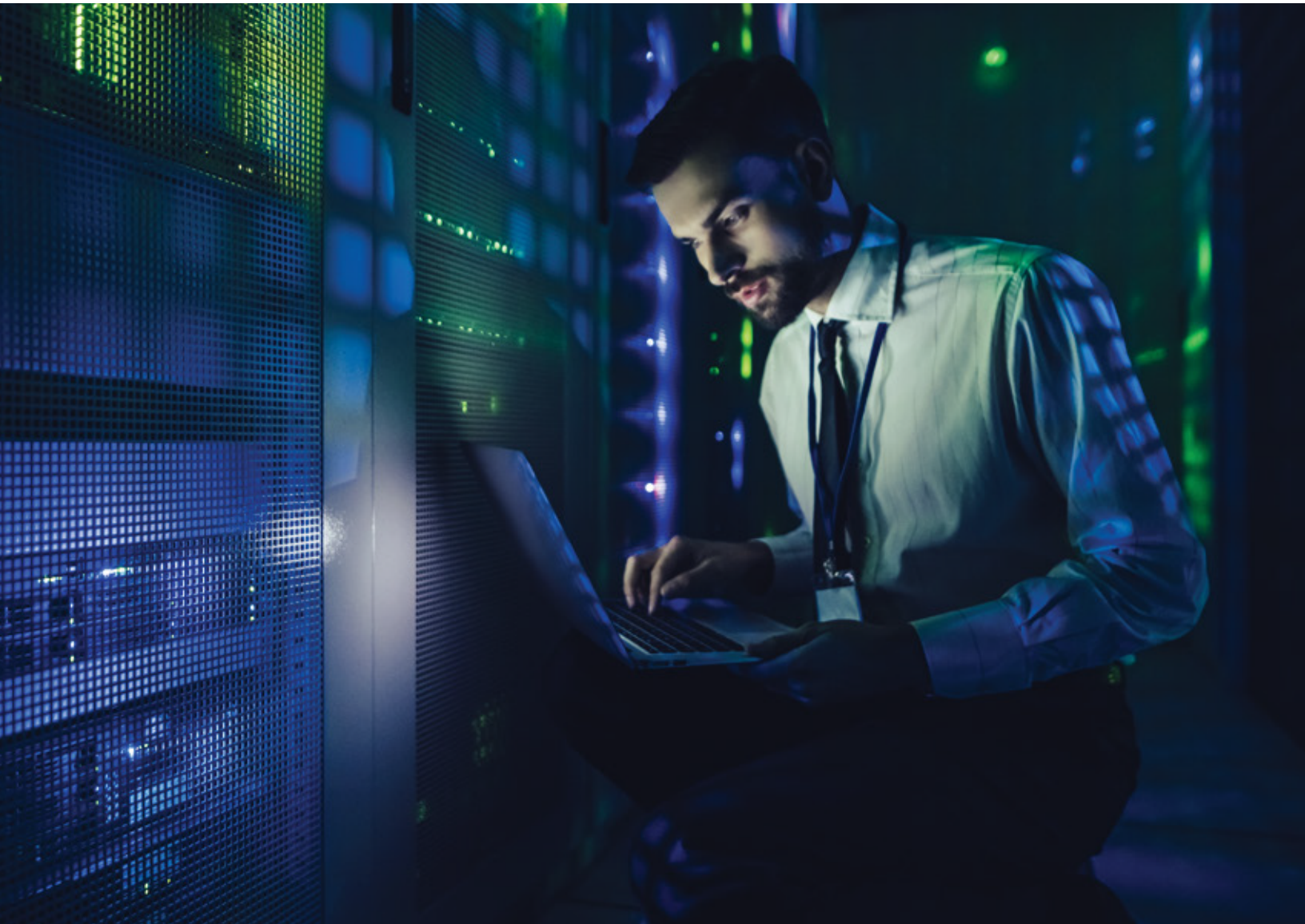
LTIMindtree

POV

The New Essentials of **Cyber Security Management**

Author **Akshata Ghadge**
Project Manager – Cyber Security Practice, LTIMindtree



Most compliance and regulatory guidelines mandate the move to go beyond periodic assessments to a continuous monitoring of their cyber security risk. This puts increasing pressure on a CISO to quantify the maturity and justify the investments made in boosting Information Security. Continuous Cyber Risk Management in real-time is the answer. It portrays the current security and compliance posture, helps prioritize the key focus areas among your assets, identifies most vulnerable technology assets and ensures that adequate measures towards holistic cyber security maturity are adopted throughout the organization.

While your current risk management tools may have worked in the past managing security issues, today they have become expensive posturing in a struggle against adversaries who have evolved to newer modes of attack. Traditional defense systems have inundated security teams with information about the data that passes through their networks, without giving visibility into active threats trying to subvert their networks. Without it, organizations are fending off attacks in the dark with their vulnerabilities exposed. The impacts of a breach can involve data loss, business disruption, brand and reputation damage, and possible regulatory and legal implications.

That's why there's an urgent need for organizations to truly understand their cyber security status and take remedial action. They need to have a complete picture of their cyber security status in order to understand concerns like – What are the current measured levels of cyber security risk? Who will handle it, how will they do it and how much will it cost? What's our prioritized plan to bring these risks down?

