Cyber Security Risk Management

Cybersecurity risk management is the process of identifying cybersecurity potential risks facing the organization and prioritizing and planning defenses to avert those risks. **Cybersecurity** risk management applies a comprehensive strategy to deliberately accept, avoid, mitigate, and transfer risks.
Good cybersecurity risk management programs enable businesses to prioritise risks and apply the right kinds of security controls to actively minimise the impact of risks. In this article, we help you understand the best practices in developing such a program and effectively protecting your organization.

Cybersecurity Risk Management: The Best Practices

1. Know Your IT Environment and Assets

It is a must to have comprehensive knowledge of your organization's IT environments and assets for effective cybersecurity risk management. How do you secure critical assets or gateways that you do not know exist?
Scope of IT environment that your organization needs to know includes all data and other digital assets, BYOT devices, networks, systems, third-party components and services, technology, endpoints, and so on. You must continuously monitor the IT environment and keep prioritizing your assets. This way, you can accord more resources and more closely guard your most valuable and business-critical assets.

2. Develop a Robust Cybersecurity Risk Management Strategy

Engaging in risk management without a well-thought and robust cybersecurity risk management strategy and plan can be detrimental. So, organizations need to develop a proper strategy and plan and keep updating them. You must identify your risk tolerance and develop a risk profile before strategizing. Include incident response and escalation plans, the role of employees and other key stakeholders, etc. in your risk management plans.

Develop best practices for employees to follow and integrate employee training into your strategy. This is because humans are often the weakest links in cybersecurity. They can accentuate cybersecurity risks massively through avoidable errors such as clicking on an unknown link or accessing the company account on an unsecured network. Incorporate ways to make cybersecurity everybody's responsibility in your strategy itself.

3. Embed Cybersecurity Risk Management into Your Culture and Values

It is pointless to develop cybersecurity risk management programs and procedures if it is not properly implemented across the organization. So, document your strategies, plans, and procedures and communicate them to all stakeholders. Embed cybersecurity risk management into the organization's culture and values. Every stakeholder must be aware of and understand their role in managing **cyber risks**.

4. Risk Assessments Must be Adaptive, Continuous, and Actionable

One of the most important aspects of risk management is risk identification and assessment. Cybersecurity risks are continuously evolving. New technologies may be introduced, or business processes may change. The risk posture of the organization changes as a result. So, the processes must be regularly reviewed for gaps and updated for effective security. This is possible only if the **risk assessments are continuous and adaptive**.

Risk assessments only tell the organization where vulnerabilities exist, what threats are emerging, and so on. It is through the cybersecurity risk mitigation processes that organizations secure their IT environments and invaluable digital assets. For risk mitigation to be effective, risk assessments must provide actionable insights.

5. Enforce Strict Security Protocols

Comprehensive and intuitive security is necessary for effective risk mitigation. Here are some ways to do it:

- Employ an intelligent and managed Web Application Firewall like **AppTrana** placed at the edge of the network. It should monitor traffic, provide actionable, real-time insights, and round-the-clock security against known and emerging threats.
- Employ automated patching where possible.
- Enforce strict authentication policies and access controls.
- Extend security to all devices in your IT environment including BYOT devices.
- Enforce strict security protocols for remote workers as well.
- When possible, consolidate systems and data into one source as scattered and siloed data

are harder to monitor and protect.
• Backups and updates are indispensable.

6. Real-time and Reliable Visibility is Necessary

Cybersecurity risks are evolving and everywhere – within the organization as a trusted insider, a third-party component that has inbuilt vulnerabilities, avoidable human errors, and so on. Real-time and reliable visibility into the dynamic risk profile of the organization is a must. When cybersecurity risk mitigation is based on real-time insights, it is most effective.

Conclusion

The threat landscape is growing continuously, vulnerabilities keep multiplying, technology keeps evolving, the business processes change and so do the risks facing the organization. Given the budgetary and time constraints, total protection from all these risks is simply unattainable. Therefore, a continuously evolving cybersecurity risk management program that is designed using the best practices is indispensable for all organizations.