“CYBERSECURITY IS A SHARED RESPONSIBILITY, AND IT BOILS DOWN TO THIS: IN CYBERSECURITY, THE MORE SYSTEMS WE SECURE, THE MORE SECURE WE ALL ARE.”

– JEH JOHNSON
FORMER UNITED STATES SECRETARY OF HOMELAND SECURITY

SECTION 2

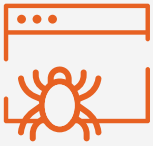
CYBERSECURITY

2. CYBERSECURITY OVERVIEW

"Why do we care?" about cybersecurity and some key concepts to get started.

Understanding Cybersecurity Governance – Section 2.1

- Cybersecurity governance & who should be involved (2.1.1 - 2.1.2)
- Information security policy & its importance (2.1.3)
- Draft your security policy (2.1.4)
- Frameworks & standards for managing cybersecurity risk (2.1.5)



Understanding Cyberattacks – Section 2.2

- Identify what's collected (2.2.1)
- Cyberattacks & cyberattackers (2.2.1 - 2.2.2)
- Types of cyberattacks (2.2.3)
- Stages of cyberattack (2.2.4)
- Cyber Boom Model (2.2.5)

Best Practices in Cybersecurity – Section 2.3

- Prevent & protect from cyberattack (2.3.1)
- During a cyberattack (2.3.2)
- After a cyberattack (2.3.3)

Check out the resource repository at the end of the section.

usignite

2.CYBERSECURITY

WHY DO WE CARE?

Cybersecurity is the risk management of a city or community's digital operations and data. *It refers to a set of practices, policies, and standards that can help prevent and protect against cyber incidents.* Effective cybersecurity measures lay the foundation for robust risk management, harmonize business processes, provide protection from potential civil and legal liabilities, assures security, policy compliance, and protects the trust and confidence of the public.

A cyberattack cost a city in Maryland over $18.2 million. The city officials were denied access to their computer networks for weeks and residents had to resort to mail-in and in-person visits to pay their bills. Later an audit report found that the city lacked appropriate cybersecurity measures to prevent the attack. This is just one example of the many cyberattacks that we have seen on local governments.

Local governments are easy targets as they: (i) are a treasure trove of personal data; (ii) often have outdated/legacy systems; (iii) are historically underfunded and understaffed; and (iv) customarily lack sufficient training in cybersecurity measures and defenses. Consequently, cyberattacks pose a major risk of irreversible damage to the city and community's assets and reputation.

Interestingly, cities and communities identify cybersecurity as their top priority but often fail to invest or allocate sufficient budget and resources for it.[2] A part of the reason is that cybersecurity has largely remained a very technical and inaccessible issue for city and community officials. This section aims to simplify the discussion of how cities and communities can take appropriate measures to address their cybersecurity concerns. We discuss the following:

1. Understanding Cybersecurity Governance
2. Understanding Cyberattacks
3. Best Practices in Cybersecurity
4. Cybersecurity Resource Repository for Cities and Communities

KEY DEFINITIONS:[1]

- **Adversary** – Individual, group, or organization that conducts, or has the intent to conduct, detrimental activities.
- **Application(s)** – System/function for collecting, saving, processing, and presenting data by means of a computer.
- **Computer System** – Also referred to as system; is a basic, complete and functional hardware and software setup with everything needed to implement computing performance.
- **Incident** – An adverse network event in an information system or network or the threat of the occurrence of such an event.
- **Legacy Systems** – An environment containing older systems or applications that needs to be secured to meet today's threats.
- **Malicious Code** – Software that appears to perform a useful or desirable function, but actually gains unauthorized access to system resources or tricks a user into executing other malicious logic.
- **Network** – Two or more computers that are linked in order to share resources (such as printers), exchange files, or allow electronic communication.

1 Glossary of Security Terms. (n.d.). SANS. Retrieved April 2021, from https://www.sans.org/security-resources/glossary-of-terms/?msc=securityresourceslp; NIST. (n.d.). Computer Security Resource Center. Retrieved April 2021, from https://csrc.nist.gov/glossary/term/adversary.

