The New Enterprise Security Model: Intelligent, Risk-Based Vulnerability Prioritization and Management
# Table of Contents

- Executive Summary 1
- Cyber Security Challenges 2
  - A Growing Attack Surface 2
  - Silo-Based Security Tools 2
  - Manual Data Aggregation and Analysis 3
  - Lack of Context 3
- The New Enterprise Security Model: Cyber Risk Management 4
- The Three Pillars of Intelligent Cyber Risk Management 4
  - Identification 4
  - Prioritization 5
  - Remediation 5
- Implementing an Effective Cyber Risk Management Program 6
- The RiskSense Vulnerability Prioritization and Management Platform 6
  - Attack Surface Validation Service (pen testing) 6
  - The RiskSense SaaS Platform 6
- For More Information 7
Executive Summary

Although today’s enterprises are spending huge sums of money to maintain a security perimeter designed to fend off cyber and insider threats, daily reports of new data breaches are raising doubts about the effectiveness of these investments.

One of the biggest challenges in cyber security is how to efficiently manage the massive volume, velocity, and complexity of data generated by the myriad of today’s IT security tools. Feeds from these disconnected, siloed tools must be analyzed, normalized, and the resulting remediation efforts prioritized. The more tools in the arsenal, the more difficult the challenge for those responsible. This type of security model requires legions of staff to comb through huge amounts of data to correlate and evaluate the potential impact of each identified risk. These efforts often take months, during which time malicious attackers may have already exploited any unidentified vulnerabilities and extracted valuable customer and corporate data.

Rather than adding even more tools to the mix, organizations need to implement a new and more efficient enterprise security model. Cyber risk management solutions that leverage intelligence-driven analytics can help organizations operationalize their cyber security practices, break down silos, and enhance security operations tasks through automation.

This white paper explores this emerging discipline of cyber risk management as a response to the burgeoning number cyber-attacks, advanced persistent threats, and insider leaks. It outlines not only today’s cyber security challenges, but provides practical advice on how to operationalize an organization’s cyber security practices across a growing attack surface.
Cyber Security Challenges

Cyber threats are now one of the most significant business risks facing today's organizations. For many companies, the Target data breach in 2013 was the watershed event and call to action. The hack affected over 41 million customer accounts, just ahead of the holiday season. Not only did the breach cost the retail chain millions of dollars in lost sales, the subsequent lawsuits and settlements totaled in the tens of millions of dollars.

The size and impact of malicious breaches has grown exponentially since then, with events such as the exposure of private data of over 87 million Facebook users in May of 2018, and the personal information of over a billion citizens of India when their Aadhaar numbers (12-digit unique identifier of India's citizens) were disclosed in January of 2018.

The scale and financial impact associated with cyber-attacks continues to escalate. Since boards of directors have a fiduciary responsibility to preserve corporate financial value, these breaches have been a loud wake-up call at the executive level. Meanwhile, the United States courts are increasingly holding businesses accountable for implementing appropriate security practices to protect consumers' personal information. The Home Depot, which had to book $161 million of its pre-tax expenses in 2016 to cover its 2014 data breach, including $19.5 million for the consumer settlement, is a good example of the impact a breach can have on the corporate bottom line.

In response, companies are now spending huge sums of money every year to maintain an ever-expanding security perimeter to fend off cyber and insider threats. According to Gartner Inc., worldwide spending on information security products and services will reach more than $114 billion in 2018, an increase of 12.4 percent from the previous year, and will grow an additional 8.7 percent to $124 billion in 2019. However, mounting security incidents and data breaches of massive scale at supposedly “protected” companies, including Equifax, Under Armour, and Yahoo, are raising doubts about the effectiveness of these lofty investments.

A Growing Attack Surface

Organizations face an uphill battle when it comes to ensuring cyber security, as the attack surface they have to protect has grown significantly over the last several years and is expected to balloon even further. While it was sufficient in the past to focus on just network and endpoint protection, the increasing number of applications, cloud services, mobile devices (e.g., tablets, mobile phones, Bluetooth devices, and smart watches), and the Internet of Things (e.g., physical security systems, lights, appliances, heating and air conditioning systems) represent a broadly extended attack surface. Although the majority of cyber attacks are now targeting the application layer, many organizations and technology vendors are still focusing their attention on just the network and endpoints. Clearly, today's organizations are requiring a more holistic approach to cyber security.

