White Paper

HardenStance

The Fundamentals of Cyber Risk Management

By Patrick Donegan, Principal Analyst, HardenStance

Sponsored by

noetic | paloalto NETWORKS | UNIT 42 BY PALO ALTO NETWORKS | CYBER THREAT ALLIANCE

February 2024

Executive Summary

- Cyber risk management has been the right approach to cybersecurity for many years. Increasingly, regulators are making it mandatory to adopt it.
- Cyber risk management centres on active management of business risk. If you're largely 'setting and forgetting' your cybersecurity posture, you're not managing it.
- Very few organizations are doing cyber risk management really well. Leaders should get comfortable with basing it on largely qualitative cyber risk assessments.
- Continuous cyber asset management and threat-informed defence are key enablers. Leveraging them to actively manage the chaos of an IT environment is key to driving down the cost of incidents that occur, and the probability of incidents occurring.

Regulators expect better cyber risk management

With most new cybersecurity regulations, such as the new incident disclosure rules of the Security and Exchanges Commission (SEC) in the U.S and the EU's Network and Information Services (NIS2) Directive, much of the attention is focused on the new incident reporting rules themselves and the challenges of complying with them.

Most organizations are far from being where they need to be with cyber risk management.

Set just a little further back in prominence, underpinning not just the regulator's expectations of incident reporting but also the overall direction of cybersecurity regulation is a doubling down of the modern day regulator's expectations that organizations must fully embrace cyber risk management.

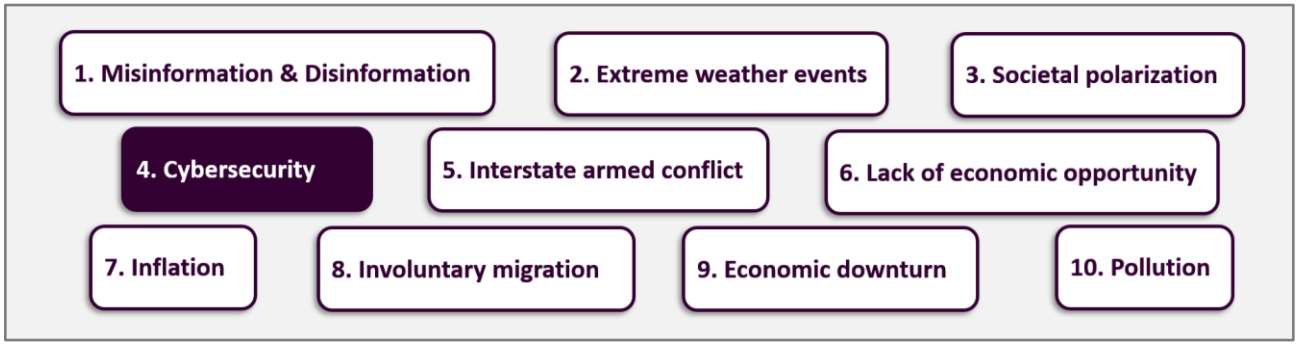
Review the text of the new SEC or NIS2 regulations and you'll see a requirement to adopt cyber risk management clearly set out. Adopting it is certainly a sure means of complying with those incident reporting requirements with minimum friction. But a risk management approach is also the surest way to minimise the number of cyber incidents that impact your organization as well as to minimise the harm that arises from incidents.

What is risk management?

Let's start by defining risk management more broadly in the context of traditional corporate or enterprise risk management covering geopolitical, financial, legal, legislative, operational, privacy and environmental risk as well as the still-nascent discipline of cyber risk management.

HardenStance defines risk management as a formal process for determining risk appetite and then identifying, ranking, monitoring and managing those risks so as to maintain risk exposure at or below that chosen risk appetite. As shown in **Figure 1,** despite organizations having to manage escalating risk across several key risk management disciplines in 2024, cyber risk invariably features at or near the top of the pile when they're ranked in order of potential severity.

Figure 1: World Economic Forum Estimated Severity of Global Risks



Source: World Economic Forum's 'Global Risks Perception Survey' 2024

The 'management' part is what really counts in cyber risk management. The term captures how some amount of risk is unavoidable. It can be reduced but it can't be reduced to zero. 'Management' also captures risk management's defining characteristic: It is a discipline whose assumptions and policies need to be continuously monitored, optimized and enforced. If you're still 'setting and forgetting' your cyber risk posture until you review it again in the distant future, you're not managing it.

