Protect your bits, bytes & reputation

Be cyber aware & prepare

Niles Kostick, Center Manager
Center for Government Innovation
August 14, 2024

Center for Government Innovation

Be cyber aware & prepare

01
The threat landscape

02
Protect yourself

03
Threat trends

04
How can SAO help?

Be cyber aware & prepare

The threat landscape

Social engineering attacks

How bad is it?

$2.9 billion in losses

Social engineering

- Phishing
- Business email compromise (BEC) attacks

3.4 billion

Spam emails sent every day

91%

Of successful data breaches begin with a phishing email to an employee/victim

Ransomware attacks

How bad is it?

More than 400

Ransomware attacks carried out against US government organizations since 2018

250 million

People impacted due to unavailable services

$ 860 million

In down time costs

Cyber incident reports to SAO

168

Cases submitted since 2018 *(through 8/14/24)*

$35 million

In total losses

40

WA local governments reported as targeted in the past two years

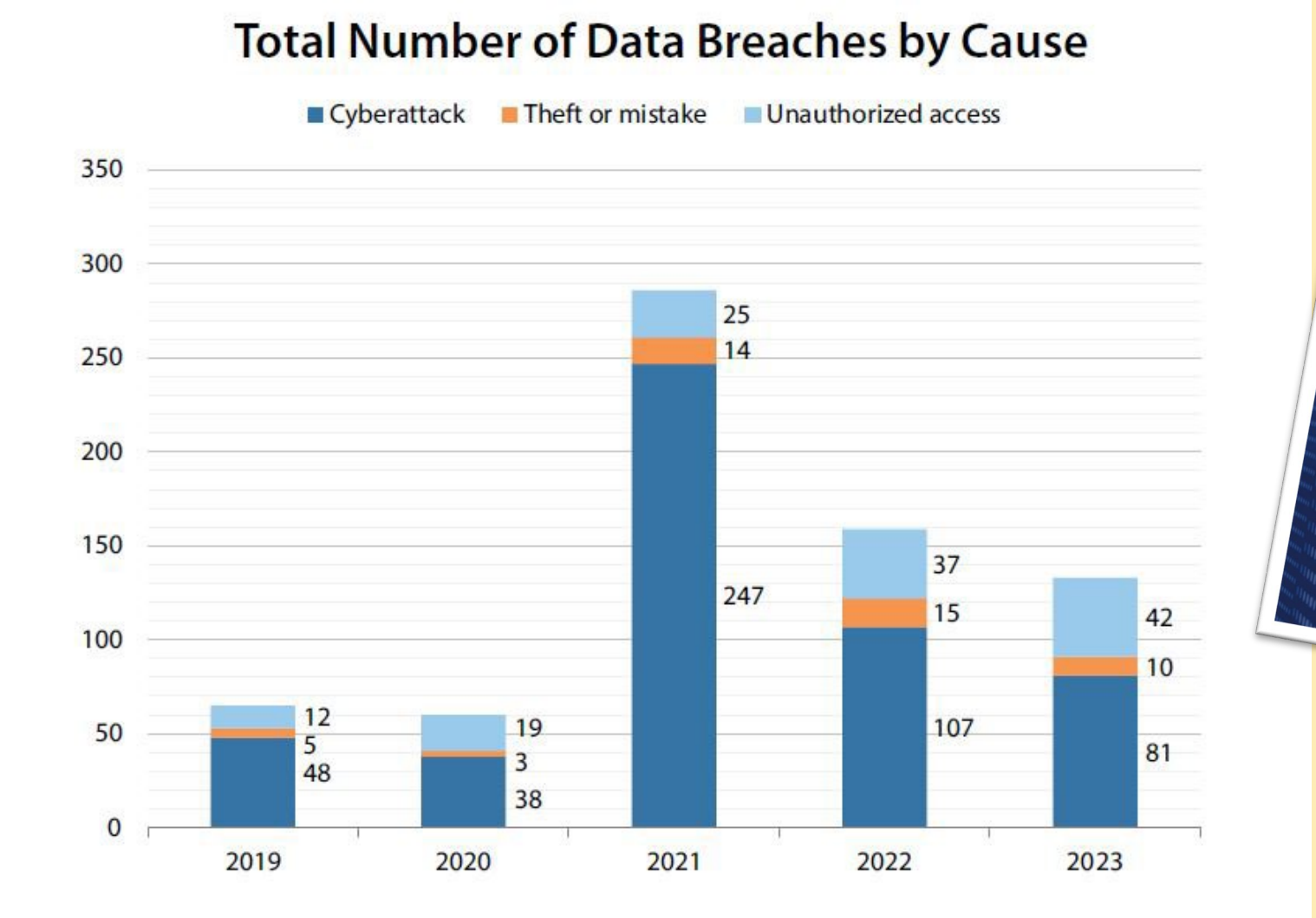
Cyber loss Reported to SAO

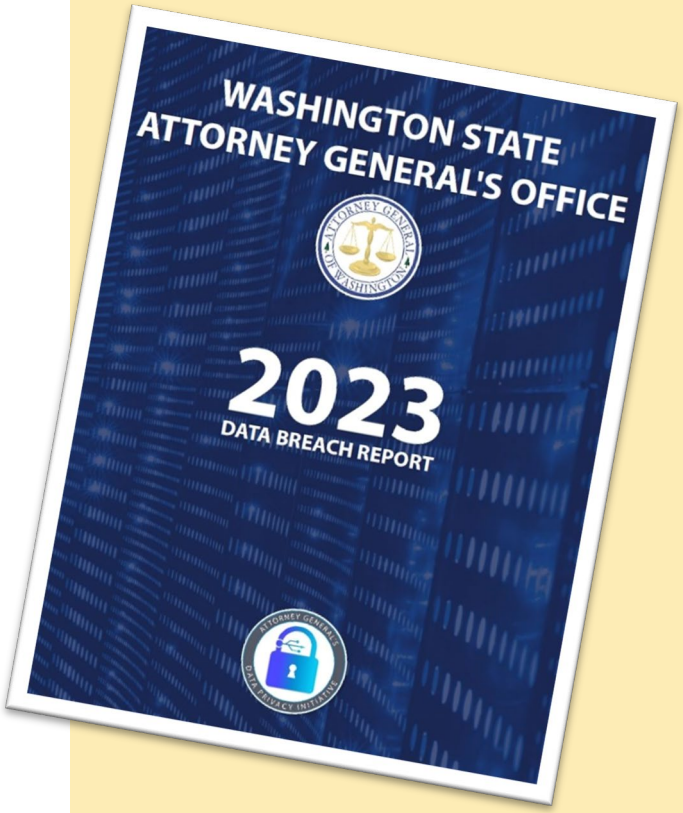
Total cyber losses reported to our Office totaled $35M since 2018

- Gift card
- Payroll
- Vendors

So far, $1.4M in 2024

Cyber incidents reported to AGO





What this means

Average cost of a 2023 data breach in the public sector was $2.6 million

- Lost business costs
- Detection costs
- Post-breach response costs
- Public perception costs

Disruption

- Utility billing
- 911 dispatch
- Property taxes
- Property sales
- Paychecks
- Vendor payments
- Email and voicemail

"It takes 20 years to build a reputation and five minutes to ruin it."

- Warren Buffet

What this means

Be cyber aware & prepare

