Strengthening Business Resilience Through Proactive Cyber Risk Management

Dr.M. Irshad Ahamed, E.G.S. Pillay Engineering College, Nagapattinam, Tamil Nadu, India. irshadahmed@egspec.org

Introduction

In today's environment of digital infrastructure driving almost every business activity, the issue of cyber risk has shifted from being a purely technical aspect to becoming a key element of business resilience. Companies can no longer afford to approach cybersecurity as a secondary concern or something to address only out of obligation. Rather, cyber risk management needs to be incorporated into all aspects of planning, operations, and organizational culture. Business resilience – an ability to plan for, withstand, and recover from disruptions – relies increasingly on the degree of successful management of cyber risk prior to the occurrence of the event. This paper addresses the importance of proactive cyber risk management for business resilience, analyzes the methods for achieving this goal, and provides practical recommendations.

Why Reactive Security Is No Longer Sufficient

For years now, many organizations have been reacting to cybersecurity risks by simply installing antimalware software and applying patches after vulnerabilities have been discovered. The old thinking behind such an approach is that the threat remains stable for a long time, and once security measures are put in place, they will protect the organization indefinitely.

Today's cyberthreats are flexible, well-funded, and may even have the same levels of sophistication as a regular enterprise. Cyber criminals who specialize in ransomware use affiliate programs. Nation states employ prolonged reconnoitering operations. And criminal organizations sell credentials stolen in data breaches on dark web forums within hours. In this context, being reactive is to be consistently lagging behind an opponent and feeling the consequences of the attack to its fullest extent.

A reactive approach to security will also prove expensive. The cost of the negative impact caused by a breach, which includes fines, customer loss, liability, and cleanup costs, always outweighs the cost of prevention. Research carried out by reputable cybersecurity organizations shows that the cost of a data breach has been increasing every year, with a growing disparity between the cost of prevention and breach costs. This means that resilience is more than the ability to recover from a breach; it is the ability to avoid such breaches entirely.

Defining Proactive Cyber Risk Management

Proactive cyber risk management refers to the continuous identification, assessment, and mitigation of cyber risks to ensure that they do not pose a threat. The organization should focus more on how to prevent the threat, detect the problem early, and contain the effect of the threat rather than focusing on how to address the threat after it has occurred.

Key Components of a Proactive Approach Include

Continuous Risk Assessment: Instead of performing risk assessments annually or biannually, resilient organizations perform risk assessment as a continuous activity. This means keeping an updated list of all the digital assets, knowledge about the threat environment concerning the specific industry and geographical location of the business entity, and periodic analysis of probabilities and impacts of different threat scenarios.

Threat Intelligence Integration: Companies which are proactive in their approach are capable of investing in capabilities that would enable them to know about attack vectors which can be employed against them and how the attackers may be planning to target their environment.

Vulnerability Management: Vulnerability identification and remediation through an organized and prioritized process rather than a cyclical patching schedule greatly decreases the attack surface that is exploitable by the adversaries. Such a process would include not only patch management but also configuration management, third-party risk management, and cloud security posture management.

Security by Design: Incorporating security aspects into the very beginning of system design and software engineering, as well as business process engineering, is far less costly and damaging than applying security to existing systems.

Scenario Planning and Tabletop Exercises: Through realistic simulation of attack scenarios, leadership and technical staff can find gaps in their ability to respond to an incident before they have to face any real threat.

The Governance Dimension: Risk Management as a Board-Level Priority

Cyber risk management will not be effective as an isolated IT function. To be truly resilient, there needs to be as much focus on cyber risk as on other risks, like financial, legal or operational risk meaning they need to be visible and actionable in the context of the boardroom.

This change has come about faster in the past few years because regulators in many countries have put rules in place for board responsibility for cybersecurity, disclosure of significant cyber incidents, and cyber risk governance. Organizations that look at these rules as a mere formality do not grasp the

significance of this change, which is that board members who understand cyber risks will make better decisions and be better equipped to handle any crisis situation. Effective governance structures typically include:

- An explicit risk appetite statement which describes how much cyber risk the organization is ready to take on to achieve its objectives.
- Reports provided regularly by the CISO or equivalent position to the board in terms of business-related metrics and not just technical language.
- Risk Committees comprising IT, Legal, Compliance, Finance, and Operations staff in order to assess risks comprehensively.
- Accountability framework clearly outlining which individuals own which elements of the cyber risks.

Building Resilience Through Layered Defense

A proactive risk management strategy is best suited for a defense in depth structure. There will never come a time where any security control, regardless of its complexity, will be able to protect against all threats. It would therefore be wise to implement layers of protection, and if one layer fails, another one comes into play.

A resilient security architecture typically includes:

1. **Perimeter and network security** — Firewall, Intrusion Prevention and Detection System, and Network Segmentation to limit the lateral movement of an attacker in case of the first penetration.
2. **Endpoint protection** — endpoint detection and response (EDR) software that looks for unusual activity on each individual machine.
3. **Identity and access management** — multi-factor authentication, least privilege access controls, and privileged access management can be used to lower credential compromise risks.
4. **Data protection** — Encryption while at rest and while in transit, data loss prevention solutions, and solid backup systems that have been thoroughly tested and secured against ransomware attacks.
5. **Detection and response capabilities** — Security information and event management (SIEM), security operations center (SOC) monitoring, and comprehensive incident response strategies.

This approach of combining these defenses serves two purposes: first, it decreases the likelihood that a hacker can successfully break through the defenses; second, it buys valuable time during which the security professionals can catch the intruder.

The Human Element: Culture as a Resilience Multiplier

Resilience can't be achieved solely via technology. The human element continues to be among the most prevalent causes of breaches, including through vulnerabilities such as susceptibility to phishing scams, misconfiguration, and bad password habits. Creating a resilient organization, then, necessitates building a culture where security is regarded as everyone's job instead of being something only the IT folks handle.

Security awareness training, accessible channels for reporting threats, and senior-level commitment to making security a priority are all necessary steps here. Employees who have an understanding of why things need to be done, not just what needs to be done, will actively help defend their organizations instead of posing an additional risk.

Measuring and Communicating Resilience

An important but frequently underappreciated element of proactively managing risk is measurement. For a company to determine whether its efforts to increase its resilience are effective, it must have relevant metrics in place. Such metrics can include MTTD (mean time to detect) and MTTR (mean time to respond) for security incidents, percentage of vulnerabilities addressed within specific time frames, results of phishing simulations, and results of tabletop exercises and red team operations.

In addition, these metrics should be relayed on a consistent basis to senior executives through language that ties security effectiveness to business success, such as potential savings from the reduction of the risk of losses, maintaining regulatory compliance, or protecting customer trust. Figure 1 shows the foundations of a robust security stance, showing the interrelationship between sound governance and oversight by the board, defensive technology, threat intelligence, and security culture.

Figure 1: Key framework at a glance

Conclusion

Proactive cyber risk management is an integral part of business resilience in the digital age. The firms that will treat security only once a threat materializes will remain constantly vulnerable, having to pay unnecessary costs and damaging their reputation in the process. On the other hand, firms that will incorporate the principles of continuous risk assessment, multiple technical controls, effective governance, and a security-focused culture in their activities will have a chance not only to survive but to prosper in a hostile digital environment. The process of becoming resilient is not a one-off project that has a clear end point, but rather a constant practice. Firms that will realize this aspect of business resilience will be better prepared for protecting themselves and their operations.