9-1-1 SYSTEMS

Cyber Threat Protection & Response

Welcome & Introductions

Jeff Troyer

KCCDA Executive Director
and
Chairman of State 911 Committee (SNC)

Jon Moored

KCCDA Network & Systems Administrator
and
SNC Emerging Technology Subcommittee Member

Emergency Systems

DON'T FORGET...Providers

- **911 Service**
- **Non-Emergency/Admin Phone**
- **Internet Service**
- **Agency Connections**

Most Common Cyber Threats for Emergency Systems

Cybersecurity threats attacking emergency communications centers are a growing concern. Cybercriminals and hackers know the importance of these systems and target them to *access sensitive information or to cause disruptions*. Understanding these risks is fundamental for maintaining the integrity of our nation's public safety services.

Malware

MOST COMMON - Malicious software, including spyware, ransomware, viruses, and worms, which gets installed into the system when the user clicks a dangerous link or email. Once inside the system, malware can block access to critical components of the network, damage the system, and gather confidential information, among others.

Ransomware

Malicious actors may target emergency response systems, encrypting critical information and holding it hostage for ransom. This could interrupt emergency response efforts and endanger public safety services.

Distributed Denial of Service (DDoS) Attacks

DDoS attacks flood PSAPs with malicious traffic, overwhelming servers and preventing actual 911 calls from being answered

