Massachusetts new CCSMM participant

The Commonwealth of Massachusetts has chosen to participate in the Community Cyber Security Maturity Model, announced the Center for Infrastructure Assurance and Security Director Gregory White, Ph.D. Selected by the Department of Homeland Security after a rigorous self-nominating process, Massachusetts joins California, Delaware, Texas, Illinois, Nevada and North Carolina as the seventh state in the Center’s national program to strengthen cyber defense.

Associate Director Larry Thompson said that the call for submissions went to 41 states and territories, with more than 30 showing interest in committing to the process.

“It’s an extremely thorough, exhaustive analysis of a state’s readiness to adopt the model. The enthusiasm from Massachusetts leadership really put them over the top,” said Thompson.

The Center for Infrastructure Assurance and Security (CIAS) of the University of Texas at San Antonio is the world’s foremost center for multidisciplinary education and development of operational capabilities for infrastructure assurance and security. CIAS was established in 2001, developing and delivering cyber security training, exercise programs, and competitions for the past decade. It is a nationally recognized leader in the advancement of state and community cyber security capabilities and collaboration. (cont’d page 4)

CIAS & City of San Antonio: October Cyber Security Campaign

The City of San Antonio and the UTSA Center for Infrastructure Assurance and Security join forces again this October in marking the 9th Annual National Cybersecurity Awareness Month. A three-pronged, month-long campaign to strengthen San Antonio cybersecurity defenses will focus on community leadership, an informed citizenry, and workforce development. Briefings to promote awareness of the threat and appropriate responses will take place throughout the city in each district. CIAS, home of the National Collegiate Cyber Defense Competition, also will conduct a more raucous “Panoply” competition for up-and-coming collegiate cyber warriors.

San Antonio officials are at the forefront of developing a strong community cyber security incident response, said Center Director Dr. Greg White. “We have worked with the city for more than a year developing a new protocol for its emergency response plan concerning cyber disruption.” (cont’d page 4)
6 Top Risks to Print, Imaging Systems

Cyber may rule, but let’s not forget the paper along with the plastic

In a new Information Security Media Group/HP 2012 Print Security Survey, 86% of polled agencies say print/imaging security is either important or very important to their organization. Yet 35% of these same agencies do not even know whether they have suffered any breaches involving printers or imaging devices in the past year.

Here’s HP’s list of the top six risks:

#1—Printed hard copies
One of the most common printing security risks involves printed hard copies where an employee will request a print job and delay or forget to pick it up. A document containing sensitive or confidential information that sits idly in the paper tray or elsewhere for any length of time is a security risk.

#2—Data on printer hard disks
Unknown by many, today’s modern printers and MFPs contain hard disks similar to servers or personal computers. Printer hard disks store material such as passwords, routing information, address books, identification data, and confidential information as well as thousands of print jobs that can be stored for years. Increasing the risk, printers can be removed to an offsite location for repair, resale, or demolition—with the hard disk intact and data exposed to the device’s NEW OWNER.

#3—Print jobs sent over the network
Print jobs are usually sent from a computer to the printer via the network. Layered security ensures the network is secured with firewalls and other security software to protect communications between servers and endpoint computers. But what about the data communications between a computer and a printer? Many organizations do not apply encryption to print jobs, making it easy to snag a print job as it travels over the network to a printer.

#4—Controls and access to printers
Today there is no such thing as a “dumb” printer ... Today’s imaging and printing devices are incredibly sophisticated with intelligence, memory, and operating power on a par with a computer. Yet access to the printers and their control settings is rarely restricted. In most offices, employees and even outside contractors are free to walk right up to an MFP and print, fax, email, or copy any document they choose.

#5—Tampering and fraud
Printing systems are at risk from the tampering and fraud of insiders. In-office printing systems are often used for special print jobs such as check printing, prescriptions, patient wristbands, and other special-purpose activities. An unprotected printer makes it too easy for an insider to commit a fraudulent act. An employee with a grudge and access to special paper and media can print forged checks, write new prescriptions, or alter them with new names, quantities, or dosages. They can make changes to other sensitive documents right on one of the official internal printers.

