Cybersecurity Checklist

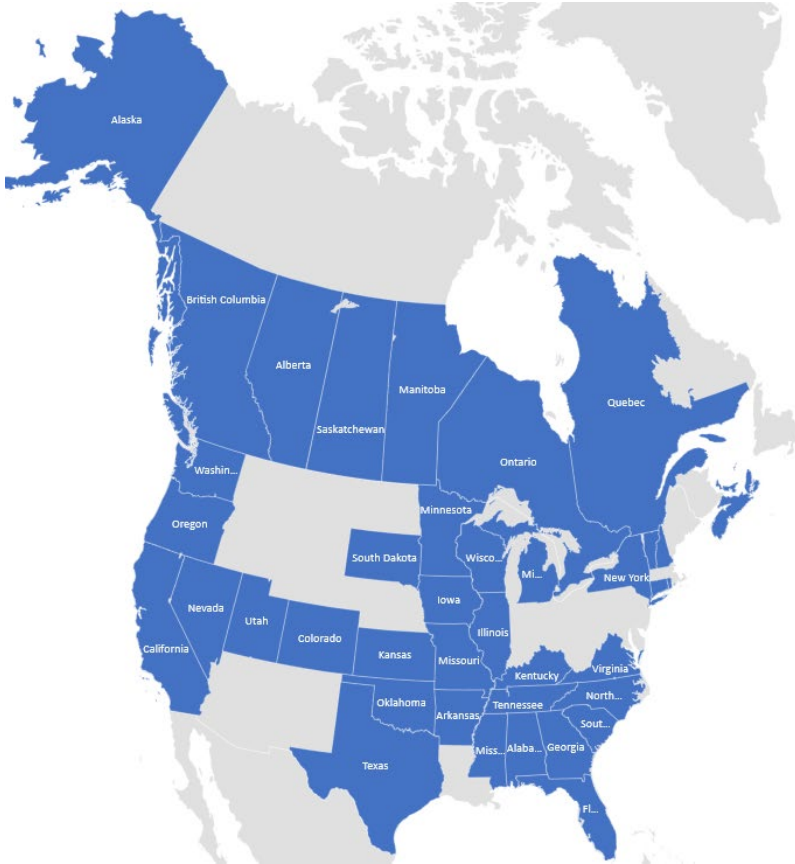
COREY KAUFMAN, GENERAL MANAGER

VC3 CALIFORNIA

Welcome!

Corey Kaufman
General Manager, US West

- Corey Kaufman, General Manager for VC3 & Registered Practitioner for the Cybersecurity Maturity Model Certification Accreditation Body
- Serving Municipalities, Special Districts, and small to medium sized businesses since 2001
- More than 75 employees in California and almost 600 nation wide
- Serving more than 1100 cities and towns and over 900 small to medium sized businesses across 32 states and 8 Provinces



Agenda

- What Does the Landscape Look Like Today
- Review of Revolving Threats & Targets
- The Checklist: Protect, Detect, & Recover
- What to Focus On First

Municipalities a Big Cyber Target

In 2020 **44%** of cyberattacks targeted **municipalities.**

More than **70%** of ransomware attacks target **state/local** government.

Nation states like to **target municipalities.**

90% of successful cyberattacks start **in email.**

More than **70%** of phishing attacks against government orgs go after **login credentials.**

Only **38%** of state/local government employees trained about ways to **prevent ransomware**.

97% of municipal officials use email to share sensitive documents.

