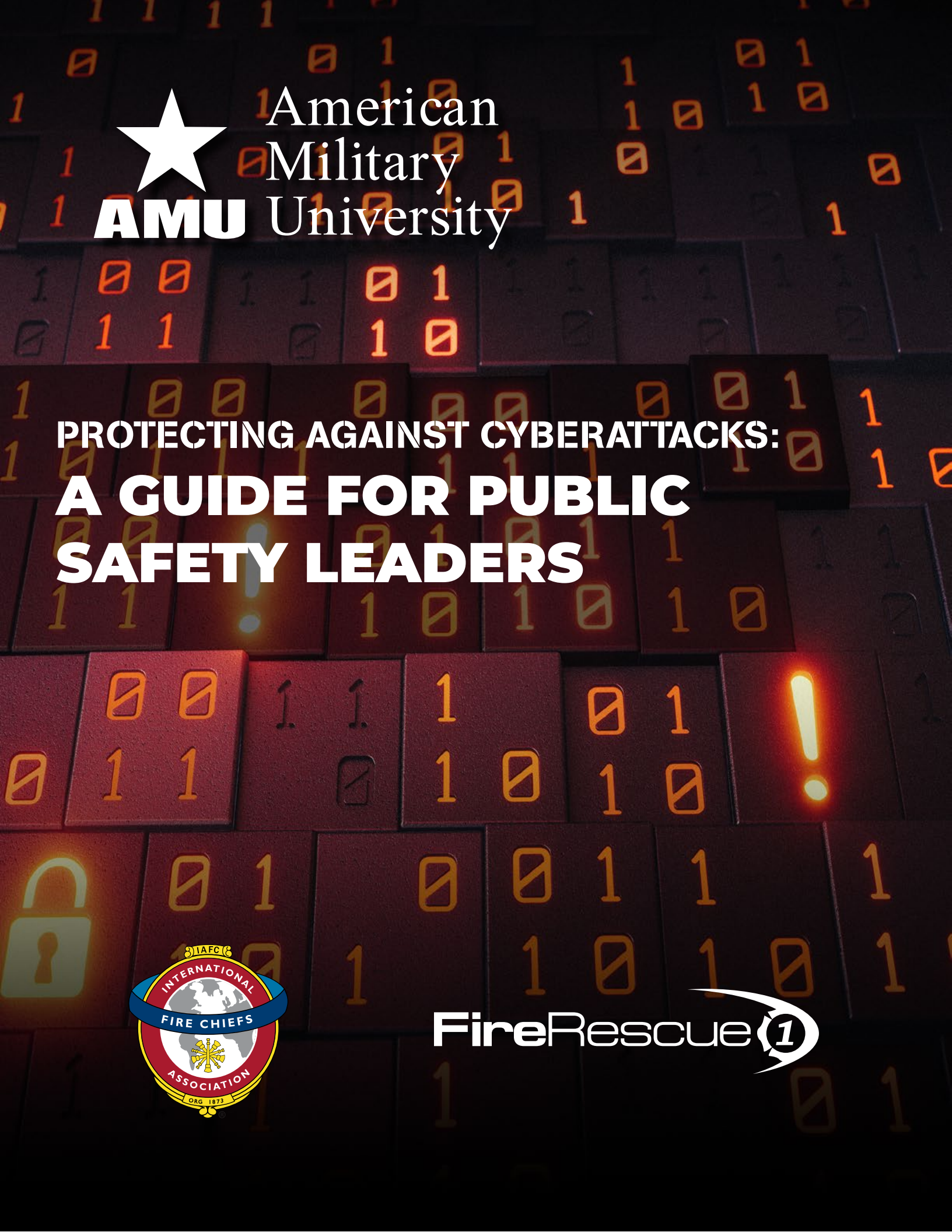


American Military University

PROTECTING AGAINST CYBERATTACKS:

A GUIDE FOR PUBLIC SAFETY LEADERS

IAFC International Fire Chiefs Association

FireRescue1

A NOTE FROM THE CHIEF

One of the most prevalent changes in today's fire service is the advent of technology, which quite literally has infiltrated every aspect of our professional lives.

Technology is keeping firefighters safer and better protected. For example, self-contained breathing apparatus (SCBA) not only weigh much less today than in the past, but also include technology such as thermal imaging cameras (TICs) and personal alert safety system (PASS) devices integrated directly into the packs.

Firefighters have access to advanced technologies to improve firefighting capabilities, such as compressed air foam systems (CAFS) and positive pressure ventilation (PPV) fans. Fire trucks are equipped with mobile data computer (MDC) software, portable radios that are actually mini-computers, and have direct access to the data and information within computer-aided dispatch (CAD) systems.

However, as the digital world continues to proliferate into our professional infrastructure, so does risk. Cyberattacks can cripple these technological systems and jeopardize our ability to protect lives and property.

As a result, fire leaders have a new task. Cybersecurity has become our collective responsibility, not just the responsibility of our IT department. This publication intends to enlighten fire leaders about issues related to cybersecurity, including identifying threats to departments and strategies to protect networks.

Fortunately, fire leaders don't have to know all the terminology, understand the details of how systems work, or know how to best protect those systems. Instead, leaders need to know how to ask the right questions. Included in this publication are questions to ask your IT professionals, tips for building a stronger working relationship with them, training strategies, and much more.

Do not wait until it's too late to learn about cybersecurity. Do not learn the lessons the hard and costly way. Just as fire leaders have embraced technology to improve safety and operations, let's tackle cybersecurity with that same passion and be instrumental in continuing to protect our departments.

Be safe,

Sam Greif
Fire Chief of Plano, Texas
Member, IAFC's Terrorism and Homeland Security Committee

TABLE OF CONTENTS

SECTION 1: VULNERABILITY TO CYBERATTACKS

SECTION 2: PROTECTING AN AGENCY FROM CYBERATTACKS

ABOUT THE PUBLICATION

American Military University produces high-quality, thought-provoking publications that address important issues for professionals who work in the fire service, law enforcement, corrections, emergency response, and public health. To access our library of publications, please visit InPublicSafety.com/library.

This magazine was designed in collaboration with FireRescue1 and the International Association of Fire Chiefs (IAFC). IAFC represents the leadership of firefighters and emergency responders worldwide. IAFC members are the world's leading experts in firefighting, emergency medical services, terrorism response, hazardous response, natural disasters, search and rescue, and public safety legislation. Since 1873, the IAFC has provided a forum for its members to exchange ideas, develop professionally and uncover the latest products and services available to first responders."

A special thanks to the contributors who lent their experience and expertise to create this magazine as well as IAFC's Terrorism and Homeland Security Committee members for their input.

For questions, comments, submission guidelines, or requests for print copies of this publication, email IPSauthor@apus.edu.

Executive Editor: Leischen Kranick
Assistant Editor: Jinnie Chua

Agencies Under Cyberattack:

Staying Ahead of the Hackers

Government agencies are conducting more and more services online, but they are struggling to stay ahead of hackers trying to steal valuable personal information.

By Dr. Harry Cooper, Faculty Member, Cybersecurity and Information Technology, American Military University

The launch of personal computers (PCs) has significantly changed our world during the past three decades. Computers, once restricted to use by corporations or government agencies, became accessible for use in the home.

This expansion and availability of PCs spurred the 1993 National Partnership for Reinventing Government (NPR), which was launched during the Clinton administration to review and reform how the government delivered services in the 21st century. It is through the NPR that government agencies redesigned their processes, enabling basic tasks—such as electronic benefits transfer, access to government information, creation of a national law enforcement network, and filing taxes—to go from lengthy in-person processes to simpler online processes.

From these humble beginnings, government services at all levels have drastically evolved. Today, almost all services handled by government can be accessed and completed online.

While this level of access is a great step toward bringing the government closer to its constituents, it is not without significant flaws. These flaws include government employees failing to adhere to policies and procedures or not receiving proper training, both of which can lead to compromised network systems. There is also a lack of proper funding for technology, security upgrades, and initiatives to protect systems, resulting in potentially large breaches of improperly secured information.

