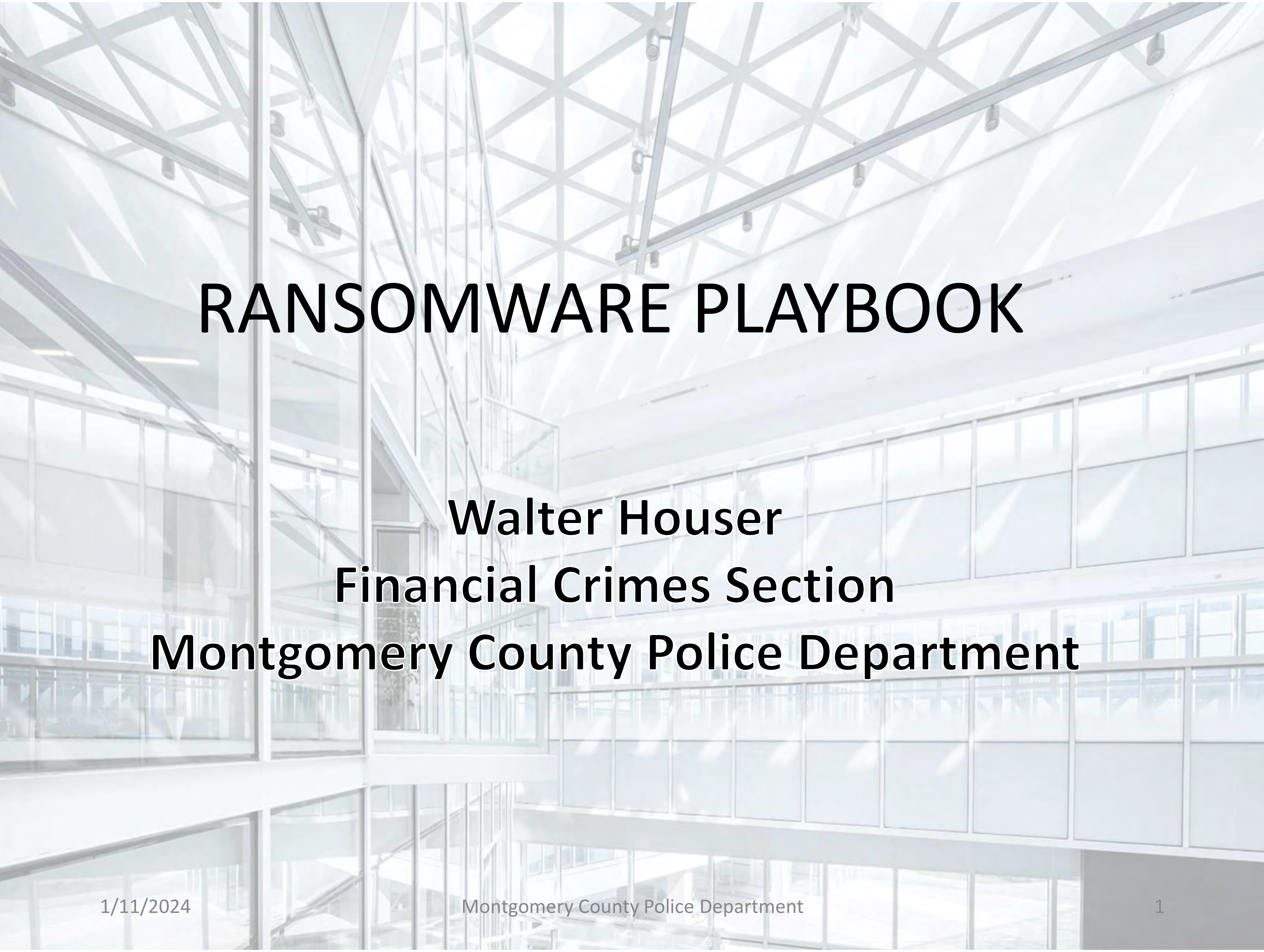


RANSOMWARE PLAYBOOK

Walter Houser
Financial Crimes Section
Montgomery County Police Department

YOUR PERSONAL FILES ARE ENCRYPTED
Make payment or private key will be destroyed in
12 Hours 01:34
YOUR PERSONAL FILES ARE ENCRYPTED
Make payment o
will be de
12 Hou

RANSOMWARE PLAYBOOK

This presentation covers ransomware, threat actor motivations and gains, and measures to prevent these attacks and protect your organization.

The information presented will inform you and your organization of the risks, impacts, and preventative actions associated with ransomware incidents.

This presentation is broken down into the following two sections:

- Prevention
- Response

YOUR PERSONAL FILES ARE ENCRYPTED
Make payment or private key will be destroyed in
12 Hours 01:34
YOUR PERSONAL FILES ARE ENCRYPTED
Make payment o
will be de
12 Hou

RANSOMWARE PLAYBOOK: Prevention

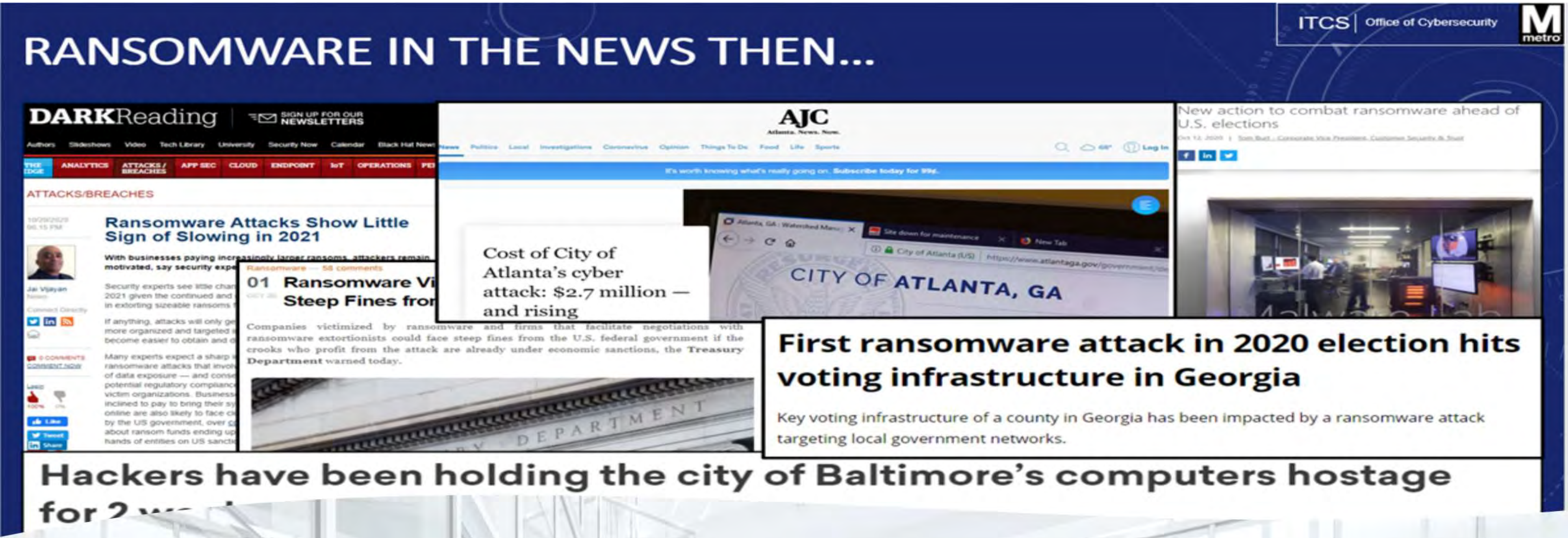
In the first section, we define ransomware, outline the common vectors used to infect networks and devices, list the preventative measures to protect your organization, and offer checklists for specific mitigation measures.

Applying these measures enhances your cyber hygiene and protection against cyber incidents and threat actors, including ransomware.

RANSOMWARE PLAYBOOK: Response

The second section includes guidance on immediate actions when the ransomware is discovered, recovery measures that will get you back to business, and methods to evaluate the incident and enhance security measures.

Following the action items in this section can enhance your ability to respond to an incident and decrease the risk of your organization becoming a repeat ransomware victim.



RANSOMWARE IN THE NEWS THEN...

ITCS | Office of Cybersecurity

DARKReading

ATTACKS/BREACHES

Ransomware Attacks Show Little Sign of Slowing in 2021

With businesses paying increasingly larger ransoms, attackers remain motivated, say security expe

Jai Vijayan

Security experts see little chan 2021 given the continued and in extorting sizeable ransoms

If anything, attacks will only ge more organized and targeted become easier to obtain and d

Many experts expect a sharp ransomware attacks that invol of data exposure — and conse potential regulatory complianc victim organizations. Business inclined to pay to bring their sy online are also likely to face c by the US government, over about ransom funds ending up hands of entities on US sancti

Ransomware — 58 comments

01 **Ransomware Vi Steep Fines fro**

Companies victimized by ransomware and firms that facilitate negotiations with ransomware extortionists could face steep fines from the U.S. federal government if the crooks who profit from the attack are already under economic sanctions, the **Treasury Department** warned today.

AJC

Atlanta. News. Now.

It's worth knowing what's really going on. Subscribe today for 99¢.

Cost of City of Atlanta's cyber attack: $2.7 million — and rising

CITY OF ATLANTA, GA

New action to combat ransomware ahead of U.S. elections

First ransomware attack in 2020 election hits voting infrastructure in Georgia

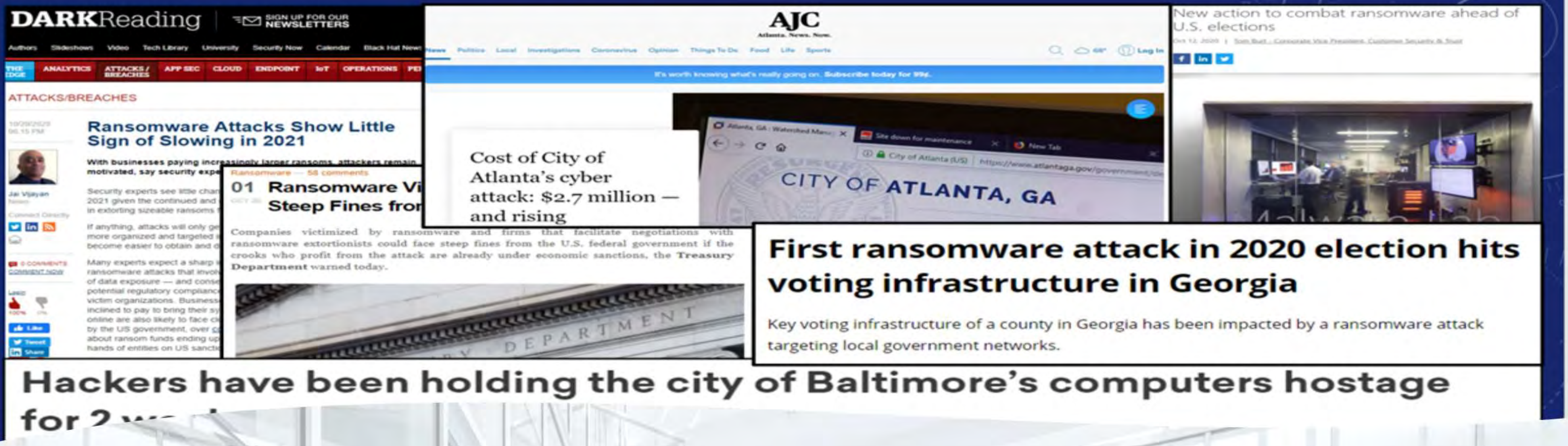
Key voting infrastructure of a county in Georgia has been impacted by a ransomware attack targeting local government networks.

Hackers have been holding the city of Baltimore's computers hostage for 2 w

WHAT IS RANSOMWARE?

- Ransomware is malware that denies users access to files or systems until a sum of money is paid.
- Ransomware incidents can devastate your organization by disrupting your business's processes and critical functions reliant on network and system connectivity.

RANSOMWARE IN THE NEWS THEN...



DARKReading

ATTACKS/BREACHES

Ransomware Attacks Show Little Sign of Slowing in 2021

With businesses paying increasingly larger ransoms, attackers remain motivated, say security expe

Security experts see little chan 2021 given the continued and in extorting sizeable ransoms

If anything, attacks will only ge more organized and targeted become easier to obtain and d

Many experts expect a sharp ransomware attacks that invol of data exposure — and conse potential regulatory complianc victim organizations. Business inclined to pay to bring their sy online are also likely to face c by the US government, over about ransom funds ending up hands of entities on US sanctio

Ransomware — 58 comments

01 Ransomware Vi Steep Fines fro

Companies victimized by ransomware and firms that facilitate negotiations with ransomware extortionists could face steep fines from the U.S. federal government if the crooks who profit from the attack are already under economic sanctions, the Treasury Department warned today.

AJC

Cost of City of Atlanta's cyber attack: $2.7 million — and rising

New action to combat ransomware ahead of U.S. elections

First ransomware attack in 2020 election hits voting infrastructure in Georgia

Key voting infrastructure of a county in Georgia has been impacted by a ransomware attack targeting local government networks.

Hackers have been holding the city of Baltimore's computers hostage for 2 w

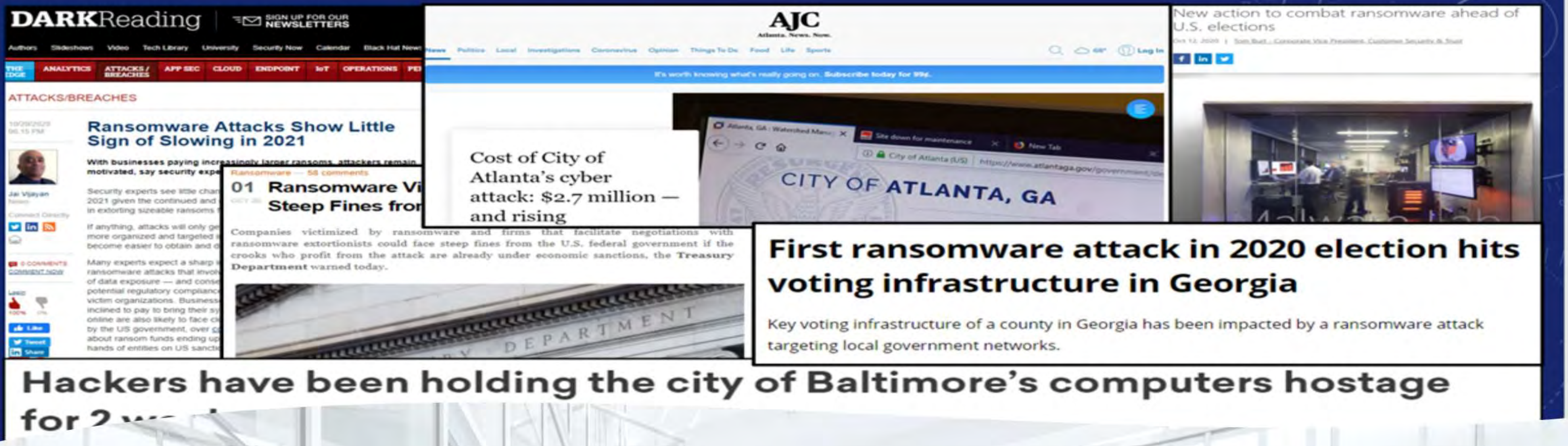
HOW DOES RANSOMWARE WORK?

When ransomware infects a device, it either locks the screen or encrypts the files, preventing access to the information and systems on your devices.

Threat actors can also use your compromised network to spread the ransomware to other connected systems and devices.

ITCS | Office of Cybersecurity

RANSOMWARE IN THE NEWS THEN…



DARKReading SIGN UP FOR OUR NEWSLETTERS

Authors Slideshows Video Tech Library University Security Now Calendar Black Hat News

THE EDGE ANALYTICS ATTACKS / BREACHES APP SEC CLOUD ENDPOINT IoT OPERATIONS

ATTACKS/BREACHES

10/29/2020 05:15 PM

Jai Vijayan

Ransomware Attacks Show Little Sign of Slowing in 2021

With businesses paying increasingly larger ransoms, attackers remain motivated, say security expe

Security experts see little chan 2021 given the continued and in extorting sizeable ransoms

If anything, attacks will only ge more organized and targeted become easier to obtain and d

Many experts expect a sharp ransomware attacks that involv of data exposure — and conse potential regulatory complianc victim organizations. Business inclined to pay to bring their sy online are also likely to face c by the US government, over about ransom funds ending up hands of entities on US sancti

Ransomware — 58 comments

01 **Ransomware Vi Steep Fines fron**

Companies victimized by ransomware and firms that facilitate negotiations with ransomware extortionists could face steep fines from the U.S. federal government if the crooks who profit from the attack are already under economic sanctions, the **Treasury Department** warned today.

AJC

Cost of City of Atlanta's cyber attack: $2.7 million — and rising

CITY OF ATLANTA, GA

New action to combat ransomware ahead of U.S. elections

Oct 12, 2020 | Tom Burt - Corporate Vice President, Customer Security & Trust

First ransomware attack in 2020 election hits voting infrastructure in Georgia

Key voting infrastructure of a county in Georgia has been impacted by a ransomware attack targeting local government networks.

Hackers have been holding the city of Baltimore's computers hostage for 2 w

WHAT CAN GO WRONG WITH RANSOMWARE?

- Lost of revenue resulting from downtime
- Collateral disruption of service and the resulting loss of customers
- Lost reputation
- Loss of sensitive data: financial, sales, patent, code, and research.
- Damage to customers and suppliers as ransomware spreads up and downstream.
- Lawsuits by customers and suppliers for information disclosure, damage to assets
- Decryption keys from the attacker don't work, so information is lost
- Fines and sanctions by regulators for failing to comply with rules

HOW DOES RANSOMWARE WORK?

- Human weaknesses, including phishing and social engineering, are crucial in compromising systems.
- Around 82% of all breaches in business environments are attributed to human error.

YOUR FILES ARE ENCRYPTED

Your photos, documents and other important files have been encrypted with unique key, generated for this computer.

HOW DOES RANSOMWARE WORK?

What are the ways our networks and devices can be infected with ransomware:

- Opening emails or files from familiar or unfamiliar sources (phishing);
- Clicking on links in emails, social media, and peer-to-peer networks;
- Visiting unsafe, suspicious, or compromised websites (known as a drive-by download);
- Inserting an infected peripheral device (e.g. USB flash drive) into a device;
- Exposing your systems to the internet unnecessarily;
- Failure to patch vulnerabilities; or
- Lack of multi-factor authentication (MFA).

YOUR FILES ARE ENCRYPTED

Your photos, documents and other important files have been encrypted with unique key, generated for this computer.

RANSOMWARE VECTORS

Phishing is an attack that uses text, email, or social media to trick users into clicking malicious links or attachments.

- Phishing attempts are often generic mass messages, but the message appears legitimate and from a trusted source (e.g., a bank).
- Malicious code will execute commands using your account privileges.
- Threat actors may also use this opportunity to install a backdoor to your devices.

RANSOMWARE VECTORS

Drive-by download occurs when a user unknowingly visits an infected website where malware is downloaded and installed without the user's knowledge.