Protect yourself

Protect yourself

Understand common vulnerabilities

Majority of data breaches include an employee interaction

- Social engineering
- Hacking
- Malicious insiders
- Innocent human error

Protect yourself

Minimize 3rd party vendor risks

Do your homework

- Perform a vulnerability assessment
  - Cyber risk= threat X vulnerability X information value
- Assess vendors in the selection process
- Include requirements in vendor contracts
- Keep an inventory and monitor

Address common risks

- Lack of written/approved IT policies

Policies

What policies do you need?

- Acceptable use
- Passwords
- Incident response
- Email
- Personal device use
- Use of multifactor authentication (MFA)
- Social media accounts

Policies

Training

Address common risks

- Lack of a training program including exercises
- Discussing the importance of following IT policies

Training

Preparedness is critical

What should your program address?

- Our trusting human nature
- How to be responsibly suspicious
    - Slow down
    - Consider the source
    - Question the unusual

Training

Preparedness is critical

Common social engineering schemes:

- Fraudulent emails
- Malicious links & attachments
- Look-alike email addresses
- Posing as an employee, vendor, or executive management

Training

Preparedness is critical

Persuasion & pressure tactics:

- Learn your operations & timetables
- Use pretexting to improve chances of success
- Expressions of urgency and/or anger
- Multiple requests in short period of time

Address common risks

- Lack of a formal patch management plan
- Application misconfiguration
- Lack of system monitoring

System Management

What should system management practices include?

