Ransomware Preparedness and Response

Rehmann

EMPOWER YOUR PURPOSE

Presenter

Jessica Dore

Principal, Technology Solutions, CISA

989.797.8391 | Jessica.dore@rehmann.com

As a leader in Rehmann's Technology Solutions Group, Jessica oversees cybersecurity assessments, information security assessments, vulnerability and penetration testing, social engineering testing, and information security training. She provides information technology (IT) consulting and security services to a wide range of clients.

Our Agenda for Today

- Cybersecurity Update
- Ongoing Security Threats
- Building and Improving Your Response Plan
- Question and Answer

CYBERSECURITY UPDATE

What is Ransomware

A type of malicious software designed to block access to a computer system until a sum of money is paid.

These attacks can last days to months.

Ransomware can spread by phishing emails through downloading attachments and links.

The Rise of Ransomware

1 68% of breaches involved a human element

2 32% of breaches involved Ransomware or Extortion

3 $265 Billion dollars predicted global ransomware cost to victims annually by 2031

4 70% of IT leaders have witnessed a ransomware attack.

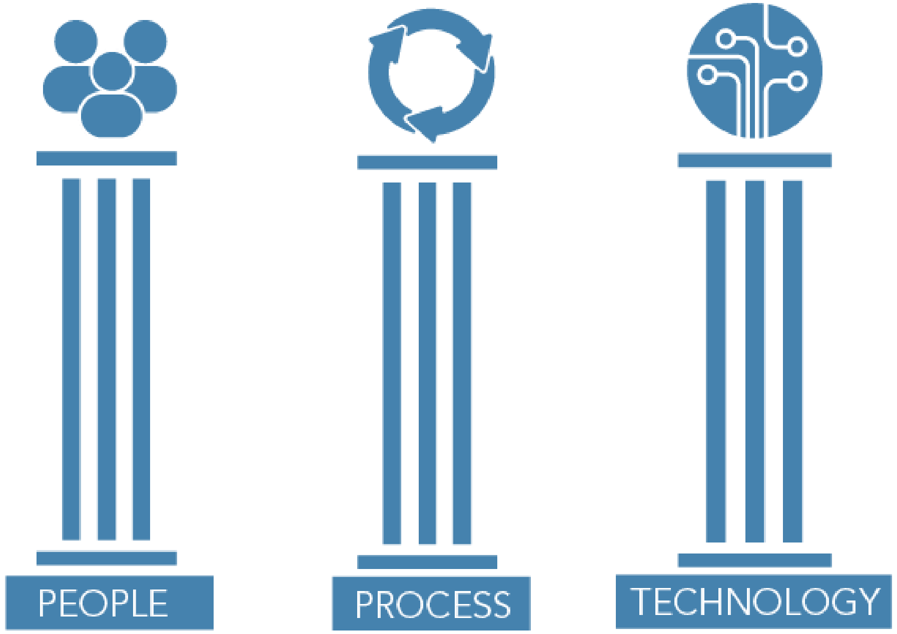
Sources: WatchGuard
2024 Verizon Data Breach Investigation Report

Cybersecurity Trends

- Continued increase in sophisticated phishing attacks
- Using cybercriminal services-for-hire
- Sharing victim information
- Diversifying approaches to extorting money
- Targeting the Cloud
- Targeting Managed Service Providers
- Targeting on Holidays and Weekends

Who’s Responsible for Cybersecurity?

Cybersecurity is an organization wide issue, not just an IT issue!



Cybersecurity Concentrates On How To Protect:

Confidentiality

Protecting information from unauthorized access and disclosure.

For example, what would happen to your organization if employee or information such as usernames, passwords, or sensitive information was stolen?

Integrity

Protecting information from unauthorized modification.

For example, what if payroll information or sensitive records had unauthorized changes?

