UNIT V

SECURITY ASSESSMENT

Information Risk Reporting

What is a cyber risk report?

A cyber risk report details information about potential risk within an organization's digital footprint and vendor ecosystem. Cyber risk reports may also identify gaps in security controls and outline the performance of security programs.

A cyber security risk assessment report pinpoints areas in an organization that are vulnerable to a cyber attack. These areas can include networks, computers & laptops, mobile devices, databases, servers, and other types of company assets. The assessment details how these devices could be targeted and the type of damage that could be done to both the organization's data and its reputation in the event of an attack.

The purpose of a cyber security risk assessment report is to educate company stakeholders about the potential threats the organization could face and the type of mitigation efforts that would need to be in place in order to deal with those threats.

Why is managing cyber risk so much more complex today than ever before?

Start with the explosion of cloud services and third-party vendors contacting sensitive data. A Ponemon Institute study estimates the average company shares confidential information with 583 third parties. IT security teams have their hands full, managing complex infrastructures full of vendor risk.

Meanwhile, organizations face a growing number of laws and regulations that govern how confidential data must be protected. Today's enterprises are held accountable for third parties processing data on their behalf. As if handling your own risk wasn't challenging enough, today's organizations must also manage vendor risk.

What is Cybersecurity Risk Management?

Cybersecurity risk management is an ongoing process of identifying, analyzing, evaluating, and addressing your organization's cybersecurity threats.

Cybersecurity risk management isn't simply the job of the security team; everyone in the organization has a role to play. Often siloed, employees and business unit leaders view risk management from their business function. Regrettably, they lack the holistic perspective necessary to address risk in a comprehensive and consistent manner.

Each function has its agenda, often with limited understanding and empathy for others. IT leads with fresh ideas and new technologies, often viewing security and compliance as annoying roadblocks to progress. Security knows safety but is often out of touch with regulations and evolving technologies. The sales team is looking to keep their customers happy, clamoring for an efficient way to complete security audits.

Compliance wants to keep everyone out of trouble with strict adherence to regulations, often operating without an in-depth understanding of security.

Effectively managing cybersecurity risk requires all functions to operate with clearly defined roles and be tasked with specific responsibilities. The days of siloed departments stumbling along in disconnected confusion are over. Today's risk landscape requires a unified, coordinated, disciplined, and consistent management solution. Below are some key risk management action components all organizations must keep in mind:

- Development of robust policies and tools to assess vendor risk
- Identification of emergent risks, such as new regulations with business impact
- Identification of internal weaknesses, such as lack of two-factor authentication
- Mitigation of IT risks, possibly through training programs or new policies and internal controls
- Testing of the overall security posture
- Documentation of vendor risk management and security for regulatory examinations or to appease prospective customers