- Current operating systems & software
- Principle of least privilege authorization
- System hardening
- Tracking user behavior

System Management

Address common risks

- Failure to maintain, protect & test data backups

Backup & recovery

What should your backup & recovery practices include?

- Recovery plan testing
- Encrypted, offline data backups
- Multiple backup storage locations

Backup & recovery

Be cyber aware & prepare

Threat trends

Threat trends

Improper use of valid accounts via stolen or compromised credentials increased 71 percent

It's easier to login than hack-in

Threat trends

Backups are increasingly becoming a target for cybercriminals

Higher ransom, more successful ransom payments

Threat trends

Targeting infrastructure for maximum disruption

Physical infrastructure + technology = opportunity for havoc

Finance worker pays out $25 million after video call with deepfake ‘chief financial officer’

By Heather Chen and Kathleen Magramo, CNN
2 minute read · Published 2:31 AM EST, Sun February 4, 2024

Threat trends

Generative AI creating more convincing deep fakes

Attendees looked and sounded just like colleagues he recognized

Threat trends

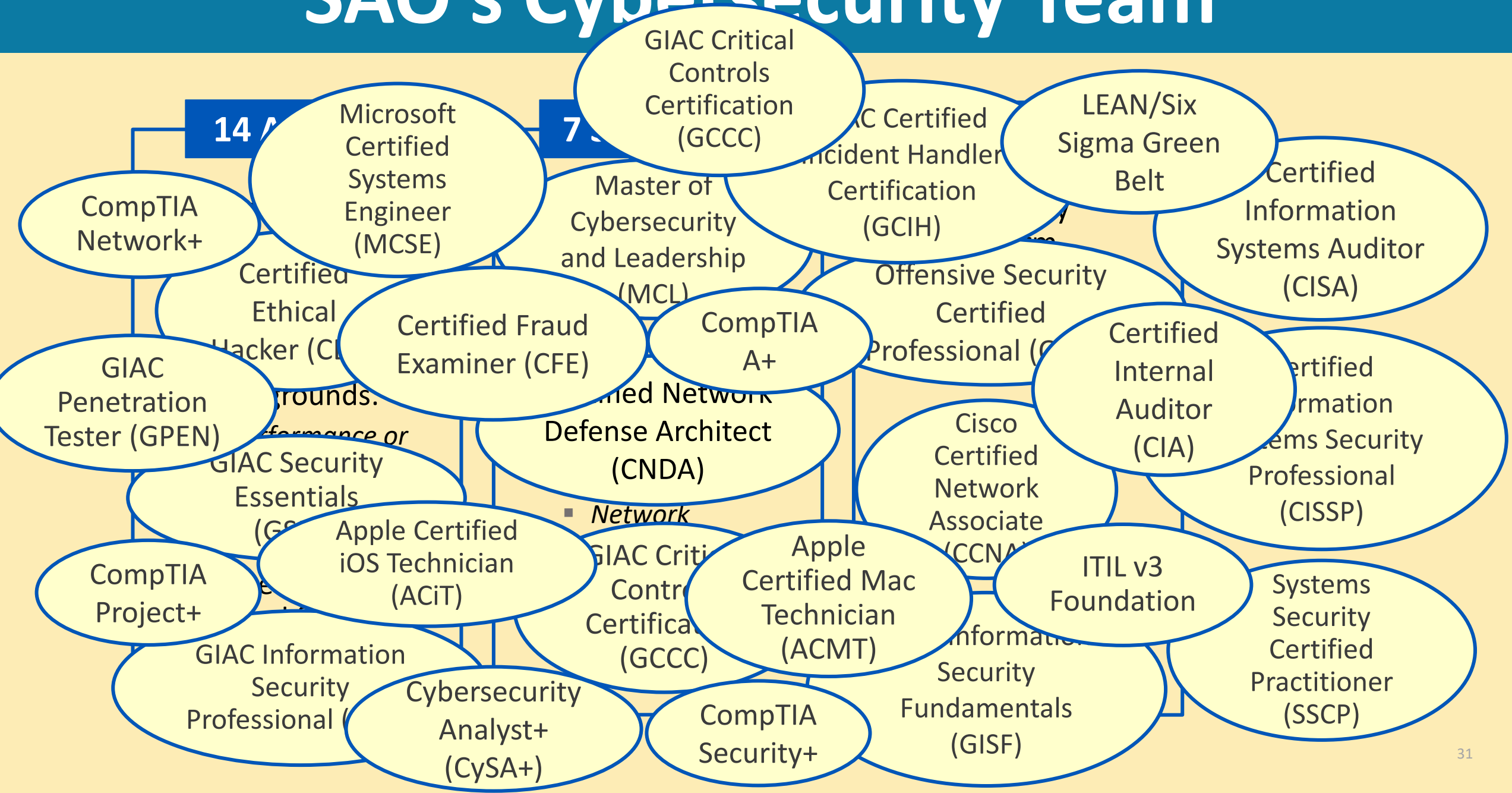
Malicious AI chatbots

WormGPT produced “an email that was not only remarkably persuasive but also strategically cunning.”

