Cybersecurity Guide for State and Local Law Enforcement

June 2016

National Consortium for Advanced Policing

Acknowledgements

Cybersecurity working group

We would like to extend a special thank you to all of the members of the Cybersecurity Working Group. The group's expertise and insights informed the development of this guide and ensured the value of this document for law enforcement.

The Working Group members were:

- Rebekah Brown, Cyber Threat Intelligence Analyst, Corporate Information Security, Nike Corporation
- Ed Cabrera, Special Agent, Criminal Investigative Division, Cyber Operations Unit, U.S. Secret Service
- David Carabin, Director, Boston Regional Intelligence Center
- Jack Furay, Special Agent, Electronic Crimes Task Force, Los Angeles Field Office, U.S. Secret Service
- Cecily Garcia, Cyber Intelligence Analyst, Orange County Intelligence and Assessment Center
- Chuck McNeal, Director, Louisiana State Analytical and Fusion Exchange
- Kenn Nelson, Lieutenant, San Diego Sheriff's Department, Cyber Task Force
- Michael Papay, Chief Information Security Officer, Northrop Grumman
- Mike Sena, Director, National Fusion Center Association
- Keith Squires, Commissioner, Utah Department of Public Safety
- William Wright, Director of Cybersecurity Partnerships, Symantec

* We would also like to acknowledge the contributions of Traci Lashbrook of the U.S. Secret Service and Chris Wilson of the Joint Regional Intelligence Center.

Acknowledgements

Citation:
Sutliff, Usha and Richardson, Tara, National Consortium for Advanced Policing. *Cybersecurity Guide for State and Local Law Enforcement*, June 2016.

Cybersecurity Program Team

Lafayette Group

Usha Sutliff, Program Manager

Tara Richardson, Senior Consultant

Center for Cyber & Homeland Security, The George Washington University

Center for Cyber & Homeland Security
THE GEORGE WASHINGTON UNIVERSITY

We would like to thank Frank Cilluffo (Director), Christian Beckner (Deputy Director) and Joseph R. Clark (Policy Analyst) for their contributions to this project. The team helped NCAP select members of the Cybersecurity Working Group and conducted a survey that gave us insight into cybersecurity awareness among our core audience.

Major Cities Chiefs Association, Intelligence Commanders' Group

Major Cities Chiefs Association

We would like to thank the members of the Major Cities Chiefs Association's Intelligence Commanders Group for taking their time to inform this guide.

National Consortium NCAP for Advanced Policing

Table of Contents

Table of Contents

National Consortium NCAP for Advanced Policing

PREFACE

This guide was created to help state and local law enforcement agencies in the United States gain a better understanding of how the term "cybersecurity" relates to their unique and complex world. We all operate daily in the cyber realm – we check email, we search the Web and we stream videos. The same holds true for the daily life of a police chief, a sergeant or a patrol officer. The difference between police and rest of us lies in the risk that comes with all of those virtual activities. An unprotected database with confidential informant information can lead to lives lost. An unsecured network that is hacked can paralyze an entire department.

This guide provides a high-level overview of the dangers of not having cybersecurity awareness and protection at any law enforcement agency, big or small. As we describe, the cyber threat is at the door of state and local law enforcement and only through collaborative approaches such as the ones described here will they be prepared to face that threat.

In this guide, you will find real-world examples of how law enforcement agencies have been successfully targeted, an overview of the range of threats they face and resources that can be used right away. We understand that there are many more resources out there, particularly in the private sector. Our list is meant to be a starting point and not the final destination. We hope that you can use this guide as a resource to brief your agency's decision makers and to get the help you need to improve your cybersecurity practices.

One note: To develop the guide, we did extensive open source research and consulted some of the best minds in the cybersecurity business. They came from the worlds of law enforcement, intelligence, academia and the private sector. Our many conversations all focused on finding the answers to one question: What do cops need to know when it comes to cybersecurity? The strategies detailed in this guide are largely the result of their input.

National Consortium for Advanced Policing

Section One: Understanding Cybersecurity

Introduction

The 2014 shooting of Michael Brown by police in Ferguson, Missouri served as a lightening rod for social issues that still dominate national conversations, policy and funding at every level of government.

Less covered on an ongoing basis was a smaller story in Ferguson that may, in the long run, have borne the most long-term and complex implications for American law enforcement. The story emerged a few days after African-American teenager Michael Brown was shot by a white police officer. The hacker collective Anonymous posted a video[1] that contained a threat both direct and unambiguous:

"To the Ferguson Police Department and any other jurisdictions who are deployed to the protests, this is your warning: We are watching you very closely. If you abuse, harass or harm the protesters in Ferguson, we will take every Web-based asset of your departments and federal agencies offline. That is certainly not a hollow threat but it is a promise.

"If you attack the protesters, we will attack every computer and server you have. We will dox[2] and release the personal information on every single member of the Ferguson Police Department, as well as any other jurisdiction that participates in the abuse. We will seize all your databases and e-mail spools and release them to the public. You have been warned."

This was not an empty threat. In the span of a few days, Anonymous hackers shut down the city's website, released the personal and family information of St. Louis County's police chief, took phone lines and e-mail offline and rendered all technological means but two – text message and cell phone – completely unavailable to government workers, including police and others who were coordinating response to the protests.

The cautionary aspect of this tale lies less in the specifics of what happened in Ferguson – and has happened before then and since in cities and towns across the country – and more in what this means in the long run for American law enforcement: Gone are the days when police can only be concerned about the physical aspects of policing. In this era, law enforcement agencies can literally be crippled by well-placed malware, clever network intrusions and a few keystrokes.

[1] https://www.youtube.com/watch?v=BIUKAt1iLlw

[2] Doxing will be covered in this document. Generally defined it refers to when hackers obtain personal information through illicit means and then release it publicly.

So what does this mean? As this story illustrates, the cyber threat is at the doorstep of state and local law enforcement agencies. Across the country, these agencies are seeing intrusion and disruption attempts – some successful and devastating – on a regular basis.

This places law enforcement executives in an interesting position: Understand the cyber threat and prepare your agency or risk being seriously compromised by a cyber attack. In this case, the stakes are personal. Cyber attacks on law enforcement agencies, in intent and execution, often extend far beyond the theft of data that are valuable to the agency itself. Officers' most private information – family members' names, where children go to school, home addresses, financial information and social security numbers – can and has been obtained through hacks and posted on the most public of websites. Widen the lens from the personal to the operational and the very lives of cops, which often depend on the ability to communicate with each other and their command, can be put at risk by taking down or commandeering a network. Widen the lens a bit more and extend it beyond police operations and an entire city can be incapacitated by an orchestrated cyber attack that takes the delivery of critical services such as electricity and water offline.

This heralds a new era for police. The cyber threat is not one that state and local law enforcement agencies have traditionally been charged with understanding or responding to. Information Technology (IT), in the world of law enforcement, is often considered an entirely back-room function handled by a specific unit in the city, county or state that rarely, if ever, interacts directly with law enforcement executives.

While certain detectives and officers receive training on cybercrime investigation techniques, their attention is often focused on citizens rather than their own departments. The reality is that officer safety and all aspects of police operations have a cyber component. To secure one area – the physical world of policing – and not to secure the other – the virtual world of policing – no longer makes sense. In short, cybersecurity has not been placed firmly in the wheelhouse of the typical law enforcement executive or officer – until now. *In today's world of policing, cybersecurity must be "owned" across the entire law enforcement and city or county enterprise and must be woven into every aspect of operations.*

WORST-CASE SCENARIOS

No longer are these scenarios mere speculation. In today's world, these scenarios are both possible and probable.

Systems Hijacked: Hackers have taken control of official email accounts and gained access to other incident control systems. Viruses and other methods of attack have been used to bring down information and communications systems used daily.

Sensitive Data Accessed: Hackers have gained access to sensitive police department data, including employee records, investigative files, criminal intelligence databases, organizational plans and procedures, email, and intel bulletins.

Officers Targeted: Information has been accessed in personnel files and through social media accounts to target officers.

911 Call Centers Hacked: Hackers have intercepted calls, replaced mapping systems, and disabled centers to prevent responders from reaching the correct incident locations.

Fusion Centers Compromised: Foreign actors have gained access to some fusion center systems. The information gained through these may help gain access to more sensitive national security systems.

Protect your agency by becoming educated about the cyber scenarios that can affect your operations.

Obtaining these capabilities and skills will ultimately shape what policing looks like in the future. Cyber-prepared police departments in the next decades will likely include officers and civilians who are, in essence, "patrolling" and securing the cyber realm of their own agency in the same way that uniformed officers patrol the physical one. These departments will have cyber capabilities – both reactive *and proactive* – built into all of their operations and their executives will have a firm grasp of the management and development of cyber capabilities throughout the enterprise.

We are not there yet. Law enforcement is getting much better in this area but has a long way to go when it comes to developing the cyber awareness and capabilities it needs.

This guide will provide a road map to the cybersecurity landscape. Coupled with the valuable resources offered by government entities, the private sector and non-profit organizations, this document can serve as a primer for the law enforcement executive or officer who seeks to "understand cyber" and take steps to increase the security of his or her agency. This guide also will take you on a tour of the threat landscape, the vulnerabilities, the steps to take and where to turn for more in-depth information and assistance.

At a glance, here are the steps toward cybersecurity that your agency can take. They are covered in depth in this guide.

1. Make cybersecurity a priority for the entire organization.
2. Make a case for funding.
3. Identify and connect with the entity responsible for your cybersecurity.
4. Designate a cybersecurity contact.
5. Identify POCs and formalize partnerships.
6. Conduct a cyber threat assessment.
7. Provide cyber-awareness training.
8. Establish and maintain executive support.
9. Develop and follow a cybersecurity maintenance plan.
10. Develop a cyber response and recovery plan.
11. Conduct organization-wide cyber exercises.
12. Share and consume cybersecurity information.
13. Develop a cyber career track for your agency.

Do you have a cyber emergency?
The Multi-State Information Sharing & Analysis Center has been designated by the U.S. Department of Homeland Security as the central resource for cyber threat prevention, protection, response and recovery for the nation's state, local, territorial and tribal (SLTT) governments as well as fusion centers. If you have a cybersecurity issue, call the MS-ISAC Cyber Operations Center 24 hours a day, 7 days a week at 1-866-787-4722. You can learn more at http://msisac.cisecurity.org/

WHO THEY ARE: THREAT GROUPS AND INDIVIDUALS

We will start by asking a simple question: Who is targeting law enforcement agencies and why? As you will learn, the threat groups and individuals are a diverse lot. They can include state and non-state actors, terrorists and hacktivists. They can even include law enforcement personnel, as we will explore later.

While not an exhaustive list, this section presents a brief overview of general threat groups covered in publicly reported cyber attacks. More extensive information can be found through the organizations listed in the guide's resource section.

