Managing Cybersecurity Risk:

A Law Enforcement Guide

August 2017

International Association of Chiefs of Police

INTRODUCTION

Purpose of the Document

This paper is designed to aid in educating law enforcement executives on their responsibility to ensure the cybersecurity of their organizations is managed in an effective manner. It provides essential background material to create a greater understanding of the complex issues involved. This paper will be of assistance to any law enforcement executive, whether they are involved in state, province, local, or tribal law enforcement organizations.

Background

Why is cybersecurity such a critical concern for law enforcement executives?

There is an ever-growing risk of law enforcement organizations being the target of a cyber-attack. Law enforcement agencies are using and relying more on technology today than ever in almost every aspect of their operations including: dispatch (computer-aided dispatch), records (records management systems), communications (mobile devices, social media, situational awareness), Next Generation 911 (NG911) systems, voice over Internet protocol (VOIP) telephone systems, and evidence (cloud storage, digital media servers). There is also an ever-increasing amount of digital evidence that comes to law enforcement from various sources and such evidence must be properly managed. With law enforcement's increased use of technology comes increased risks, including the following:

- Exposing confidential information related to ongoing investigations
- Exposing personal information on victims, witnesses, and informants
- Exposing personal information on officers and organization employees
- Compromising the integrity of critical information and evidence
- Incurring compromises to organizational systems and alteration of webpages
- Experiencing denial of service attacks, that not only put the organization at greater risk, but citizens as well
- Experiencing increasing risk of ransomware attacks (In one recent attack a U.S. police organization is reported to have lost 8 years of information.)

Unauthorized access of law enforcement systems by way of a cyberattack has serious operational and privacy implications for law enforcement organizations. A law enforcement organization collects vast amounts of information, so the importance of cybersecurity needs to be considered from multiple perspectives—stakeholders, citizens, victims, and informants, as well as protection of privacy, continuity of evidence, and support of prosecution. Members of law enforcement are sworn

to protect the rights and privacy of their citizens so this issue is worth the concern of any law enforcement executive.

It is important to understand that cyber events could put a law enforcement organization at a disadvantage in its ability to protect life, ensure the safety of community members, keep the peace, and enforce laws. It could also significantly impact the public's confidence in the organization, damaging its trustworthiness and credibility. Finally, the cost of a cyber breach and loss of personal information could significantly and negatively impact an organization's budget due to possible ransomware payments, costs related to the response to a cyber event and restoring systems, and conducting operations without the aid of technology. If the data breach included the loss of personal information, the cost of notifying all of the impacted individuals and possibly providing identity theft services could be significant.

Cybersecurity, like any other type of security for the organization, is the ultimate responsibility of the law enforcement executive, and specific action is necessary to ensure a high level of protection.

In 2013, the IACP and the Canadian Association of Chiefs of Police (CACP) completed a survey of American and Canadian law enforcement executives from agencies of all sizes. The survey results confirmed that many law enforcement executives understand that the security and privacy of their agencies' records are at risk if a cyberattack is successful. Overall, 79 percent of respondents believed cyberattacks were a risk (from moderately serious to very serious) to their organizations. Not surprisingly, of those who had been attacked, 92 percent viewed cyberattacks as a risk from moderate to serious.

The respondents also understood the potential for serious privacy repercussions from a successful cyberattack. The breakdown follows:

- 89 percent felt the loss of credibility in electronically stored records was a moderate to very serious impact.
- 82 percent saw the loss of critical data in ongoing investigations as a moderate to serious impact.
- 73 percent saw a potential loss of cases before the courts as a moderate to serious impact.
- 87 percent of respondents felt that it is between somewhat and very important to do regular cybersecurity audits (although only 13 percent said that they were doing such audits).

In many cases law enforcement organizations are using municipal information technology (IT) resources and do not have direct control over the employees, procedures, or hiring process of the IT resources they use. When faced with this situation, it may seem prudent and even preferable to rely on the city or county to protect the law enforcement systems from cyberattack. However, it is ultimately the responsibility of law enforcement executives to ensure all aspects of security, including cybersecurity, are adequate for their organizations. If a law enforcement system is breached, the media and elected officials will want to ask questions of the chief, not the local IT staff or the staff of the city or county department housing the IT resource. Therefore, it is important to understand the

significance of working with an IT partner and the respective roles of the law enforcement executive and that of the IT partner.