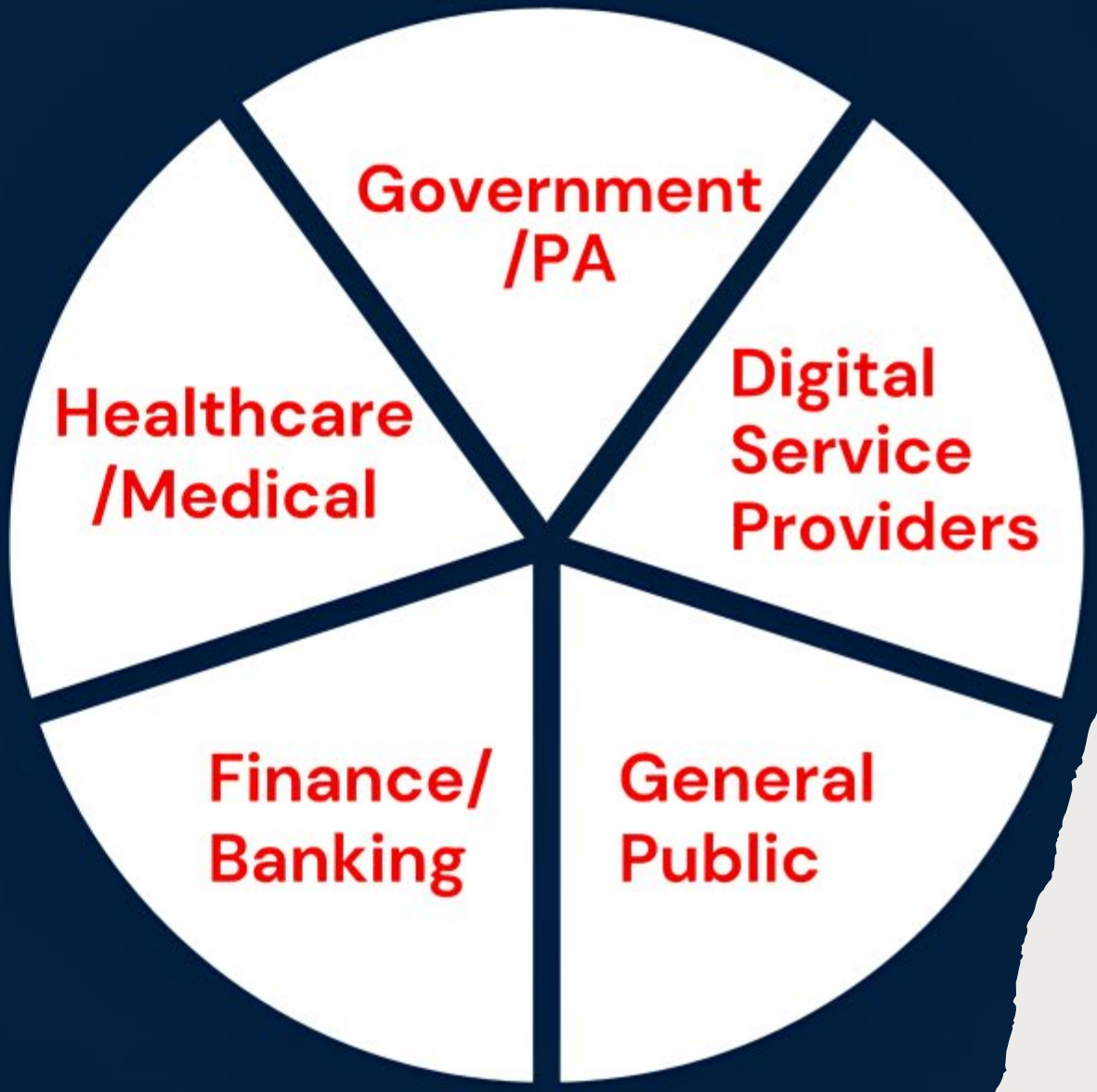
Data Breaches

Emergency systems store sensitive information, including caller location, details and data. A breach of this information can expose individuals to identity theft or other malicious practices.

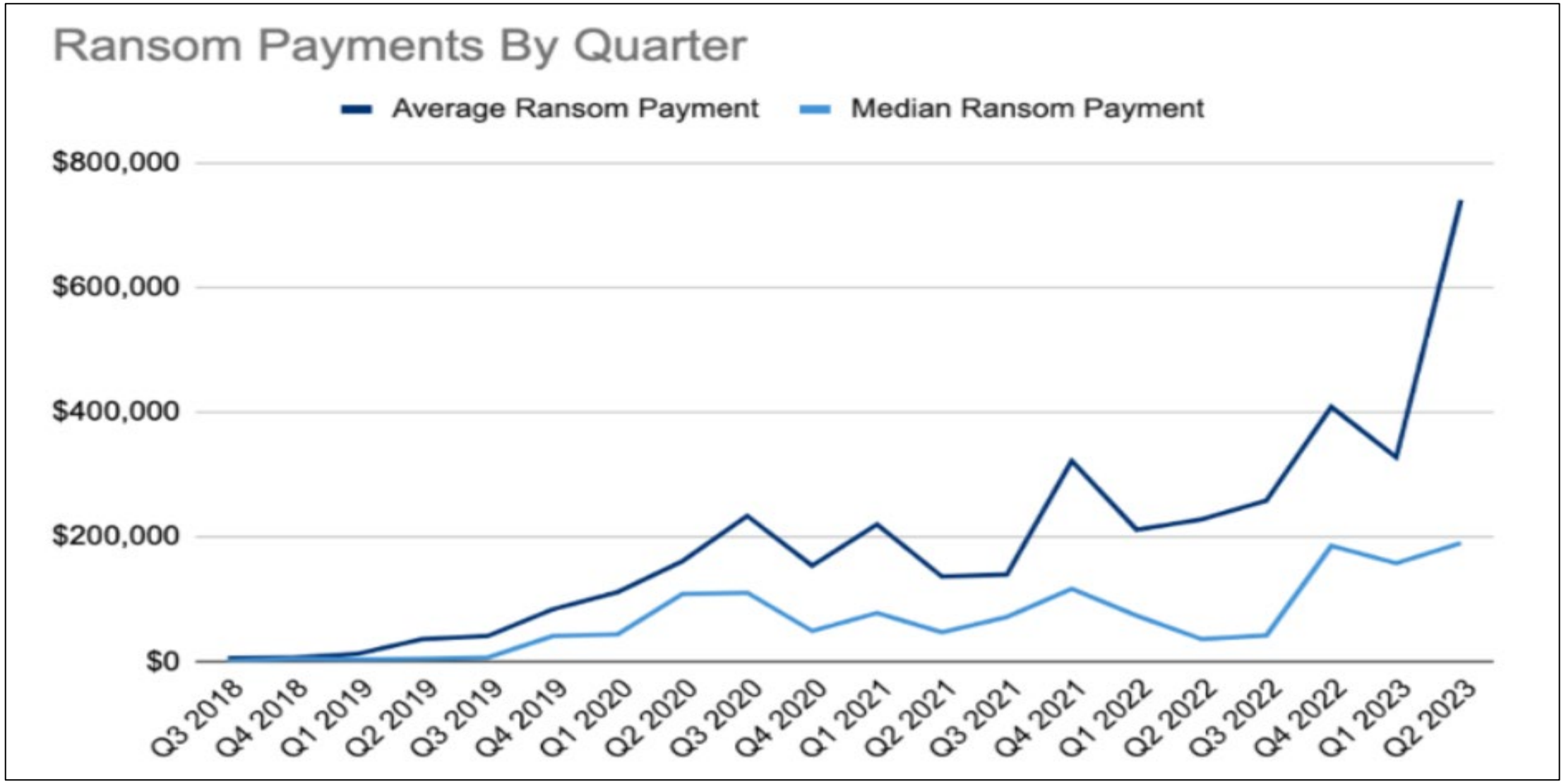
AI Manipulation

AI (artificial intelligence) plays a growing role in managing call volumes, routing, and triage. However, it can be exploited through data poisoning or adversarial inputs, leading to misclassification of emergency calls or resource misallocation.