Threat groups:

- Hacktivists
- State Actors
- Terrorist Organizations
- Criminal Organizations
- Purposeful or Accidental Insider
- 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 to all agencies – public and private – that hackers are very clever 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.

HACKTIVISTS

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[3].

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.

[3] http://www.huffingtonpost.com/2014/11/17/anonymous-kkk_n_6173332.html

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.

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.

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.

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 servers.

BEST PRACTICES: COUNTERING THE PURPOSEFUL INSIDER

Reduce risk related to the purposeful insider through:

- ✓ Extensive background checks for all employees and contractors
- ✓ 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

Lower the risk of the accidental insider through:

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

WHY THEY DO IT: MOTIVES

The motives behind cyber attacks range from revenge to notoriety. Here we cover a few of the most common.

Motives:

- Disabling Websites and Releasing Information
- Public Exposure of Private Information
- Espionage
- Interference with Police Operations and Sabotage
- Defacing to Cause Embarrassment or Retaliate
- Retribution
- Profit
- Notoriety
- Disinformation

DISABLING WEBSITES AND RELEASING INFORMATION

Denial of Service attacks are the techniques hackers generally use when aiming to take websites offline. These attacks generally fall into two categories. A Denial of Service (DoS) attack aims to take a website or other service offline by flooding a server with external requests that essentially exceed the bandwith capability and overwhelm the server. A Distributed Denial of Service Attack (DDoS) attack involves multiple requests coming from servers and computers often distributed around the globe. The sheer volume of a DDoS attack makes it much harder to recover from. This was the technique used by Anonymous in March 2014 against the Albuquerque Police Department in protest of the death of James Boyd; it was used again by a group claiming affiliation with Anonymous against the Saint Louis County Police in August in the wake of the shooting death of Michael Brown[4]. In that case, the group hacked a server and released police dispatch calls from the shooting and the name of a man they thought was the officer involved; as mentioned earlier, it wasn't and the wrong person was named and had his personal information circulated online. In May 2015, Anonymous hacked into the City of Madison's IT system in response to an officer-involved shooting. In a video posted after the attack, Anonymous incorporated officer-dispatch radio transmissions that it "liberated" during its hack.[5] The hack also slowed access to mobile data systems used by law enforcement, fire and emergency medical agencies across Dane County.

[4] http://www.cnet.com/news/st-louis-police-website-suffers-ddos-attack/
[5] http://www.wkow.com/story/28325831/2015/03/09/emergency-government-systems-in-dane-county-threatened-by-cyber-attack

PUBLIC EXPOSURE OF PRIVATE INFORMATION

A variation on this theme hits closer to home: Hackers have targeted databases kept by law enforcement agencies and professional associations and have released information ranging from officers' names and other personal details to the identities of informants[6]. In 2011, Anonymous targeted 70 mostly rural police departments in retaliation for the arrests of its sympathizers in the United States and the United Kingdom. Information related to investigations, citizens' tips, credit card numbers and e-mails sent and received by officers were leaked online. In May 2015, a hacktivist called AnonGhost defaced the website of the Wayne County Sheriff's Department and leaked employee log-in credentials[7].

ESPIONAGE

On the other end of the spectrum is the nation state or its proxy who secretly infiltrates systems in order to stealthily gather sensitive information – a form of espionage, as we covered earlier. An example of this is the breach of the U.S. Office of Personnel Management (OPM) systems in 2015, which resulted in the compromise of the identities and personal information of millions of federal workers, contractors and others who went through background investigations in order to obtain security clearances. That breach is believed to have been carried out by a nation state. Another example is the case of the Chinese military officer and hacker known as UglyGorilla, who infiltrated the computers of utilities on what officials believe is a surveillance mission aimed at finding information China could use during a cyberwar[8]. UglyGorilla's surveillance sorties were part of a broader Chinese-directed operation that, over the course of about seven months, targeted systems that control the electrical grid and water purification plants. Again, with the increasing interconnectedness of systems across the intelligence community and to state and local law enforcement agencies, comes an increased risk of being targeted in this manner.

INTERFERENCE WITH POLICE OPERATIONS AND SABOTAGE

This is perhaps the most serious and potentially life threatening of motives. Hackers can gain access to real-time information to interfere with or mislead law enforcement operations. In one scenario, they could infiltrate and tamper with Computer-Aided Dispatch (CAD) systems, 9-1-1 communications centers, and Record Management Systems (RMS) to misdirect resources or orchestrate the issuing of false orders. They could also create an entirely fictional scenario in these systems to drain or divert resources or to lure respondents into a trap. Hacking efforts can also simply have the goal of slowing down computers and jamming communications to make operations more difficult.

---

[6] http://www.cnet.com/news/antisec-hackers-post-stolen-police-data-as-revenge-for-arrests/
[7] https://www.hackread.com/wayne-county-sheriffs-dept-website-defaced/
[8] http://www.bloomberg.com/news/articles/2014-06-13/uglygorilla-hack-of-u-s-utility-exposes-cyberwar-threat

DEFACING TO CAUSE EMBARRASSMENT OR RETALIATE

Hackers have defaced law enforcement websites in order to cause the department public embarrassment, to make a statement or to retaliate after a police action.
In 2012, Anonymous retaliated against the Boston Police Department by defacing its website and alleging police brutality against Occupy Wall Street protestors[9].

RETRIBUTION

A disgruntled employee who has administrative access to a network, databases or other parts of the IT infrastructure can wreak havoc by denying access or purging data. An example of this is the case of Terry Childs, the then-network administrator for the City of San Francisco who was arrested in 2008 for computer tampering after he locked everyone out of the Fiber Wide Area Network (WAN) – the city's IT backbone – by changing administrative passwords to switches and routers and refusing to provide them.[10] This and similar stories speak to the danger of providing one person with "the keys to kingdom[11]" instead of having policies in place that create checks and balances for critical IT administrative functions.

PROFIT

An attack for profit aims to hold information or a system "hostage" until a ransom is paid to return information, restore a system, or provide a new password. A ransomware attack is one example of this. Criminal groups or others may also steal information from a system and sell it for a profit.
There is a potential market for any type of information available on a law enforcement system, from personnel records to case files. Anyone who has access to a system could potentially monetize, or sell, that access information.

NOTORIETY

Successfully executing an attack against a law enforcement entity can provide individuals or groups with notoriety and credibility in the hacker community. Even when it appears that an attack is related to a social movement, a hacker may just be piggybacking on media coverage in order to gain greater notoriety rather than in true support of the cause.

[9] http://www.huffingtonpost.com/2012/02/03/anonymous-boston-police-occupy-wall-street_n_1252718.html
[10] http://www.wired.com/2008/07/sf-city-charged/
[11] http://www.computerworld.com/article/2517653/security0/after-verdict--debate-rages-in-terry-childs-case.html?page=2

DISINFORMATION

Social media has emerged as a tool for sophisticated disinformation campaigns such as the one that Duval Arthur, head of the Office of Homeland Security and Emergency Preparedness in St. Parish, Louisiana woke up to one morning in 2015. A concerned citizen called him after receiving a text – purportedly from Arthur's office – that there was a large-scale chemical leak that morning. The story was completely false. Hacking into a department's social media accounts and posting incorrect or inflammatory information can interfere with department operations or stoke public outrage.

How They Do It: Tactics and Methods

Tactics are the strategies used to execute an attack or to hack into a system to achieve a specific aim. Methods are how they carry out the hack. Here we touch on some of them.

Tactic	Method
Denial of Service Attack: A Denial of Service (DoS) attack aims to disable a website or network so it 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 (PSAPs) 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 or websites that deploy the malware or let the hacker into the system. This often involves sending e-mails to employees' work addresses that contain an attached file and/or an embedded link. The e-mail 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 and devices. Once downloaded, the malware either causes immediate damage or quietly lurks in the background, serving as a backdoor that the hacker can use to access the system.
Deployment of Ransomware: Ransomware essentially locks a user or entire agency out of a network and forces the victim to pay a set sum to regain access.	This malicious software can attack specific files and/or make a network inaccessible until a ransom is paid. The person controlling the ransomware sets the terms, including the amount of the ransom and the deadline. If the ransom is not paid, the data are rendered irretrievable by the users until they are "unlocked" by the person behind the malware. Law enforcement agencies that have been targets of ransomware have tried to find ways around it, but, in the end, agencies have paid the ransom to regain access. Other agencies that have regularly backed up their data and systems have been able to restore their systems and files and avoid paying the ransom.
Deployment of Malware: Malicious software deployed onto a department's devices or network can: disable or alter operations; delete, gather, or alter information; track how people use the system; access or alter passwords; monitor all keystrokes and traffic; bog down the system; and provide misinformation to field or software operations.	Malware, which can be created from scratch by a hacker or found on an online hacker forum, can find its way onto a system through a variety of means, including being placed directly by a hacker or by an employee or contractor who unknowingly accesses an infected e-mail or website. The software can also avoid detection by making changes slowly or delaying deployment until long after it has infiltrated the system. When the malware uses this approach it can spread to many new and different department systems before it is finally detected. However, there is also malware that takes quick and decisive action and exacts great damage.

TACTIC	METHOD
Deployment of a Virus: A virus can slow down a system, delete information, corrupt or modify files.	Computer viruses enter a system through one device or network access point and infect multiple devices or servers across a network.
Deployment of a Worm: Like a virus, a worm can alter data and files.	Worms often enter a network by exploiting a weakness in the network or operating system. It takes a specially tailored tool to wipe it from a system and, even then, can take weeks or months to eradicate. Worms, which can be customized to target – or omit – certain networks and can self-replicate, can also provide backdoor access to their creators once in place. Unlike a virus, a worm does not need to attach itself to a program to replicate and spread itself throughout the network while remaining undetected. Worms can also "sit" in the network in a dormant state waiting to be activated on a particular date or by a particular command or function. Hackers have announced activation dates as a tactic to stoke fear.
Deployment of a Trojan Horse: Once in the network, a Trojan Horse program may simply provide backdoor access to a hacker seeking to access data or system information.	Just as the Greek Trojan Horse entered the gates of Troy as a stealth vessel of attack, so can a cyber Trojan 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 work very hard to appear routine and benign so that you will download them onto your computer. 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 exploits 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, which aggregate personal information, 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 about someone 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 pays people to carry out malicious attacks online.
Social Engineering: Social engineering involves manipulating or tricking people so	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

TACTIC	METHOD
they unknowingly divulge network information or provide access to networks.	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.
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 theme is a zero day vulnerability – a weakness in the software's original code that was not caught by the original developers – that can be exploited by hackers. 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 wireless communication (e.g., Wi-Fi, Bluetooth, ZigBee) 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 and 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 a law enforcement context, disrupt operations. A variant of this is signal hijacking, which is when a hacker(s) intercepts a signal and takes control of it.
Physical Disruption and Theft: This tactic involves both a physical and 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 not 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, tablets, smart phones, 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 STATE AND LOCAL LAW ENFORCEMENT AGENCIES

The list of cyber vulnerabilities for law enforcement agencies, as with most organizations, may well be limitless. Most organizations depend on information systems or devices during every step of their operations, and it will likely be only after an attack or an intrusion that the extent of that dependence really sinks in.

