THE SAGE GROUP

Mentoring Solutions for Law Enforcement

"Solutions that Empower your Workforce"

Cyber Security

Understanding the Cyber World

Overview

Let's begin with a simple question.

Who targets Law Enforcement agencies and why?

The following list of Threat Groups (according to the FBI) represent a large percentage of Cyber attackers to Law Enforcement entities:

1. Hacktivists
2. State Actors
3. Criminal Organizations
4. Terrorist Organizations
5. Purposeful or Accidental Insider
6. Individuals

Hackers Find "The Weakest Link"

An online Chinese takeout menu proved to be the way into the servers of a major Oil Company. When employees clicked on the menu, they unknowingly downloaded malicious code that gave the hackers access to the network. This is known as a "watering hole" attack. This story has served as a cautionary tale since and a lesson – that hackers are very resourceful at finding "The Weakest Link" in the most unlikely of places.

Tip: Every time an employee clicks on an external Website it is like opening a window into your organization. Work with your IT personnel to ensure that the department controls what windows can be opened and who or what is coming through them. Early detection is the key in the event of a breach.

HACTIVISTS

Hacktivists (hacker + activist) target law enforcement to further an ideology or political agenda. Their activities may relate to an established ideology, a specific issue, or a particular event such as a law enforcement action. One of the better-known Hacktivist collectives is Anonymous, which has backed a range of issues and taken part in numerous attacks on public safety organizations that resulted in the release of highly sensitive information. Interestingly, Anonymous has also declared “cyber war” on groups like ISIS and the Ku Klux Klan.

STATE ACTORS

This category includes state-sponsored military or intelligence services, groups and individuals acting on behalf of foreign governments such as China, Iran, North Korea and Russia. These state-sponsored actors do pose a threat to state and local law enforcement in the United States and have executed successful attacks.

The United States military and intelligence services have long been the target of state-sponsored Cyberespionage – the virtual stealing of confidential or classified information by illicit means. As state and local law enforcement agencies continue to build their intelligence capabilities and integrate with the federal intelligence community, they will increasingly become the holders of information considered valuable by foreign governments.

After the shooting of Michael Brown in Ferguson, Anonymous publicly named who it thought was the officer involved – it was the wrong person. Anonymous also hacked Twitter accounts associated with the KKK after the hate group threatened protestors. This Hacktivist category also includes individuals acting alone.

CRIMINAL ORGANIZATIONS

The Internet has been a boon for criminal organizations, which have quickly learned that cybercrime, with its anonymity, low physical risk and global opportunities, pays often and well. Cybercriminals have targeted law enforcement agencies by infecting computers with ransomware, which, in one variant called CryptoLocker, encrypts files until the agency pays a specified amount, or ransom, to decrypt them again.

Police departments large and small have been the victims of this crime and, often faced with no other way to restore the corrupted files, have paid for the key that unlocked their data. The amount was typically a few hundred dollars. If the agency did not pay, the data remained inaccessible and the price went up. The departments that haven’t had to pay had backups of all of their data and, after purging the infected files, were able to restore their systems. With ever-expanding cybercrime capabilities by these organizations, ransomware is likely only the beginning of the methods these groups use to target law enforcement agencies.

TERRORIST ORGANIZATIONS

Terrorist organizations, which for years have used the Internet to radicalize, recruit and fundraise, have expanded the scope of their cyber activities. The Islamic State is a good example of this. In 2015, the so-called "Islamic State Hacking Division" released its "hit list," which consisted of the names and addresses of 100 U.S. military personnel. Given that law enforcement personnel have been identified as legitimate targets by the group, it is not outside the realm of possibility that the same approach could be used with them.

PURPOSEFUL OR ACCIDENTAL INSIDER

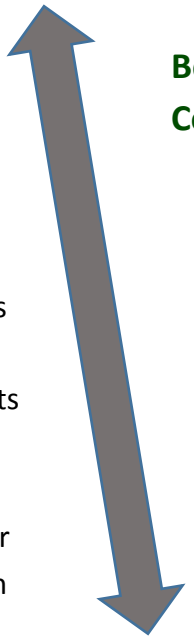
This may well be the most pernicious threat to state and local law enforcement agencies. This category includes employees and contractors who would purposefully cause harm to an agency.
It also includes the accidental insider who is unaware that he or she has become the organization's weakest link in the cyber chain.