RANSOMWARE VECTORS

- ***Malvertising*** injects malicious code into legitimate online advertisements.
- When a user clicks the ad, malware spreads to their device.

RANSOMWARE VECTORS

Exposed services*,* such as Remote Desktop Protocol (RDP)and content management systems, allow access to your devices.

Threat actors can use a variety of tactics, such as exploiting common vulnerabilities and password spraying, to access your devices via these exposed systems and deploy ransomware.

RANSOMWARE AIDS

While the following items are not traditional vectors, they are options for threat actors to initiate a ransomware attack.

- ***Third parties and managed service providers (MSP)*** can be used by threat actors to spoof emails or conduct phishing attacks against your organization.
- ***Supply chain attacks*** allow threat actors to infiltrate a service supply organization and force an update to connected customers, infecting their systems and devices with ransomware.
- ***Ransomware as a Service (RaaS)*** is a model in which threat actors, regardless of their skills, can purchase malware from developers on the dark web. The developers receive a portion of the ransom paid by the victim.

RANSOMWARE VECTORS

How are attacks are getting more sophisticated?

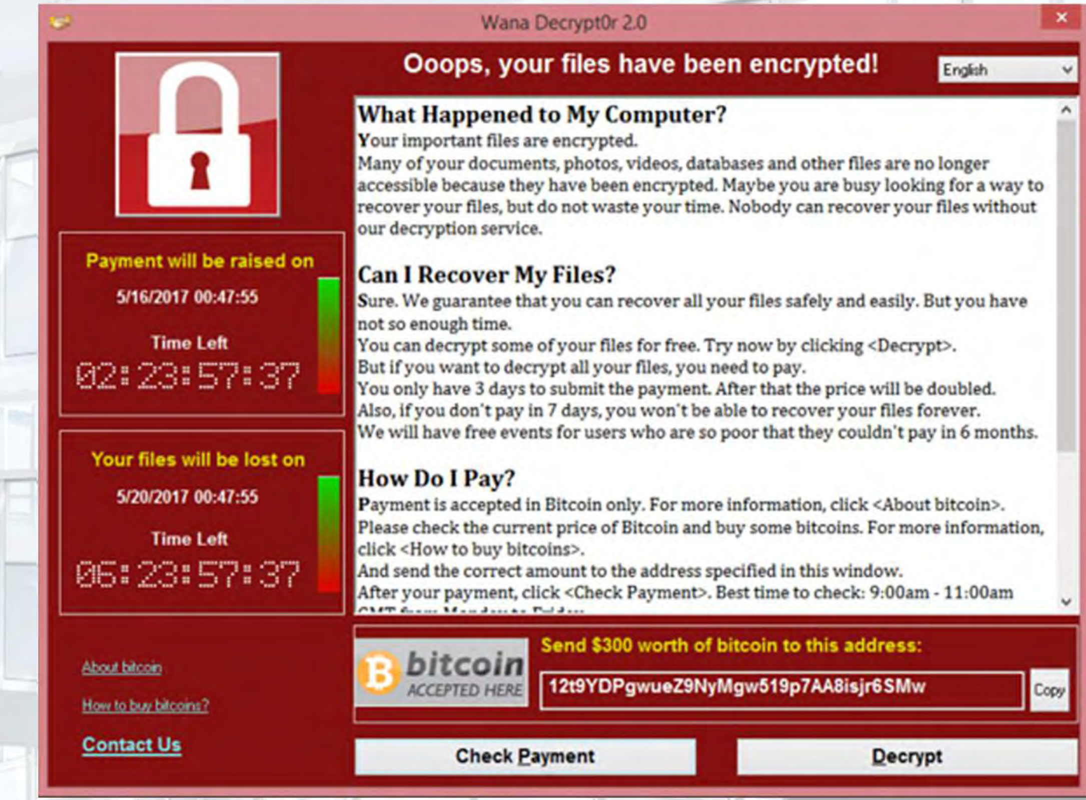
Time-delayed Attacks - an evasion tactic where an email that is inbounded as 'safe' can be weaponized later post-delivery through time-delayed malicious links and attachments

BEC-driven Attacks - when attackers use previously obtained credentials to launch attacks from compromised emails inside the organization, making them even more difficult to detect since end users trust messages from internal parties

Polymorphic Attacks - an advanced form of phishing that randomizes components of an email, such as copy, subject line, or sender name, tricking signature-based email security.

WHAT DOES A RANSOMWARE ATTACK LOOK LIKE

- If your device is infected with ransomware, you will receive a notice on your screen indicating your files are encrypted and inaccessible until the ransom is paid.
- You may also receive a message on your lock screen indicating your device is locked and inaccessible until the ransom is paid. The message will instruct you to pay a ransom to unlock the device and retrieve the files.



Ooops, your files have been encrypted!

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

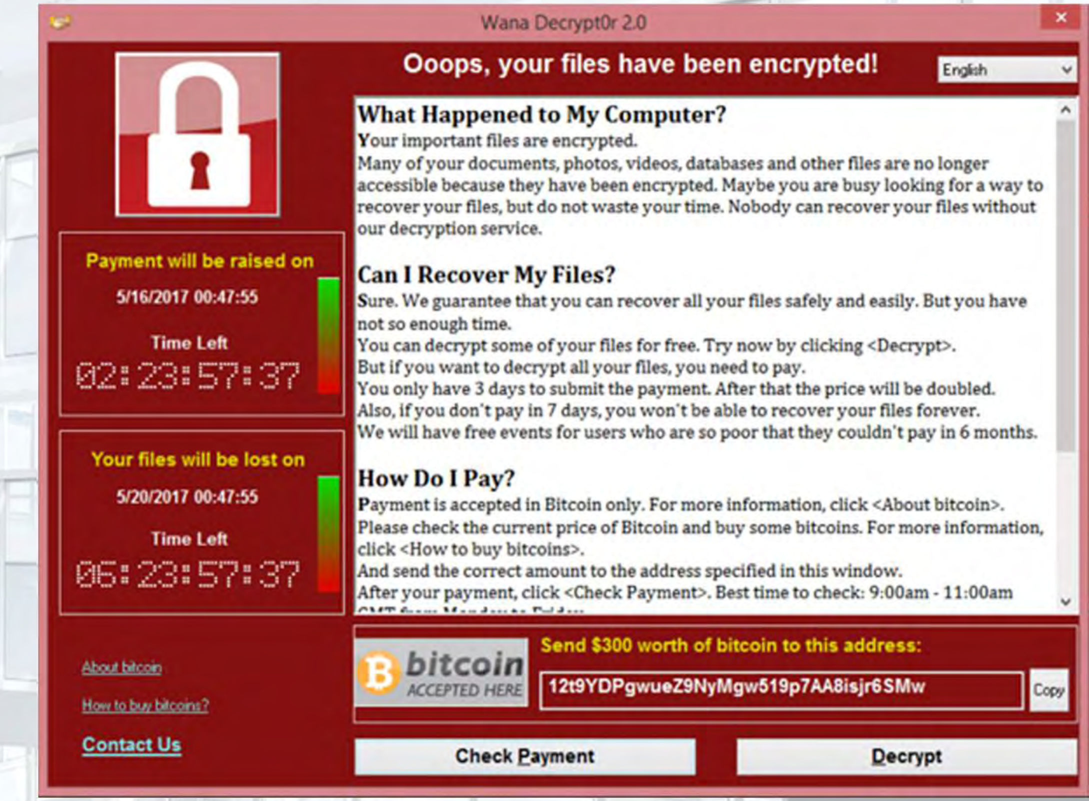
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

WHAT DOES A RANSOMWARE ATTACK LOOK LIKE

Payment is often requested in digital currency, such as Bitcoin, because the transfer would be more difficult to trace. Prepaid credit cards or gift cards may also be requested.

You will be given a time limit to pay the ransom, after which threat actors may increase the ransom amount, destroy your files permanently, or leak your data.



Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

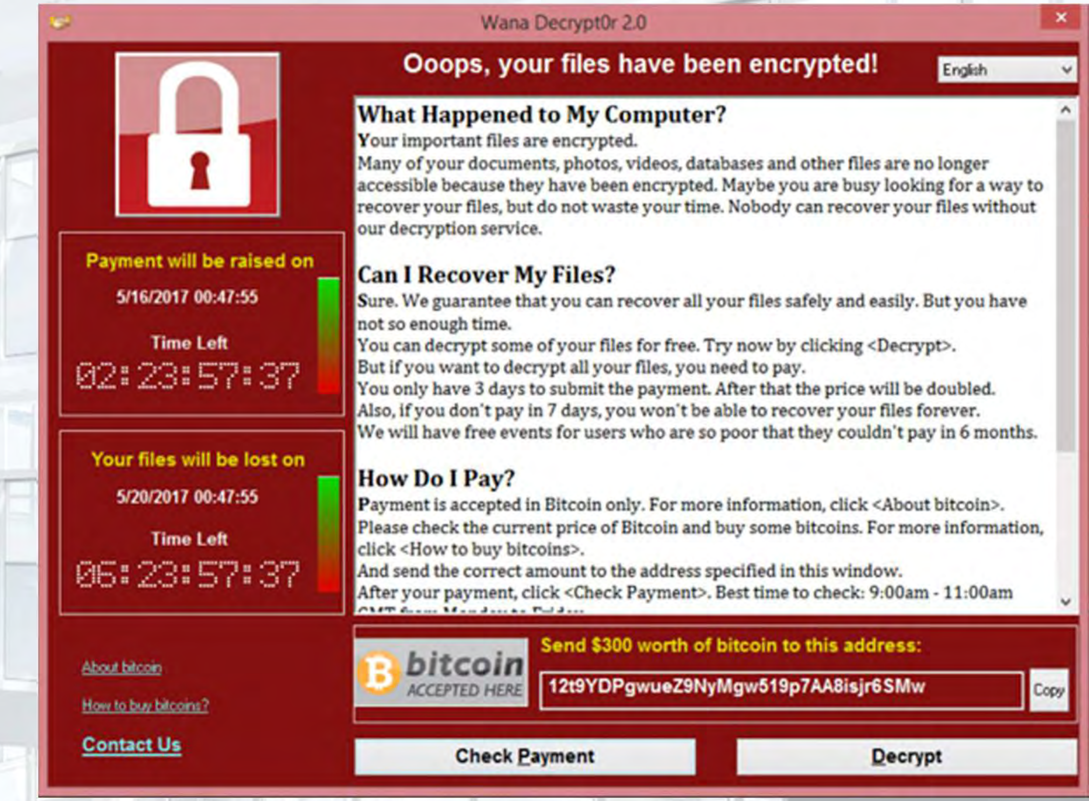
Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

WHAT DOES A RANSOMWARE ATTACK LOOK LIKE

Recent changes in tactics:

- A threat actor may threaten to release your data publicly if you do not pay the ransom.
- Distributed denial of service attacks put additional pressure on the victim.
- Encrypting data is time-consuming and error-prone so some attackers only exfiltrate and extort data disclosure.
- An attacker filed a complaint with the SEC that their victim failed to file a timely SEC-8.



Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

Send $300 worth of bitcoin to this address:

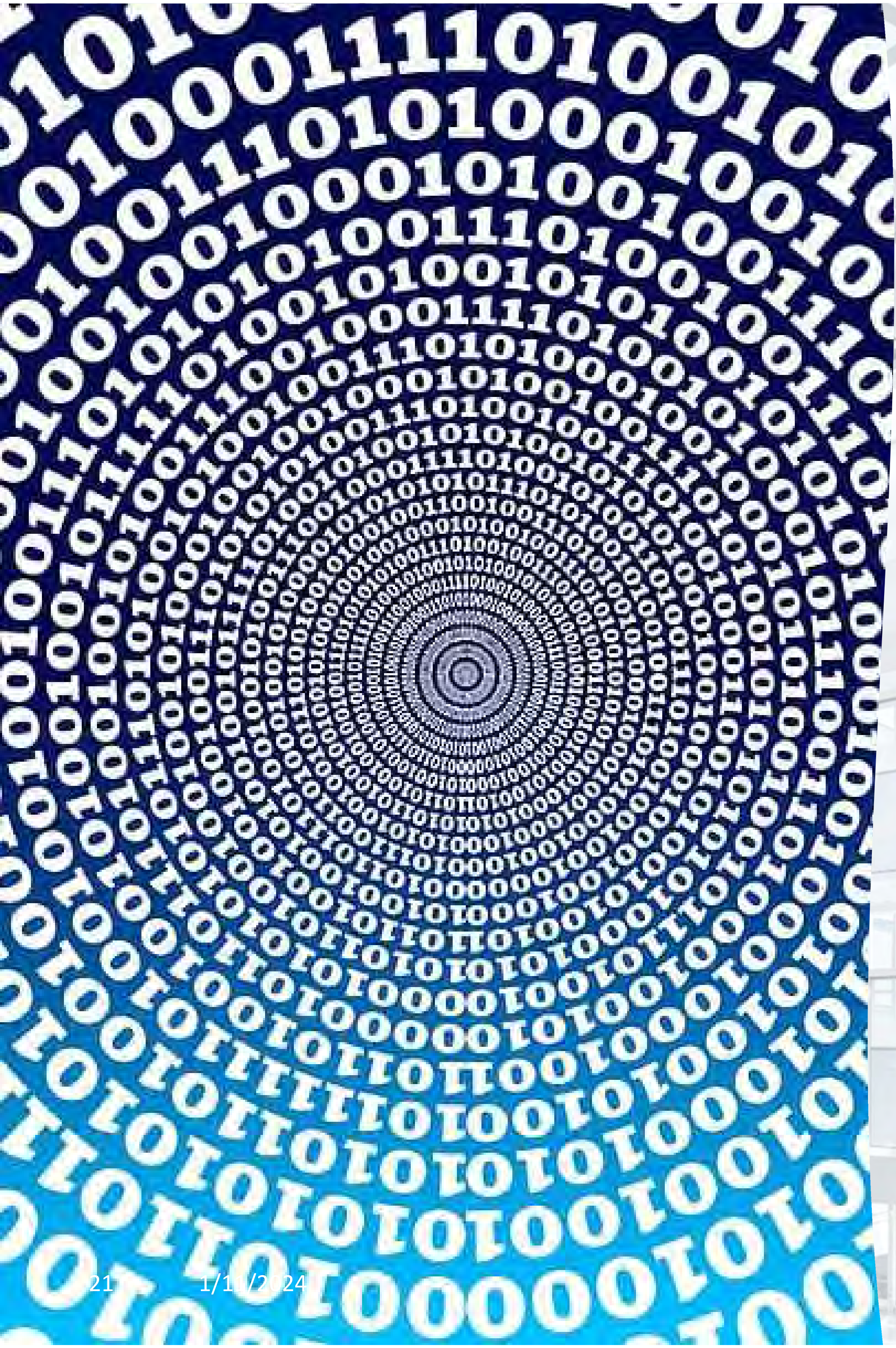
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Why Ransomware?

- As with most cybercrimes, ransomware is usually financially motivated.
- Threat actors will target organizations of any size and demand a ransom based on what they believe the organization will pay to recover their encrypted data.
- Ransomware attacks can have major impacts, including privacy and data breaches, reputational damage, productivity loss, legal repercussions, recovery expenses, and damage to infrastructure and operations.
- Organizations that cannot allow sustained disruptions are more likely to pay millions of dollars to restore their operations quickly.

WHO DO CYBERCRIMINALS TARGET?

- Ransomware attackers continue to target large enterprises and critical infrastructure providers.
- This, however, does not mean other organizations or individuals are safe from the threat of ransomware. Given the need for data to conduct core business functions, any organization can be the victim of ransomware.
- Threat actors consider small and medium-sized organizations to be targets, as their security protection measures are weaker and more susceptible to an attack.
- Ransomware victims will likely continue to give in to ransom demands due to the severe costs of losing business and rebuilding their networks and the potentially destructive consequences of refusing payment.

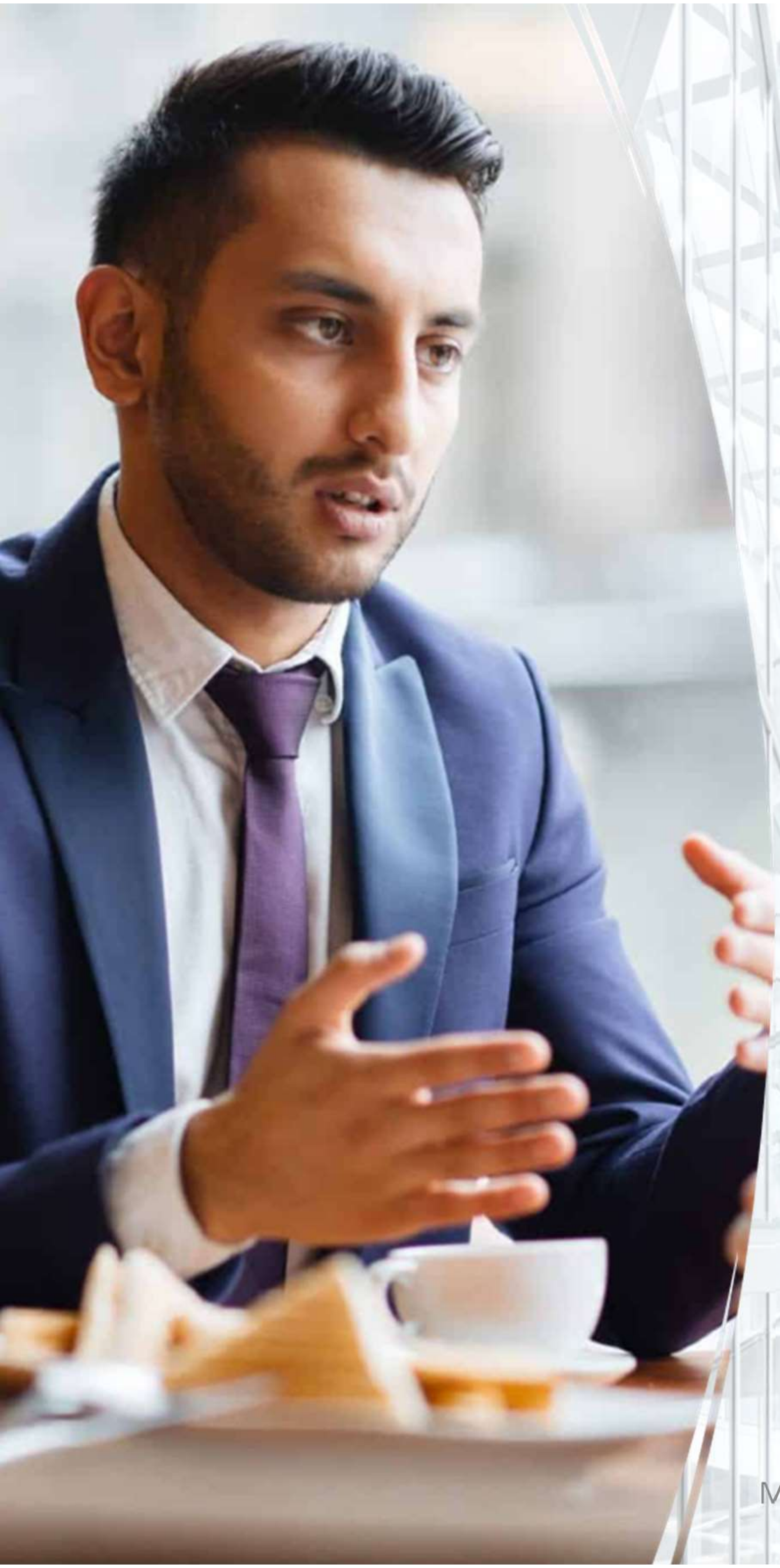


Data Extortion

- Information is often stolen by cyber threat actors concurrently with the ransomware attack.
- Threat actors can hold data for ransom, sell it, or use it to gain an unfair competitive advantage by exploiting proprietary or patented information.
- The theft of organizational information, including intellectual property and customer and client data, can have short- and long-term financial consequences for victims, including impacts on global competitiveness, reputational damage, and identity theft.