At the very least, it is important to understand that any device that connects to the Internet or operates on radio frequencies can be hacked: If it is connected, it is vulnerable. Any organization can be the target of a cyber attack. For a skilled hacker, all it takes to compromise an ENTIRE system is access to ONE device or individual.

Cyber Vulnerabilities:

- Personnel
- Organizational Barriers
- Information Networks and Systems
- Public-Facing Websites
- Data Storage Devices
- Social Media Accounts
- Communications Centers, Systems, Equipment and Applications
- Wireless Devices
- 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

Every organization is perennially vulnerable to the accidental insider, but not conducting regular cyber training across the organization greatly increases that vulnerability. Vulnerability also increases in the absence of clear policies on the use of technology, personal devices and accessing outside websites.

Finally, it is important for third-party vendors and contractors to maintain the same level of IT security as your organization, particularly if they are handling sensitive data.

Many government agencies are adopting practices where IT security requirements are written into contracts with its vendors and contractors. While that is a great measure to take, it is also important to include in the contract a way for you, as the government agency, to confirm and monitor adherence to those requirements.

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.

Organizations must also implement strong controls protecting and documenting access to the network and databases, have checks and balances in place when it comes to access and have clear policies regarding the use of portable storage devices.

ORGANIZATIONAL BARRIERS

Changing attitudes and behaviors toward cybersecurity is key to overcoming organizational barriers. This is the one area in which law enforcement agencies can make big changes without a lot of technical expertise.

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

Employees must all understand that their activities online either bolster or jeopardize cybersecurity efforts. Here are some ways to accomplish this.

- Provide regularly scheduled cyber-awareness training to the entire organization.
- 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.
- Ensure all employees know to whom they should report a suspected cyber incident.

Technical Personnel

Vulnerability stems from not having qualified and capable IT and cyber professionals integrated into the fabric of an organization. Without these professionals monitoring and reacting to cyber events, an agency will likely not be able to implement a comprehensive cybersecurity initiative. As you build your IT and cyber team, ensure that you put checks and balances in place so that they work as a team and there are no single points of failure. Positions to consider adding, include:

- Network administrator
- Cyber threat analyst
- Cyber forensics specialist

Establishing rewarding cyber-related career tracks – complete with promotional and training opportunities – is key to attracting the level of talent and skill your organization will need. Remember that you are competing with the private sector when it comes to recruitment. These positions must offer comparable salaries and recognition within your organization if you hope to attract qualified professionals. If you can't compete with the

private sector in terms of salaries, which is likely, then ensure that the cyber career tracks offers rewards in other forms such as the ability to innovate, to hold a job that "makes a difference" in terms of service to community and country and, as promotions occur, to be a respected member of the executive staff. Your organization may also have employees who are curious about how they can enter this field. Provide them with information on necessary qualifications and job responsibilities. You may find that some of your most talented and motivated cyber personnel already work for you in other capacities. For more information, refer to the Develop a Cyber Career Track for Your Agency entry in Section Two.

INFORMATION NETWORKS AND 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.*** That means including personal and department-issued equipment such as smartphones that infiltrate and exfiltrate data. *Everything should be included in the city or county assessment process and put on the map.* In the event your agency experiences a serious breach, that assessment of the entire network, or IT ecosystem that you are one part of, will be one of the first items needed in the investigation. Also consider finding an outside vendor to conduct a penetration test (also referred to as a pen test) to find vulnerabilities in your network.

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. This vetting involves having a programmer go through every line of code *before* the

software is used to make sure there are no hidden back doors or malware. This third-party review is provided by government entities such as US CERT, which you can find in the resource section at the end of this document, and by some universities.

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

GATEWAY TO NATIONAL SECURITY INFORMATION

For some hackers, the real value of accessing a state or local law enforcement agency's system may be in the potential to access federal systems with national security information. Accessing law enforcement systems can help hackers to accomplish the following:

- Plant keylogger software to collect passwords to Federal systems
- Access e-mail correspondence with Federal personnel for system access clues
- Find personal information to recruit insiders
- Access federal intelligence products to fill gaps in operational plans while searching for final key to Federal systems

Tip: Be aware of broader motives of hackers and look for connections to larger plots when your agency has been attacked or hacked. Fusion centers are a good place to turn to for that kind of strategic information.

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 Systems

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. Even a website only used for informational purposes can be hacked and defaced in order to make a statement, particularly if the police department is involved in a controversial incident. Assessing the following will help to identify technical vulnerabilities:

- Internal or external hosting
- Website hosting and security configuration
- Relationship of 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[12]. 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. Review how these are used in your department and include them in your assessment and your policies. What are employees taking out and putting on their personal devices? What security measures do they have in place on those personal devices to protect the information if those devices or lost, stolen or hacked?

Here are some that are used on a daily basis:

- Thumb Drives
- Internal and External Hard Drives
- Servers
- CDs/DVDs
- Printers and Copiers
- Computers and Laptops
- Smartphones (Department-issued and personal)

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.

[12] http://www.cnet.com/news/stuxnet-delivered-to-iranian-nuclear-plant-on-thumb-drive/

COMMUNICATIONS 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. These run the gamut from night vision gear, which uses thermal-infrared (IR) imaging, to remote controls, which use IR data transmission.

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

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.

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

Section Two: What Agencies Do

This section presents steps that law enforcement agencies can take to improve their cybersecurity immediately.

What Agencies Can Do to Integrate Cybersecurity into the Whole Enterprise

1. Make cybersecurity a priority for the entire organization
2. Make a case for funding
3. Identify and connect with the entity responsible for your cybersecurity
4. Designate a cybersecurity contact within your agency
5. Identify points of contact and formalize partnerships within your city/county, with federal agencies, with your fusion center and with the private sector
6. Conduct a cyber threat assessment
7. Provide cyber-awareness training
8. Establish and maintain executive support for cybersecurity
9. Develop and follow a cybersecurity maintenance plan
10. Develop a cyber response and recovery plan
11. Conduct organization-wide cyber exercises
12. Share cybersecurity information within your organization and with external partners
13. Develop a cybersecurity career track for your agency

Breaking it down

1. Make Cybersecurity a Priority for the Entire Organization

How can cybersecurity make it to the top of your agency's list with so many competing priorities? The case for cybersecurity hinges on the fact that nearly all of your agency's other operations rely on a healthy and functioning network. This also touches directly on officer safety, a top priority for any law enforcement agency. Making cybersecurity a priority for your agency is very much like installing locks on the windows and doors. At its core, it's that basic in terms of its criticality. It is the unseen foundation for most other law enforcement functions.

2. Make a Case for Funding

It may seem curious to include this as the second item on the list, but identifying a funding stream takes time. Start by identifying existing sources and work from there by advocating for new streams, whether through grants, line-item funding, or other creative approaches that might be proposed to industry. Technology investments are expensive and the rate at which technology becomes outdated and vulnerable to threats means there will be ongoing funding requirements. Make sure that you know what those costs will be months and even years down the line. Ultimately, if those funding streams don't exist now, law enforcement executives may need to start raising the issue and providing briefings to grantmakers, legislators and others on the urgency of the situation.

3. Identify and Connect with the Entity Responsible for Your Cybersecurity

Establishing a relationship with the entity responsible for your agency's cybersecurity is best done *before* a cyber event. Regardless of who controls your agency's cyber infrastructure, ensure that the following exist and are created and regularly updated:

- Threat, vulnerability and risk assessment
- Cybersecurity maintenance plan
  - Regularly update contact lists
- Cyber response and recovery plan
- Suspicious activity reporting
- Cybersecurity messaging and crisis communications plans
  - Executive Messaging Plan (internal to employees, external to media/public)
  - Development of Common Terminology for Use in Briefings and with Regional Partners
- Cyber personnel management plan
  - Background check requirements for cyber personnel
  - IT training plan for cyber personnel
  - Human resources plan for managing access rights for all IT personnel, including at-risk personnel
  - Career track plan for cyber personnel

4. Designate a Cybersecurity Contact

This does not need to be a person with cyber expertise; rather, find someone who is suitable for a liaison role and keen to learn – and keep learning – about cybersecurity. Ideally, he or she will have some technological knowledge but this person will primarily serve as the central contact in your agency for all things cyber. Anyone in the agency should be able to contact this person with any suspicions or concerns. This will be the person to contact for cyber "roadside assistance."

MAKING THE CASE FOR CYBER FUNDING

Here are a few approaches that agencies have used to secure funding.

Demonstration Project
Develop a demonstration project that lasts a set amount of time (e.g., three months, six months, 12 months) and gives you the performance metrics you need to make your case for more funding. This approach can work in a number of scenarios, including hiring cyber analysts, subscribing to a real-time monitoring solution or updating the network architecture.

Reducing Risk
Conduct a cyber threat assessment to demonstrate the risk that is faced by your agency and your city/county network. This assessment will help you communicate both the cyber threat and the potential consequences of an attack or intrusion. Present a list of priorities for reducing risk with details on the costs, benefits and timeframe for implementation.

Case Studies
Look to the success stories of other agencies that have implemented the ideas you are proposing. Compile as many examples as you can with supporting facts and figures.

Tip: Develop a case for the ongoing funding of your cybersecurity effort by backing it with hard facts about vulnerabilities at your specific agency and what is at risk if nothing is done.

Depending on the size and capabilities of your agency you may have the ability to have more than one person responsible for cyber to address different cyber components:

- Cybersecurity
- Information technology
- Cybercrime
- Cyber investigations
- Cyber analysis and information sharing

5. Identify POCs and Formalize Partnerships

No matter the needs or location of your agency, there are resources out there for you. First, identify all of the potential partners in your area and begin your outreach effort. As you proceed, you will uncover new partners and can reach out to them. This cycle will likely continue for many months as you fully explore all that your region has to offer. Partnerships are a two-way street: You receive benefits from partners and they from you. Think of these as collaborative relationships and consider what you can offer. As a law enforcement agency you may be able to include these groups in your information sharing loops. You may also serve as a conduit for them to other federal law enforcement resources. Eventually, once your agency has invested in developing a cyber investigative capability, you can directly support cybercrime investigations. For your public sector counterparts you can lend radios, personnel, and other resources to be supportive. Also consider offering and asking for: site tours; informative briefings, or introductions to other partners. These actions will increase the visibility of your cyber unit, which will ultimately help you to attract more partnerships.

A likely benefit of this effort will be that more formalized relationships can emerge. This can translate into the formation of an association, a working group, or even a formalized mutual aid agreement or Memorandum of Understanding (MOU). These legal agreements, set in place *before* a cyber event, mean a shorter response and recovery time for all involved.