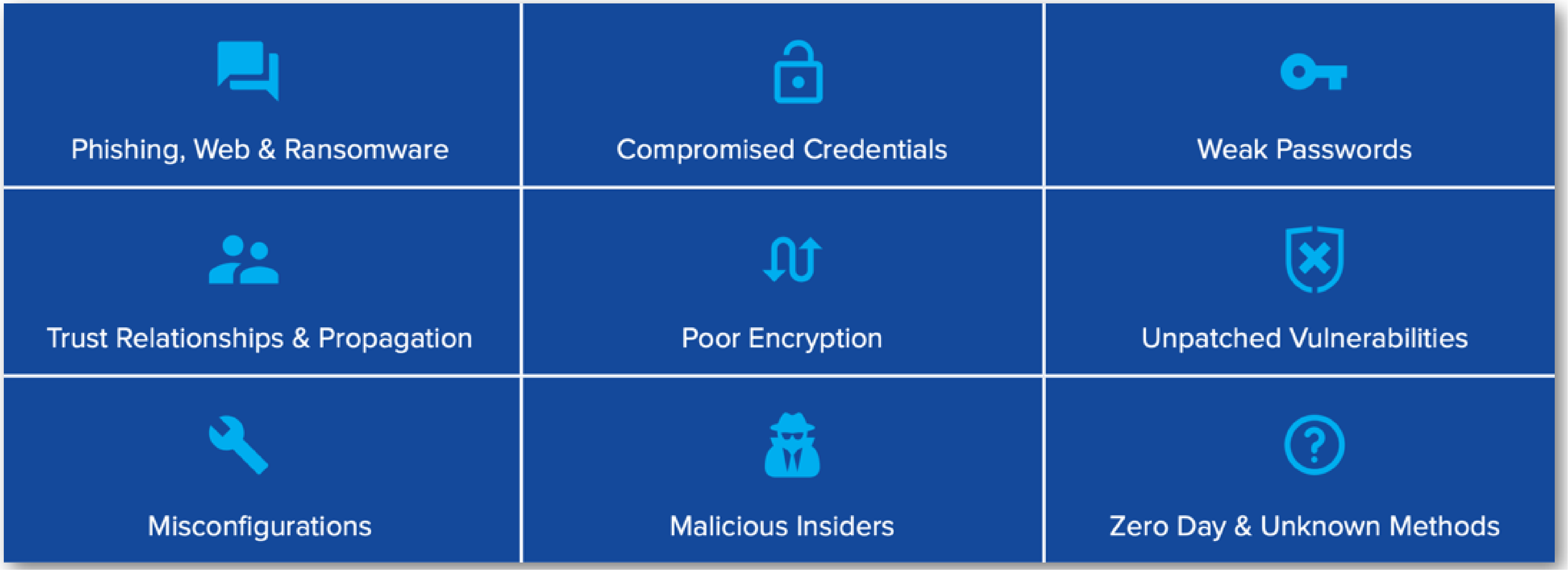
Availability

Protecting disruption in how you access your information.