The average time to identify a breach is over **200 days**

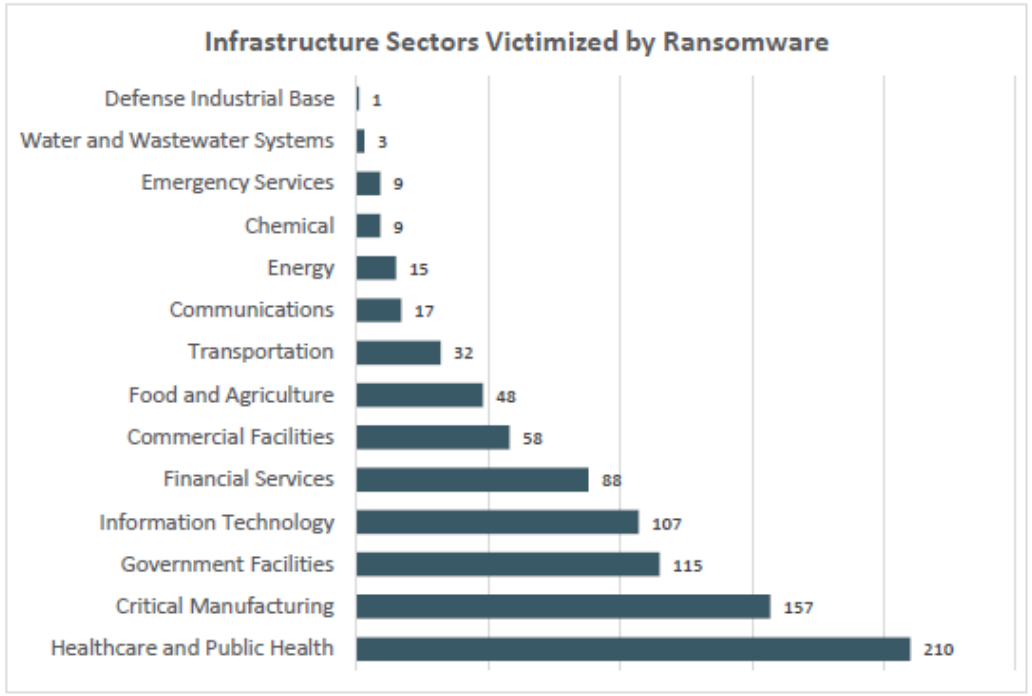
Big Cyber Target: The Headlines

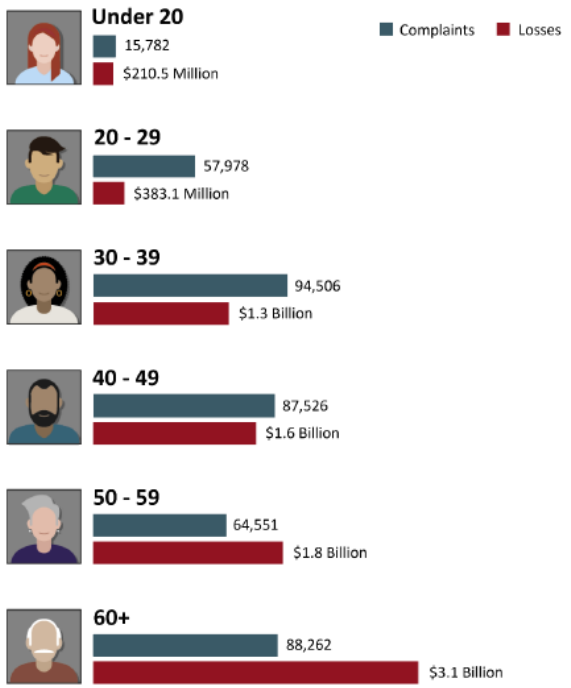
IT WONT HAPPEN TO ME RIGHT??

- **December 18th 2019: "**1000+ Schools Hit in October Alone By Active Ransomware Attack"
- **January 14th 2021: "**Fast Work By Cops Recovers $710,000 After CEO Fraud Attack Hits Long Island County Government"
- **August 15th 2022**: "Are Local Government and Municipalities Part of a Coordinated Attack on the US?"
- **September 24th 2022:** "Cyberattacks Targeting State and Local Government Increase by 50%"
- **January 3rd 2023:** " Cities and Governments are the Latest Target in a New "Leakware" Attack"
- **February 10th 2023:** "One Pricy Hospital Bill: Ransomware Attack Costs Hospital $1 Million"
- **February 15th 2023:** "US Cities Remain at Risk of Cyber Attacks"
- **March 23rd 2023:** Phishing Scam with Fraudulent Invoice Costs City of Fresno Over $600,000
- **May 9th 2023:** Dallas Police Department is latest Victim of a Ransomware Attack

Where Are we Today

According to the Department of Justice's 2022 Internet Crime Report:





$10.3 Billion
Victim losses in 2022

2,175+
Average complaints received daily

2021
2019
2018
2017
2016

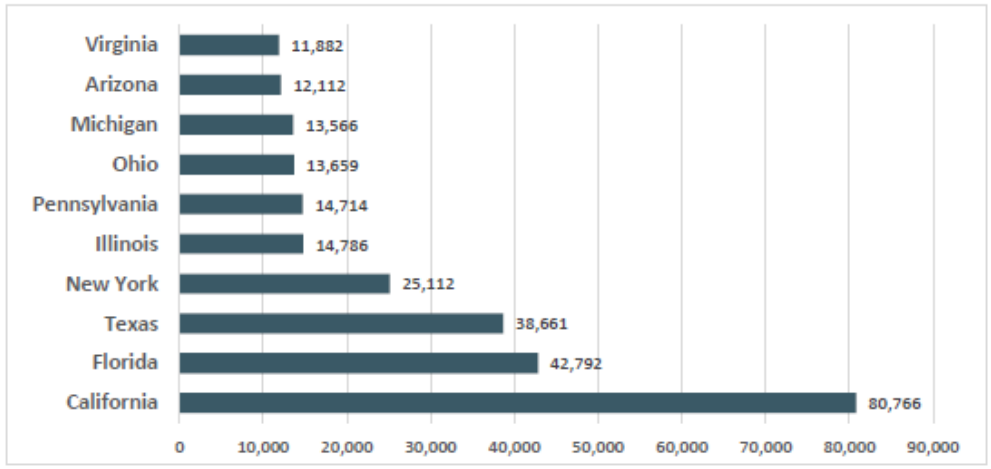
651,800+
Average complaints received per year (last 5 years)