What cyber risk management is (and isn't)

HardenStance defines cyber risk management as the use of business processes and technical controls to identify, rank, monitor and manage the risks that stem from an organization's use of IT and OT systems and the Internet. Today, many companies would claim to be practising cyber risk management. A lot of them are really not doing that – what some of them are doing is cybersecurity that is somewhat or largely independent of business risk and without actively managing that business risk. Of those that are doing cyber risk management, a subset of leaders have operationalized it to an advanced level, such as in the financial sector. As implied by **Figure 2**, most organizations are far from being where they need to be with cyber risk management.

Cyber risk management is the use of business processes and technical controls to identify, rank, monitor and manage the risks that stem from an organization's use of IT and OT systems and the Internet.

It's important not to be too dependent on off-the-shelf formulae for setting up or improving a cyber risk management function. Cyber risk management is a less mature discipline than other types of risk management. There is no end of guidance on good cybersecurity posture (e.g., turn on Multi-Factor Authentication). But there are not many metrics for measuring the efficacy of cybersecurity actions. Mean time to detect an incident or mean time between incidents are good examples but they are not widely used today. There are even fewer metrics for measuring the efficacy of the cyber risk management function as a whole. Moreover, as of today, none of these approaches are universally agreed and standardized for all businesses.

The NIST Cyber Security Framework is highly regarded and can make a very useful contribution to a cyber risk management strategy. But even in the Q&A section of its own website, NIST has a clear response to the question "Does NIST provide a recommended checklist of what all organizations should do?" NIST's own response is:

> *"No, the Framework provides a series of outcomes to address cybersecurity risks; it does not specify the actions to take to meet the outcomes. Because standards, technologies, risks, and business requirements vary by organization, the Framework should be customized by different sectors and individual organizations to best suit their risks, situations, and needs. Organizations have unique risks – different threats, different vulnerabilities, different risk tolerances – and how they implement the practices in the Framework to achieve positive outcomes will vary."*

Figure 2: Even in the UK, Cyber Risk Management is Very Much a Work in Progress (April 2023)

Survey question put to business organizations	All businesses (%)	Large businesses (%)
Do you have a formal cybersecurity strategy in place?	52%*	68%
Have you carried out a risk assessment covering cybersecurity risks in the last 12 months?	29%	N/A
Do you have a formal policy in place covering cybersecurity risk?	29%**	79%
Have you undertaken action in all 10 of the NCSC's recommended '10 steps to cybersecurity'?	2%	20%
Do you have a formal incident response plan?	21%	64%
** Medium and large businesses combined **includes small and microbusinesses*		

Source: UK's National Cyber Security Centre (NCSC) "Cyber Security Breaches Survey, 2023", April 2023.

As depicted in **Figure 3,** accountability for cyber risk management should rest with the Chief Information Security Officer (CISO). A CISO must be capable of having a deep understanding of the organization's business. They must be fluent in the language of business risk. With enough depth of technical expertise in their team, a CISO doesn't necessarily need a deep mastery of technical controls.

Recognizing that cyber risk management must be a high priority requires that the CISO must in turn be fully supported by management and the board. All CISOs may share the same four-letter acronym including the 'O' for 'Officer', but they don't all have peer status with the executive management team. Once you've appointed the right CISO, management needs to accord them high status. That's because a business-driven CISO with high status is much more likely to drive a good cyber risk management programme than one who isn't business-driven and doesn't have high, executive-level status.

Management and the board should expect cyber risk reporting to be rolled into an overall view of total organizational risk and how effectively it is being managed.

