TETRA TECH

Surviving SCADA Ransomware Attacks

Preparing for and Recovering from Sophisticated Cyber Attacks

David Espy
- CISSP

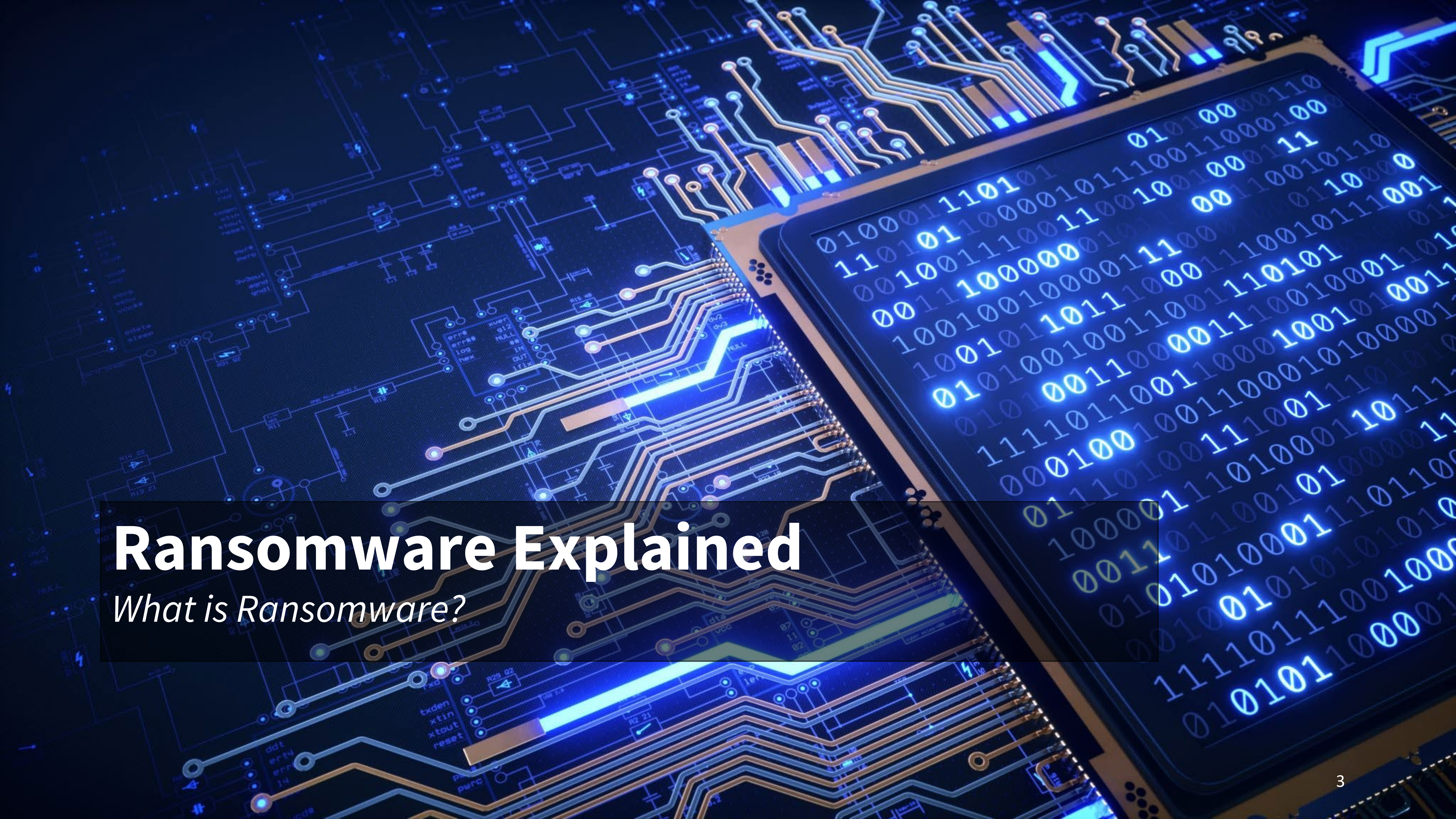
NATIONAL OPERATIONAL TECHNOLOGY PRACTICE LEADER

PNWS-AWWA
Water 2022
Tacoma, WA • April 27-29

American Water Works Association
Pacific Northwest Section

Knowledge Goals

- Understand what ransomware is
- Understand how & who of ransomware
- Understand how to prepare/prevent ransomware
- Understand how to react to a ransomware incident



Ransomware Explained

What is Ransomware?