Over 7.3 Million
Complaints reported since inception

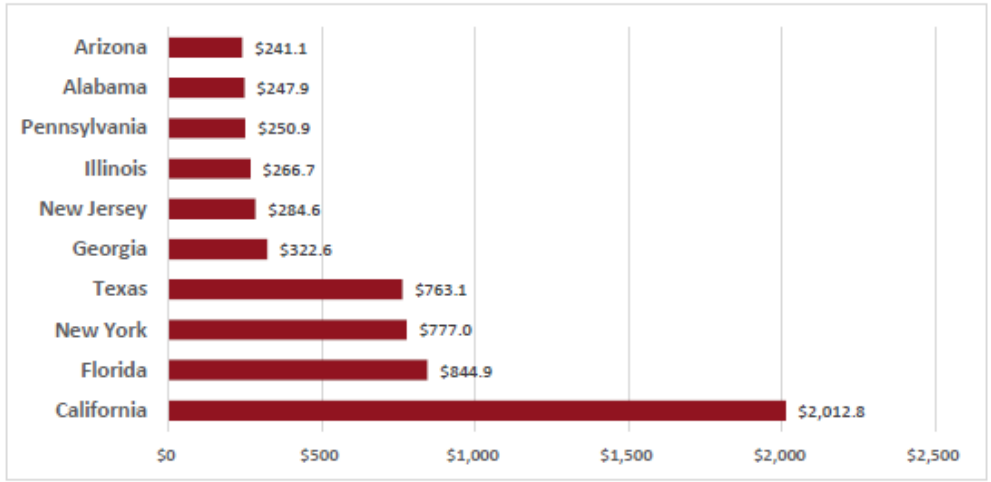
Where Are we Today

According to the Department of Justice's 2022 Internet Crime Report:

2022 - TOP 10 STATES BY NUMBER OF VICTIMS[19]



2022 - TOP 10 STATES BY VICTIM LOSS (IN MILLIONS)[20]