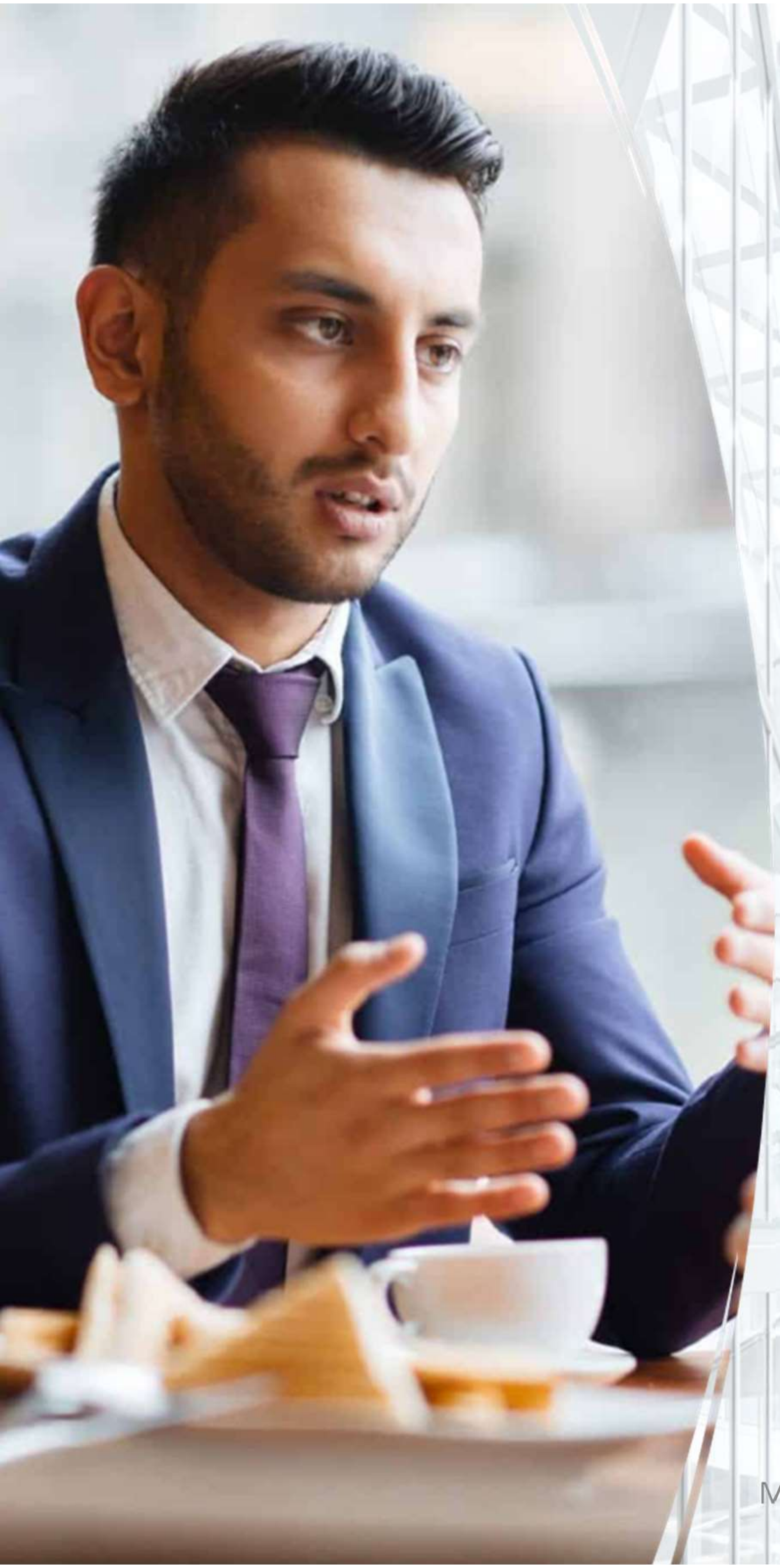
SHOULD YOU PAY THE RANSOM?

- The decision to pay a cyber threat actor to release your files or devices is difficult, and you may feel great financial pressure to restore operations by giving in to their demands.
- Before you pay, contact and report the cybercrime to your local police department and the FBI at IC3.GOV.
- Paying the ransom does not guarantee access to your encrypted data or systems.
- The decision to pay the ransom is yours, but your organization needs to be fully aware of the risks associated with paying the ransom.
- For example, threat actors may use wiper malware, which alters or permanently deletes your files once you pay the ransom.



SHOULD YOU PAY THE RANSOM?

- Payment may also be used to fund and support other illicit activities. Even if you pay, threat actors may still carry out the following actions:
  - ➢Demand more money;
  - ➢Continue to infect your devices or other organizations' devices;
  - ➢Re-target your organization with a new attack;
  - ➢Copy, leak, or sell your data.



SHOULD YOU PAY THE RANSOM?

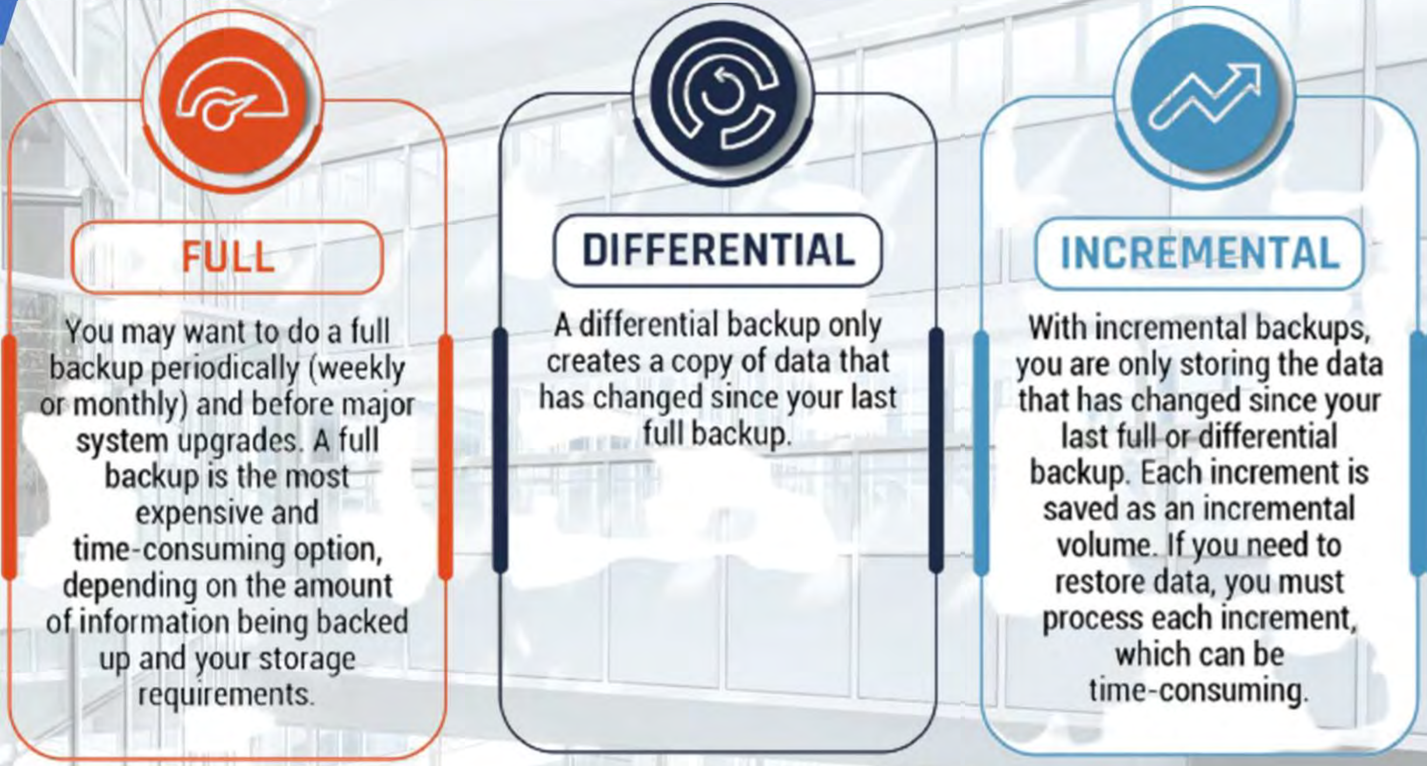
- Because the attackers are financially motivated, paying the ransom rewards their attack.
- Many say that a legal ban on ransom payments is the best way of stopping ransomware because it would remove the financial incentive for the practice.
- However, few victims are prepared for ransomware.
- Victims who have not paid out have experienced grave losses.

HOW TO DEFEND AGAINST CYBER THREATS

- Ransomware is one of the most common types of malware and can be one of the most damaging cyber attacks on your organization.
- Single mitigation measures are not robust enough to combat the evolving ransomware threat.
- Your organization should adopt a ***defense-in-depth*** (multi-layer) strategy to protect its devices, systems, and networks from ransomware and other types of malware and cyber-attacks.
- Your strategy should include several layers of defense with several mitigation measures or security controls at each layer.

DEVELOP YOUR BACKUP PLAN

- Who here has a backup plan and process?
- A backup is a copy of your data and systems that can be restored during an incident.
- Here are three backups you can implement to protect your organization's information.



FULL

You may want to do a full backup periodically (weekly or monthly) and before major system upgrades. A full backup is the most expensive and time-consuming option, depending on the amount of information being backed up and your storage requirements.

DIFFERENTIAL

A differential backup only creates a copy of data that has changed since your last full backup.

INCREMENTAL

With incremental backups, you are only storing the data that has changed since your last full or differential backup. Each increment is saved as an incremental volume. If you need to restore data, you must process each increment, which can be time-consuming.

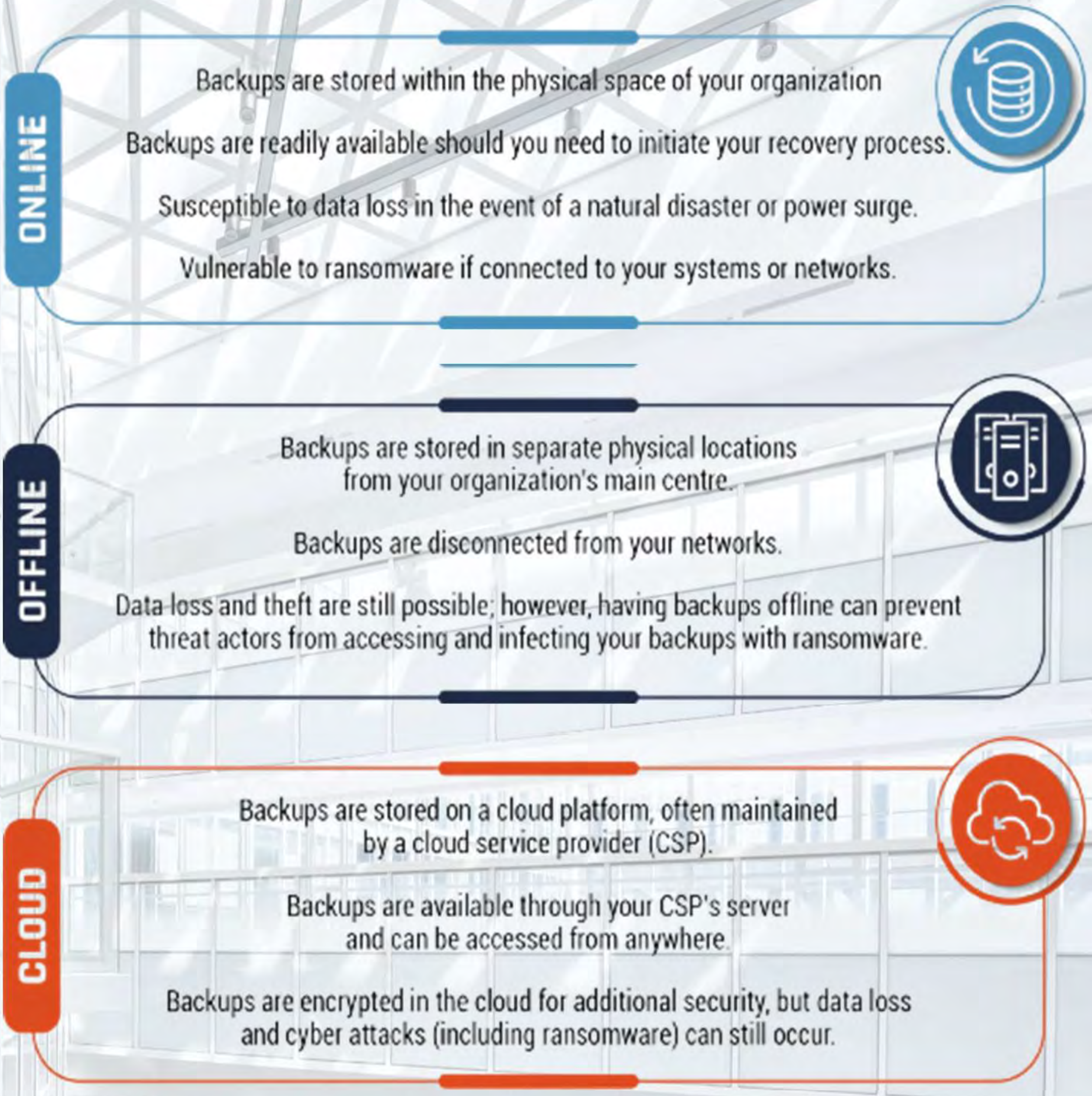
Storing your backups

There are three options for storing your backups: online, offline, and cloud.

Online backups are stored on a remote server or computer connected to your network.

Unlike online backups, **offline backups** ("cold backups") remain unconnected to your network and devices.

Cloud backups are stored on a cloud platform maintained by a service provider.



ONLINE

Backups are stored within the physical space of your organization

Backups are readily available should you need to initiate your recovery process.

Susceptible to data loss in the event of a natural disaster or power surge.

Vulnerable to ransomware if connected to your systems or networks.

OFFLINE

Backups are stored in separate physical locations from your organization's main centre.

Backups are disconnected from your networks.

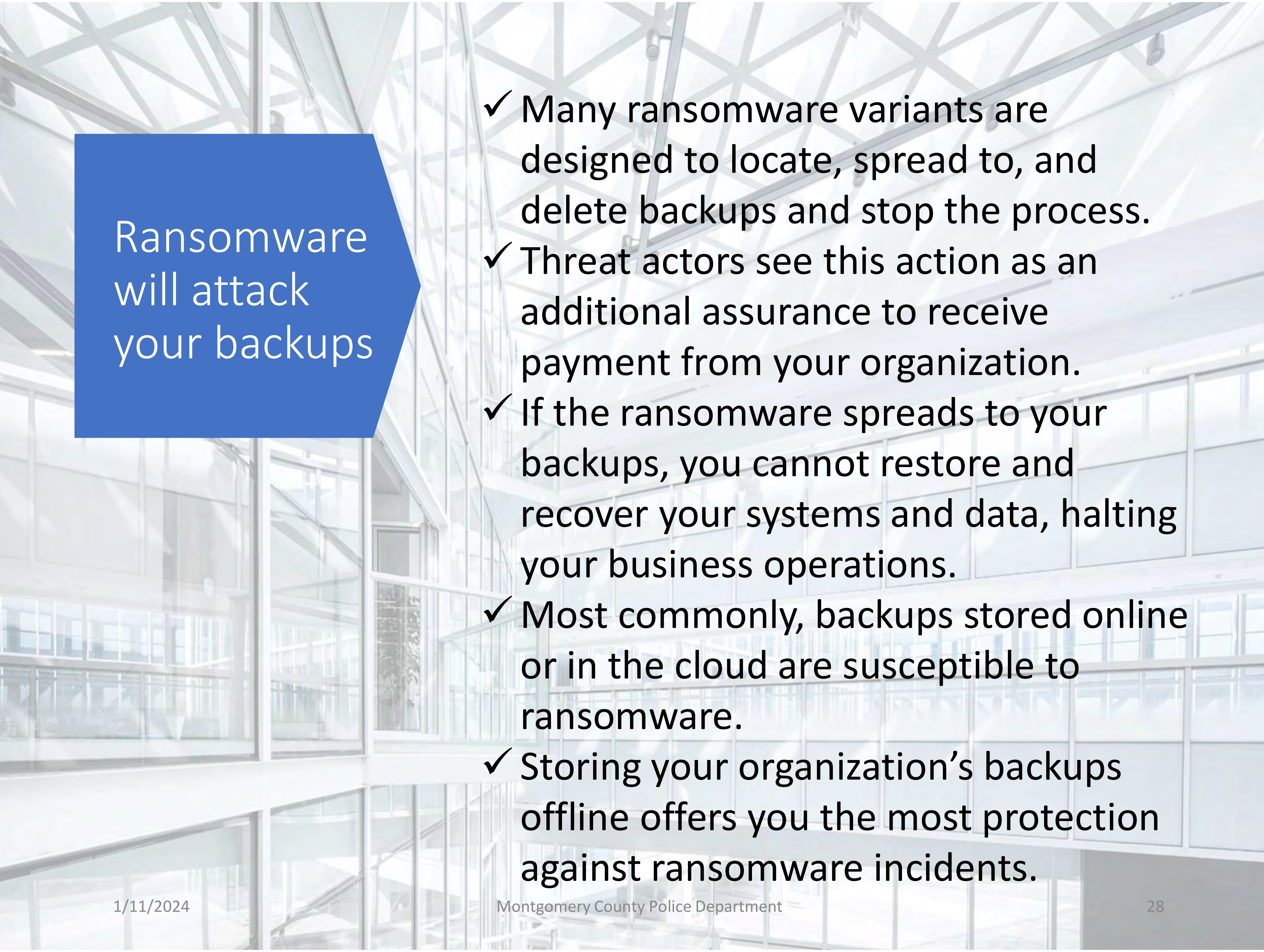
Data loss and theft are still possible; however, having backups offline can prevent threat actors from accessing and infecting your backups with ransomware.

CLOUD

Backups are stored on a cloud platform, often maintained by a cloud service provider (CSP).

Backups are available through your CSP's server and can be accessed from anywhere.

Backups are encrypted in the cloud for additional security, but data loss and cyber attacks (including ransomware) can still occur.



Ransomware will attack your backups

✓ Many ransomware variants are designed to locate, spread to, and delete backups and stop the process.

