AON

ALDRIDGE

LEADING THROUGH A CYBER ATTACK

THE FIRST 24 HOURS THAT SHAPE YOUR RECOVERY

Heather Hughes
Vice President, Cyber Solutions
Stroz Friedberg, an Aon Company

Chad Hiatt
Chief Technology Officer
Aldridge

TOP THREAT THIRD-PARTY ATTACKS

Your security is only as strong as your weakest partner.

Every vendor, contractor, and supplier you trust is an extension of your business — and a potential path in for attackers.

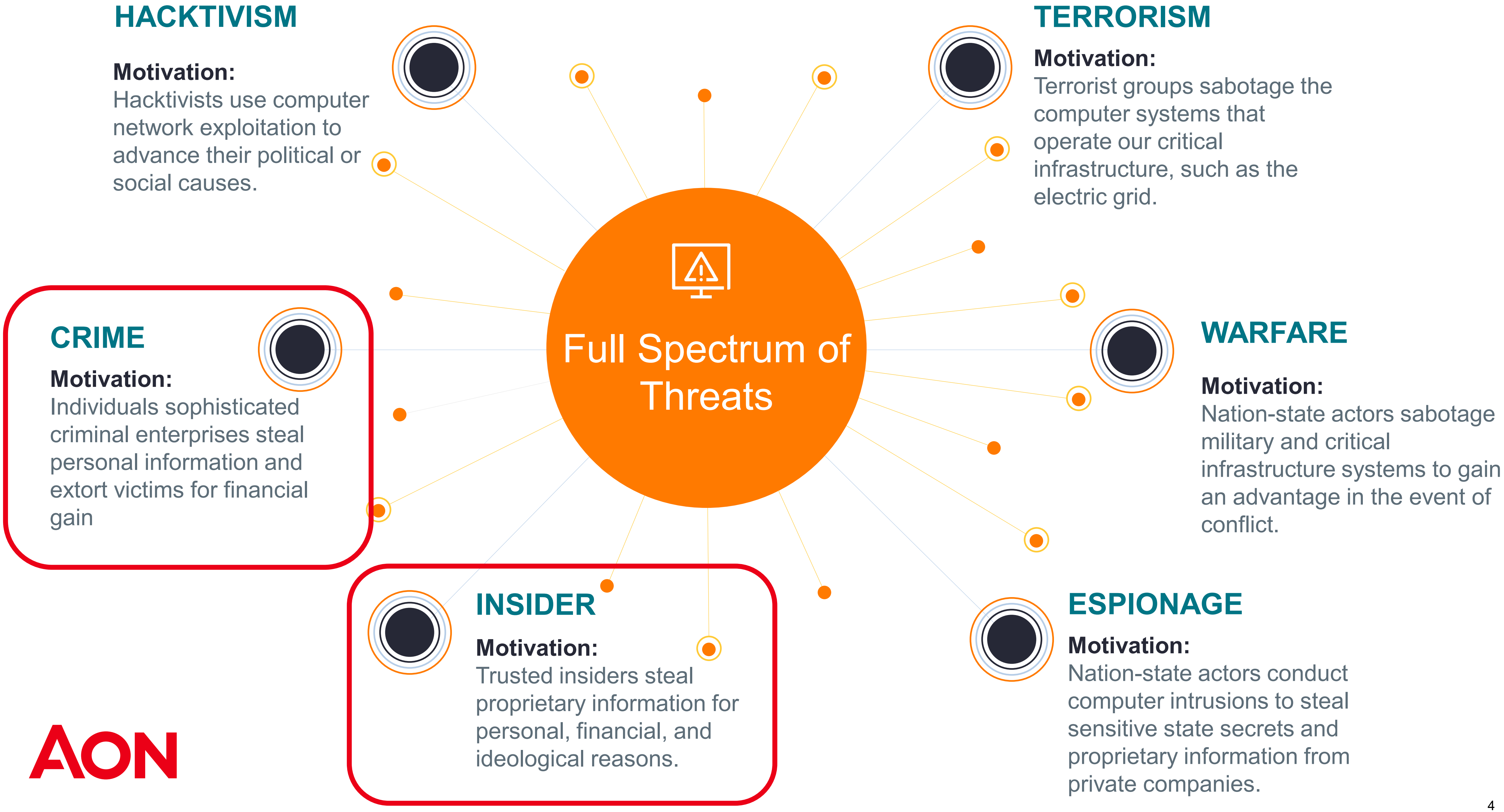
TOP THREAT THIRD-PARTY ATTACKS

Your contact at a trusted vendor has their email compromised.