TOP 5 SECTORS AFFECTED BY CYBERSECURITY THREATS



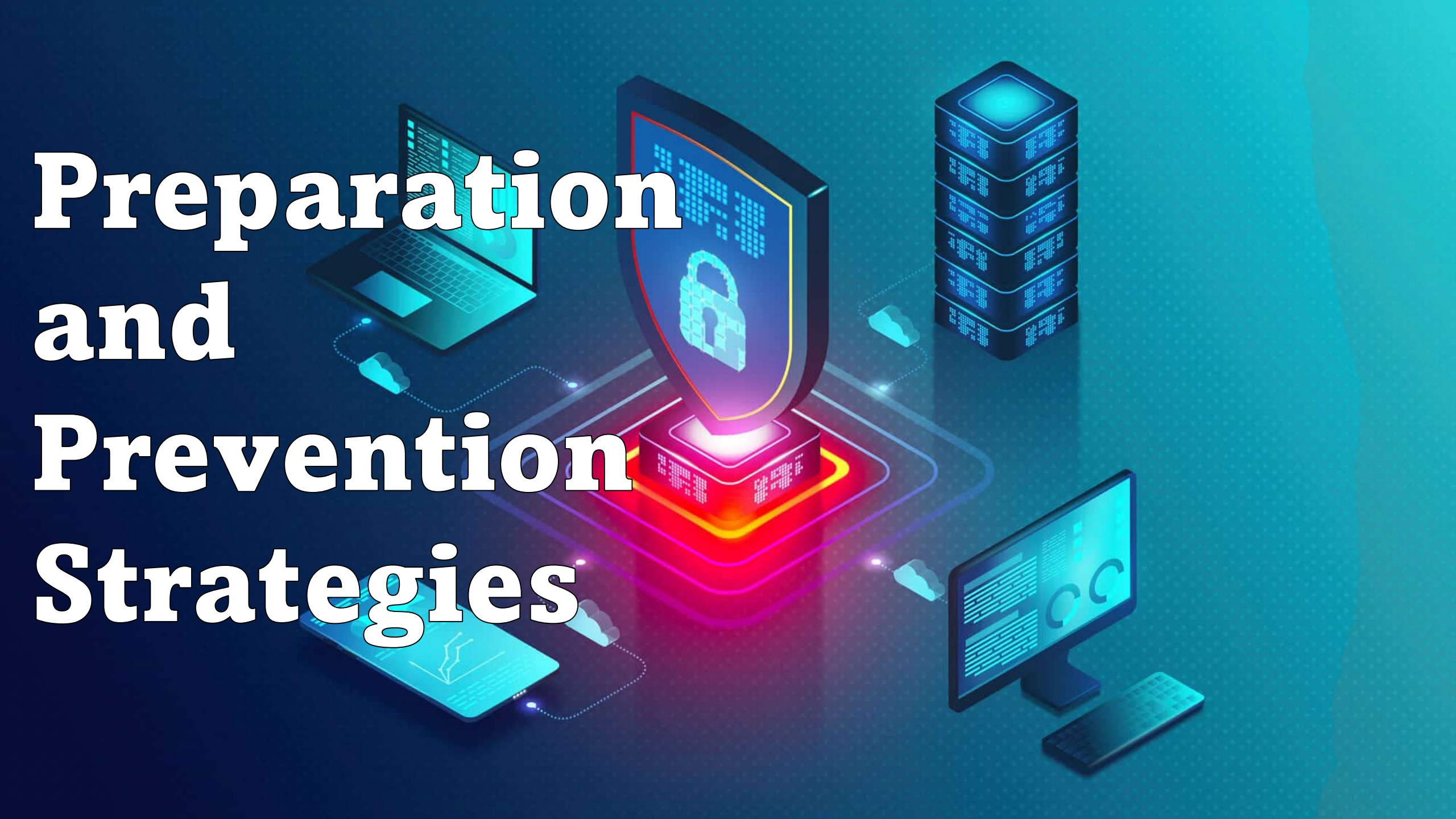
These sectors are at high-risk due to valuable stored data for potential attackers.