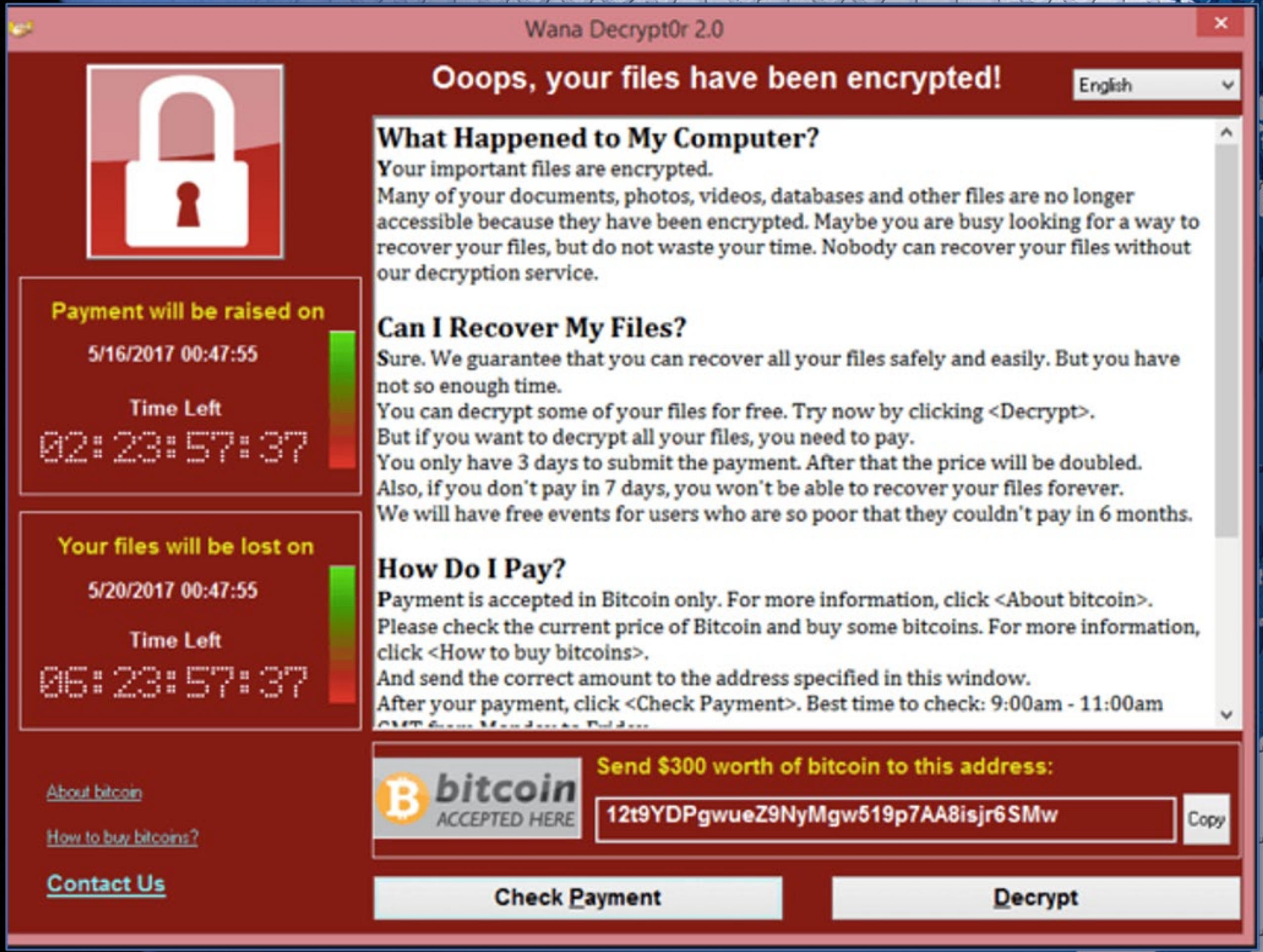
What is a Ransom?

The release of property (Data) in return for payment of a demanded price.

What is Ransomware?

Ransomware is a class of malware

- Encrypts accessible files.
- May target specific file types or all files
- Demands payment for the encryption key.
- May have a mechanism to exfiltrate 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.

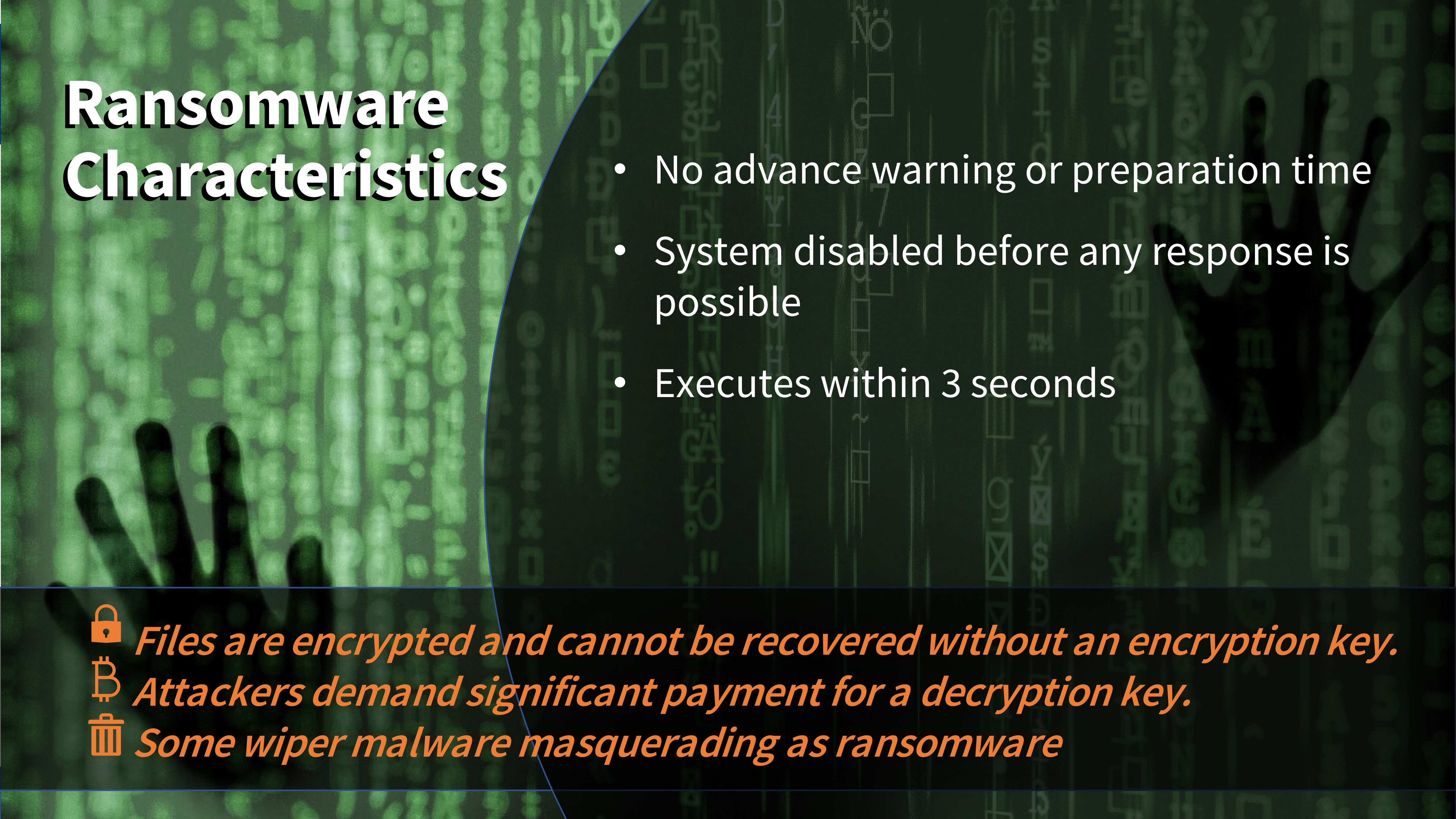
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the 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