2022 CRIME TYPES

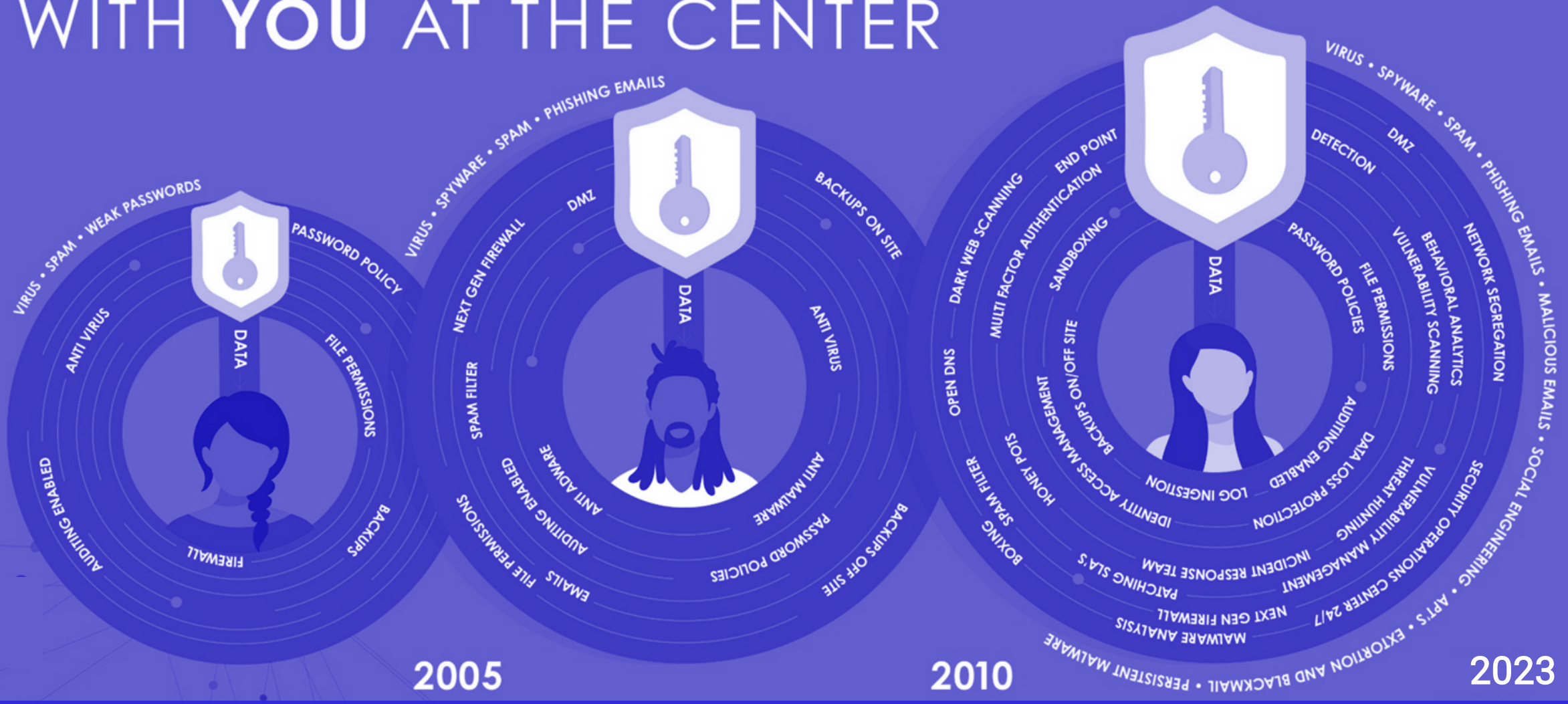
By Victim Count

Crime Type	*Victims*	*Crime Type*	*Victims*
Phishing	300,497	Government Impersonation	11,554
Personal Data Breach	58,859	Advanced Fee	11,264
Non-Payment/Non-Delivery	51,679	Other	9,966
Extortion	39,416	Overpayment	6,183
Tech Support	32,538	Lottery/Sweepstakes/Inheritance	5,650
Investment	30,529	Data Breach	2,795
Identity Theft	27,922	Crimes Against Children	2,587
Credit Card/Check Fraud	22,985	Ransomware	2,385
BEC	21,832	Threats of Violence	2,224
Spoofing	20,649	IPR/Copyright/Counterfeit	2,183
Confidence/Romance	19,021	SIM Swap	2,026
Employment	14,946	Malware	762
Harassment/Stalking	11,779	Botnet	568
Real Estate	11,727		

*Descriptors**			
Cryptocurrency	31,310	Cryptocurrency Wallet	20,781

*These descriptors relate to the medium or tool used to facilitate the crime and are used by the IC3 for tracking purposes only. They are available as descriptors only after another crime type has been selected. Please see Appendix B for more information regarding IC3 data.

LAYERED PROTECTION
WITH YOU AT THE CENTER



Evolving Threats

- **Access to user credentials continues to increase.** With so many ways to steal user credentials, the risk of a breach continues to increase.
- **Hackers continue to exploit software vulnerabilities and outdated operating systems** through zero-day vulnerabilities, support of sophisticated nation states, and going after soft targets.
- **Cyber threat detection has become a bigger issue**. Once inside your systems, hackers often remain undetected for many, many months.

Many smaller cities and agencies are…

At risk: Permanent data loss, downtime, operational disruptions, lack of compliance

Unprotected: Risk of ransomware, cyberattacks

On their own: Figuring it out themselves, getting by, shortcuts, reactive support

“Where do I begin with cybersecurity?”

It’s one of the most common questions we get from municipalities & special districts.

To answer this question, we’ve created a checklist that cities and special districts can use to find cybersecurity gaps and create an action plan.

IT Security Checklist:

Protect, Detect, & Respond

Being prepared for a cyber emergency means starting with the basics and practicing good cybersecurity hygiene.

Implementing these controls will help you cover all the bases when you are faced with a cyber emergency.

Protect

- Employee policies and training
- Multi-factor authentication
- Antivirus
- Antispam/email filtering
- Malware protection
- Data loss prevention
- Software patching
- Intrusion prevention
- Change control policies and procedures
- Mobile strategy
- Web content filtering

Protect: Employee policies and training

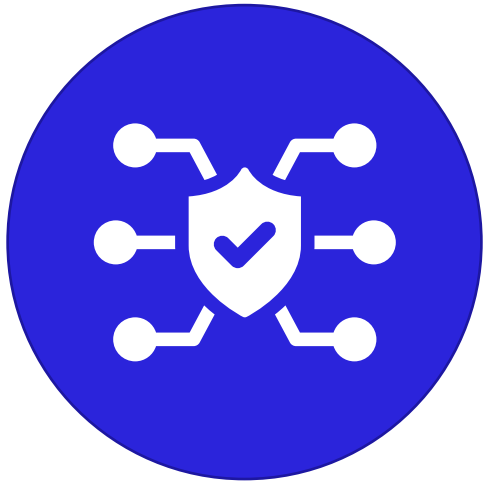
Periodic training helps teach employees how to detect and avoid common cyber threats in areas such as:

- Phishing and social engineering training
  - Create a culture of cyber awareness – See something say something
- Passwords
  - At Least 8 characters (Longer passwords vs frequent change)
  - Implement lock out attempts
  - Disable password hints
  - Avoid using the same passwords for multiple services
- Physical security
  - Don't forget about physical security – it is important

Protect: Multi-factor authentication

Multi-factor authentication is a method of verifying users' identities before granting them access to a system.

- MFA may require that you input a code sent to your phone as an extra layer of protection.
- Minimum requirement for cyber insurance coverage.
- Financial audits increasingly expecting MFA.



THIS IS THE NUMBER 1 THING YOU CAN DO TO PROTECT YOURSELF.. AND IT'S FREE!

MULTI-FACTOR AUTHENTICATION

Don’t Believe Me?

