The concept of exposure management is emerging as a **transformative force in cybersecurity.**

Unlike conventional methods that often view risk in isolation, exposure management encourages a contextual understanding of threats, situating them within a broader framework of business objectives. This shift is not merely a change in perspective; it's a foundational reimagining of how businesses approach security.

The threats facing organizations today will only continue to grow in number and complexity, demanding commensurate growth in how organizations conceive of cyber risk. No longer can security be siloed within the IT department. Instead, it must be a shared responsibility, with every aspect of the business playing a role in identifying, mitigating and managing risk. This collaborative approach enhances an organization's resilience and serves to foster innovation and drive competitive advantage.

The continued emergence of exposure management has the potential to fundamentally alter the field of cybersecurity and how it's viewed at a business level. We believe the following five projections are not only possible but likely outcomes of that emergence.

Five Strategic Shifts of Exposure Management

01

Organizations will shift towards an all-encompassing view of cybersecurity risk.

02

The concept of "attack surface" will significantly broaden.

03 Cybersecurity risk will transition from subjective to objective evaluation.

04

Cybersecurity strategy will guide operational investments.

05

C-suite executives will prioritize informed cybersecurity management.

01

Organizations will shift towards an all-encompassing view of **cybersecurity risk.**

Today, risk management rests largely, if not entirely, with your IT team. It's a siloed discipline, such that its implications for the core business are not properly aligned with how it's treated at an organizational level.

Furthermore, it also often revolves around point products: solutions designed to address specific security threats as they arise, creating a feedback loop of siloed specialization rather than a holistic view of cyber risk. As point products often fail to properly integrate with one another, the gaps in their cooperation can leave resulting gaps in your security coverage.

To step away from that flawed methodology is to consolidate your risk data and pursue a comprehensive, contextual view of cybersecurity risk. Here are some practical steps you can take towards holistic risk management.

Data Collection and Integration

Create a comprehensive inventory of all your cybersecurity tools and platforms in use across the organization and implement a centralized platform to aggregate risk data from those tools.

Contextual Risk Assessment

Develop a risk assessment framework that considers the broader context of the organization, evaluating the potential impact of risks and prioritizing them accordingly.

Integrated Risk Management

Take a unified view of your risk posture with an integrated risk management platform, enabling real-time monitoring and automated workflows to streamline response and remediation.

Strategic Alignment

Develop executive-level reports that provide a clear, concise view of the organization's risk posture, integrating cybersecurity into business planning.

By following this approach, organizations can achieve a more comprehensive and contextual view of cybersecurity risk, integrating it into core business objectives and enhancing their overall resilience and competitive edge.

02

Your organization's attack surface is far from static. It's changing quickly, and the traditional parameters that once defined it – software and hardware – fail to capture a number of key considerations for any modern security strategy.

As the technology that powers today's businesses becomes yet more interconnected, a given company's attack surface expands along with it. New elements like cloud environments, third-party vendors and a growing list of human factors introduce unique vulnerabilities that organizations can't afford to ignore.

The concept of **"attack surface"** will significantly broaden.

These are some of the many factors that should be considered part of the attack surface.

Beyond Software and Hardware

Recognize that the attack surface extends beyond traditional IT assets. Include considerations for cloud environments, IoT devices, third-party vendors, supply chain partners, human factors and additional critical areas.

Cloud Security

Integrate data from cloud security posture management (CSPM) tools to monitor and manage risks associated with cloud services. Ensure that cloud environments are continuously assessed for compliance and security best practices.

IoT Devices

Incorporate data from IoT security solutions to address the unique vulnerabilities of connected devices. Implement robust monitoring and management practices to secure IoT devices and mitigate potential risks.

Third-Party Risk

Collect and analyze data from third-party risk management (TPRM) tools to assess the security posture of vendors and partners. Regularly evaluate third-party relationships to ensure they meet your organization's security standards and compliance requirements.

Human Factors

Include data from security awareness training programs and phishing simulation tools to understand and mitigate risks associated with human behavior. Foster a culture of security awareness and continuous training to reduce the likelihood of human-related security incidents.

Digital Risk Protection

Integrate data from digital risk protection systems to monitor risks across digital channels, including social media, the dark web and other online platforms, helping to identify and respond to threats such as brand impersonation and data leaks.

By expanding the attack surface to include these additional areas, organizations can achieve a more comprehensive and contextual view of cybersecurity risk, enhancing their overall resilience.

03

Cybersecurity risk will transition from subjective to **objective evaluation**.