Ransomware Characteristics

- No advance warning or preparation time
- System disabled before any response is possible
- Executes within 3 seconds

🔒 *Files are encrypted and cannot be recovered without an encryption key.*

₿ *Attackers demand significant payment for a decryption key.*

🗑 *Some wiper malware masquerading as ransomware*

Ransomware Facts

- The Cybersecurity and Infrastructure Security Agency *reported in February 2022* that it is aware of ransomware incidents against 14 of the 16 U.S. critical infrastructure sectors.
- There are more than 130 different ransomware strains
- The rate of cybercrime *increased by 600%* during the COVID-19 pandemic.
- In the first half of 2021, **33.8% of industrial control systems** (ICS) **were attacked**, indicating a 0.4% increase from the second half of 2020.

Ransomware Facts

- Most threat actors are using double extortion (encrypt and export for leaking or selling information)
- Does not need to be a direct attack to affect your organization
  - *The Kaseya attack, affected at least 1,500 of its managed service provider customers.*
  - *Colonial Pipeline affected gas prices and perceived availability of supply.*
- Ransomware will come for you no matter how big you are
- RaaS is a reality, no longer just well funded criminal groups
- Most ransomware exploits known vulnerabilities instead of 0-days
- Phishing is the most common method of launching Ransomware attacks (90%)

ICS are Specific Targets

- APTs have become more sophisticated and more selective.
- Criminals are fully aware of the importance of SCADA/ICS.
- New-gen APTs specifically target SCADA/ICS applications, industrial networks, and control system equipment.

Why is Ransomware so Effective?

Poor Cyber Hygiene

Hardware & software with unpatched vulnerabilities

Legacy software or hardware (Long SCADA/ICS lifecycles)

Poor backup practices

Improperly configured firewalls

Unfettered network access (lack of segmentation & access control)

Why is Ransomware so Effective?

Inadequate risk management/ cybersecurity program

Poor business continuity planning

Poor disaster recovery planning

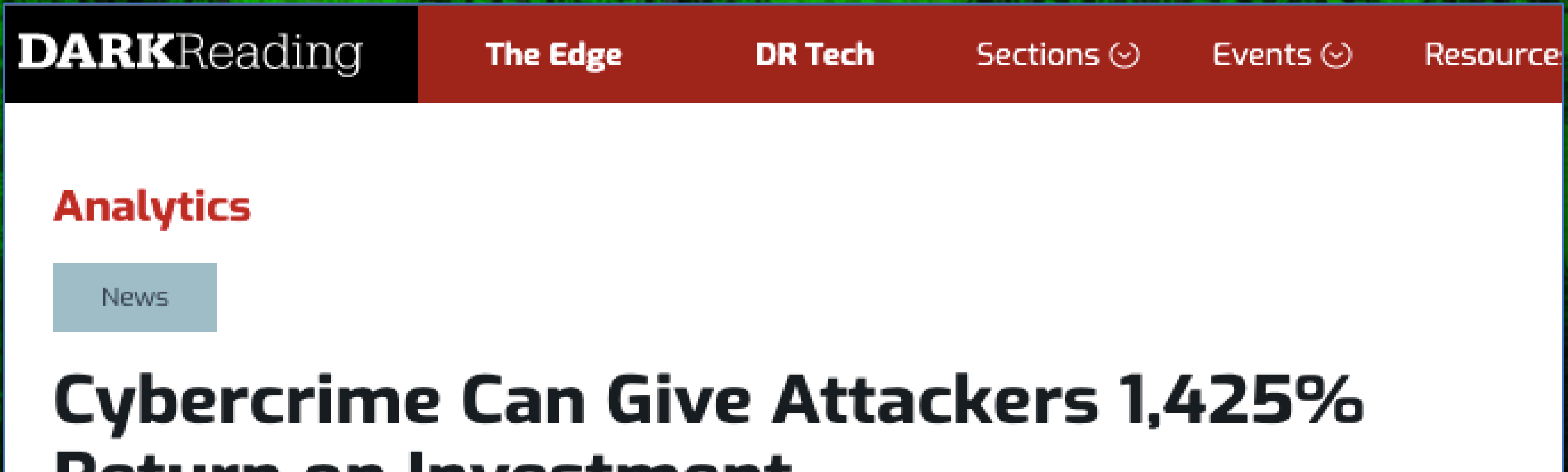
Lack of policies and procedures

Lack of security awareness training

People (the biggest security risk)

Why is Ransomware so Prolific?

- *It pays well*
- *It is easy (for hackers; RaaS)*
- *People are easy targets for deception*
- *Digital currency took out money exchange complication*