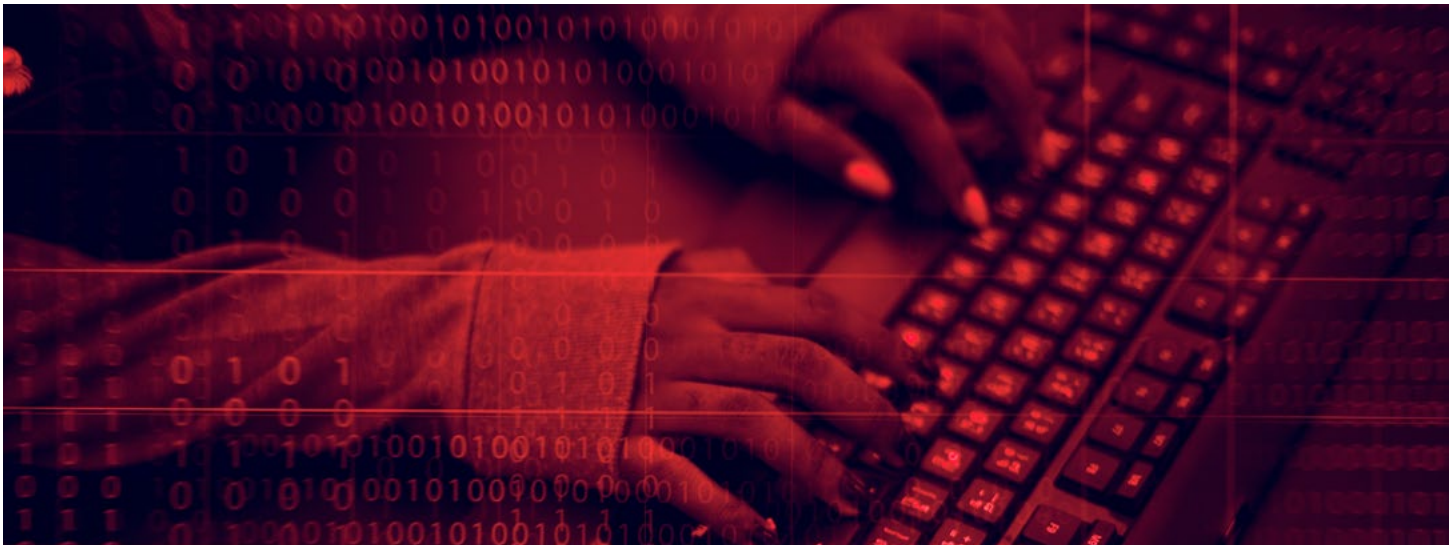
Government Failing to Keep Up with Technology

One of the earliest "hacks" against government took place in 1983 against the Los Alamos National Laboratory by a hacker group called "The 414s." The 414s were six teenagers who became some of the first "famous" hackers. Part of their fame has been attributed to the same-year release of WarGames, a film about a teenager nearly launching World War III by unknowingly hacking into North American Aerospace Defense Command (NORAD).

Unfortunately, the government was forced to play catch-up, as there was no federal law in place to prosecute such computer crimes. It was not until 1986 that the Computer Fraud and Abuse Act was passed. Legislation continues to struggle to keep up with technology. While numerous amendments have been made to the Computer Fraud and Abuse Act over the past 30 years, it has not been enough to deter hackers, hacktivists, phishers, scammers, nation-states, and many others from committing acts of cybercrime. ■

About the Author

Dr. Harry Cooper is an instructor in the STEM school at American Military University, focusing on cybersecurity and information technology with experience in both academics and as a practitioner. Dr. Cooper has taught at various colleges and universities on a wide range of technology topics. Before entering academia, Dr. Cooper served as CEO/partner for Thimbleweed Consulting and TWC Security. Dr. Cooper received his D.Sc. in Cybersecurity from Capitol Technology University, where his research focused on the Mosaic Theory of Intelligence, its role in today's society, and how it has become available to most average users. He also completed his M.S. in cybersecurity, intelligence, and forensics at Utica College and his B.A. in political science at the University of Pittsburgh.



TERMINOLOGY TO KNOW

Attack
An attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity.

Authentication
The process or action of verifying the identity of a user or process.

Bot
A computer connected to the internet that has been surreptitiously or secretly compromised with malicious logic to perform activities under the command and control of a remote administrator.

Encryption
The transformation of data to hide its information content.

Encryption key
A random string of bits created explicitly for scrambling and unscrambling data. Encryption keys are designed with algorithms intended to ensure that every key is unpredictable and unique.

Firewall
Hardware or software designed to prevent unauthorized access to a computer or network from another computer or network.

Hacker
Someone who violates computer security for malicious reasons, kudos, or personal gain.

Malware
Software intended to infiltrate and damage or disable computers; shortened form of malicious software.

Pharming
A cyberattack intended to redirect a website's traffic to another, fake site.

Phishing
Method used by criminals to try to obtain financial or other confidential information (including usernames and passwords) from internet users, usually by sending an email that looks as though it has been sent by a legitimate organization (e.g., a bank). The email usually contains a link to a fake website that looks authentic.

Ransomware
Malware that is a form of extortion. It works by encrypting a victim's hard drive, denying his or her access to key files. The victim must then pay a ransom to decrypt the files and gain access to them again.

Spyware
Malware that passes information about a computer user's activities to an external party.

Trojan
A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program.

Virus
Malware that is loaded onto a computer and then run without the user's knowledge or knowledge of its full effects.

Worm
Malware that replicates itself so it can spread to infiltrate other computers.

Ransomware and Other Cyberattacks: How Criminals Are Targeting Personal Information

Information breaches are often caused by personnel who unintentionally allow hackers to access private networks. Here are the methods hackers are using to mislead employees and steal sensitive data.

By Dr. Harry Cooper, Faculty Member, Cybersecurity and Information Technology, American Military University

There has been a significant and steady surge in online criminal activities. For the past decade, Verizon Enterprise Solutions has released a yearly Data Breach Investigations Report (DBIR) that tracks data breaches across all sectors. We can use these reports, along with examples of recent cyberattacks against organizations in the public sector, to better understand how cybercriminals are targeting governmental bodies, and what can be done to identify and protect against threats.

Hackers Want More than Credit Card Information

In 2008, hackers primarily focused on stealing payment card data. Verizon's DBIR reported that in 84 percent of breaches, credit cards

were the top item of interest to hackers. This is because it was very easy at the time to monetize credit cards with little risk of exposure to the perpetrator. Credit card theft was especially lucrative for organized crime groups who orchestrated an estimated 50 percent of all credit card breaches.

But organized crime groups are no longer just after credit card data; they are after personally identifiable information or PII. This critical information often lives within government agency databases, so public-sector entities are a highly desirable target. Their networked systems hold valuable PII collected from tax submissions, financial benefits, healthcare information, and more.

The 2018 DBIR showed that of the 304 confirmed data disclosure cases that it reviewed from the public sector, 55 percent had been targeted for PII. Another 24 percent of cases were targeted for "secrets" that are believed to also contain PII.

Role of Personnel in Security Breaches

The DBIR determined that personnel are one of the leading causes of information breaches. In the majority of these cases, personnel are "unwitting participants." An unwitting participant is an individual who works for an organization and carries out actions that, while seemingly legitimate or benign, actually enables a perpetrator to gain access to the organization's systems and data.

Phishing Attacks

Perpetrators use many different types of malicious tools to target personnel and carry out their attacks. Phishing, for example, is the act of getting someone to give up their credentials via an email solicitation. Phishing attacks were used in roughly 74 percent of the breaches reviewed in the DBIR. Phishing can be very convincing and presented in a way that looks completely legitimate. For example, phishing can appear to be real emails sent from human resources asking personnel to update their beneficiaries on their retirement plan or to submit their vacation schedule. The goal of a phishing attack is to get personnel to provide sensitive personal information without questioning the request.