PROCEDURES FOR MAINTAINING CYBERSECURITY

Law Enforcement Executive's Role and Responsibility

The law enforcement executive holds the responsibility for cybersecurity within the organization. Attitudes toward cybersecurity and engagement in ensuring everyone is vigilant and active in protecting the organization's operations will be significantly enhanced if the executive champions the cause.

The law enforcement executive should appoint someone in the organization to manage the cybersecurity considerations of the organization, and that person should report directly to the executive. This can be an existing position that simply takes on this portfolio, or the organization may be large enough to have a full-time person in this role. This ***function*** will be referred to as the cyber security risk manager (CSRM). For example, the CSRM is responsible to maintain the organization's cybersecurity risk management program that describes, among other things, the security posture of the organization, threats to the cybersecurity of the organization, the training plan for members, and prevention efforts. The CSRM must keep the law enforcement executive aware of the risks and mitigation efforts that the organization is considering. Periodic reports will ensure that the executive is kept up to date on this matter.

Some of the specific considerations taken on by the CSRM would include the management of passwords and access to computing systems, the termination of access, the classification of information (evaluating the sensitivity of the information), data encryption needs, managing vendor access to the system, ensuring security vulnerabilities are found and corrected, monitoring the network for unusual traffic, considering disaster recovery options, ensuring background checks are done for those who have access to computer systems and facilities, and ensuring a policy governs the use of the available information resources.

While most law enforcement executives do not need to fully understand the intricacies of a comprehensive cybersecurity policy, they can do a number of things to ensure that their organization is protected. In cases where the IT resources are provided by an IT partner, the law enforcement executive is still responsible for ensuring the security of the organization's information. A law enforcement executive should not accept casual assurances from any IT partner that the security is acceptable. Some of the areas for specific answers are listed below.

Working with the IT Partner

The IACP Computer Crime and Digital Evidence Committee has developed a list of questions to be used as a tool to aid in improving cybersecurity discussions between the law enforcement executive or agency and the IT partner. If the agency is a large organization, it may be the IT Director who gets the list of questions. If the agency is a smaller organization, it may be the IT Director for the city, or a third-party organization. The IACP Cyber Report Card is a document listing 18 questions that will help you in assessing your risk.[1]

After an organization reviews the questions provided, a good first step is to speak to the IT partner about these questions, allowing the organization and the IT partner to develop an understanding of the current level of cybersecurity. A written response should be requested to impress upon the IT partner the importance of this request. However, the response should be requested in nontechnical terms to facilitate communication and understanding. It is recommended that before the questions are sent to the IT partner, assure them that they provide a vital service to your organization and that their approach or capabilities are not being attacked. They should understand that the law enforcement executive is ultimately responsible for all aspects of organizational security—and cybersecurity is an important part of that. It is also important that they understand the expectation of a written report in plain English that will help the law enforcement executive comprehend the security posture of the organization's systems.

Developing a proper cybersecurity framework for the organization is an important function. There are a number of resources that can provide reference material for law enforcement organizations. Some resources follow:

- The Chief Information Security Officer (CISO) of the IT partner can help you gain an understanding of cybersecurity concerns and risks and help to ensure your needs are prioritized.
- The law enforcement agencies in the organization's area with cybercrime, cybersecurity, or forensic capabilities are also beneficial resources.
- The local fusion center has the ability to reach out to the entire network of fusion centers to access cyber knowledge.
- The National Guard (or equivalent organization) for the organization's state or province can also be a source of information.
- The Multi-State Information Sharing and Analysis Center (MS-ISAC) is the U.S. Department of Homeland Security (DHS) designated cybersecurity resource for all state, local, tribal, and territorial governments.
- There are many tools that can be used as guidelines, including but not limited to, the NIST Generally Accepted Principles and Practices for Security Information Technology Systems,[2] the ISO 27000 Series,[3] the IACP Technology Policy Framework,[4] the Law Enforcement Cyber Center (LECC),[5] the NIST Framework for Improving Critical Infrastructure Cybersecurity,[6] and the IACP Cyber Report Card.[7]