✓ Threat actors see this action as an additional assurance to receive payment from your organization.

✓ If the ransomware spreads to your backups, you cannot restore and recover your systems and data, halting your business operations.

✓ Most commonly, backups stored online or in the cloud are susceptible to ransomware.

✓ Storing your organization’s backups offline offers you the most protection against ransomware incidents.

Keep backups offline and test them regularly

- The recommended approach to backing up your information is to have multiple backups in multiple locations.
- You should have two or more backups stored offline and inaccessible by your networks and internet connection.
- You could then have a secondary backup in the Cloud with your CSP.
- You should implement a schedule to test your backups regularly (e.g. monthly).
- Having one or more backup files available increases your organization’s chance of recovering and getting back to business faster if you are the victim of ransomware or any other cyber incident.

DEVELOP YOUR INCIDENT RESPONSE PLAN

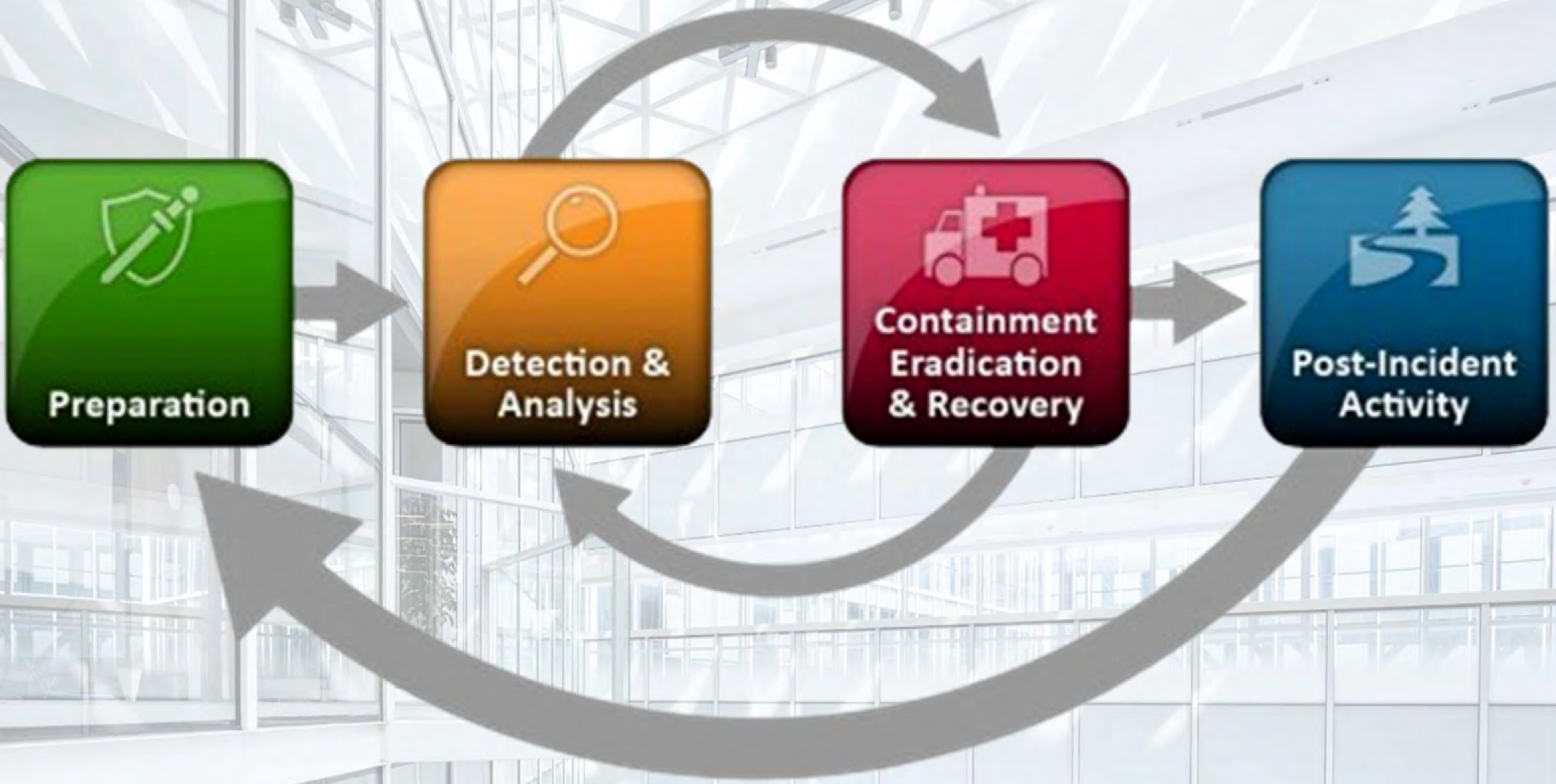
- Developing an **incident response plan** for your organization is the keystone to your cyber defense strategy. Your incident response plan helps you detect and respond to cybersecurity incidents.
- You should also consider developing a **disaster recovery plan** for your business. Your disaster recovery plan focuses on how the organization recovers and resumes critical business functions after an incident.
- Through these two plans, your organization considers major events that could cause an unplanned outage and require you to activate your recovery response.

DEVELOP YOUR INCIDENT RESPONSE PLAN

The benefits of an incident response plan

- Effective incident management lessens the impact of a cyber incident;
- Practice your plan so you will make good decisions under the pressure of a real incident;
- Approve Key actions in advance, allowing financial authorities and resources to be available in the immediate steps of your incident response;
- A well-managed response, with clear communication throughout, builds trust with shareholders and customers; and,
- Learning from incidents identifies gaps and issues with your response capability

NIST SP 800-61 R2 COMPUTER SECURITY INCIDENT HANDLING GUIDE



Preparation

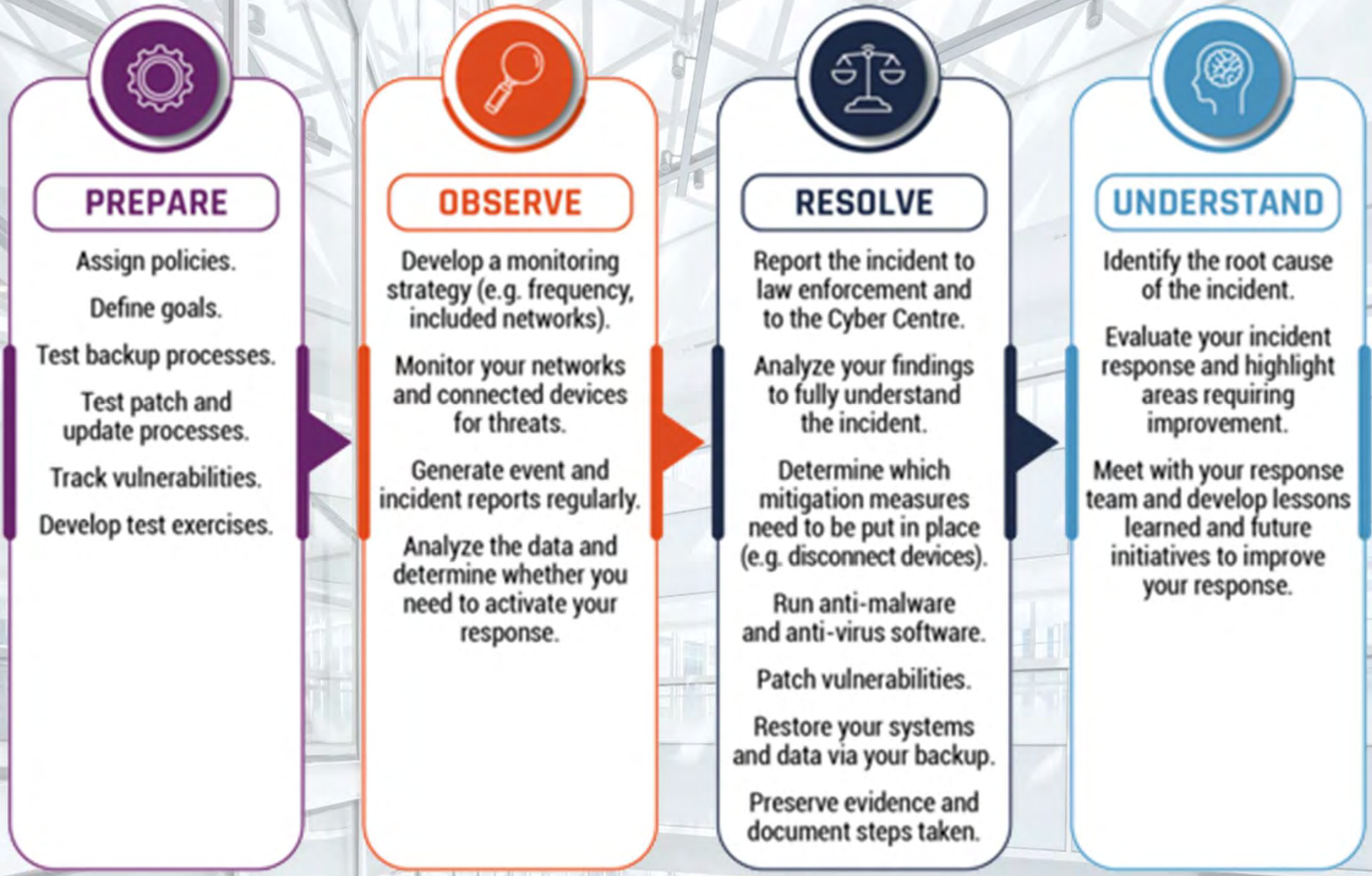
Detection & Analysis

Containment Eradication & Recovery

Post-Incident Activity

Figure 3-1. Incident Response Life Cycle

Figure 5: Incident Response Phases



PREPARE

Assign policies.

Define goals.

Test backup processes.

Test patch and update processes.

Track vulnerabilities.

Develop test exercises.

OBSERVE

Develop a monitoring strategy (e.g. frequency, included networks).

Monitor your networks and connected devices for threats.

Generate event and incident reports regularly.

Analyze the data and determine whether you need to activate your response.

RESOLVE

Report the incident to law enforcement and to the Cyber Centre.

Analyze your findings to fully understand the incident.

Determine which mitigation measures need to be put in place (e.g. disconnect devices).

Run anti-malware and anti-virus software.

Patch vulnerabilities.

Restore your systems and data via your backup.

Preserve evidence and document steps taken.

UNDERSTAND

Identify the root cause of the incident.

Evaluate your incident response and highlight areas requiring improvement.

Meet with your response team and develop lessons learned and future initiatives to improve your response.

Out-of-band (OOB) communications

Establish an alternative system or technology for incident responders to collaborate, coordinate, and inform

OOB should be independent of existing IT infrastructure.

OOB should provide email, voice, and real-time communications capabilities; and file storage.

OOB should provide mass one-way communications to employees, clients, and the public.

Ensure that your OOB solution meets any internal legal requirements.

Set up OOB before an incident occurs.

Test your OOB platforms.

Your incident response plan

- The main goal is to recover from an incident in the least amount of time possible.
- The following checklist provides an overview of the key elements you should include in your incident response plan.
- It is not a comprehensive list of incident response requirements but does provide a structured approach and action items your organization can implement.
- By including these elements in the early development stages of your incident response plan, you can ensure you identify your risks, devise a plan of action to mitigate them, and
- Prepare your organization for an efficient recovery that will allow you to get back to business faster.

Your incident response plan

RISK ASSESSMENT

- Identify your key systems and assets that are critical to your business operations.
- Analyze the likelihood and impact of these systems being compromised.
- Prioritize your response efforts to ensure the most critical systems and assets are protected and backed up offline frequently and securely.

Your incident response plan

POLICIES & PROCEDURES

- Develop an incident response policy that establishes your organization authorities, roles, and responsibilities.
- Ensure pre-authorizations to contract assistance is established and communicated to key incident response contacts.

Your incident response plan

MEASURE

- Set clear recovery objectives.
- Define backup and recovery strategies.
- Test your plan.

Your incident response plan

ESTABLISH YOUR CIRT

- Create a CYBER INCIDENT RESPONSE TEAM (CIRT) to assess, document, and respond to incidents, restore your systems, recover information, and reduce the risk of the incident reoccurring.
- Include employees with various qualifications and have cross-functional support from other business lines.
- Designate backup responders to act for any absent CIRT members in the event of an incident.

Your incident response plan

TRAINING

- Tailor your training programs to your organization's business needs and requirements and your employees' roles and responsibilities.
- Ensure your training includes the cyber security controls listed in section 2.2 (e.g. spotting malicious emails and phishing attacks and using strong passwords or passphrases).
- Consult CISA for advice and guidance on cyber security event management training.

Your incident response plan

IDENTIFY STAKEHOLDERS

Identify the internal and external key stakeholders who will be notified during an incident.

Connect with your managed service providers (MSPs) to identify areas where they can assist you with your recovery efforts.

Engage IT Security Specialists prior to an event to ensure you have subject matter experts weighing in on your response and recovery efforts.

You may have to alert third parties, such as your insurer, clients, suppliers, and managed service providers.

Including the FBI, law enforcement, your lawyers, and regulators.

Your incident response plan

COMMUNICATIONS PLAN

Detail how, when, and with whom your team communicates.

Include a central point of contact for employees to report suspected or known incidents.

Ensure you have external contact information for all members and backup members of your response team, key personnel, and key stakeholders.

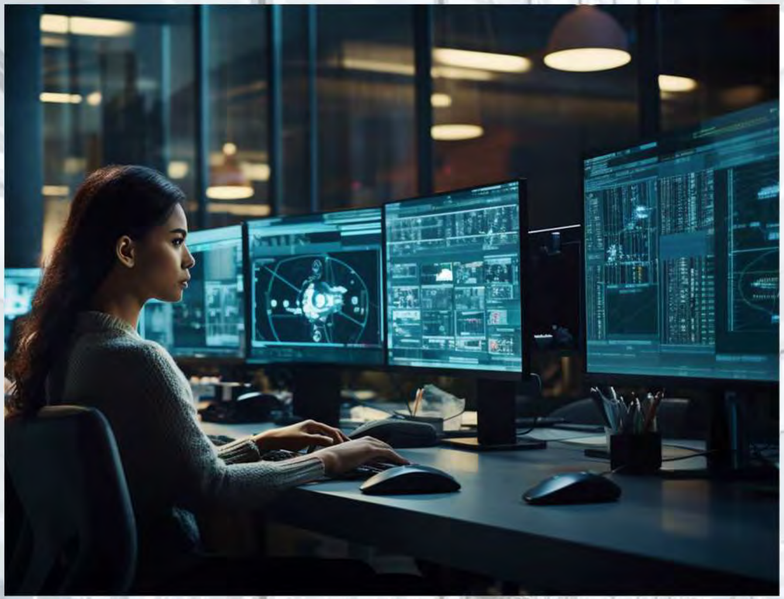
Prepare sample media statements that can be tailored to cyber incidents as they occur.

Consider retaining a third-party organization that can guide you through your incident response and recovery process.

Table 1: Incident Response Plan Checklist

PRIORITY ELEMENT	REQUIREMENTS
1. RISK ASSESSMENT	• Identify your key systems and assets that are critical to your business operations. • Analyze the likelihood and impact of these systems being compromised. • Prioritize your response efforts to ensure the most critical systems and assets are protected and backed up offline frequently and securely.
2. POLICIES & PROCEDURES	• Develop an incident response policy that establishes the authorities, roles, and responsibilities of your organization. • Ensure pre-authorizations to contract assistance is established and communicated to key incident response contacts.
3. ESTABLISH YOUR CIRT	• Create a CYBER INCIDENT RESPONSE TEAM (CIRT) to assess, document, and respond to incidents, restore your systems, recover information, and reduce the risk of the incident reoccurring. • Include employees with various qualifications and have cross-functional support from other business lines. • Designate backup responders to act for any absent CIRT members in the event of an incident.
4. TRAINING	• Tailor your training programs to your organization's business needs and requirements, as well as your employees' roles and responsibilities. • Ensure your training includes the cyber security controls listed in section 2.2 (e.g. spotting malicious emails and phishing attacks and using strong passwords or passphrases). • Consult CISA for advice and guidance on cyber security event management training.
5. IDENTIFY STAKEHOLDERS	• Identify the internal and external key stakeholders who will be notified during an incident. You may have to alert third parties, such as clients and managed service providers. Include the FBI, law enforcement, or a lawyer.
6. COMMUNICATIONS	• Detail how, when, and with whom your team communicates. • Include a central point of contact for employees to report suspected or known incidents. • Ensure you have external contact information for all members and backup members of your response team, key personnel, and key stakeholders. • Prepare sample media statements that can be tailored to cyber incidents as they occur. • Consider retaining a third-party organization that can guide you through your incident response and recovery process.

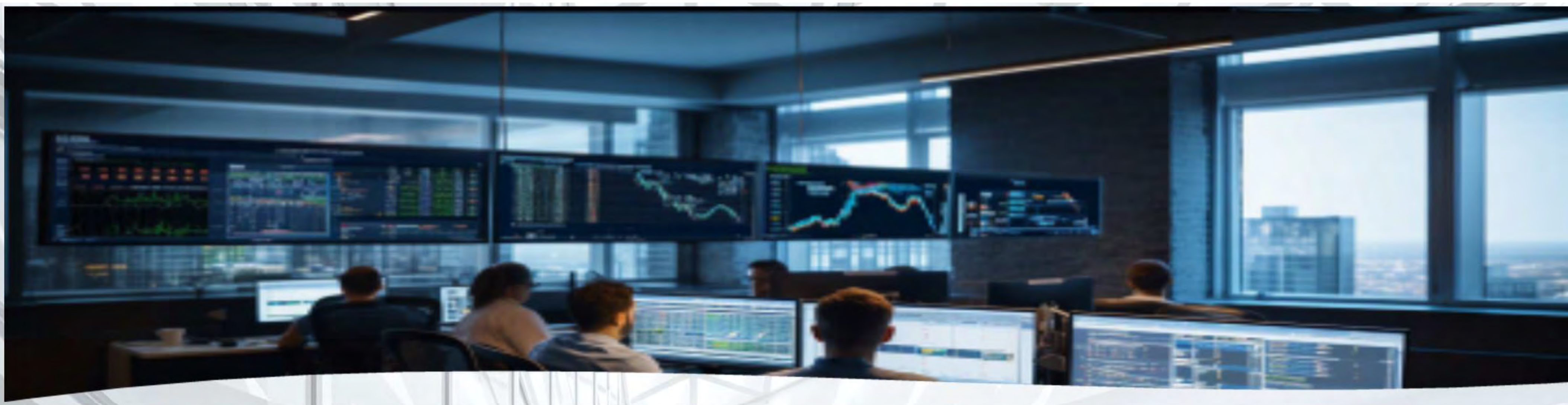
DEVELOP YOUR RECOVERY PLAN



- Your recovery plan should complement your incident response and backup plans.
- When developing your recovery response, you should consider many variables and clearly identify and document what will be recovered, by whom, when, and where.
- Consider the following guidelines detailed in Table 2 when developing your recovery plan.

