SECURITY RISK MANAGEMENT

for M&A

FORTRESS
SECURITY RISK MANAGEMENT
A Division of **MCPc**

SECURITY RISK MANAGEMENT
for M&A

Fortress has established a robust security risk management practice and developed an attractive and affordable security risk assessment program for mergers and acquisitions.

According to McKinsey, an additional technology risk that is often overlooked is cybersecurity. Acquirers need to do their homework on the target's history of cyberattacks as well as evaluate the strength of the target's cybersecurity defenses to determine if there is higher than expected risk of an attack or breach in the future. Smaller target companies are often less sophisticated than their acquirers, leaving them more vulnerable to cyberattacks. From the announcement of a deal to the close, the frequency of attacks typically increases by ten to 100 times. Hackers seek to exploit temporary vulnerabilities that can appear as organizations bring their IT environments together, including using previously compromised systems as launchpads into the combined company's environment, leading to significant financial and reputational damage. Once a deal is announced, target companies are often reticent to do any further digging into their cybersecurity vulnerabilities for fear of jeopardizing the transaction—making rigorous examination of cybersecurity risks even more important*.

Our M&A Security Risk Assessment Program helps acquiring organizations understand and identify the security risks inherent in the target company as well as reveal the cyber risk issues associated with the IT integration of a new, often smaller business into a larger enterprise.

Enterprises going through M&A reap the benefits of new products and other assets, but also acquire the liabilities, threats, risks, and technology debt. Without a clear understanding of the threats that the organization is inheriting, the business valuation may be flawed, and go-to market strategies may be negatively impacted.

This assessment is designed for client organizations seeking a rapid cybersecurity analysis and covers five core security domains, each of which is mapped to compliance, security and industry frameworks. This methodology gives focus around current data protection capabilities, and the soundness of current protection and detection capabilities. These areas are often the highest risk to the acquiring organization.

* **Source:**
https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/how-to-find-and-maximize-digital-value-in-any-ma-deal

1. Data Protection

Evaluation of the data protection framework and capabilities to determine whether adequate data classification, data loss, and identification capabilities exist to define sensitive information assets. Data storage and external data transfer mechanisms are also reviewed.

2. Identity & Access Controls

Review identity & access controls, policies, and procedures to assess whether suggested security controls appear to be leveraged to reduce the risk of inappropriate access to sensitive data. Onboarding and termination procedures are also reviewed to ensure proper data access controls are enforced.

3. Incident Detection & Response

Review the existing people, processes, and technologies deployed to detect, analyze, escalate, respond to, and contain advanced attacks.

4. Network & Application Security

Review protection mechanisms, policies, processes, and configurations deployed throughout the network and endpoints to ensure that effective controls are in place to prevent compromise. Email and web filtering, IPS/IDS, remote access tools, monitoring capabilities and other technologies are reviewed to determine maturity and level of protection.

5. Endpoint Security

Review security of endpoints (laptop, desktop, server, tablet, smartphone) to determine the effectiveness of operations to maintain, defend, monitor, and protect these devices from attack.

Report findings inform decisions on whether initiatives to connect the businesses should continue or if additional remediation/mitigation efforts are required before the target company can be acquired.

Full-Spectrum Cybersecurity Protection

Fortress SRM is a nationwide team of over 200 cybersecurity professionals with exceptional expertise from the Fortune 500 to middle market – senior cybersecurity leaders & consultants, security architects, analysts and engineers, incident response and remediation experts, digital forensics specialists, governance, risk & compliance (GRC) experts, cyber attorneys, and cyber insurance experts. Fortress has strong partnerships with FBI Cybersecurity Teams and the Cybersecurity and Infrastructure Security Agency (CISA), threat hunting firms, law firms and insurance providers to help clients with incident response intelligence in the event of an attack.

Security Consulting

Assessments

- Framework Assessments
- M&A Cyber Due Diligence
- 3rd Party Vendor Risk
- Technical Testing
  - Penetration Tests
  - Vulnerability Scans
- Regulatory Compliance

Program Development

- Virtual CISO
- Multi-Factor Authentication
- GRC Advisory
- Identity & Access Management
- Threat Management
- Training / Phishing Tests

Incident Response Preparedness

Managed Security

Managed Services

- Cybersecurity-as-a-Service
- **Guardian** Managed Patching
- **Sentinel** Endpoint Detection & Response (EDR)
- **VantagePoint** Managed SIEM
- **Vault** Managed Backup
- **Frontline** Help Desk

* Monitoring & Management via wholly owned 24/7/365 U.S. Security Operations Centers

Incident Response

Full-Service IR

- Contain & Control
- Assess & Analyze Attack Impact
- Threat Elimination & Disaster Recovery
- Digital Forensics & Investigation
- Litigation Support
- Remediation Services
- Crisis Project Management
- Post Incident Assessment & Improvement Roadmap