss of data (34%), and the separation of personal and business data (21%).[14]

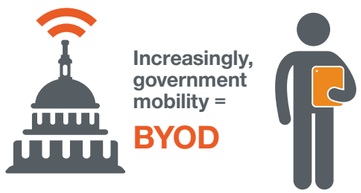
By the year 2022...

the average household with two teenage children will own roughly 50 Internet-connected devices, up from approximately 10 today.

SOURCE: ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

Motivations for Going Mobile

CDG surveyed government leaders about what entices them to go mobile. Overwhelmingly, productivity rules the day.



But there continues to be challenges hampering BYOD adoption:

SOURCE: CENTER FOR DIGITAL GOVERNMENT, 2013

The New Threats to Critical Physical Infrastructure

The recent Hollywood movie *Tron: Legacy* fictionalized a concern that has arisen in the popular consciousness of late. In the 1980s and 1990s, computer experts were primarily worried about the havoc that could be wreaked inside computer systems. They were worried about hackers stealing data, compromising systems and commandeering electronic resources. As the drama of *Tron: Legacy* calls to mind, the growing concern of the 2000s is about what happens when computer-based problems make the jump into the real world.[15]

Protection Strategies from Chester County

Robert J. Kagel, the deputy director for emergency management for Chester County, Pa., describes the county as a vibrant and populous center of industry. It is the highest-income county in Pennsylvania and the 24th highest in the nation, with a population of just over half a million. The county produces 90 percent of the health care industry's imaging systems and 47 percent of the country's mushroom product. As Kagel puts it, "You've got about a 50 percent chance of having a mushroom that was grown in Chester County."[16] Like many other government officials, Kagel has a greater than 50 percent chance of being targeted by electronic hackers with malicious intent.

As the head of the county's emergency management division within the Department of Services, Kagel is charged with protecting the county from a range of potential threats. His department provides 911 services, hazardous material disposal, disaster response and fire rescue training. Rather than dismissing cybersecurity as a remote, technological concern, Kagel recognizes it as a necessary component of protecting his organization and the people it serves.

"We're responsible for anything that could potentially affect the county," he says, "and one of them happens to be a cybersecurity threat, unfortunately." Kagel doesn't see cybersecurity as an isolated threat, or something that only affects the computers themselves. As communities increasingly rely on computers, cybersecurity becomes related to everything else.

In order to comprehensively manage cyber threats and the fallout from cyber incidents, Kagel approaches cybersecurity from several different angles. His department is in close communication with the county's IT department, and passes along intelligence bulletins from the Department of Homeland Security and the FBI on emerging threats. In the event of a cyber event, his department provides necessary assistance to the computing department's incident response team.

And when Kagel thinks about critical infrastructure, he thinks big. Eighty percent of the country's critical infrastructure is owned and operated by the private sector, but Kagel believes that this percentage is even higher in southeast Pennsylvania. "The water systems, the wastewater system, the electricity, the gas — all of those infrastructure elements are owned and operated by the private sector." As such, Kagel's department has a close relationship with private companies to ensure their continued operation.

Cyber attacks on the private sector can have devastating consequences for the county's infrastructure and its citizens. "The reality is that if the electricity goes out because of an attack on a supervisory control and data acquisition (SCADA) system ... there's real impact to the economy and tax base here in Chester County," says Kagel. In such cases, Kagel and his team must then shift their focus from managing cyber threats to dealing with the immediate consequences of the attack. "We're having to ensure that public safety continues and that the public has access to basic needs," Kagel says.

In this vein, Kagel identifies several cybersecurity issues that should receive more attention and resources. One such issue is the threat posed by the loss of technology. Kagel explains how society has moved towards a complete reliance on technology, to the point that when a computer system goes down, employees go home because they cannot be productive without access to email. To address this issue, Kagel suggests that companies and government agencies take a hard look at their processes. They need to put procedures in place for dealing with system failures in order to ensure business continuity.

> "THE REALITY IS WE'LL NEVER BE ABLE TO ELIMINATE THE THREAT, BUT IT'S MORE IMPORTANT TO BE ABLE TO MITIGATE IT."
>
> *Robert J. Kagel, Deputy Director for Emergency Management, Chester County, Pennsylvania*

Unfortunately, there can never be complete security on the cyber front. Chester County, and every county in the country, will always be vulnerable to cyber attacks. Kagel explains, "The reality is we'll never be able to eliminate the threat, but it's more important to be able to mitigate it." To do this, Kagel focuses on the existing challenges and problems within the county's cybersecurity strategies and works to find effective solutions.

Critical Protection in Michigan

In October 2011, Daniel J. Lohrmann became Michigan's first chief security officer (CSO) and deputy director for cybersecurity and infrastructure protection. Now he is leading the development and execution of a comprehensive security strategy for the state's resources and infrastructure. In his time as CSO, Lohrmann has successfully revamped the state's cybersecurity awareness training, developed an advanced training facility for cybersecurity professionals and started initiatives for providing security protection to the private sector.

Lohrmann and his team have also made great strides in developing security protection for the private sector. In February 2013, President Obama released an executive order called "Improving Critical Infrastructure Cybersecurity." The president emphasized that cybersecurity is not just about identity theft, Social Security numbers and credit card numbers. It is also about maintaining the grid in critical sectors, including water and transportation. In response to this order, Lohrmann is working to make Michigan an example of how the government can work with the private sector to provide the necessary cybersecurity protection.

