CYBERATTACK HORROR STORIES

LESSONS FROM THE FRONTLINE

Chad Hiatt
Chief Technology Officer
Aldridge

Seth Bursell
Senior Security Engineer
Aldridge

ALDRIDGE

THE STATE OF CYBERSECURITY

AI and automation is enabling attackers to launch highly personalized attacks faster and drastically shorten the time to strike once they gain access.

Many business owners felt secure in their defenses—until they were attacked.

ALDRIDGE

HOW BUSINESSES EVALUATE RISK

LEADER – PRIORITIZING RISKS

Security role: Define security culture, drive risk management, and balance cost-benefit. Ultimately accountable for security outcomes.

MANAGER – MANAGING MY TEAM AND TASKS

Security role: Link strategy with execution, ensuring processes align with security standards and fostering team buy-in.

END USER - GETTING MY WORK DONE

Security role: Use delegated access responsibly, maintaining security in daily operations.

ALDRIDGE

RISK MANAGEMENT OPTIONS

ACCEPT

Acknowledge and live with the risk

TRANSFER

Shift consequences of the risk to another party

CONTROL

Reduce likelihood or impact of the risk

AVOID

Eliminate exposure to risk

ALDRIDGE

MANAGE RISK BY IMPLEMENTING LAYERS OF SECURITY

ALDRIDGE

LAYERS OF SECURITY

TECHNOLOGY

- Air-gapped Backup
- E-Mail & Internet Threat Filtering
- Managed Detection & Response (MDR)
- Conditional Multi-Factor Authentication
- Security Information & Event Management (SIEM)
- External Vulnerability Scanning
- Security Awareness Training & Testing

PEOPLE

- IT Team
- Cybersecurity Insurer
- Attorney
- Security Incident Response Team
- Security Operations Center (SOC)
- Security-Minded Culture

PROCESSES

- Incident Response Plan
- Business Continuity Plans
- Security Standards & Policies

THREAT TRENDS

Shorter Dwell Time
Attackers complete objectives quickly, reducing time for defense or forensic investigation.

Session Replays
Cyber attackers exploit session replay tools to track user behavior, steal data, and identify security gaps.

Use Of Applications To Gain Persistence
Attackers use legitimate applications to embed malware, enabling undetected, long-term access to systems.

VICTIM OF ALL 3 THREAT TRENDS

HORROR STORY

0. Established Culture

1. Security Indicator Alert

2. Indicator Investigation/ Validation

3. Remediation

4. Lessons Learned

WHAT WAS MISSING?

TECHNOLOGY

- Air-gapped Backup
- **E-Mail & Internet Threat Filtering**
- Managed Detection & Response (MDR)
- Conditional Multi-Factor Authentication
- **Security Information & Event Management (SIEM)**
- External Vulnerability Scanning
- **Security Awareness Training & Testing**

PEOPLE

- IT Team
- Cybersecurity Insurer
- Attorney
- Security Incident Response Team
- **Security Operations Center (SOC)**
- **Security-Minded Culture**

PROCESSES

- Incident Response Plan
- Business Continuity Plans
- **Security Standards & Policies**

