Cybersecurity Guidebook for Local Government 2.0

A publication made possible by:
GMIS International-Indiana Chapter

Technical assistance provided by:
Cybersecurity Infrastructure and Security Agency (CISA)
Indiana Executive Council on Cybersecurity

Cyber Guidebook

A practical guide to secure local government IT

Protecting a local government agency or department is a challenge, and it's not always easy to know where to start. Whether your job is working in the IT department, fulfilling a larger role, as a director, Chief Information Officer, or Chief Information Security Officer, or you're an elected official, this updated guidebook is intended to serve as a roadmap for attaining – and having in place -- the key components needed for maintaining a good cybersecurity posture.

Keep in mind, this is not a comprehensive list of every cybersecurity solution you *should* have; rather, it represents what you must have that's essential for protecting your data.

This guidebook is based on government, commercial, and academic best practices, and insurance industry requirements, as well as an analysis of real-world local government cybersecurity incidents.

The only secure computer is an offline computer. No solution will provide 100 percent protection. However, you can use this guide – beginning with the "Necessary Nine" checklist – for helping you and your department or organization stay protected as much as possible in today's ever-changing world while, at the same time, serving the people in your community.

TABLE OF CONTENTS

“Necessary Nine”

The following are nine steps that are essential for protecting your critical system that you can review with your cybersecurity/IT staff, managed service provider (MSP). A detailed explanation can be found on the pages as referenced in the table of contents. This is just a starting point, not an all-inclusive list, but rather a list of things that are critical to having a good cybersecurity posture.

NECESSARY NINE		
1	**Backups**	
	System in Place	☐
	Tested	☐
2	**Endpoint Detection and Response (EDR)**	
	System in Place	☐
3	**Firewall**	
	System in Place	☐
	Monitored	☐
4	**Email Filtering**	
	System in Place	☐
	Monitored	☐
5	**Multifactor Authentication**	
	System in Place	☐
6	**Web Filter**	
	System in Place	☐
7	**Security Awareness Training**	
	System in Place	☐
8	**Updates**	
	System in Place	☐
9	**Policies/Plans**	
	Policies in Place	☐
	Disaster Recovery Plan	☐
	Incident Response Plan	☐

Backups

Odds are, you will eventually experience a cyber incident or a cyberattack, and you'll need to be sure you can recover both data AND operations.

There are two basic categories of backup:

1) Data – Content, such as files and emails
2) Operations – The equipment required to access the files and email

How to identify what to back up?

The easy answer is everything. Easy to say, difficult to achieve. Start by focusing on the processes your agency performs. If all the computers were turned off, what would you *not* be able to do? Pay employees, take tax payments, book-in/book-out out inmates, provide emergency services – dispatch police or fire, conduct court? It's important to identify those systems required to keep local government operational.

Ensure backups are:

- **Offline/Airgap/Immutable** – Make sure your backups are either offline, not physically connected to your network, or are immutable (cannot be changed).
- **Tested** - Untested backups are not backups. The internet is filled with case histories from victims who thought they had backups, but when they went to restore their systems, they discovered something went critically wrong.

Common Implementations:

- Plan ahead for your data backup.
- Establish a lifecycle operations calendar.
- Review backup logs daily.
- Follow the 3-2-1 rule of backup
- Identify and resolve backup window failures daily.
- Locate and back up orphan system and volumes.
- Centralize and automate backup management.
- Test your backups.
- Employ proper security
- Use your vendors effectively.

Resources:

- 10 Steps to Creating an Effective Data Backup Strategy (techtarget.com)
- Backup Strategy Best Practices Organizations Should Follow (nakivo.com)Weathering the Storm: 5 Step Backup Strategy - North Carolina Bar Association (ncbar.org)

Endpoint Detection and Response (EDR)

Keep your computers from performing malicious activity.

What is Endpoint Detection and Response?

Endpoint Detection and Response, or EDR, is modern antivirus. Software that is installed on computers to identify, stop, and remove malicious software and activity. Unlike traditional antivirus, EDR watches for the behavior of malicious software and not for the file itself.

Endpoint is another name for a computer device. Servers, PC's, and laptops are all endpoints.