Analytics

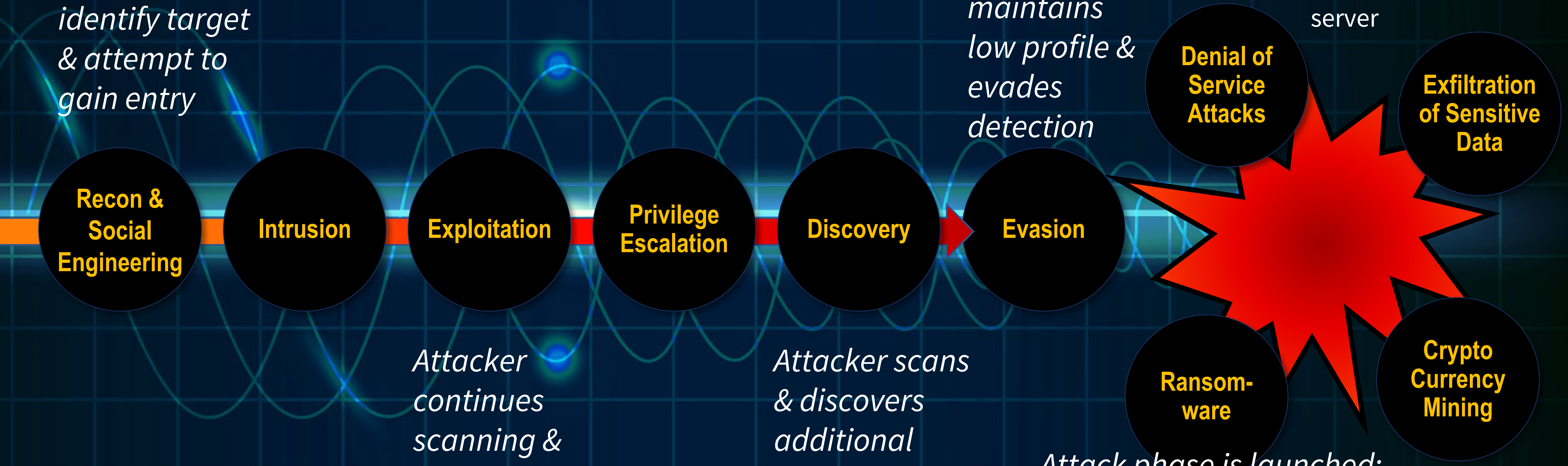
Cybercrime Can Give Attackers 1,425% Return on Investment

Ransomware Attack Kill Chain

Attack Sequence

The Cyber Kill Chain

Attackers identify target & attempt to gain entry



Recon & Social Engineering

Intrusion

Exploitation

Privilege Escalation

Discovery

Evasion

Denial of Service Attacks

Exfiltration of Sensitive Data

Ransom-ware

Crypto Currency Mining

Attacker continues scanning & exploitation activities

Attacker scans & discovers additional internal systems

Attacker maintains low profile & evades detection

Attacker exploits vulnerabilities & plants additional tools:

- Time bombs
- Dead man's switch
- Exfiltration & analysis
- Phone home to command & control server

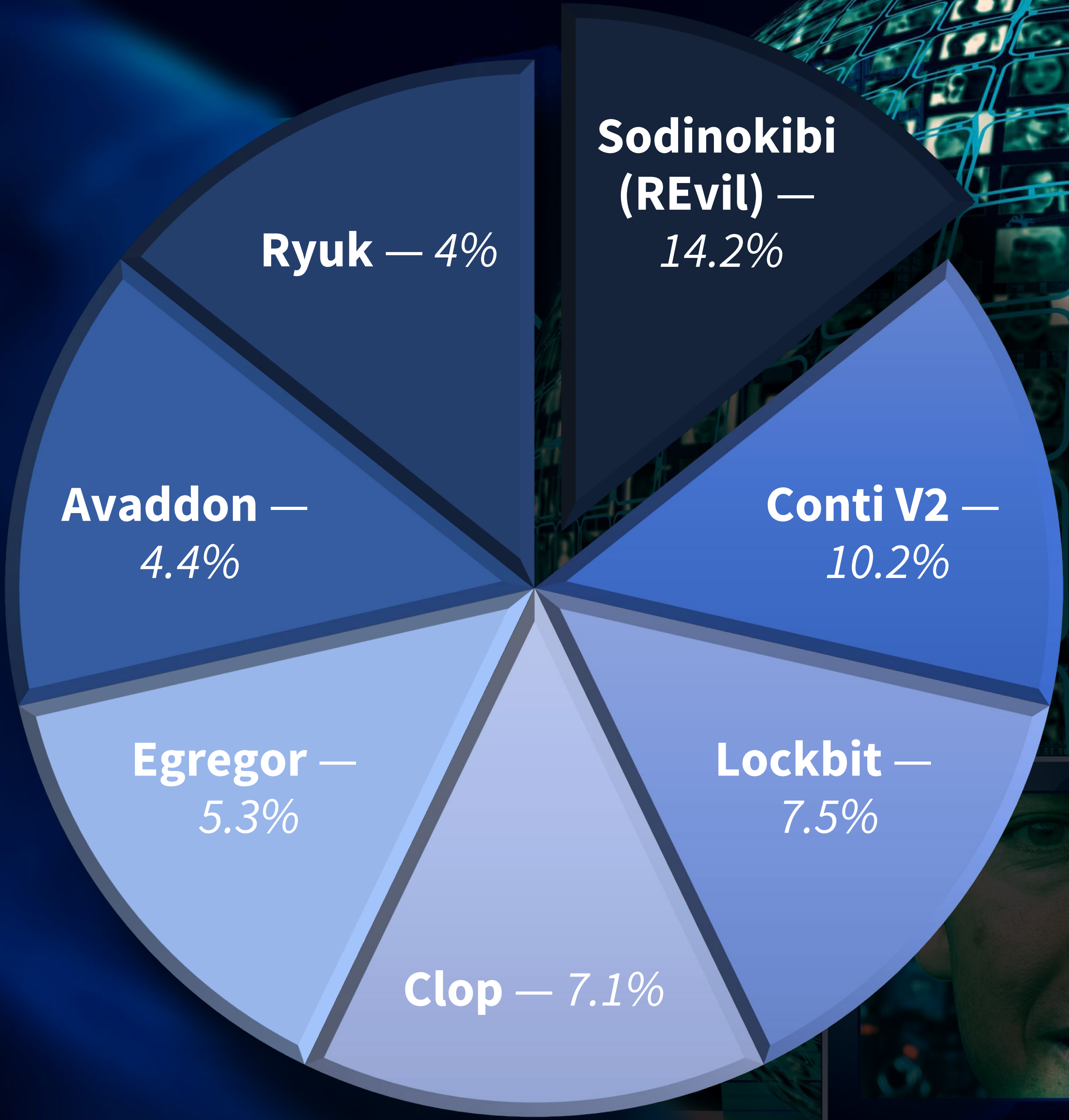
Attack phase is launched:

- Upon detection
- At moment of the attacker's choosing

Who are the Ransomware Perpetrators?