2 Newcombe, T. (2021, April 23). Cybersecurity in 2019: A Time for Bigger Budgets and More Talent (Contributed). GovTech. https://www.govtech.com/opinion/cybersecurity-in-2019-a-time-for-bigger-budgets-and-more-talent-contributed.html

2.1. UNDERSTANDING CYBERSECURITY GOVERNANCE

2.1.1 WHAT IS CYBERSECURITY GOVERNANCE?[3]

Cybersecurity (also referred to as just security) governance refers to the business practices, processes and controls that are put in place to ensure organizational security and manage potential cybersecurity risks.[4] Even for cities and communities that outsource cybersecurity services, cybersecurity governance is important because outsourcing does not guarantee absolute protection.

Cybersecurity governance should include the following:

- Defining and assigning roles and responsibilities to security professionals who will play an active role in protecting the daily operations and resident privacy.
- Cybersecurity practices and processes that govern operations and protect critical assets.
- Code of conduct for employees for securing and protecting data and systems.
- Internal as well as external rules and regulations needed to ensure the integrity of systems, networks, and data (compliance requirements). Refer to the resource repository for a cybersecurity compliance guide.
- Guidelines to safeguard the reputation of the organization.

TIP: CHARACTERISTICS OF AN EFFECTIVE SECURITY GOVERNANCE

- Applies to the entire organization.
- Holds leaders accountable.
- Clearly defines roles and responsibilities.
- Takes a risk-based approach.
- Complies with relevant requirements including laws, ordinance, and other organizational policies.
- Addressed and enforced in Security Policy.
- Commits and sets aside adequate budget/resources.
- Well communicated with staff and external vendors/partners.
- Reviewed and audited.

Source: Modified based on Educause.

2.1.2 WHO SHOULD BE INVOLVED IN CYBERSECURITY GOVERNANCE?

The goal should be to build a multi-disciplinary team of:

- **Business Executives** – Individuals that are involved with the business side of operations. They can be department heads who ensure integration and cooperation of security practices with the operations of their department.
- **Chief Information Security Officer (CISO)** – Cities and communities may have a Chief Technology Officer (CTO), Chief Information Security Officer (CISO) or even an Information System Security Officer (ISSO). Regardless of the title, it is paramount to have a designated leader who will be responsible for overseeing all information security practices.

TIP

- Refer to the guidance document on Information Security Governance for a list of questions to consider for successful implementation of Information Security Governance.
- Read about more about the role of a CISO here.

3 Educause. (n.d.). Information Security Governance. Retrieved April 2021, from https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program/resources/information-security-guide/toolkits/information-security-governance

4 Ibid.

- **Information Technology (IT) Personnel** – Individuals directly involved in overseeing network and system operations and security.
- **Steering Committee** – A diverse group of individuals from across the departments as well as some external security experts responsible for addressing security concerns and creating accountability.
- **Cyber Incident Response Team** – In addition to these roles, build an exclusive cyber incident response team including lawyers, public relations (PR) professionals, and IT professionals who will be the first responders and firefighters during a cybersecurity incident.

TIP

Refer to Infocyte's practical guide to build your own cyber incident response team.

2.1.3 WHAT IS AN INFORMATION SECURITY POLICY AND WHY IS IT IMPORTANT?[5]

Information security policy is a set of rules, directives, procedures and practices that provide clear guidance on how the organization manages, protects, and shares information. The policy should concur with relevant laws, legislation, applicable standards such as the National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) as well as other internal organizational policies that exist. Security policy is a critical aspect of security governance, and without it there is no mechanism to enforce standards and govern effectively.

TIP

For guidance refer to Information Security Policy of the following cities:

- San Jose
- New York
- Seattle

2.1.4 HOW CAN CITIES AND CONNECTED COMMUNITIES DRAFT A SECURITY POLICY?[6]

A well-designed security policy is implementable, enforceable, and easy to understand. It should include the following:

i. **Policy Rationale** – Clearly define why the policy is needed. This can include a business, legal or a regulatory rationale.

ii. **Scope** – Define who and to which systems the policy applies and clearly state any exceptions and exclusions that apply. The policy should be mandatory for everyone to whom it applies.

iii. **Policy Statement** – Describe expected outcomes and goals, and detail how employees should follow the policies in their work.

TIP

- Refer to 50 security policy templates provided freely by SANS to draft your own policy.

