IBM Security

Risk management that advances zero trust

Risk management that advances zero trust

In today's cyber environment, risk management is no small task. Gone are the days of the firewall as an organization's primary cyber defense. Enterprises today are moving to the cloud, adding new users and devices to their network each week, creating terabytes of data every day, and employing dozens—if not hundreds—of 3rd party software and systems within their IT environment. At the same time, attackers are evolving their methods to capitalize on these changes and also increasing the volume and sophistication of their attacks.

To contend with these trends, business leaders must be able to collect, contextualize and prioritize their organization's areas of risk in order to keep their exposure to a minimum and execute a security strategy based on zero trust principles.

This paper will explain what a modern approach to risk management looks like, and how a zero trust framework can help strengthen an organization's existing risk management strategies or serve as a foundation for organizations that are rebuilding theirs from scratch.

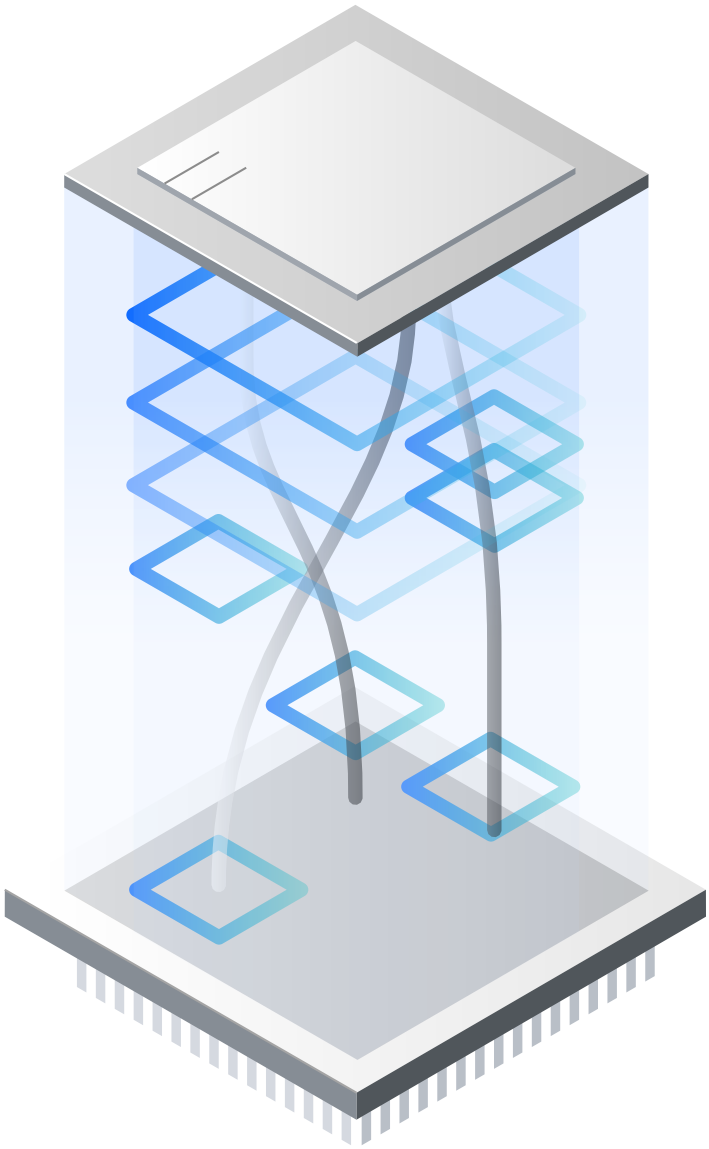
What is risk management?

For many people, risk is subjective. Picture walking the floor of a casino and the range of people you'll see at the tables. At one roulette table you may find a person repeatedly making large bets on the numbered squares—which have a very low probability of success, but come with a high, 25:1 payout. At the same table you'll likely see another person who is more risk-averse, making small or moderate bets on red or black, bets that offer nearly 50:50 odds, but also a much smaller 2:1 payout. The difference between these two people is their willingness or ability to tolerate a financial loss—the amount they bet on that spin of the wheel.

Companies, like people, have their own threshold for risk, which are influenced by myriad factors, such as its place in the market, the degree to which it is insured, its capital structure, the laws or regulations of the jurisdictions where it operates and many, many more. Just like with individuals, companies have their own tolerance for how much of a financial loss they can absorb under certain probabilities. This exposure to a potential financial loss is what we mean when we talk about risk in a business context.

Risk management is about how an organization combines technology, processes, policies and personnel to achieve and maintain an acceptable level of risk in a cost-effective manner.[1] Since a key part of maximizing profit is to minimize losses, all businesses engage in some form of risk management. Yet not all employ a strategic approach, and many can only speculate about whether they are managing risk cost-effectively.

What makes risk management so challenging for today's enterprises?



- Comparing subjective definitions of risk: Security ecosystems consist of a variety of tools designed to protect data, set and enforce user permissions, identify and stop threats, and remediate vulnerabilities, among others. Many modern security tools provide users with a risk analysis. These analyses are subjective, relying on different definitions of risk, using different variables. The difficulty in comparing risk data from different tools can be a significant barrier to understanding an organization's overall risk posture.

- Measuring and quantifying risk: Significant financial and strategic decisions are made with potential risks in mind, however quantifying security risk can be challenging. Assumptions lie at the heart of all risk analyses—assumptions about the probability of a threat event occurring, about the threat exploiting known vulnerabilities to maximum effect, and about the abilities of your defenses to resist the threat. Without a consistent set of assumptions applied across the enterprise, measuring risk accurately in the aggregate is not possible.