As you identify potential partners in your area, consider the following possible outlets:

- **IT Departments** – These can be internal, city, county or multi-agency departments. These are the organizations that directly provide IT products and services to your law enforcement agency. There may be more than one of them, so make sure all are included. Also consider that there may be sources of support in one agency that are not available in another. Tap into those, if you can.
- **Fusion Centers** – The intelligence fusion centers can provide access to federal cyber resources, and in some cases they have resources to support your agency directly. Each fusion center has different capabilities so ask them to provide you with a briefing on the support they can offer. The National Fusion Center Association also has a number of initiatives to support the cyber efforts of the fusion centers.
- **Federal Offices** – Contact the local office of the Federal Bureau of Investigation or Secret Service. They can provide direct support or serve as a conduit to support from the national offices.
- **Other Law Enforcement Agencies** – Contact the cyber leads at neighboring state, county, and local law enforcement agencies. In the absence of a formal cyber lead, try to find someone in the organization with existing cyber or technology roles (e.g., systems administrator, cyber investigations, cyber forensics). Call on your agency leadership to help you make those connections and to loop in executive participation from the beginning. Consider partnering with other local law enforcement agencies to reroute calls for service or to provide back-up when communications and services are interrupted during a cyber attack. Formalize those mutually supportive partnerships with MOUs.

- **Other Public Safety and Government Agencies** – Think about utility providers, emergency managers and others from the critical infrastructure arena with a vested interest in cybersecurity.
- **Communications Centers** – These merit special attention because these centers, including Public Safety Answering Points (PSAPs) and dispatch centers, are increasingly vulnerable to cyber attacks. While they may or may not be directly operated by a law enforcement agency, law enforcement operations certainly rely on these centers running without any disruptions.
- **Associations** – Associations can give you more return than just approaching companies or other organizations one-by-one. They also offer educational events, technology briefings and demonstrations, purchasing collaboratives, networking opportunities, a resource for finding subject matter experts, an environment for developing and exercising response plans, and an incident support network. If you do not find the type of association you are looking for, consider starting one on your own. The following types of associations are worth investigating:
    - Law enforcement IT professionals
    - Public sector IT professionals
    - Private sector IT professionals
    - Critical infrastructure owners, operators, and technology professionals
    - Chief Information Officers
- **Technology Companies** – Reaching out to the private sector will educate you on available technologies and services and will help you get a clearer picture of the required level of investment. Comparing multiple offerings in the same space will help you to assess your options.
- **Critical Infrastructure** – These organizations know the importance of cybersecurity perhaps more than more than most. Find opportunities to connect with them and learn from their experiences.
- **Academia** – Your local universities may provide opportunities such as:
    - Partnering on cybersecurity-related research
    - Providing cybersecurity classes
    - Participating in working groups
    - Identifying subject matter experts
    - Speaking at educational presentations and briefings

It may be helpful to consider developing partnerships in different categories: education, response, recovery, investigation, intrusion detection, operational support, and mutual aid.

6. Conduct a Cyber Threat Assessment

The Department of Homeland Security's National Cybersecurity and Communications Integration Center (NCCIC) will conduct an assessment for free. The results of this assessment are presented in an easy-to-read score sheet format that clearly conveys the areas of greatest vulnerability. This is especially helpful for agencies that don't have the resources or expertise to do this on their own.

To complement the DHS assessment, your agency can also use an established assessment process, like the National Institute of Standards and Technology (NIST) Cybersecurity Framework, to conduct your own. You can also blend the two – ask DHS to assess while you conduct your own assessment.

A third option is to hire a private company that has extensive experience in this type of work. The investment in this service might have a greater return after going through the government-sponsored assessment process. The DHS process will give you a greater exposure and familiarity with the assessment process so you will be in a better position to take advantage of what a private company can offer. It will also help you to understand the level of service you need from a private provider. Remember to consider the (pen test) we mentioned before to find weaknesses an attacker could exploit.

The assessment process typically includes quantifying and qualifying the following:

- Cyber personnel (e.g., capabilities, training, management, established career track, addressing at-risk personnel)
- Personnel (i.e., awareness-level training completion rates, background checks)
- Agency policies (e.g., technology use policies)
- Physical security
- Organization planning (e.g, cyber maintenance, response, and mitigation plans)
- System design

A comprehensive assessment should also include the following:

- An inventory of each and every device that is connected to your network, whether it be department-owned or personal (What are they? Where are they? Who has access?)
- An inventory of third parties that have access to your network (Who are they? What level of access do they have? What are their cybersecurity practices?)

As part of your assessment, the cybersecurity practices of vendors whose systems interface with the police department's and who manage sensitive data should be evaluated. Ultimately, law enforcement agencies are responsible for the data they produce and are entrusted to securely store them – whether this is done in-house or through a vendor. The vendors to include in your assessment range from companies that provide building access and control services such as heating and air conditioning to vendors that provide the department with data management services. The department and, by extension, the city or county that negotiates and approves its contracts, should ensure that stringent cybersecurity practices be contractually required of vendors. It should also be specified in the contract that those cybersecurity practices extend to any subcontractors those vendors use.

Once the assessment is completed, there is an important step to take as you continue to brief executives and build the case for ongoing funding: What is the potential loss of a major cyber attack? While loss is traditionally calculated in monetary terms, for law enforcement the calculus extends beyond that to response times, the ability to provide

critical services and, for a major event, risk of injury to officers and civilians. Your assessment(s) will give you the information you need to paint a clear picture of the threat. Your goal will be to take that and overlay the bottom line – what is at stake. While we won't cover it in this guide, it should be noted that several of the major insurance companies are now offering cybersecurity insurance.

7. Provide Cyber-Awareness Training

Every employee of your organization must be trained on basic cybersecurity practices. *This is the single most important thing you can do for your organization.* Cybersecurity practices that are practiced by all, include: changing passwords regularly; backing up computers and other devices regularly; adhering to security protocols when using personal devices that contain work-related material or that connect to the department's network; and a host of other practices that should be ingrained into your workforce through regular training, daily practice and regularly scheduled cyber exercises.

Keep your agency's employees engaged and alert by conducting regular, internal spear phishing campaigns or regularly distributing cyber awareness bulletins between more formal training sessions. Ensure that the training provides awareness information *and* easy-to-follow cybersecurity practices that they can adopt on a daily basis.

There may be existing online training that covers the following:

- Reducing cyber risk
  - Public website browsing guidelines
  - Password management practices
- Managing social media
  - How to change social media settings to protect privacy
  - How to limit publicly viewable connections with law enforcement community
  - How to reduce likelihood of being targeted
  - How to create a private alias identity
  - Maintaining your personal network of contacts – good vs. bad contacts
  - Online comments and content guidelines
- Awareness of cyber threats and vulnerabilities
- Warning signs
  - Recognizing phishing attempts and other malicious activities
  - Identifying suspicious activities

You may want to supplement pre-packaged awareness-level training with the following:

- Who to report suspicious activity to within your agency and the importance of reporting things early, even if they just "think" there might be something amiss
- Who to call for cyber "roadside assistance"
- How to follow agency's policies for the use of:
  - Private devices
  - Public websites from government devices
  - Government websites from private devices

In addition to the organization-wide training, more in-depth training can be considered for: executives, traditional investigators; cyber investigators; crime and intelligence analysts; cyber analysts; and information technology personnel.

8. Establish and Maintain Executive Support

As we've emphasized, while cybersecurity may have previously been seen as an IT issue, it is now an organization's issue. Trying to instill this cultural change and understanding will require establishing and maintaining executive support and leadership. To start down this path, set up an initial executive training or briefing session to provide the background information needed to create executive-level understanding of the issues. The briefing can tailor many of the topics addressed in this guide to your specific agency situation, including:

- Cybersecurity overview
  - Threats, vulnerabilities, risks, consequences
  - Case studies
- Agency cybersecurity status
  - Known agency-specific threats, vulnerabilities, risks
  - Current management and responsibility for agency IT and cybersecurity
  - In-house cyber resources
  - Existing cyber maintenance, response and recovery plans
- Federal partner briefings
- Prioritized next steps
  - Providing organization-wide training
  - Conducting assessments
  - Developing maintenance, response and recovery plans
  - Prioritizing current and future IT investments

A follow-up executive cyber briefing should be scheduled for 10 minutes once a week to provide leadership with updates on threat information and any planning or resource needs. You can also develop a one-pager to leave behind with updated cyber statistics. Statistics to collect can include the number of: suspected, attempted and successful intrusions; thwarted intrusions; ongoing cyber investigations; suspicious cyber activity reports; loss of services; and estimated "costs" of losses communicated in either monetary terms or in terms of potential loss in service or compromised, sensitive information. Regular briefings from federal partners can also be incorporated into these or other updates.

In the end, it often helps to provide real-world examples of what is happening to the agency or similar agencies to make cyber more understandable. The briefing can be provided by the agency's cyber lead, the IT administrator, or a combination of the two.

It may be easiest to deliver the cybersecurity message by relating it to the physical security world that is already so familiar to law enforcement. Imagine that a computer network is a house. Think about what kind of a neighborhood surrounds the house and whether it is a good or bad neighborhood. Now consider the vulnerabilities of the security of the house, which depend on whether there are locks on the doors, bars on the windows, or a security system. Lastly, think about the potential consequences of a breach if the house contains jewels, firearms, or even a family.

Consider how law enforcement officers will do their difficult job when their private information, including details about their family or children, or information on their status as an undercover officer is compromised and out there for bad guys to see. Now lives are at risk and officers will second guess their safety on the job. There is an expectation that the personal information contained in systems will be protected. This may be the easiest way to convey the seriousness of the cybersecurity issue in real-world terms.

Your agency will need to make some big commitments to fully embrace cybersecurity across the enterprise – a process that include investments in technology, training and personnel. Providing executives with the information they need to understand this issue will help them to make cybersecurity, and the associated commitments, a priority.

9. Develop and Follow a Cybersecurity Maintenance Plan

A cybersecurity maintenance plan is a document that details how your agency is going to devote resources to cybersecurity on an ongoing basis. The plan should address the following:

- Collecting and monitoring of IT activity logs
- Regular data backups
- Regular "patching" of software and reports of such activity
- System recovery files
- Software updates
- Training
- Personnel
- Real-time monitoring
- Domain Name System (DNS) log scanning

The maintenance plan should include a regular schedule for conducting all of the maintenance activities. There should also be a way to track when maintenance has been performed and for that information to be available for review by leadership at any point.

10. Develop a Cyber Response and Recovery Plan

By this point you will have done the cyber assessment and the outreach to find a network of supportive partners. Now is the time to develop the plan that details how your agency will respond to and recover from a cyber incident. The response and recovery plan addresses what to do from the time a suspicious activity is reported to when an intrusion has been thwarted and full capabilities have been restored.