Malicious Files

Another common tool used by perpetrators is malicious files. Malicious files come in many shapes and forms, but the underlying goal is to get personnel to open a seemingly legitimate file often attached to an email. Unfortunately, the malicious file contains more than what is expected; it includes exploits that will infect the user's computer and install a backdoor malware that gives the perpetrator complete access to the user's computer, as well as the organization's network. Once a perpetrator has gained access to a network through a foothold in a single machine, they work to gain access to and compromise other machines, servers, routers, and any other networked device.

What Happens After a Breach

After accessing a network, the perpetrator must decide what their end goal is for the attack. They may choose not to take any noticeable action in any of the machines they have gained access to and instead passively monitor information flowing throughout the network. This strategy allows them to spend time evaluating information to determine what is critical and valuable and then silently collect, package, and exfiltrate data on a schedule that matches periods of increased network traffic in order to elude detection from the organization's IT department. This type of an attack is called an Advanced Persistent Threat (APT). Because of the low-key manner in which the malicious code acts,

APTs are capable of running for very long periods of time, from weeks and months to even possibly years.

The other strategy a perpetrator might employ after a breach is to immediately strike. There are many ways for a perpetrator to harm an organization in extremely destructive ways, such as wiping hard drives or blowing up industrial systems. Less destructive and more common actions include the use of malware and ransomware, which was used in 45 percent of attacks.

Ransomware

Ransomware is a malicious attack against an organization's data where the malicious program surveys the contents of a machine's hard drive along with any network-attached or network-accessible drives. It then encrypts all the data using high-grade encryption methods and algorithms. Once the data has been encrypted, the underlying encryption key is sent to a server controlled by the perpetrator and a message notifies the user of the encryption and demands a ransom payment for access to the encryption key.

When this happens, organizational leaders must decide whether to pay the perpetrator for the encryption key or lose all the locked information. For organizations that have exceptionally strong IT departments with up-to-date backups of critical systems and data, the decision will be not to pay the ransom and instead to rebuild the affected machines.

Unfortunately, many organizations do not have such robust IT departments, so they are often forced to pay the ransom. Once the payment is received, the perpetrator will either release the encryption key or they may simply ignore the victim. It is estimated that only about 20 percent of organizations that pay actually get their files back unharmed. Many ransomware variants have bugs in the code that corrupt the encrypted files, making them impossible to be restored regardless of whether the organization has the key or not.

Citizens want their government to be more accessible, but this comes at a price that many would not have anticipated when e-government systems were first developed. There is no perfect solution when it comes to data security, and security measures are often guided by risk assessments and limited budgets. Therefore, it is important for government agencies to do everything they can to lessen vulnerabilities and deter perpetrators from taking advantage of security flaws. ■

About the Author

Dr. Harry Cooper is an instructor in the STEM school at American Military University, focusing on cybersecurity and information technology with experience in both academics and as a practitioner. Dr. Cooper has taught at various colleges and universities on a wide range of technology topics. Before entering academia, Dr. Cooper served as CEO/partner for Thimbleweed Consulting and TWC Security. Dr. Cooper received his D.Sc. in Cybersecurity from Capitol Technology University, where his research focused on the Mosaic Theory of Intelligence, its role in today's society, and how it has become available to most average users. He also completed his M.S. in cybersecurity, intelligence, and forensics at Utica College and his B.A. in political science at the University of Pittsburgh.

AGENCIES STRUCK BY RANSOMWARE

Numerous governmental bodies have fallen victim in the past few years to costly ransomware attacks. These attacks aren't just affecting organizations' digital assets; they are also harming their physical systems.

November 2016

San Francisco, California

San Francisco Municipal Transportation Agency hit by massive ransomware attack that shutdown its ticketing and management systems for railways and buses. Agency unable to accept fares and forced to allow passengers to ride for free for at least 2 days.

COST: Attackers demanded $73,000 to restore data.

March 2018

Baltimore, Maryland

City's CAD system that supports 9-1-1 and emergency calls hacked, forcing officials to resort to manual operations to handle calls.

COST: Undisclosed.

September 2018

Port of San Diego, California

Ransomware compromises port's information technology systems, disrupting administrative operations at the shipping hub.

COST: Undisclosed amount of bitcoin demanded.

March 2018

Atlanta, Georgia

Municipal systems attacked causing widespread outages and halted many city services.

COST: Attackers demanded $50,000 in digital currency, but recovery costs are estimated to be much higher.

February 2018

Leeds, Alabama

Hit by a ransomware attack that locked all city computers and data, including fire and police departments.

COST: Reportedly paid $8,000 in bitcoin.

Technology is Changing Healthcare, But Not Without Risk

Like any device connected to a network, advanced medical devices are vulnerable to cyberattacks. They must be protected to ensure patient care and the security of entire systems are not compromised.

By Dr. Kevin Harris, Program Director, Cybersecurity, Information Systems Security and Information Technology Management, American Military University

Modern-day healthcare is being revolutionized by technological innovations in Internet of Things (IoT) devices including wearable, portable, and implantable devices. These devices have been essential to improving patient care.

For example, patients who need constant monitoring of vital signs can be outfitted with a wearable device that measures temperature, blood pressure, and heart rate. Patients can return home while medical personnel remotely monitor data received from the wearable devices. Medical professionals can then analyze data trends and notify a patient if it's determined they need to seek further treatment.

Similarly, implantable devices allow for medical treatment to be administered without direct medical staff intervention, often in life-threatening situations. One such device is an implantable defibrillator that not only detects and reports when a patient's heartbeat is irregular, but also initiates an electric shock to restore the heart's rhythm. Other implantable devices include an insulin pump that delivers insulin based on registered levels and cochlear implants that provide the ability to hear for those who have hearing loss.

Vulnerability of IoT Devices to Cyberattack

While the benefits of IoT devices are many, these devices can be targeted by cyberattackers. If the devices and associated data are not properly protected, not only could sensitive medical information be exposed, but lives could potentially be at risk.

If an insulin pump is compromised, an attacker could alter data and cause the pump

to deliver a potentially lethal dose of insulin. If an individual's defibrillator is accessed, not only could the patient's life be in jeopardy, but others could also be harmed if that person is incapacitated while driving, for example.

Networked devices used by hospitals are also not immune from risk of cyberattack. For example, if an attacker were to gain access to an infant warmer, they could alter the temperature a few critical degrees, which could prove fatal.

There are also vulnerabilities in the growing trend of concierge healthcare, where medical professionals travel to the patient. While this can have many benefits, including improved and personalized medical care, there are also risks. For example, if medical providers use networked equipment in the field and receive updates to this equipment remotely, this could potentially open the door for an unauthorized party to gain access. An attacker could alter settings on the medical equipment, which could lead to incorrect diagnosis and treatment. All this could happen without the medical professional detecting the intrusion.

Regardless of whether a device is used by a medical provider or a patient, there is significant risk that an unauthorized party could access private data. Such a breach could have a devastating impact on the patient, cause strain on the relationship with their medical professional, and also require significant financial costs to rectify impeded or incorrect treatment.

Ways to Reduce Risk

To mitigate risks of cyberattack in healthcare, which has been identified as one of the critical infrastructure sectors by the Department of Homeland Security, a team approach is necessary. Software developers, manufacturers, medical facilities, regulatory bodies, users, academic institutions, and information technology professionals must all work together.

When it comes to using IoT devices, medical facilities must ensure their network infrastructure is secure. Equipment calibration verification policies and processes must be continuously reviewed and updated. Training should be provided to users and patients to ensure they're aware of the risks associated with using IoT devices. Similarly, manufacturers need to invest in security and devices must be developed with robust encryption protocols, redundancy, and potential attack-notification systems.

As with all technological advances, safety should not be overlooked for the sake of convenience and innovation. IoT certainly has the potential to revolutionize healthcare, but the proper steps need to be taken to ensure it is secure and protected. ■

About the Author

Dr. Kevin Harris has 25 years of experience in the information technology field. During this time, he protected various organizations' infrastructure and data in positions ranging from system analyst to chief information officer. His career encompasses diverse experiences both in information technology and academia. His research and passion are in the areas of cybersecurity, bridging the digital divide, and increasing diversity in the tech community. As an academic, he has served students at various types of institutions including community colleges, HBCU, public, private, graduate, undergraduate, as well as online. Dr. Harris has trained faculty from multiple institutions in the area of cybersecurity as part of an NSF multistate CSEC grant. He has delivered instruction in several disciplines, including business, computer science, and computer networking, with a particular interest in information security, cybersecurity, and computer forensics. Currently, Dr. Harris serves as program director for Cybersecurity, Information Systems Security and Information Technology Management at American Military University.