But, having EDR software on a computer is not enough. Someone needs to configure the software appropriately and respond when malicious activity occurs.

Ensure EDR:

- Installed on every device
- Monitored with response 24x7x365

Resources:

- **SLCGP Endpoint Program**
  - Federal grant program administered by the state that provides local governments Crowdstrike EDR for no cost. Solution is monitored, with response and cleanup, by Crowdstrike Falcon IT security professionals (who are not employed by the state).

- **MS-ISAC EDR**
  - The mission of the Multi-State Information Sharing and Analysis Center® (MS-ISAC®) is to improve the overall cybersecurity posture of U.S. State, Local, Tribal, and Territorial (SLTT) government organizations through coordination, collaboration, cooperation, and increased communication.
  - There is no cost to join the MS-ISAC, and membership is open to all U.S. SLTT government organizations. The only requirement is agreeing to the Terms and Conditions, which outlines a member's responsibilities to protect information that is shared.

Firewall

Keep the bad guys out of your network.

A firewall is the border wall between your computers and the Internet. It is what controls what network traffic is allowed in and out.

All day every day, criminal gangs, foreign governments, and would be cybercriminals are scanning the Internet indiscriminately for systems prone to attack.

Do's (You Want to be Sure to Do):

- No incoming Remote Desk Protocol (RDP)
- Up-to-date firmware
- Administrative access from inside only
- Geo-filtering (helps improve security by blocking traffic from regions with high fraud or cyberattack risks.

Resources:

- CISA – Securing Network Infrastructure Devices
- Firewall as a Service (FWaaS) – StateTech Magazine

Email Filtering

Stop malicious emails before employees even see it.

Even today, by far, email continues to be the most common and primary means of compromise. An email filter is software that scans incoming email for spam, fraud, and malicious content and removes it.

The following is a list of attachment file that should never be allowed:

Blocked Attachment File Types				
386	diagcab	jse	pptm	settingcontent-ms
1qy	dmg	lzh	printerexport	shb
3gr	docm	mcf	ps1	shs
add	dotm	mdb	ps1xml	sldm
ade	exe	mde	ps2	theme
all	fan	msc	ps2xml	url
appcontent-ms	grp	msh	psc1	vb
arc	gz	msh1	psc2	vbe
asp	hip	msh1Xml	psd1	vbp
bas	hpj	msh2	psdm1	vbs
bat	hta	msh2xml	PY	website
bz2	htm	mshxml	pyc	ws
cer	html	msi	pyo	wsh
chm	Iha	msp	pyw	xbap
class	inf	mst	pyz	xii
cmd	Ink	msu	pyzw	xla
cnt	ins	ocx	r09	xlm
com	iso	pcd	rar	xlsm
cpl	isp	pif	reg	xltm
ct1	jar	pl	scf	xnk
dbx	jnlp	potm	scr	zip
der	js	ppsm	set	

Ensure by:

- Using Realtime Block Lists
- Enabling SPF, DKIM, DMARC

Resources:

- CISA Insights - Cyber: Enhance Email & Web Security
- How state, local government need to build a cyber resilience strategy for email | StateScoop

Multi-Factor Authentication

Make sure it's really your employees logging in.

What is MFA?

MFA stands for Multifactor Authentication, sometimes referred to Two-Factor Authentication (2FA). Simply put, it requires you to have 2 of the following types of authentication methods: **something you know** (password), **something you have** (phone), and **something you are** (biometric data -face or fingerprint).

Why?

Passwords get stolen. Maybe not from your agency, but a good portion of people reuse the same password at a lot of places. When a target is breached, that password is used everywhere, in the event that the password was or is being reused with other accounts.

Ensure MFA is required for:

- VPN
- Email
- Cloud Services

Resources:

- More than a Password | CISA
- Require Multifactor Authentication | CISA

Web Filter

Don’t let malicious traffic in.

What is a web filter?

A device or service that monitors Internet traffic content and blocks computers from connecting to malicious and unauthorized websites.

Why?

Malicious emails get through email filters, employees accidentally go to fake websites by mistyping or clicking ads, websites get compromised, and you MUST have a way to stop that traffic before it impacts your network.