Threat actor jumps in the middle of a billing conversation and alters the invoice with their banking info.

You trust that it’s a standard billing change, you send money to the threat actor, and you move on with your day.

ALDRIDGE



Full Spectrum of Threats

HACKTIVISM

Motivation:
Hacktivists use computer network exploitation to advance their political or social causes.

TERRORISM

Motivation:
Terrorist groups sabotage the computer systems that operate our critical infrastructure, such as the electric grid.

CRIME

Motivation:
Individuals sophisticated criminal enterprises steal personal information and extort victims for financial gain

WARFARE

Motivation:
Nation-state actors sabotage military and critical infrastructure systems to gain an advantage in the event of conflict.

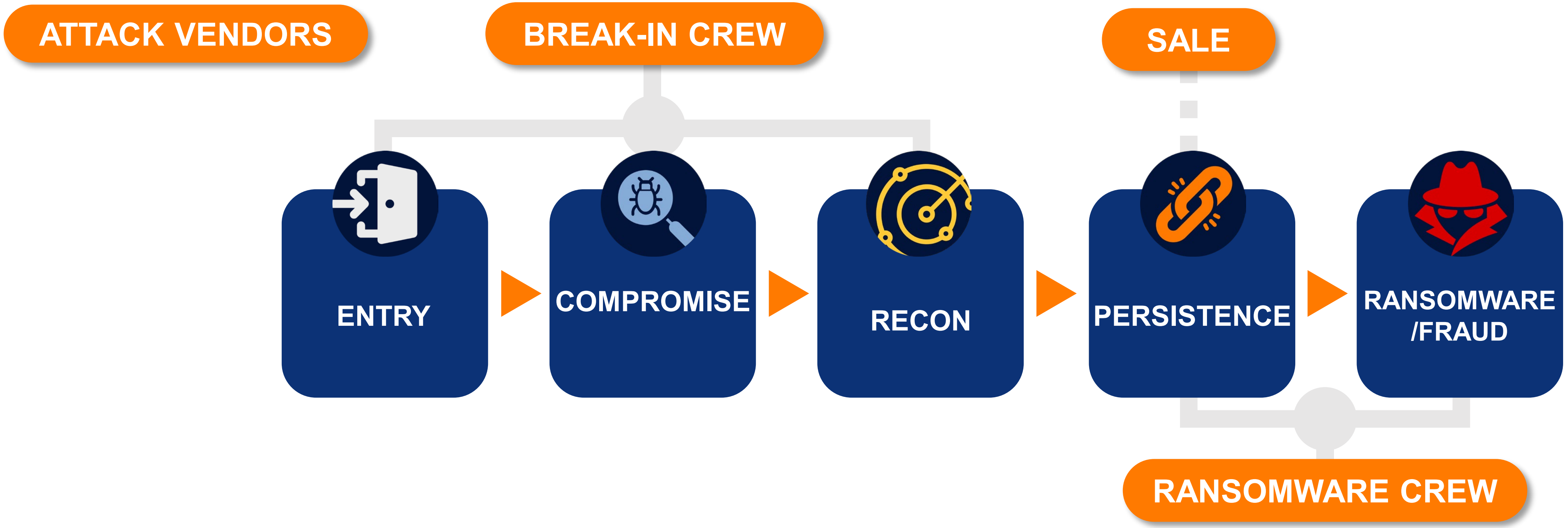
INSIDER

Motivation:
Trusted insiders steal proprietary information for personal, financial, and ideological reasons.