#6—Fleets of printers, networks, and users elevate risk
In the real world of a government agency, there isn’t just a handful of individual printers, but a fleet of hundreds and even thousands of printers, MFPs, servers, computers, scanners and fax machines that comprise the organization-wide printing system. The risks are compounded many times over if printer security and management is not applied. A large fleet is best controlled and managed centrally, but many organizations have not implemented this model.

6 Top Risks to Print, Imaging Systems

Cyber may rule, but let’s not forget the paper along with the plastic

In a new Information Security Media Group/HP 2012 Print Security Survey, 86% of polled agencies say print/imaging security is either important or very important to their organization. Yet 35% of these same agencies do not even know whether they have suffered any breaches involving printers or imaging devices in the past year.

Here’s HP’s list of the top six risks:

#1—Printed hard copies
One of the most common printing security risks involves printed hard copies where an employee will request a print job and delay or forget to pick it up. A document containing sensitive or confidential information that sits idly in the paper tray or elsewhere for any length of time is a security risk.

#2—Data on printer hard disks
Unknown by many, today’s modern printers and MFPs contain hard disks similar to servers or personal computers. Printer hard disks store material such as passwords, routing information, address books, identification data, and confidential information as well as thousands of print jobs that can be stored for years. Increasing the risk, printers can be removed to an offsite location for repair, resale, or demolition—with the hard disk intact and data exposed to the device’s NEW OWNER.

#3—Print jobs sent over the network
Print jobs are usually sent from a computer to the printer via the network. Layered security ensures the network is secured with firewalls and other security software to protect communications between servers and endpoint computers. But what about the data communications between a computer and a printer? Many organizations do not apply encryption to print jobs, making it easy to snag a print job as it travels over the network to a printer.

#4—Controls and access to printers
Today there is no such thing as a “dumb” printer ... Today’s imaging and printing devices are incredibly sophisticated with intelligence, memory, and operating power on a par with a computer. Yet access to the printers and their control settings is rarely restricted. In most offices, employees and even outside contractors are free to walk right up to an MFP and print, fax, email, or copy any document they choose.

#5—Tampering and fraud
Printing systems are at risk from the tampering and fraud of insiders. In-office printing systems are often used for special print jobs such as check printing, prescriptions, patient wristbands, and other special-purpose activities. An unprotected printer makes it too easy for an insider to commit a fraudulent act. An employee with a grudge and access to special paper and media can print forged checks, write new prescriptions, or alter them with new names, quantities, or dosages. They can make changes to other sensitive documents right on one of the official internal printers.

#6—Fleets of printers, networks, and users elevate risk
In the real world of a government agency, there isn’t just a handful of individual printers, but a fleet of hundreds and even thousands of printers, MFPs, servers, computers, scanners and fax machines that comprise the organization-wide printing system. The risks are compounded many times over if printer security and management is not applied. A large fleet is best controlled and managed centrally, but many organizations have not implemented this model.
Verizon 2012 Data Breach Investigations Report


Access the complete report here.

Who is behind data breaches?

- 98% stemmed from external agents (+6% change)
- 4% implicated internal employees (-13%)
- <1% committed by business partners (<>)
- 58% of all data theft tied to activist groups

No big surprise here; outsiders are still dominating the scene of corporate data theft. Organized criminals were up to their typical misdeeds and were behind the majority of breaches in 2011. Activist groups created their fair share of misery and mayhem last year as well—and they stole more data than any other group. Their entrance onto the stage also served to change the landscape somewhat with regard to the motivations behind breaches. While good old-fashioned greed and avarice were still the prime movers, ideological dissent and schadenfreude took a more prominent role across the caseload.

As one might expect with such a rise in external attackers, the proportion of insider incidents declined yet again this year to a comparatively scant 4%.

How do breaches occur?