5 Educause. (n.d.-b). Security Policies. Retrieved April 2021, from https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program/resources/information-security-guide/security-policies

6 Ibid.

iv. **Roles and Responsibilities** – State who is responsible for enforcing the policy and monitoring its implementation. The policy can also define who is involved in security governance.

v. **Definitions** – Define any acronyms, jargons or words that may be ambiguous or may have different interpretations.

vi. **Related/Relevant Documents** – Include any related or relevant standards, frameworks, or policies that should be referred to in order to gain a thorough understanding of the policy.

vii. **Policy History (if any)** – Include reference to previous versions of policy (if any) and highlight all significant changes in the new policy vis-à-vis the previous version.

A comprehensive security policy can also include standards, procedure, and guidelines.

QUESTIONS TO CONSIDER

- Who should be consulted and included in the process of drafting a security policy?
- How will the policy be communicated with both internal and external stakeholders?
- How to make the policy enforceable?
- Who is responsible for enforcing the policy?

TABLE 1. STANDARDS, PROCEDURES, AND GUIDELINES

	ROLE	DESCRIPTION
Standards	Measurement (How much?)	Minimum action needed to comply with policies.
Procedures	Detailed Steps (How? When? Who?)	Detailed step-by-step checklists to perform a task.
Guidelines	Recommendations (What? How? When? Who?)	Advice and recommendations for employees to do their job appropriately in line with policies.

Source: Educause.

2.1.5 WHAT ARE SOME FRAMEWORKS AND STANDARDS FOR MANAGING CYBERSECURITY RISK?

There are several frameworks and standards that provide guidance on managing information security risk. Prominent ones include Minimum Safety Requirements for Federal Information and Information Systems (FIPS 200), Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy (NIST Special Publication (SP) 800-37 Rev. 2), Center for Internet Security (CIS) controls, and Risk Management – Guidelines (ISO 31000:2018).

TIP

Refer to a list of cybersecurity standards here.

The NIST Cybersecurity Framework, when complemented with the NIST Risk Management Framework, provides the most comprehensive framework for cybersecurity risk management. The Risk Management Framework provides inputs and guidance on how to establish controls, standards and requirements to manage risk given the functions, categories, and sub-categories defined in the Cybersecurity Framework. Take into account the resources, culture, organization structure, and legal requirements when selecting a framework that works best for your organizational goals and needs.

TIP

Refer to GCTC-SC3 Cybersecurity and Privacy Advisory Committee Guidebook for step-by-step guidance on how to implement NIST Risk Management Framework.

CAUTION: GOVERNANCE AND MANAGEMENT SHOULD NOT BE CONFUSED. WHILE GOVERNANCE RELATES TO "DOING THE RIGHT THING", MANAGEMENT IS ABOUT "DOING THINGS RIGHT."

GOVERNANCE	MANAGEMENT
Oversight	Implementation
Authorizes decision rights	Authorized to make decisions
Enact policy	Enforce policy
Accountability	Responsibility
Strategic planning	Project planning
Resource allocation	Resource utilization

Source: Educause.

2.2. UNDERSTANDING CYBERATTACKS

2.2.1 WHAT IS A CYBERATTACK?

Cyberattack is defined as an "attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information."[7] Cyberattacks can be grouped into un-targeted and targeted cyberattacks. The un-targeted cyberattacks target systems, devices, and users indiscriminately. A targeted cyberattack is where the attacker strategically singles out a system because they have some interest in the organization's business. Targeted attacks can be more dangerous as they may even extend to an employee's personal computer system, or those of family members.

7 NIST. (n.d.). Computer Security Resource Center. Retrieved April 2021, from https://csrc.nist.gov/glossary/term/Cyber_Attack

2.2.2 WHO ARE CYBER ATTACKERS?

Cyber attackers can be classified into four major groups based on their intent:

TABLE 2. TYPES OF CYBER ATTACKERS

TYPE	DESCRIPTION
Cyber Criminals	They usually target organizations, systems, or personal data that can be monetized on the dark web or controlled in demand for a ransom payment. They can indulge in sophisticated hard-to-discover attacks.
Hacktivists	They are individuals who perform the attack to reinforce their political, social or religious, or personal ideology.
State-sponsored Attacks	These are attacks carried out against a particular targeted country or its assets or interests, under the sponsorship of an adversary nation-state, where the attacker wants to create social, political, economic or military instability advantageous to the penetrating state.
Insider Threats	These are attacks carried out by someone with knowledge of and access to an organization's computer system, usually by virtue of employment or a working relationship with the targeted organization. Attacks can be from employees, vendors or external partners. The trust factor involved makes it hard to detect. They can be malicious, accidental or even a result of negligence.

