Incident Response & Forensic Services

Stop active breaches in their tracks

Cyber threats are ever-present, and their potential impact can be devastating. Therefore, it's imperative for businesses of all sizes to have a well-defined cybersecurity incident response plan. It's not just about responding to incidents when they occur but also about proactively preparing to minimize the damage and protect your organization's interests.

A cyber breach can have far-reaching consequences, causing financial losses, affecting an organization's operations and compliance in the short term, as well as potentially damaging your reputation for years to come, leading to lost business and a competitive disadvantage.

According to the IBM's Cost of a Data Breach report, the average cost savings of an organization that has an incident response team and proactive IR testing versus organizations with no IR team or testing is USD 1.5 million.

Recommended Steps:

Two key steps that can help businesses enhance their cyber preparedness and incident response effectiveness:

1. **Create A Detailed Incident Response Plan and Playbook:** It's important to develop plans and playbooks that are customized to your organization's environment, technologies, and resources. This enables you to account in advance for the resources required in the event of a security incident, establish those contacts as well as have an Incident Response retainer subscription that will make incident response services readily available during a cyber crisis.
2. **Rehearse and Test Your Incident Response Under Pressure:** It's not a matter of if an organization's security team will be tested by a cyberattack, but a matter of when. By conducting simulation exercises your organization and security team can experience what it's like to respond under pressure and identify your gaps and areas or processes you need to improve in order to effectively activate in the event of a real-life security event. This includes ensuring external security teams or solution providers integrated into your response team.

Incident Response stages

Incident response strategies layout what defines a breach, the roles and responsibilities of the security team, tools for managing a breach, steps that will need to be taken to address a security incident, how the incident will be investigated and communicated, and the notification requirements following a data breach. Incident response is comprised of the following stages:

- **Preparation:** Developing an Incident Response Plan (IRP), identifying key personnel, and establishing communication protocols.
- **Detection and Analysis:** Monitoring for suspicious activities, analyzing indicators of compromise (IoCs), and determining the scope of the incident.
- **Containment and Eradication:** Isolating affected systems, removing malicious elements, and preventing further spread.
- **Recovery and Restoration:** Restoring systems and data, ensuring data integrity, and validating the recovery process.
- **Digital Forensics:** Analysis recovery investigation, comprised of identification, preservation, analysis, documentation, and presentation.
- **Lessons Learned:** Post-incident review to learn from the incident and enhance future incident response efforts.

Call our Security team today.

They'll ask you some preliminary questions about your security environment and schedule a time for a free consultation.

2401 West Monroe Street, Springfield, IL | 217-793-3800 | www.lrssecuritysolutions.com | security@lrs.com

Incident Response & Forensic Services

LRS SECURITY SOLUTIONS

Cyber strategy and resiliency services

There is no shortage of challenges facing security teams today. Factors such as an increased proliferation and interconnectivity of endpoints and data and security skills gaps, coupled with the rise of malicious activities from threat actors, have created a substantial threat to business continuity for organizations, as well as highlighting a need for faster threat detection. Learn about the most common types of cybersecurity threats.

Most common cyber threats

Phishing Attack
- Employees receive deceptive emails with malicious links or attachments.

Ransomware Infection
- Malicious software encrypts critical files, demanding a ransom for decryption.

Data Breach
- Customer data is stolen.

Distributed Denial of Service (DDoS) Attack
- Web services are overwhelmed with traffic, rendering them inaccessible.

Insider Threat
- A disgruntled employee steals or sabotages sensitive company information.

Malware Outbreak
- A widespread malware strain infects multiple systems across the organization.

Physical Security Breach
- Unauthorized individuals gain physical access to sensitive areas or equipment.

Zero-Day Exploit
- Attackers exploit a previously unknown vulnerability in software.

IoT Device Compromise
- Internet of Things (IoT) devices are compromised and used as a foothold for network infiltration.

Social Engineering Attack
- Attackers manipulate employees into revealing confidential information or performing actions against security protocols.

Cyber threat management services

LRS is a leading provider of end-to-end cyber security, digital forensics and incident response services. Our experts quickly contain the compromise and smoothly guide you to recovery, with minimal business disruption and your reputation intact.

Threat Hunting
- → Proactively searching for security events and threats within an organizations network
- → Continuous monitoring
- → Average dwell time of APT is 21 days

Incident Response
- → Preparation and planning
- → Detection and identification
- → Containment, eradication, and recovery
- → Lessons learned

Forensics
- → Evidence collection and preservation
- → Analysis and attribution
- → Reporting and documentation

Call our Security team today.

They'll ask you some preliminary questions about your security environment and schedule a time for a free consultation.

2401 West Monroe Street, Springfield, IL | 217-793-3800 | www.lrssecuritysolutions.com | security@lrs.com