- Prioritizing areas of risk for remediation: Without a consistent way to measure, compare and quantify risk, business leaders will rely on intuition to decide which areas of risk to prioritize for remediation. Their intuition—because it's not based on data—may be faulty and lead to financial loss for the company.

- Tracking the effectiveness of remediation and applying learnings over time: As mentioned above, risk management is not just about reducing exposure to loss but doing so in a cost-effective way. Without quantification, business leaders have no realistic way to evaluate their return on investment for the security tools they've deployed or the teams they've assembled. They cannot measure over time the impact of the processes they've established to remediate threats.

[1] "Measuring and Managing Information Risk: A FAIR Approach" by Jack Freund and Jack Jones

What can the zero trust model do for security risk management?

To cope with the changing security landscape, where there is no perimeter and threats can emerge from a variety of vectors, **Forrester Research** created the zero trust framework. At its crux, zero trust is about ensuring that all of an organization's data and resources are inaccessible by default and that they can only be accessed on a limited basis and under the right conditions.[2]

In order to implement the zero trust approach successfully, security leaders need to build an IT infrastructure that weaves together information from across the enterprise to provide the context required to validate whether or not a requested connection is trustworthy.[3] An ideal approach for generating the context necessary for zero trust security is to follow four guiding tenets:

1. **Define context:** Businesses need to understand what users, data and resources are connected across the organization. Defining context includes discovering and classifying resources based on risk.
2. **Verify and enforce:** Every instance where access to a resource is requested, continually require verification and monitor activity to ensure it aligns with permissions.
3. **Resolve incidents:** As threats emerge or changing conditions require the business to adapt and evolve, the organization will need to resolve incidents with minimal impact on business continuity. This includes changing to users, devices and networks, remediating threats, and reporting on compliance
4. **Analyze and improve:** Zero trust is meant to be adaptive; as the nature of threats continue to evolve, and organizations' IT ecosystems adapt to new business needs, security and IT leaders must review and adjust their strategy to match changing realities. This process of continuous improvement should be conducted in a way that minimizes disruption to business continuity.

[2] "Protect your workforce; Grow your business with context-based zero trust," Forrester Research **[source]**

[3] "Protect your workforce; Grow your business with context-based zero trust," Forrester Research **[source]**

Building an effective risk management strategy through a zero trust approach

A zero trust strategy is an effective approach to addressing and prioritizing risk across the organization. For business leaders looking to minimize their organizations' exposure to potential loss, they should focus on connecting information from the security tools already deployed in their IT environment through a unified security analytics platform. Since some of these solutions will come with pre-existing risk analysis features, business leaders should deploy a solution to collect risk data from these sources, normalize the data for easy comparison, and correlate the data to derive insights.

An ideal risk management solution will run the disparate risk data through a common algorithm to provide an analysis explaining the probable impact and magnitude of a risk event. The solution should provide drill-down tools to investigate specific areas of risk as well as integrate with a Security Orchestration and Automation and Response (SOAR) solution to expedite issue remediation with minimal impact on business continuity.

Finally, in the interest of continuous improvement, an ideal solution would show users how risk trends have changed over time as a result of previous remediation tactics. This feedback loop is essential; security leaders would have the visibility needed to determine the effectiveness of their event response actions and make adjustments as needed.

Solutions and services that help manage risks

One such solution is **IBM Security Risk Manager for IBM Cloud Pak for Security**. It empowers security leaders to collect and contextualize risk data from across their security environment. By sourcing risk data inputs from a variety of vectors—including identity and access management solutions, data security solutions, and infrastructure security solutions connected to a **Cloud Pak for Security** instance—and analyzing the inputs using a common risk engine, Risk Manager helps create a more complete image of their risk landscape and provide business leaders the information they need to prioritize and remediate areas of risk. **The solution** presents a unified view of the enterprise's risk to the user in a single dashboard. As part of the Cloud Pak for Security, Risk Manager integrates seamlessly with the platform's other native applications, like Data Explorer and SOAR, further expanding the investigative and issue remediation capabilities of the solution.

As mentioned earlier, quantifying security risk can be a barrier to managing risk, yet communicating risk into financial terms is essential for effective enterprise planning. Security risk quantification also helps provide a clear strategy and roadmap for both security teams and business leaders to implement their zero trust projects. By showing the biggest security impacts for a business, risk qualification can flag risks and liabilities needing to be resolved before implementing a zero trust strategy. With that knowledge in advance, zero trust projects can follow through to insulate a business from anticipated and unexpected risks by requiring validation and authorization for all connections. The end result is enterprise executives get assurance on the security risk from both technical and business perspectives by putting a number to that risk.

To achieve this outcome, you need to connect security risk management with your overall business strategy by integrating security intelligence into quantified business risks and metrics. **Security Risk Quantification from IBM** offers C-level executives a holistic approach for building risk programs that use quantified financial terms.

No one-size-fits-all approach

Each organization is different—with unique business priorities and risk tolerances. Expert risk quantification consulting teams can help your organization understand the true monetary impact of potential threats, prioritize security risks in a contextually relevant manner and convey the return on security investment to the business.

For security leaders seeking to quickly and efficiently minimize their business's risk profile, they need a solution that normalizes and contextualizes risk data, facilitates prioritization and helps them determine the best course of action to reduce overall risk. And since no two organizations are the same, explore the solution that meets the needs of your organization, is flexible and can easily scale with your organization.