Like Robert Kagel in Chester County, Lohrmann is developing a Cyber Disruption Response Plan. Still in the development stages, this initiative seeks to establish a communication strategy and best practices for the necessary actions following a major cyber incident. The government responds quickly and efficiently to natural disasters, and Lohrmann believes the same preparations should be in place for cyber attacks. As such, the initiative seeks to provide early warnings and rapid information dissemination for the private sector during a cyber crisis. "These are the same type of plans that already exist for fires, floods and tornadoes," Lohrmann says. "Now you can add cyber to the list."[17]

PIV-I and the Proliferation of User Identities

Another potential threat is that posed by weak and ineffective identity and access management. In today's technologically complex world, it can often be difficult to ascertain a person's identity, and individuals can easily maintain several different identities. As an example, Kagel describes how he has a computer that is not connected to any of his organization's systems. This leads to potential holes in the system, because it is impossible to determine, "Well, am I really who I say I am?"

One of the challenges within this area is regulating which personnel receive administrative access. Kagel describes how those in positions of authority will often grant access to certain individuals without going through the proper channels. "[They think,] 'Oh, I'll go give this person administrative rights to the system because I don't want to have to deal with it, and they know what they're doing,'" says Kagel. Unfortunately, this lax approach to administrative access causes holes in the system. Unauthorized individuals are given free rein to download programs, install features and make changes to the computer settings. This broadens the threat environment and exposes the organization to vulnerabilities.

Another challenge in cybersecurity is finding the necessary funding for expenses. Kagel explains how "leadership wants a safe, reliable computer environment, but they don't want to make any investment necessary to achieve those results." Those in leadership positions often prioritize easy access to information over cybersecurity. It is only after a cyber incident that executives realize the importance of a safe and secure network.

To this end, Kagel is working at the federal level with the Department of Homeland Security to try to get the emergency response community to adopt PIV-I.

PIV-I, which stands for Personal Identification Verification Interoperable, is a certificate-based mechanism that provides federal-approved standards for identity proofing. It is able to prove the identity of the individual presenting the credential, and allows the user to be authenticated into the system. It then provides the right access level based on the attributes assigned to the individual's identity.

Kagel says that strong identity and authentication capabilities are critical to cybersecurity, especially at the state and local level. Adopting PIV-I would benefit many governmental systems, including welfare, food stamps, fishing licenses and the regulation of online access.

"All of these things we can do with a single identity, using this technology," Kagel explains, "and overall, help reduce those costs."

Strides have been made with PIV-I on a policy level. The Office of Management and Budget (OMB) issued a memo in 2011, stipulating that any computer systems implemented from that point forward need to be able to support the capability to authenticate using PIV-I.[18] But Kagel still anticipates several barriers to widespread adoption.

The main challenge lies in engaging the vendor community in the adoption process. Currently, the cost of adopting PIV-I is prohibitive. "If you talk to the vendors, the vendors say, 'Well, it's the government's fault,' and if you talk to the government, they say, 'Well, it's the vendor's fault,'" says Kagel, who says that the government and the vendors need to work together to lower the cost, so that the technology can become accessible to everyone.

Kagel has already put several of these solutions into practice within his organization. His department has credentialed all of its emergency responders using the PIV-I standard. This means that emergency responders can arrive at an emergency scene and immediately authenticate who they are and what they can do. It also provides them access to different online county services, which allows for secure information sharing.

Another ongoing initiative in Kagel's department is the development and implementation of a hazard mitigation plan. As required by the federal government, the purpose of this plan is to reduce the impact of future disasters. While the original mitigation plan only addressed naturally occurring disasters, the new one will encompass cyber incidents.

BEHIND THE SCENES: EFFECTIVE STRATEGIES FROM THE FIELD

Building Cyber City, USA

One could be forgiven for thinking that the mighty Department of Defense, with its formidable resources in the Washington, D.C., area wouldn't be interested in partnering. But even the U.S. military is looking to share resources with universities, private firms, high schools and communities around the nation.

"Partnering is an absolute necessity in the development of tomorrow's cyber warriors," says General McLaughlin. "The 24th Air Force has the advantage of being located in San Antonio, a.k.a. Cyber City USA, which has fostered an amazing partnership of government organizations, industry leaders and cutting-edge academic institutions that are working together to make our nation safer." Indeed, the 24th Air Force worked closely with city leaders and the Air Force Association in making San Antonio a leader in the CyberPatriot program — the premier national high school cyber defense competition. They also get involved in local internship programs in order to foster the development of the next generation of cyber talent.

"We are also expanding our support to the National Collegiate Cyber Defense Competition," says McLaughlin, "a nationally recognized competition developed in cooperation with the University of Texas at San Antonio's Center for Infrastructure Assurance and Security and regularly hosted in San Antonio." The command also works closely with private sector companies as well to stay innovative. "The Air Force has entered into Collaborative Research and Development Agreements with several industry partners to find mutual benefit in sharing problem sets and solutions," he says.

"The most important aspect of the nation's defense in this domain, both now and in the future, is the development of a world-class cyber workforce," says McLaughlin. "We are committed to encouraging interest and inspiring creativity in this domain through the mentorship of the next generation of cyber leaders."

Partnering for Dollars

Dan Lohrmann in Michigan has undertaken massive efforts to forge a relationship between government agencies and the private sector, and they have already begun to pay off. Many of Michigan's cybersecurity initiatives, including the cybersecurity training facility (known as the "Cyber Range"), have received private contributions from many different industries. "The state kicked in some money," Lohrmann explains, "but [it was] very small compared to what the private sector kicked in."

public cio
PUBLIC CIO SPECIAL REPORT

DENNIS BURNETT

General McLaughlin says partnering is an absolute necessity in the development of tomorrow's cyber warriors. As an example, the 24th Air Force worked closely with city leaders and the Air Force Association in making San Antonio a leader in the CyberPatriot program — the premier national high school cyber defense competition.

He noted that a single company donated over a half a million dollars to the Cyber Range.