Source: Appsealing.

2.2.3 WHAT ARE THE DIFFERENT TYPES OF CYBERATTACKS THAT CITIES AND COMMUNITIES SHOULD KNOW ABOUT?[8]

Cyber attackers are becoming more sophisticated and so are the types of cyberattacks. The two most common type of cyberattacks that every city and community employee should know about are:

- **Malware** – The term is used to describe a malicious code and includes ransomware, spyware, viruses and worms.
    - **Ransomware** is a form of attack where the adversary blocks access to key components of the network or system unless a ransom is paid. CISA's Ransomware Guide provides guidance on best practices for ransomware prevention and a checklist for ransomware response. Refer to a resource repository for a list of resources on ransomware.

TIP

Read about 10 most common types of cyberattacks of all times.

TIP

This two-hour interactive experience allows city officials and community members to learn what it takes to combat ransomware.

8 Cisco. (n.d.). What Is the Difference: Viruses, Worms, Trojans, and Bots? Retrieved April 2021, from https://tools.cisco.com/security/center/resources/virus_differences#3 ; Cisco. (n.d.-a). What are the Most Common Cyber Attacks? Retrieved May 2021, from https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html

- **Spyware** covertly extracts information. Read more about top 15 malicious spyware actions.
- **Viruses** as the name suggest are malicious codes that can spread from one computer to another from an infected host. It works by inserting a copy of itself into and becoming part of another program. The severity of the virus may range drastically from temporary effects to damaging data or software causing denial-of-service (DoS) conditions.
- **Worms** are much like viruses; they differ in that they can be standalone and do not need a host software to spread.

Other kinds of malware include Trojans Horses and Bots.

- **Phishing** – The use of e-mails that appear to originate from a trusted source to trick a user into entering valid credentials at a fake website. Phishing is an increasingly common cyberthreat and the easiest to prevent if employees are repeatedly trained to detect, avoid, and report it. Learn about different types of phishing attacks here.

TIP

Take the Jigsaw Phishing quiz to test if you can identify a phishing email.

Take Cisco's Phishing Awareness Quiz here.

2.2.4 HOW DO CYBERATTACKS WORK?

To defend better, it is important to understand the different stages of a cyberattack. The Cyber Kill Chain framework created by Lockheed Martin defines the different phases of a cyberattack – Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and Control, and Actions on Objectives – knowing these stages can help in early identification and prevention of cyber incidents. For simplicity, these phases can be condensed into four primary stages.

DEFINITION

Vulnerability refers to weakness in an information system, security procedure, or internal control that could be exploited by an adversary.

TABLE 3. STAGES OF CYBERATTACK

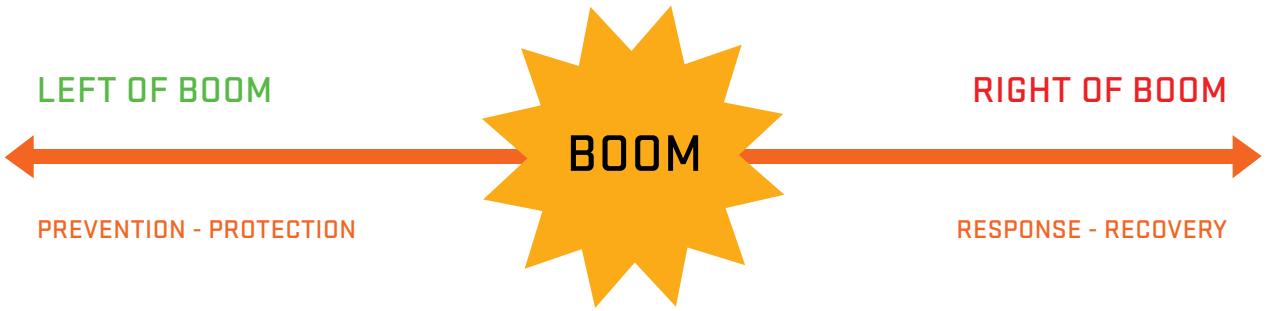
STAGE	DESCRIPTION
Survey	Investigating preliminary information about the target and potential vulnerability to design a plan for attack.
Delivery	Reaching to a point in a system or network where the vulnerability can be exploited.
Breach	Gaining unauthorized access by exploiting the vulnerability.
Affect	Meeting the goals of the attack by carrying out malicious activities or altering the system.