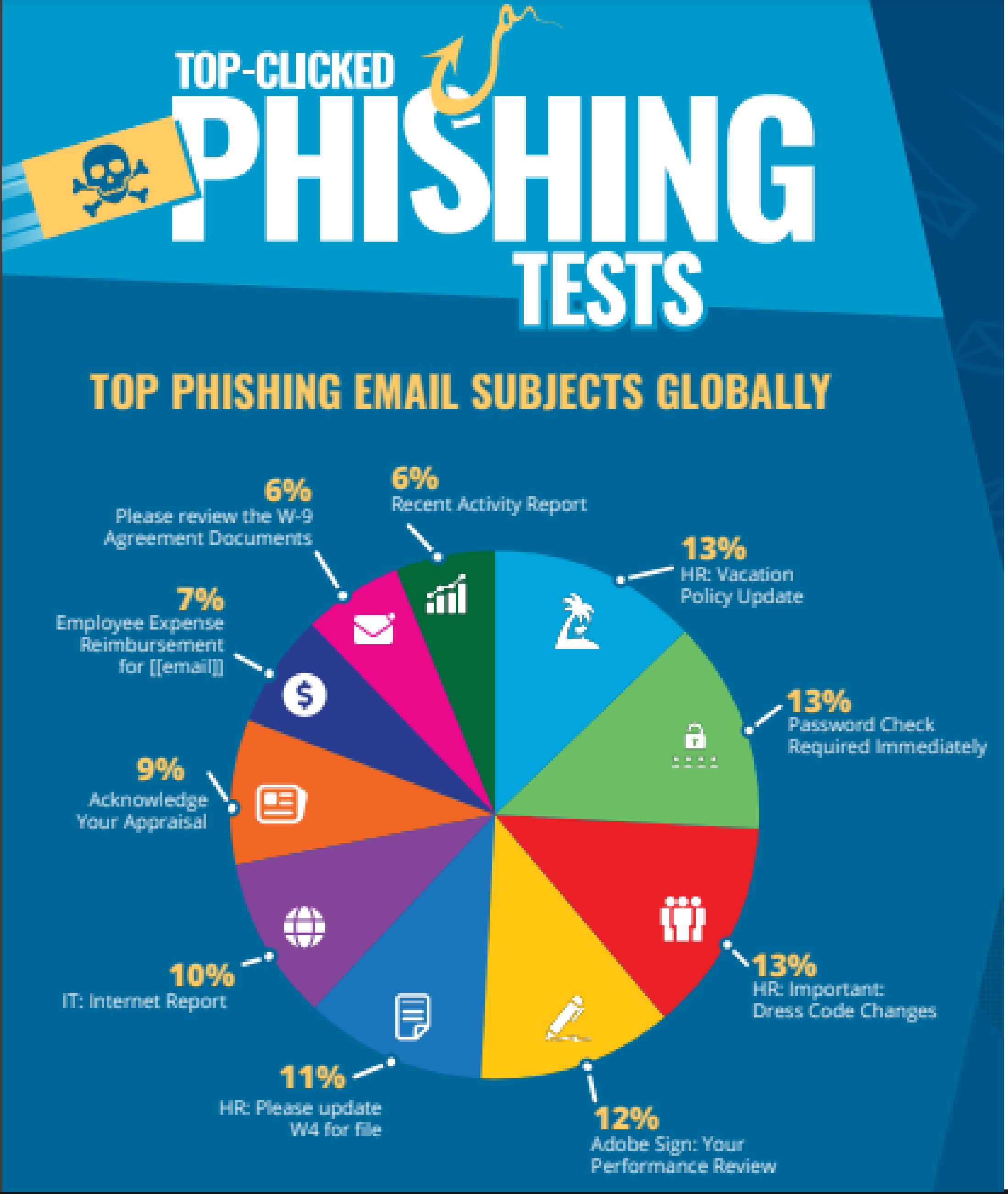
For example, what if you couldn’t process transactions or access your information?

ONGOING SECURITY THREATS

Threat Vectors – How the Bad Guys Get In



Phishing, Web & Ransomware	Compromised Credentials	Weak Passwords
Trust Relationships & Propagation	Poor Encryption	Unpatched Vulnerabilities
Misconfigurations	Malicious Insiders	Zero Day & Unknown Methods