ALDRIDGE

THREAT ACTORS GAMEPLAN

ACCESS

PERSISTENCE

EXPLOITATION

EXPLOITATION

EXFILTRATION

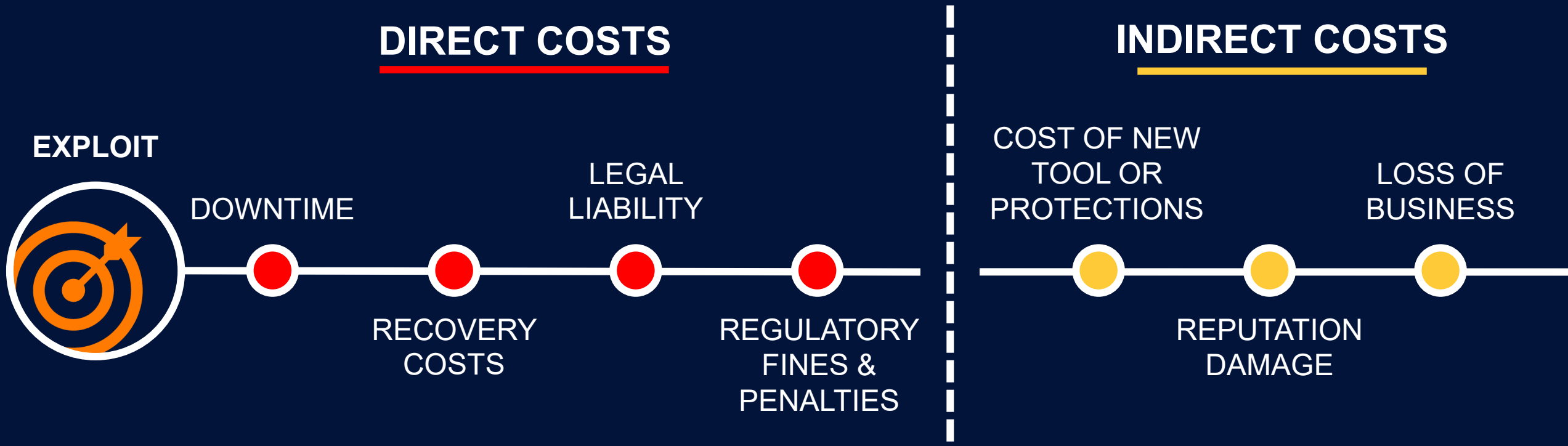
FRAUD

RANSOM

OR ALL 3?

ALDRIDGE

COST OF EXPLOITATION



ALDRIDGE

HOW CAN CYBER INSURANCE HELP?

INCIDENT RESPONSE & RECOVERY
Funds investigations, e-discovery, and recovery.

BUSINESS CONTINUITY & OPERATIONAL COST
Covers downtime and disruption.

EXTORTION & RANSOMWARE PROTECTION
Mitigates ransom and extortion expense.

HARDWARE & SYSTEM SECURITY
Covers hardware damage and replacement.

FINANCIAL FRAUD & SOCIAL ENGINEERING
Protects against theft, fraud, and social scams.

MUST-HAVES FOR CYBER INSURANCE

MULTI-FACTOR AUTHENTICATION (MFA)

Adds multiple verification steps to confirm your identity.

AIR-GAPPED BACKUPS

Stores backups separately from main systems to reduce encryption and ransomware risk.

MANAGED DETECTION & RESPONSE (MDR)

Integrates advanced threat detection and response tools, leveraging real-time monitoring and expert analysis to identify and neutralize emerging cyber threats.

PATCHING & VULNERABILITY MANAGEMENT

Proactive scans to identify and patch vulnerabilities.

