THREAT MANAGEMENT:

Staying Safe in an Unpredictable Environment

LRS®
SECURITY SOLUTIONS

DEFINING CYBERSECURITY POSTURE

Exactly how strong is your organization's cybersecurity strategy? How secure your business' software and hardware assets, networks, services, and data are, determines your cybersecurity posture. This also includes:

- **Internet Vulnerability**
- **Defense capability**
- **Recovery ability**

Understanding Risk & How to Defend Against It

As cyber threats and hackers continue to advance, in numbers and sophistication, it's now more important than ever to have a clear vision of your organization's cybersecurity posture. Here are the steps for evaluating the maturity of your cybersecurity posture and identifying your business' needs and objectives.

1. Business Critical Resources

What can't your business function without? Determine the intellectual property, data, and business functions essential to your everyday operations. You must know what needs protecting to be able to provide the best defense.

2. Define Your Priorities

Your business-critical assets need to be identified and protected properly to ensure minimal disruption in case of an attack. Less important assets may not need the commensurate level of cybersecurity.

3. What is Your Risk Appetite?

Your organization's risk appetite is partly informed by agreed strategic objectives. What level of risk will your business willingly assume to achieve your defined goals and what are the areas where you need to be more conservative to protect business continuity?

4. Employ a Framework for Cybersecurity

Your framework needs to:

- **Implement cybersecurity processes and programs aligned company wide**
- **Increase resilience of infrastructure and security**
- **Effect processes with assessable value**

Guidelines, standards, policies and processes are all a part of your framework that aligns with your security requirements and business perspective.

5. Evaluate Your Cybersecurity Controls

It's essential to assess your safeguards and controls, check for gaps and ensure you are compliant with required regulations. Any gaps need to be addressed as a part of your framework.

6. Check Your Exposure

Assess whether your critical functions and data are exposed to cyber threats via the internet and deploy appropriate security measures to protect against an attack.

ATTACK TRENDS IN 2020

Exploiting the Global Crisis

Threat activity has risen during the global crisis as more people are working and communicating online. Using malicious domain names like "coronavirus," "vaccine," "chloroquine" and "remdesvir," they aim to distribute spam and malware, and harvest personal data.

Remote Workers Vulnerability

With the huge shift to remote working, attackers have grabbed the opportunity to exploit. With the quick transition and companies taking time to fully equip workers and shore up security, attackers have concentrated on penetrating unsecure networks.

Browser Vulnerability

Attacks through browsers increased with the surge in remote working. Individuals have been targeted using web-based malware in phishing scams, these attacks were more common than their email counterparts.

Ransomware Attacks

Ransomware attacks have been relentless, hiding ransomware in messages with COVID themes, and expanding to exploit Remote Desktop Protocol (RDP) and posting data on public spaces threatening exposure if the ransom is not paid.

KEY STATISTICS

Data Breaches

- Hackers attack on average 2,244 times a day, every 39 seconds.
- The lifespan from breach to containment the average lifespan is 314 days.
- 5% of organization' folders on average are appropriately protected.
- Hacking was 52% of breaches, malware featured in 28% and phishing/social engineering 32–33%.

Where Do Cyberattacks Come From?

- Internal actors were involved in **34%** of data breaches.
- IoT devices encounter **5,200** attacks a month on average.
- Office files account for **48%** of malicious email attachments.

Who is Affected?

- SMBs account for **43%** of breach recipients.
- Smaller businesses (1–250 employees) are the most at risk for targeted malicious email rate at **1 in 323**.
- The industry with the highest number of attacks by ransomware is the **healthcare industry**.

Are You at Risk?

- **53%** of companies had over 1,000 sensitive files open to every employee.
- On average, every employee had access to **17 million files**.
- Only **5%** of folders properly protected.

Counting the Cost

- Data breaches on average cost **$3.92 million**.
- Malware attacks on average cost organizations **$2.6 million**.
- Ransomware attacks on average cost **$133,000**.
- Per record stolen it's an average cost of **$150**.
- Damage linked to cybercrime is predicted to reach **$6 trillion annually by 2021**.

A SMARTER SECURITY SOLUTION TO MANAGE THE FULL THREAT LIFECYCLE

When properly implemented and integrated, a standards-based threat management solution can provide the following critical business outcomes:

Transparency

Uncovering all connected devices and providing an open book solution

Speed

Automation increases speed to action

Consistency

Prescriptive action increases consistency

Quality

Enriched investigation results in higher quality

Collaboration

Joint development of security maturity roadmap and execution

Governance

Routine advisory service and continuous optimization

LRS IT Solutions' Threat Management Services

provide an end-to-end, integrated threat management program that provides services across each phase of the NIST cybersecurity framework:

1. Identify

- Asset discovery
- Device Mgmt
- AD Assessment
- Risk Assessments
- Identity and Access Management
- User Awareness Training/Testing
- Vulnerability Assessment

2. Protect

- Vulnerability Management
- Patch Management
- Policy, Standards & Procedures
- Configuration Management
- Access Control – AD

3. Detect

- Managed SIEM
- Email Security
- Advanced Threat Protection
- Internal/External Penetration Test
- Log Management

4. Respond

- Incident Response
- Managed SOC
- Network Forensics
- Threat Hunting

5. Recover

- Incident Remediation
- Disaster Recovery

LRS SECURITY SOLUTIONS

CONTACT US TO SCHEDULE YOUR FREE CONSULTATION

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