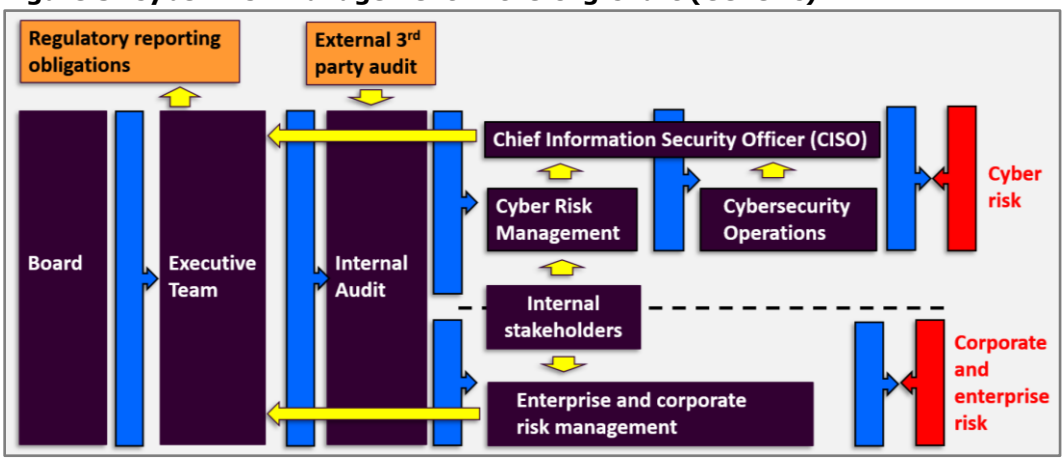
Cyber risk management needs to take account of all stakeholders

The cyber risk management function should liaise extensively with all relevant internal stakeholders. The Responsible, Accountable, Consulted and Informed (RACI) assignment matrix can be useful in defining roles and responsibilities. A big challenge here is arriving at a common nomenclature, since different stakeholders often have different perceptions of risk and express it with different terminologies. Many organizations also have to comply with multiple different regulatory regimes.

Figure 3 depicts five layers of responsibility for cybersecurity. (i) Security operations (SecOps), which directly faces the threat landscape on the right, behind SecOps are (ii) cyber risk management; (iii) internal audit; (iv) the C-Suite; and (v) the board on the left. CISOs should be accountable for cyber risk management as well as security operations. A positive consequence of regulators imposing new reporting obligations and cyber risk management disciplines is that it incentivizes the board to fulfil its statutory obligations on risk oversight. It discourages boards from offloading responsibility for cyber risk management further down the organization to the audit committee or the CISO. Instead, it drives them to be proactive in supporting CISOs with the resources they need.

Management and the board should expect cyber risk reporting to be rolled into an overall view of total organizational risk and how effectively it is being managed. This requires that the CISO's role be clearly scoped and that points of integration with other risk management functions are clearly defined. That said, the metrics and tooling that each risk management discipline uses, and the cadence of some of the key events that drive each one, make these disciplines very difficult to align or synchronize. Hence trying to aggressively enforce organizational alignment or convergence between cyber and other types of risk management disciplines can easily do more harm than good.

Figure 3: Cyber Risk Management in the Org Chart (Generic)



Source: HardenStance

To avoid being daunted or deterred by the challenge, organizations should embrace an iterative 'crawl, walk, run' approach to adopting cyber risk management. Committing to incremental improvements over time will go a lot further than pointing the finger at the sizable gap between what you're currently getting and what it is you ultimately want.

Committing risk appetite to a formal document

Cyber risk management starts with the expression of the organization's risk appetite as captured in a formal document. Targets can be expressed quantitatively, such as a target ceiling on the amount of losses the organization is willing to incur per year or per incident (although as discussed further on, accurately estimating the cost of specific incidents can be fiendishly difficult). Risk appetite can also be expressed qualitatively, such as a requirement to prioritize the protection of intellectual property against theft. Risk appetite statements can include both quantitative and qualitative targets.

A cyber risk management strategy should be up to the task of keeping the exposure at or below the target or targets set out in the risk appetite statement.

An organization's risk appetite is in part pre-determined by the sector that it operates in. For example, a vehicle engine manufacturer's cyber risk appetite should be lower than that of a manufacturer of tennis balls. Nevertheless, depending on the sector, one organization can arrive at a significantly higher or lower risk appetite than another's because it has a very different business strategy.

A high risk tolerance isn't 'bad' from a cyber risk management perspective, nor is a low risk tolerance 'good'. A business can suffer as much harm from over-spending on cybersecurity or allowing security controls to introduce too much friction into day-to-day business operations, as it can from being impacted by a massive data breach due to weak cybersecurity. It's all about the right risk trade-offs. The only thing that matters is that a cyber risk management strategy – and the resourcing of it – should be up to the task of keeping the exposure at or below the target or targets set out in the risk appetite statement.