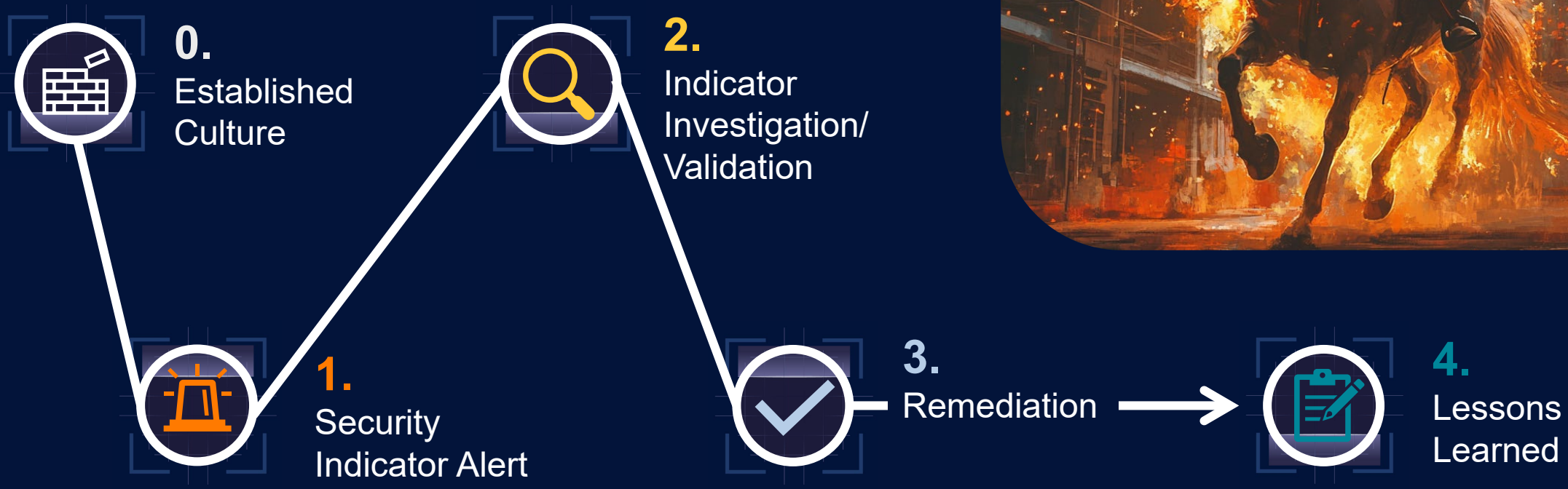
SECURITY AWARENESS TRAINING

Educates employees on recognizing and avoiding cybersecurity threats, particularly phishing, to enhance organizational defense against human-targeted attacks.

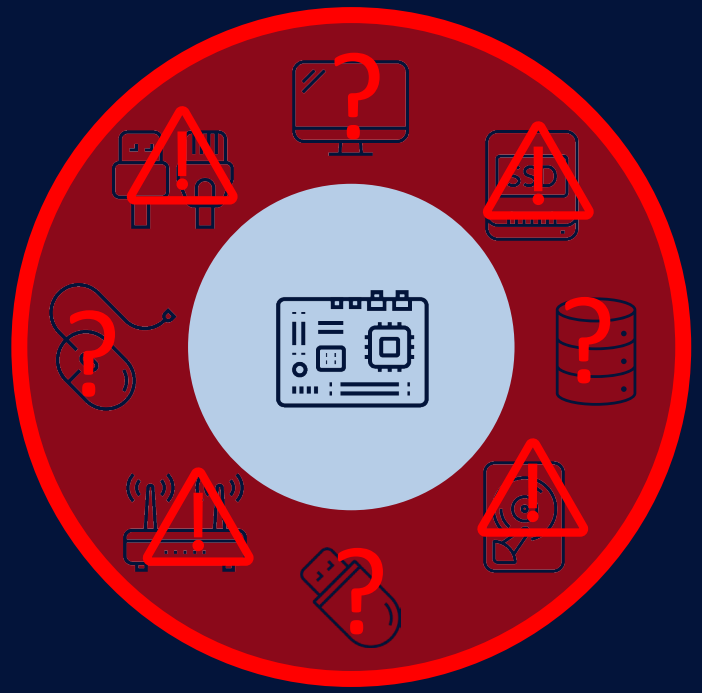
ALDRIDGE

WAKING UP TO TOTAL DESTRUCTION

HORROR STORY



REBUILDING A BUSINESS BY RE-ESTABLISHING TRUST



ALDRIDGE

REBUILDING A BUSINESS BY RE-ESTABLISHING TRUST

ALDRIDGE

REBUILDING A BUSINESS BY RE-ESTABLISHING TRUST

ALDRIDGE

EXPLOITATION

EXFILTRATION

FRAUD

RANSOM

OR ALL 3?

ALDRIDGE

WHAT WAS MISSING?

TECHNOLOGY

- Air-gapped Backup
- **E-Mail & Internet Threat Filtering**
- Managed Detection & Response (MDR)
- **Conditional Multi-Factor Authentication**
- **Security Information & Event Management (SIEM)**
- **External Vulnerability Scanning**
- **Security Awareness Training & Testing**