ESPIONAGE

Motivation:
Nation-state actors conduct computer intrusions to steal sensitive state secrets and proprietary information from private companies.

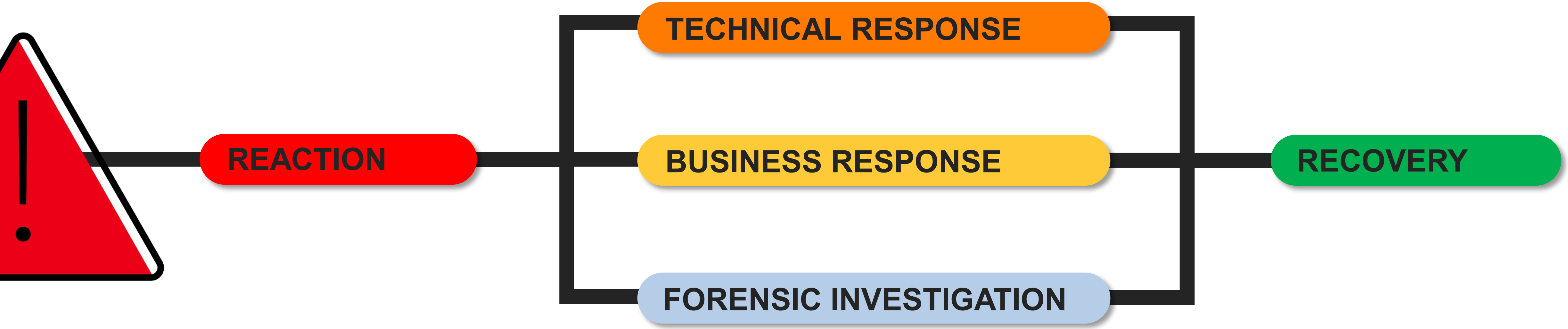
HOW A CYBER ATTACK WORKS



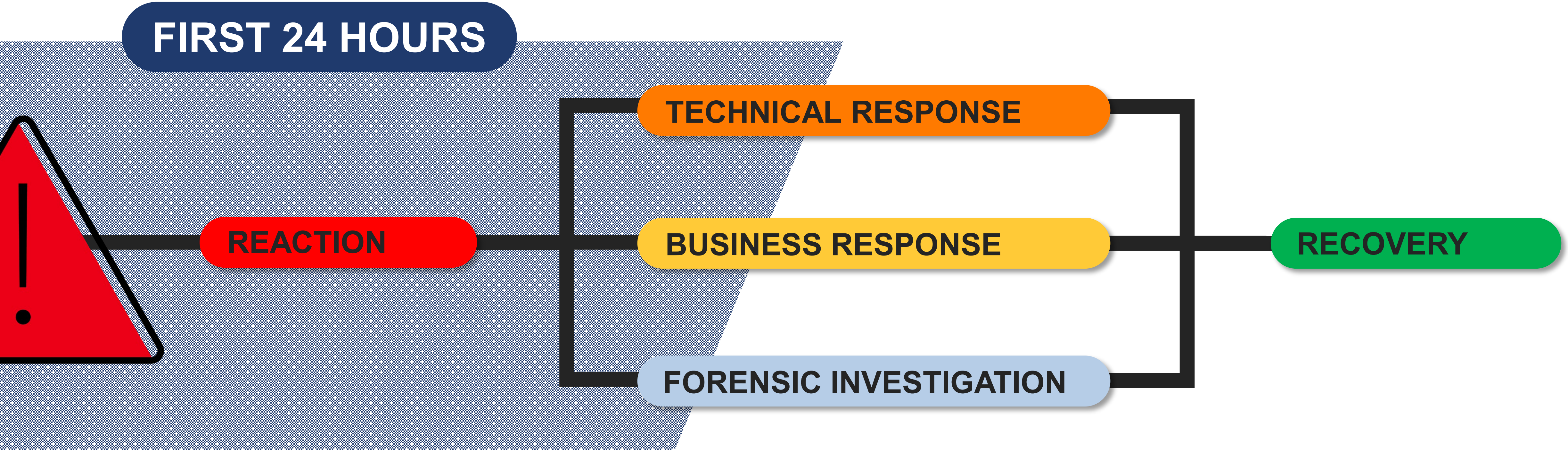
It’s Saturday morning, and you get a call from your IT team: they’ve detected unusual activity and think there may be a security issue that needs your attention.