Silo-Based Security Tools

One of the biggest challenges in cyber security is how to manage the volume, velocity, and complexity of data generated by the myriad of IT and security tools used in an organization's network. All of the feeds from these disconnected systems must be analyzed, normalized, and the resulting remediation efforts prioritized. With more tools and a broader the attack surface, the challenge is almost insurmountable. The amount of data analyzed by enterprise information security organizations is growing exponentially. Organizations must now find ways to break down these silos, as cyber-attackers are moving both vertically and horizontally across the entire attack surface.
According to the 2018 Verizon Enterprise Data Breach Investigations Report, most data breaches took just a few minutes or less, only 3% of those breaches were discovered as quickly, and a full 68% went undiscovered for months or more. The Target data breach was a good example. Despite the fact that best-of-breed tools were in place and detected the initial breach, the outsourced security operations team was not able to respond to the alert in a timely fashion. They were simply overwhelmed by the data coming their way and therefore could not decipher this huge impact on the business. Ultimately, the data breach was revealed by an outsider and not by the company's security operations team. By then, it was already a financial and public relations disaster.

Despite 95 percent of CIOs expecting cyber threats to increase over the next three years, only 65 percent of their organizations currently have a cybersecurity expert on board, according to Gartner’s 2018 CIO Agenda Survey. The Gartner survey also revealed that skills challenges continue to plague organizations that undergo digitalization, with digital security staffing shortages considered a top inhibitor to innovation. Unfortunately, there is currently a serious shortage of well-trained IT security professionals. For most organizations, the prospects of hiring all of the staff needed to aggregate, normalize, and analyze the vast amounts of data needed to assess cyber risk exposures are slim. Breaking down existing silos and automating traditional security operations tasks with the help of technology as a force-multiplier is essential, in light of the increasingly scarce cyber security operations talent pool.

**Manual Data Aggregation and Analysis**

Traditional cyber security approaches require significant teams to review all the data to identify and prioritize the most probable vulnerabilities. With limited staff, these efforts can take months, meaning that attackers have already struck and have vanished into the cyber-ether. In fact, the limitations of manual cyber security operations have created a major risk in itself. Relying on manual processes to comb through mountains of data is one of the main reasons that critical issues are not being addressed in a timely fashion by today’s security teams.

According to the 2018 Verizon Enterprise Data Breach Investigations Report, most data breaches took just a few minutes or less, only 3% of those breaches were discovered as quickly, and a full 68% went undiscovered for months or more. The Target data breach was a good example. Despite the fact that best-of-breed tools were in place and detected the initial breach, the outsourced security operations team was not able to respond to the alert in a timely fashion. They were simply overwhelmed by the data coming their way and therefore could not decipher this huge impact on the business. Ultimately, the data breach was revealed by an outsider and not by the company's security operations team. By then, it was already a financial and public relations disaster.

Despite 95 percent of CIOs expecting cyber threats to increase over the next three years, only 65 percent of their organizations currently have a cybersecurity expert on board, according to Gartner’s 2018 CIO Agenda Survey. The Gartner survey also revealed that skills challenges continue to plague organizations that undergo digitalization, with digital security staffing shortages considered a top inhibitor to innovation. Unfortunately, there is currently a serious shortage of well-trained IT security professionals. For most organizations, the prospects of hiring all of the staff needed to aggregate, normalize, and analyze the vast amounts of data needed to assess cyber risk exposures are slim. Breaking down existing silos and automating traditional security operations tasks with the help of technology as a force-multiplier is essential, in light of the increasingly scarce cyber security operations talent pool.

**Lack of Context**

According to Gartner, by 2020, 30% of global 2000 companies will have been directly compromised by an independent group of cyber activists or cyber criminals. This prediction is not surprising, considering the fact that leading risk indicators are difficult to identify when the cyber attacker’s strategy, competences, and actions are all unknown. Many organizations still focus on control gaps and vulnerabilities when performing risk assessments and neglect taking threats into account. Focusing solely on findings from internal security intelligence – including vulnerability scanners, configuration management databases, and SIEM systems – can lead to inaccurate prioritization of remediation actions and inefficient allocation of scarce security resources.

Two conditions are required for a security incident to occur: a vulnerability must be present in some form (e.g., a software flaw or insecure programming; insecure configuration of IT infrastructure; insecure business operations; or risky behavior by internal staff or other people, conducted maliciously or by mistake) and secondly, of course, that threat must be exploited.
Security professionals typically have very little direct control over potential threats. As a result, organizations have tended to focus on the more visible facts and data – including vulnerabilities and control failures – while neglecting potential threats as a major factor in cyber risk assessments. However, as the volume of vulnerabilities, of holes in the armor, has exploded over the past few years, it has become almost impossible to remediate all of them without some system of vetting the impact and likelihood that they will be exploited. The point is, why dedicate resources to fixing vulnerabilities that have very little threat associated with them and are not even reachable?