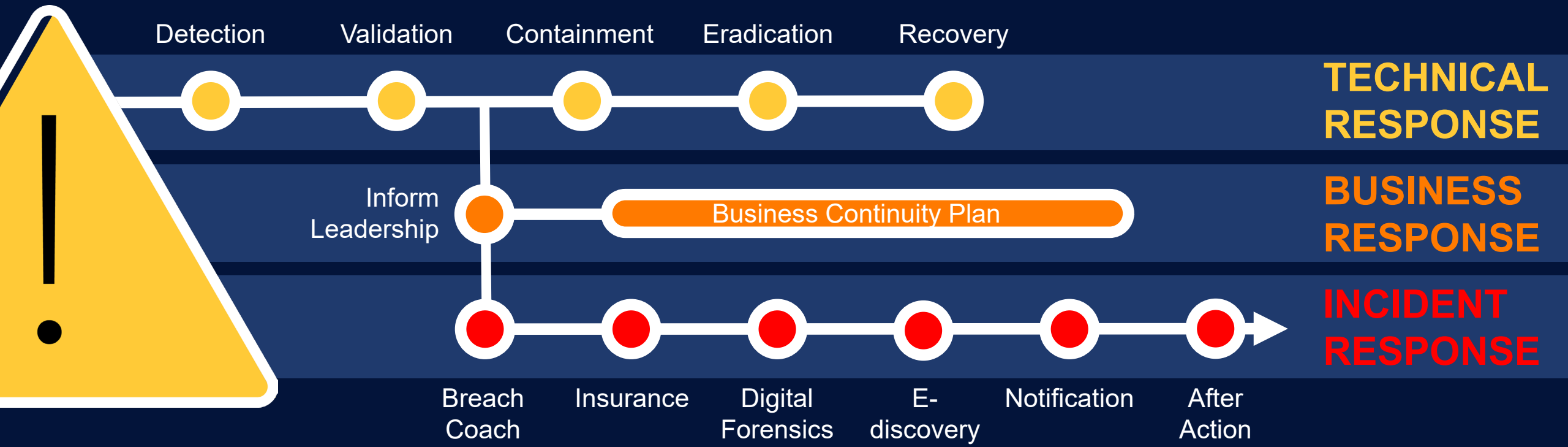
PEOPLE

- IT Team
- Cybersecurity Insurer
- **Attorney**
- **Security Incident Response Team**
- **Security Operations Center (SOC)**
- **Security-Minded Culture**

PROCESSES

- **Incident Response Plan**
- **Business Continuity Plan**
- **Security Standards & Policies**