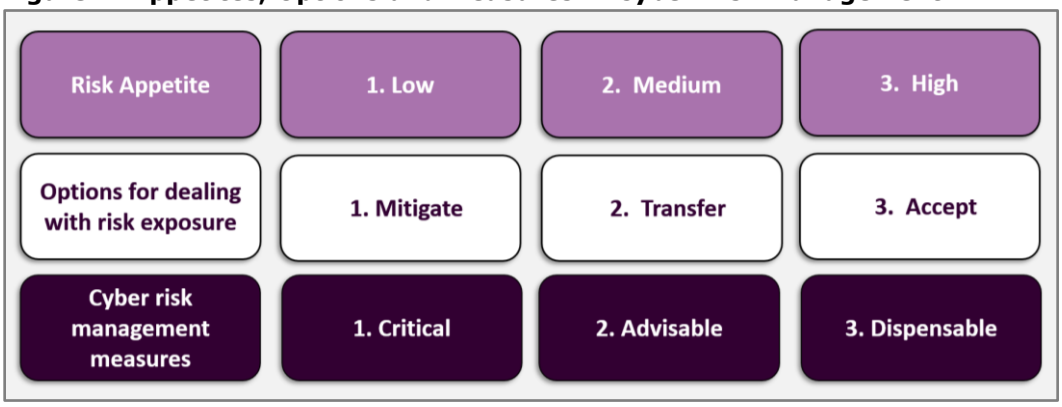
For most organizations, ensuring that cyber risk appetite and cyber risk management measures are tightly aligned comes down to decisions that are complex at the granular level of the CISO's team but straightforward at an executive level. As depicted in **Figure 4**, there are three options for executing on cyber risk management strategy:

1 Mitigating or buying down cyber risk oneself through investment in business processes and technical controls. This can potentially include partners such as a Managed Service Partner (MSP), Managed Security Services Provider (MSSP) or Managed Detection and Response (MDR) partner.

2 Transferring the risk to a 3rd party via a cyber insurance policy.

3 Accepting the remaining risk by knowingly choosing not to invest in mitigation measures on the grounds that if this risk materializes, the likely cost is acceptable.

Figure 4: Appetites, Options and Measures in Cyber Risk Management



Source: HardenStance

The use of cyber risk assessments

Cyber risk assessments should be used to identify, estimate and prioritize risks. The pareto principle is applicable here. Committing 80% of resources to mitigating the top 20% of highest risks is a good rule of thumb for running an effective programme.

The greatest cyber risk to an organization can be divided into two main categories:

- disruption to the critical networks, systems, applications or data that the business depends on to run its operations efficiently.
- exposure of the business' high value information to cyber criminals.

Risks need to be assessed and ranked in order of severity within each of these two categories. Maintaining the uninterrupted availability of real-time payment processing, call centre response times, customer billing and business email should be ranked differently from one organization to the next. Risk arising from the exposure of sensitive data that an organization owns or has access to, like IP, operational data or customer records, needs to be ranked as well as assessed too.

Committing 80% of resources to mitigating the top 20% of highest risks is a good rule of thumb for running an effective programme.

All risk calculation equates to the probability of an incident occurring multiplied by the cost of that incident occurring. So if the cost of an incident is estimated at $10 million, and the probability of it occurring in any one year is estimated at 40%, that's an annual risk of $4 million. Management and the board may crave that exposure to risk be expressed in hard monetary terms to be able to understand how well the operational reality maps to its risk appetite. Unfortunately, it's just not reasonable to expect that for most cybersecurity risk.

Banks and other financial services firms have certainly become adept at making robust monetary assessments of their cyber risk exposure. But that's because managing quantities of money is their core business and because they're a particular target for cybercrime which has made them leaders in cyber risk management. As described below, most organizations find making cyber risk assumptions that drive dependable dollars and cents estimates a lot more challenging.