11 Questions to Ask Your IT Department to Protect Against Cyberattacks

Public safety leaders do not have to be experts in cybersecurity to ensure their agencies are adequately protected—they just have to know the right questions to ask.

By Sam Greif, Fire Chief of Plano, Texas

Fire chiefs have plenty to be concerned about while trying to protect the public and our personnel. Over the last several decades, new threats and challenges have emerged, including active shooter events, health epidemics, hazmat disasters, emergencies requiring technical rescues, and high-rise fires, to name a few.

One additional new threat that has devastating consequences and that many fire leaders are not adequately prepared for is cyberattacks. While many fire chiefs feel their IT departments should be more cognizant of cyber threats, many do not consider threats of cyberattack as part of their day-to-day operations.

It is understandable that there is a gap in grasping the complexities of cybersecurity. After all, terms such as authentication, declaration of conformity, DMZ, encryption, firewall, IDS, ISP, IPS, LAN, malware, proxy server, spyware, VPN, WAN, worm, and the rest of the IT alphabet soup are not part of the traditional fire service lexicon.

The good news is fire chiefs do not have to know the details of how to protect our departments and our personnel against cyberterrorists. However, we do need to know what questions to ask IT experts to ensure they fully understand all the vulnerable technology we use on a daily basis.

Systems that need to be protected include 9-1-1, public safety radios, CAD (computer-aided dispatch), electronic patient reporting, records management systems, mobile data computers, and phone PBX systems. These systems are all potential targets for those who wish to do harm to our departments and communities.

Leaders in the fire service need to make sure they are asking the right questions to the right people.

To find out what questions I should be asking, I went directly to my local IT department. I met with IT to learn how we could ensure the systems my department uses are protected as much as possible. Here are the questions all fire chiefs should ask:

Photo credit: Jeremiah Lancaster

11 Questions to Ask Your IT Department:

1 What is the configuration of our firewall?

The firewall should not allow any connections from the outside. All connections to computer-aided dispatch (CAD) and records management systems (RMS) should be made over a virtual private network (VPN).

2 Do our systems meet CIS benchmarks?

The Center for Internet Security (CIS) benchmarks aid in server setup. Requirements can be found here.

3 Do our critical networks have a firewall between the internal network and the protected networks?

Critical networks include SCADA, building safety, and CJIS. Critical networks include supervisory control and data acquisition (SCADA), building safety, and Criminal Justice Information System (CJIS). All traffic in and out of the protected networks should be monitored and recorded.

4 Have all default passwords been changed?

Many systems come with a default password or built-in account from the manufacturer or vendor. These passwords must be changed to lessen the chance they can be hacked.

5 Does the network have a central time server called a NTP?

A network time protocol (NTP) allows for the clocks on all equipment to stay in sync for logging and audit purposes. Also, some encryption technologies require this.

6 Do all critical systems send their log files to a central server?

Using a central server allows for logging and audit in case of a breach, and some systems send an alert when it detects a breach.

7 Are user permissions on systems set to the minimum necessary for them to do their job?

Granting permission greater than the minimum necessary can increase compromises and removes accountability within those systems. If access is limited, it will reduce the chance of changes—accidental or intentional—being made within the system. Limited access also reduces the chance of exfiltration of information from the network.

8 Is there an ongoing and updated inventory of assets?

This should include date of purchase and disposal, who owns the equipment (IT), and who owns the data on the equipment (PD, fire).

9 Does IT use tools to monitor servers for patches?

Many departments use tools like Nessus (free for up to 25 servers) or Qualys to monitor systems and send notifications when server patches are needed and available in order to keep them secure.

10 Does IT limit the number of administrator accounts on systems?

Administrators can expand their power by granting permission to accounts they do not normally have access to. Since administrators have the ability to delete entire systems and shut down access to all computers within the system, background checks should be in place for all administrators.

11 For departments storing HIPAA or CJIS data on its server, are those hard drives properly encrypted?

Encryption is critical to protecting personal data stored on servers. While encryption is required by HIPAA, it's smart to verify that IT has proper encryption protocol in place.

Most of the answers to these questions are still foreign to me, and I certainly would not know how to achieve getting them done. However, by having the conversation with my IT department and discussing all the technology involved, I feel more confident they are on track working hard to protect our systems. This dialogue also led to IT providing

According to the 2016 Deloitte-NASCIO Cybersecurity Study, state officials, including emergency managers and chiefs of police, are more confident in their states' ability to address cybersecurity (66 percent) than state chief information security officers are (27 percent). This confidence gap signals a need for increased communication about cybersecurity risk and methods to prevent and mitigate against potential harm.

me with tips for my personnel about how to help protect our systems against phishing, vishing (voice phishing), and pharming attacks—all of which are designed to steal information or cripple an organization's technology.

Until fire chiefs take an interest in cybersecurity and make time to have ongoing conversations with IT, they risk being vulnerable to cyberattacks. ■

About the Author

Chief Sam Greif began his career as a paramedic in 1982 and joined the Fort Worth (CO) Fire Department as a firefighter in 1985, where he worked his way up through the ranks to assistant chief of operations. In June 2015, after an extensive nationwide search, it was announced that Greif was selected as the new fire chief for the City of Plano, Texas.

Chief Greif holds an associate in applied science degree in fire science, a bachelor's degree in leadership from Midwestern State University, a master of public administration from the University of Texas at Arlington, and is a graduate of the National Fire Academy's Executive Fire Officer Program.

Chief Greif has served on numerous state and national boards and committees. He currently is the chair of the International CAD Consortium and was on the board of directors for Tarrant County 9-1-1 for eight years. He is a member of the IAFC's Terrorism and Homeland Security Committee, Metro Chiefs, and Collin County Fire Chiefs, and is an active member of the Plano Rotary Club.

Tips for Improving Communication with IT

It often seems like IT professionals speak their own language. To help bridge the communication gap, a chief information officer provides insight on how employees can work better with technology departments.

By Chris Chiancone, Chief Information Officer of Plano, Texas

Effective communication is often cited as one of the greatest challenges within any organization, but communication with an organization's technology department can be especially challenging.

During the 20-plus years of my working career—nearly half of which I've been either a deputy or chief information officer for large cities—I have spent a lot of time and energy trying to better understand what makes communication so poor between technology departments and others within an organization. My experience has shown that problems arise because people outside IT do not understand the personality traits of the average technologist, and they don't fully comprehend all the serious problems that IT staff are simultaneously trying to solve.

The Anatomy of a Technologist

True technologists are, in my opinion, one of the easiest groups of people I have ever had the opportunity to lead. Technologists who have embraced the mission and vision of the organization and understand its business problems work tirelessly researching issues, triaging problems, and leveraging workarounds to make sure that services are operating at the best levels possible. They do all these things to avoid three things: system failure, vulnerabilities and risk, and personal failure.

When a problem arises with an unknown solution, technologists often collaborate online, building micro-communities of fact-finding armies to sift through innuendo to find the truth. These technical professionals will keep posting, responding, and evaluating hundreds of posts until the answer to the issue becomes apparent. Once solutions are identified, they often report fixes to technology forums to help other technologists shorten their problem-solving process.