Table 2: Guidelines for Your Recovery Plan

PHASE	GUIDELINE
PLANNING	• Identify stakeholders, including clients, vendors, business owners, systems owners, and managers. • Identify your response team members, as well as their roles and responsibilities. • Take inventory of your hardware and software assets. • Identify and prioritize critical business functions, applications, and data. • Prepare emergency documentation, such as a contact list for all employees, clients, service providers and suppliers, to ensure you can react quickly and efficiently in the event of a ransomware incident. • Conduct a tabletop exercise to ensure all required participants are aware of their role and required actions in the event of a ransomware attack. • Invest in cyber security insurance if you determine it to be beneficial for your organization. Your policy may add an additional layer of protection and may also provide your organization with incident response expertise in the event of a ransomware attack.
MEASURE	• Set clear recovery objectives. • Define backup and recovery strategies. • Test your plan.
COMMUNICATIONS	• Develop a communications plan to inform key stakeholders. • Develop a training program for employees to ensure everyone is aware of their roles, responsibilities, and order of operations during an incident. • Connect with your managed service providers (MSPs) to identify areas in which they can assist you with your recovery efforts. • Engage IT Security Specialists prior to an event to ensure you have subject matter experts weighing in on your response and recovery efforts.



DEVELOP YOUR RECOVERY PLAN

To create an effective plan, you should identify your organization's critical data, applications, and functions. Critical information may include financial records, proprietary assets, and personal data.

Critical applications are the systems running your key business functions and are imperative to your business.

These are the systems you need to restore immediately to have business continuity in the event of an unplanned outage or incident.

You should consider conducting a risk assessment to help identify critical business functions and the relevant threat and vulnerability risks.

DEVELOP YOUR RECOVERY PLAN

To ensure your response is effective, your organization should run through specific scenarios (e.g., cyber-attack, significant power outage, or natural disaster) to help you identify key participants and stakeholders, address the significant risks, develop mitigation strategies, and identify the recovery time and effort.

You can conduct a business impact analysis (BIA) to predict how disruptions or incidents will harm your operations, business processes, systems, and finances.

During your BIA, you should also assess the data you collect and the applications you use to determine their criticality and choose priorities for immediate recovery.

It is also critical to take note of your recovery efforts, documenting what went well and what areas require improvement.

MANAGE USER AND ADMINISTRATOR ACCOUNTS

- Oversee the creation and assignment of user and administrator accounts with secure access in mind.
- Consider creating separate accounts for non-administrative functions (e.g. access to email and limited access to internal systems) to reduce the risk of ransomware infecting your administrator accounts and system access that is associated with those accounts.
- You should limit administrator accounts to those who need full or specialized access to your organization’s network, systems, and devices.

MANAGE USER AND ADMINISTRATOR ACCOUNTS

- If a threat actor gains access to an administrative account, they can use the elevated privileges to affect your organization’s operating environment, attack your network and access sensitive information.
- Attackers can also learn which detection and recovery activities are in place on your systems, helping them avoid discovery and preventing you from stopping further attacks.

MANAGE USER AND ADMINISTRATOR ACCOUNTS

- To manage access to your systems and data, apply the ***principle of least privilege: only provide employees with access to the functions and privileges necessary to complete their tasks***.
- You should also use the principle of least privilege when allowing remote access to your devices.
- Ensure you enable multi-factor authentication (MFA) at all access points into your network and consider using single sign-on (SSO) access where possible to enhance the security of your devices and connected networks.

MANAGE USER AND ADMINISTRATOR ACCOUNTS

- Restrict administrative privileges and require confirmation for any actions that need elevated access rights and permissions
- In addition to managing your accounts, you must also manage the decommissioning and disconnecting of obsolete or retired systems and devices.
- These systems and devices must be removed from your network, sanitized, and disposed of securely.

MANAGE USER AND ADMINISTRATOR ACCOUNTS

When assigning administrator accounts or privileged access, take the following measures:

- Use strong authentication methods for your accounts;
- Use MFA for all administrative accounts;
- Use a unique password for each privileged account;
- Change default passwords for applications and devices;
- Authenticate users before they are granted access to applications or devices;

MANAGE USER AND ADMINISTRATOR ACCOUNTS

When assigning administrator accounts or privileged access to users, you should take the following measures:

- Ensure that unique, identifiable accounts are attributed to individual users;
- Log and monitor actions on privileged accounts;
- Provide training on expected behaviors or privileged account users;
- Remove special access privileges when users no longer require them; and,
- Decommission and delete user accounts when someone leaves the organization.

CYBER SECURITY CONTROLS

When implementing and maintaining a defense-in-depth model, it is imperative that your organization layers security controls throughout your networks to protect the security, confidentiality, integrity, and availability of your networks, devices, and information.

CYBER SECURITY CONTROLS

The following diagram (Figure 6) once again highlights the three stages of a ransomware incident: the threat actor gains access to your network, takes control of your systems and connected devices, and then deploys the malware payload and infect your systems and connected devices with ransomware.

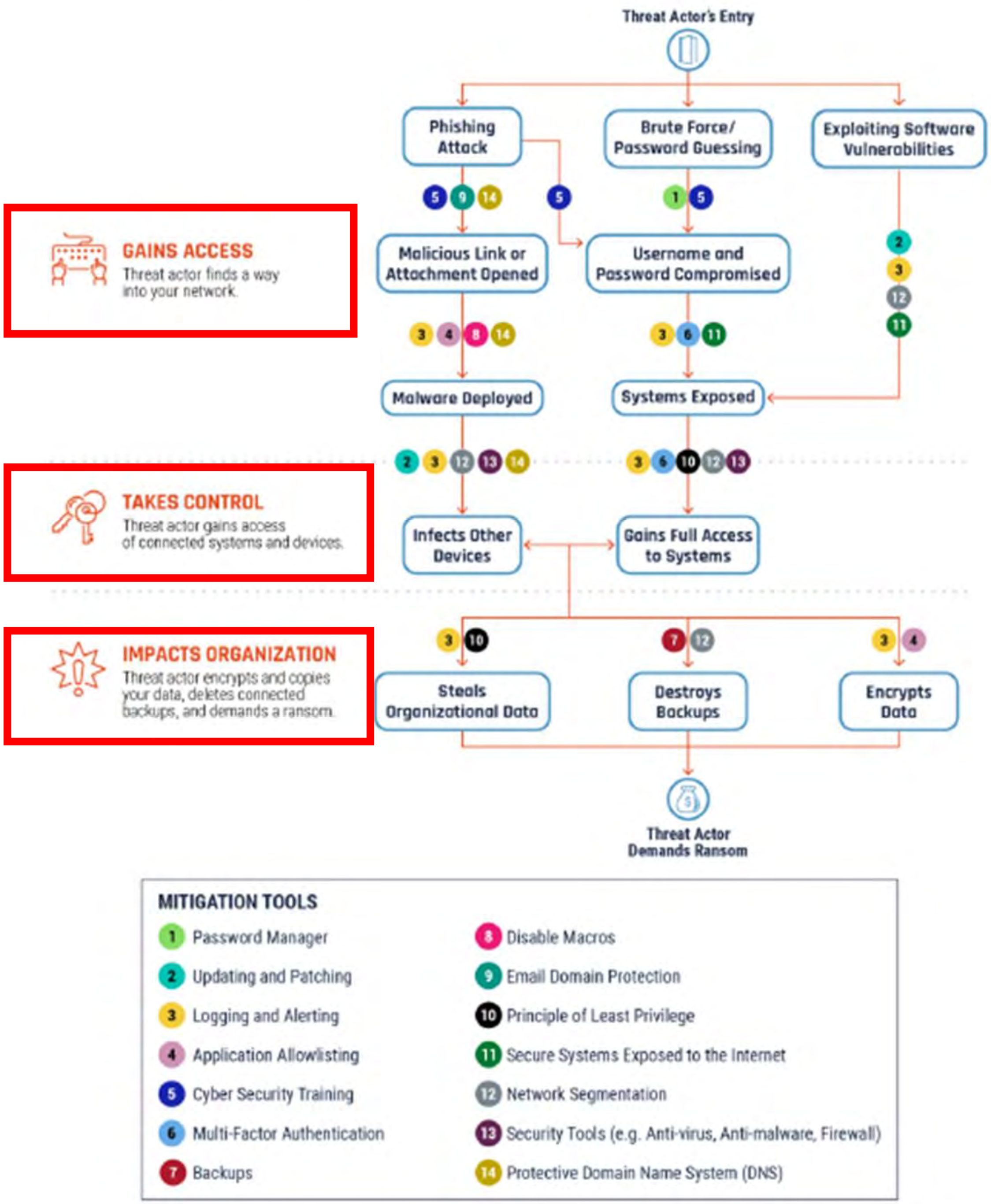
As shown in Figure 6, a variety of security controls, layered throughout your networks, can enhance your ability to defend against ransomware.

Note: Some cyber security controls identified in Figure 6 can be applied at various stages or areas within your network and systems. For example, logging and alerting and network segmentation are applied at all layers of your defence-in-depth strategy.

Montgomery County Police Department

CYBER SECURITY CONTROLS

Figure 6: Security Controls to Reduce the Risk of Ransomware [10]


Threat Actor's Entry
Phishing Attack
Brute Force/ Password Guessing
Exploiting Software Vulnerabilities
5 9 14
5
1 5
2 3 12 11
GAINS ACCESS
Threat actor finds a way into your network.
Malicious Link or Attachment Opened
Username and Password Compromised
3 4 8 14
3 6 11
Malware Deployed
Systems Exposed
2 3 12 13 14
3 6 10 12 13
TAKES CONTROL
Threat actor gains access of connected systems and devices.
Infects Other Devices
Gains Full Access to Systems
3 10
7 12
3 4
IMPACTS ORGANIZATION
Threat actor encrypts and copies your data, deletes connected backups, and demands a ransom.
Steals Organizational Data
Destroys Backups
Encrypts Data
Threat Actor Demands Ransom

MITIGATION TOOLS

1	Password Manager	8	Disable Macros
2	Updating and Patching	9	Email Domain Protection
3	Logging and Alerting	10	Principle of Least Privilege
4	Application Allowlisting	11	Secure Systems Exposed to the Internet
5	Cyber Security Training	12	Network Segmentation
6	Multi-Factor Authentication	13	Security Tools (e.g. Anti-virus, Anti-malware, Firewall)
7	Backups	14	Protective Domain Name System (DNS)

CYBER SECURITY CONTROLS

GAINS ACCESS
Threat actor finds a way into your network.

In the **first stage** of a ransomware incident, there are some preventative mitigation measures that can be put in place to protect your organization. The following is a list of such controls:

1. Provide your employees with tailored cyber security training to ensure they are aware of attack vectors like phishing and how to identify suspicious emails or links.
2. Use of strong passwords, or preferably passphrases, to attempt to prevent threat actors from being successful in brute force attacks.
3. Implement MFA for your organization’s devices.
4. Create an application allow-list to control who or what is allowed access to your networks and systems. Application-allow lists help to prevent malicious applications from being downloaded and infecting your server.

CYBER SECURITY CONTROLS

GAINS ACCESS

Threat actor finds a way into your network.

The list of first stage controls continues:

5. Scan your hardware, software, and operating system for vulnerabilities and apply patches and updates to mitigate the risk of the vulnerabilities being exploited by a threat actor.
6. Segment your network to ensure sensitive and high-value information is in a different zone of your network.
7. Setup monitoring and logging functionality for your systems and networks and ensure you receive automated alerts if any anomalies are detected.
8. Protect your systems that are connected or exposed to the Internet with encryption, firewalls, MFA, and frequent vulnerability assessments.
9. Disable macros to decrease the risk of spreading ransomware through Microsoft Office attachments.

TAKES CONTROL

Threat actor gains access of connected systems and devices.

CYBER SECURITY CONTROLS

In the second stage of a ransomware incident, there are mitigation measures you can employ:

Enhance the protection of your systems and networks and prevent ransomware from spreading across your network and connected devices.

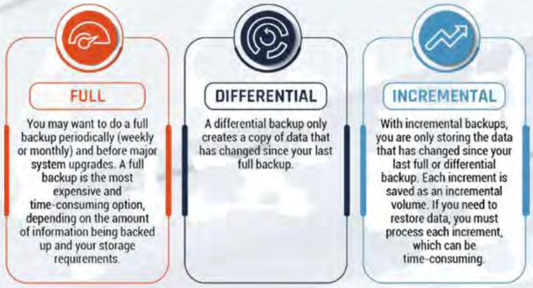
Implement security tools, such as anti-virus and anti-malware software, as well as firewalls, to your networks to add layers of protection to potential entry points for threat actors.

Apply the principle of least privilege; provide individuals only the privileges that are essential for them to perform authorized tasks.

IMPACTS ORGANIZATION
Threat actor encrypts and copies your data, deletes connected backups, and demands a ransom.

CYBER SECURITY CONTROLS

In the third stage of a ransomware incident, your backup plan is the number one mitigation measure.



FULL

You may want to do a full backup periodically (weekly or monthly) and before major system upgrades. A full backup is the most expensive and time-consuming option, depending on the amount of information being backed up and your storage requirements.

DIFFERENTIAL

A differential backup only creates a copy of data that has changed since your last full backup.

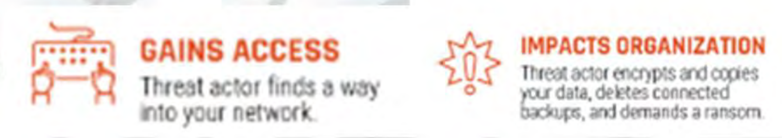
INCREMENTAL

With incremental backups, you are only storing the data that has changed since your last full or differential backup. Each increment is saved as an incremental volume. If you need to restore data, you must process each increment, which can be time-consuming.

Ensure you have multiple copies of your backup stored offline and if possible, in the cloud through a CSP.

Disconnect your backups from your network so threat actors cannot delete or infect them with ransomware.

Schedule tests of backups and restore processes and adjust any issues immediately to ensure your backup files are ready so your organization can recover quickly from an incident.


GAINS ACCESS
Threat actor finds a way into your network.
IMPACTS ORGANIZATION
Threat actor encrypts and copies your data, deletes connected backups, and demands a ransom.

ESTABLISH PERIMETER DEFENSES

- Create perimeter defenses to protect the boundary between the network security zones through which your traffic is routed.
- If this is defended by basic security protocols like **firewalls, anti-virus, and anti-malware software**, your overall protection is significantly enhanced.
- Installing **anti-phishing software** is another option for enhancing your organization’s cyber security. Anti-phishing software blocks phishing emails to prevent attacks from occurring or spreading further.
- Ensure your users access your network using your **virtual private network (VPN).** A VPN acts as a secure tunnel through which you can send and receive data on an existing physical network. Using a VPN provides a secure connection between two points, such as your laptop and your organization’s network.

IMPLEMENT LOGS AND ALERTS

- Implementing continuous monitoring of your networks will help you establish a baseline for acceptable activity patterns within your organization.
- Automated monitoring of your networks and systems can help manage risk.
- Your monitoring system should generate logs that can be reviewed by IT specialists and AI when necessary.
- Access to your logs should be limited to those who need to review them.

GAINS ACCESS

Threat actor finds a way into your network.

TAKES CONTROL

Threat actor gains access of connected systems and devices.

IMPACTS ORGANIZATION

Threat actor encrypts and copies your data, deletes connected backups, and demands a ransom.

GAINS ACCESS
Threat actor finds a way into your network.

TAKES CONTROL
Threat actor gains access of connected systems and devices.

IMPACTS ORGANIZATION
Threat actor encrypts and copies your data, deletes connected backups, and demands a ransom.

IMPLEMENT LOGS AND ALERTS

- Implementing automatic alerting within your monitoring practices is also necessary to flag and review anomalies in activity patterns.
- Mitigate potential vulnerabilities and investigate suspicious events.
- Do not permit modifications to your logs once they have been received from the system.
- Log entries should have a time stamp and additional data set by policy to assist you in understanding what led to an event or an incident.

GAINS ACCESS
Threat actor finds a way into your network.

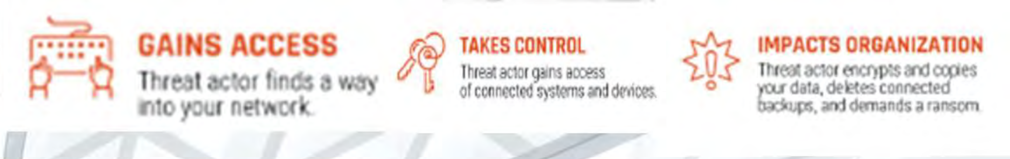
TAKES CONTROL
Threat actor gains access of connected systems and devices.

IMPACTS ORGANIZATION
Threat actor encrypts and copies your data, deletes connected backups, and demands a ransom.

IMPLEMENT LOGS AND ALERTS

If your organization becomes a victim of ransomware or another type of cyber incident,

- your logs could provide you with insight into how the incident occurred and
- what controls or mitigation measures can be implemented to protect your networks and systems from future incidents.



GAINS ACCESS
Threat actor finds a way into your network.

TAKES CONTROL
Threat actor gains access of connected systems and devices.

IMPACTS ORGANIZATION
Threat actor encrypts and copies your data, deletes connected backups, and demands a ransom.

CONDUCT PENETRATION TESTING

- Penetration testing is a method for gaining assurance of the security of a system.
- During a penetration test, the tester attempts to breach some or all of the system's security using the same tools and techniques that an adversary may use.
- Pen tests are not meant to be a primary method of identifying vulnerabilities but rather a method of ensuring your organization’s vulnerability assessment and management processes are effective.

SEGMENT YOUR NETWORKS

TAKES CONTROL
Threat actor gains access of connected systems and devices.

IMPACTS ORGANIZATION
Threat actor encrypts and copies your data, deletes connected backups, and demands a ransom.

When segmenting your network, you divide your network into smaller sections or zones.

With network segmentation, traffic is directed and flows through the different sections of the network.

Segmenting your network allows you to stop traffic flow in certain zones and prevent it from flowing to other areas in your network.

In the same manner, segmentation also allows you to isolate and stop the spread of malware to different sections of your network and control and restrict access to your assets

When segmenting your network, ensure your information technology (IT) and operational technology (OT) networks are identified, separated, and monitored.

In addition to segmenting your IT and OT networks, you should also identify interdependencies between them and implement measures that can be put in place during a cyber incident to protect critical information and functions.

GAINS ACCESS

Threat actor finds a way into your network.

CONSTRAIN SCRIPTING ENVIRONMENTS AND DISABLE MACROS

- If your organization uses Windows, you may want to constrain your scripting environments.
- Microsoft PowerShell provides attackers with an automated system administration capability.
- It is a powerful and important part of the system administration toolkit.
- PowerShell has many benefits, but it is not needed by most employees.
- Threat actors can exploit PowerShell and inject malicious code into your device’s memory.
- More concerning is the fact that PowerShell is a trusted source.
- Therefore the threat actor’s code injection will typically not be blocked by anti-virus or anti-malware software or by your systems’ event logs.

GAINS ACCESS
Threat actor finds a way into your network.

IMPACTS ORGANIZATION
Threat actor encrypts and copies your data, deletes connected backups, and demands a ransom.

