eBook

TREND MICRO™

THE PROACTIVE CISO'S PLAYBOOK

How to Close the Exposure Gap and Manage Cyber Risk with Confidence

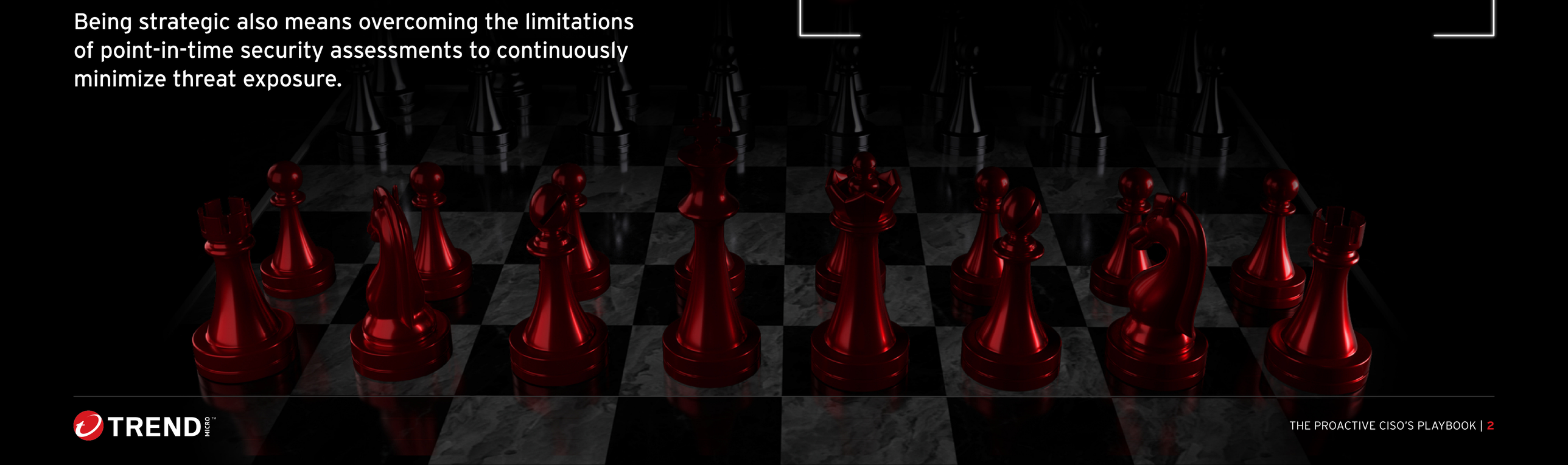
WHAT DOES IT MEAN FOR A CISO TO BE STRATEGIC?

It means thinking about cyber threats in terms of business risk, and taking steps to get out of firefighting mode and manage it proactively.

Being strategic also means overcoming the limitations of point-in-time security assessments to continuously minimize threat exposure.

This playbook sets out the foundations of a strategic, proactive security approach, including:

- What many organizations misunderstand about managing cyber risk today
- The three essential pillars of cyber risk management
- The roadmap to proactive security
- Critical success factors



THE RISK THAT NEVER SLEEPS

Cyber risk is unlike other business risks because it is dynamic, continuous, and shared. There are no hard boundaries, and there's no end state. Your attack surface will continue to change in tandem with the latest threats and technologies.

With breaches continuing to climb and corporate leaders increasingly accountable for the consequences, mitigating cyber risk is no longer just a technical concern; it's a strategic imperative.

Advanced cybersecurity technologies can help, but having too many specialized tools adds complexity instead of reducing risk. Meanwhile, attackers keep looking for—and finding—the paths of least resistance.

All of this makes cyber risk uniquely hard to manage. Therefore, CISOs need a defined pathway that can take them from reactive security operations to a proactive and strategic, risk-based approach.

Cyber risk demands visibility into every digital asset in the enterprise, including:

- Endpoints
- Internet-facing assets
- Applications
- Accounts
- Cloud assets

More than

60%

of organizations say unknown, unmanaged, or poorly managed internet-facing assets have contributed to breaches.[1]

75%

say it takes them a day or more to identify risks they face.[2]

WHERE ORGANIZATIONS GET CYBER RISK WRONG

Most CISOs today use a "risk treatment" methodology to evaluate vulnerabilities. While taking a structured approach to managing identified risks sounds good on paper, in practice, it often does little to reduce cyber risk in a meaningful way.

Here are **six common risk treatment pitfalls**. On the whole, these are ineffective approaches because they confuse theoretical solutions and compliance activities. What's really needed is **proactive risk management**.

01

Inaction

Identifying risks while leaving them unaddressed because they haven't done any actual harm—yet.

02

"Checkbox" mitigation

Adding documentation, creating policies, or holding training sessions that don't convert into measurable security improvements.

03

"Don't look back" mitigation

Implementing security controls without verifying they work or tracking to see if vulnerabilities have been reduced.

04

Insufficient follow-through

Assuming risk mitigation is finished because preventative efforts have been initiated, with no verification or ongoing penetration tests, red teaming exercises, or real-time monitoring.