Source: National Cybersecurity Center, Government of U.K.

2.2.5 WHAT IS THE CYBER BOOM MODEL? HOW DOES IT HELP CITIES AND COMMUNITIES APPROACH CYBERSECURITY?[9]

Cybersecurity experts are increasingly using counter-terrorism models and strategies to prevent and protect against cyberattacks. A "cyber boom" refers to the time of the cyber incident; "left of boom" refers to events preceding the attack, and "right of boom" refers to events after the attack. This model provides a clear approach to cybersecurity measures for cities and communities by breaking down an incident into three phases.

FIGURE 1. CYBER BOOM MODEL



Source: Labor Relations Institute

- **Left of Boom** refers to the strategies that can be undertaken to prevent and protect against cyberattacks.
- **Boom** refers to the time when the cyber incident happens and is ongoing.
- **Right of Boom** is when the incident has happened, and the organization and authorities are assessing the damages. It refers to the strategies that can be undertaken to document the assessment, identify the cause and source of attack, repair or make up for the damage and learn lessons from what went wrong.

Part 3 of this section provides a litany of best practices that cities and communities should follow based on the three phases of the cyber boom model.

9 Nyotron. (2019, October 4). What is "Cyber Boom" and Why Should You Care? https://www.nyotron.com/what-is-cyber-boom-and-why-should-you-care/; Celaya, T., & Winkler, I. (2020, February 28). You Can Stop Stupid. RSA Conference. https://www.rsaconference.com/library/presentation/you-can-stop-stupid

2.3. BEST PRACTICES IN CYBERSECURITY

2.3.1 WHAT BEST PRACTICES CITIES AND COMMUNITIES CAN ADOPT TO PREVENT AND PROTECT FROM CYBERSECURITY INCIDENTS (LEFT OF BOOM)?[10]

- **Establish Cybersecurity Governance and Define Roles** – Much of the problem with cybersecurity is that cities and communities fail to document and communicate their processes, controls, and procedures properly. The first step to effective cybersecurity is to set up cybersecurity governance and define roles to create accountability.

- **Cybersecurity Assessment** – What is unknown cannot be protected. Cybersecurity risk assessments can help cities and communities identify vulnerabilities and risks across people, processes, systems, and vendors. The risk assessment should include:

    - *Asset management* – accounting for all the assets that are owned and should be protected by the city and community.

    - *Maturity assessment* – identify where the city or community is in terms of cybersecurity maturity and assess the gaps that need to be filled. Refer to the resource repository for a list of cybersecurity maturity assessment frameworks.

    - *Penetration testing* (pen test or ethical hacking) – a simulated authorized cyberattack on a computer system to evaluate the strength of the system security. For cities and communities that do not have in-house expertise, they can hire independent analysts or external vendors to undertake the assessment. Partnering with local academic institutions is also a cost-effective way to undertake cybersecurity assessment.

- **Awareness Training and Education** – Cybersecurity is everyone's responsibility irrespective of their role in the city or community. Cybersecurity is not a matter of "if" an incident occurs but rather "when" it occurs. Make cybersecurity awareness a part of all onboarding procedures. Provide regular training to every city employee and community member on good cybersecurity hygiene and how to detect and report potential cyberattacks. The primary goal of education and training should be to equip employees with the tools, information and controls needed to perform their duties safely.[11] Refer to the resource repository for a list of cybersecurity awareness and training resources available for cities and communities.

TIP

MIT has a public interest cybersecurity clinic that helps cities and towns with their cybersecurity vulnerability assessment.

TIP

Refer to these cybersecurity Dos and Don'ts!