CONSTRAIN SCRIPTING ENVIRONMENTS AND DISABLE MACROS

Another item to consider when using Windows is macros in Microsoft Office applications.

- Macros are written sequences that imitate user keystrokes and mouse commands to repeat application tasks automatically.
- Macros are used in many Office products to automate processes and data flows.
- They are embedded in the code of the files, enabling users to create shortcuts for specific tasks (e.g., sort worksheets alphabetically, unmerge all merged cells, unhide all rows and columns).
- Threat actors can create malicious macros and include them in documents that they may then send to employees in your organization.
- To decrease the risk of ransomware being spread through Office attachments, you should set your user defaults to disable macros and ensure users cannot re-enable disabled macros.
- You should also ensure macros cannot contain sensitive information, such as personal credentials, and use organization-developed or signed macros that are verified by technical authorities within your organization.

GAINS ACCESS
Threat actor finds a way into your network.
TAKES CONTROL
Threat actor gains access of connected systems and devices.

PATCH AND UPDATE

To protect your connected devices from ransomware, you should ensure you check the operating system, software, and firmware regularly for updates and install security patches.

There are a variety of patches available; however, the following three types are most common:

1. **Bug fix patch**: Repairs functionality issues in software (e.g., error that causes unexpected device behavior;

2. **Security patch**: Addresses security vulnerabilities to protect the system from threats (e.g. malware infecting devices through security flaws) or

3. **Feature patch**: Adds new functions to the software (e.g. enhancements to application performance and speed).

CREATE APPLICATION ALLOW LISTS

GAINS ACCESS
Threat actor finds a way into your network.

IMPACTS ORGANIZATION
Threat actor encrypts and copies your data, deletes connected backups, and demands a ransom.

Application allowing involves the creation of an access control list that identifies who or what is allowed access in order to provide protection from harm.

- An allow list selects and approves specific applications and application components (e.g. executable programs, software libraries, configuration files) to run on organizational systems.
- Application allow lists help prevent malicious applications from being downloaded and infecting your server.
- Your organization can create a list of applications authorized for use in the workplace or known to be from a trustworthy vendor.
- When an application is launched, it is compared against the allow list.
- The application is only permitted if it is on that list. Hashing is used to verify the application’s integrity, meaning the application is what it says it is.
- Hashing generates a value from a string of text and is unique to every application.
- If an application is updated or patched, the hash changes to ensure that you are only running the newest version of the application.
- By implementing an application allow list, your organization will enhance your defensive posture against cyber threat actors and prevent incidents such as ransomware.

USE PROTECTIVE DOMAIN NAME SYSTEM (DNS)

Domain Name System (DNS) is a protocol that maps domain names easily read by the human eye to Internet Protocol (IP) addresses easily read by machines.

- It is often referred to as the address book for the Internet. DNS is used for both human-initiated actions (e.g. visiting a website) and machine-initiated actions (e.g. running an update).
- Protective DNS is a tool that can be implemented by your organization to block employees using corporately issued devices from visiting potentially malicious domains on the internet.
- Protective DNS identifies malicious domains against your organization’s blocklist, which lists domains and IP addresses that users are not permitted to visit using corporate assets or while on your organization’s network.

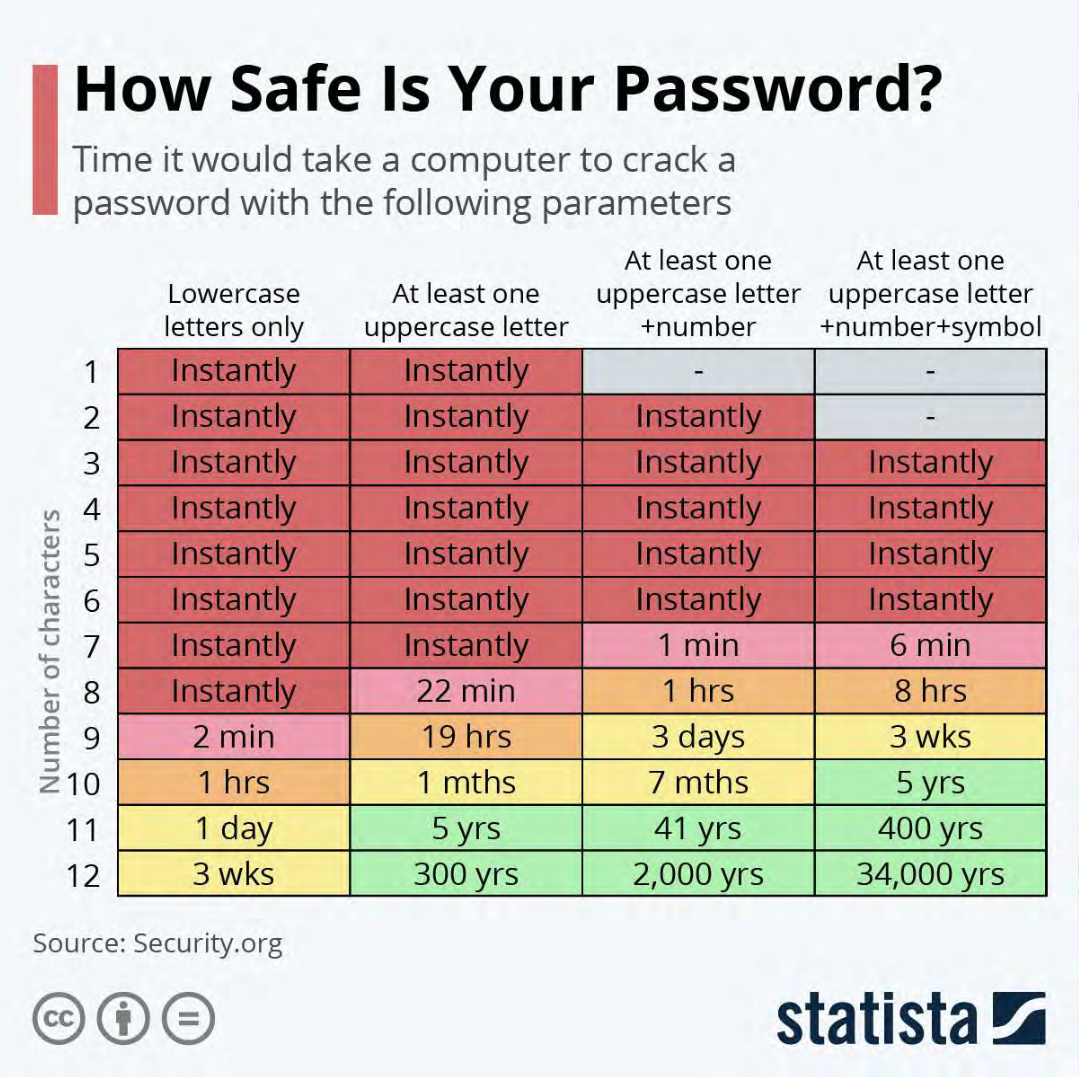
GAINS ACCESS
Threat actor finds a way into your network.
TAKES CONTROL
Threat actor gains access of connected systems and devices.

USE PROTECTIVE DOMAIN NAME SYSTEM (DNS)

- You should also consider implementing protective DNS filtering on any mobile devices used by employees of your organization, especially if they can connect to your network and systems remotely.
- Manually configure DNS settings on your organization’s devices through a mobile device management (MDM) tool.
- Ensure personal devices always use a trusted DNS and filter out malicious IP addresses.
- By replacing the default DNS server settings on your devices with a trusted DNS server you can better protect your devices.

GAINS ACCESS
Threat actor finds a way into your network.
TAKES CONTROL
Threat actor gains access of connected systems and devices.

GAINS ACCESS
Threat actor finds a way into your network.



How Safe Is Your Password?

Time it would take a computer to crack a password with the following parameters

Number of characters	Lowercase letters only	At least one uppercase letter	At least one uppercase letter +number	At least one uppercase letter +number+symbol
1	Instantly	Instantly	-	-
2	Instantly	Instantly	Instantly	-
3	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 min	6 min
8	Instantly	22 min	1 hrs	8 hrs
9	2 min	19 hrs	3 days	3 wks
10	1 hrs	1 mths	7 mths	5 yrs
11	1 day	5 yrs	41 yrs	400 yrs
12	3 wks	300 yrs	2,000 yrs	34,000 yrs

Source: Security.org

statista

APPLY PASSWORD MANAGEMENT

- When permitted, your organization should consider implementing passphrases in place of passwords.
- However, most systems are set up to require a username and password to grant access.
- Using strong passwords is one step in protecting your systems and sensitive information,
- but it is not enough to prevent a threat actor from gaining access.
- Password guessing is a common tactic used by threat actors to gain access to networks and systems.

GAINS ACCESS
Threat actor finds a way into your network.

APPLY PASSWORD MANAGEMENT

- In conjunction with MFA, implementing the use of a password manager for your staff members can be a beneficial tool in remembering and securing passwords required to access your networks and systems.
- Password managers can be a valuable tool for your organization to keep track of the numerous passwords for individual and administrative accounts.
- Your organization should also consider implementing password vaults for administrative accounts.
- Password vaults ensure a higher level of protection as the passwords are cycled and synched with your systems.
- This ensures a password can only be used once and provides tracing capabilities that can determine who used a password at a given time for specific access.

GAINS ACCESS
Threat actor finds a way into your network.

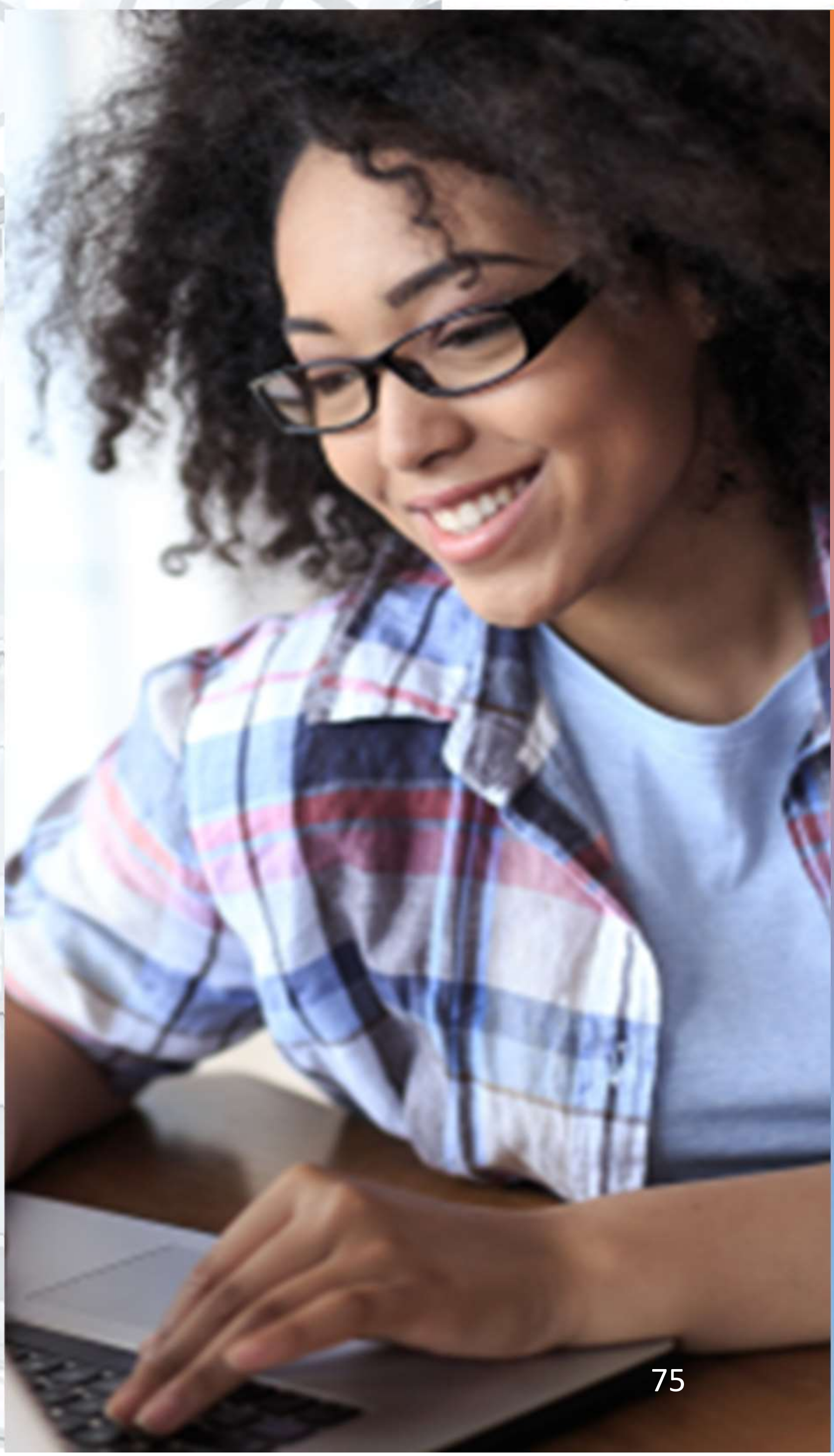
APPLY PASSWORD MANAGEMENT

What responsibility do organizations have to ensure that their employees are

- Using strong passwords, even at home?
- Not reusing past passwords?
- What can organizations do to prevent these problems?

What responsibility do organizations have to ensure that their customers do these steps?

And their suppliers?



GAINS ACCESS

Threat actor finds a way into your network.

USE EMAIL DOMAIN PROTECTION

- Consider implementing technical security measures to protect your organization’s domains from email spoofing, preventing the delivery of malicious messages sent on behalf of your domain, and identifying the infrastructure used by threat actors.
- These measures also help prevent phishing emails from being delivered to your organization.
- You can reduce a threat actor’s chance of carrying out successful malicious email campaigns by implementing the following three security protocols that act jointly to protect email domains from spoofing.

GAINS ACCESS
Threat actor finds a way into your network.

PROTECT EMAIL WITH SPF

Sender Policy Framework (SPF):

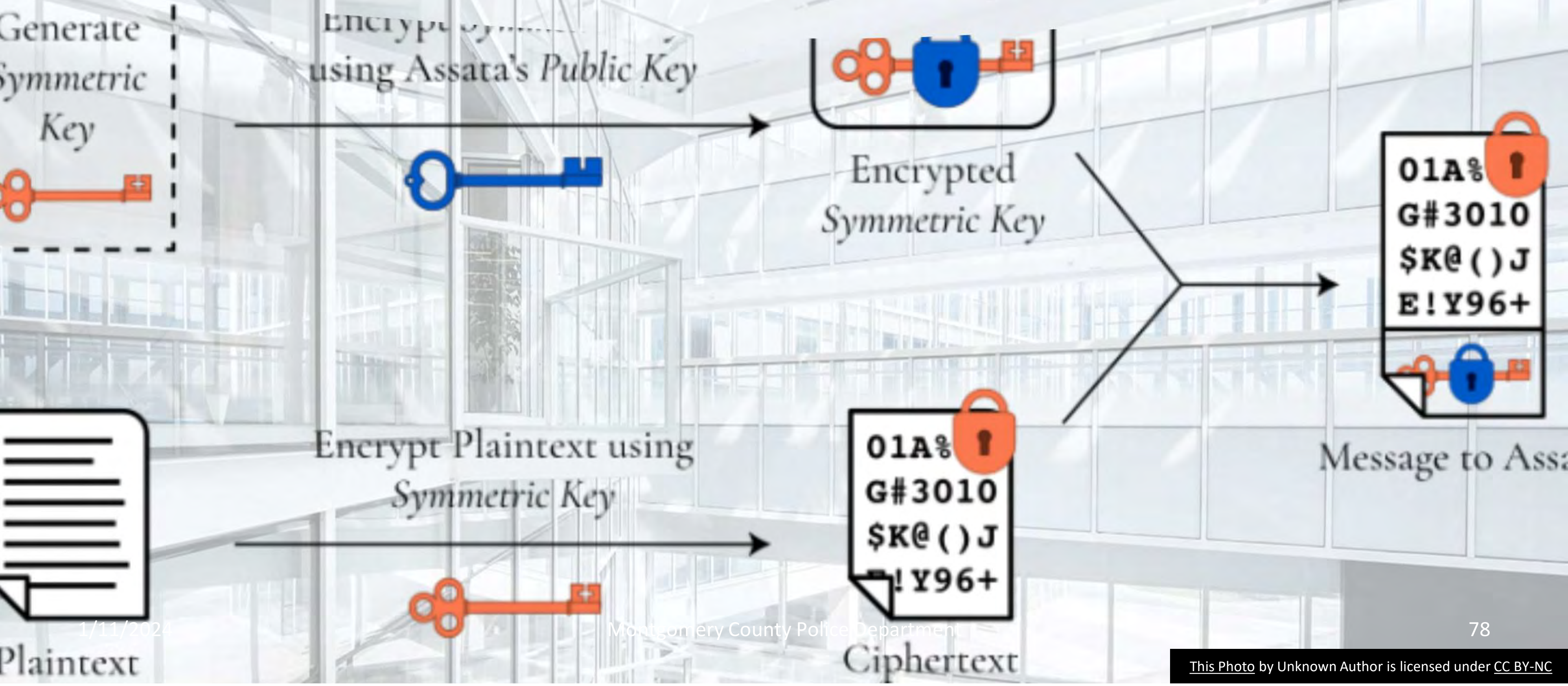
- You can use SPF to specify the Internet protocol (IP) addresses from which emails can be sent on a domain’s behalf.
- When a message is received, an email system that supports SPF will retrieve the SPF record associated with the sending domain
- … and verify that the IP address used to send the message has been authorized.

GAINS ACCESS
Threat actor finds a way into your network.

PROTECT EMAIL WITH DKIM

DomainKeys Identified Mail (DKIM):

- Use DKIM to provide a mechanism to authenticate email messages using a cryptographic signature.
- When an email system that supports DKIM receives a DKIM-signed message, it retrieves the record associated with the message’s DKIM header and verifies the message’s signature using the published public key.
- This DKIM check cryptographically confirms that the message was sent by an authorized sender and was not altered in transit.
- If the signature is invalid or no DKIM record is available, the message will fail DKIM. Messages that fail this DKIM check may be rejected.