Ensure:

- Users are diligent about clicking only good links.
- You are filtering traffic to harmful websites.

Resources:

- MS-ISAC DNS Filtering
- Three tips for protecting your business with web filtering - NH Business Review (nhbr.com)
- Top Practices for Effective Content Filtering (safedns.com)

Security Awareness Training

People are the weakest link.

Why is security awareness training important?

Training people on how the bad actors compromise critical systems will help educate them so they know how to better protect themselves and the agency or department they work for to help avoid being vulnerable to a cyber incident or cyberattack.

You're only as "protected" as your least-trained user. Training and educating users on good cyber hygiene is critical in helping to ensure that your agency's vulnerability is as minimal as possible.

Ensure:

- How to identify suspicious email
- MFA

Resources:

- KnowBe4
- SLCGP Security Awareness Training

Updates

What?

Keeping your hardware and software up to date is incredibly important. Installing updates (known as patching) ensures that you are protecting your hardware and software from the latest known threats.

Why?

Over time, vulnerabilities are discovered in software and hardware that allow cyber criminals to access systems. Manufacturers will put out updates that address those vulnerabilities, and those should be applied regularly.

Ensure:

- Automatic
- Not just Windows – Patching is done automatically with ALL systems from ALL companies.
- Externally facing devices

Resources:

- **Understanding Patches and Software Updates - CISA.GOV**

Policies/Plans

Have a plan in place.

What?

Just like Employee Handbooks have policies to help prevent lawsuits, local governments need Cybersecurity policies to help prevent cyber incidents. Incident Response Plans are needed when the policies are ignored. Disaster Recovery Plans might be needed if the incident is not caught in time.

Why?

A boat doesn't go anywhere if everyone isn't paddling in the same direction. People in the agency need to know what's expected of them and how to do it.

Ensure:

- Cybersecurity Policies are taught – don't just hand employees a paper to sign.
- Incident Response Plan – What happens when you are hit?
- Disaster Recovery – It happened. Now who do you call?
- Tabletop Exercises – Until you test your plan, it is just paper.
- Payroll / ACH updates – In person only

Resources:

- CyberTrack Assessments
- IOT: Local Government Services (in.gov)
- CISA.gov https://www.cisa.gov/resources-tools/resources/incident-response-plan-irp-basics
- Indiana Information Sharing and Analysis Center (IN-ISAC) CISO-in-a-Box

What's Next?

Talk with your IT Director or MSP about the topics covered in this document. Cyber security is CRUCIAL to ensuring that your agency remains operational, so make it a priority.

In addition to the "Necessary Nine" here are some other key checklist items:

- Inventory/Asset management
  - If you don't know what you have, you don't know what you need to protect. Be sure to keep an up-to-date inventor of all assets.
- Zero Trust
- USB Drives
- Assess /Audit
  - Having a trusted third party assess the systems you have in place is highly recommended. The State of Indiana's Cybertrack program, scheduled through the Indiana Office of Technology, is a great option for assessments.
- Framework
  - Following a framework is key to making sure you continue to make progress on your cybersecurity posture. Following the Center for Internet Security's IG standards beginning with IG1 and continuing through IG3 is a great way to make sure you are on the right path.
  - IG1 -> IG2
- Insurance
  - Take time to understand your cybersecurity insurance policy. Do you have one? What are the terms? Who is the insurer?
  - You can visit the Indiana Cyber Hub and upload for FREE, the Cyber Insurance Toolkit from the Indiana Executive Council on Cybersecurity.
- Intrusion Detection System (IDS) / Intrusion Prevention System (IPS)
  - Monitor network traffic looking for specific activity indicating a compromise.
  - Alert suspicious activity.
  - Respond – IDS is passive, IPS is active.

SLCGP Committee

- The Indiana State and Local Cybersecurity Grant Program Planning Committee ("SLCGP Committee") is formed in response to the federal Infrastructure Investment and Jobs Act (IIJA). The committee will develop, approve, implement, monitor, review, and revise, as appropriate, a strategic plan that establishes funding priorities and approves cybersecurity projects.

Offerings for Local Governments

- Crowdstrike