To further strengthen this relationship, Lohrmann has created a sub-group within the Cyber Range dedicated to defending critical infrastructures in both the private and public sector. As he explains, the idea behind the group is that "the public sector, the private sector, nonprofits and education institutions can connect virtually." Lohrmann wants the Cyber Range to be more than just a government entity. He wants it to be able to defend the security of the state at every level.

Sharing Information — Quickly

Will Pelgrin, the CEO of the Center for Internet Security (CIS), has extensive experience with the wide-ranging issues of cybersecurity. He led New York's cybersecurity efforts for many years before broadening his focus with the founding of the Multi-State Information Sharing and Analysis Center, an organization that serves as a cybersecurity resource for all 50 states, several territories and tribal entities, and hundreds of local governments. And in April, Pelgrin was named the 2013 Technology Champion by the National Association of State Chief Information Officers (NASCIO), an honor awarded to those who promote excellence in information technologies and government operations.

With all of this experience, Pelgrin can offer some hard-won wisdom on how to prevent cybersecurity attacks and handle their fallout. Above all else, he emphasizes the importance of collaboration. In fact, if you know one thing about Will Pelgrin, you know that he is a fervent proponent of information sharing among organizations.

"My goal is to see how we can get that information to the right people as soon as possible," Pelgrin says.[19] "I keep saying the bad guys already have it, so all we're doing to ourselves, if we're not sharing, is keeping it out of the hands of the good guys. ... There are people out there who think information is power. I think *sharing* is power."

In keeping with this objective, Pelgrin's organization has an information distribution list that crosses jurisdictional, governmental and private sector lines. As Pelgrin explains, "I try to make our organization a value-add, even to those outside our jurisdiction." Pelgrin works to ensure that the pertinent data reaches all the necessary parties. In this way, the different organizations can work together to build a collective view of any potential threat, and to develop a set of best practices to prevent and handle threats in the future.

Pelgrin also stresses the importance of not over-planning cybersecurity initiatives. He explains how many of his initiatives would have eventually veered off track if he had tried to stick to a pre-planned roadmap. Cybersecurity is a constantly evolving field, and so it requires constant re-evaluation. As Pelgrin says, "I look at how secure I was yesterday and how secure I am today, and if I'm more secure, I keep moving forward. You do have a plan, it's just that plan has to be flexible enough to understand that this environment changes that quickly."

Enrolling Top Leadership

In addition to flexibility, effective cybersecurity requires the support and involvement of those in high positions. Pelgrin advocates raising cybersecurity discussions to the top executive level. In states, this means the governor needs to care. In cities, the mayor and city council need to be on board. And in the federal world, it means agency heads, cabinet secretaries and yes, even the commander-in-chief.

Pelgrin believes that high-level leaders need to be involved in order to fully discuss the risks and potential consequences of each cybersecurity decision. "That would be one of the best practices," Pelgrin says, "making sure that those decisions are made at a higher level, [and] making sure that cybersecurity has a voice at the table."

public cio
PUBLIC CIO SPECIAL REPORT

> "MY GOAL IS TO SEE HOW WE CAN GET THAT INFORMATION TO THE RIGHT PEOPLE AS SOON AS POSSIBLE. ... THERE ARE PEOPLE OUT THERE WHO THINK INFORMATION IS POWER. I THINK SHARING IS POWER."
>
> *Will Pelgrin, CEO, Center for Internet Security*

Moving as Fast as Possible — *But Not Faster*

We all know that cybersecurity threats are "mutating" and proliferating at a blistering rate. We need to respond quickly to roll out new defenses as fast as possible. That said, it is possible to shock users by moving too quickly when implementing new tools and techniques.

For this reason, organizations should be wary about which technologies they allow into the offices. "I love technology," Pelgrin says. "I love new gadgets — but at the same time, I want to make sure that I understand why I'm allowing them into my environment. What I do with gadgets at home may not be the type of gadgets I want in a work environment." Pelgrin uses the example of social media sites. These sites are often frequented from both home and office computers, but they may pose security risks for organizations. Hackers can cultivate an individual's credentials from a social media site, and use these credentials to exploit the individual or the organization.

Technologies cannot be secure or effective unless they are well implemented and integrated into the culture of the organization. As Pelgrin puts it, "The best technology in the world that sits on a shelf is not going to help you."

Defining the "New" Threats

Technology — and the people who use it — has to keep up with the rapidly evolving nature of cyber threats. In this constantly shifting environment, it can be difficult to pin down whether a threat is actually new or just newly discovered. "Is it new because it's really new? Is it new because we're making it more known? Is it new because we just found out about it and it's been happening for the last three or four years?"

Despite these ambiguities, Pelgrin does see a definitive change in the level and scope of the threats as compared to the past. When he first started working in cybersecurity, the most common cyber attack was a form of cyber graffiti. A hacker would break into a government website and deface it by, for example, swapping out photos. "We thought they were horrible at the time," Pelgrin says. "I almost wish for those days to come back."

Unfortunately, Pelgrin and his organization grapple with cyber threats that are not merely aesthetic in nature. Instead, these threats come packed with malware and the ability to cripple systems and infrastructures. But despite the escalation of these attacks, Pelgrin emphasizes that they aren't necessarily any more sophisticated. "The actors out there, whether they're nation state actors, script kiddies ... or the traditional hackers, they take the least resistant path. They will take the lowest common denominator." This means that instead of mounting well-planned attacks, hackers merely look for existing vulnerabilities to exploit.

These vulnerabilities include bad passwords, unsupported software and public social media sites. Pelgrin describes how one of the big indicators of cyber hacking in the past was failed logons. And so, his organization checked for failed overnight logons on a daily basis. Now, however, they can't rule out the possibility that an attacker logged on appropriately.