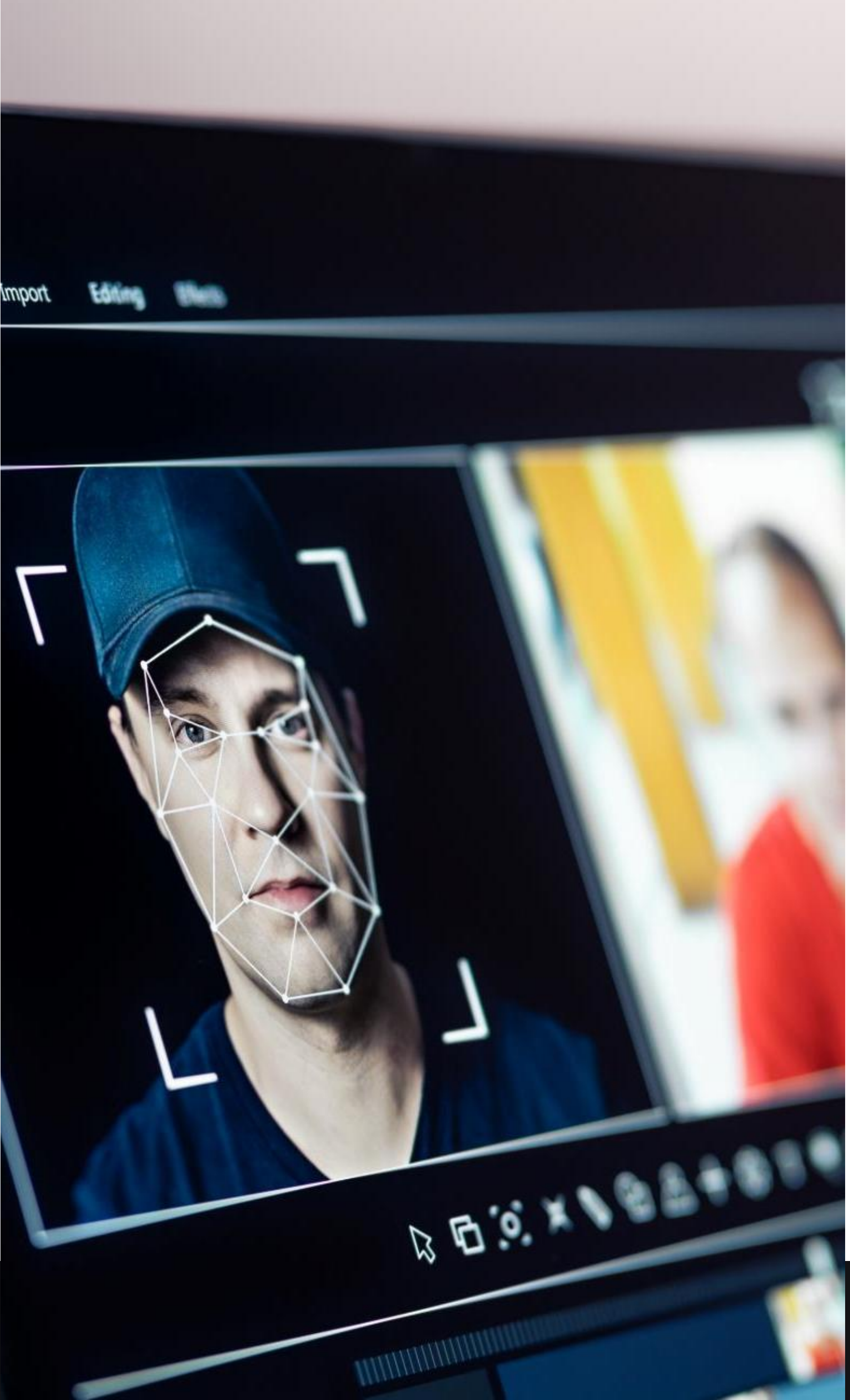
Phishing Emails

RECENT "IN THE WILD" ATTACKS SUBJECT LINES

- Please review updated financial policies
- Zoom: The meeting has started! Where are you?
- IT: Laptop Refresh
- Meta: Suspicious Activity
- Sharepoint: [[manager_name]] shared "Test_Data" with you
- Microsoft: Microsoft's new password requirement
- HR: Please verify your banking information
- DocuSign: DocuSign Account Suspension Notice
- Webmail: Security alert for [[email]]
- Refund has been processed to your account

According to Gartner, in 2025, **85% of successful attacks will leverage the human factor**, **rather than using advanced malware.** Compared to technology, the human factor will be by far the slowest one to evolve, and the most stable.

Source: KnowBe4, Gartner



Deep Fakes

Deepfake Audio

Deepfake audio is a type of synthetic media that uses artificial intelligence to generate audio recordings of people saying things they never actually said.

Voice Phishing

Voice phishing, also known as vishing, is a type of social engineering attack that uses voice communication to trick people into revealing sensitive information, such as passwords or credit card numbers.