Generate Symmetric Key
Encrypt Sy... using Assata's Public Key
Encrypted Symmetric Key
01A% G#3010 $K@()J E!Y96+
Message to Ass
Encrypt Plaintext using Symmetric Key
Plaintext
01A% G#3010 $K@()J E!Y96+
Ciphertext

This Photo by Unknown Author is licensed under CC BY-NC

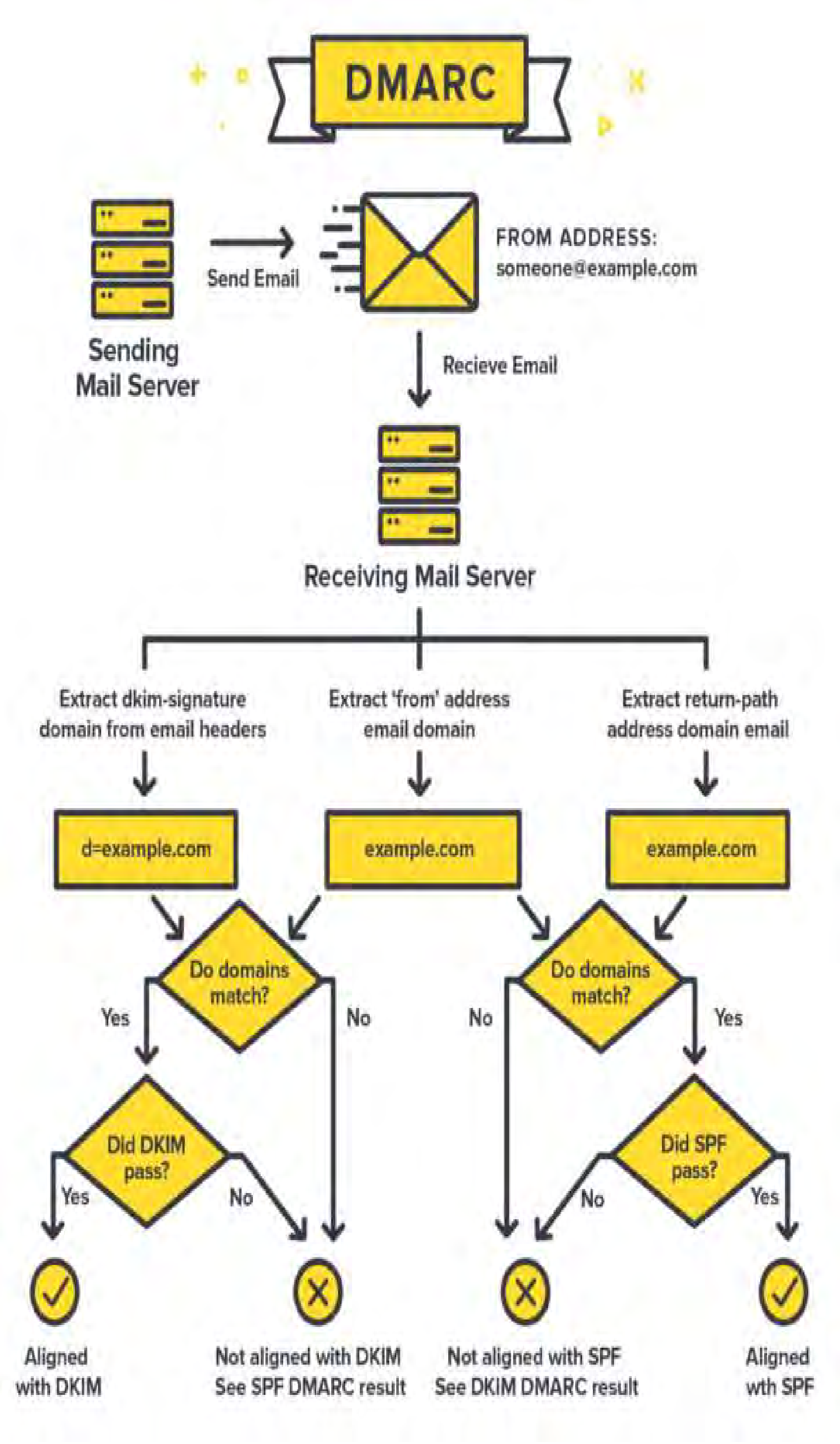
PROTECT EMAIL WITH DMARC

GAINS ACCESS

Threat actor finds a way into your network.

Domain-based Messaged Authentication, Reporting and Conformance (DMARC):

- Implementing DMARC policy and verification can enhance your security protocols and protect your email domains from being spoofed.
- If an email passes through the DMARC validation, it will be delivered to the intended recipient.
- If the email fails DMARC validation, the receiving email system applies the policy specified in the sending domain's DMARC record and will either deliver the email, deliver the email marked as suspicious, or reject the email.



HOW TO RECOVER FROM RANSOMWARE

- Recovering from ransomware can be a lengthy process and recovering your organization’s brand and reputation can be an even longer process.
- Working on the assumption that your organization will encounter some form of malware will assist you in developing your planned response and could speed up your recovery processing time.
- Following this guidance will
  - reduce the time it takes to recover from an attack and
  - reduce the likelihood of an attack occurring or minimize the impact of an infection.

RECOVERY PROCESS

- Having reliable backups that are secured and stored offline can significantly enhance your ability to recover from a ransomware attack.
- If your organization has been hit with ransomware, there are immediate steps you can take to minimize the impact of the infection.

YOUR PERSONAL FILES ARE ENCRYPTED
Make payment or private key will be destroyed in
12 Hours 01:34

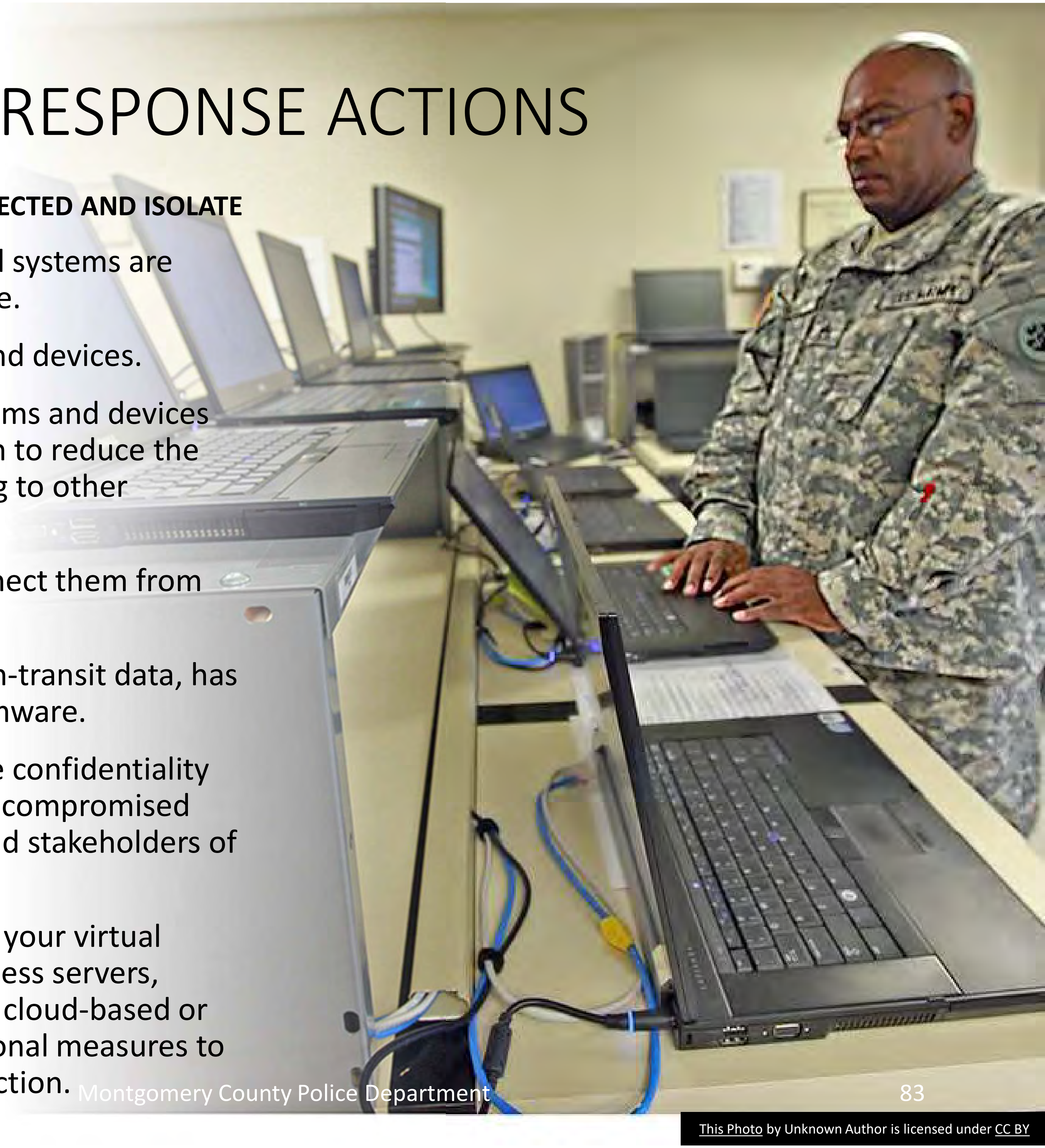
IMMEDIATE RESPONSE ACTIONS

- Threat actors can infiltrate your network and continue to have visibility into your systems, connected devices, and communications.
- Assume the threat actor has visibility into your organization.
- Therefore, implement an alternative communication method (e.g., external email accessed by a device not connected to your network) that is not accessible to them.
- This will also block the threat actor from gaining insight into your intended incident response plans and recovery actions.
- Next is a checklist to follow within the first few hours against a ransomware attack.

IMMEDIATE RESPONSE ACTIONS

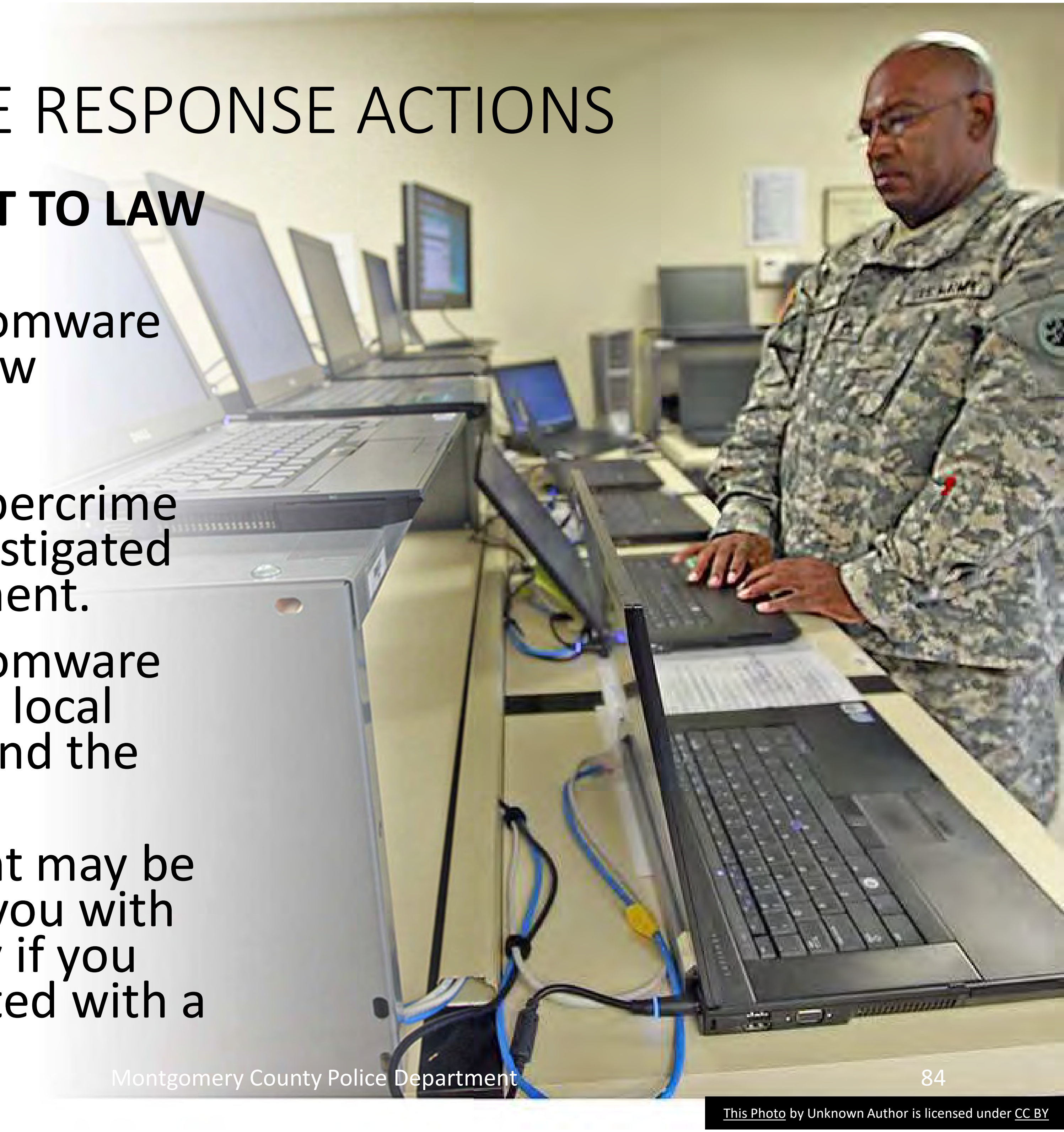
Priority 1. DETERMINE WHAT IS INFECTED AND ISOLATE

- Determine which devices and systems are infected with the ransomware.
- Isolate all infected systems and devices.
- Disconnect the infected systems and devices from any network connection to reduce the risk of the infection spreading to other connected devices.
- You may also need to disconnect them from the Internet.
- Determine what data, even in-transit data, has been impacted by the ransomware.
- Establish the likelihood of the confidentiality or integrity of the data being compromised and inform data managers and stakeholders of potential impacts.
- You may also need to disable your virtual private networks, remote access servers, single sign-on resources, and cloud-based or public-facing assets as additional measures to contain the ransomware infection.



This Photo by Unknown Author is licensed under CC BY

IMMEDIATE RESPONSE ACTIONS



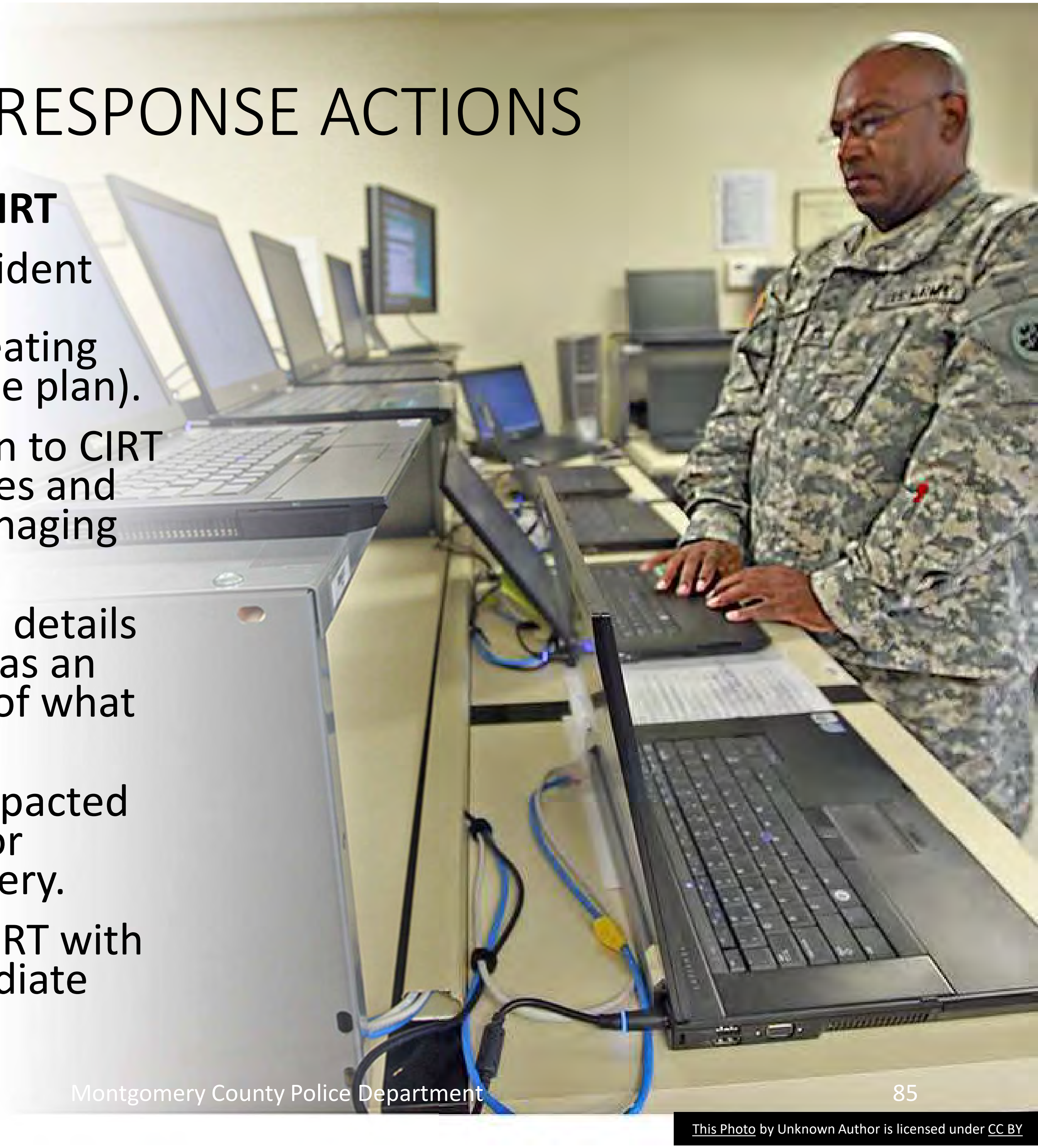
Priority 2. REPORT TO LAW ENFORCEMENT

- Report the ransomware attack to local law enforcement. Ransomware is considered a cybercrime and may be investigated by law enforcement.
- Report the ransomware attack to the FBI local office, the IC3, and the FTC.
- Law enforcement may be able to provide you with a decryption key if you have been infected with a known type of ransomware.