"We now say, 'Check your valid logons ... look at the time of that [logon],'" Pelgrin says, "Was it appropriate? You may have really dedicated staff, but are they really working at 3:00 in the morning?"

The Evolution of an Attack: Phishing with a Spear

Cyber hackers also cultivate information about the targeted individuals in order to gain access to confidential information. Spear fishing, for example, is a form of cyber attack in which hackers send out fraudulent, targeted emails with links to malware.

These hackers are looking for intellectual property and other confidential data. In order to get access to this information, the hackers use subject-relevant content to entice individuals into opening the fraudulent emails. Targeted individuals mistakenly believe that the email is coming from someone who knows them, even though the relevant information can usually be easily culled from online sources.

Pelgrin offers the example of attending a publicized conference, in which his name would be out on different websites: "Will Pelgrin is doing the keynote at such and such a place." Then Pelgrin or his assistant could get an email reading, "We need to move your time for speaking. Here's the new agenda, is this okay? Can you confirm?" with a link on the bottom. "Who's not going to open that up?" Pelgrin says, "I would."

In one of the spear phishing scams Pelgrin's organization has responded to, government employees in two states began receiving emails that appeared to be coming from individuals with certain job titles; instead, they were scams containing malware. Through further analysis, Pelgrin's organization was able to identify a third state receiving similar emails, and immediately notified that state. The state was able to locate the phishing emails and delete them from the user's mailboxes before the network was compromised or any other malicious activity could occur. In this case, collaboration among organizations paid off in a demonstrable way.

Still Not Enough Collaboration

Pelgrin still sees a lack of necessary collaboration, especially in the management and operations side of organizations. "I think that there's still a disconnect between events and consequences [among] the people who are controlling the budgets [and] who control the management side of the house," he says. Pelgrin explains that many people on the operational side often dismiss cyber incidents if there are no visible consequences. But actually, "[these threats] are running in your background. They can be stealing all your data, and more scary for me, even, is that they're manipulating your data."

This problem could eventually have disastrous consequences for the health industry and the privacy of medical information. Pelgrin predicts that everyone will soon have their medical information stored on their smartphones. This offers many benefits, especially for travelers who may need their medical history on their person in the case of an emergency, but also makes medical information more vulnerable to cyber attacks.

Pelgrin also predicts that technology and our lives will become increasingly automated. However, he cautions that smart technology needs to be deployed in a secure way. As phones and other devices become more computerized, users need to ensure that they have updated software and the necessary patches. This of course applies to desktop and laptop computers as well.

"If you buy a new computer," Pelgrin advises, "it may need patches and you need to make sure it's secure. Most people don't. The last time I bought a computer, which wasn't that long ago, it had over 200 MBs of security patches that needed to be put in place."

Pelgrin also believes that the globalization and commercialization of technology will most likely bring cyber attacks to the forefront. CIOs and other cybersecurity professionals are going to have to remain vigilant to prevent and manage these ever-evolving cyber incidents. When asked what advice he would give to other CIOs, Pelgrin states that "you need to be a champion of this yourself. You can't say it's good for everybody else, but I don't need to do it. The champion starts at the top and the leadership starts at the top."

public cio
PUBLIC CIO SPECIAL REPORT

EQUIPPING PERSONNEL WITH CYBER AWARENESS 2.0

Engaging Your Employees and Eliminating "Death by PowerPoint"

It is important to build a culture of security among your employees that incorporates security in from the start, rather than retrofits it as an afterthought. Employees may be your greatest asset, but if they aren't properly trained and educated, they can also be your weakest link.

When Dan Lohrmann first started his position in 2011, a series of audits revealed that more than 60 percent of government breaches in Michigan could have been avoided had the end user done something differently. At the time, only 5,000 of 55,000 state employees actually participated in the available cybersecurity awareness training. "It was dismal quite frankly," Lohrmann admits. "The numbers spoke for themselves."

So, Lohrmann's first task as CSO was to overhaul the training program. "We wanted to do a paradigm shift," Lohrmann explains, "The idea was, can we do something that is engaging, interactive and relevant? We even used the word fun." Unlike the old training program, which was a series of PowerPoint presentations, Lohrmann's program is Internet based and uses games and other interactive material to engage employees in subject matter. Lohrmann also designed the program to fit into employees' schedules. Rather than forcing them to endure a multi-hour program in one sitting, employees now receive 10 minutes of training once every other month.

The program has been a huge success. It was first implemented in Michigan's executive branch, but soon spread to the judiciary and legislative branches. In total, 60,000 people from state and local governments have adopted the program. "The feedback has been phenomenal," Lohrmann says. "In an overall grade, we are getting nines out of ten on feedback forms." Lohrmann also quotes some surprising feedback from one employee: "My kids love it. Is it okay that I brought this home to my family?"

The program's success has even garnered out-of-state attention. As Lohrmann explains, "A lot of other states are talking to us about following our lead on [the program]." Now Lohrmann's team is working on metrics to prove whether the program has led to reduced incidents and improved security.

Robert Kagel and his team have also made positive strides in the area of employee education. Kagel emphasizes the importance of

When Dan Lohrmann first started his position in 2011, a series of audits revealed that more than 60 percent of government breaches in Michigan could have been avoided had the end user done something differently.

online education, "whether it's teaching an older generation to be smarter in an online environment, [or] educating the younger folks in society at an early age on how to be smart in an online environment. Don't click that suspicious link: A Nigerian prince really doesn't want to send you $10 billion."

To educate employees, Kagel puts on routine presentations on how to be smart and safe in the online environment. And every time an employee opens an Internet Explorer browsing page, they are able to read through different cybersecurity tips. Kagel's educational strategy is to be "right there in [the employee's] face, and pretty prominent every time."