Typically, technologists all share some common traits:

1. They genuinely care and strive to find answers to common and complex business and technical issues.
2. As individuals, they are generally more introverted, non-confrontational, and have difficulty operating in foreign, non-technical social environments. Technologists sometimes have a hard time expressing challenges, especially if the challenge is beyond their control. Because of their personality, sometimes technologists will not challenge business requests in order to maintain harmony with the customer, even if it means that it creates additional work for the technology department or other domino-effect complications.
3. They generally have incredibly high intelligence levels, moderate emotional intelligence quotients (EIQ), and complex social skills.
4. They typically will find a way around bureaucracy, obstacles, and other perceived non-logical situations. Some outsiders interpret this behavior as being rogue, but it is the way technologists are wired. They do not have time to watch and wait, especially when a system has critical issues. They need to start troubleshooting and look for workarounds to restore service.
5. They recognize the need for paperwork, but they often do not like it. The more electronic reporting systems that are in place, the more adoption you will get from a technologist.
6. They don't have all the answers for every system at their fingertips, but the more experience they have, the faster they can generate action. Many times, systems are very complex to diagnose, especially when the hardware, software, and/or connectivity are not standardized or are heavily customized.
7. Intra-departmental technology communication is as tricky to foster as department-to-department communication. Highly evolved technology organizations make extensive use of technologies through their service desk software to make sure events revolving around an issue are both memorialized and shared with customers. These systems also help build transparency to problem resolution and allow for the department to be managed from metrics.

My experience has shown that problems arise because people outside IT do not understand the personality traits of the average technologist, and they don't fully comprehend all the serious problems that IT staff are simultaneously trying to solve.

8. Technologists work in a world of abbreviations, analogies, and theory; it is okay to ask them to explain issues and problems in an easy to understand manner or provide a real-life example.
9. Technology is both an art and science; answers are not typically tangible and are very difficult to diagnose.

If technologists are treated with respect and trusted to fix the issues within their control, you will have some of the most dedicated, hard-working staff members in modern-day organizations.

How to Work Better with Your Technology Department

Around five years ago, technology became the engine driving organizations rather than the caboose following behind to support it. Today, technology and its services are viewed as an essential tool of modern-day business operations.

The staff who were once holed up in the basement of many organizations are suddenly expected to be able to effectively communicate with stakeholders, participate in marketing meetings, interface with customers, and attend corporate events; all with the same charismatic entrance and gregariousness as traditional "business" talent. I have some breaking news: it is going to take a while for the communication skills within an IT department to catch up with these new and burgeoning expectations.

Technology departments deal with a multitude of issues and are always working to keep systems operational and technology as advanced as possible. One of the biggest challenges for IT departments is that it must not only support itself as a department, but also provide support to every other department. With this massive organizational responsibility comes frustration. While technologists are working diligently to come up with solutions, they can't solve all the problems all at once, leading to frustration. As a result, many people feel it is difficult to work with technology departments, but I believe there are a few things those outside IT can do to help improve communication and collaboration:

Understand the department is not only there for you. Many IT departments provide support for 10, 20, or even 50 other departments within an organization or municipality. To serve all these interests, technology departments are constantly prioritizing and weighing risk, and working on issues that impact the greatest number of people. If they cannot address your problem or question immediately, there is usually a good reason. However, due to their communication limitations or heavy workload, you may not always know when they will get to your problem. You may need to ask them for an ETA or escalate your issue to a manager.

Work on explaining your needs and not what you want. Technology departments are good at solutions, but poor at implementing systems they have no investment in or understanding about. IT personnel are best used when helping develop a solution that meets your needs, so work to tell them what the problem is and what you need from them without trying to insert what you think you want the system to do.

Troubleshooting is not easy and takes time. There are likely a multitude of factors contributing to your issues, many of which you are not aware of. Sometimes, it's essential to conduct a thorough evaluation of your system and business processes that feed the system. This can be a time-consuming and highly involved process. Just because a solution worked one time for an organization does not mean it will continue to work. Many systems are not configured correctly and are too heavily customized, which leads to failure.

It's okay to push the boundaries of technical possibilities. In our highly technological era, it's expected that many users believe anything is possible with enough time, money, and resources. However, those possibilities can often be overwhelming to IT staff who understand the technological requirements of implementing such ideas. You do not have to take an answer of "it can't be done" at face value. Technologists work within boundaries, but it's important for others to challenge both internal and technical staff to be innovative and bring solutions, not more challenges.

Have conversations about Service Level Agreements with your technology department. Service Level Agreements are negotiated, pre-arranged documents between the information technology department and their customer departments. These documents outline details such as expected response times based on the severity of issues, which can help IT managers better staff, plan, and prioritize support according to the expectations of departments.

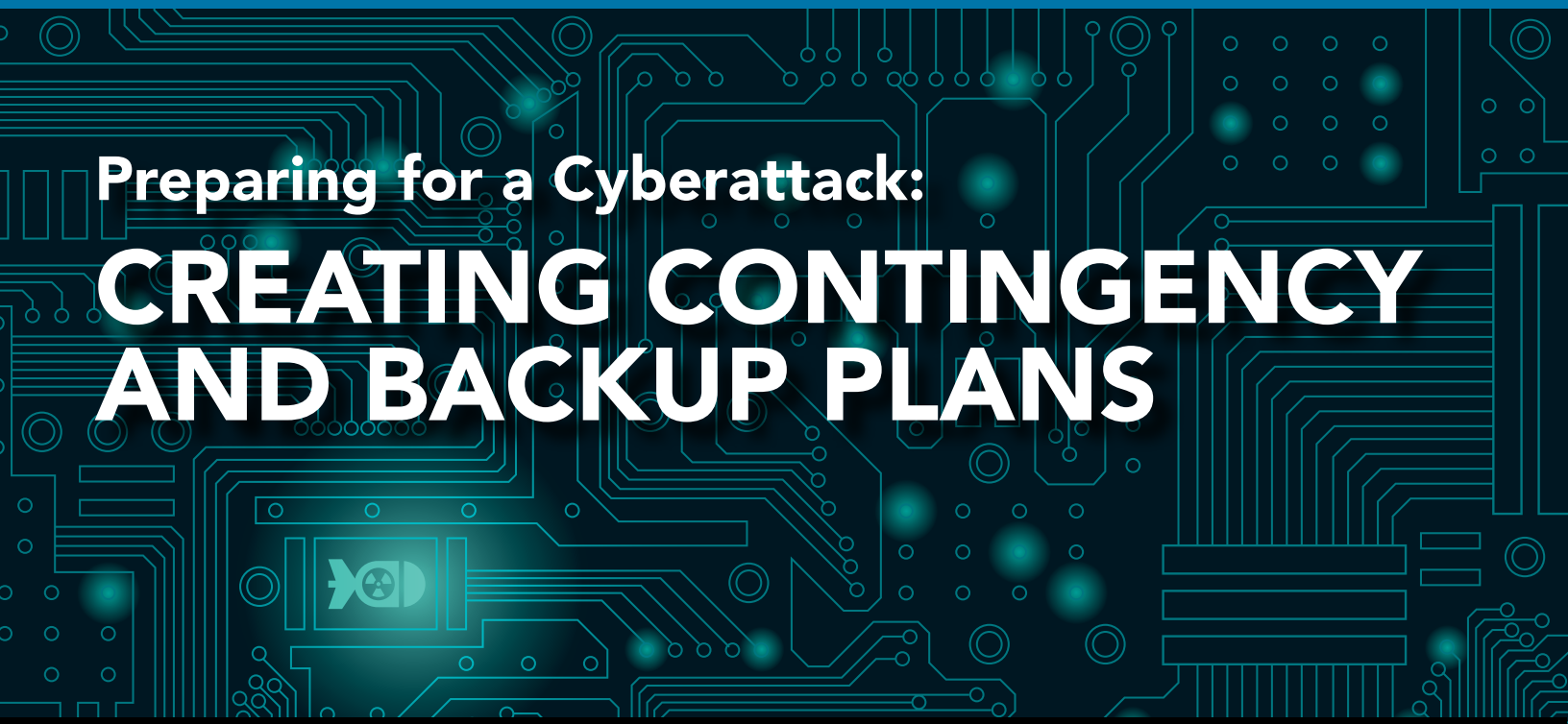
When new technology is introduced, require your staff to attend training and information sessions. IT departments regularly introduce new technology and, in order for it to operate properly and be effective, all staff need to know how to use it. In my experience, only about 35 percent of staff attend training, of which 25 percent need additional help. Out of the 65 percent who do not attend training, 70 percent end up requesting support, of which 90 percent of the type of support requested was covered in the training. Such requests dilute the IT service desks' ability to respond to legitimate needs, creates a backlog, and ends up slowing down other assistance that is duly needed. This problem could easily be solved if staff attended the provided training.