The metrics used by security operations teams today don't effectively translate to strategic planning, owing to a lack of universally accepted standards. While security frameworks and standards provide some guidance, they often focus more on what needs to be done rather than how to do it.

Exposure management will lead to more rigorous measurement of decision-making data, while streamlining the output that ends up in front of executives: actionable, objective information that can guide organizations towards their desired security posture.

These are the steps you can take to get there.

Analyze Asset Value

To effectively manage risks associated with your assets, begin by understanding the value of each asset. As part of that analysis, use information specific to your organization – like internal data, risk appetite and unique vulnerabilities – versus general market trends.

Gauge Risk Probability

Next, evaluate the frequency and severity of risks to create relevant scenarios for your organization, helping you understand the probability and potential impact of different risk events.

Categorize By Risk Impact

Assets should be categorized based on their risk profile, using quantitative methodologies like Value-at-Risk (VaR) and Conditional Value-at-Risk (CVaR).

The continued evolution of machine learning will help drive this transition, making precise, real-time risk assessments available to organizations as they make decisions.

Today, cybersecurity is primarily managed by technical specialists who often struggle to effectively communicate their needs to the C-suite. At the same time, while executives are fully aware of the critical importance of cybersecurity, and the risks associated with neglecting it, they aren't always equipped to bridge the knowledge gap between them and their IT/security teams.

This disconnect makes it challenging for any organization to define what constitutes a 'good' and 'reasonable' cybersecurity budget or strategy. As a result, decisions are too often made on the basis of fear or industry trends, rather than informed judgment. That approach introduces misaligned priorities, inefficient resource allocation and a lack of accountability. Taken together, even an organization that believes it's taking the right steps to protect itself can fail to do so.

Cybersecurity strategy will guide **operational investments.**

To meet these challenges, organizations should implement a strategic approach to cybersecurity, integrating operational priorities with performance data. Here's how:

Data-Driven Decision Making

Continuously collect and analyze performance data to determine which activities produce the most meaningful results and which do not provide an adequate return on investment.

Enhanced Communication

Establish clear communication channels between cybersecurity specialists and executive management. This can include regular briefings, workshops and training sessions to bridge the knowledge gap.

Comprehensive Oversight

The broader C-suite should oversee a comprehensive decision-making and feedback loop. This ensures that security initiatives are aligned with business objectives, enabling the organization to right-size investments.

Performance Metrics

Develop and track key performance indicators (KPIs) that measure the effectiveness of cybersecurity initiatives. This will provide a clearer picture of what constitutes a 'good' and 'reasonable' cybersecurity budget.

Foster a Security-Centric Culture

Integrate security as a value-add rather than a cost center. This cultural shift will drive smarter investments and better outcomes.

By implementing these strategies, organizations can make more informed decisions about their cybersecurity investments, aligning them with business objectives and driving better outcomes.

05

C-suite executives will prioritize **informed cybersecurity management.**

Absent shared, legible metrics, cybersecurity risk can't be properly articulated to the executives tasked with making decisions. It falls to the C-suite to effectively guess at the organization's security strategy without being able to objectively measure the results.

There are no reliable processes today that provide objectivity and a direct line to data-driven decisions. Integrating cybersecurity into business strategy thus becomes difficult if not impossible, hindering or preventing a robust assessment of the organization's risk appetite.

Exposure management will enable C-suite executives to cultivate a core competency in making informed, consistent and explainable cybersecurity risk management decisions. Equipped with robust data and advanced analytics, leaders will be able to situate risk in business terms, facilitating better communication and collaboration across the organization.

Achieving this requires not just new capabilities from vendors, but a change in corporate culture and a willingness to revisit decision-making processes. Here's what needs to happen and thoughts on how to approach it:

Establish a Risk Appetite Framework

Define the organization's risk tolerance and align it with business objectives. This framework will guide decision-making and ensure consistency.

Implement Advanced Analytics

Leverage data-driven insights to identify trends, predict threats and measure the effectiveness of security controls with a holistic view towards the risk landscape.

Communicate Risk in Business Terms

Translate technical risks into business impacts to engage stakeholders and drive informed decision-making with a common risk language and legible metrics.

Foster Cross-Functional Collaboration

Break down silos and encourage collaboration between security, IT and business teams, establishing regular meetings and workshops to align efforts.

Regularly Review and Adapt

Make informed decision-making an ongoing process. Regularly review risks, controls and assumptions to adapt to the evolving threat landscape.

ivanti

For more information,
or to contact Ivanti,
please visit ivanti.com.