10 Thompson, L. N. (n.d.). Cybersecurity Best Practices for Municipalities. New Hampshire Municipal Association. Retrieved April 2021, from https://www.nhmunicipal.org/town-city-article/cybersecurity-best-practices-municipalities

11 Celaya, T., & Winkler, I. (2020, February 28). You Can Stop Stupid. RSA Conference. https://www.rsaconference.com/library/presentation/you-can-stop-stupid

- **Start with Small Steps** – The State and Local Government Security report found that most cyberattacks on state and local governments are not sophisticated and can be prevented by following simple cybersecurity practices. Some of these steps include:
    - **Move Beyond Passwords.** Passwords are passé. Passwords should indeed be strong but even strong passwords place too much trust in the users. As such, password use has largely been abandoned by non-password schemes such as Microsoft's login tools that leverage push requests to your phone. Make a move towards passwordless security—a form of zero trust. To get started read NIST's Zero Trust 101, read this guide on how to move beyond passwords, review these top 10 passwordless use cases and ask these top 10 questions to your potential passwordless provider/vendor.
    - **Two/Multi-Factor Authentication (2FA/MFA)** provides an additional layer of security. In addition, to a username and password, it requires additional information to log the user into their system or network. 2FA/MFA can prevent a cyberattack even if the password is guessed, leaked or hacked.
    - **Encryption** should be used to ensure the safety of all devices (computers, laptops, hard drives etc.) owned by the city or community. Full-disk encryption is used to protect "data at rest", it can be used to prevent data breach in case a device is lost or stolen. Refer to the resource repository for resources on encryption best practices.
    - **Regular Updates** are needed to maintain the security of all devices. Outdated systems expose a major vulnerability making systems prone to cyberattacks. System updates should be done routinely and made mandatory across departments. Applications that don't run after security updates should be updated themselves rather than indefinitely deferring updates.
    - **Regular Data Backup** is the best way to prevent data loss. A recent data backup can be a savior in the event of a ransomware attack. All systems and devices should perform routine backups of all files and data, and backups should be stored offsite to protect against loss of both the primary and backup information in case of fire or other disaster.

DEFINITION

Zero Trust is a security concept that requires all users, even those inside the organization's enterprise network, to be authenticated, authorized, and continuously validating security configuration and posture, before being granted or keeping access to applications and data.

TIP

Follow these best practices for data backup.

These steps if taken diligently can go a long way in preventing cyberattacks, mitigating potential damage in an event of a cyberattack and even bring about a change towards a culture of security.

- **Enforce Security Standards on Vendors and Others** – Cities and communities engage with external vendors to meet their organizational needs. When online and when communicating via email or other digital methods ensure vendors comply with the city or community's security protocols and enforce security requirements and standards applicable to the vendors. Perform thorough due diligence and assessment of all vendors who have access to confidential data or who interact with the city or community's systems and networks. Due diligence should include the evaluation of the tool or technology that the city or a community is procuring. The benefit of adopting a technology should be weighed against its cyber-risks. A report by the Center for Long-Term Cybersecurity ranked different smart city technologies based on their cybersecurity vulnerability to help local policymakers make decisions regarding technology adoption based on varying degrees of cyber-risk levels.

- **Known Mechanism for Reporting a Potential Cyberattack** – Inform employees how and to whom they should report a potential cybersecurity attack. For instance, if an employee receives an email that seems suspicious, they should know who to contact to verify the authenticity of that email and whom to report to in case it is in fact a phishing email.

- **Incident Response Planning** – Build a cyber incident response team who will act as first responders in the time of crisis. The team should have a response plan in place. To create a response plan, think through different threat scenarios and draft a chain of reaction that should be triggered to stop, mitigate, and address the attack. Moreover, know who should be informed in case of a breach, and who should you report to – police department, FBI, CISA, or some other federal agency – depending on the nature and magnitude of the attack. In case of a data breach, know which breach notification applies depending on the city or community's jurisdiction.

- **Cyber Insurance** – Allocate a portion of IT budget to cybersecurity depending on the size of the city or community. Use a part of this allocated budget to purchase cyber insurance to mitigate the economic cost that would be incurred in case of an incident.