Criminal Hacking Groups

Ransomware by Criminal Groups



Preparation & Prevention Strategies

Assumed Breach Philosophy

FBI's List of Suggestions

- *Keep operating systems, software, & applications current & up to date.*
- *Make sure anti-virus & anti-malware solutions are set to automatically update & run regular scans.*
- *Back up data regularly & double-check that those backups were completed.*
- *Secure your backups. Make sure they are not connected to the computers & networks they are backing up.*
- *Create a continuity plan in case your business or organization is the victim of a ransomware attack.*

CISA’s Recommendations on Recovery

- Practice good cyber hygiene
  - *Backup*
  - *Update*
  - *Allow list apps*
  - *Limit privilege*
  - *Use multifactor authentication*
- Segment your networks
- Develop containment strategies
- Know your system’s baseline for recovery (is it back to normal?)
- Review disaster recovery procedures and validate goals with executives

Top 5 Preventative Steps

Perform System Maintenance

1. Patch firmware and software

- Most attackers exploit well known vulnerabilities
- It does take more planning to patch the ICS
- Utilize a patch management solution
- Know your vulnerabilities and what updates are available
- Use a change control process for patching

Top 5 Preventative Steps

Deploy & Update AV/Malware Protection

2.

Use AV Protection

- *Recommend Next Gen XDR/EDR Solution*
- *Most ICS AV is not maintained or monitored*
- *Update through DMZ/Proxy*
- *In ICS, use different product from Enterprise IT*

Top 5 Preventative Steps

Backup, Test Backups, Secure Backups

3.

Secure Backups

- *3-2-1-1 Methodology*
- *Test, Test, Test your backups*
- *Offsite/Offline is imperative*
- *Immutable (can't be changed) backups are ok for offsite*

Top 5 Preventative Steps

Secure Your Greatest Weakness - People

4.

Cyber Security Awareness Training

If Cybersecurity awareness training is just a check box, no one will benefit.

Search for awareness training products that engage and build a positive view of the training.

Training should shift staff mindset to care about securing the organization.

It should encourage staff to be part of the solution. To do that they must understand.

AWWA uses Curricula

Top 5 Preventative Steps

Figure Out What Systems You Can Live Without

5.

A Day Without SCADA

- *Tabletop exercises*
- *Actual manual control, can you really do it?*
- *Do not engineer or design out manual control*
- *Train staff on manual control*

Other Preventative Steps

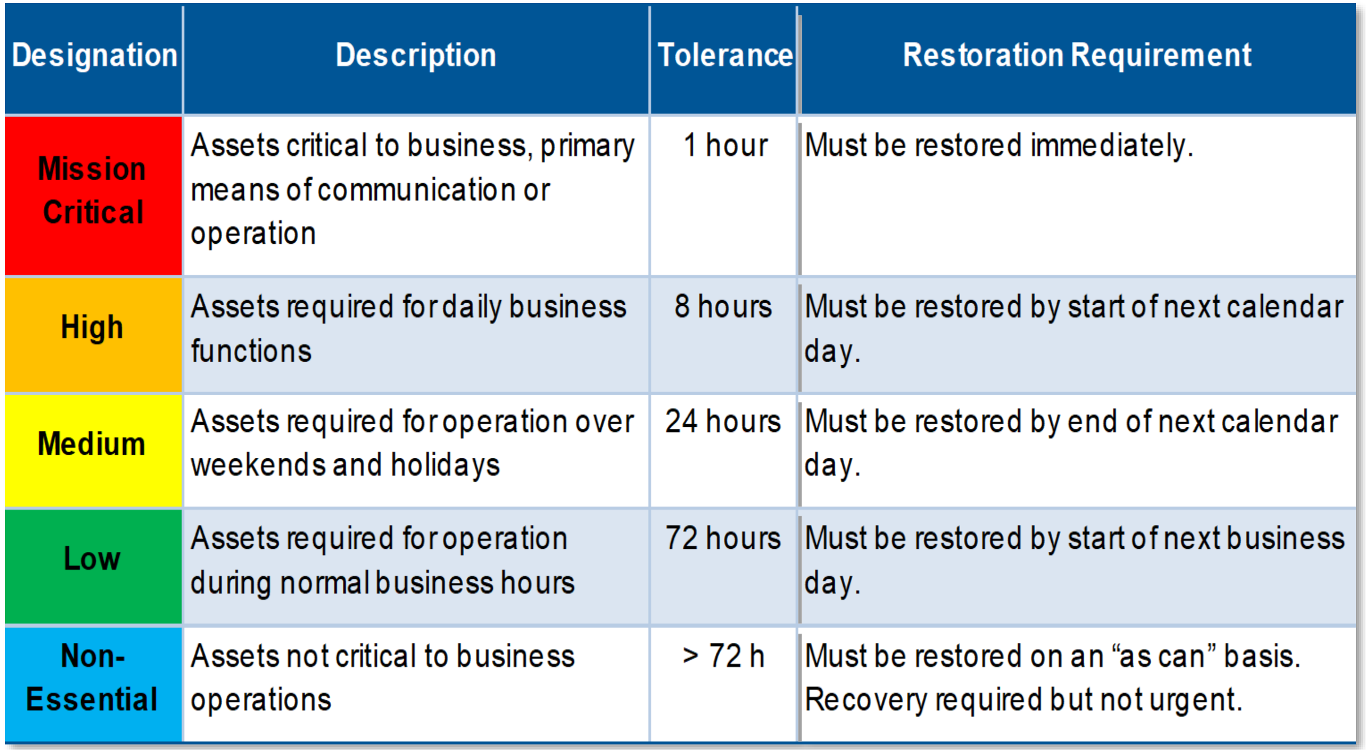
- Use Multi-Factor Authentication
- Employ a Zero-Trust Strategy
- Follow established standards
- Cybersecurity Policies and Procedures – Human Factor
- Business Continuity Plan
- Incident Response Plan
- Disaster Recovery Plan

Other Preventative Steps

- Know FBI Contact
- Know how to contact CISA
- Know your cyber insurance policy well
- Alternative billing and collection options
- Regular Vulnerability Assessments
- Use a Privileged Access Management Solution

Some cyber problems do not require a cyber solution

Other Preventative Steps – Asset Criticality Ratings



Designation	Description	Tolerance	Restoration Requirement
Mission Critical	Assets critical to business, primary means of communication or operation	1 hour	Must be restored immediately.
High	Assets required for daily business functions	8 hours	Must be restored by start of next calendar day.
Medium	Assets required for operation over weekends and holidays	24 hours	Must be restored by end of next calendar day.
Low	Assets required for operation during normal business hours	72 hours	Must be restored by start of next business day.
Non-Essential	Assets not critical to business operations	> 72 h	Must be restored on an “as can” basis. Recovery required but not urgent.