INDIVIDUALS

Individuals may adopt the causes or tactics of groups and, through hacking and Cybercrime forums on the Web, can gain access to a multitude of hacking tools. Because of their singularity, these individual attackers are dependent on their own hacking skills, which can run from the extremely advanced to the very basic – the so-called "script kiddies," a derogatory term used in the hacker community for neophyte hackers who modify existing computer scripts or codes because they lack the expertise to create their own. The global nature of cyber-attacks means that individuals can be physically located anywhere in the world and obscure their identities through a series of anonymous proxy server.

Best Practices:
Countering the Purposeful Insider

- Extensive Background Checks
- Controlled Access to only necessary networks and files
- Redundancy among the IT Team in terms of access to key systems
- Automated unauthorized download alerts
- Limiting use of portable data storage devices
- Swift investigation of suspicious behavior
- Follow up after official disciplinary action



Best Practices:
Countering the Accidental Insider

- Regular organization-wide cyber mentoring/training
- Follow-up training exercises mentoring/training
- Incentivized reporting of suspicious activities
- Controlled access to networks and files
- Technology use policies
- Limited use of personal devices

THE SAGE GROUP

Mentoring Solutions for Law Enforcement

"Solutions that Empower your Workforce"

Why They Do It – What Are The Motives?

The Motives behind Cyber Attacks range from revenge to notoriety. Below are a few of the most common:

1. Disabling Websites
2. Public Exposure of the Private Information
3. Espionage
4. Interference with Police Operations and Sabotage
5. Defacing to Cause Embarrassment or Retaliation
6. Retribution
7. Profit
8. Notoriety
9. Disinformation

HOW THEY DO IT – TACTICS & METHODS

TACTIC	METHOD
Denial of Service Attack: A Denial of Service Attack aims to disable a website of network so that is inaccessible to its end user. A Distributed Denial of Service (DDoS) attack can prevent access to all or parts of networks and render communications systems inoperable.	A DoS Attack can be executed using widely available software tools that overwhelm a police department's public-facing website with traffic so it crashes. Some of these DoS attacks can take a system offline for an extended period of time and make it difficult or impossible for a department to fully function. There are also telephony denial of service attacks (TDoS) in which Public Safety Answering Points (PSAP's) and emergency communications centers are flooded with calls that overwhelm their telephone networks and make them unable to answer legitimate calls for service.
Phishing: Phishing is a tactic used to deploy malicious code, or malware, or allow the hacker access to the network.	The most common method is to take advantage of unsuspecting employees and contractors by enticing them to click on infected attachments of websites that deploy the malware or let the hacker into the system. This often involves sending emails to employees' work addresses that contain an attached file and/or an embedded link. This email looks legitimate or enticing enough to motivate the recipient to click on a link or open an attachment. That click unleashes malicious code onto systems/devices. Once downloaded, the malware either causes immediate damage or quietly lurks in the background, serving as a backdoor for the hacker to access the system.

TACTIC	METHOD
Deployment of a Trojan Horse: Once in a network, a Trojan Horse program may simply provide backdoor access to a hacker seeking to access proprietary data or system information.	Cyber Trojans can enter your network without being detected. One interesting method is to hide a Trojan Horse in a program that claims to rid your computer of viruses. Trojan Horses are named as such because they very hard to appear routine and benign so that users will download them onto their computers. It can also release malicious code to damage the network, hamper computer performance, and exfiltrate, modify, block, or delete data. It cannot self-replicate like a worm and does not inject itself into other files like a virus. There are a number of classifications for Trojans. Some are Backdoor, which gives the hackers remote control over your system; exploit, which a vulnerability in the software; and rootkit, which works to conceal the activity of the Trojan Horse.
Planning and Carrying out Attacks on Social Media: Social Media Platforms such as Facebook and Twitter are used to plan or carry out attacks on a network, organization, or individual.	As one example, an attacker can identify a target on social media, find out personal information about the target and then use websites such as Spokeo and Intelius to round out the research. Depending on the privacy settings of the target, the attacker may be able to directly post information to the victim's Facebook page or Twitter account or direct others to inundate the victim's page. Other types of attacks that often have a social media component include: doxing, in which personal information is illegally obtained and released publicly with malicious intent; swatting, in which someone tricks police into deploying SWAT teams to someone's home based on a false report – a tactic sometimes used in conjunction with a Cyber Attack like Denial of Service; or malicious crowd sourcing, in which an attacker pay people to carry out malicious attacks online.
Social Engineering Social Engineering involves manipulating or tricking people so they unknowingly divulge network information or provide access to networks.	The attacker identifies a target within an organization using social media and other tools or finds information out about a person that can be exploited. The unsuspecting individual may play a very small role in a much larger plan, which means that this tactic may not be immediately identified as what it actually is. In one approach, an attacker will pose as a member of the department's IT unit and call employees to provide "technical support." During the conversation, the attacker will ask questions of employees that elicit enough information to infiltrate the network. Another approach is to give the unsuspecting employee a series of commands that launch malware or give access.