Since a threat is the agent that takes advantage of a vulnerability, this relationship must be a key factor in the risk assessment process. Advanced security operations teams need the ability to leverage threat intelligence to gather insight into the capabilities, current activities, and plans of potential threat actors (e.g., hackers, organized criminal groups, or state-sponsored attackers) to anticipate current and future threats. Once internal security intelligence is contextualized with external threat data (e.g., exploits, malware, threat actors, reputational intelligence), these findings must then be correlated with business criticality to determine the real risk of the security gaps and their ultimate impact on the business.

The New Enterprise Security Model: Cyber Risk Management

In response to the escalating security challenges, many boards of directors have started shifting their view of cyber security as being just a core function of IT management, and are demanding that C-suites view cyber threats from a strategic, company-wide, economic perspective. These executives are now taking a very active interest in cyber security and demand to be kept informed of current and evolving risks, as well as the organization’s security preparedness level and response plans.

Considering the aforementioned skill and expertise shortage and the increasing frequency and sophistication of threat activities, many organizations are now rethinking their enterprise security model. The objective has to be a move to full and/or semi-automation of operational activities. At the same time, they seek to enable a truly adaptive and risk-based response to advanced threats, which assures continuous, pervasive monitoring and analysis across the entire attack surface, not just the network or endpoints. In this context, intelligence-driven cyber risk management is often seen as the clear path for organizations to operationalize their cyber security practices, enhancing security operational tasks through automation.

Fortunately, new cyber risk management technologies are now emerging that will help enterprises not only aggregate internal security intelligence and external threat data, but more importantly, correlate these data feeds with their business criticality or risk to the organization. The end result is automated, contextualized security metrics that align with business objectives. Besides the operational advantages that cyber risk management brings to the table, it also propagates better collaboration among otherwise siloed stakeholders across the organization, ranging from the board of directors, C-suite, business stakeholders, to security and IT operations teams and internal/external auditors.

The Three Pillars of Intelligent Cyber Risk Management

Effective cyber risk management solutions should be built upon three pillars: identification, prioritization, and guidance of specific remediation actions.

Identification
In order to understand what “act” (remediation action) is needed to minimize an organization’s cyber risk exposure, identification is the first step. With so many organizations being overwhelmed with the volume, velocity, and complexity of internal security data, it has become crucial to streamline the identification process. The gathering of all potentially relevant information is necessary, but the resultant data overload has become the Achilles heel of day-to-day security operations. The intelligence-driven cyber
risk management concept calls for automated aggregation of data across different data types; mapping of assessment data to compliance requirements; and normalization for ruling out false-positives and duplicates and to enrich data attributes.

**Prioritization**

In the past, the majority of organizations focused solely on their internal cyber security posture, and therefore had a difficult time prioritizing their remediation actions based on business criticality. By leveraging emerging cyber risk management tools, organizations can now place internal security intelligence, external threat data, and operational importance into context to derive a holistic view of risk posture. In this way, security teams can determine what imminent threats they face from cyber adversaries, and which ones really have the highest potential impact to the business or mission. They can then “hit-the-ground-running” and direct scarce resources to the appropriate threat.

**Remediation**

Increasing collaboration between security and IT operations teams — with one being responsible for identifying security gaps and the other focused on remediating them — continues to be a challenge for many organizations. The intelligence-driven cyber risk management concept calls for combining workflow, ticketing, and remediation capabilities, the assignment of detailed remediation steps for each vulnerability, and automating real-time risk management.

Using the cyber risk management concept as a blueprint, it's possible to implement automated processes for proactive security incident notification and human-guided loop intervention. By establishing thresholds and pre-defined rules, organizations can guide specific remediation actions to fix the most critical security gaps. Meanwhile, cyber risk management provides a way to measure the effectiveness of remediation actions and ensure risks have been successfully eliminated. The board of directors and oversight committees are especially interested in this assessment. To increase remediation effectiveness, emerging cyber risk management tools can provide this measurement and also develop playbooks that include step-by-step instructions on how to tackle the most critical vulnerabilities.