Additional Cost of Recovery

- **Downtime**
- **Staff Hours**
- **Investment in Cybersecurity Protections**
- **Legal Defense and Settlements**
- **Reputation**
- **Higher Insurance Premiums**

Preparation and Prevention Strategies



Preparation and Prevention

Cyber Security Threat Assessment

- Physical Security
- Network Vulnerability Assessment
- Internal & External Penetration Testing
- Best Practices

Strong Passwords

Regular Updates

- All computers and servers
- Anti-virus and threat protection applications
- Eliminate all outdated applications

Multi-factor Authentication

Encryption

Preparation and Prevention

Employee Training & Security Awareness

- Phishing campaigns
- Strict 3rd party device policy

Network Monitoring/Intrusion Detection

System and Service Redundancies

- Data and System Config back-ups
- Two or more providers: 911, Admin Lines, ISP's.

Wireless and Public Network Separation

- No Wireless access to critical systems without VPN
- Strict User Access Controls

Preparation and Prevention

Next Gen Antivirus and Firewalls

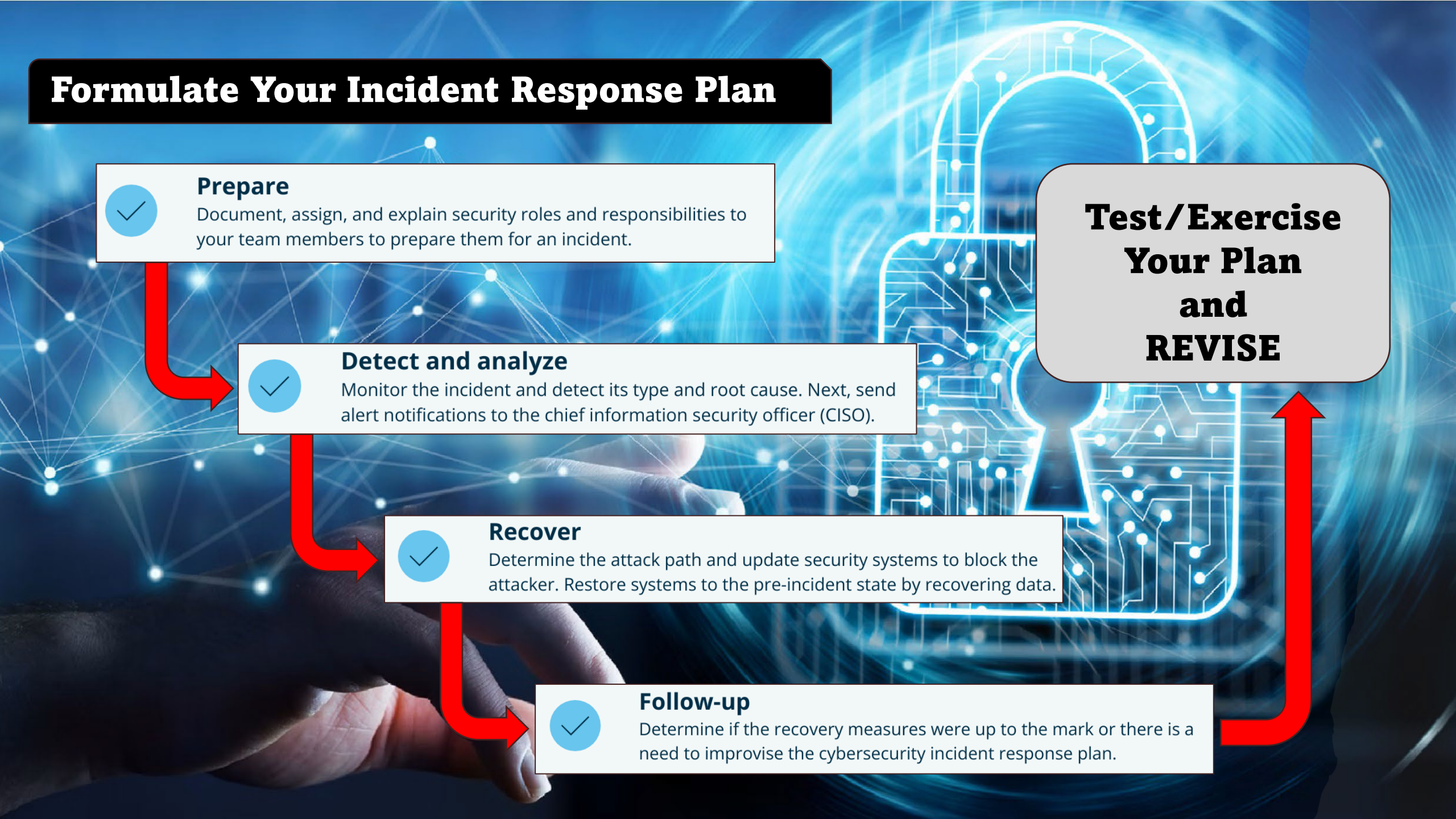
- Behavioral Based
- Monitor entire environment and not just a single machine
- Not just Allow and Deny