There is no doubt that technology will continue to evolve at breakneck speeds changing how organizations operate. Therefore, it is critical to have both constant and effective communication with technology staff. Once barriers, moats, and gorges have been crossed and staff begins to develop a dialog, personnel in all departments can truly work together to improve the operation of the organization. ■

About the Author

Chris Chiancone is a strategic thought leader with more than 20 years of experience delivering advanced hardware and software solutions for private corporations and public-sector organizations. Programs implemented by Chris and his team help organizations deliver strong technological innovation, helping align industry leaders with a substantial competitive advantage while (or by) focusing on technology transformation, increasing productivity, reducing cost, cloud migration, and organizational security.

Chris has a strong track record of building versatile, top-tier technology teams. His skillset includes strategic planning, technological innovation, IT architecture, applications, security and production with large ERP, cloud providers, ITIL, and data science technologies.



Preparing for a Cyberattack:

CREATING CONTINGENCY AND BACKUP PLANS

All agencies must have a contingency plan in place should they be hit by a cyberattack. Learn how leaders can work with their IT department to create a backup strategy to mitigate damages in a worst-case scenario.

By Dr. Kenneth Williams, Executive Director, Center for Cyber Defense at American Military University

Organizational leaders are expected to conduct due diligence in order to protect valuable resources and assets within their information systems. While many leaders clearly understand this need and their responsibilities, very few have the expertise and technological background to make an informed decision about how to actually protect their systems from intruders.

The first thing leaders must understand is that an organization's networked systems can never be 100 percent protected from attackers. No matter how many detection systems or proactive measures are installed to protect a network, there is no guarantee against intrusion.

The best way for an organization to protect itself is to prepare as if the network is going to be attacked. Then, the organization can take measures to mitigate the risk by developing strong contingency plans and instituting comprehensive backup and restoration measures to minimize data loss.

Creating Business Continuity Plans

Business continuity planning is the implementation of a comprehensive strategy

to maintain business operations during a catastrophic event like a data breach or ransomware invasion. By creating contingency plans, an organization mitigates its risk and minimizes the loss of critical assets if an attack were to happen.

A continuity strategy should be planned and developed at the highest echelons of the organization and implemented throughout the organization. To begin, leaders must ask themselves some important questions, including:

- What are the critical interconnection points among people, processes, technologies, suppliers, and customers? What systems are vital for the operation? This could include phone systems, VPN networks, digital radio systems, and email, all of which are critical for operation.
- Assess all these current technologies and create a contingency plan to safeguard data within those systems, including backup, disaster recovery, vaulting, snapshots, and replication.
- If these critical systems were to go down, how could the organization maintain operations using alternative systems? Ideally, these alternative systems should be located far enough away not to be jeopardized during an attack.
- Who will be part of the incident response team? How will those people be notified? How will they notify others in the organization about the attack and changes to operational procedures?
- What are the recovery objectives and what is the organization's recovery time profile?

In addition to developing detailed contingency plans that address those questions, it is vital for an organization to regularly review and practice these plans. Organizations should:

- Monitor the organization's data flow processes.
- Refine contingency plans to address changes in personnel and infrastructure and/or changes in organizational strategy.
- Initiate a robust testing plan that documents and measures the results of all successes and failures. Execute such tests at least once per year using various scenarios.
- Schedule regular reviews and updates to business continuity plans to accommodate the changing nature of technology and any changes in the organization's strategy.
- Repeat the entire process continuously.

Organizational System Backup Considerations

While a contingency plan defines how the organization will operate during an attack, the organization must also take steps to minimize potential loss of data and other information after an attack. The organization must have an effective backup plan in place to rapidly restore service following a cyberattack.

An organization's backup strategy will depend on its operational priorities, as well as on its size and specific operational environment. For example, small organizations with limited networks can use digital devices such as thumb drives or DVDs to store important files, while larger organizations should consider online resources such as redundant arrays of independent disks (RAID), automatic failover, server clustering, or mirrored systems.

Organizational leaders should talk to their IT department about its backup strategy and ask questions such as:

- **Are systems fully redundant and load-balanced?**
- **Is data mirrored so that if something happens, the system can be restored?**
  One technique to consider that protects against data loss is the concept of Stripe and Mirror Everything (SAME). This assures robust flexibility through mirroring technologies at the database file level rather than the entire disk level. Mirroring at the file level is duplicating data in individual files instead of the entire hard drive; this saves space on the hard drive and increases speed.
- **Are files spread across all available storage and not located in a single storage location?**
- **Does the organization have Service Level Agreements (SLAs) with commercial entities?**
  SLAs are similar to a service contract with a telephone company or car dealer. It provides technical expertise to repair IT equipment, similar to a mechanic for a car.
- **Is data backed up on different devices?**
  This could include anything from magnetic disks, tape or optical disks, and thumb drives. It depends on the organization's choice for backup, which could include electronic vaulting, network storage, or tape libraries.
- **Does the department use automatic failover and server clustering?**
  Automatic failover is when a hard drive fails and a backup hard drive automatically takes over the function without delay or interruption in service. Server clustering is when more than one server is used to increase the service to the user. This is similar to having a main server with multiple backup servers that will take over if the main server fails.
- **Is the organization prepared for a loss of power during an attack?**
  Organizations should consider implementing Uninterruptible Power Supply (UPS) to prevent data loss due to an unexpected power outage. UPS is designed to store enough energy in its internal battery to allow for active response time by users and for the safe shutdown of all systems.

When Are Backups Conducted?

It's also important to clarify how and when backups of the network will take place. Regular backups of company data should be conducted either once a day or once a week, and usually during hours when the data and network are not in use, such as around 1:00 a.m. on Sunday morning.

Selecting a time when the system is not in use will lessen the chance that it will cause interruptions to regular business processes. There are three common methods for conducting backups:

1. **Full backup:** This captures all files on the disks and occurs on a single medium. The time required for a full backup is greater than that of incremental or differential backup, but ensures a greater level of accuracy. Due to the associated time and cost, a full backup is usually performed during the initial phases or following a data restoration.
2. **Incremental backup:** This captures files created or changed since the last backup and requires less time and cost to run than a full backup. One issue with this technique is the need to use different devices during recovery. For example, if differential backups are captured on different devices such as a tape and a USB drive, recovering the data will require access to each media separately.
3. **Differential backup:** This type of backup is the storage of data since the last full backup, which occurs following a full backup, and is faster and less costly than a full backup. This type is considered slower than an incremental backup, but offers a faster recovery time. During recovery, a differential backup only requires the use of the full backup device and the differential backup.

Best Practices for Hardening a Network against a Cyberattack

Organizational leaders should also verify that their IT department is following best practices when it comes to hardening a network. Leaders should confirm the following recommendations are being followed:

1. Select, purchase, and install all hardware, software, and licenses for the system.
2. Verify the installation of antivirus software on all computers and turn on automatic updates.
3. Configure all computers to use junk e-mail filtering and install spam filtering on the mail server.
4. Turn on automatic software updates for all computers.
5. Locate the server in a locked room with controlled access.
6. Institute backup and restoration procedures across the entire organization. Implement daily backups with a full backup conducted weekly. Store the backed-up data in a location outside of the organization's geographical area.
7. Configure services on the server to enforce strong passwords of at least 10 characters with at least two uppercase characters, two lowercase characters, two numerals, and two special characters.
8. Configure individual computers to log users out after a five-minute period of idleness, so that those users are required to log back on.