The following are components of response and recovery:

- **Initial Assessment**
  - Detail how suspicious activity is reported or detected and encourage people to report things early, even if they just "think" there might be something amiss
  - Determine if there is an incident and detail the criteria for doing so
  - Alert your IT and cyber team using a 24-hour emergency contact list that is regularly checked and updated
  - Clearly outline the notification chain in an organization once a verified incident has occurred
    - IT personnel, including systems administrator(s) and vendors
    - Investigative units, including cyber investigators, cyber intelligence analysts, cyber forensics specialists
    - Contracted support, if relevant
    - Command staff
    - Media relations (if systems are taken offline)
  - Request outside resources
    - Federal partners
    - Fusion center
    - Private sector resources
  - Alert your information sharing partners
  - Enter incident into reporting systems and report to federal and state authorities
  - Identify the extent of the intrusion/attack
  - Determine the criticality of the system impacted
  - Assess what kind of attack/attacker this could be
  - Gather logs along the way (e.g. access, firewall, Intrusion Detection/Prevention Systems-IDS/PS, mail)
  - Gather as much information as possible from your team and your partners
  - ***Document everything and create forensic images***

Develop a preliminary communications plan that includes both communication to employees and communication to the media and general public

- Develop the narrative for the event and ensure that all potential spokespeople know what it is and use it
- Determine who the spokesperson/spokespeople will be
- Determine in advance what internal methods of communication will be used in different scenarios (e.g. e-mail compromised, department's social media accounts compromised, website compromised)
- Determine the different ways information will be disseminated to the media and to the public
  - Social media, including Twitter and Facebook
  - Traditional news conferences and press releases
  - Text messages
- Determine how much information will be released about extent of the attack
- Build in notifications to officers/employees whose information, including home addresses, may have been compromised
- In the case of a serious breach of, for example, confidential informant (CI) information, develop a plan ahead of time on how to quickly notify the CIs' handlers and, possibly, the CIs themselves
- Build in a regular schedule for updates of information so your agency drives the narrative of the attack and there are no extensive lags between updates, even in the absence of new information

- **Mitigation**
  - Determine what to do to limit further spread/damage
  - Determine if the system can be taken offline and if the capabilities can be transferred to a supporting partner agency
    - Take sensitive systems, including those with case and CI information, offline while this is being assessed
    - Take systems shared with other law enforcement partners, such as the District Attorney's Office, offline while this is being assessed
  - Prioritize which systems to address
  - Gather logs along the way (e.g. access, firewall, Intrusion Detection/Prevention Systems-IDS/PS, mail)
  - Gather as much additional information as possible
  - Refine the communications plan
  - ***Document everything and create forensic images***
- **Recovery**
  - Gather logs along the way (e.g. access, firewall, Intrusion Detection/Prevention Systems-IDS/PS, mail)
  - Gather as much information as possible
  - Prioritize which systems to bring back online
  - Implement the communications plan
  - ***Document everything and create forensic images***

- **Investigation**
  - Gather logs along the way (e.g. access, firewall, Intrusion Detection/Prevention Systems-IDS/PS, mail)
  - Gather as much additional information as possible
  - Ensure that your communications plan supports your investigative strategy
  - ***Document everything and create forensic images***

There may be some debate over whether the criminal investigation needs to take precedence over mitigation activities, but both can be conducted in concert. There are steps that can be taken to preserve information for the investigation while still mitigating the effects of the incident. Keep detailed logs, notes, and forensic images all along the way.

It may also be helpful to think of cyber response in terms of the steps that are usually taken in battlefield triage as presented in the table below.

4 Steps of Battlefield Triage Used in Cyber Response[13]

Battlefield Triage	Cyber Response
Stop the Bleeding	**Stop the Spread (malware or otherwise):** prevent attack from gaining ground, maybe pull system(s) offline, determine how access was gained
Start the Breathing	**Start Essential Services:** make forensic image of affected machine(s), have a backup, restore from backup
Protect the Wound	**Protect from Future Attacks:** patch systems to avoid same issue, change your passwords, use an intrusion prevention system (IPS) or firewall
Treat for Shock	**Investigate:** keep channels of communication open, both within the organization and with outside entities, partner with others to get the resources you need

11. Conduct Organization-Wide Cyber Exercises

As with any other public safety plan, the cyber response and recovery plan needs to be exercised *often* and with all potential participants and partners. After a new plan is developed it may take multiple back-to-back exercises to iron out all of the details. Inevitably, there are things that will go wrong and plans will need several revisions before they work as they should. It is important for all involved to understand ahead of time that there will be bumps in the road but that is what exercises are designed to undercover. The objective is to recognize your plan's weak spots in an exercise rather than during a real incident. To borrow the oft-cited military quotation, "The more you sweat in peace, the less you bleed in war." The same principle holds true here. Practice and practice some more until your plan works and people know what to do in different scenarios. The one guarantee is that no matter how much planning and exercising takes

[13] Based on the model developed by Cecily Garcia and Rebekah Brown, both members of the Cybersecurity Working Group referenced at the start of the document.

place, there will still be unanticipated events and consequences. The plans can be designed to accommodate those eventualities and the exercises can test the resilience of the plan and the team.

Once the initial rounds of exercises are completed and the plan is in place, exercises can be conducted on a semi-annual or annual basis. Participants in the exercises should include all partners that have any chance of being involved in an incident or providing support.

Consider taking advantage of the Federal Emergency Management Agency's (FEMA) exercise planning and evaluation offerings. With their nationwide exposure, they may already have exercises designed that can be adapted to fit your needs. They can also serve as a valuable and objective resource for evaluation of the exercises and, by proxy, the plan.

12. Share and Consume Cybersecurity Information

Information sharing on cyber threats and best practices should be a top priority within your own agency. It should also be a major component of your relationship with your partners. Sharing with them will help to make everyone in your region more informed and prepared. It will also encourage them to share information with you. Much of the cyber information you see developed within your agency will be valuable to your partners, including:

- Threat information
- Technical details on malicious software and actors
- Information on upcoming training and exercises
- Best practice updates
- Cyber intelligence products developed in-house

You can package this information into the following products for distribution within your agency and to your core partners in fusion centers, law enforcement, and other public safety agencies:

- Regular Cyber Bulletins – These will maintain organization-wide awareness and vigilance and reemphasize points presented in trainings (i.e., not clicking on e-mails from banks). These can include awareness information, case studies and profiles of key cybersecurity figures in your organization and region. The more you can put a face on this issue and humanize it, the more effective your messaging will be.

FUSION CENTERS

Fusion centers are increasing their cyber expertise. Turn to them for:

- Cyber Quarterly: Sign up to receive their cyber intelligence products. Some are tailored to issues in your region; others are national in scope.
- Cyber Intelligence Network: This is a relatively new effort established by the National Fusion Center Association that encourages real-time information sharing on cyber incidents.
- Real-Time Monitoring: While they may not be able to provide this service, fusion centers may have some best practices to share.
- Risk Assessments: If a fusion center does not offer this it can direct you to a federal provider.
- Conduit to Federal Resources: Fusion centers are often co-located with federal agencies. Most fusion centers also have DHS and other federal staff assigned to the center and can provide direction on available federal resources.

Tip: In addition to these resources, ask your fusion center about their cyber analytic support.

- Alerts – These can heighten attention when there are credible threats against the agency or when there are large-scale intrusions in any industry. Their purpose is to advise personnel to take extra care in opening e-mails and clicking links.
- Intelligence Products – These can be developed as time permits to address a cyber topic in greater depth. Alternatively, it is also possible to draft public versions of sensitive documents working in conjunction with the fusion centers or federal agencies that originally authored them.

To increase the amount and quality of information received by your agency sign up to receive as many information resources as possible through your partner network. Over time it may make sense to only continue to request the most valuable resources in order to prevent being overwhelmed with information.

13. Develop a Cyber Career Track for Your Agency

As with any cultural shift in law enforcement, cybersecurity requires the funding and will of leadership to create new positions and a career track in support of the efforts detailed in this guide. The knowledge base required to understand the cyber threats to your agency is wide and deep and must be developed over time. The same goes for the skills required to respond to those threats, accurately brief executives, work with a broad range of partners and maintain this function. Once you orient your agency to the cybersecurity mission, it is time to find, select and train the right people to support it. A first step can be doing an IT skills assessment in the department.

Here are some general guidelines for parsing out the roles involved:

Network Security – This is the responsibility of a dedicated IT team that works closely with your chosen cyber lead at the police department. This team of civilians trained in cybersecurity is responsible for mapping out the department's network and all of its access points, cataloging and prioritizing all of the department's IT assets, upgrading and updating those assets and software, regularly conducting penetration tests (or working with a vendor to do so) and providing detailed logs of all intrusion attempts, both successful and unsuccessful. The team should also be the one that the department's employees work with when there is a suspected cyber incident. Given their critical role, every member of the team should be vetted to the same extent as their law enforcement counterparts. Checks and balances in terms of who controls access must also be in place. *No one person, even the Chief Information Security Officer (CISO), should ever be the sole holder of the keys to the kingdom*; access control must be a responsibility spread among the team so that there is no potential for a single point of failure. Most cities and counties have IT teams already established so there is no need to create these from scratch. However, there is a need to ensure that the IT team incorporates best practices such as the checks and balances and supports the overall cybersecurity mission by conducting the activities detailed here.

CYBER ANALYST

A cyber analyst can play a key role in your agency's cyber team. The analyst's responsibilities include keeping tabs of cyber threats through methods including reviewing reports and other products produced by the Intelligence Community (IC), working with your agency's IT team to conduct threat assessments and brief decision makers and analyzing data to understand threats specific to your agency.

Additional responsibilities can include:

- **Suspicious Activity Reports** – Receive and follow up on reports of suspicious activities in the cyber realm.
- **Executive Briefings** – Brief executives at your agency and others.
- **Planning** – Contribute expertise to agency cyber planning efforts.
- **Training** – Coordinate and participate in agency-wide training.
- **Exercises** – Support the development, coordination and evaluation of cyber exercises.
- **Develop Peer-Reviewed Cyber Intelligence Products** – Develop these internally and with partners.
- **Share Information** – Distribute information, resources, and threat alerts within the agency and to partners.
- **Shake Hands** – Identify and create opportunities for partnerships.

Tip: Hire a cyber analyst to increase your agency's in-house expertise, build a trained cyber team, and provide a direct link for partnerships in the broader law enforcement and intelligence communities.

Cybersecurity Liaison – This is your cyber lead and is a position most likely filled by a sworn officer. Ideally, this person is relatively fluent in using technology but does not necessarily have to have any formal training in network security. Part of creating the career path is providing access to the training to support that position's professional development over time. The one indispensible trait that we recommend in this person is curiosity and the desire to learn about cybersecurity. As we mentioned before, the knowledge base is wide and deep and takes time to grow. This position – and the people who are selected for it – must be allowed a certain amount of time in the post before they are rotated out. If and when that times comes, establish processes from the start that enable the outgoing liaison to provide the incoming person with all contacts, key documents and progress reports on ongoing initiatives.
If your department can't spare someone full-time, start with a half-time position and expand that as the need arises. In the event of a major breach, it is likely that your department will work closely with a federal agency to investigate.