Voice Cloning

Voice cloning is a technique that uses machine learning algorithms to create a synthetic voice that sounds like a real person.

Deepfake Video

A deepfake video is a type of synthetic media where a person's likeness in an image or video is swapped with another person's likeness using artificial intelligence. These videos are created to make the manipulated content appear authentic.

Incident Response Commonalities

Double Extortion

No / Limited Cyber Liability Insurance

Backup Systems Compromised

Limited Depth of Logging

No Security Awareness Training

Lack of Layered Defense

Weak Password Policies

Legacy Systems & Technology Debt

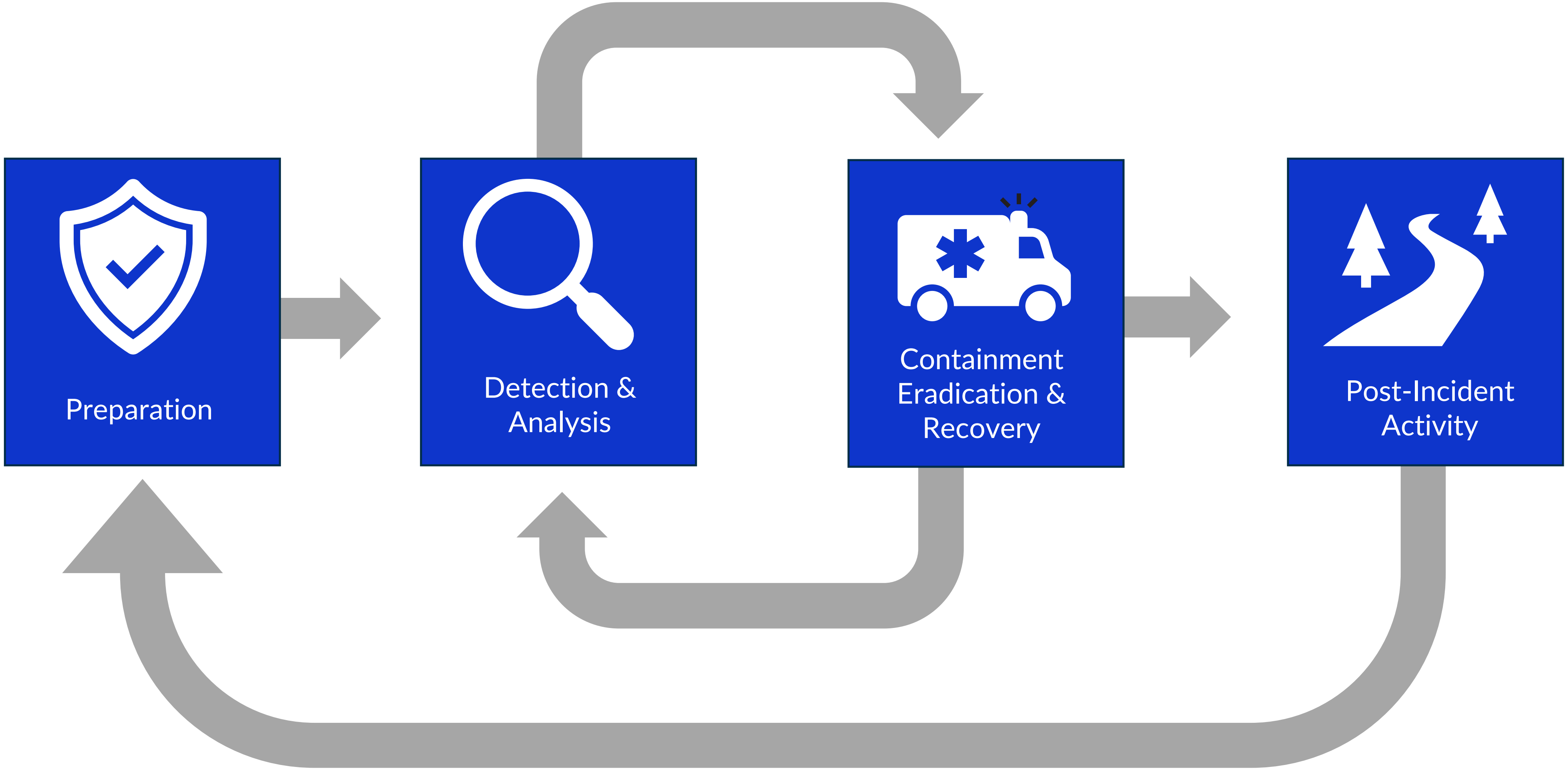
Patching & Firmware Out-of-Date

No Incident Response Planning

- Incident Response Plan
- Business Continuity
- Disaster Recovery

BUILD THE RESPONSE PLAN

The Phases of Incident Response



The Phases of Incident Response

Preparation

- Create incident response policy
- Create procedures to address incidents as efficiently as possible
  - May have references to BC/DR Plan
- Prevention: Implement reasonable controls according to risk assessments to reduce incident occurrence
- Prevention: Take “due care” steps to protect critical infrastructure and systems needed for recovery
- Work with a 3rd party such as a legal review to audit your plans & procedures, ensure they are available offline
- Ensure your incident response team is trained and table-top exercises are performed regularly
- Legal Obligation - Ensure evidence protection through the incident response phases

The Phases of Incident Response

Detection & Analysis

- Invoke notification process
  - Execute notification call tree
  - Contact security staff
  - Notify inside & outside counsel
  - Notify Insurance (Cyber liability policy)
  - Notify Law Enforcement
  - PR Firm or public relations engagement depending on incident severity
- Ensure most recent backups are ready and available
- Ensure critical logging is preserved (Many hardware & software vendors will roll logs)
- Ensure time across systems is accurate, will impact logging and timelines (NTP)
- Document all actions and information (Critical for forensics & litigation, lessons learned)

The Phases of Incident Response

Containment
Eradication &
Recovery

Containment

- Prevent incident spread, limit impact to the organization
- Preserve evidence, chain of custody, capture images