Be cyber aware & prepare

How can SAO help?

SAO's Cybersecurity Team



How can SAO help

		Engagement Type			
		Cyber Checkup	Critical Infrastructure Audit	Ransomware Resiliency Audit	Cybersecurity Audit
Types of Work	Controls Assessment	Interviews, documentation, & limited evidence	Limited to one interview w/o evidence	Interviews, documentation, evidence, & technical testing	Interviews, documentation, evidence, & technical testing
	External Penetration Testing	No	Unauthenticated only	No	Comprehensive, depending on scope
	Internal Penetration Testing	No	No	No	Comprehensive, depending on scope
	In-house technical Testing	Limited	No	Comprehensive, depending on scope	Comprehensive, depending on scope

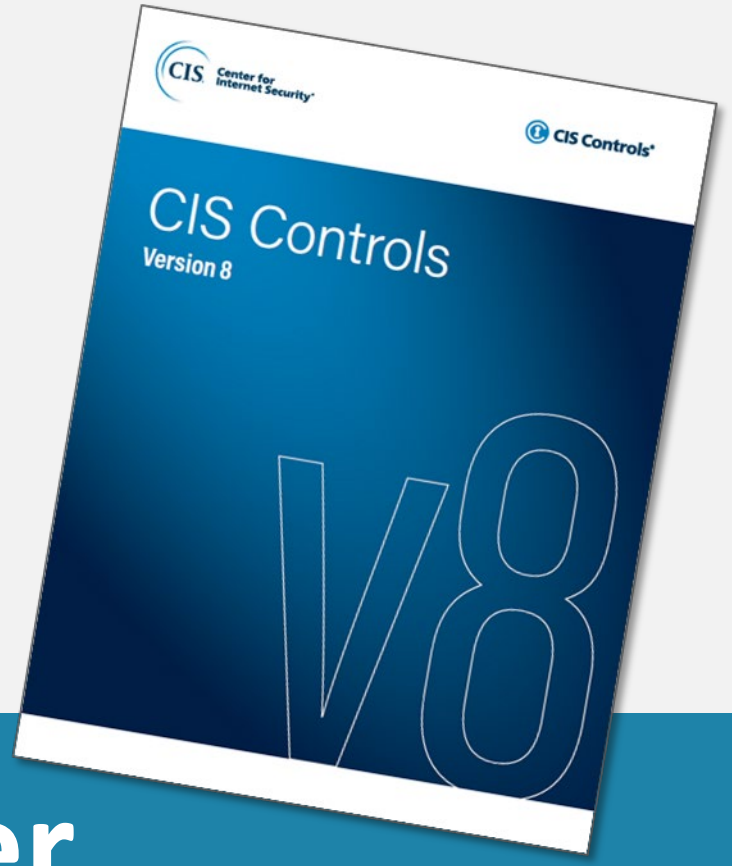
What is a cyber checkup?

- Free 20-point inspection to diagnose cybersecurity gaps
- Recommendations on how to address identified gaps

Cyber checkups

What are they based on?

- The framework provided by the Center for Internet Security's (CIS) Critical Security Controls, Version 8.0
- SAO Cybersecurity audits are based on the same control framework



Cyber checkups

Our control choices…

- CIS Group 1 controls allow the service to be flexible & efficient
- No external software installation
- No elevated privileges required
- Accessible to all skill levels

Cyber checkups

At-a-glance overview

"…results…brought my eyes to something I was overlooking that needed a new solution."

"It was great to have an outside party objectively look at our cyber security…."

"Our team has a background in cybersecurity…checkup easy to understand for anyone."