Innovations now allow law enforcement more effective ways of managing investigations and human resources. However, those same innovations also open up vectors for attacking law enforcement organizations. Such organizations must therefore continually monitor their cybersecurity posture to ensure sensitive information is protected. This will require time, effort and resources, but is absolutely necessary for maintaining the organization's security. For any technology currently deployed or any new technology being considered, the security capabilities of the technology and

security implications of integrating the technology into the organization's operation must be thoroughly evaluated.[8]

Training

Training is required to enable all personnel to take a proper stance against attacks that threaten the organization. From end-user training that creates an awareness of legitimate looking (but fake) email requests, hazards related to USB devices, proper password protocols through to proper use of technology, it is important to understand that the easiest way for malicious actors to access information systems is through the exploitation of the organization's personnel. Some of this training can come from qualified third-party security auditors that advise all personnel on practices that can enhance security. A reliable and experienced third-party may be more objective in approaching and assessing vulnerabilities in security and be generally skilled and knowledgeable regarding current threats. A third-party can enhance the practices of your organization through periodic training and security checks. If a third-party has not evaluated an organization's security posture, a law enforcement executive might not fully understand the strengths and weaknesses of his or her current situation.

Discussions regarding cybersecurity between the law enforcement executive and the IT partner are a collaborative opportunity. If the IT partner is the city or county, it is likely that they have responsibility for all other municipal departments in the organization's jurisdiction. Working collaboratively can result in enhanced security for the entire jurisdiction while bringing peace of mind to the law enforcement executive who is ultimately responsible for the cybersecurity of law enforcement systems.

Another key area of organizational training involves the risk that can be created by officers and employees in their personal lives. The use of social media at home or at work, or using the same USB storage device at home and at work, for example, can create risk for the organization. The weapons for many cyberattacks originate in social media or other activities engaged in by the officers or employees in their personal life.

Digital Evidence

One of the key issues facing law enforcement organizations today is the flood of digital evidence. The property and evidence room is often no longer the largest location of property and exhibits. Rather the computer system has become a storage area for all kinds of digital evidence including law enforcement reports, statements, pictures, videos, PDF files, and many other kinds of documents that support a law enforcement investigation. The importance of securing the evidence room door is fully understood by law enforcement executives, and procedures are in place to ensure the security and integrity of evidence. Audits and procedures related to the storage of digital evidence should be considered as important as those related to the property and evidence room.

The organization must provide security for digital evidence while providing limited access for investigators and others who need it. Original copies must be absolutely protected, and a resilient approach to data safeguarding (e.g., backups) is essential.

Independent Testing of the Organization's Cyber Risks

An independent third-party test can supply you with information that will greatly assist in knowing what can be done to enhance security. An independent party can describe the risks and report on areas where improvement is necessary. Most importantly, an unbiased third-party appraisal provides a base line for monitoring improvement. As the saying goes, "what is measured, improves." A reliable IT partner will recognize the threats that exist and support independent testing.

Security threats can occur at any time, therefore cybersecurity is not a one-time effort, but rather is a matter for ongoing review. Monitoring access permissions on an organization's system requires constant vigilance. If procedures become lax, permissions may remain for those who no longer have the right to use the system. An example requirement is the removal of permissions for temporary staff members at the end of their work term, which is a Criminal Justice Information Services standard. (CJIS is a U.S. standard, but similar standards exist in many other countries).

Incident Response

Law enforcement executives must understand their systems will be attacked. Preparing for and rehearsing the response to such an incident is critical. It must be determined how the IT partner will respond to such an attack, because experience has shown that virtually no organization has all of the highly-trained resources necessary to mount a comprehensive response. If internal resources do not exist to respond, the services of external professionals will be necessary to manage all aspects of a response. These include detection, triage, and communication; evidence preservation; hard drive imaging; and network-based evidence acquisition. These specialized services will be less expensive if arranged in advance rather than introduced during an emergency.

CAUTIONARY CONSIDERATIONS

There are two factors that could cause inaction on the part of a law enforcement executive:

- Cyber Fatigue**:** Cybersecurity is a complex subject with almost daily media reporting of incidents. Not understanding where to start or how to approach this matter can impede the process. Doing nothing is not an effective strategy!

- Law enforcement executives may be tempted to abdicate their responsibility in this important security issue. Verbal assurances from an IT partner that security is sufficient is not enough. As previously stated, the responsibility for the cybersecurity of law enforcement systems rests with the law enforcement executive!

In both cases a good discussion with the IT partner, followed by a request for a written response in plain language, will help to establish the level of security and demonstrate that the law enforcement executive is serious about protecting his or her IT operations.