Per Microsoft:

99.9%

of account
compromise attacks
can be blocked by MFA

Per Arete:

94%

of ransomware
victims investigated
did not use MFA

Sources: https://www.microsoft.com/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/

Protect: Antivirus

Classic cybersecurity – still important to prevent basic viruses from infecting systems.

- Need an enterprise-grade rather than a consumer-grade version.
- Centrally managed.
- Do not let employees update antivirus software.

Protect: Antispam/email filtering

Basic antispam and email filtering tools prevent many potential phishing email messages from reaching employees' inboxes.

- This is not a set it and forget it solution
  - This is always a game of catch up (Bad guys make a change and the good guys figure out how to stop it
- There are much smarter solutions out there now
  - Advanced Threat Protection
  - Specific protections for users that are likely targets
    - General Managers, Finance teams, & Operations Leaders
  - Identity based protections
    - Based on user behavior, habits and locations
- **PRO TIP: DON'T ALLOW AUTO FORWARDING!**

Protect: Malware protection

Special tools can detect and filter out malware.

- Viruses (code) different than malware (software)
  - Ransomware
  - Scareware
  - Adware
  - Spyware
- Anti-malware uses different approaches to detect malware (which evolves rapidly)
- Many antivirus tools also include malware protection, but you need to make sure

Protect: Data loss prevention

Monitor for unauthorized or suspicious access to data.

- Unauthorized people can steal, delete, corrupt sensitive data.
- How would you know?
  - Think about all the different ways data can leave your organization
  - How would you know if some one accessed critical data they shouldn't have?
    - Would you know what they did with it?
- You may need this tool for compliance.

Protect: Software patching

Government particularly lags on replacing outdated software and patching current software. It's not unusual to see cities using software that is 10 (or more) years old and hasn't been supported by the software vendor for a long time.

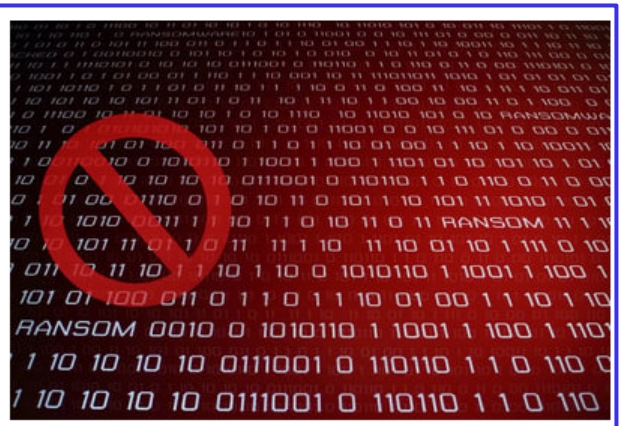
Hackers continue to exploit software vulnerabilities and outdated operating systems through:

- Zero day vulnerabilities
- Support of sophisticated nation states
- Going after soft targets (like municipalities!)

Protect: Software patching

Government particularly lags on replacing outdated software and patching current software. It's not unusual to see cities using software that is 10 (or more) years old and hasn't been supported by the software vendor for a long time.

Despite a lot of focus on phishing and remote access as initial access vectors, new data shows the use of vulnerabilities is not only on the rise, but simply isn't being properly addressed.



The report, Ransomware 2023, put out jointly by cybersecurity vendors Securin, CybersecurityWorks, Ivanti, and Cyware, highlights the use of vulnerabilities within ransomware attacks. According to the report, vulnerabilities are alive and well in modern attacks:

- 81 vulnerabilities exist that provide attackers with end-to-end access – from initial access to exfiltration – have been identified within popular operating systems, databases, storage, virtualization and firewall solutions.
- 76% of vulnerabilities exploited by ransomware are old – *really old*. Many of them were discovered between 2010 and 2019!
- The number of vulnerabilities associated with ransomware attacks has grown 19% with a total count of 344 since 2019

At present, according to the report, there are a total of 11,778 weaponized vulnerabilities documented; this reaches far beyond just ransomware and represents all known vulnerabilities including those that have been addressed with updates.

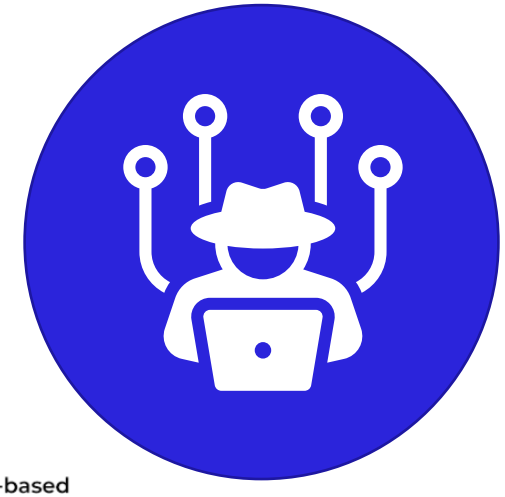
Source: KnowBe4 Blog March 8th, 2023
Blog.knowbe4.com/most-ransomware-vulnerabilities-discovered-before-2020