Supporting Ongoing Monitoring and Maintenance

In addition to revamping the state's cybersecurity awareness training, Lohrmann is also working to make the state's security operation center open 24/7. As Lohrmann explains, the center receives after-hours calls, and a full-time center will be better prepared to address these needs. The center will be fully equipped with staff and tools to detect and handle threats at any hour of the day. Many states have already made this transition, and Lohrmann is dedicated to bringing Michigan's operation center up to the current standard. "There is a lot going on with this," Lohrmann says of the initiative. "We call it our bat cave."

But according to Lohrmann, the biggest cybersecurity challenge facing state governments is still the necessity of retaining a talented staff. However, right now cybersecurity professionals are in high demand, and a well-trained, well-experienced cyber worker will often have many job offers from which to choose. "Keeping good, talented security professionals is very difficult right now," Lohrmann says. "I think that is a big challenge."

In this vein, Lohrmann has been instrumental in developing the aforementioned Cyber Range. The facility offers training in the logistics of detecting, preventing and stopping cyber-based threats. As Lohrmann puts it, the Cyber Range "has been more technical training for our geeks, if you will."

What distinguishes the Cyber Range from similar training programs is that it offers practical application scenarios. Whereas many state and local governments provide knowledge-based training, the Cyber Range offers practical applications for this knowledge. As Lohrmann explains, "Everybody knew what gun ranges or proving grounds were where I grew up in Maryland. You prove tanks and military equipment." Similarly, the Cyber Range allows its students to conduct "live fire" simulations to prove their knowledge and skills in a real-world setting.

The facility seeks to answer the question, "How will the students respond to different real-world scenarios?" These scenarios include: "How do you do [network penetration] tests? How do you become certified in a variety of different areas around business continuity? What does your team do when they are attacked?" Lohrmann has already sent 30 members of his staff to the training program. And other states have been impressed by the applicability of the Cyber Range's training and have also sent members of their staff.

Additionally, the facility offers the capability to test devices outside of the operational network. Lohrmann uses the example of a black box. A vendor may make grand claims about the capabilities of the black box, and the Cyber Range can test these claims. "Let's throw a service attack at it," Lohrmann says, "and throw a billion packets at it. Let's throw this virus at it. Let's throw a series of things at it, and see how it responds and what it can do." In this way, the Cyber Range ensures the quality and functionality of vendor-provided devices.

public cio
PUBLIC CIO SPECIAL REPORT

KEEPING PEOPLE AND CRITICAL INFRASTRUCTURE SAFE

In a recent webinar on security hosted by CDG, a participant asked, "Will we always be reactive, or will we ever get ahead of the game when it comes to security?" It's a tough and challenging question that really brings all of today's conversations around security together.

The barbarians aren't just at the gates — they are on top of them, around them, behind them and everywhere in between. Cyber threats evolve, mutate and metastasize faster than ever before. But with the right tools, techniques and strategies, your organization can stay far ahead of the game. And our constituents — the men, women, children, businesses and institutions that you serve — will be the better for it.

In the quest for 100 percent perfection, it is easy to overdo it when the inevitable failures do present themselves. It's especially easy for a sense of outrage to sit in when something goes wrong in the cyber arena.

Will Pelgrin emphasizes the importance of developing a supportive environment for discussing cybersecurity issues. If an employee makes a mistake, for example, by clicking on a link that allows malware into the system, then he or she should feel comfortable alerting leadership without fear of being reprimanded or fired. As Pelgrin puts it, "Senior leadership within government really has to build a culture that creates a safe haven. ... You need to really build that culture of, 'Bring it forward, we'll deal with the issue, and we'll modify our process to improve our cyber position.' ... It's through education. It's awareness, but it's [also] leadership."

In response to many people believing that technology will solve all of their cybersecurity problems, Will Pelgrin stresses that it's more about human behavior than it is about the technology.

In fact, Pelgrin cites the human factor as the most important aspect of cybersecurity. Many people believe that technology will solve all of their cybersecurity problems, but as Pelgrin says, "No one can guarantee 100 percent security. ... It's more about human behavior than it is about the technology."

CENTURYLINK: HELPING GOVERNMENT FIGHT CYBER CRIME

THERE'S NOT A DAY THAT GOES BY without news of anarchy on the Internet: DDoS (distributed denial-of-service) attacks are launched on American institutions; overseas hackers run away with our industrial know-how; and hacktivist groups use cyber threats to promote political agendas.

The definitive indicator that Internet crime is on the rise is the huge uptick in money spent on cybersecurity. Three years ago, the cybersecurity market was worth $1.36 billion; this year it's estimated to hit $33 billion, an astronomical increase of more than 2,000 percent, according to the consulting firm Frost & Sullivan.

"When you look at how the budget is shifting in government and business, you see that the top priority, even during an economic downturn, is protecting communications infrastructure from cyber intrusions," says Diana Gowen, Senior Vice President and General Manager for the Public Sector at CenturyLink, a global communications company based in Monroe, La.

CenturyLink, the third-largest telecommunications company in the U.S., is at the forefront of the cybersecurity battle. A multinational company with roots in rural communications services dating back to the 1930s, CenturyLink now provides voice, data, hosting and cloud services.

With more than 50 data centers around the world, CenturyLink has invested heavily in advanced technology and works closely with the U.S. Department of Homeland Security (DHS) and other government agencies to prevent Internet security intrusions.

"We have a full complement of cybersecurity mitigation tools for government and commercial clients, including leading financial institutions," Gowen says.

Cyberthreats come from nations — some of them known adversaries, some trading partners — that steal intellectual property. They also come from those who launch malicious DDoS attacks on our nation's banking system and other critical infrastructure sectors.