TIP

Refer to New York City's Cybersecurity Requirement for Vendors & Contractors.

TIP

- Refer to Tabletop Exercises – Six scenarios to help prepare your cybersecurity team.
- Refer to data breach notification laws by state.
- Refer to CISA's guidance on reporting cyber incidents.
- Report a cyber incident to CISA.

TIP

Refer to this guidance from National Association of Insurance Commissioners (NAIC) for tips on purchasing Cyber Insurance Policy.

QUESTIONS TO CONSIDER

- Who should be consulted for cybersecurity assessment?
- What is the minimum level of cybersecurity training and awareness every employee should receive irrespective of their position and role?
- How to create a culture of cybersecurity?
- Who will undertake the vendor due diligence to ensure that the vendor complies with the security standards?
- How will security standards be enforced on vendors and external partners?
- Who is responsible for reviewing and documenting suspicious cyber activities reported by employees?
- Who should be informed about the incident?
- Where and how should the incident be reported?

2.3.2 WHAT ARE THE BEST PRACTICES DURING A CYBERATTACK (BOOM)?[12]

This is where the planning steps taken to the left of boom will come in handy. Once the attack has been detected the cybersecurity leadership should move fast to:

- **Contain** – If the attack is still on-going take immediate steps to contain it and take measures to mitigate harm. Shutting down networks and systems may save some of them.
- **Orient** – Identify the type of attack and ensure safety of employees, then data, and finally organization's reputation.
- **Prepare to Act** – Prepare to inform stakeholders, report the incident to concerned authorities, preserve evidence, and alert legal and PR team. This is where the incident reporting planning will help cities and communities move faster in the time of crisis.

TIP

Five to-dos to maintain reputation after cyberattack.

12 IBM. (2018). Beyond the Boom Improving decision making in a security crisis [Slides]. IBM. https://www.ibm.com/downloads/cas/BEGYVQZV

2.3.3 WHAT ARE THE BEST PRACTICES AFTER A CYBERATTACK (RIGHT OF BOOM)?

After the incident has taken place, prepare to respond and recover. These steps would include:

- **Act** – Inform stakeholders and report the incident to relevant authorities.
- **Document** – Identify the source and the timeline of the incident. Take stock of the damages. Hold people accountable for their mistakes by documenting the organizational, economic and social cost of the incident. Identify gaps in security procedures that led to the boom.
- **Initiate Recovery** – Undertake damage control with regards to the technical, economic, and reputational costs incurred by the organization.
- **Correct** – Focus on making corrections and remedying processes that created the vulnerability. Improve your cybersecurity standards, procedures, and practices based on the lessons learned from the incident. It is important to understand that cybersecurity is an iterative process, and no one gets it right all the time.

QUESTIONS TO CONSIDER

- Who should be involved in the documentation process?
- How will the costs be evaluated?
- How will the learning be communicated with the stakeholders?
- What needs to be changed, improved or eliminated to prevent a similar attack in the future?

If you want assistance, there are companies which specialize in cyberattack response. If you have a cyber insurance, you may want to take specific steps. It will be beneficial to know whom you plan to engage in case of a cyberattack before it happens.

2.4. CYBERSECURITY RESOURCE REPOSITORY FOR CITIES AND COMMUNITIES

NO.	TITLE/ORGANIZATION	LEVEL	WHAT CAN YOU EXPECT TO LEARN?
		CYBERSECURITY COMPLIANCE	
1	Cybersecurity Compliance: A Comprehensive Guide	Beginner	A simple guide to understand cybersecurity compliance. It describes the regulatory, legal and security controls to ensure the integrity of data, systems and networks.
		RANSOMWARE	
2	A Starting Point for Smart Cities and Communities on Managing Ransomware Risk	Beginner – Intermediate	A great easy to read paper that explains ransomware and associated risks and consequences. It also discusses consideration for planning, controls, and training.
3	Ransomware Protection Plan	Beginner – Intermediate	A short four-page document that provides tips for protecting and preparing against ransomware.
4	Securing Data Integrity Against Ransomware Attacks	Intermediate – Advanced	This NIST document provides guidance to prepare organizations to address any future data incidents.
5	FBI's Ransomware Guidance	All	FBI's guidance on ransomware prevention and what to do in event of an attack.
		CYBERSECURITY MATURITY ASSESSMENT	
6	Security Maturity Self-Assessment	All	A guide from Contra Costa County Employment & Human Services. It helps to quantitatively assess your current level of cybersecurity measures.
7	SIMM 5300-C – Cybersecurity Maturity Metrics (XLSX)	All	Cybersecurity Maturity Assessment from the California Department of Technology. Read more about how they developed the metrics here.
		TRAINING AND AWARENESS	
8	SANS Security Awareness Kit	All	A comprehensive kit from SANS with templates for security awareness program charter, annual program scheduler, presentation slides, phishing planning guide, work from home deployment kit and a program planning kit.
9	Security Infographics	Beginner – Intermediate	A collection of over 56 easy to read infographics that can be used for awareness training and security education.