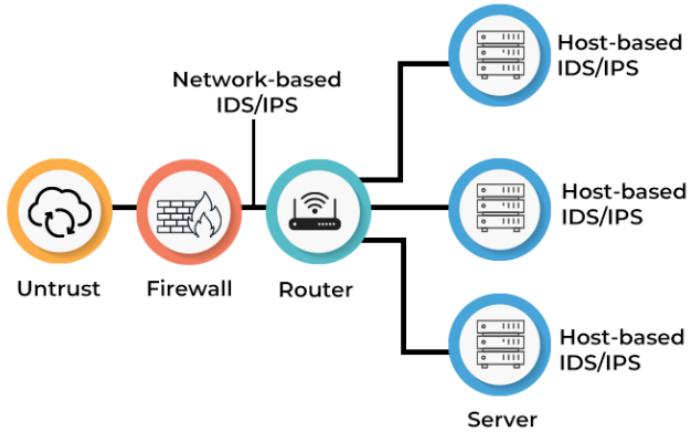
- **PRO TIP: SOMEONE WILL TELL ME WHEN IM IN DANGER RIGHT? Well…**

Protect: Intrusion prevention

Tools which work with your firewall to detect and often automatically prevent attacks related to specific vulnerabilities.

- Options to send an alert, block, or drop traffic depending on severity
- Often automated
- Can prevent known and unknown (based on behavior) vulnerabilities





Protect: Change control policies and procedures

Includes logging and understanding the repercussions of all changes made to your security equipment and applications.

- Who has access to your equipment and applications?
- What changes can they make?
- Are there processes in place to ensure that only authorized personnel can make critical changes?
  - Only give the access that is necessary for the job function
  - Many times a breach could have been prevented simply by limiting access
    - You can't impact what you don't have access to
- **PRO TIP: THIS APPLIES TO INTERNAL FINANICAL CONTROLS AS WELL!**

Protect: Mobile strategy

Are you securing mobile devices as well as your network?

May involve:

- Issuing work-only devices to employees
- Providing secure access to sensitive and confidential data if they use a personal device

Protect: Web content filtering

Special tools can place restrictions on what internet content employees can access.

When employees browse the internet, it's easy to make a mistake and access a malicious website. Examples include:

- Typing in the wrong URL to a well-known website
- Clicking on a malicious search engine result that looks correct
- Accessing websites that employees really shouldn't access during work hours

Protect (Here is the PROTECT Checklist)

- Employee policies and training
- Multi-factor authentication
- Antivirus
- Antispam/email filtering
- Malware protection
- Data loss prevention
- Software patching
- Intrusion prevention
- Change control policies and procedures
- Mobile strategy
- Web content filtering

Shifting Mindset From Prevention to Detection

As we discussed MFA will prevent more than 90% of cyber emergencies

It isn't realistic to think MFA or any other tools can stop all cyber emergencies

80,000 fall for a scam every day and share personal information (including usernames, credit card numbers, passwords) resulting in stolen identities, financial loss, credit card frauds and other Internet scams (10% of links clicked)

We must shift our mindset from we can prevent a cyber emergency to we need to be able to detect a cyber emergency and respond as quickly as possible

Detect: Why is Detection Important?

You May Not Know Your At Risk	Without the proper detection tools or teams in place you may be at risk without even knowing it – There could be someone in your network today without your knowledge
Quick Response is Key	The average time an attacker has to “dwell” in an environment before detection is somewhere between 11 and 24 days
What is Next is Key	Understanding how to respond once you have detected the emergency can be the difference between an inconvenience or significant impact (A cyber emergency can quickly go from emergency to catastrophe)

Detect

- Security scanning
- Dark web monitoring
- Intrusion detection
- Managed detection and response (MDR)
- Endpoint detection and response (EDR)
- Security information and event management (SIEM)

Detect: Security scanning

Regular security scans of your systems help identify vulnerabilities and holes that you can then fix.

- Regular Internal scans are important – simply having access to your network isn't enough, malicious actors look for ways to exploit systems
- Legacy applications may be using old protocols to communicate
- External scans are critical to making sure your doors are locked
  - Your external IP address tells everyone where you are on the web – work on making yourself invisible
  - Did you lock the car?

Detect: Security scanning

Did you lock the car?

Detect: Dark web monitoring

IT professionals can monitor the Dark Web in case account credentials (such as administrative passwords) appear on the black market.

- Awareness that compromised data exists on the dark web allows you to proactively change compromised passwords and disable unused accounts.
- A training opportunity for employees - encourage your employees to use unique passwords for different services.
- A compromised password goes onto the “forever banned” list
- **PRO TIP: YOUR PERSONAL PASSWORDS SHOULD FOLLOW THIS SAME PROTCOL – BE CAREFUL WITH SAVING PASSWORDS AND CREDIT CARDS IN BROWSERS**

Detect: Intrusion detection

Watches for suspicious network traffic and alerts you when it detects anomalous activity.