- In the event of a Cyber incident, do not power off affected systems. (Critical forensic artifacts can be lost) Better option: Disconnect from the network
- Critical systems containing sensitive data may need additional containment measures
- Log all activities, export device and system logs if no centralized logging in use to ensure critical audit trail is not overwritten or lost

Communication

- Users may need to be notified of incident status, out-of-band communication
- Work with internal public relations & legal counsel, follow procedures for communication with media and other public entities

Eradication

- Clean-up and remove infection, establish secure perimeter
- This phase begins at the approval of forensic investigators
- System wipe and purging for rebuilds or restore
  - Verify backup data is clean, restore to sandbox first and scan
- Continue to log activity and steps taken

Recovery

- Restoring systems and operations to a nominal state
- Follow DR plan to recover systems according the pre-established BIA order
- Restore and validate backup data
- Reset critical admin passwords
- Continue to log all efforts and recovery actions
- Maintain continuity of communication in all directions

The Phases of Incident Response

Post-Incident Activity

Clean-up & Lessons Learned

- Critical feedback loop & reporting phase
- Review log of activities and outcomes relative to the IR plan
- What gaps were identified in the plan?
- Identify total time, cost and impact incurred by the incident
- Produce final reporting required for forensics, legal or law enforcement action
- Feedback of performance to 3rd party providers, adjustments of contractual expectations.

Incident Planning & Testing

- Test the plan on an annual basis
- Train team members on the plan
- Subject the plan to an independent audit and review
- Update the plan based upon changes to personnel and the internal and external environments
- Update the plan based upon changes with vendors or third-party providers

Top Recommendations

- Verify Backup Position & Ensure Recoverability (Offsite, Tested, Air-Gapped)
- Establish Cyber Risk Ownership & Oversight
- Incident Response & Disaster Recovery & Business Continuity Plan
- Cyber Liability & Crime Insurance
- Security Awareness Training
- Multi-Factor Authentication (VPN, O365, Cloud Apps)
- Endpoint Detection & Response
- Vendor & Patch Management
- Password Management

PANEL DISCUSSION