“How serious is this?”

RESPONDING TO A CYBER ATTACK



RESPONDING TO A CYBER ATTACK



FIRST 24 HOURS

REACTION

TECHNICAL RESPONSE

BUSINESS RESPONSE

FORENSIC INVESTIGATION

RECOVERY

RANSOMWARE ATTACK

Threat actor alerts IT team that systems are encrypted

REACTION

REACTING TO AN INCIDENT

a) **Stay calm and don't make rash decisions driven by panic.**

DON'T Communicate with the threat actor

DON'T Unplug or turn off affected machines, delete files or wipe compromised systems

b) **Assemble your internal Incident Response Team and get your external experts involved.**

DO Initiate your Incident Response Plan and contact your forensic investigator, outside counsel and cyber insurance broker ASAP

DO Establish an out of band communication channel

RANSOMWARE ATTACK

Threat actor alerts IT team that systems are encrypted

TECHNICAL RESPONSE

LEADER’S ROLE DURING THE TECHNICAL RESPONSE

a) **Own Internal Communications:** Control internal messaging to prevent confusion or panic.

b) **Support Internal Response Team:** Ensure 24/7 coverage, provide needed resources, and take care of the team’s well-being.

c) **Coordinate Technical Teams:** Ensure internal teams are supporting external responders with timely access and information.

d) **Make Critical Business Decisions:** Be ready to act quickly based on technical findings—shutdowns, disclosures, or escalations.

RANSOMWARE ATTACK

Threat actor alerts IT team that systems are encrypted

TECHNICAL RESPONSE

LEADING THE BUSINESS RESPONSE

a) **Activate Continuity Plan:** Enable critical business functions to operate during disruption.

b) **Ransom Decision:** Decide whether to pay—and verify the threat actor isn't sanctioned.

c) **Plan Notifications:** Identify who must be notified (clients, partners, regulators), what to say, and when.

d) **Law Enforcement:** Decide if and how to engage with law enforcement.

e) **External Communications:** Align on timing and content; prep customer-facing teams with clear messaging.