TACTIC	METHOD
Use of Exploit Kits: This tactic delivers a malicious payload to a user's computer that gives the hacker access to sensitive information that varies by target.	These malicious codes can hide in commonly trafficked and trusted websites whose servers have been hacked. When a user clicks on the legitimate site that has been compromised, he or she is stealthily redirected to another server that has the exploit kit. The user's computer is scanned to identify vulnerabilities such as outdated virus protection or unsecured software. Once a vulnerability is identified, the malicious payload is delivered. Exploit kits are widely available through underground or public sources and can be used by relatively inexperienced hackers. A variation on this them is a zero day vulnerability – a weakness in the software's original code that was not caught by the original developers. The time between when the flaw is detected and when the original developers or security vendors release patches is the hackers' so-called golden hour. There are also zero day viruses; these are viruses for which no anti-virus software has been developed.
Signal Disruption and Hijacking: All devices that rely on Wi-Fi or Bluetooth have the potential to have their signals disrupted.	This strategy could be used to disrupt Law Enforcement operations. These include radios, cell phones, wireless routers, laptops, tablets, and building access & control systems. We are used to signal disruption because of high system traffic, buildings, trees, limited signal range, conflicting signal waves, and atmospheric conditions. However, there are also jammers and other devices that deliberately interfere with signals and, in Law Enforcement context, disrupt operations. A variant of this is signal hijacking, which is when a hacker intercepts a signal takes control of it.
Physical Disruption and Theft: This tactic involves both a physical cyber component. In the physical realm, it involves the theft of physical items such as thumb drives. In the cyber realm, it involves virtually disrupting physical systems that regulate everything from heating and air conditioning to the locking and unlocking of doors.	It must be overlooked that all data and network systems have physical components that can be compromised and destroyed. Wires and cables can be cut, power can be shut off, and devices can be stolen, Hard drives, thumb drives, mobile devices, and laptops are small enough that they can easily be taken. The devices can also be valuable to cyber criminals because they can potentially provide access to the wider network. The physical security, including access control, of Law Enforcement buildings must also be maintained. For these reasons, some organizations prevent people entering sensitive facilities from bringing in any technological device that could be used to store data or access networks.

Cyber Vulnerabilities of Law Enforcement Agencies

1. Personnel
2. Organizational Barriers
3. Information Networks & Systems
4. Public-Facing Websites
5. Data Storage Devices
6. Social Media Accounts
7. Communications Centers, Systems, Equipment and Applications
8. Wireless Devices
9. Facility Systems and Physical Infrastructure

PERSONNEL

Ironically, it is not technology but human behavior that is an organization's greatest vulnerability. Even the most advanced cyber protection systems are vulnerable to an insider – anyone in an organization, not just an employee or contractor with network administrator responsibilities.

Accidental Insider

Becoming an accidental insider can happen through an unintentional misstep or as a part of a social engineering scheme. Accidental insiders can:

- Be specifically identified and recruited by hackers
- Open or click on content in a phishing e-mail
- Access an untrusted, compromised website
- Unknowingly open a corrupted document from a trusted website
- Share passwords among colleagues

Purposeful Insider

The purposeful insider is someone who intentionally targets an organization while working as an employee or contractor. The purposeful insider can have designs on an organization from the beginning or have experiences that cause him or her to turn against the organization, such as in the wake of a disciplinary action.

The purposeful insider can act swiftly and directly, recruit unknowing accomplices from within the organization, or try to operate under the radar while continuing to compromise the system or gather information. To decrease vulnerability to the purposeful insiders, organizations must put processes in place to carefully select employees with a high level of integrity and clean backgrounds.

ORGANIZATIONAL BARRIERS

Executive Support

Executive support is vital to making cybersecurity a part of the culture and everyday practices of an organization. The following are the tools to accomplish this; all of them require executive support to succeed.

- Write policies and guidelines that ensure cybersecurity is integrated throughout the organization.
- Hire and extensively vet full-time staff or contracted support in cybersecurity, information technology, and cyber investigations.
- Integrate cybersecurity and cyber threat briefings into regular command staff meetings.
- Dedicate funding and develop a plan for continuing funding that accounts for equipment and software upgrades years after the initial investment.
- Publish a timeline for developing and maintaining cyber capabilities.
- Develop the cybersecurity messaging from executives and command staff so that it is consistent and informed and propagates throughout the organization and beyond.