Why cyber risk can be very difficult to quantify accurately

Here's why expecting to be able to rely on quantitative inputs to arrive at hard dollars and cents assessments of cyber risk is so challenging:

- Gaps in your asset inventory – blind-spots in your visibility of your attack surface – drive overly optimistic quantitative risk probability assessments.
- A trusted third party report may state that 1 in 10 comparable firms has recently been impacted by the same type of incident. However, another 2 in 10 might also have been attacked but that fact is either not known to the victims yet or is known but has not yet been reported.
- Where incidents are prevented from running their full course, costs incurred can vary greatly depending on what specific stage of the attack security operations is able to remediate it.
- Without a very well-developed incident response plan, and high confidence in it being well executed on, a quantitative assessment of the costs of recovering from an incident is largely guesswork.
- Incidents can trigger runaway costs arising from the fallout from negative media or social media coverage. These can be very hard to contain – even with an excellent incident response plan.

As these examples demonstrate, known flaws in quantitative assessments have to be adjusted for as best as possible with qualitative judgements.

Most cyber risk assessment is more art than science

Especially in the early stages of evolving a cyber risk management programme – but even in later stages – a lot of cyber risk assessment has to be more art than science. Consistent with embracing an iterative approach, leaders need to be willing to live with substantial gaps in the quantitative data they would ideally like to have.

That doesn't make assessments anywhere near as random or unguided as it may sound. For example, most organizations should be able to make a reasonable estimate of the cost of all their IT systems going down for a day. However, the probability of that occurring can be hard to calculate with anything like the same precision. But it's arguably not all that important; it certainly shouldn't get in the way of making the management of that risk a top priority.

Useful quantitative metrics can be derived from probabilistic cyber risk scores. The best ones are algorithmically extracted from an organization's infrastructure (manually completed questionnaires are much less reliable). These are the cybersecurity equivalent of credit scores and can be calculated internally, derived from reputable vendor solutions, or a combination of the two. Cyber risk scores are evidenced-based and easy to understand. Given the dearth of reliable quantitative data they are useful inputs to an organization's own cyber risk management. Partners such as cyber insurers and prospective M&A targets tend to pay close attention to them too.

Consistent with embracing an iterative approach, leaders need to be willing to live with substantial gaps in the quantitative data they would ideally like.

But the limitations of cyber risk scores should also be recognised and adjusted for. They tend to be useful for identifying generic strengths and weaknesses, but they tend to be calculated without much critical business context. That's an important shortcoming because a cyber risk management approach demands that you prioritize fixing a low-to-medium risk score that can impact a critical asset over a high risk score that can't. Many risk scores also offer a snapshot in time view, in which case they quickly lose their value.

Good cyber risk assessments require high fidelity asset inventories

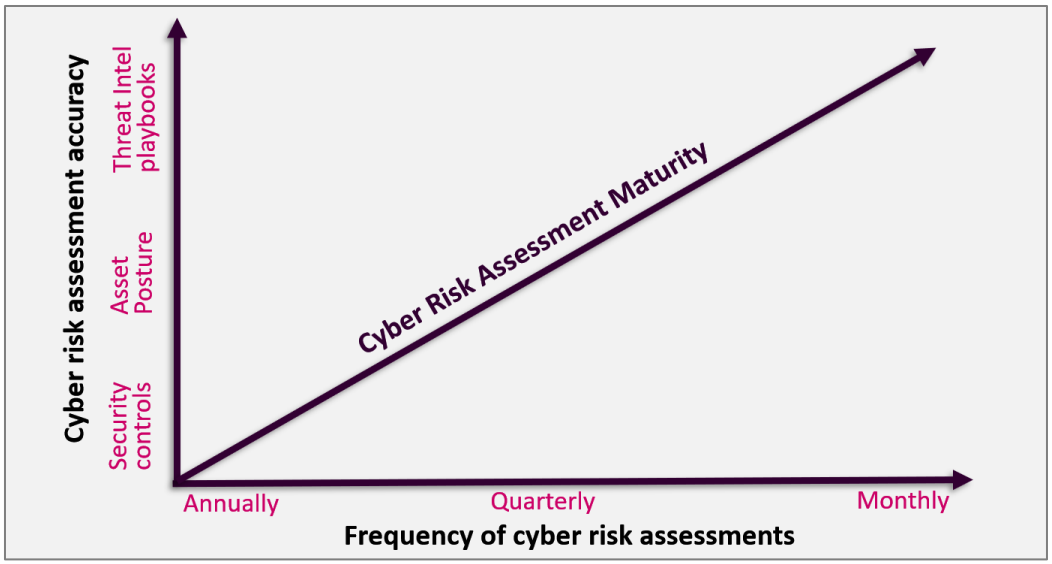
Understanding all the risks to the IT environment, and determining which ones should be prioritized, has to start from a single source of truth in the form of an asset inventory. A lot of effort should go into making this as comprehensive and unified as possible, specifying each asset's desired state, configuration, and update and patching cadence.