BUSINESS RESPONSE

RANSOMWARE ATTACK

Threat actor alerts IT team that systems are encrypted

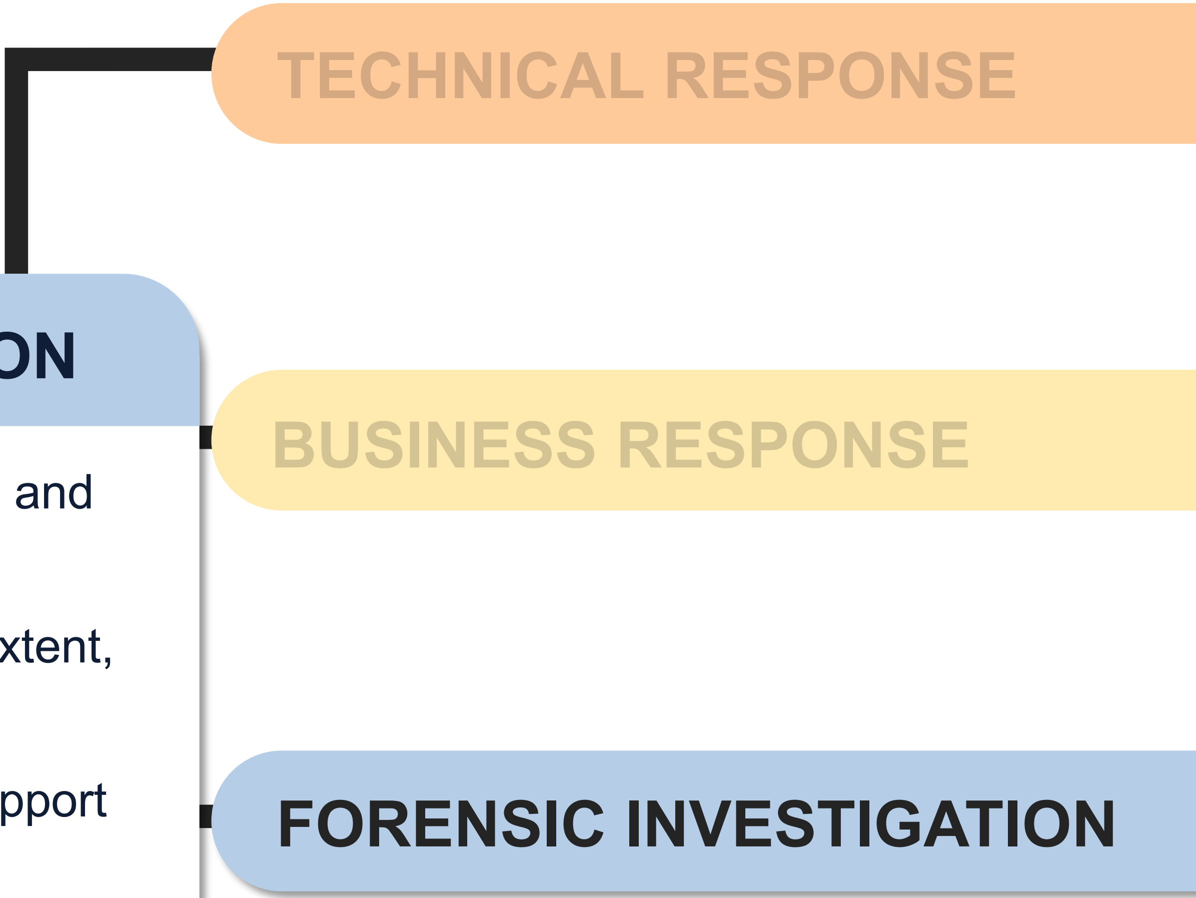
PURPOSE OF A FORENSIC INVESTIGATION

a) **Uncover Full Scope:** Identify how the incident occurred and determine the full range of impacted systems and data.

b) **Assess Impact:** Define who was affected and to what extent, to inform legal, regulatory, and customer responses.

c) **Preserve Evidence:** Secure logs and key artifacts to support legal, regulatory, and insurance processes.

d) **Enable Safe Recovery:** Confirm systems are clean, trusted, and free of backdoors before restoration. **This part takes time.**