- Otherwise, you may not know a breach occurred.
- Allows you to detect the intrusion and act.
- Should be part of your security monitoring tools.
  - Someone has to be responsible for monitoring this

Detect: Managed detection and response (MDR)

MDR is a strategy where a security team will proactively look for cyberthreats across your servers, computers, and entire IT network—specifically looking for threats that may have already gotten inside your systems by watching for behavior and activity that looks suspicious.

Once you identify a possible threat, you can take action against the threat. When you hear about MDR, it's usually describing the 24/7 work of a security team actively monitoring IT systems for threats.

Detect: Endpoint detection and response (EDR)

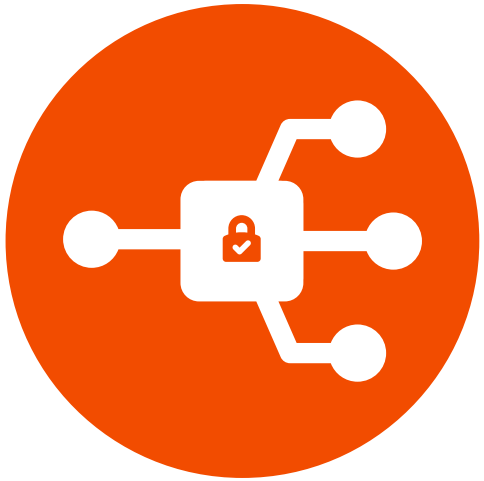
EDR is an MDR tool focused on a single "endpoint device"—a fancy name for a specific server or computer.

- For example, if a threat is found on your computer, an EDR tool can cut your computer off from your organization's network—preventing further spread of a dangerous virus.
- An EDR tool can be deployed, run in an automated fashion, and enhance the level of security protection for an organization at a low cost.
- **EDR is the new antivirus—essential and usually required if you want cyber insurance.**

Detect: Security information and event management (SIEM)

Identifies the most important and critical security alerts received from different systems.

- Collects log files from different sources (servers, firewalls, VPN, email, cloud services, EDR, etc.)
- Identifies anomalies – such as a user logging in from another country
- Meets CJIS requirements for weekly log reviews



Detect: Here is your Detect Checklist

- Security scanning
- Dark web monitoring
- Intrusion detection
- Managed detection and response (MDR)
- Endpoint detection and response (EDR)
- Security information and event management (SIEM)

RESPOND (AND RECOVER)

- Data backup and disaster recovery
- Offsite log retention
- Incident response planning
- Cyber liability insurance

Respond/Recover: Data backup and disaster recovery

A cybersecurity essential…

- Onsite & Offsite Backups
- Backups need to be segregated from production
  - Do I have an immutable backup?
- Periodic testing
- Monitoring
- Basic requirement for cyber insurance
- Affects ability to recover after a cyberattack

- **PRO TIP: What about my employees working at home? Is the company data they are working on backed up?**

Respond/Recover: Offsite log retention

Used for evidence related to cyber incidents.

Without this data, you will be unable to analyze the full nature of a cyberattack, deduce the source of the attack, and remediate effectively.

- Can we see how our data has been impacted?
- Has our critical data been exfiltrated?

Respond/Recover: Incident response planning

Developing a plan detailing how you respond to a cyberattack will help you react to an incident with "muscle memory"— like a fire drill.

Covers:

- How you will respond to a cyber incident
- Who will respond
- Planning and testing the plan long before an incident happens

MAKE TIME TO PLAN

Planning is critical to the success or failure of a cyber emergency

- Work with your IT team to identify critical systems, data, & process
- Not all data and systems have the same value to your organization – understand the priority
- *Your incident response plan MUST be written down*
- Ask your team to identify who will do what and how long it might take in an emergency scenario
- The “who” might not always be in your organization – you may need to reach out to your cyber insurance or authorities to start the process

How will I ensure my team is ready? Did we think of everything?

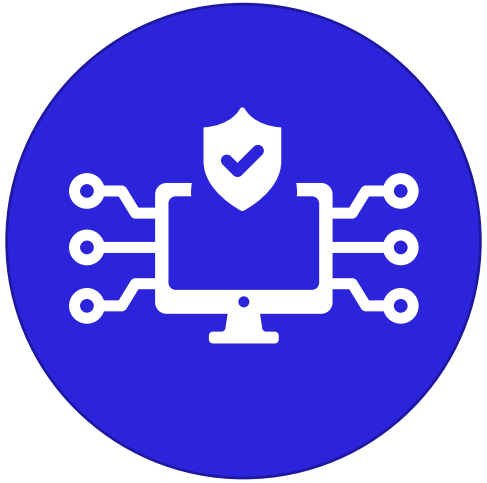
Is my team ready?