Primary System(s) and Network Segmentation

Relationships and Team Identification

- Liability Insurance Provider
- Key appointed and elected officials

Formulate Your Incident Response Plan



Prepare

Document, assign, and explain security roles and responsibilities to your team members to prepare them for an incident.

Detect and analyze

Monitor the incident and detect its type and root cause. Next, send alert notifications to the chief information security officer (CISO).

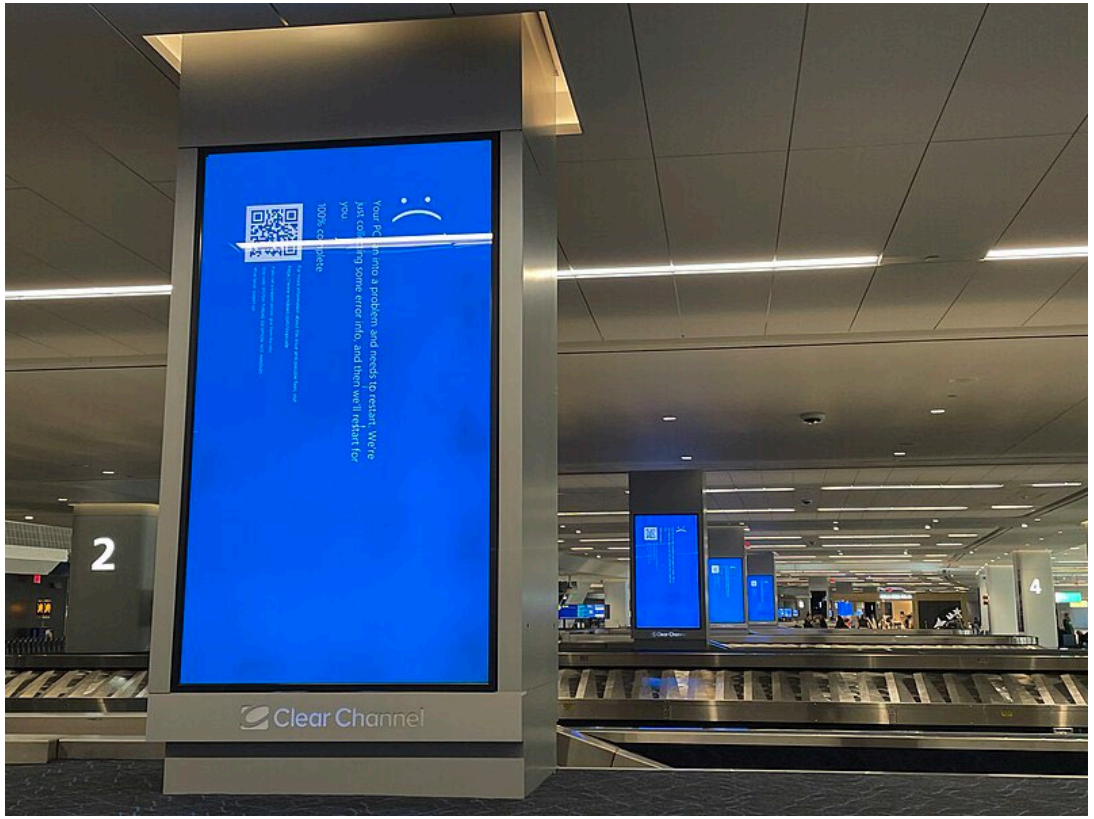
Recover

Determine the attack path and update security systems to block the attacker. Restore systems to the pre-incident state by recovering data.