CONCLUSION

Cyberattacks are becoming more common and more sophisticated. This presents a serious risk to law enforcement organizations and their information systems.

A successful cyberattack could put a law enforcement organization at a disadvantage in protecting citizens as well as keeping the peace and enforcing laws. The cyberattack would have serious operational and privacy impacts to a law enforcement organization, which could result in the loss of trust and confidence in law enforcement.

Cybersecurity, like any other type of security for the organization, is the ultimate responsibility of the law enforcement executive.

While the law enforcement executive does not need to be an expert on cybersecurity, the establishment of a Cybersecurity Risk Manager (a function, not necessarily a person) within the organization, with clear responsibilities and mandate, will assist in updating or creating policy that will make cybersecurity everyone's concern.

Third-party security audits are the best way to test your organization's ability to withstand a coordinated cyberattack. Generally, these security auditors think more like a real attacker than staff whose main job is to provide services.

This is a critical issue that should be managed and prioritized on an ongoing basis because security threats can occur at any time. An article entitled "A Police Chief's Evolving Perspective on Cybersecurity," in the Nuix Black Report, stated "It is imperative for law enforcement executives to educate themselves in cybersecurity measures to ensure their data is protected and independently audited against intrusion or tampering."[9] That statement has never been more true.

DEFINITIONS

Computing System: This includes laptops, desktops and servers, email and business applications, confidential information, report management systems, and informant and investigative files.

Cybersecurity: The discipline of protecting the computer systems, communications, and networks of an organization against attack.

Cybersecurity Incident: An attack, against the computer systems and networks of a given organization, that causes some level of disruption or damage.

Cybersecurity Risk Manager (CSRM): The individual who is assigned the responsibilities of managing cybersecurity risk within the law enforcement organization. This position may be full time or part time or filled by an external employee or contractor.

Cyber Threat Action Plan: An ongoing and updated plan to manage a cybersecurity incident.

Cybersecurity Risk Management Program: An overarching document that describes the security posture of the organization, threats to the cybersecurity of the organization, training plan for members, and prevention efforts.

Cybersecurity Risk: Any factor that increases the ease with which the computer systems and networks of an organization may be attacked.

Digital Evidence (DE): Digital recording of images, sounds, and associated data. Also referred to as digital multimedia evidence (DME).

Information Technology (IT) Partner: The person or organization that supplies IT resources and services. In a large organization, this may be the IT director; whereas, in a small organization, this may be the IT director for the city or county.

Information Technology (IT) Resources: The computers or networks of a given organization.

MS-ISAC: Multi-State Information & Analysis Center.

Security Posture: The overall readiness of an organization to withstand a focused attack on its computing systems.

ENDNOTES

1. Law Enforcement Cyber Center. The IACP Cyber Report Card. http://www.iacpcybercenter.org/wp-content/uploads/2015/09/Cyber-Report-Card-7815.pdf
2. Marianne Swanson and Barbara Guttman. 1996. *Generally Accepted Principles and Practices for Securing Information Technology Systems.* Gaithersburg, Maryland: National Institute of Standards and Technology. http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf
3. International Organization for Standardization. The ISO 27000 Series. https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en
4. IACP Technology Policy Framework. 2014. http://www.theiacp.org/portals/0/documents/pdfs/iacp%20technology%20policy%20framework%20january%202014%20final.pdf
5. Law Enforcement Cyber Center. Home page. http://www.iacpcybercenter.org
6. National Institute of Standards and Technology. *Framework for Improving Critical Infrastructure Cybersecurity*. https://www.nist.gov/sites/default/files/documents/cyberframework/Cybersecurity-Framework-for-FCSM-Jan-2016.pdf
7. The IACP Cyber Report Card (see note 1).
8. IACP Technology Policy Framework (see note 4).
9. Terry L. Sult. "A Police Chief's Evolving Perspective on Cybersecurity." *The Black Report: Decoding the Minds of Hackers.* 37. https://media.scmagazine.com/documents/287/nuix_the_black_report_2017_71550.pdf

International Association of Chiefs of Police

44 Canal Center Plaza, Suite 200
Alexandria, VA 22314

Direct: 703-836-6767 | Main Line: 800-THE-IACP | Fax: 703-836-4543

www.theIACP.org