CenturyLink fights back with a portfolio of products that it has developed for business and government. Among them are its DDoS mitigation service; its Managed Trusted Internet Protocol Service (MTIPS), which provides trusted Internet connections; and its Intrusion Prevention Security Service (IPSS).

DHS has approved CenturyLink to offer enhanced cybersecurity services (ECS) to state and local governments, as well as to key business sectors, to keep America's critical infrastructure safe and secure.

"CenturyLink understands that this country is under cyberattack. "It's important to us that we help our government make all of our Internet pathways safer," says Gowen. The future, she believes, is one of government and businesses sharing threat information, building stronger partnerships and switching from a reactive approach to a proactive one. "We're fighting to win."

CenturyLink® Government

For more information from CenturyLink, visit **centurylink.com/gov**

Expert Security, Smooth Access

Dell Software Identity and Access Management solutions give organizations the best of both worlds

CYBERCRIMES, CYBER THIEVERY AND CYBER WARFARE have become everyday realities in the 21st century. Organizations need to protect themselves from these threats while continuing to benefit from the advantages that modern communications and data technology bring to the table. Robust security systems can keep the wrongdoers out — but they also must ensure that authorized personnel can access the information they need.

Dell Software identity and access management solutions can help you meet requirements for access governance, privileged account management, identity administration and user activity monitoring in a unified manner while simplifying key functions.

Access governance: Improve the efficiency of business processes and reduce the administrative burdens for IT by empowering your users with key access governance functions. Help managers understand what employee entitlements actually mean and enable them to certify access accordingly. Establish a continuous process to prevent malicious activity, and ensure that every individual employee has the right access to do his or her job while maintaining regulatory compliance.

Privileged account management: Dell solutions for privileged account management help control and audit administrator access. Automate, control and track the entire process of granting administrative credentials. Capabilities for access control and separation of duties plus comprehensive activity monitoring and audit functionality help you achieve and maintain compliance. Solutions specifically designed for Microsoft® Windows®, Linux® and UNIX® or sudo environments provide the appropriate level of access for administrators to do their jobs — no more, no less.

Identity administration: Gain a better grasp of day-to-day management of users and their associated accounts and identities across your most important systems. Automate and secure account management to authorize user accounts and manage identities. Simplify password management with policies that span platforms and applications. Provide single sign-on capabilities for all platforms, systems and applications while strengthening authentication for the enterprise. Adopt a modular and integrated approach to account management, building on existing investments to achieve a rapid time to value.

User activity monitoring: With Dell solutions for monitoring user activity and system access, you can ensure tight control while simplifying compliance and auditing. Discover potential vulnerabilities, prevent unauthorized access, address policy violations, and immediately and effectively respond to crises. Capitalize on automated functions and consolidated reporting to demonstrate compliance easily.

DELL Software

For more information about Dell Software identity and access management solutions, call **(301) 820-4800**, contact your Dell sales representative, or visit **www.software.dell.com** and get in touch via **www.quest.com/PS-IdentityManagement**

In Here, Your Data Has a Bodyguard

Guarding Government Data

AT&T security solutions help the public sector protect its most valuable asset: information

As data continues to expand and proliferate at an astounding rate, the need for organizations to protect their digital assets becomes ever more pronounced. When data is available 24x7, the potential risk of fraud, theft and other forms of cyber attack increases exponentially. The use of a diverse set of mobile devices by an increasingly "on the go" workforce only adds to the challenge.

AT&T has the security solutions to help keep public sector organizations safe from the threats lurking in the digital world. Whether data is being handled in the office or on the go, AT&T helps protect it with some of the most cutting-edge resources and solutions available. At the heart of it all is AT&T's comprehensive, multi-step security strategy and roadmap. It's an enterprise-wide security program that unifies the security efforts from business to IT and everywhere in between, helping you to meet governance, risk and compliance needs.

AT&T has a long history of developing and managing security services that support a defense-in-depth architecture to help with your security policies. AT&T takes a holistic approach to information security, addressing elements of people, technology and processes. Contact us today to learn more about the AT&T world-class portfolio of assessment, compliance and related security services.

Key components of AT&T's security strategy and roadmap include:

- **Needs Analysis and Framework Establishment** to better understand the unique characteristics and requirements of the organization and map out its ideal security foundation.
- **Risk Assessment and Analysis** to thoroughly study and identify the most pressing risks for the organization and determine which gaps and deficiencies most need to be addressed.
- **Strategy Development** to provide the guidance needed to address the previously identified risks, keeping in mind the organization's unique list of priorities.
- **Roadmap Development** to create a high-level roadmap that outlines and guides the organization's transition to its desired information security program, including short-, medium- and long-range objectives. Highest priorities are identified along with educated estimates of the time and energy required to tackle each step.

at&t

To see how government is transforming with the help of AT&T, visit **www.att.com/govsecurity**.

Connect with Confidence

Security solutions from Cisco keep data everywhere safe

CONNECTIVITY TO NETWORKS via mobile devices and remote sites is rapidly expanding in government organizations striving to improve productivity and efficiency, as well as employee and citizen satisfaction. Connectivity leads to better operations and greater success in all areas. However, it can also create added risk — with the introduction of a new class of threats that are infiltrating networks through both innocent and adversarial intentions. Wherever a connection exists — wireless or otherwise — there are malicious actors lying in wait, looking for a chance to exploit it. And with the expansion of mobility and cloud computing, there are many more connections to protect than ever before.

Android malware alone grew by over 2,500 percent in 2012.[1] Expanding connectivity is having a significant impact on the threat landscape. Although the volume of spam is down, targeted, personalized attacks are up — cybercriminals are becoming more sophisticated in their efforts, creating content that unwitting users will be more inclined to access.[2] Search engines are 27 times more likely than counterfeit software to deliver malicious content.[3] According to statistics from Dark Reading, 8 of the top 10 government security breaches in 2012 occurred in state and local agencies.