05

Unclear accountability

Failing to specify who is accountable for which aspects of cybersecurity beyond security and IT teams.

06

Risk handoffs

"Dealing with" risk by shifting responsibility to vendors, partners, or insurers without directly addressing vulnerabilities.

THE EVOLUTION OF CYBER RISK MANAGEMENT

The growth and increasing complexity of the enterprise attack surface has put CISOs under pressure. They not only need to protect against threats but are also expected to actively manage risk. That pressure is only going to intensify as AI continues to evolve.

Key developments up to now:

Exposure management

In response to increased threat exposure, cybersecurity professionals have started to focus on attack surface management.

Growing awareness of risk

Experts quickly realized it's not just the attack surface that needs to be managed, but also the risks emerging across it. Authorities like the U.S. National Institute of Standards and Technology (NIST) then rolled out cyber risk management frameworks.

Impacts beyond IT

It soon became clear that cyber risks aren't restricted to the IT environment. They affect productivity, revenue, and corporate reputations. This necessitated new tools like cyber risk scoring and quantification.

A continuous process

Experts quickly observed risk monitoring and assessment needed to be full-time, continuous activities, prompting Gartner to roll out its concept of continuous threat exposure management (CTEM).

Cyber risk management today is still a new field. While AI risks increase the challenges, AI tools promise to make cyber risk management more proactive than ever before.

THE 3 PROACTIVE PILLARS OF CYBER RISK MANAGEMENT

Cyber risk management ultimately hinges on the threefold combination of visibility, prioritization, and mitigation. Each of these addresses key cybersecurity needs—and comes with its own set of considerations.

01 Visibility

You can't protect what you can't see. Unmanaged assets must be found and addressed.

What's required

Continuous insight

Historically, security teams have had to rely on single-point-in-time checks on the environment. This isn't enough to keep up with today's threat landscape. Since adversaries only need to find one weakness, proactive risk management requires ongoing, real-time identification of vulnerabilities, threats, and risks across all digital assets and business operations.

Continuous compliance monitoring

Proactive cyber risk management helps organizations constantly discover and contextualize risk. In addition, continuous monitoring should be applied to all compliance requirements.

Consolidated tools

Many organizations are dealing with tool sprawl, shadow IT, and unmanaged assets, all of which interfere with the ability to manage risk effectively. If tools can't fully be consolidated, the data they collect should at least be integrated into a single view.

PILLARS CONTINUED →

02 Prioritization

If everything's a priority, nothing's a priority. You need to know which risk insights to act on first.

What's required

Continuous risk assessment

Ongoing monitoring can unearth a high volume of vulnerabilities, but not all of them pose the same level of risk. Operationalizing cyber risk management means continuously reassessing and reprioritizing risks based on live threat intelligence, vulnerability scans, and real-time asset management insights. AI-powered tools can help contextualize risk data and its significance to the business.

Cyber risk quantification (CRQ)

CRQ goes beyond prioritization to calculate the possible business impact of a breach, attack, or loss associated with a given cyber risk. It helps integrate proactive decisions into the overall corporate strategy, making cybersecurity core to the business.

03 Mitigation

Attackers move fast, so mitigation can't afford to be slow. Rather than simply addressing breaches when they occur, a proactive risk response strategy is essential—and can prevent them from occurring at all.

What's required

Rapid, active mitigation

High-priority vulnerabilities need to be addressed as quickly as possible. That could mean deploying zero trust architectures, automating patches, and actively responding to threats in real time.

Verification and feedback

Security teams can't afford to simply trust that cyber risk mitigation tactics are going to be effective. Every step taken needs to be verified, and strategies need to be adjusted immediately if they aren't delivering results.

Automation

With effective prioritization, you can determine where action needs to be taken most urgently. Automated playbooks and tools radically accelerate this process. Proactive cybersecurity solutions and capabilities leveraging the latest technology, including agentic AI, can help security teams prioritize and address risk while reducing strain on resources and staffing.

THE ROAD TO CYBER RISK MATURITY

Understanding the three pillars of proactive cyber risk management is a critical starting point. For many CISOs, the question is how to operationalize those pillars and embed proactive cybersecurity into their organizations. It's a progressive journey that begins by identifying the stage you're at today.

01

Reactive mode

Most organizations are at this stage when they start the journey.

Shift to active threat and exposure monitoring

02

Tactical mode

"Going tactical" is about managing your organization's exposure to cyber risk.

Key indicators of reactive mode include:

- Overwhelmed security teams with too many incidents and alerts
- Low visibility into assets, threats, and risks
- Focus on patching vulnerabilities and responding to breaches
- Insufficient context to address alerts effectively
- Too many tools and silos
- Patching based on common vulnerability and exposure (CVE) scores
- Incomplete inventories, spreadsheet-based management

In this kind of environment, incident response is slow and costly. Attackers have abundant opportunities to lurk undetected. Compliance is driven by checklists, not real-world risk.

While tactical efforts deliver benefits, progress is limited due to:

- Manual processes
- Inconsistent prioritization, chasing high-CVSS (common vulnerability scoring system) vulnerabilities instead of real risk
- Outdated patches
- Security and IT silos

While you benefit from better insights, being stuck in tactical mode means your security team is still going to be chasing after issues instead of getting out ahead of them. This increases your risk of being overwhelmed and missing threats.