The intelligence-driven cyber risk management concept also mandates a closed-loop remediation process, which assures that a ticket is only closed once the effectiveness of a patch has been revalidated by an organization's internal security tools. Unfortunately, many organizations close out tickets as soon as they apply a patch without testing to see if it was really effective. This leaves them vulnerable to a big blind spot if the patch fails. To implement this concept, progressive organizations are using cyber risk management software as an overlay to their existing security infrastructures. This approach provides the necessary aggregation, intelligence-based analysis, and orchestration capabilities to identify and respond to cyber threats early in the kill chain.
Implementing an Effective Cyber Risk Management Program

Cyber risk is made up of many factors, including compliance posture, threats, vulnerabilities, reachability, and business criticality. New intelligence-driven cyber risk management technologies are emerging that help to not only aggregate internal security intelligence and external threat data, but more importantly, to correlate overwhelmingly large data feeds with the all-important business criticality to the organization. The end result is automated, contextualized security metrics that align with the enterprise’s business objectives. Organizations can now be provided with a playbook for this serious task.

In addition to leveraging the power of cyber risk management tools, organizations must also implement the following measures to ensure they’re operationalizing security intelligence as effectively as possible:

- Take seriously the ongoing grouping and threat-categorization of assets within the organization to establish a benchmark for determining the business impact of risks and the prioritization of remediation actions.

The RiskSense Vulnerability Prioritization and Management Platform

RiskSense provides a vulnerability prioritization and management solution that dynamically controls and measures cybersecurity risk. The cloud-based RiskSense platform uses a foundation of risk-based scoring and technology-accelerated pen testing to identify critical security weaknesses with corresponding remediation action plans, dramatically improving security and IT team efficiency and effectiveness. The RiskSense vulnerability prioritization and management offerings include an Attack Surface Validation Service (pen testing) and the RiskSense SaaS platform:

Attack Surface Validation Service (pen testing)
RiskSense provides an in-house, AI-assisted penetration testing services and delivered via the RiskSense cloud-based vulnerability management platform that uses domain expertise and data to correlate vulnerability scan data with threat intelligence and asset criticality to measure risk, provide early warning of weaponization, predict attacks, and prioritize remediation activities. The service empowers organizations to dramatically improve how security and IT teams collaborate and take effective action to achieve cybersecurity risk goals.

The RiskSense SaaS Platform
The RiskSense SaaS Platform is the industry’s most advanced and scalable platform that continuously correlates and analyzes comprehensive internal and external vulnerability data, threat intelligence, human pen test findings, and business asset criticality to arrive at a fully informed plan of attack. The platform provides:

- Comprehensive Coverage – contextualized cyber risk picture incorporating internal and external vulnerability data and threat intelligence for all asset classes (network, web applications, databases, and IoT devices) including support for industry-leading scanners and custom data sources.

- RiskSense Security Score (RS³) – similar to a credit score, the RS³ represents an organization’s robustness against cyber risks posed to it from existing vulnerabilities and associated threats. The score considers several factors including vulnerability risk rating, the business criticality of the assets themselves, numerous threat intelligence sources, and external accessibility.

By implementing these measures, organizations can operationalize their cyber security practices to shorten time-to-detection, and ultimately, time-to-remediation of cyber threats.
• **Attack Surface Validation** – pen testing service findings are synchronously presented through the platform.

• **Vulnerability Findings** – provides the ability to prioritize remediation activities with confidence, taking into account severity, business risk, weaponization, proof of compromise and active exploits using data from over 100 independent sources.

---

**For More Information**

RiskSense is dedicated to enabling organizations to identify critical security weaknesses in IT/OT infrastructure and prioritize specific risk-based remediation actions for the benefit of the business, its partners, employees, and customers. For more information on how your organization can implement an intelligent cyber risk management platform, visit www.risksense.com or follow us on Twitter at @RiskSense.

---

**About RiskSense**

RiskSense®, Inc. provides vulnerability prioritization and management to measure and control cybersecurity risk. The cloud-based RiskSense platform uses a foundation of risk-based scoring, analytics, and technology-accelerated pen testing to identify critical security weaknesses with corresponding remediation action plans, dramatically improving security and IT team efficiency and effectiveness. The RiskSense Platform® embodies the expertise and intimate knowledge gained from real world experience in defending critical networks from the world’s most dangerous cyber adversaries. As part of a team that collaborated with the U.S. Department of Defense and U.S. Intelligence Community, RiskSense founders developed Computational Analysis of Cyber Terrorism against the U.S. (CACTUS), Support Vectors Intrusion Detection, Behavior Risk Analysis of Vicious Executables (BRAVE), and the Strike Team Program.