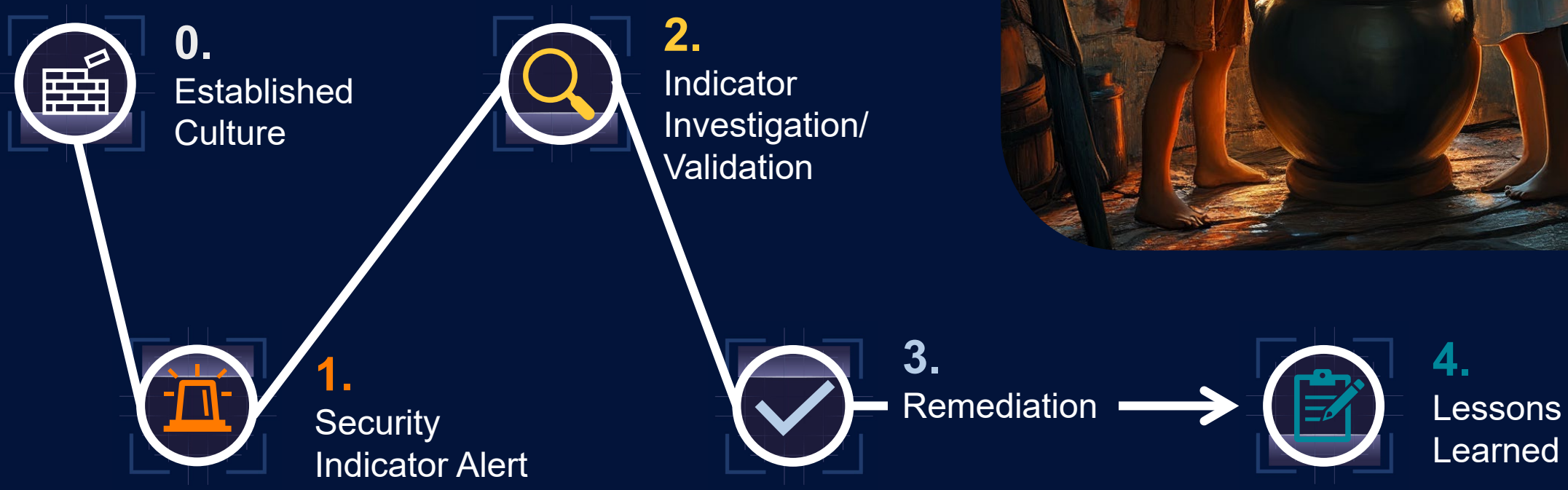
RESPONDING TO AN INCIDENT



ALDRIDGE

WE'RE TOO SMALL TO BE TARGETED

HORROR STORY



WHAT WAS MISSING?

TECHNOLOGY

- Air-gapped Backup
- E-Mail & Internet Threat Filtering
- **Managed Detection & Response (MDR)**
- **Conditional Multi-Factor Authentication**
- **Security Information & Event Management (SIEM)**
- External Vulnerability Scanning
- Security Awareness Training & Testing

PEOPLE

- IT Team
- Cybersecurity Insurer
- Attorney
- Security Incident Response Team
- **Security Operations Center (SOC)**
- **Security-Minded Culture**

PROCESSES

- **Incident Response Plan**
- **Business Continuity Plan**
- **Security Standards & Policies**

ALDRIDGE

SECURITY TEAM ROLES & RESPONSIBILITIES

ALDRIDGE

INTERNAL IR TEAM

INCIDENT RESPONSE LEAD

Coordinates internal & external IR teams. Person with the authority to trigger your IRP.

ALDRIDGE

EXTERNAL IR TEAM

IT MSP/MSSP

Lead short-term recovery and assists DFIR team with investigation.

BREACH COACH

Lawyer, specialized in cyber, that quarterbacks your incident response

INSURANCE

Files your claim and coordinates insurance incident response resources.

DIGITAL FORENSICS & INCIDENT RESPONSE (DFIR)

Uncovers full impact of the incident.

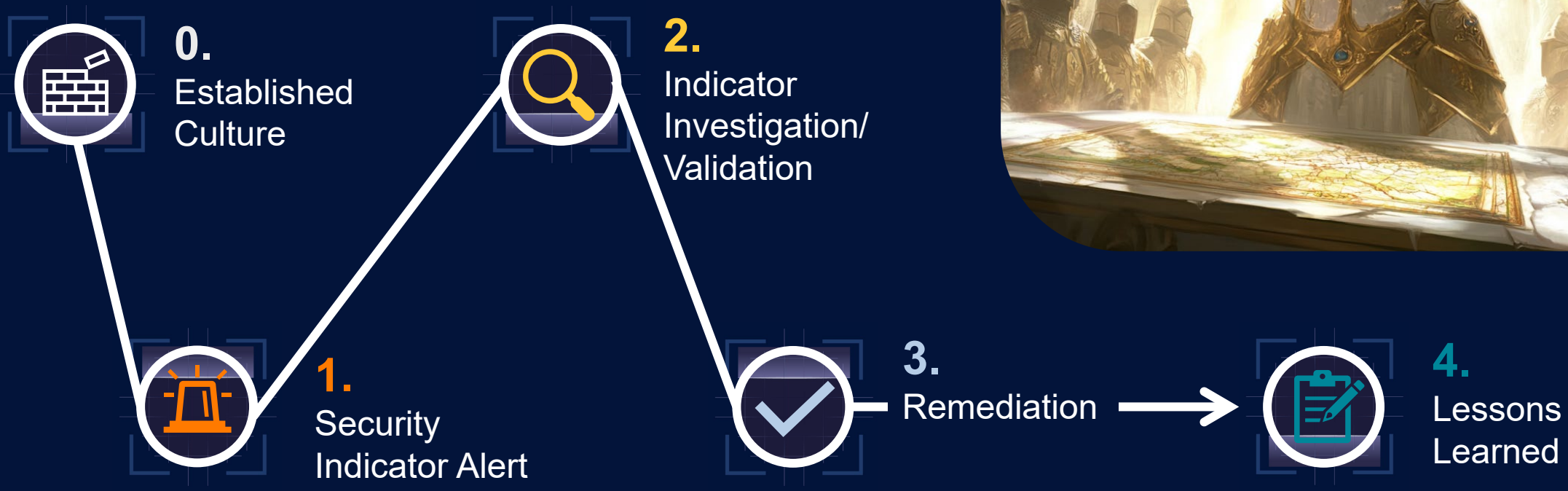
INCIDENT RESPONSE LEAD

Responsible for assembling external IR team, maintaining the relationship, and reaching out in the event of a potential incident.

