Risk management – protecting assets, practice of identifying potential risk

Cybersecurity risk management – rely on strategies, and user education to protect enterprise against cybersecurity attacks

Basic steps of risk management

1. **Characterize the system**
    a. What it is
    b. What kind of data
    c. Who is the vendor
    d. Who uses the system
2. **Identify threats**
    a. Unauthorized access
    b. Misuse of information
    c. Data leakage
    d. Loss of data
    e. Disruption of services or productivity
3. **Determine inherent risk and impact**
    a. **High** – substantial
    b. **Medium** – damaging but recoverable
    c. **Low** – minimal
4. **Analyze the control environment**
    a. **Risk management control** – set of methods by firms to address the threat, take action to reduce the threat
    b. **User provision control** – ensure user account are created, given permission, and deleted
    c. **Administration control** – policies and procedures
        i. Training
        ii. Restricting access
    d. **User authentication control** – user identity and credentials
        i. Username
        ii. Password
    e. **Infrastructure data protection controls** – safeguard sensitive information
        i. Antivirus
        ii. Security audit
        iii. Spam solution
    f. **Data center physical and environmental security control** – measure taken to protect system, building, and infrastructure
        i. Access control
        ii. Surveillance

g. **Continuity of operations control**

Control assessment categories

Satisfactory – meets control objective

Satisfactory with recommendation – meets control objective but with observation

Needs improvement – partially meets control objectives

Inadequate – does not meet control objectives

5. **Determine likelihood rating** - frequency or probability
    a. **High** – threat source is highly motivated
    b. **Medium** – threat source is motivated
    c. **Low** – threat source lack motivation

Value	Percent	Description
0	0%	Not present
1	10 – 50 %	Rare
2	50 – 90 %	Possible
3	50 – 90 %	Likely
4	90 – 100%	Almost certain to certain

6. **Calculate the risk rating** – determine whether or not it is safe enough to continue with the work

Impact * likelihood = risk rating

Severe – significant and urgent

Elevated – visible threat

Low – threats are normal but still has impact

5 categories of cybersecurity risk assessment

1. Strategic – adverse business decision and operation
2. Reputational – related to negative public opinion
3. Operational – loss resulting from inadequate process
4. Transactional – problems related to service or product delivery
5. Compliance – violation of laws, rules and regulations, non compliance

Risk monitoring and response

Monitoring of cyber risk management – board level involvement to set the tone and priorities around cybersecurity risk

4 key functional areas

1. Alignment – whole organization, horizontal and vertical
2. Data – event detection
3. Analytics – indication driven approach to pattern detection approach
4. Talent – from reactive to proactive action models

Addressing the alarming level of cyber risks

1. Start by understanding and addressing common pitfalls
    a. **Delegating problem to IT/CISO** – cyber risk are treated as technical issues and leaves it for the IT to handle
    b. **Throwing resources to the problem** – organization purchase malware detection systems even it doesn't suit the company's needs
    c. **Treating the problem as compliance issue** – traditional response of blindly following checklist has proven inadequate

Other reasons why cybersecurity often breaks down in companies

- Does not have an inventory of digital assets
- Does not identify who is most likely to come
- Does not resolve system vulnerabilities
- No security plans
- Employees are not oriented and trained

2. Device a more proactive, collaborative approach
    a. Treat it as risk management issue
    b. Addresses within a business context
    c. Dealt with on multiple levels
    d. Calls for adaptive defenses
    e. Calls for collaborative governance

Processes for security incident handling

1. Prepare for handling incidents
2. Identify potential security incidents through monitoring documents and all incidents
3. Asses identified incidents for mitigating the risk

4. Respond to incident by containing, investigating, and resolving
5. Learn and document key takeaways from every incident

Best practices for security incident management

1. Develop a security incident management plan
2. Establish an incident response team
3. Develop a comprehensive training program
4. Perform a post-incident analysis to learn from success and failures

Incident documentation – documenting all workplace injuries, near misses, and accidents. Should be completed at the time an incident occurs

What is considered an incident

- Causes interference to an organization
- Causes significant risk that could affect members within organization
- Impacts on the systems and operations of workplace
- Attracts negative media attention