RMI Risk Masters International LLC

Cyber Impact and Strategy Analysis

Senior management often has two questions regarding cyberattacks: How would cyberattacks affect our organization and what should we do about them? Business Impact Analyses, as they have been performed for decades, are inadequate. The determination of RTO and RPO may be meaningless in the face of stolen information and ransomware attacks that reflect what business leaders would *like* to be done rather than what IT *can* do. Moreover, new government rules require analysis and disclosure that necessitate an understanding by executive management of what the impact of a cyberattack would be if an attack were to occur. This one-day seminar/workshop, combining instruction with a hands-on case study, presents practical methods for understanding the potential impact of cyberattacks, as the basis for remediation, reporting and recovery.

Intended audience: Management and staff in Information Security, Business Continuity Management, IT Auditing, Risk Management, Finance, Office of General Counsel

Learning objectives: Participants in this seminar will learn:

- How cyberattacks change the context of Business Impact Analyses
- The differences in effects of different types of cyberattacks
- How to conduct a Cyber Impact Analysis
- Different techniques to develop cyberattack recovery strategies
- How IT can shorten the time needed for recovery
- Including insurance in cyber resilience strategies
- How to plan for resilience over the longer term

Seminar Outline:

A. The Context of Cyber Impacts
    a. Different types of attacks, different impacts
        i. Theft of information
            1. Personally identifiable information (PII)
            2. Secrets
            3. Digital resources
        ii. Attacks on data integrity
            1. Ransomware
            2. Destructive attacks
        iii. Inability to perform business activities
            1. Untrusted information
            2. Lost or unavailable data
    b. How the impacts would be felt
        i. Financial
        ii. Sales
        iii. Operational
        iv. Reputational
        v. Regulatory
        vi. Societal
    c. Case study exercise #1

B. Why Traditional Business Impact Analyses Are Inadequate
    a. Planned vs. actual variance
    b. Emphasis on premises, personnel and equipment
    c. Lack of meaningful metrics
    d. Do Business Impact Analyses still make sense

C. The Cyber Impact Analysis Process
    a. Scope and objectives within the cyberattack cycle
        i. Awareness through post-recovery
        ii. The “Danger Zone”
    b. Planning
        i. Top-down versus bottom-up
    c. Research
    d. Data gathering
        i. IT view of impacts
        ii. Business view of impacts
    e. Analysis
        i. Leading to strategies
        ii. Categorization
            1. Data theft
            2. Critical application unavailability
    f. Reporting
        i. Obtaining buy-in for needed changes
    g. Case Study exercise #2

D. Strategies to Mitigate Business Impact of Cyberattacks
    a. Dependency-based strategic approaches
        i. Cash flow and capital
        ii. Human resources
        iii. Information
        iv. Technology
        v. Systems
        vi. 3rd parties
        vii. Equipment
    b. Business process-based strategic approaches
        i. Procure to Pay (P2P)
            1. Financial systems
            2. Alternate SaaS applications
        ii. Order to Cash (O2C)
            1. Contingent arrangements
            2. Co-opetition
    c. Case Study exercise #3

E. Strategies to Shorten System Recovery Times
    a. Digital Forensics and Incident Response (DFIR)
    b. Cyber health check
    c. Scanning software and data
    d. Retention of backups
    e. Practice
    f. The Human Factor

F. Cyber Insurance to Mitigate Cyber-Related Losses
    a. Cyber insurance concepts
    b. Cost and coverage
    c. Policy complexity
        i. Cyber Liability vs. Cyber Breach insurance
        ii. First Party vs. Third Party insurance
        iii. Other cost factors

G. Long-Term Cyberattack Mitigation Strategies
    a. Cyber-response governance
    b. Specialized personnel
    c. Zero Trust Architecture
    d. Threat intelligence
    e. Artificial intelligence

H. Conclusion

Seminar logistics: This is a one-day seminar/workshop (8 CPE hours). Because of the intensive case study workshop, the seminar attendance should be limited to approximately 35 people.

Contact:

Steven Ross, Executive Principal, stross@riskmastersintl.com, (917) 837-2484

Allan Cytryn, Principal acytryn@riskmastersintl.com (201) 569-5623