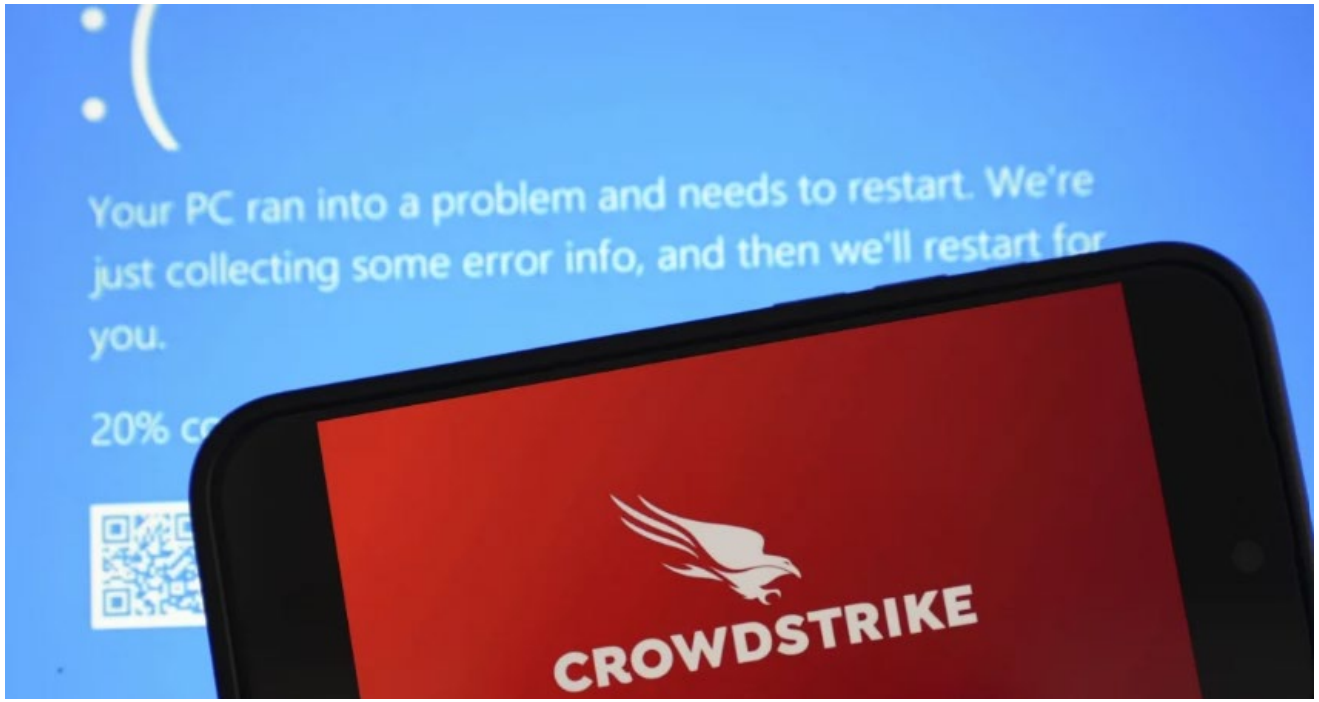
Follow-up

Determine if the recovery measures were up to the mark or there is a need to improvise the cybersecurity incident response plan.

Test/Exercise Your Plan and REVISE



Where were you?



MIDNIGHT - FRIDAY, JULY 19TH

DATE: October 29-30, 2024 **TIME:** 9:00 – 4:00 p.m.
LOCATION: Horizons Event Center, Saginaw, MI

CYBER THREAT ASSESSMENT AND PLANNING WORKSHOP

PURPOSE

This workshop assists PSAP leadership and emergency managers in learning how to develop a Cyber Incident Response Process and a Cyber Incident Response Plan. To help the participants understand the nature of these incidents, day one the instructors will provide education on cyber incidents and conduct several live demonstrations of different cyber-attacks including phishing/credential harvesting, ransomware, and business email compromise.

The second day of the workshop begins with an overview of a typical Cyber Incident Response Plan. This is followed by a discussion regarding the connection CSIRP and Continuity of Operations Planning. The remainder of the day is used to help participants use the template to build a response plan for a ransomware attack.

WHO SHOULD ATTEND

- PSAP Governing Body Representatives
- PSAP Coordinators, Directors, Leaders
- PSAP IT Support
- Other organizational Response Team Members

Thank you – Questions?

Jeff Troyer

jtroyer@kccda911.org
Mobile: (269) 718-2195

Jon Moored

jmoored@kccda911.org
Mobile: (269) 303-5544