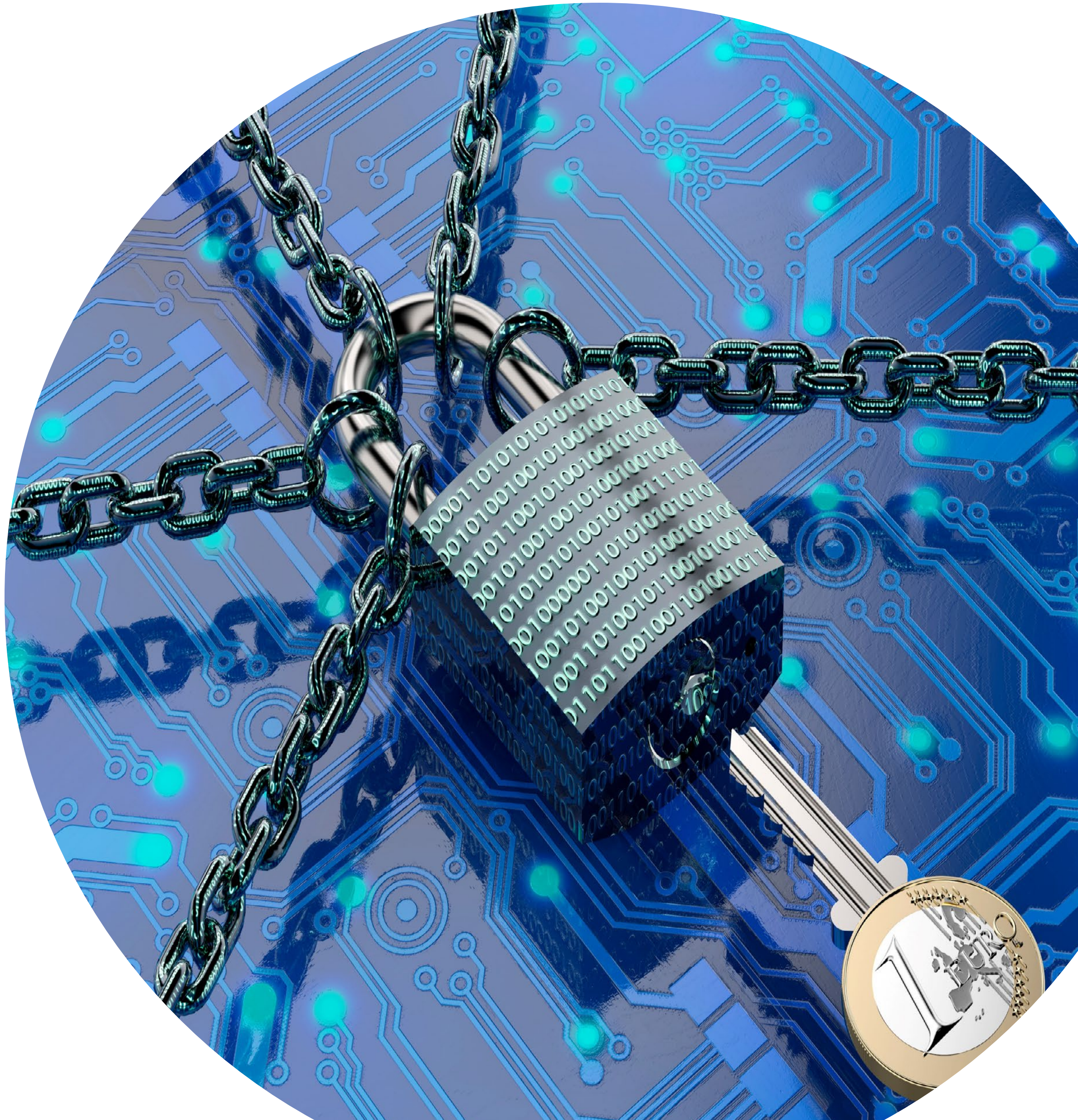
- Start with an asset inventory
- Identify the time window in which each critical asset must be restored
- Identify the criticality of each asset
- *Then* determine how to protect it appropriately.

Without knowing what’s critical, effective planning is impossible.

Notes from a Victim of Ransomware

Things to do in advance

- Decide: will you negotiate with hackers?
- Business continuity plan (plan to be down for 2 weeks)
- Have password reset plan
- Have communications plan
- Have clean laptops on standby
- Identify and secure sensitive data
- Assume hackers can access your network
- Continually test your backups
- Classify data and beware of what you share publicly