The liaison will be one of the main coordinators, facilitating communication between the command staff, detectives and the federal agency.

Cyber Analyst – This civilian analyst is an expert on cyber intelligence analysis and operations and can contribute to the network forensics work of the IT department in the event of a breach. A full-time employee, this person also coordinates with the fusion centers, analysts at other departments, the IT department and the range of public and private partners. The analyst and cyber liaison work together regularly to create products for training and briefing purposes. In the event of a serious breach, this analyst works with the detectives tasked with investigating the crime, the cyber liaison, the IT department, the fusion center and any federal agency that may assist.

Detectives – Given the prevalence of crimes facilitated by the Internet, detectives trained in cybercrime investigation and forensic cybersecurity methods, including how to collect and preserve evidence for prosecution, are an asset to any department. There are a number of good training resources outlined in the following section that all of your key cybersecurity personnel can take advantage of. Ensure that your detectives understand the federal and state laws guiding cyber investigations and the collection of private information.

Once you have established these roles in your organization, it is important to provide a road map for each that shows how those roles grow and expand over time. This can be done in a professional development guide for cybersecurity that defines what each role is and the minimum level of training and qualifications for each. Without hope of advancement in a promotion-based culture, it is unlikely you will attract the most qualified people for these posts. To successfully integrate into the law enforcement culture, cybersecurity expertise – like other specialized skill sets that are critical to the law enforcement mission – should be acknowledged and rewarded in the promotional process.

Section Three: Resources

Organizations

*The asterisk at the start of descriptions of organizations indicates they were pulled directly from their websites and published here in their original, verbatim form. Where descriptions were not available, as in the case of password-protected portals, a one- or two-line description has been written by us.

Federal

Federal Bureau of Investigation

Criminal Justice Information Services (CJIS)

https://www.fbi.gov/about-us/cjis

The FBI's Criminal Justice Information Services Division offers a variety of services, including crime statistics, fingerprints and other biometrics, the Law Enforcement Enterprise Portal, the National Data Exchange, Identity History Summary Checks, the National Instant Criminal Background Check System and the National Crime Information Center, which is described in this section.

The CJIS Division also offers the CJIS Security Policy, which "provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of [Criminal Justice Information]." The policy, which was updated in October 2015 with input from the criminal justice community across the country, can be found here:

https://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center

National Crime Information Center (NCIC)

https://www.fbi.gov/about-us/cjis/ncic

*Criminal justice agencies enter records into NCIC that are accessible to law enforcement agencies nationwide. For example, a law enforcement officer can search NCIC during a traffic stop to determine if the vehicle in question is stolen or if the driver is wanted by law enforcement. The system responds instantly. However, a positive response from NCIC is not probable cause for an officer to take action. NCIC policy requires the inquiring agency to make contact with the entering agency to verify the information is accurate and up-to-date. Once the record is confirmed, the inquiring agency may take action to arrest a fugitive, return a missing person, charge a subject with violation of a protection order, or recover stolen property.

The NCIC database currently consists of 21 files. There are seven property files containing records of stolen articles, boats, guns, license plates, parts, securities, and vehicles. There are 14 persons files, including: Supervised Release; National Sex Offender Registry; Foreign Fugitive; Immigration Violator; Missing Person; Protection Order; Unidentified Person; Protective Interest; Gang; Known or Appropriately Suspected

Terrorist; Wanted Person; Identity Theft; Violent Person; and National Instant Criminal Background Check System (NICS) Denied Transaction.

National Cyber Investigative Joint Task Force (NCIJT)

http://www.fbi.gov/about-us/investigate/cyber/ncijtf

*In 2008, the U.S. President mandated the NCIJTF to be the focal point for all government agencies to coordinate, integrate, and share information related to all domestic cyber threat investigations. The FBI is responsible for developing and supporting the joint task force, which includes 19 intelligence agencies and law enforcement, working side by side to identify key players and schemes. Its goal is to predict and prevent what's on the horizon and to pursue the enterprises behind cyber attacks. Cyber Fellow Program – This is an FBI program available to state and local law enforcement through the NCIJTF.

Cyber Task Forces (CTFs)

http://www.fbi.gov/about-us/investigate/cyber/cyber-task-forces-building-alliances-to-improve-the-nations-cybersecurity-1

*While national-level coordination is important to securing the nation, teamwork at the local level is also essential. After more than a decade of combating cybercrime through a nationwide network of interagency task forces, the FBI has evolved its Cyber Task Forces (CTFs) in all 56 field offices to focus exclusively on cybersecurity threats. In addition to key law enforcement and homeland security agencies at the state and local level, each CTF partners many of the federal agencies that participate in the NCIJTF at the headquarters level. This promotes effective collaboration and deconfliction of efforts at both the local and national level.

Cyber Shield's iGuardian

http://www.fbi.gov/stats-services/iguardian

*The iGuardian portal is an evolution of eGuardian, the platform through which the FBI's law enforcement partners provide potential terrorism-related threats and suspicious activity reports. While eGuardian enlists law enforcement users, iGuardian was developed specifically for partners within critical telecommunications, defense, banking and finance, and energy infrastructure sectors and is available over the sensitive but unclassified InfraGard network. … As iGuardian yields an important, additional source of relevant cyber intrusion information, it also lends focus to a big-picture view of the threat posed by terrorists, nation-states, and criminal groups conducting network operations against the U.S. Creating this broad base of threat awareness and partnership is all-important to the FBI cyber mission.

FBI Virtual Academy

https://fbiva.fbiacademy.edu/BETS/Login.aspx?ReturnUrl=%2fBETS%2f

This portal offers registered users online training on topics related to cybersecurity.

The Internet Crime Complaint Center (IC3)

http://www.ic3.gov/default.aspx

*The mission of the Internet Crime Complaint Center is to provide the public with a reliable and convenient reporting mechanism to submit information to the Federal Bureau of Investigation concerning suspected Internet-facilitated criminal activity and to develop effective alliances with law enforcement and industry partners. Information is analyzed and disseminated for investigative and intelligence purposes to law enforcement and for public awareness.

The Internet Crime Complaint Center (IC3) is a partnership between the FBI and the National White Collar Crime Center, serving as a vehicle to receive, develop, and refer criminal complaints regarding the rapidly expanding arena of cybercrime. IC3 was intended to serve and continues to emphasize serving the broader law enforcement community, including federal, state, and local agencies, which employ key participants in the growing number of Cyber Crime Task Forces.

Resource

- **Law Enforcement Cyber Incident Reporting Fact Sheet -** http://www.fbi.gov/about-us/investigate/cyber/law-enforcement-cyber-incident-reporting

U.S. SECRET SERVICE

Electronic Crimes Task Forces (ECTF) and Working Groups (ECWG)

http://www.dhs.gov/sites/default/files/publications/USSS%20Electronic%20Crimes%20Task%20Force.pdf

*… [T]he USSS developed a new body, the Electronic Crimes Task Force (ECTF), to increase the resources, skills and vision by which State, local, and federal law enforcement agencies team with prosecutors, private industry and academia to fully maximize what each has to offer in an effort to combat criminal activity. The common purpose is the prevention, detection, mitigation, and aggressive investigation of attacks on the nation's financial and critical infrastructures. The agency's first ECTF, the New York Electronic Crimes Task Force, was formed based on this concept in 1995.

National Computer Forensics Institute (NCFI)

https://www.ncfi.usss.gov/ncfi/

*NCFI training courses are offered to state and local law enforcement, prosecutors and judges through funding from the federal government. Travel, lodging, equipment (in some classes), and course fees are provided at no costs to attendees or their agencies. NCFI is a federally funded training center dedicated to instructing state and local officials in digital evidence and cybercrime investigations. The NCFI is run by the United States Secret Service's Criminal Investigative Division and the Alabama Office of Prosecution Services.

U.S. DEPARTMENT OF HOMELAND SECURITY

Office of the Assistant Secretary for Cybersecurity and Communications (CS&C)

http://www.dhs.gov/office-cybersecurity-and-communications

*Congress created the Office of the Assistant Secretary for Cybersecurity and Communications in 2006. CS&C carries out its mission through its five divisions:

- The Office of Emergency Communications
- The National Cybersecurity and Communications Integration Center
- Stakeholder Engagement and Cyber Infrastructure Resilience
- Federal Network Resilience
- Network Security Deployment

In addition, CS&C operates the Enterprise Performance Management Office, which ensures that the Assistant Secretary's strategic goals and priorities are reflected across

all CS&C programs; measures the effectiveness of initiatives, programs, and projects that support those goals and priorities; and facilitates cross-functional mission coordination and implementation between CS&C components, within DHS, and among the interagency.

Enhanced Cybersecurity Services Program, National Protection and Programs Directorate

http://www.dhs.gov/enhanced-cybersecurity-services

*The Department of Homeland Security's (DHS) Enhanced Cybersecurity Services (ECS) program is a voluntary information sharing program that assists U.S.-based public and private entities as they improve the protection of their systems from unauthorized access, exploitation, or data exfiltration. DHS works with cybersecurity organizations from across the federal government to gain access to a broad range of sensitive and classified cyber threat information. DHS develops cyber threat indicators based on this information and shares them with qualified CSPs, thus enabling them to better protect their customers. ECS augments, but does not replace, entities' existing cybersecurity capabilities.

The ECS program does not involve government monitoring of private networks or communications. Under the ECS program, information relating to threats and malware activities detected by the CSPs is not directly shared between CSP customers and the government. However, when a CSP customer voluntarily agrees, the CSP may share limited and anonymized information with ECS.

The Office of Cybersecurity and Communications (CS&C), National Protection and Programs Directorate

http://www.dhs.gov/national-protection-and-programs-directorate

*The Office of Cybersecurity and Communications (CS&C), within the National Protection and Programs Directorate, is responsible for enhancing the security, resilience, and reliability of the Nation's cyber and communications infrastructure. CS&C works to prevent or minimize disruptions to critical information infrastructure in order to protect the public, the economy, and government services. CS&C leads efforts to protect the federal ".gov" domain of civilian government networks and to collaborate with the private sector—the ".com" domain—to increase the security of critical networks.

In addition, the National Cybersecurity and Communications Integration Center (NCCIC) serves as a 24/7 cyber monitoring, incident response, and management center and as a national point of cyber and communications incident integration.

United States Computer Emergency Readiness Team (US-CERT)

https://www.us-cert.gov/

*US-CERT is part of DHS' National Cybersecurity and Communications Integration Center (NCCIC).

The Department of Homeland Security's United States Computer Emergency Readiness Team (US-CERT) leads efforts to improve the Nation's cybersecurity posture, coordinate cyber information sharing, and proactively manage cyber risks to the Nation while protecting the constitutional rights of Americans. US-CERT strives to be a trusted global leader in cybersecurity—collaborative, agile, and responsive in a dynamic and complex environment.