NO.	TITLE/ORGANIZATION	LEVEL	WHAT CAN YOU EXPECT TO LEARN?
10	National Cybersecurity Awareness Month (NCSAM) Resource Kit	All	A list of resources for cybersecurity awareness. It also explains what the NCSAM is and why is it important.
11	Rochester Institute of Technology (RIT)	Beginner	RIT provides posters and videos for security awareness training.
12	List of Glossaries	Beginner	Refer to this resource for a list of glossaries that explains security and privacy terms and concepts.
13	Cybersecurity: A Social Engineering Approach at MIT	All	A cybersecurity clinic at MIT that helps cities and nonprofits with their cybersecurity assessments as well as provides resources for training and education.
14	CISCO Phishing Awareness Quiz	Beginner	Use this quiz to test employee's awareness of phishing.
15	Cybersecurity for Critical Urban Infrastructure (Course on edX)	Beginner – Intermediate	A course to prepare city officials, agency staff and a new generation of students seeking to serve as cybersecurity consultants to understand, help prevent and manage cyberattacks on vulnerable communities across America.
16	CISA – Stop.Think.Connect	All	List of resources and tips from CISA to increase understanding about cyberthreats.
	ZERO TRUST		
17	10 Tips to Enable Zero Trust Security	All	Read Microsoft's top 10 tips for zero trust security.
18	Getting Started with Zero Trust – Never Trust Always Verify	Intermediate – Advanced	A white paper that explains the concept of zero trust, how it works, its challenges, and the different stages involved in laying the foundations for zero trust security.
	ENCRYPTION		
19	Best Practices Encryption	Intermediate – Advanced	This short document provides guidance on three best practice encryption approaches.
20	Operation Best Practices for Encryption Key Management	Intermediate – Advanced	This resource from CISA discusses six key management use cases and provides guidance on encryption best practices.

NO.	TITLE/ORGANIZATION	LEVEL	WHAT CAN YOU EXPECT TO LEARN?
		INCIDENT PLANNING AND RESPONSE	
21	Cyber Incident Response	All	A list of resources from CISA on cyber incident response. It provides guidance on how to report cyber incidents to the federal government and training for incident response.
22	Sensitive Data Exposure Checklist	All	A template that can be used to document the data exposed in an event of a cyber incident.
23	Data Incident Notification Toolkit	All	Templates for notifying data incidents.
24	AT&T's Insider's Guide to Incident Response	All	A comprehensive guide from AT&T on how to prepare your incident response team, response processes and procedures and tools for response.
		MISCELLANEOUS	
25	Cybersecurity Resources for Local Governments	All	A compilation of information security resources available to local governments in Washington State.
26	Protecting Our Data: What Cities Should Know About Cybersecurity	All	A report by the Nation League of Cities presents results from a survey on cybersecurity preparedness of cities. The report discusses policy landscape and resources of local governments and provides examples and recommendations for local leaders.
27	NIST Small Business Cybersecurity Corner	All	A list of resources provided by NIST for small business which can also be used by local governments for education and training purposes.
28	Michigan Cyber Partners	All	A partnership between various divisions at the State of Michigan, including Michigan Cyber Security and the Michigan State Police, and local public entities across Michigan to strengthen, improve, and promote cybersecurity resources and best practices.
29	Cybersecurity Planning Guide/ Federal Communications Commission	Beginners	This simple easy to read guide provides best practices, resources and examples for information security practices.