Organizational Culture

Executive support and organizational culture go hand-in-hand. Likely, a strong cyber culture will develop from both the top down and bottom up. An organization is going to be more vulnerable if cybersecurity is not an accepted element of every agency operation, plan, and decision. An agency will also be more vulnerable if its personnel do not take ownership of cybersecurity in their daily roles. Here are some tools to accomplish this.

- Formalize cyber partnerships with other agencies in areas such as information sharing and emergency response.
- Provide cyber awareness training and keep track of the number of employees who have gone through it; aim for 100% compliance.
- Identify the employees who were hired for their cybersecurity and information technology qualifications.
- Feature cybersecurity personnel and initiatives in newsletters and on the organization's website.
- Publish agency contact(s) for reporting cyber-attacks and suspicions.
- Create a cybersecurity response plan and ensure that all employees know what it is; update it annually at a minimum.
- Conduct cyber exercises and keep track of the number of employees who participate; increase that percentage each year.

Training & Mentoring

Here are some ways to accomplish this.

- Cyber-awareness training and integration of Cyber Security Practices into the mentoring plan.
- Integrate cyber and proper security practices into the organization's training plan.
- Teach each employee to recognize the signs of an attack and phishing attempts and proper reporting.

INFORMATION NETWORKS & SYSTEMS

Whether an agency has its own dedicated network or one that is controlled by a city or county, it is important to proactively understand the cyber threats and vulnerabilities. Work with your IT team to conduct an assessment that provides you with information about how the entire city/county network works – not only the piece that affects your agency. *This assessment should include all devices across the spectrum.*

The following should be assessed for vulnerabilities:

- Systems Access Management
- File Access Management
- Continuous Monitoring Systems
- Agency Intranet and Internet
- Cloud Storage – official and unofficial (e.g., DropBox)

Software

Hackers can infiltrate software to allow ongoing backdoor access that enables them to:

- Overwhelm network systems to slow or disable
- Lock out agency users
- Corrupt systems or files
- Gather sensitive information on an ongoing basis
- Plant dangerous information or misinformation into files or response systems
- Control response systems

A prime example is keylogger software, which allows hackers to track every keystroke typed on a keyboard in order to identify passwords and other information. This leads into the concept of supply chain security, or making sure that all of the various software your agency uses has been vetted by a government body and deemed secure and safe.

Once it has been vetted by a third party and employed by your agency, software must be regularly updated across the enterprise. Organizations should also assess the myriad third-party vendors and applications that access their systems such as:

- Tablet and Smartphone Applications
- Internet Browsers
- E-mail Clients
- Training Solutions
- Cloud Storage
- Web Conferencing

Data Files

The types of data that will likely be of most interest to hackers include files that: can be used against the agency; can help or harm outside individuals; are Law Enforcement Sensitive or fall into the national security realm; or can be manipulated to incite havoc or influence an outcome. Personal information that might not be easily accessible anywhere else is especially vulnerable. The following types of files and sources of data should be examined for vulnerabilities:

- Personnel Records
- Confidential Informant Databases
- Records Management Systems
- Computer-Aided Dispatch
- Mobile Data Terminals
- Laptops and Tablets Used by Officers in the Field
- Case Files
- Footage from Body-Worn and Dash-Mounted Cameras
- Organization Plans and Procedures
- E-mail Clients
- Mapping/GIS System

PUBLIC FACING WEBSITES

An agency's public-facing website – versus one that is viewable only by employees – plays multiple roles. Pubic-facing websites that offer e-government services are potentially more vulnerable to cyber intrusions if they are directly connected to the rest of the agency's network assets. Assessing the following will help to identify technical vulnerabilities:

- Internal or external hosting
- Website Hosting and Security configuration
- Relationship to website server to other computer systems in the agency

DATA STORAGE DEVICES

Small and portable data storage devices can have a big impact on security if they are compromised or stolen. Consider the destructive and stealthy Stuxnet computer worm, which was introduced to Iran's Natanz nuclear facility through a standard thumb drive.

That powerful payload, which was activated when an unsuspecting employee clicked on a Windows icon, provided the attacker(s) with the ability to physically control the operations of a nuclear power plant.
Here are some that are used on a daily basis:

- Thumb Drives
- Internal and External Hard Drives
- Servers
- CDs/DVDs
- Printers and Copiers
- Computers, Laptops, and Smartphones

SOCIAL MEDIA ACCOUNTS

The adage "birds of a feather flock together" is particularly true when it comes to social media platforms – and the criminals know it. One publicly identified law enforcement officer on a social media platform can lead hackers and other bad actors to an entire network of cops.