Through its 24x7 operations center, US-CERT accepts, triages, and collaboratively responds to incidents; provides technical assistance to information system operators; and disseminates timely notifications regarding current and potential security threats and vulnerabilities. … US-CERT partners with private sector critical infrastructure owners and operators, academia, federal agencies, Information Sharing and Analysis Centers (ISACs), state and local partners, and domestic and international organizations to enhance the Nation's cybersecurity posture.

Services provided by CERT include:

- **The Federal Virtual Training Environment (FedVTE) -** This is a flexible, multi-media, e-learning environment that can be accessed anywhere, anytime. Over 45,000 active users enhance their job-related skills through videotaped lectures, demos, and hands-on labs. The environment is accessible from any Internet-enabled computer and is available to U.S. government personnel only. Courses include topics such as traffic analysis, ethical hacking skills, risk management, malware analysis, network monitoring, software assurance. Instruction in specific software (e.g., ACAS, HBSS) is also available. See the FedVTE Course Library for more details. http://www.cert.org/cyber-workforce-development/fedvte.cfm

- **Cyber Resilience Review (CRR) –** The CRR is a no-cost, voluntary, non-technical assessment to evaluate an organization's operational resilience and cybersecurity practices. The CRR may be conducted as a self-assessment or as an on-site assessment facilitated by DHS cybersecurity professionals. The assessment is designed to measure existing organizational resilience as well as provide a gap analysis for improvement based on recognized best practices. http://www.us-cert.gov/ccubedvp/self-service-crr

- **Continuous Diagnostics and Mitigation (CDM) -** Through the CDM program, DHS works to deploy and maintain an array of sensors for hardware asset management, software asset management and whitelisting, vulnerability management, compliance setting management, and feed data about an agency's cybersecurity flaws, and present those risks in an automated and continuously-updated dashboard. CDM provides stakeholders with the tools they need protect their networks and enhances their ability to see and counteract day-to-day cyber threats. http://dhs.gov/cdm

- **Cybersecurity Evaluation Tool (CSET) and On-Site Cybersecurity Consulting -** The tool can be downloaded for self-use or organizations can request a facilitated site visit, which could include **basic security assessments**, network architectural review and verification, network

scanning using custom tools to identify malicious activity and indicators of compromise, and **penetration testing**. http://ics-cert.us-cert.gov/assessments

- **The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)** - ICS-CERT works to reduce risks within and across all critical infrastructure sectors by partnering with law enforcement agencies and the intelligence community and coordinating efforts among Federal, state, local, and tribal governments and control systems owners, operators, and vendors. Additionally, ICS-CERT collaborates with international and private sector Computer Emergency Response Teams (CERTs) to share control systems-related security incidents and mitigation measures. https://ics-cert.us-cert.gov/

- **ICS-CERT Training** - Training in industrial control systems security at the overview, intermediate, and advanced levels, including web-based and instructor-led formats. More information on ICS-CERT training opportunities are available at: http://ics-cert.us-cert.gov/training-available-through-ics-cert

- **Cybersecurity Advisors (CSAs)** - CSAs are regionally located DHS personnel who direct coordination, outreach, and regional support to protect cyber components essential to the sustainability, preparedness, and protection of the Nation's critical infrastructure and SLTT governments. CSAs offer immediate and sustained assistance to prepare and protect SLTT and private entities. For more information about CSAs, please e-mail cyberadvisor@hq.dhs.gov

- **Protective Security Advisors (PSAs)** - PSAs are trained critical infrastructure protection and vulnerability mitigation subject matter experts. Regional Directors are Supervisory PSAs, responsible for the activities of eight or more PSAs and geospatial analysts, who ensure all Office of Infrastructure Protection critical infrastructure protection programs and services are delivered to federal and SLTT stakeholders and private sector owners and operators. The PSA program focuses on physical site security and resiliency assessments, planning and engagement, incident management assistance, and vulnerability and consequence information sharing. http://dhs.gov/protective-security-advisors

- **SLTT Cybersecurity Engagement Program** - The Department's Office of Cybersecurity and Communications (CS&C) Stakeholder Engagement & Cyber Infrastructure Resilience (SE/CIR) division established the SLTT Cybersecurity Engagement program to build partnerships with non-federal public stakeholders including governors, mayors, state Homeland Security Advisors (HSA), Chief Information Officers (CIO), and Chief Information Security Officers (CISO). The SLTT Cybersecurity Engagement Program can provide cybersecurity risk briefings and information on available resources to governors and other appointed and elected SLTT government officials. More importantly, the program can also assist these officials with identifying cybersecurity initiatives and partnership opportunities with federal agencies,

as well as State and local associations, that will help protect their citizens online. To learn more about available resources and programs for the SLTT government community, e-mail sltcyber@hq.dhs.gov

- **Network Security Deployment (NSD)** - NSD strives to improve the cybersecurity of federal Government departments, agencies, and partners, including State Governments, by delivering the technologies and services needed to fulfill the Department's cybersecurity mission. NSD is responsible for designing, developing, acquiring, deploying, sustaining, and providing customer support for the National Cybersecurity Protection System (NCPS). NCPS satisfies aspects of the Department's mission requirements under the Comprehensive National Cybersecurity Initiative by delivering intrusion detection, advanced analytics, information sharing, and intrusion prevention capabilities that diminish the potential impact of cyber threats. http://dhs.gov/network-security-deployment

- **Cyber Incident Response and Analysis** - The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) offers incident response services to critical infrastructure asset owners that are experiencing impacts from cyber attacks. Services include digital media and malware analysis, identification of the source of an incident, analyzing the extent of the compromise, and developing strategies for recovery and improving defenses. Incident response teams also provide concepts for improving intrusion detection capabilities and ways to eliminate vulnerabilities and minimize losses from a cyber attack. For more information or to request response services, e-mail ics-cert@hq.dhs.gov

Critical Infrastructure Cyber Community (C³) Voluntary Program

https://www.us-cert.gov/ccubedvp

*The C³ Voluntary Program's focus during the first year will be engagement with Sector-Specific Agencies (SSAs) and organizations using the Framework to develop guidance on how to implement the Framework. Later phases of the C³ Voluntary Program will broaden the program's reach to all critical infrastructure and businesses of all sizes that are interested in using the Framework. The C³ Voluntary Program and organizations can interact through the following engagement channels:

- Regionally located DHS personnel from the Cybersecurity Advisor (CSA) and Protective Security Advisor (PSA) programs. These personnel interact directly with organizations in their regions about cybersecurity and critical infrastructure protection.
- The Critical Infrastructure Partnership Advisory Council (CIPAC) Framework, a partnership between government and critical infrastructure sector owners and operators that enables a broad spectrum of activities to support and coordinate on critical infrastructure protection.
- Direct engagement between the C³ Voluntary Program and interested organizations. Organizations may access the C³ Voluntary Program website or contact the C³ Voluntary Program at ccubedvp@hq.dhs.gov.

- Requests for Information (RFI), which create opportunities for the general public to provide input on cybersecurity solutions and policies.

Resources

- **Getting started for SLTT** – https://www.us-cert.gov/ccubedvp/getting-started-sltt

- **Cybersecurity Workforce Planning Diagnostic** – The Cybersecurity Workforce Planning Diagnostic tool, which was developed by NICE, introduces a qualitative management aid to help organizations identify the data they need to gather to execute effective cybersecurity workforce planning. By considering implications of specific organizational characteristics around two factors – risk exposure (as a function of mission cybersecurity dependence aligned to compliance standards) and risk tolerance – organizations will gain insight into what types of data they need to better plan for and manage their cybersecurity workforce. http://niccs.us-cert.gov/careers/cybersecurity-workforce-planning-diagnostic

- **National Cybersecurity Workforce Framework** - The National Cybersecurity Workforce Framework classifies the typical duties and skill requirements of cybersecurity workers. The Framework is meant to define professional requirements in cybersecurity, much as other professions, such as medicine and law, have done. Each Specialty Area detail displays the standard tasks and the knowledge, skills, and abilities needed to successfully complete those tasks. http://niccs.us-cert.gov/training/tc/framework/overview

- **National Cyber Awareness System (NCAS)** - The National Cybersecurity and Communications Integration Center (NCCIC) produces advisories, alert & situation reports, analysis report, current activity updates, daily summaries, indicator bulletins, periodic newsletters, recommended practices, Weekly Analytic Synopsis Product (WASP), weekly digests, and year in review to alert partners of emerging cyber threats, vulnerabilities, and current activities. More information on obtaining NCAS products is available at: http://us-cert.gov/ncas, http://us-cert.gov/mailing-lists-and-feeds or http://public.govdelivery.com/accounts/USDHSUSCERT/subscriber/new

- **Industrial Control Systems Computer Emergency Readiness Team (ICS-CERT) Recommended Practices** - A list of recommended practices aimed at helping industry understand and prepare for ongoing and emerging control systems cybersecurity issues, vulnerabilities, and mitigation strategies. http://ics-cert.us-cert.gov/introduction-recommended-practices

- **U.S. Computer Emergency Readiness Team (US-CERT) and ICS-CERT Alerts, Bulletins, Tips, and Technical Documents** - Access to alerts, bulletins, tips, and technical documents published by ICS-CERT and US-CERT. ICS-CERT also offers an extensive bibliography of relevant standards and references. Both sets of documents and references provide a better understanding of relevant control systems vulnerabilities and the measures

critical infrastructure owners and operators can take to address them. http://ics-cert.us-cert.gov

- **Cybersecurity Service Offering Reference Aids** - DHS's National Protection and Programs Directorate (NPPD) has developed a list of freely available reports and resources pertinent to managing the acquisition of cybersecurity services. It is not intended to be exhaustive, but covers a wide range of cybersecurity services including cloud service providers, cyber incident response, cloud computing, software assurance, and industrial control systems. https://www.uscert.gov/sites/default/files/c3vp/cybersecurity_service_offerings_reference_aids.pdf

FEDERAL EMERGENCY MANAGEMENT AGENCY

Emergency Management Institute (EMI) Virtual Table Top Exercise (VTTX)

http://www.training.fema.gov/programs/emivttx.aspx

*The Emergency Management Institute (EMI) conducts a monthly series of Virtual Table Top Exercises (VTTX) using a video teleconference platform to reach community based training audiences around the country and provide a virtual forum for disaster training. The VTTX process involves key personnel from the emergency management community of practice reviewing a pre-packaged set of exercise materials then convening for a four hour table top exercise discussing a simulated disaster scenario. The event allows the connected sites to assess current plans, policies and procedures while learning from the other connected sites as they provide their perspective and practices facing a similar situation. A standard VTC system is required for participation.