IMMEDIATE RESPONSE ACTIONS

Priority 3. ASSEMBLE CIRT

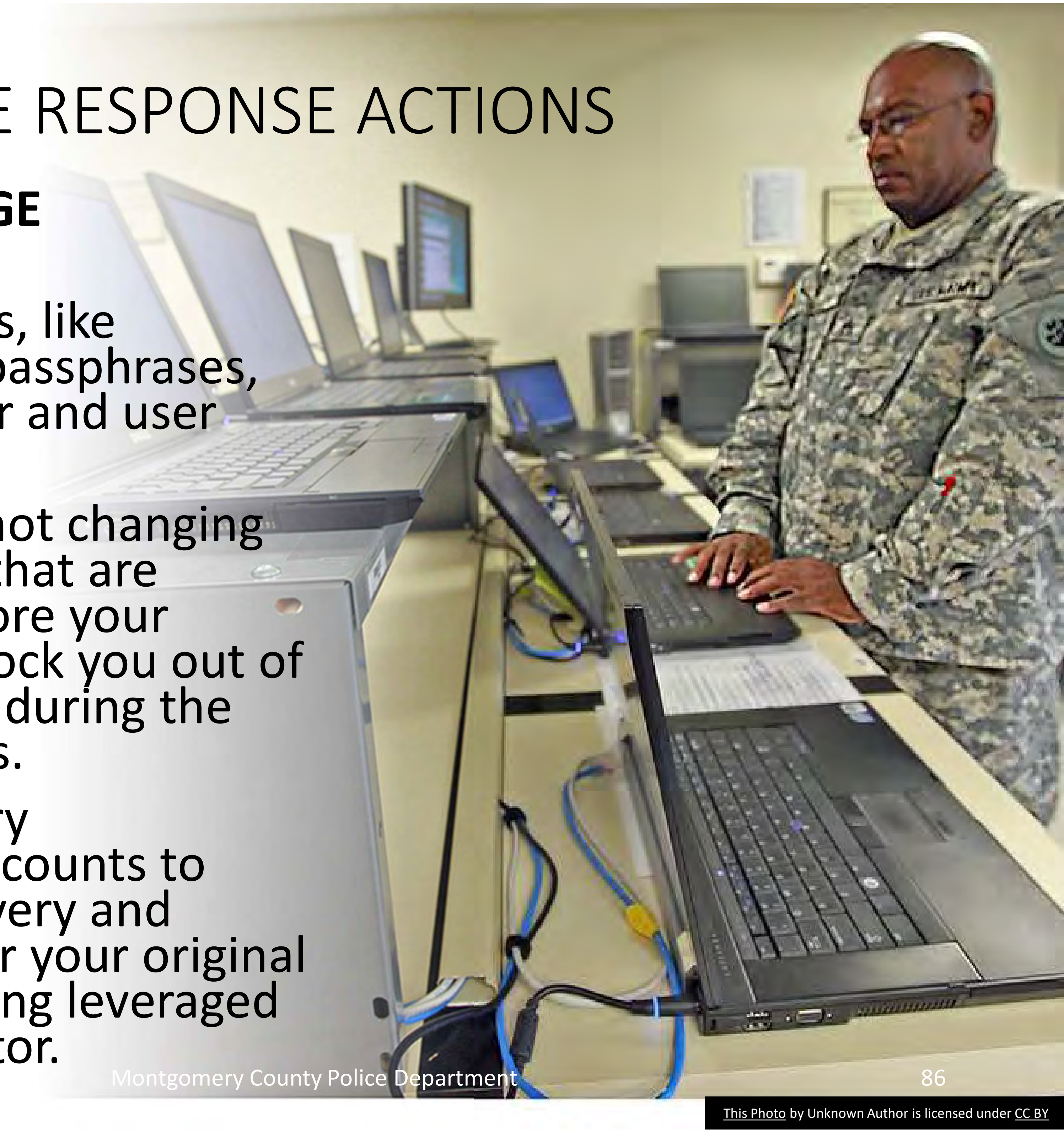
- Communicate the incident details to your CIRT (established while creating your incident response plan).
- Provide clear direction to CIRT members on their roles and responsibilities in managing the incident.
- Document the known details to ensure your CIRT has an initial understanding of what has occurred.
- Triage the systems impacted by the ransomware for restoration and recovery.
- This will assist your CIRT with where to focus immediate actions.



IMMEDIATE RESPONSE ACTIONS

Priority 4. CHANGE CREDENTIALS

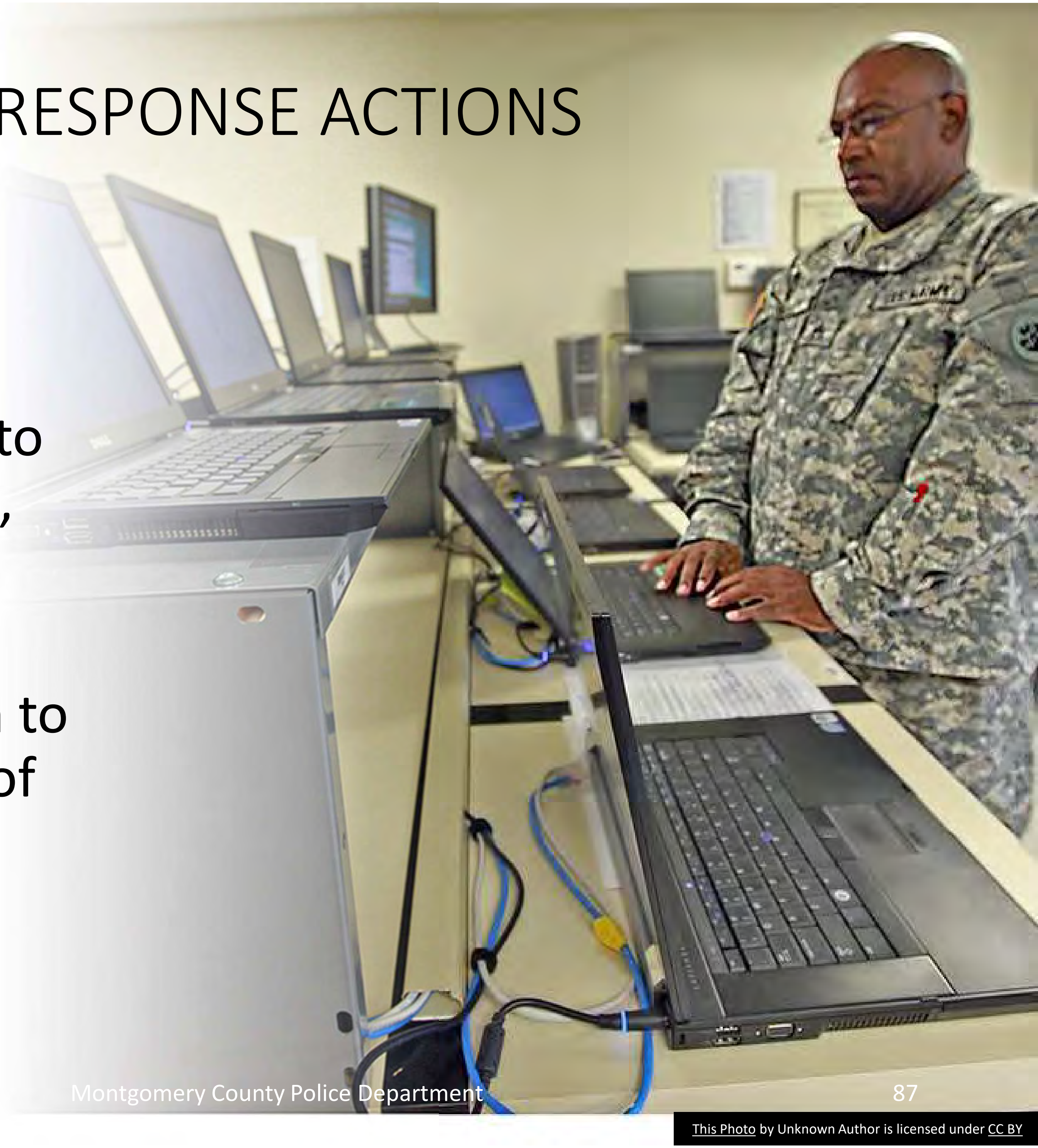
- Reset credentials, like passwords and passphrases, for administrator and user accounts.
- Ensure you are not changing any credentials that are required to restore your backup or may lock you out of systems needed during the recovery process.
- Create temporary administrator accounts to begin your recovery and monitor whether your original accounts are being leveraged by the threat actor.



IMMEDIATE RESPONSE ACTIONS

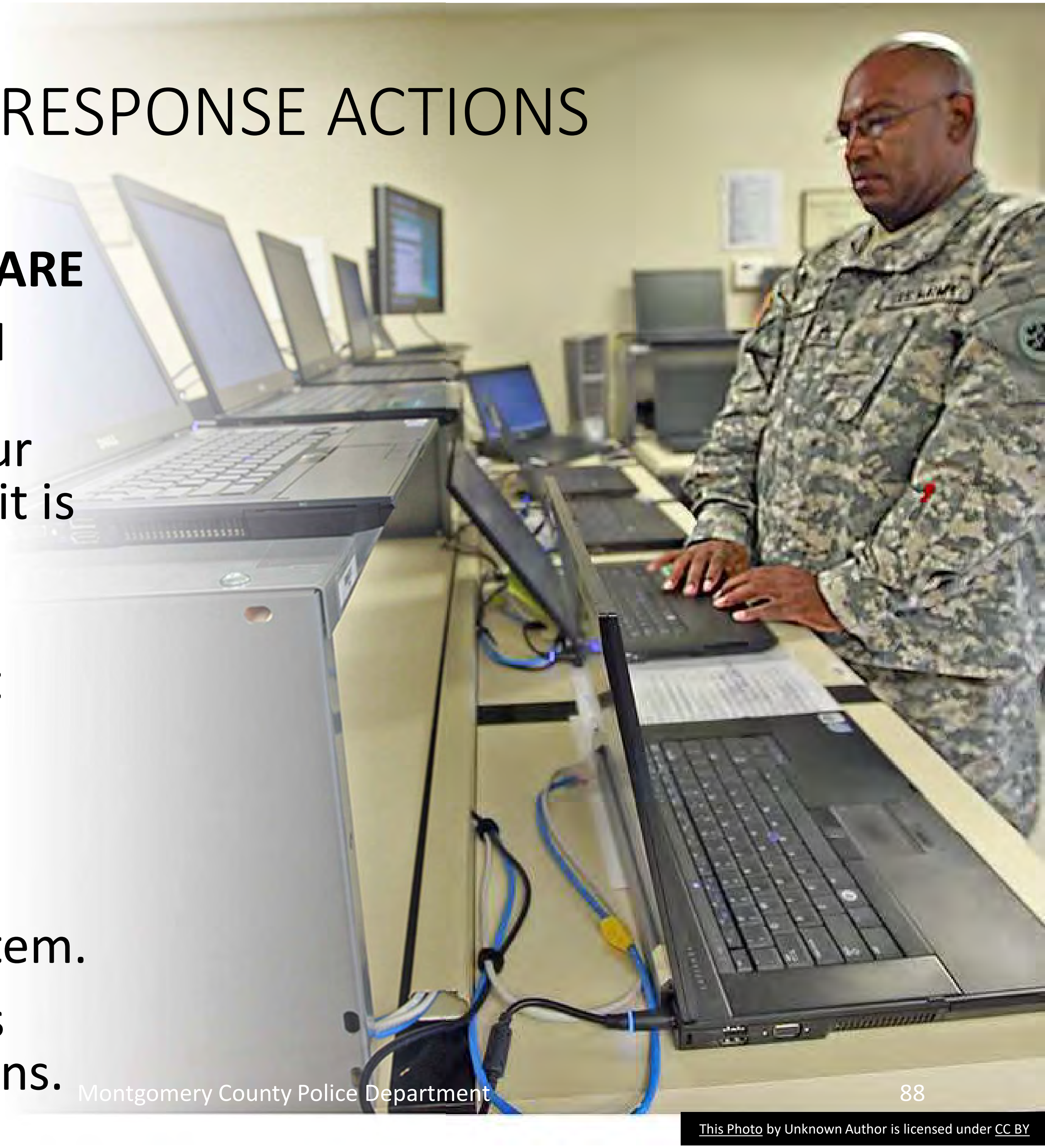
Priority 5. WIPE & REINSTALL

- Safely wipe your infected devices to remove malware, bugs, or viruses.
- Reinstall the operating system to rid your devices of the infection.



IMMEDIATE RESPONSE ACTIONS

- **Priority 6. RUN SECURITY SOFTWARE**
- Run anti-virus and anti-malware diagnostics on your backup to ensure it is clean before you begin restoring.
- Scan any files that might have been accessed by the threat actor or extracted from a compromised system.
- Address any items flagged by the scans.



This Photo by Unknown Author is licensed under CC BY

RECOVERY ACTIONS

- Despite temporary disruptions to your business, isolating your infrastructure from the Internet is the most important course of action.
- Isolation will temporarily remove the threat actor's access to your infrastructure, allowing you to gain control and further your incident investigation, response, and recovery.
- Once you have completed the preceding steps and you are positive that both your backups and your devices are clear of any malware or viruses, you should begin your recovery process.

REMEDIATE THE POINT OF ENTRY

- To recover successfully and avoid reinfection, you will need to identify how the threat actor was able to enter your network, systems, and devices and address the vulnerability immediately.
- Ensure you remediate the point of entry before connecting your systems or devices to your network or the Internet to thwart the threat actor's ability to gain access in the same manner.

This Photo by Unknown Author is licensed under CC BY-SA

This Photo by Unknown Author is licensed under CC BY-SA

IMPLEMENT YOUR BACKUP PLAN

- Ensure your organization is protected by having a detailed backup plan in place.
- You will execute this plan if your main systems and data storage are compromised and need to be restored with your copied information.
- The plan will ensure your organization can restore critical systems and data and get back to business quickly.
- You should recover your systems using offsite backups that are not connected to your networks.
- Before restoring from a backup, scan and analyze it to ensure it hasn’t been compromised by the threat actor.

RESTORE YOUR SYSTEMS

- Following your incident response plan, identify the critical systems and data that need to be recovered first.
- Ensure that the ransomware attack has not impacted these systems and data and that they do not have signs of any other malware infection.
- There are several options to consider when implementing your recovery strategy.
- Choose a recovery strategy that meets your business needs and security requirements.

ENGAGE CYBER SECURITY PROFESSIONAL ASSISTANCE

- Procuring professional services from a highly rated cyber security agency or professional can be a helpful asset when preparing for and responding to a ransomware incident.
- If your organization has a cyber insurance policy, your provider will often include the assistance of a third-party cyber security professional in the event of an incident like a ransomware attack.
- They will provide you with incident response expertise and a recovery strategy tailored to your organization. They may also deploy an incident handling team to lead your organization’s response and recovery process.
- If you do engage professional cyber security assistance, ensure you clearly identify the service expectations, roles, and responsibilities.

INFORM STAKEHOLDERS

- When an incident occurs, and especially when it compromises your systems and data, it is imperative that you inform key stakeholders, clients, and your staff members.
- You should consider preparing a statement in advance that can then be tailored to the incident, as well as a contact list of all stakeholders to be notified.
- Ransomware attacks can jeopardize your organization’s reputation, so your communications plan must be implemented swiftly following an incident to ensure your stakeholders are informed and able to enact their own incident response plans if necessary.

INFORM STAKEHOLDERS

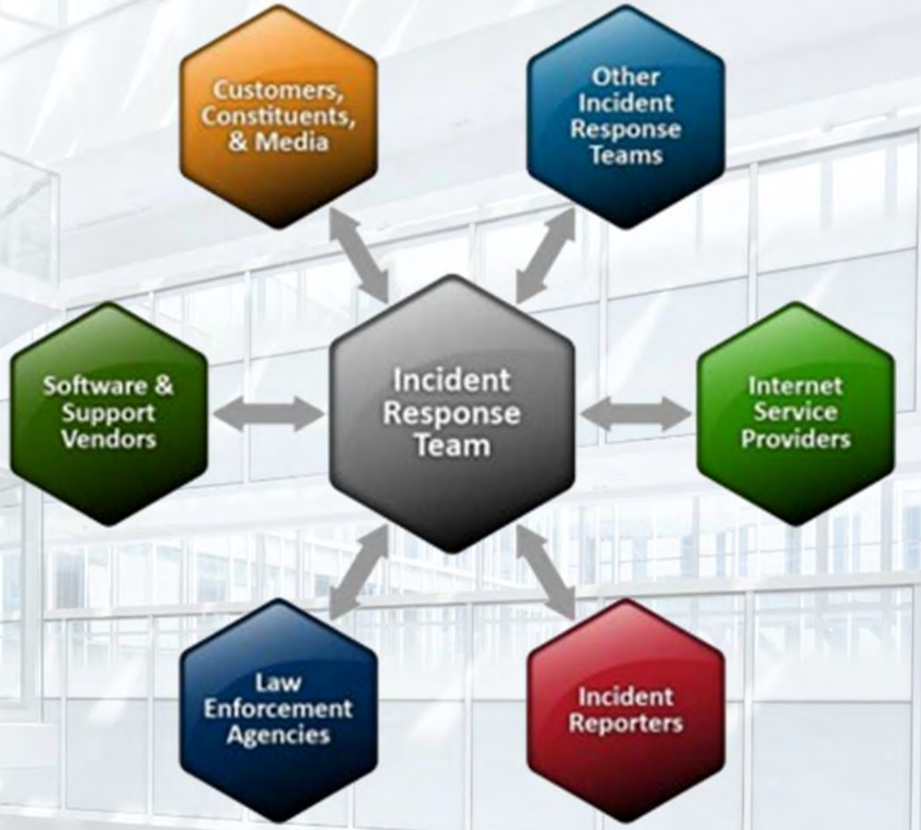

Customers, Constituents, & Media
Other Incident Response Teams
Software & Support Vendors
Incident Response Team
Internet Service Providers
Law Enforcement Agencies
Incident Reporters

Figure 2-1. Communications with Outside Parties

ANALYZE THE INCIDENT

- Determining the root cause of the incident is key.
- How did the threat actor access your network and deploy the ransomware? Often, the ransomware incident is a symptom of a more serious hack or intrusion by the threat actor.
- Without identifying how they gained access and applying appropriate security measures to prevent it from happening again, threat actors may continue to exploit the vulnerability.
- Determining what systems, accounts, and information have been accessed by the threat actor is a vital step in your incident analysis.
- This will enable you to determine the extent of the damage, such as what accounts were compromised and what data was exfiltrated, which will inform your approach to control the attack, prepare, and implement a proper response, and execute a successful recovery.

LEARN LESSONS AND REVISE PLAN

- If your organization has fallen victim to ransomware, conducting a lessons-learned exercise post-recovery is an excellent method to implement further mitigation measures and correct actions and strategies that did not go as planned.
- Revise your incident response plan based on these lessons learned to ensure your organization has the most robust response and recovery plans possible.
- Report cyber incidents to law enforcement.

LEARN LESSONS AND REVISE PLAN

- If you are comfortable doing so, share your findings, including the tools, techniques, and procedures used by the threat actor, with CISA, FBI, USSS, and the relevant ISAC.
- This will enable them to provide alerts and guidance to the public to help individuals and organizations protect their assets from the same ransomware attack.
- Sharing your lessons can benefit other organizations and the cybersecurity community.

SUMMARY

- Ransomware is an ever-present threat to your organization.
- It can devastate your business, often halting your ability to produce products and services.
- Ransomware incidents can also cause you to incur financial loss, data breaches, and reputational damage to your organization.
- Preparing your organization and applying proactive measures to protect your network, connected devices, and information is critical for your ability to respond to and recover from ransomware.

Questions

CONTACT INFORMATION

- File a police report. Report cybercrime to MCPD at 301-279-8000.
- Call your insurance company to claim the loss.
- Call the Baltimore FBI office at (410) 265-8080.
- Or call 1-800-CALLFBI (225-5324) for the Major Case Contact Center.

References

- Canadian Centre for Cybersecurity (2021). Ransomware playbook (ITSM.00.099). Retrieved from https://www.cyber.gc.ca/sites/default/files/cyber/2021-12/itsm00099-ransomware-playbook-2021-final3-en.pdf
- Cybersecurity & Infrastructure Security Agency (CISA), “Ransomware Guidance and Resources,” https://www.cisa.gov/ransomware
- Institute for Security and Technology, “A Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force,”
- National Institute of Standards and Technology (NIST), “Cybersecurity Framework,” https://www.nist.gov/cyberframework
- PALO ALTO NETWORKS: UNIT 42, 2021 RANSOMWARE THREAT REPORT 5 (2021).
- RANSOMWARE Federal Agencies Provide Useful Assistance but Can Improve Collaboration, United States Government Accountability Office, gao-22-104767, September 2022.
- US Senate Report - Case Studies in Ransomware