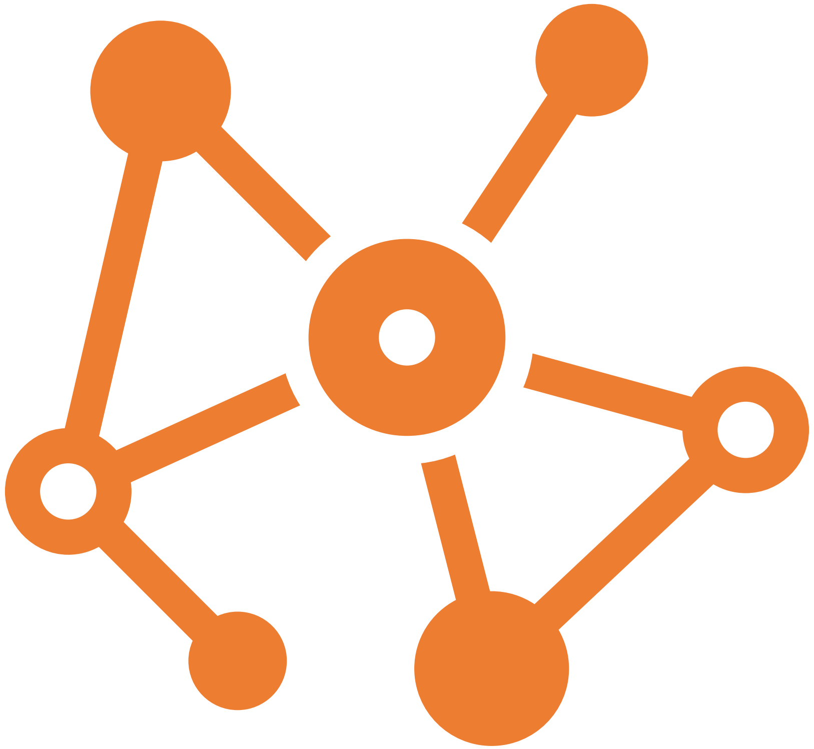
Notes from a Victim of Ransomware

Cybersecurity Preventative steps

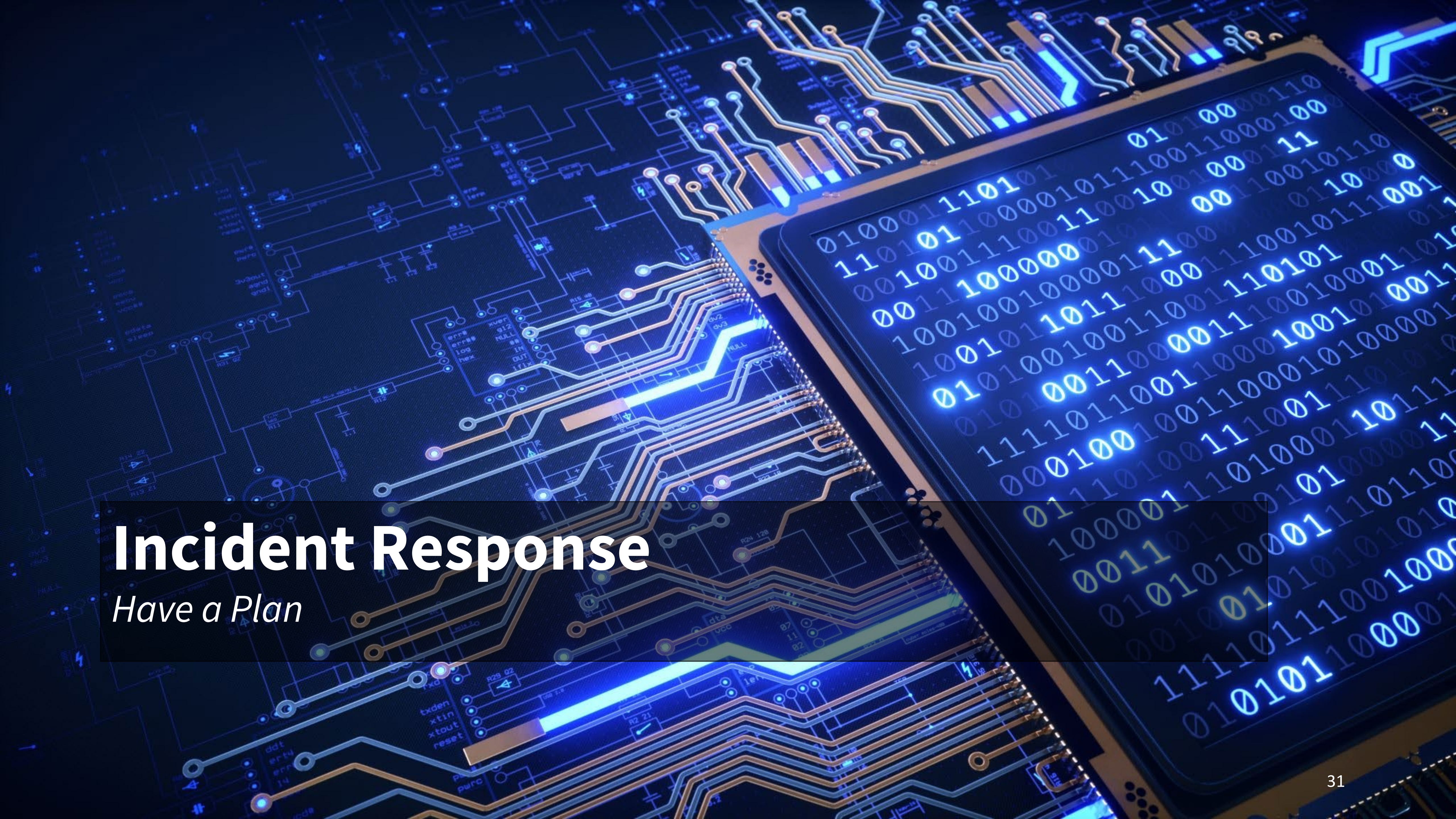
- Use MFA for any access outside the network
- Increase segmentation (more VLANs)
- CIS benchmark level 2 for desktops and servers
- Use secure/privileged remote access solution
- Implement a zero-trust strategy (assume your compromised)
- MS privilege access enterprise model
- Increase cybersecurity/phishing awareness training – use results to target more training
- Disable macros across network

ICS & Business Networks do not Belong Together

“DOE, CISA, NSA and the FBI recommend all organizations with ICS/SCADA devices … isolate ICS/SCADA systems and networks from corporate and internet networks using strong perimeter controls, and limit any communications entering or leaving ICS/SCADA perimeters,” they wrote.