ROAD CONTINUED →

Shift to risk-based exposure management

03

Risk driven mode

In a risk-driven organization, cybersecurity is anchored in an awareness of risks—and oriented toward mitigating them.

Shift to strategic, continuous risk management

04

Proactive mode

At this stage, your visibility, prioritization, and mitigation strategies work together. This is a continuous cycle of discovery, assessment, and strategic action to minimize risk exposure and potential business impacts.

This involves:

- Risk-based security frameworks
- Automated cyber risk scoring, determining asset-by-asset risk levels based on configuration, interconnectivity, and vulnerabilities
- Automated risk quantification for a scenario-based understanding of cyber risks in context of the business
- Risk-based prioritization to guide decision-making
- Automated remediation and compliance management

Automated solutions and tools help your organization maintain a real-time view of attack surface conditions, while threat intelligence helps you address known, unknown, and zero-day threats.

Instead of responding to threats after the fact, proactive cyber risk management anticipates and addresses them pre-emptively, aided by AI and automation.

With insight into the business impacts of risks and continuous monitoring and measurement, proactively secure organizations can quantify the business impact of cybersecurity, demonstrating its value. Cybersecurity becomes an enabler of ongoing digital transformation, supporting and protecting innovation while preserving customer trust.

Other benefits include:

- Alignment of cybersecurity with business and innovation objectives
- Fast, automated protection and better-informed decisions
- Integration of cybersecurity into board-level risk management, with better communication about cyber risks and protection measures

92% **Risk-driven approaches reduced ransomware probability by 92% for Trend Micro customers and drove their risk scores below the industry average.[3]**

CISO-BACKED BEST PRACTICES

Beyond the core requirements and journey stages, a few other factors serve as important enablers of successful cyber risk management.

Avoid "risk theater"

Managing cyber risk demands focus, effort, and discipline. Less risk-mature organizations often find their security activities don't reduce risk in a measurable way, or that risk reporting becomes less meaningful as it travels up the management chain.

Be on the lookout for cybersecurity activities and processes that may not be delivering optimal results, and strive to make measurement-based decisions as soon as possible.

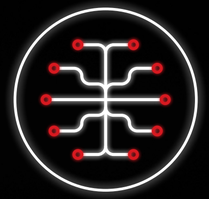
Ensure leadership buy-in

The tone set by leaders who take cybersecurity seriously can have a significant impact on the implementation and long-term effectiveness of cyber risk management. Buy-in isn't just about authorizing investments into proactive security solutions; it's about internalizing risk management as part of your organization's cybersecurity culture.

This requires CISOs to make a strong business case for cyber risk exposure management, including outcome-driven metrics (ODMs) and protection-level agreements (PLAs). It also necessitates good communication and accountability around cybersecurity issues.

Don't mistake "compliant" for "secure"

Complying with cybersecurity policies and data protection laws and regulations is critically important. But satisfying compliance criteria does not make your security posture stronger on its own. It's essential to understand the actual risks your organization faces, and to address them in a disciplined, prioritized way.



Leverage simulations

Outside of monitoring the live attack surface and network environment, models and simulations can shed valuable light on possible vulnerabilities—and let organizations safely 'live out' the impacts of security incidents to better understand the potential consequences. These can include virtual red teaming, penetration testing, and breach attack and Monte Carlo simulations, the latter being computational tests of randomized scenarios.

AI, machine learning, probability indicators, and digital twins are all technologies that can help in this regard, helping establish a shared way of talking about risk and providing a further mechanism for engaging leaders in the conversation.

A CLEAR VISION OF CYBER RISK MANAGEMENT

Cyber risk is a key strategic concern for organizations today. That means CISOs are expected to talk about cyber risk in strategic terms—what it means for the business, not just for IT—and ensure that risk is managed in a continuous, proactive, and measurable way.

Doing so requires complete attack surface visibility, a fast and effective means of prioritizing risk, and the ability to minimize exposure and reduce risk where it matters most.

None of that can happen overnight. The journey to cyber risk maturity is long and continuous. Get started by understanding your current risk state and taking steps to implement a proactive security strategy, giving you the opportunity to outpace threat actors.

TREND VISION ONE™

is the only enterprise cybersecurity platform that centralizes cyber risk exposure management, security operations, and robust layered protection, empowering you to predict and prevent threats while accelerating proactive security outcomes with greater visibility, precise prioritization, and automated mitigation all built in.

Learn more about Trend Vision One and how it will help you achieve your cyber risk exposure management goals.

Book a meeting with our team today.

Sources:
[1] ESG Research Brief: Continuous Cyber Assets Analysis is Key to Effective Risk Mitigation and Threat Management, January 2025
[2] Analysis Perspective: Worldwide SIEM, Exposure Management, and AI-Related Technologies, IDC, September 2024, Doc # US52584624
[3] Trend™ Research blog: Anubis: A Closer Look at an Emerging Ransomware with Built-in Wiper, June 2025