If an individual is trying to target one specific officer he or she may take a more strategic approach by trying to "friend," follow, or add others into his or her network before approaching the real target. By the time the real target is approached, the bad actor looks like a friend because he or she has successfully been camouflaged by mutual contacts. The unfamiliar – and, in this case, potentially dangerous – becomes familiar simply through some clever online networking. Once in, the individual can potentially identify the target's family members, the locations of residences, places of work, schools and patterns of life. Bad actors also use social media platforms to release personal information about officers (i.e., doxing) or agency network vulnerabilities, incite potentially violent behavior during protests and other civil actions and generally create flash points around certain issues.

COMMUNICATION CENTERS, SYSTEMS, EQUIPMENT, and APPLICATIONS

The emergency communications "ecosystem" is a complex web that relays information critical to first responders' jobs. While communication tools make that delivery of services easier, they also carry inherent vulnerabilities. In one example, "secure" spectrum chips that support the government-only FirstNet network can be illicitly installed onto private devices, creating a window through which network traffic can be monitored.

In another example, mapping systems can be hacked to misdirect response resources away from an incident without the call center's knowledge. Here are some of the technologies that are part of the "ecosystem" and should be reviewed:

- Personal and Official Devices
- Public Safety Answering Points/ 9-1-1 Centers
- Computer-Aided Dispatch Systems
- Text to 9-1-1
- Mapping Systems & Radios
- Smartphones
- Tablets & Laptops
- Officer-Worn Sensors
- Body-Worn Cameras (devices and streaming video)
- Dash-Mounted Cameras
- Closed-Circuit Television (devices and streaming video

WIRELESS DEVICES

The Internet of Things (IoT) is the term used to describe the ever-growing network of "things" – objects embedded with unique identifiers that are able to transfer data over a network without human involvement. As the IoT becomes a reality, it is important to understand that any piece of wireless equipment can be accessed to disable, hijack, misdirect, or mislead.

More specifically, any wireless device that can receive and transmit data and/or commands to make another system do something or provide information to another system has the potential to be exploited.
This could mean that hackers could take control of vehicles, drones, robots, and weapons systems because many of them now have wireless components. The same goes for devices that use various forms of infrared.

The list of devices equipped with wireless capabilities is exhaustive, but here is an initial list that can be considered for vulnerabilities:

- Radios
- Mobile-Data Systems
- Body-Worn Cameras
- Dash-Mounted Cameras
- Navigation Systems
- Tactical Gear
- Smartphones and Tablets
- Body-Worn Sensor

FACILITY SYSTEMS AND PHYSICAL INFRASTRUCTURE

Just about every aspect of building management can now have a wireless component that makes it vulnerable to those trying to gain access to the building or to compromise the health and safety of those inside the building.

Consider these facility systems that may have a wireless component to them:

- Heating, Ventilation, and Air Conditioning (HVAC)
- Water Systems
- Elevators
- Parking Garages
- Lighting Systems
- Security and Access Control Systems

INTERNET OF THINGS: TECHNOLOGICAL STRENGTHS COUPLED WITH MYRIAD POTENTIAL VULNERABILITIES

The Internet of Things (IoT) is only at the beginning of its evolution, especially in public safety. As more devices are incorporated into everyday life it will be important to understand their potential vulnerabilities. Each of these benefits to law enforcement exposes a concurrent vulnerability that can be exploited by hackers.

Locate Officers and Monitor Health: Identify the location of officers in the field to analyze their movements or to target them. New sensors will also monitor officers' vital signs.

Vehicle Access and Control: Many capabilities in modern vehicles, even the automated tire pressure sensors, have wireless components that can provide means to access and control.

Real-Time Video Monitoring: Systems will eventually be able to access real-time video streaming from Body-Worn Cameras.

Communications Equipment Disruption: Radios, phones, tablets, 911 call centers, and CAD systems can all be accessed, hijacked, and disrupted.

Track and Redirect Deployments: Sensors will likely be placed on all types of equipment and personnel to track where and when they are deployed. Sensors on K-9 officers or tactical weapons could indicate when they have been released, automatically alerting command staff that a situation has escalated.

Catalog Inventory: Sensors may also be placed on all types of inventory to track their availability, location, and quantities. Hackers will be able to access this same information and possibly disable or alter information.

Facility Compromise: Wired building control and access systems can be manipulated by hackers.

Tip: As you conduct your cyber threat assessment and map your entire IT infrastructure, take an inventory of all of your agency's devices and systems. Identify vulnerabilities and either work with in-house or outsourced cybersecurity professionals to secure all of the links in your cyber chain.