Resource

An example of a cyber-specific exercise hosted by FEMA - https://training.fema.gov/emigrams/2015/1153%20-%20training%20opportunity%20-%20v-0046%20-%20virtual%20tabletop%20exercise%20series%20(vttx)%20cyber.pdf?d=3/6/2015

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology (NIST), National Cybersecurity Framework

http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

*The Framework enables organizations – regardless of size, degree of cybersecurity risk, or cybersecurity sophistication – to apply the principles and best practices of risk management to improving the security and resilience of critical infrastructure. Organizations can use the framework to determine their current level of cybersecurity, set goals for cybersecurity that are in sync with their business environment, and establish a plan for improving or maintaining their cybersecurity. It also offers a methodology to protect privacy and civil liberties to help organizations incorporate those protections into a comprehensive cybersecurity program.

Resources

- **National Cybersecurity Framework -** http://www.nist.gov/cyberframework/index.cfm
- **Companion Roadmap -** http://www.nist.gov/cyberframework/upload/roadmap-021214.pdf

GENERAL SERVICES ADMINISTRATION

The Federal Risk and Authorization Management Program (FedRAMP)

http://www.gsa.gov/portal/category/102371

*FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

Resources

- **FedRAMP compliant cloud services –** http://cloud.cio.gov/fedramp/cloud-systems

STATE, REGIONAL, AND LOCAL

NATIONAL GUARD

http://www.nationalguard.mil/resources/statewebsites.aspx

Contact the state branch of the National Guard to determine how they can assist your cybersecurity efforts. Many are able to provide support with risk assessments, exercises, response, and recovery.

MULTI-STATE INFORMATION SHARING AND ANALYSIS CENTER (MS-ISAC)

http://msisac.cisecurity.org/

*The MS-ISAC has been designated by the U.S. Department of Homeland Security as the central resource for cyber threat prevention, protection, response and recover for the nation's state, local, territorial and tribal (SLTT) governments as well as fusion centers. If you have a cybersecurity issue, call the MS-ISAC Cyber Operations Center 24-hours, 7-days a week at 1-866-787-4722.

Resources

- **Cyber Integration for Fusion Centers, An Appendix to the Baseline Capabilities for State and Major Urban Area Fusion Centers -** https://msisac.cisecurity.org/documents/CyberIntegrationforFusionCenters.pdf

- **A series of public and free webcasts –** http://msisac.cisecurity.org/webcast/

INTERNATIONAL

EUROPOL

European Cybercrime Centre (EC3)

https://www.europol.europa.eu/ec3/

Europol's EC3 fulfills the following functions:*

- Serves as the central hub for criminal information and intelligence.
- Supports Member States' operations and investigations by means of operational analysis, coordination and expertise.
- Provides a variety of strategic analysis products enabling informed decision making at tactical and strategic level concerning the combating and prevention of cybercrime.
- Establishes a comprehensive outreach function connecting cybercrime related law enforcement authorities with the private sector, academia and other non-law enforcement partners.
- Supports training and capacity building, in particular for the competent authorities in the Member States.
- Provides highly specialized technical and digital forensic support capabilities to investigations and operations.
- Represents the EU law enforcement community in areas of common interest (R&D requirements, Internet governance, and policy development).

INTERPOL

Global Complex for Innovation (IGCI)

http://www.interpol.int/About-INTERPOL/The-INTERPOL-Global-Complex-for-Innovation/About-the-IGCI

*The INTERPOL Global Complex for Innovation (IGCI) is a cutting-edge research and development facility for the identification of crimes and criminals, innovative training, operational support and partnerships.

The Global Complex goes beyond the traditional reactive law enforcement model. This new centre provides proactive research into new areas and latest training techniques. The aim is to give police around the world both the tools and capabilities to confront the increasingly ingenious and sophisticated challenges posed by criminals.

The three main components of the Global Complex are as follows:

Digital security

- Boosting cybersecurity and countering cybercrime;
- A forensics laboratory to support digital crime investigations;
- Research to test protocols, tools and services and to analyse trends of cyber-attacks;
- Development of practical solutions in collaboration with police, research laboratories, academia and the public and private sectors;

- Addressing issues such as Internet security governance.

Capacity building and training

- Research into training and methodology and the transfer of this research into police activities on the ground;
- Classroom, field and online training programs for National Central Bureaus;
- Anti-corruption training, particularly in sport;
- Quality standards and accreditation.

Operational and investigative support

- Identifying and addressing emerging crime threats, for example, Asian Organized crime;
- A platform for disaster victim identification;
- Incident response and major events support;
- A Command and Coordination Centre operations room reinforces those already in place in Lyon and in Buenos Aires, Argentina. This presence in three continents provides truly global operational support to our member countries.

PRIVATE AND NON-PROFIT

CYBRARY

http://www.cybrary.it/

This site offers free online cybersecurity and information technology training.

CENTER FOR INTERNET SECURITY

https://www.cisecurity.org/

*The Center for Internet Security, Inc. (CIS) is a 501(c)(3) nonprofit organization focused on enhancing the cybersecurity readiness and response of public and private sector entities, with a commitment to excellence through collaboration. CIS provides resources that help partners achieve security goals through expert guidance and cost-effective solutions. The MS-ISAC is a division of the Center for Internet Security.

The Center for Internet Security Critical Security Controls for Effective Cyber Defense™ (CIS Controls) are a recommended set of actions for cyber defense that provide specific and actionable ways to thwart the most pervasive attacks. The CIS Controls are a relatively short list of high-priority, highly effective defensive actions that provide a "must-do, do-first" starting point for every enterprise seeking to improve their cyber defense. Since the CIS Controls are derived from the most common attack patterns and vetted across a very broad community of government and industry, they serve as the basis for immediate high-value action.

Resources

- **CIS Critical Security Controls are available at** https://www.cisecurity.org/critical-controls.cfm

INTERNATIONAL ASSOCIATION OF CHIEFS OF POLICE

IACP Cyber Center

http://www.iacpcybercenter.org/

This site provides a range of resources to help police chiefs and others understand cyber threats and the necessary steps to protect networks from cyber attacks. The site also provides information for officers and investigators regarding digital forensics, cyber investigations, and cybercrime training programs. The Cyber Center is a collaborative project of the International Association of Chiefs of Police (IACP), RAND Corporation, and the Police Executive Research Forum (PERF), and is made possible by funding from the Bureau of Justice Assistance, at the U.S. Department of Justice's Office of Justice Programs.

KREBS ON SECURITY

http://krebsonsecurity.com/

Brian Krebs, a former Washington Post reporter, writes on cybercrime and other Internet security topics on this widely read blog.

NATIONAL FUSION CENTER ASSOCIATION

NFCA Cyber Intelligence Network

http://www.nfcausa.org

The National Fusion Center Association coordinates a virtual situational awareness room called CINAWARE on the Homeland Security Information Network (HSIN). CINAWARE, which is stood up 24/7 during events with national implications, links members of the NFCA Cyber Intelligence Network across the country so they can share information on cyber threats in real time.

NATIONAL CONSORTIUM FOR ADVANCED POLICING

http://advancedpolicing.com/about.php

*NCAP was established to strengthen and teach the principles of advanced policing – strategies and knowledge that police professionals and organizations can apply to more effectively meet the policing challenges of the 21st Century. In addition to writing publications like this one, NCAP provides technical assistance and training on a range of topics.

POLICE EXECUTIVE RESEARCH FORUM

http://www.policeforum.org/

*The Police Executive Research Forum (PERF) is a police research and policy organization and a provider of management services, technical assistance, and executive-level education to support law enforcement agencies. PERF helps to improve the delivery of police services through the exercise of strong national leadership; public debate of police and criminal justice issues; and research and policy development.

Resource

- **The Role of Local Law Enforcement Agencies In Preventing and Investigating Cybercrime –** http://www.policeforum.org/assets/docs/Critical_Issues_Series_2/the%20role%20of%20local%20law%20enforcement%20agencies%20in%20preventing%20and%20investigating%20cybercrime%202014.pdf

SANS INSTITUTE

http://www.sans.org/

*The SANS Institute was established in 1989 as a cooperative research and education organization. Its programs now reach more than 165,000 security professionals around the world. A range of individuals from auditors and network administrators, to chief information security officers are sharing the lessons they learn and are jointly finding solutions to the challenges they face. At the heart of SANS are the many security practitioners in varied global organizations from corporations to universities working together to help the entire information security community.

Resources

- **SANS resource page with a range of offerings on topics, including digital forensics, pen testing and ethical hacking** – https://www.sans.org/security-resources/

NATIONAL CYBERSECURITY ALLIANCE

http://www.staysafeonline.org/

*NCA's mission is to educate and empower a digital society to use the Internet safely and securely at home, work, and school, protecting the technology individual's use, the networks they connect to, and our shared digital assets.

THE NATIONAL CYBER-FORENSICS & TRAINING ALLIANCE

http://www.ncfta.net/

*The National Cyber-Forensics & Training Alliance (NCFTA) is a non-profit corporation focused on identifying, mitigating, and ultimately neutralizing cybercrime threats through strategic alliances and partnerships with Subject Matter Experts (SME) in the public, private, and academic sectors. Ever vigilant in uncovering emerging cyber threats, we share threat information and (SME) resources on a real time basis across all sectors and all of our partners via multiple communication channels.

Resources

- **NCFTA Knowledge Base, which provides information on trends in malware and phishing** - http://www.ncfta.net/cyber-crime-knowledge-base.aspx

DELL SECUREWORKS

http://www.secureworks.com/consulting/security-awareness-training/

Dell SecureWorks provides many resources, including awareness-level training resources.

[Note: There is an entire industry of private companies that offer training and other products related to cybersecurity. While the list is too extensive to include here, please use your cyber network to find out about the offerings most suited to your needs and budget.]

ACADEMIA

CARNEGIE MELLON

Software Engineering Institute

http://www.sei.cmu.edu/training/

*SEI Training is administered by the SEI Professional Development Center, which is dedicated to providing the best continuing education and credentialing for engineering and software professionals in government (military and civilian), industry, and higher education.

CERT Division

http://www.cert.org/index.cfm

*[The CERT Division] regularly partner[s] with government, industry, law enforcement, and academia to develop advanced methods and technologies to counter large-scale, sophisticated cyber threats.

The CERT Division is connected to Carnegie Mellon University and located within the university's Software Engineering Institute.

CYBERCORPS SCHOLARSHIP FOR SERVICE

https://www.sfs.opm.gov/

The CyberCorps Scholarship for Service (SFS) program gives students scholarship funds in exchange for service in the federal government for a period equivalent to the length of their scholarship, typically two years. As a result of the SFS program, federal agencies are able to select from a highly qualified pool of student applicants for internships and permanent positions. The SFS program is offered by the National Science Foundation (NSF) and co-sponsored by the Department of Homeland Security (DHS).

THE CYBER ACADEMY

http://thecyberacademy.org/

The Cyber Academy integrates with a range of international initiatives, with a special focus on Cybersecurity education. This includes integration into the EU-funded DFET project, which is building a virtualized infrastructure for Cybersecurity training, with strong links into law enforcement and academia around the world.