In the exciting but increasingly dangerous interconnected world, who can you turn to for help with keeping your organization's important information safe?

CONSIDER CISCO. While others may talk of best-in-class products, Cisco offers best-in-class solutions. Cisco's value is not just what our products can do, but what they can do *together.* Cisco's integrated security solutions include the routing, switching and wireless infrastructure replete with robust security features capable of collecting and analyzing threat assessment data to protect government organizations from evolving cyber threats.

Sponsored Content

CISCO™

PROTECT YOUR ORGANIZATION with Cisco Security Intelligence Operations.
Contact Cisco today to learn more.
www.cisco.com/go/uspscybersecurity

1. www.cisco.com/en/US/prod/vpndevc/annual_security_report.html 2. www.cisco.com/en/US/solutions/collateral/ns1015/ns1238/info_graphics_c82-727889.pdf 3. Ibid.

Multiple Approaches Help Keep Data Secure

NIC helps government close open doors that may lead to security breaches

Government security breaches continue to increase as hackers, cyber criminals and cyber terrorists become alarmingly advanced and better equipped in their efforts to infiltrate systems, sites and servers.

While it's unlikely that breaches ever will be eliminated, the good news is that many may be prevented by simply implementing sound security practices. NIC partners with over 3,500 federal, state and local government agencies to provide secure web sites, services, payments and data that help constituents safely connect and do business with their city or state.

The company has developed over 7,500 unique sites and services in its 21-year history, and keeping data secure is a top priority. The company has a security department lead by Chief Security Officer Jayne Friedland Holland, who speaks regularly at government conferences about helping government protect sensitive data.

"Hackers are clever opportunists," says Holland. "While you can't eliminate the possibility of an attack, you can implement secure best practices that minimize the risk of a security breach."

Best practice considerations for government include:

✓ **Layered and modular method for information security**
Modular architecture allows for replacing, modifying and upgrading security components of sites and applications at any given time.

✓ **Multi-pronged approach to application development**
First, try to develop services that do not require the transmission of sensitive data. When sensitive data is in play, encrypt data and only retain it for business purposes. Once it is no longer needed, purge the data. Also consider time limits on pages with sensitive data that forces users out after a period of inactivity. Finally, run security scans before any application goes live.

✓ **Network integrity that limits malicious traffic**
There are a multitude of security strategies that help ensure malicious traffic is not allowed on the network, including, but not limited to, firewalls, access control lists, intrusion prevention and detection systems, web application firewalls, encrypted communication channels, antivirus software and more.

✓ **Payment processing adhering to highest compliance standards**
Use a payment engine that is compliant with PCI-DSS as a Level 1 Service Provider. When payment account information must be displayed, redact the numbers so that only the last four digits of the account number are visible.

✓ **In-house and third-party vulnerability testing**
Work with third-party security vendors to audit hundreds of security controls each year.

Sponsored Content

NIC™ the people behind eGovernment®

To learn more about how NIC helps keep eGovernment services secure, contact them at NIC@egov.com

Partnering to Protect Citizens' Data from Cyber Attacks

CLEVER HACKERS AND CYBER SPIES can breach networks within a few hours, or even a few seconds. But according to a recent Verizon Data Breach report, 66 percent of such compromises go undiscovered for months, or even longer. By then, personal information, trademarked secrets and classified data are long gone.

In 2012, the average data breach cost U.S. organizations $5.4 million, and took 24 days to resolve, according to a survey by the Ponemon Institute.

As today's cyber threat landscape matures, government agencies should consider custom solutions that combine best-in-class security products to help keep government information and systems safe on slimmer budgets.

Assembling custom, best-of-breed solutions

NetApp, a leading provider of network storage and data management solutions, emphasizes highly efficient, cost-effective solutions customized to each customer's individual needs. Its storage and data management solutions help government agencies take a risk-based approach with the ability to collect, analyze and secure their data. NetApp also helps agencies quickly understand what is happening within their complex environments.

NetApp's solutions help government agencies:

- Maintain regulatory compliance
- Secure data for confidentiality, integrity and availability
- Prevent access to data if drives are stolen or repurposed
- Backup and recover storage data to help ensure business continuity
- Use at least 50 percent less storage compared to traditional storage

CDW•G, a world-leading technology provider, offers custom data security systems geared to government agencies. The company can conduct an in-depth review of the network, as well as provide related consulting and products from industry leaders to address individual agency needs.

CDW•G also supplies the following products and solutions from multiple vendors:

- **Data encryption products:** Protects data on desktops, laptops, networked systems, mobile devices and storage devices
- **Data leakage products and support:** Provides the ability to monitor, manage and protect data regardless of where it resides, and restrict that information from being printed, emailed or copied
- **Mobile device protection:** Helps public agencies keep their mobile devices secure in the age of BYOD
- **Defense in-depth:** Network assessment that allows agencies to limit their exposure to cyber attacks and data loss, and increase productivity before viruses and other threats do any damage

NetApp

CDW•G

TO LEARN MORE ABOUT HOW a customized security solution employing the industry's best products can better serve the needs and interests of public agencies, visit **www.cdwg.com/netapp**

Sponsored Content

Symantec:
A layered defense is a good defense

With targeted cyber attacks up by 42 percent, public agencies, their networks and data remain more vulnerable than ever.

Today's network risks go far beyond viruses and malware. In addition to the growing concern about state- and activist-sponsored attacks and sabotage, public agencies must also guard against increasing security breaches and espionage, including those involving social media. Sophisticated intruders now use personal profile details found online to trick specific employees into unwittingly divulging government secrets or other sensitive information.

Public organizations must also brace for increased cloud attacks, mobile malware, website invasions — and the prospect of these advanced techniques trickling down to garden variety malware authors.