Cyber Risk Management Begins @ Board Level

As per NIST, continuous security assessment is defined as "assessed, analyzed and reported at a frequency sufficient to support risk-based security decisions". With boards of over 70% organizations reviewing Cyber Risk and Compliance reports of their IT infrastructure, which is audited once or twice a year, the critical information behind decision making is already stale. In today's time, any Cyber Risk Management Program needs to address this problem by providing near Real-Time reports & Risk posture for informed decision making through accurate and updated information covering 100% of IT assets.

Cyber security requires an evolved and a top-down approach because the type of attacks keep changing and evolving at an incredible rate. The need for improvements and updates is dictated by external influences in the form of software releases, updates, patches, vulnerability alerts, and cyber criminals. Senior management require better reporting and insights which means that security team will need to have latest information available on-demand. Without real-time visibility, making the right decisions quickly will become increasingly difficult.

Organizations also need to respond faster to new threats requiring a security system of continuous improvement, which can help CISO's cope with the quickly evolving and changing landscape of cyber threats.

Cyber Risk Management unifies IT and security teams

In most organizations today, security and IT teams are at odds. Security is responsible for cyber risk, but IT is fielding the burden of work to fix or mitigate. To make matters worse, IT often doesn't have visibility, or get feedback as to the importance of their efforts. When IT and security can share responsibility and unify as a team against cyber risk, an organizations defense against cyber attacks becomes stronger and more efficient. Closed loop verification goes smoother, compliance is easier to validate, and those in IT and security that are actually doing this work will get credit for measurably improving the security posture of the company.

Is there a single source of truth?

In order to have effective risk management processes, organizations need clear visibility into the risks they face and the various related factors that could affect their security posture. This will allow decisions to be made around which risks to accept and where to set the risk tolerance thresholds. While the National Vulnerability Database (NVD) is a valuable source of vulnerability information, it only represents one piece of the puzzle and should not be used as the single source of truth when evaluating an organization's security and risk posture. Many vulnerabilities may become known and publicly disclosed prior to NVD publication. Another challenge is presenting the relevant information to C-level executives in a manner which helps to inform decision-making.

The NVD should be considered as a foundation for building a more complete risk profile, and then augmented by layering information on top of the NVD, such as threat intelligence feeds, trends in public reports or online discussions, weaponization data, and third-party and vendor-reported information.

Quantification of Cyber Risk Management

Historically, qualitative risk assessments have been used for cyber risk management due to the lack of past data – a method that doesn't take into account the financial impact of cyber risks.

An effective Cyber Risk Management Program should be able to continuously cover enterprise cyber risk in near real time basis by leveraging data science across vulnerabilities, threat intelligence, trending exploits, business criticality of assets etc.. This helps surface the highest risk exposure prioritizes remediation of gaps/vulnerabilities across the infrastructure and applications at macro and micro-levels. By knowing which risks could have the most severe impact on business/ revenue, organizations can identify their most critical risk areas and pick the weakly deployed controls or metrics to prioritize.

Quantification of cyber risks at infrastructure and application level can help organizations to focus on what matters first rather than trying to solve all the problems in one go. It will help build prioritized focus on remediation issues by using the concept of Security Risk Scoring for every asset. The quantification of cyber risk at technology levels coupled with threat intel and business criticality at every asset level leads to effective management of cyber risks at enterprise scale. The value is driven by security teams maximizing ROI on cyber security spending and setting appropriate budgets.

Risk-based vulnerability prioritization, translated into actions

Cyber Risk Management is the next evolution in enterprise technology risk and security for organizations that increasingly rely on digital processes to run their business. Security teams need to translate cyber risk from the technical into the economic language of business.

An effective Cyber Risk Management program enables organizations to build cyber resiliency, where risk frameworks and quantitative risk scoring mechanisms are designed to prevent and detect cyber threats. Organizations can respond to vulnerabilities in near real time and prioritize them manner to minimize business disruption and financial losses.

It is imperative for organizations to raise the bar whereby they can continuously and proactively map threats to CVEs, and track emerging and trending exploits in the wild which are specifically relevant to the organization. Security measures can then be implemented much before the organization gets hit by the threats.

About the Author

Akshata Ghadge

Project Manager – Cyber Security Practice, LTIMindtree

Akshata is a Cyber Security professional with diverse experience in Information Security Consulting, Risk Management and GRC. She has gained notable success in managing corporate Enterprise Security for broad range of clients across the globe in various domains like Banking & Insurance, Retail, Power & Energy, Research & Education, Telecom & Health Care. At LTIMindtree Akshata is responsible for managing and aligning clients Information Security practice as per industry standards.

About LTIMindtree

LTIMindtree is a global technology consulting and digital solutions company that enables enterprises across industries to reimagine business models, accelerate innovation, and maximize growth by harnessing digital technologies. As a digital transformation partner to more than 700 clients, LTIMindtree brings extensive domain and technology expertise to help drive superior competitive differentiation, customer experiences, and business outcomes in a converging world. Powered by 84,000+ talented and entrepreneurial professionals across more than 30 countries, LTIMindtree — a Larsen & Toubro Group company — solves the most complex business challenges and delivers transformation at scale. For more information, please visit **https://www.ltimindtree.com/.**