- 81% utilized some form of hacking (+31%)
- 69% incorporated malware (+20%)
- 10% involved physical attacks (-19%)
- 7% employed social tactics (-4%)
- 5% resulted from privilege misuse (-12%)

Incidents involving hacking and malware were both up considerably last year, with hacking linked to almost all compromised records. This makes sense, as these threat actions remain the favored tools of external agents, who, as described above, were behind most breaches. Many attacks continue to thwart or circumvent authentication by combining stolen or guessed credentials (to gain access) with backdoors (to retain access). Fewer ATM and gas pump skimming cases this year served to lower the ratio of physical attacks in this report.

Given the drop in internal agents, the misuse category had no choice but to go down as well. Social tactics fell a little, but were responsible for a large amount of data loss.

TIP FROM THE SANS INSTITUTE—**dial your combo lock!**

"Change the combination on opened laptop locks. When people have cables with combination locks for securing their laptops at their workstation, they always remember to turn the tumblers *when they secure the laptop*. But what happens when they unsecure the laptop? Many people won’t turn the tumblers on the opened lock because it is much easier to lock the laptop later if the combination is already set. About half a dozen laptops in our office disappeared one day. The laptops were stolen by someone who came by when the laptops were not there and noted the combination. The thieves came back later when the laptops were there and used the combination they had noted earlier."
Massachusetts joins CCSMM Program, cont’d

The Community Cyber Security Maturity Model (CCSMM), developed by CIAS Director Gregory White, Ph.D., is the first comprehensive state and local cyber defense program. It combines workshops, training and tabletop exercises to generate awareness of cyber threats and an ongoing community commitment to security. The process reflects the distinctions of individual communities, tailoring the program to their unique qualities and the vulnerabilities to which they must be most vigilant.

“From the onset, it’s critical for the program to be customized for that area’s community,” said Dr. White. “Not only at the state level, but by drilling down into each locality to best understand its vulnerabilities, they can be addressed more fully. Reno and Las Vegas, for instance, share many similarities on one level, but viewed through the prism of infrastructure security, they each present a very different topography.”

Initial planning sessions with the local point of contact, Jeff Tedesco of the Massachusetts Emergency Management Agency, will begin in September. Michael Fuller, CIAS Senior Information Security Project Lead and Ann Nurre, CIAS Senior Information Security Technical Lead, will be the team leaders for Massachusetts.

Fuller’s background includes business continuity, disaster recovery and incident response as well as business operations, development of service offerings and strategic accounts support. Nurre’s experience is in areas of risk assessment and abatement, IT Operations and web administration for profit and non-profit organizations. Combined, the team holds certifications as Project Management Professional, Certified Novell Engineer, Microsoft Certified Professional, Security+, Information Systems Security Professional, Certified Secure Software Lifecycle Professional, Certified Ethical Hacker and in the Governance of Enterprise IT.

San Antonio and CIAS: Partners in Cyber Security, cont’d

“It will be officially endorsed by Mayor Julián Castro at a public event on October 2nd. Following the mayor’s remarks, community leaders will participate in an Executive Tabletop Exercise incorporating the new Cyber Incident Response Plan,” concluded Dr. White. Participants will be encouraged to collaborate on individual response plans to have an impact on their own organizations.

Following this leadership-focused event, CIAS will kick off the Community Preparedness and Awareness campaign and offer briefings to the public throughout the month of October to make citizens more aware of cyber security topics. The briefings will be for business owners, end-users, public workers and other interested citizens, in neighborhoods throughout the length and breadth of the city.

For Workforce Development, CIAS is hosting training courses for IT professionals and seekers from a variety of backgrounds, from those with little experience to veterans seeking industry certifications. “In particular, we’d like to help get the word out to military personnel who are looking for opportunities in private industry,” said Dr. White. “They have training and discipline that only needs to be provided direction for the emerging industries.” Courses include Voice & Data Security, and preparation for certifications in Information Security Systems Professional (CISSP) and Security+.