ALDRIDGE

RISK MANAGEMENT & SECURITY CULTURE

SUCCESS STORY



WHAT MADE THIS A SUCCESS?

TECHNOLOGY

- Air-gapped Backup
- E-Mail & Internet Threat Filtering
- **Managed Detection & Response (MDR)**
- Conditional Multi-Factor Authentication
- Security Information & Event Management (SIEM)
- External Vulnerability Scanning
- Security Awareness Training & Testing

PEOPLE

- IT Team
- Cybersecurity Insurer
- Attorney
- Security Incident Response Team
- **Security Operations Center (SOC)**
- **Security-Minded Culture**

PROCESSES

- Incident Response Plan
- Business Continuity Plan
- **Security Standards & Policies**

SECURITY TEAM WITH THE RIGHT TOOLS

SUCCESS STORY

0. Established Culture

1. Security Indicator Alert

2. Indicator Investigation/ Validation

3. Remediation

4. Lessons Learned

WHAT MADE THIS A SUCCESS?

TECHNOLOGY

- Air-gapped Backup
- **E-Mail & Internet Threat Filtering**
- Managed Detection & Response (MDR)
- Conditional Multi-Factor Authentication
- **Security Information & Event Management (SIEM)**
- External Vulnerability Scanning
- Security Awareness Training & Testing

PEOPLE

- **IT Team**
- Cybersecurity Insurer
- Attorney
- **Security Incident Response Team**
- **Security Operations Center (SOC)**
- **Security-Minded Culture**

PROCESSES

- Incident Response Plan
- Business Continuity Plan
- **Security Standards & Policies**

HOW SIEM PROTECTED THEM

Collects data from various sources logging aggregate

Rules and AI Analyzes data to detect security indicators or unusual activity

People Monitor SIEM and investigate indicators to identify real threats

ALDRIDGE

WHERE ARE YOU RIGHT NOW?

WHERE DO YOU WANT TO BE?

"We will do the **bare minimum** for security so that we don't look completely negligent."

"We want our security to be **aligned with our industry peers**. We don't want to fall behind, but we don't want to be a leader."

"**Security is a differentiator** for us. We will win business and gain the trust of our clients and partners because of our security."

ALDRIDGE

BASIC SECURITY

TECHNOLOGY

- **Air-gapped Backup**
- **E-Mail Filtering** & Internet Threat Filtering
- **Managed Detection & Response (MDR)**
- Conditional **Multi-Factor Authentication**
- Security Information & Event Management (SIEM)
- **External Vulnerability Scanning**
- **Security Awareness Training & Testing**

PEOPLE

- **IT Team**
- **Cybersecurity Insurer**
- **Attorney**
- **Security Incident Response Team**
- Security Operations Center (SOC)
- Security-Minded Culture

PROCESSES

- Incident Response Plan
- Business Continuity Plans
- Security Standards & Policies

STANDARD SECURITY

TECHNOLOGY

- Air-gapped Backup
- E-Mail & Internet Threat Filtering
- Managed Detection & Response (MDR)
- Conditional Multi-Factor Authentication
- Security Information & Event Management (SIEM)
- External Vulnerability Scanning
- Security Awareness Training & Testing

PEOPLE

- IT Team
- Cybersecurity Insurer
- Attorney
- Security Incident Response Team
- Security Operations Center (SOC)
- Security-Minded Culture

PROCESSES

- Incident Response Plan
- Business Continuity Plans
- Security Standards & Policies

GET A SECURITY TEAM YOU CAN COUNT ON

Inform you of relevant risks to your business

Weigh the balance between cost, convenience, and security

Continually evolve your security

Ready to respond to attacks on your business and guide you through the aftermath

ALDRIDGE