Data Breach Considerations

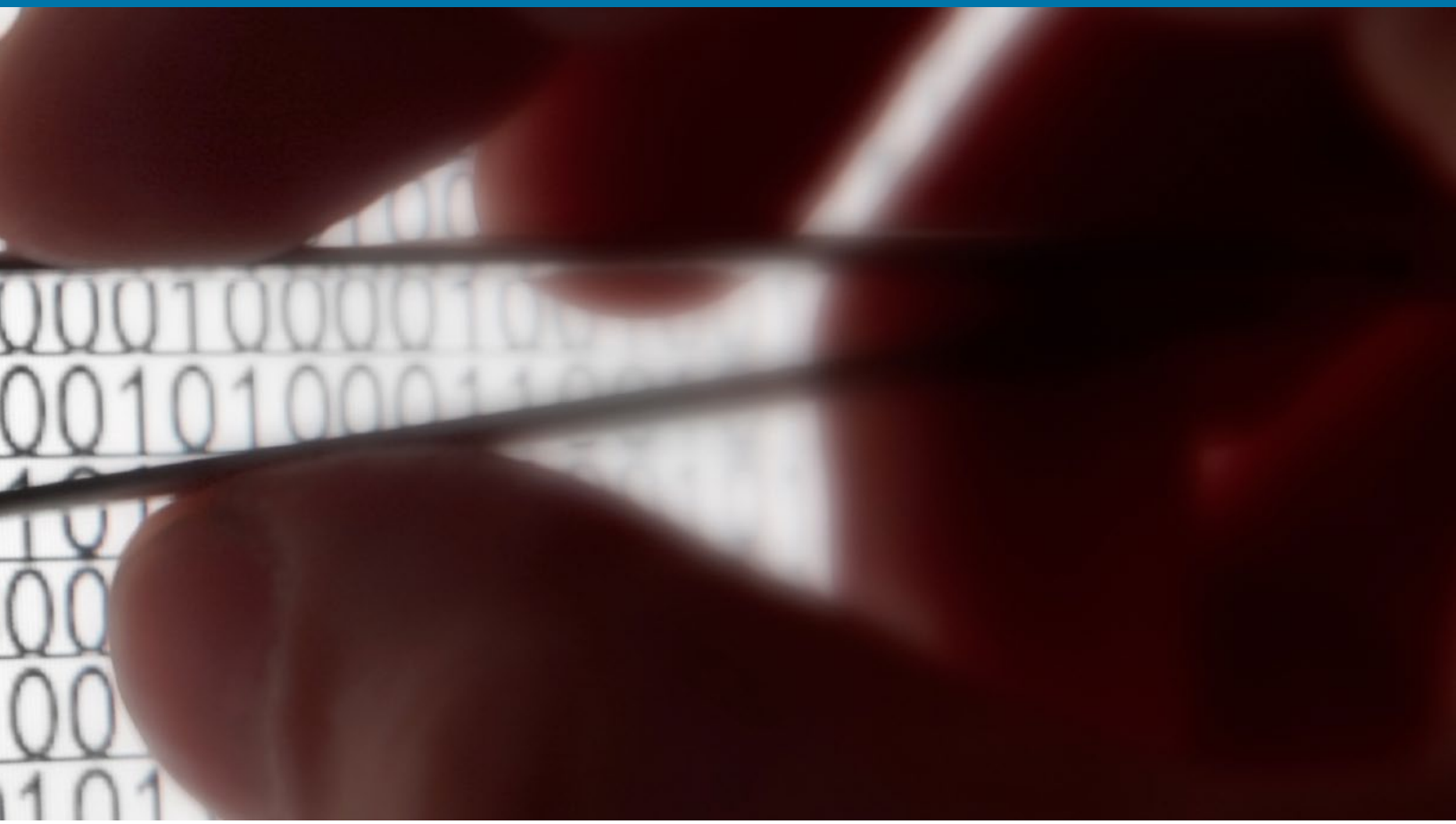
All organizations should operate under the assumption that a data breach will happen and create a plan to respond to an intrusion. Here are questions to ask your IT department about its breach response policies:

1. **What's our breach containment procedure?**
   Upon detection of a breach, the organization should immediately activate its designated incident response team. These initial steps will help the organization contain the spread of the virus to other networked systems and limit additional loss of data.

2. **How will you evaluate the risk of the breach?**
   Upon detecting a breach, an organization needs to immediately and thoroughly evaluate the risks associated with the breach, including who was affected and what harm was done.

3. **How will you notify affected individuals?**
   The incident response team should be notified first, followed by affected managers and personnel.

4. **How will you conduct a review of the incident to help you prepare for future breaches?**
   After the incident has been addressed and remedied, it is important for IT staff to have policies in place to learn from the situation. They need to evaluate how the organization responded to the incident and work to refine and further prepare for future breaches.



User Education Considerations

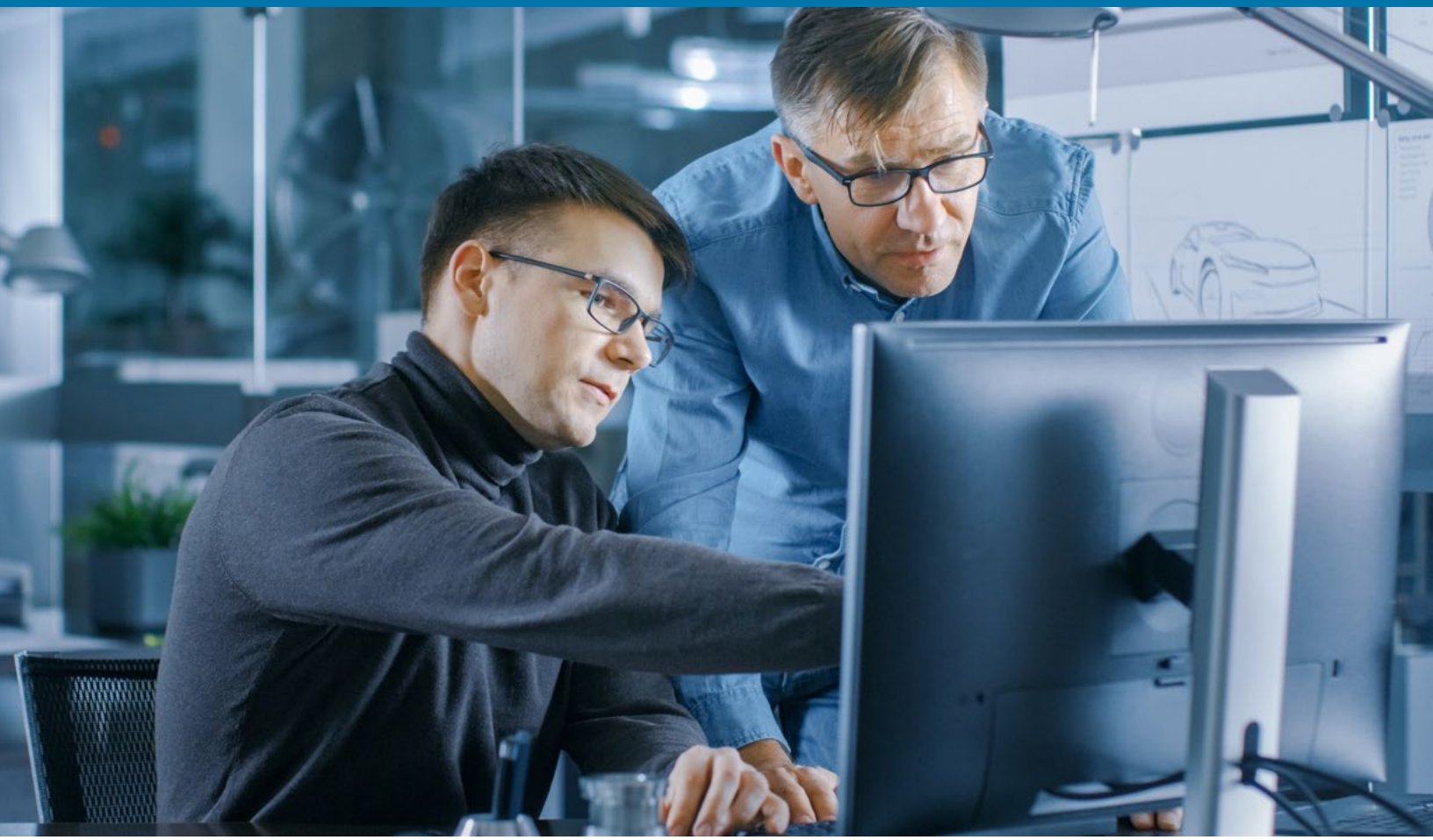
Organizations should also plan for robust user awareness training. The importance of training should not be ignored as it is common knowledge that human error is considered the greatest threat to organizations' information systems.