A keen awareness of the ever-evolving cyber threat landscape can help keep agencies a step ahead. In addition to studying regular reports issued by Symantec and other top security providers, public organizations can boost their defenses by adding multiple, overlapping layers of security, including:

- ✓ **SET STRONG POLICIES:** Create security programs with a framework to address national and other security compliance mandates, such as the Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley or the Federal Information Security Management Act (FISMA). Also establish internal policies focusing on technical controls and compliance that incorporate security best practices.
- ✓ **KEEP INTRUDERS OUT:** Rely on iron-clad, two-factor authentication software and Public Key Infrastructure (PKI) encryption to strengthen the network perimeter.
- ✓ **SAFEGUARD DATA FROM LEAVING THE NETWORK:** Employ data loss protection software to secure data, then add PKI encryption to protect that information in transit, whether online or within removable storage. Keep data backup and recovery systems up to date.
- ✓ **CLOSE VULNERABILITIES:** Use systems management technologies and software to deploy security patches as soon as available.
- ✓ **STRENGTHEN NETWORK ARMOR:** Support antivirus software and firewalls by adding protection for browsers, email and insider threats. Add application controls to prevent download of malicious content. Include end-point protection to guard against unpatched vulnerabilities, social engineering and malware.

For the greatest success, it's also crucial to engrain a culture of security within your organization that goes far beyond a once-a-year training session or seminar.

To learn more, download the Symantec Internet Security Threat Report to hear what the experts at Symantec identify as top emerging trends within the dynamic threat landscape — and what to do about them.

Symantec™

For more information, visit www.symantec.com/security_response/publications/threatreport.jsp

New Insights for Cyber Defense
Using Big Data Analytics

SAM HARRIS
Sam Harris is the Director of Enterprise Risk Management and Cyber Security Solutions for Teradata, He is an expert on information security systems and has worked with public sector business and government decision-makers on critical issues such as security, trust, privacy and compliance.

Follow Sam on Twitter:
@samuellharris and
linkedin.com/in/samharris/

As the sophistication and the variety of cyber-attacks continue to increase and evolve, from amateur hackers on one end to state-sponsored attacks trying to destroy systems on the other end, security professionals are more challenged than ever. Coupled with an exponentially increasing volume of data, this situation is making it virtually impossible for organizations to be able to identify and remediate threats in a timely fashion using traditional security tools and approaches.

Big data analytics are new tools in the arsenal for cyber warriors that answer the who, what, when, where, how and why of network traffic to respond faster and minimize the impact of an attack.

Today it's not a question if hacking will happen, it's what you do when you get hacked. Big data analytics provides the means for deep packet inspection on the netflow to uncover unfamiliar patterns and anomalies. This allows security professionals to jump on potential threats. The challenge is to detect and remediate the threat faster, before the activity results in a breach. When big data analytics are in the cyber warrior's arsenal you have a complete detailed view enabling immediate insight into network patterns and trends.

Teradata appliances and applications scale in a linear fashion, ensuring the performance necessary to ingest all of the data and make it available for immediate query response.

Additionally, Teradata offers the only truly integrated, unified architecture for capture, integration and analysis of both traditional and multi-structure data types, enabling queries of both in near real-time to shorten time to remediation.

Teradata's Discovery Platform provides out-of-the-box MapReduce functions using SQL syntax, making Hadoop available to a broader set of users. Users can issue singular queries that operate against all data types in one pass at the speed of thought. This unique functionality from Teradata allows a level of situational awareness never before possible for network security.

"Big data analysis in cyber security helps us focus on what's important and do that very quickly. What we've found is that a lot of organizations with even 10 or 20 seconds of advance warning can do a very good job of preventing or quickly containing the attack."

— Dr. Larry Ponemon, Founder, Ponemon Institute

Get the big data study here!
http://www.teradata.com/cybersecurity-threat/

TERADATA®

THE BEST DECISION POSSIBLE™

SPONSORS

CenturyLink Government

WindTalker

DELL Software

at&t

CISCO

NIC the people behind eGovernment

NetApp

CDW-G

GENERAL DYNAMICS

Symantec

TERADATA THE BEST DECISION POSSIBLE

ACKNOWLEDGEMENTS

JOHN MIRI, EDITOR-IN-CHIEF, CENTER FOR DIGITAL GOVERNMENT

After a successful career as a private sector software executive, Miri was appointed by the Texas Governor to the top regulatory board overseeing statewide electronic government. He went on to lead transformational projects for two successive Texas State Chief Technology Officers and has become an advisor and close confidant to leading state and local government CIOs around the nation. As the former Director of E-Government and Web Services for the State of Texas, Miri led the state to breakthrough results of 829 online services, 83 million citizen financial transactions, and $5 billion in online revenue. He helped found three web-based technology companies that leveraged Web 2.0 and cloud computing to achieve dramatic results for clients in the commercial markets. Miri has been a passionate advocate of next generation Internet technologies for more than a decade and is a nationally recognized speaker and author on government technology.

CENTER FOR DIGITAL GOVERNMENT

The Center for Digital Government, a division of e.Republic, is a national research and advisory institute on information technology policies and best practices in state and local government. Through its diverse and dynamic programs and services, the Center provides public and private sector leaders with decision support, knowledge and opportunities to help them effectively incorporate new technologies in the 21st century.
www.centerdigitalgov.com

public cio

Public CIO, a division of e.Republic, is an award-winning platform dedicated to technology thought leadership in federal, state and local government. Through print, online and a portfolio of events, Public CIO provides CIOs and key enterprise leaders with career critical insights on leading and navigating the innovative trends creating efficiencies, driving collaboration and impacting government services.
www.public-cio.com