Cyber Checkup Results: Overview

Area	#	Does your organization…?	Strength of your safeguard		
			Strong	Needs improvement	Not implemented
Policies & Training	1.	Establish and maintain written IT policies	✓		
	2.	Have a cybersecurity awareness program in place		✓	
Incident Response	3.	Have a process for employees to report cybersecurity incidents		✓	
	4.	Designate a lead and a backup to oversee incident response and recovery			✓
	5.	Maintain an inventory of emergency contacts and service providers			✓
Accounts & Passwords	6.	Require employees to use strong and unique passwords	✓		
	7.	Encourage employees to use password managers	✓		
	8.	Restrict administrator privileges to dedicated administrator accounts	✓		
	9.	Protect accounts with administrative			

Cyber checkups

Actionable recommendations

"The results were a wake-up call about our vulnerabilities … "

"… we were able to understand real world ways to implement better security …"

"… immediately improved. The report … included actionable items that didn't require a lot of resources to implement."


Accounts & Passwords

Safeguard 10: Require remote workers to use MFA

About this safeguard

"Remote workers" refers to employees who may access your government's systems or applications remotely. This includes any staff who work from home or who may log in from a different worksite than your main office. This control considers whether you have a policy - and a process - in place for employees working off-site to use multifactor authentication (MFA) whenever they log in to their computers and other government-issued devices or access your software or network. (See Safeguard 9 for a detailed explanation of how MFA works.)

Why this safeguard is important

Working off-site - whether from home, at a client's office, or a remote workplace - adds risks to your IT systems because remote computer connections are more vulnerable to cybercrime than those connected directly to in-office systems. For example, remote employees logging into your network via unsecured, free Wi-Fi in a public space expose their devices - and your network - to criminals who are "network snooping" in hopes of picking up passwords or credit card information. Aside from that, research has shown that remote employees tend to fall for phishing schemes more often than employees working in the office, and they are less likely to inform their manager or IT. MFA adds an extra layer of authentication that hackers will not be able to acquire when trying to log into your government's computer systems.

What we observed during the checkup

Our recommendations

- Ensure your IT policies include requirements for remote users to use MFA when accessing your government's systems.
- Ask your IT support or service provider if MFA is available for your software and network systems, and what you need to do to enable it for employees who access your system or applications remotely. Make sure they complete the activation steps.
- If MFA isn't an option, evaluate the risks of continuing to use that product or service versus the costs of switching to new services with better security features for your remote users.
- If your government can't implement MFA right now, put the following safeguards in place:
  - Monitor user logs for unexpected or suspicious activity, such as someone logging in during non-working hours or from another country. Monitor vulnerable systems like email servers, your virtual private networks (VPNs), network management systems, or other business systems that contain critical or sensitive information.
  - Require remote employees to use a separate, dedicated user account to perform any administrative tasks. (See Safeguards 8 and 9 for additional suggestions on improving security for administrative accounts.)

Resources and references you can use

- Cybersecurity & Infrastructure Security Agency (CISA) offers a succinct summary of Multifactor Authentication.

Cyber checkups

Actionable recommendations

"The results were a wake-up call about our vulnerabilities … "

"… we were able to understand real world ways to implement better security …"

"… immediately improved. The report … included actionable items that didn't require a lot of resources to implement."


Accounts & Passwords

Safeguard 10: Require remote workers to use MFA

About this safeguard

"Remote workers" refers to employees who may access your government's systems or applications remotely. This includes any staff who work from home or who may log in from a different worksite than your main office. This control considers whether you have a policy - and a process - in place for employees working off-site to use multifactor authentication (MFA) whenever they log in to their computers and other government-issued devices or access your software or network. (See Safeguard 9 for a detailed explanation of how MFA works.)

Why this safeguard is important

Working off-site - whether from home, at a client's office, or a remote workplace - adds risks to your IT systems because remote computer connections are more vulnerable to cybercrime than those connected directly to in-office systems. For example, remote employees logging into your network via unsecured, free Wi-Fi in a public space expose their devices - and your network - to criminals who are "network snooping" in hopes of picking up passwords or credit card information. Aside from that, research has shown that remote employees tend to fall for phishing schemes more often than employees working in the office, and they are less likely to inform their manager or IT. MFA adds an extra layer of authentication that hackers will not be able to acquire when trying to log into your government's computer systems.

What we observed during the checkup

Our recommendations

- Ensure your IT policies include requirements for remote users to use MFA when accessing your government's systems.
- Ask your IT support or service provider if MFA is available for your software and network systems, and what you need to do to enable it for employees who access your system or applications remotely. Make sure they complete the activation steps.
- If MFA isn't an option, evaluate the risks of continuing to use that product or service versus the costs of switching to new services with better security features for your remote users.
- If your government can't implement MFA right now, put the following safeguards in place:
  - Monitor user logs for unexpected or suspicious activity, such as someone logging in during non-working hours or from another country. Monitor vulnerable systems like email servers, your virtual private networks (VPNs), network management systems, or other business systems that contain critical or sensitive information.
  - Require remote employees to use a separate, dedicated user account to perform any administrative tasks. (See Safeguards 8 and 9 for additional suggestions on improving security for administrative accounts.)