All users should receive training in critical areas, including incident handling, disaster recovery, securing data at rest, phishing, and safe home computing. This training will educate users on the importance of security, the proper handling of passwords, laptop security, virus prevention, safe internet browsing, and consequences for unsafe and illegal actions. ■

About the Author

Kenneth Williams, Ph.D., is the Executive Director of the Center for Cyber Defense at American Military University. He holds a doctoral degree in cybersecurity and a master's degree in information security/assurance from Capella University.

In addition, Kenneth is a Certified Information Systems Security Professional (CISSP) and holds Security+ and CompTIA certifications. In the past, he has also held positions such as president/chief information officer for Thelka Professional Associates; adjunct professor for Northern Virginia Community College, DeVry University, and Sullivan University; IT specialist/cybersecurity compliance auditor for the U.S. Army Inspector General; information system security/VOIP engineer and contract lead for the U.S. Army's CECOM; and information system security engineer and technical manager/chief information officer for Onyma, Inc. He is an Army veteran with more than 24 years of active service.



Tips on Training Adult Employees in the Workplace

Teaching employees about cybersecurity is a challenging but necessary step to protecting an organization's systems. Here's how one CIO approaches employee training.

By Chris Chiancone, Chief Information Officer of Plano, Texas

For many years, I worked as a part-time night and weekend adjunct professor for a few junior and private colleges. I will never forget my first semester of teaching when I could not figure out why students were having difficulty remembering content, were not very engaged during class, and were harsh in their critique of my teaching style.

I reached out to my teaching advisor for insight and ended up having a very

enlightening conversation about adult learning. Although his evaluation of my teaching style left no room for any feeling of accomplishment, it proved to be one of the best coaching sessions I have ever had. I've applied what I learned directly to my current career, which includes training personnel how to use technological systems and protect network systems.

Why Adult Learners Are Unique

Adult learners are distracted learners, my advisor told me. Period, end of story. Adult learners often have lots of things other than learning going on in their life. When in class, they might start thinking about what they're making for dinner, how to get their kids to different events around town, concerns with household finances, and a number of other complicated and stressful things. As a result, adults require some unique approaches to help them learn and understand new information.

Delivering Effective Training

Similar to challenges in traditional academic settings, adults also have difficulties learning new information when at work in a business setting. Company training staff must remember this when conducting training sessions about new technologies, new procedures, updates on company policies, and other important company information.

When conducting training that requires in-person attendance, it's important to remember that traditional training methods are often not effective for many employees. Traditional sessions are often too long, overly structured, and don't focus on teaching applied skills.

When I deliver in-person training to employees, I employ a teaching model I developed from my academic teaching experience that I refer to as CPR, which is based on three principles:

- **Chunks:** presenting small amounts of information at a time. In order for this information to stick, it must be attached to a
- **Peg:** an image, belief, emotion, or other sensory element that the person finds
- **Relatable:** and pragmatic in nature.

Information presented using the CPR method needs to be repeated over and over, in a process called inculcation. The more the information relates to common business problems and is presented in a way that directly applies to how the person will use it, the more likely the employee will understand and retain it.

Teaching Technology Skills

Let's take, for example, training employees on how to use a new computer operating system. Traditional teaching would go through the history of the operating system, versions, advancements, high-level explanation of the use of the system, and common issues with the system. This is all well and good for technology staff who support such a system, but non-technical people would undoubtedly be bored to death.

Instead, the non-technical adult learner needs to be taught in a way that reflects how they will use the system, in less than 50 minutes of time. The training session should include:

- A computer loaded with the new operating system.
- An environment in which the employee can follow along, step by step, with the instructor as they complete common tasks.

Break

- More opportunity to follow the instructor on common tasks related to chunks of business knowledge. For instance, working through an Excel document where the instructor teaches and the student duplicates.

Break

- Present chunks of business knowledge, attached to solving a real-life work problem.

Break

- Peg the real-life problem to a feeling of accomplishment and success.

Relate the material to solving a problem so employees know that what they're learning is practical and can be applied to solving future problems they might encounter. By following the CPR method, employees will increase their knowledge about how the system works in a practical way, which will enhance their ability to use it to solve future problems they might encounter.

Instructors should also present this information repeatedly, using inculcation, which will eventually lead to better retention of information, although it may cause some frustration among employees. One way to combat this frustration is to record training sessions and allow staff to learn at their own pace, any time, and in their own environment. Conducting regular and thoughtfully structured training sessions will lead to greater adoption by employees and improved knowledge and efficiency. ■

About the Author

Chris Chiancone is a strategic thought leader with more than 20 years of experience delivering advanced hardware and software solutions for private corporations and public-sector organizations. Programs implemented by Chris and his team help organizations deliver strong technological innovation, helping align industry leaders with a substantial competitive advantage while (or by) focusing on technology transformation, increasing productivity, reducing cost, cloud migration, and organizational security.

Chris has a strong track record of building versatile, top-tier technology teams. His skillset includes strategic planning, technological innovation, IT architecture, applications, security and production with large ERP, cloud providers, ITIL, and data science technologies.

Do's and Don'ts of Online Activity

Do's!

- Set a lock password and set up your cell phone to lock after at most five minutes of not being used.
- Set up your cell phone to "wipe your data" after too many failed attempts to unlock it.
- Make sure you only purchase from websites you can find reviews on and make sure that the site is secure. Look for the lock or green box in the address bar.
- Make use of the privacy tools on your social media accounts. They are there to protect you. Use them to restrict who can see your information.
- Ensure you are running some form of anti-virus, malware detection, or firewall software. Even the best and brightest in cybersecurity fall prey to attacks—this software is necessary to protect your devices and systems.
- If you're using department-issued equipment at home, make sure your home WiFi network is secured. If you do not know how to set that up, reach out to your internet service provider.
- Update your important passwords on a consistent basis, such as every three months.

Don'ts!

- DO NOT open an email from someone you do not know.
- DO NOT open any attachments in an email unless you were expecting the attachment, even if it's from a known sender.
- DO NOT reuse the same password for multiple sites. Avoid using things such as your birthdate as your password. Try using a combination of symbols, numbers, and characters to build a memorable list of passwords.
- DO NOT use public/free WiFi for anything other than basic browsing. You should never go onto any website requiring credentials or financial information on public WiFi.
- DO NOT access any site needing log-in credentials on public computers at the library or internet cafes. If you do, make sure you ALWAYS log out as soon as you are done, and consider changing your password when you get home.
- DO NOT post information on your social media accounts that you don't want the public to see. Information can get leaked even with proper privacy settings, so if you do not want it online, do not put it there.
- DO NOT download any illegal/cracked software, music, and movies. In addition to this practice being against the law due to copyright violations, most of these files come with viruses, malware, trojans, and more.
- DO NOT click on a link in any email without verifying the address is exactly what you expect. It is very easy to miss a spelling error or an extra hyphen in a web address.
- DO NOT enter any credentials into an online website unless you type in the web address yourself.

CYBER THREATS ARE EVOLVING

SO SHOULD YOUR SKILLS

Escalating cyber attacks threaten national security and our daily lives. Are you prepared with the skills and knowledge to further safeguard our nation's most valuable digital assets? American Military University offers a variety of programs for public safety leaders to learn technology, network security, and strategies to thwart cyber threats.

AMU Offers Undergraduate Certificates in:

Cybersecurity
Cybercrime Essentials
IT Project Management Essentials
Information Security Planning
Information Systems Security Essentials

AMU Offers Bachelor of Science Degrees in:

Cybersecurity
Information Systems Security
Information Technology Management

LEARN FROM THE LEADER

Earn your degree from a university that is recognized by the Department of Homeland Security and National Security Agency as a National Center of Academic Excellence in Cyber Defense Education (CAE-CDE).

AMUonline.com/cybersecurity

AMU American Military University