All ICS security frameworks and standards agree



Incident Response

Have a Plan

CISA’s Recommendations on Recovery

- Ask for help! Contact CISA, the FBI, or the Secret Service
- Work with an experienced advisor to help recover from a cyber attack
- Isolate the infected systems and phase your return to operations
- Review the connections of any business relationships (customers, partners, vendors) that touch your network
- Apply business impact assessment findings to prioritize recovery

FBI's 100 Day Water Sector Action Plan Focus

Visibility:

- *ICS-specific Networking Tools*

Detection:

- *System Baseline*
- *Anomanly Detection*

Response:

- *Alarms/Alerts*
- *Incident Response*

Notification:

- *Know Your FBI Contact*
- *ERP Runbooks*

Notes from a Victim of Ransomware

Lessons Learned

- Reach out for help
- Don't identify the employee who downloaded the virus
- Pull the network cable, not the power
- Contact insurance early on
- End Users are the weakest link - amateurs hack systems/pros hack people
- Replace legacy systems with COTS (easy to replace)
- Use standard security policies and do not allow exceptions

Ransomware Incident Response

1. **Contain**
   - Isolate systems
   - Follow Incident Response Plan
2. **Triage**
   - Determine what was impacted
3. **Consult**
   - With resources
4. **Inform**
   - Stakeholders

Containment

Determine which systems were impacted, & immediately isolate them

1. Follow incident response plan
2. To contain the outbreak, pull network cables, not power; or take the network offline at the switch level.
   - *It may not be feasible to disconnect individual systems during an incident.*
3. Disable WiFi
4. Use out-of-band communication methods
   - *Use phone calls, text, IM, or other means to avoid tipping off actors that they have been discovered and that mitigation actions are underway*

EDR/XDR products can save your bacon!

CISA - Containment and Eradication

Take a system image and memory capture of affected devices (e.g., workstations and servers).

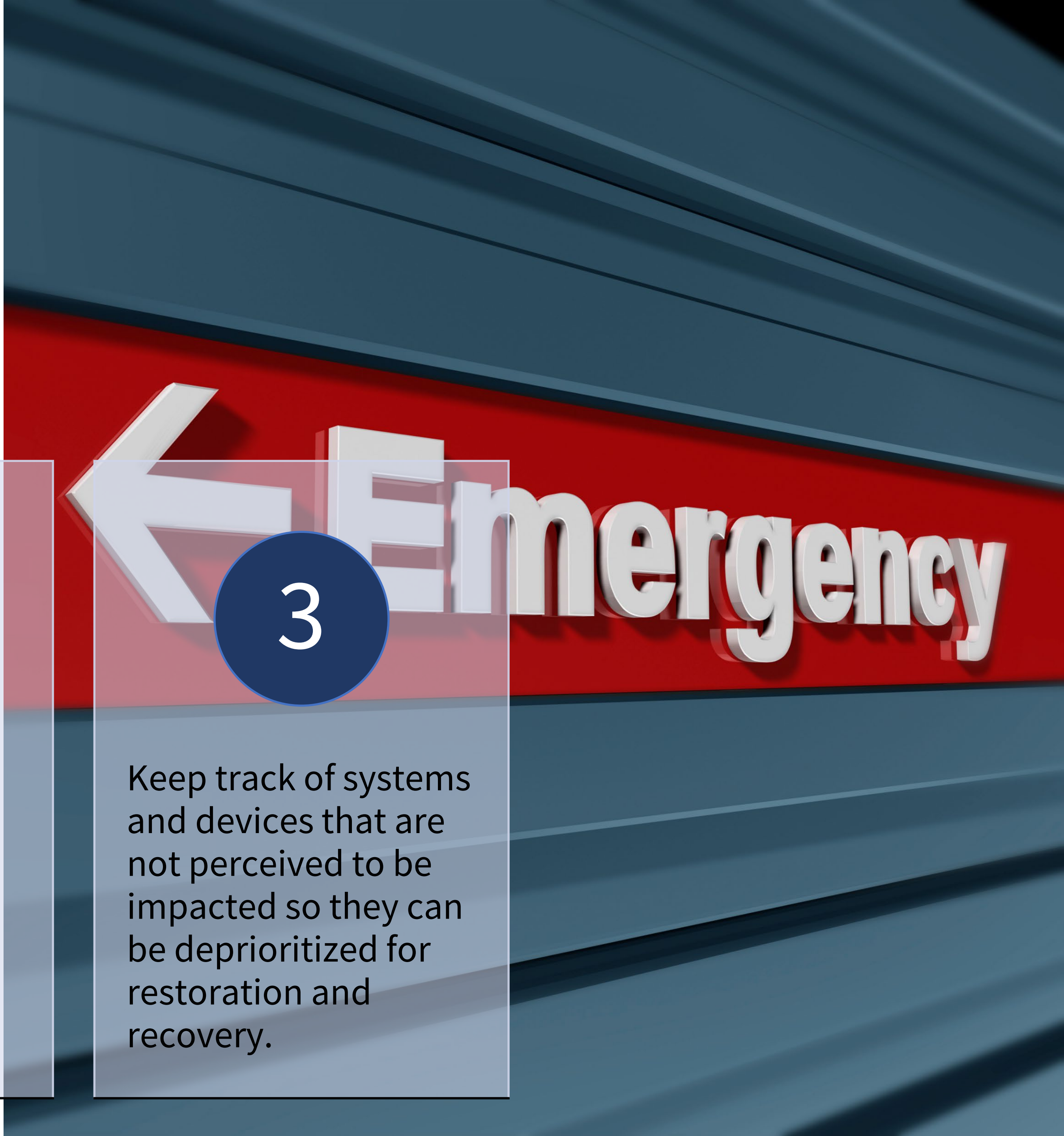
Additionally, collect any relevant Information

- Forensic data collection
- Preserve evidence

Consult federal law enforcement regarding possible decryptors available

Triage

Triage impacted systems for restoration and recovery.



1

Identify and prioritize critical systems for restoration

2

Prioritize restoration and recovery based on a predefined critical asset list

3

Keep track of systems and devices that are not perceived to be impacted so they can be deprioritized for restoration and recovery.

Consult

Consult

Consult with your incident response team

- Develop and document an initial understanding
- Define what has occurred based on the initial analysis.

Engage

Engage your internal & external teams & stakeholders

- Understand what they can provide to help you: mitigate, respond, and recover

Inform

Share the information you have at your disposal

- Share with consultants to receive the most timely and relevant assistance
- Keep management and senior leaders informed via regular updates
- Inform relevant stakeholders:
  - *Elected leaders*
  - *Departmental leaders*
  - *IT department*
  - *Managed security service providers*
  - *Cyber insurance company*
  - *Shareholders, investors, suppliers*

Questions?