Resources and references you can use

- Cybersecurity & Infrastructure Security Agency (CISA) offers a succinct summary of Multifactor Authentication.

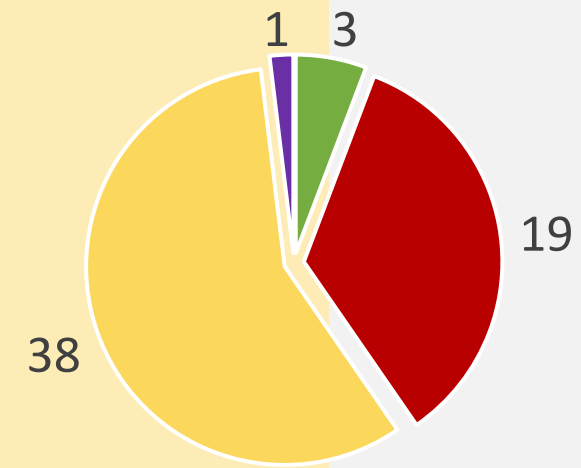
Cyber checkups

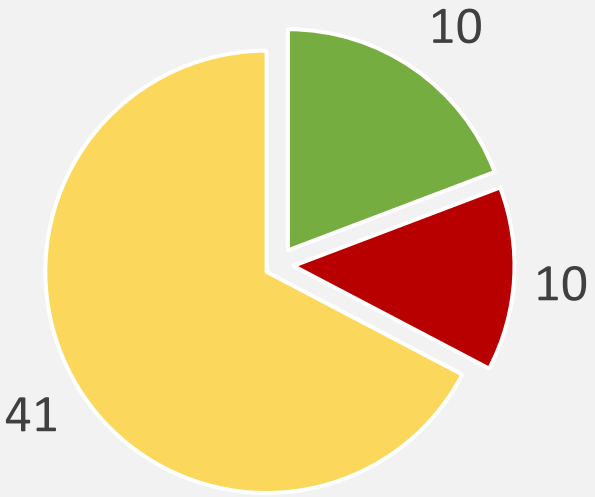
Results to date

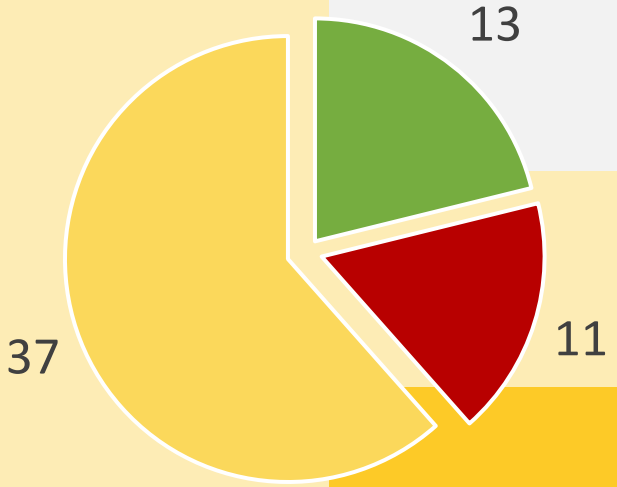
Weak or non-existent IT Policies

Weak or non-existent password requirements

Weak or non-existent plan for responding to incidents, including who to contact and when







#BeCyberSmart Program

The Center's Cybersecurity Program offers:

- Resources
- Training presentations
- Technical advice
- Cyber checkups

Center for Government Innovation

sao.wa.gov/becybersmart/

#BeCyberSmart Program

New resources

- IT Policies Guide
- Incident Response Plan Workshop

Subscribe to the SAO newsletter

Visit [sao.wa.gov](sao.wa.gov) OR scan:

Get the latest cyber information

Questions?

Center for Government
Innovation

Information

Niles Kostick, Center Manager

center@sao.wa.gov

(564) 999-0818

Website: sao.wa.gov

X (formerly Twitter): @WaStateAuditor

Facebook: facebook.com/WaStateAuditorsOffice

LinkedIn: linkedin.com/company/Washington-state-auditor-s-office