Only way to know is to test your plan:

- Do tabletop exercises with your team – you come up with the scenario and have your team run through it
- Document your results so you can update the plan as needed
- Don't just talk through it – do it! Test monitoring and restore capabilities. Ask for evidence so you can verify the effectiveness and timing
- Review the results with the team – Let them know that any failures represent an opportunity to improve and reduce stress in the case of a live emergency

Respond/Recover: Cyber liability insurance

Improving your security foundation will help you lower cyber liability insurance premiums.



RESPOND (AND RECOVER)

- Data backup and disaster recovery
- Offsite log retention
- Incident response planning
- Cyber liability insurance

Cyber Security Checklist

Corey Kaufman
General Manager

Protect

- ❑ Employee Training
- ❑ Multifactor Authentication
- ❑ Antivirus
- ❑ Email Filtering
- ❑ Malware Protection
- ❑ Data loss Prevention
- ❑ Security Patching
- ❑ Intrusion Prevention
- ❑ Change Control
- ❑ Mobile Strategy
- ❑ Web Filtering

Detect

- ❑ Security Scanning
- ❑ Dark Web Monitoring
- ❑ Intrusion Detection
- ❑ Managed Detection & Response
- ❑ Endpoint Detection & Response
- ❑ SIEM Logging

Respond

- ❑ Backup & Disaster Recovery
- ❑ Offsite Log Retention
- ❑ Incident Response Planning
- ❑ Cyber Insurance

The Must Haves

Corey Kaufman
General Manager

Protect

- ☒ Employee Training
- ☒ Multifactor Authentication
- ☒ Antivirus
- ☒ Email Filtering
- ☒ Malware Protection
- ❑ Data loss Prevention
- ☒ Security Patching
- ❑ Intrusion Prevention
- ☒ Change Control
- ❑ Mobile Strategy
- ☒ Web Filtering

Detect

- ❑ Security Scanning
- ☒ Dark Web Monitoring
- ❑ Intrusion Detection
- ☒ Managed Detection & Response
- ☒ Endpoint Detection & Response
- ❑ SIEM Logging

Respond

- ☒ Backup & Disaster Recovery
- ❑ Offsite Log Retention
- ❑ Incident Response Planning
- ☒ Cyber Insurance

The Tools That Will Save You

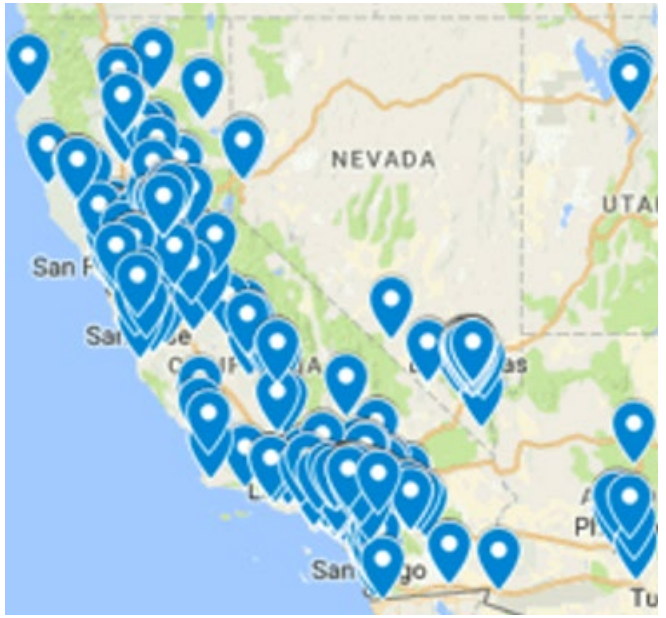
Corey Kaufman
General Manager

Protect	Detect	Respond
☒ Employee Training	☐ Security Scanning	☒ **Backup & Disaster Recovery**
☒ **Multifactor Authentication**	☒ Dark Web Monitoring	☐ Offsite Log Retention
☒ Antivirus	☐ Intrusion Detection	☐ Incident Response Planning
☒ Email Filtering	☒ **Managed Detection & Response**	☒ Cyber Insurance
☒ Malware Protection	☒ **Endpoint Detection & Response**	
☐ Data loss Prevention	☐ SIEM Logging	
☒ **Security Patching**		
☐ Intrusion Prevention		
☒ Change Control		
☐ Mobile Strategy		
☒ Web Filtering		

Some Closing Thoughts

Corey Kaufman
General Manager

- Implementing all of the controls on the cyber checklist wont make you make you bulletproof to a cyber emergency by it will put you in a great spot to avoid a cyber catastrophe
- Start by implementing MFA and endpoint threat detection tools on your systems as soon as possible
- Shift your mindset from we can prevent an emergency to we need to be able to detect an emergency and respond
- Make the time to plan – Write that plan down (A lot of times this is the hardest part)
- Don't put everything on the IT team – this is an organization/agency wide endeavor
- Test the plan once it is in place
- Lastly, we all have similar challenges – Ask your peers about their plans and experiences



Thank You!

Corey Kaufman
VC3

corey.kaufman@vc3.com
800-787-1160

Visit us on the web at
VC3.com