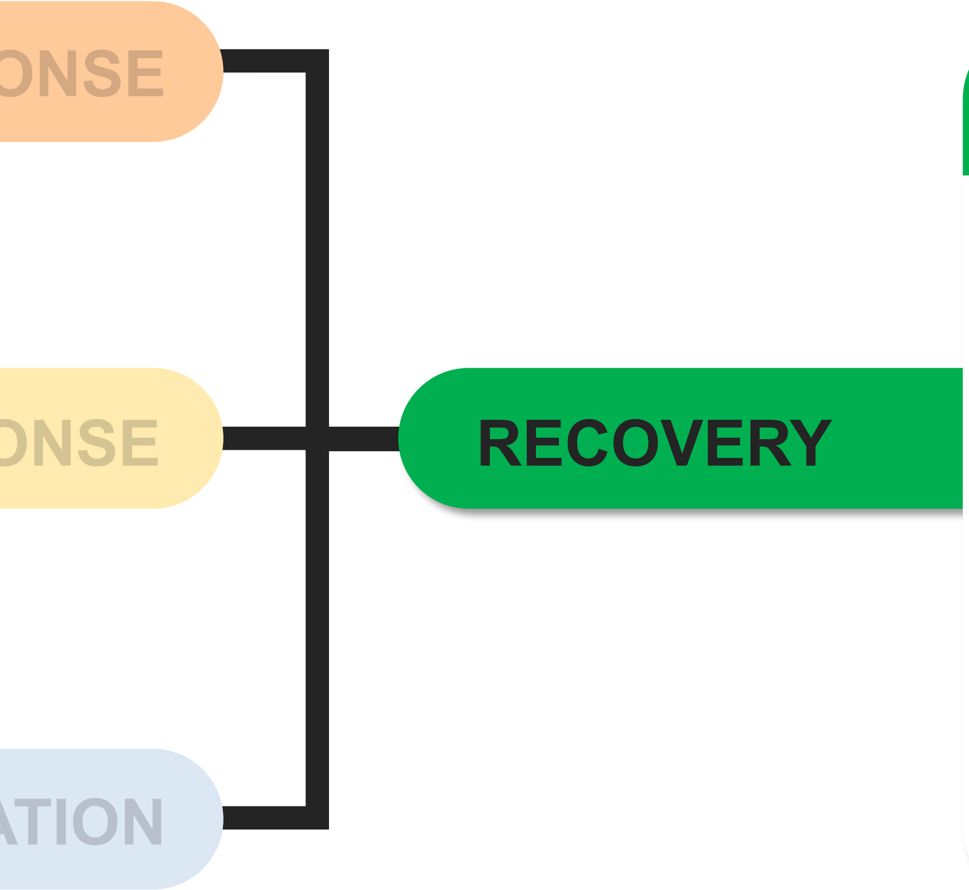
TECHNICAL RESPONSE

BUSINESS RESPONSE

FORENSIC INVESTIGATION

RANSOMWARE ATTACK

Threat actor alerts IT team that systems are encrypted



LEADERSHIP’S ROLE DURING RECOVERY

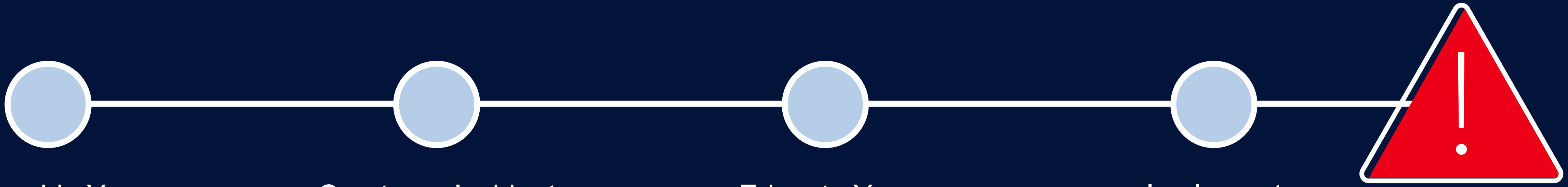
a) **Close out with external partners:** Coordinate with digital forensics, legal, and insurance to resolve the incident.

b) **Evaluate performance and lessons learned** – Assess how your security, IR plan, continuity plan, and response team performed; identify gaps and define improvements.

c) **Make affected parties whole** – Address customer, partner, or employee impact to reduce legal exposure and rebuild trust.

d) **Manage your reputation** – Preserve brand credibility and stakeholder confidence.

HOW TO PREPARE FOR AN ATTACK



Assemble Your Incident Response Team

Create an Incident Response Plan (IRP) & Practice Your Plan

Educate Your Entire Team on your IRP

Implement Core Cyber Controls

CORE CYBER CONTROLS

- Multi-Factor Authentication (MFA)
- Endpoint Detection and Response (EDR)
- Phishing Exercise/ Cyber Awareness Training
- Vulnerability Scanning & Patch Management
- Secure RDP/VPN
- Incident Response Plan/ Ransomware Exercise
- Access Control/ Service Accounts
- Disaster Recovery/Backups
- Email Filtering & Security (DMARC / DKIM)
- Zero Day Vulnerabilities and Supply Chain Risks
- Network Segmentation/ Network Monitoring
- M&A DD and Integration

AON