To assure full visibility into the entirety of the threat surface as a hacker might see it – to ensure that the security operations team isn't blind to any exploitable assets – the definition of assets should embrace much more than just traditional compute assets. The UK's National Cyber Security Centre (NCSC) defines an asset as "anything that can be used to produce value for your organization. This includes information, such as intellectual property or customer data. It encompasses many types of technology too, both IT and OT, hardware and software, physical locations and financial capital. And, of course, it includes your people, their knowledge and skills."

An asset inventory should therefore include the network's topology or design; security policies; users' specific access permission relationships to applications and whether they are Multi-Factor Authentication (MFA)-enabled; and any employee-owned devices that connect to the network. It should also be sure to incorporate any and all assets, whether deployed on-premises, in a data centre, or in the cloud.

The challenge then is to be able to understand the highly complex matrix of paths and dependencies between all those assets, including both critical and non-critical ones. That understanding can then be leveraged to prioritize remediation of vulnerabilities to critical assets themselves - or assets that are in the path of critical assets. The Exploit Prediction Scoring System (EPSS) can be a useful data-driven model for estimating the probability of a software vulnerability being exploited in the wild. That understanding can also be leveraged to help accurately optimize the allocation of cybersecurity budget against risk management criteria.

Figure 5: A Roadmap for Cyber Risk Assessment Maturity



Source: HardenStance

As depicted in **Figure 5** there are essentially three different bottom-up and top-down approaches that are typically used for undertaking cyber risk assessments. As described below, they are controls-centric, asset-centric; and threat-centric.

Organizations shouldn't choose between asset-centric and threat-centric approaches. On the contrary, the two are highly complementary.

1 **Controls-centric**: This is a bottom-up approach, typically driven by adherence to a chosen cyber security framework. It views security controls as a discrete subset of assets. Those security controls that are deemed to be of greatest value in reducing risk are selected and implemented. While a controls-centric approach is sometimes cited as a cyber risk management metric, in reality it measures an organization's commitment to implementing externally recommended controls rather than measuring actual risk posture. Hence, it aligns more closely with traditional compliance than a risk management approach.

2 **Asset-Centric or 'Inside Out':** This is also a bottom-up approach but is a much more effective way of measuring cyber risk. An asset-centric approach accords every internal asset a risk score that takes full account of the all-important context of the risk an identified flaw poses to the business - i.e. whether a flawed asset can or cannot enable access to sensitive data or support a critical business service. Remediation measures are then prioritized in the context of these internal, asset-centric, risk scores.

3 **Threat-Centric or 'Outside In'**: This is more of a top down approach and is the most advanced approach to undertaking cyber risk assessments. A threat-centric approach leverages cyber threat intelligence to undertake threat modelling against specific cyber threat playbooks that pose the highest risk to the organization. The MITRE ATT&CK Framework can be a valuable supporting tool here. In most cases, modelling the ways specific attacks can unfold in the context of the organization's attack surface, and then prioritizing remediations, is the most effective way of assessing risk exposure. The efficacy of threat centric modelling is nevertheless highly dependent on the completeness, accuracy and relevance of the threat intel that can be assembled, curated and acted on in the context of available assets. This approach is therefore the most challenging to execute well.

Organizations shouldn't choose between asset-centric and threat-centric approaches. On the contrary, the two are highly complementary; they each yield different insights into risk exposure. The ultimate aim of cyber risk assessments should be to integrate and correlate insights from both models as a basis for prioritizing remediation measures.

The 'management' part is all-important

Figure 5 depicts the three approaches to cyber risk assessments on one axis. The other axis is the frequency of those assessments. This is the 'management' part of cyber risk management that organizations have most difficulty committing to. Even leaders who expect to invest a lot in cybersecurity are still vulnerable to the error of wanting to 'set and forget' those controls. That's highly unlikely to keep risk down to the desired level in line with cyber risk management targets.

That's because cyber risk tends to fluctuate more than other types of risk. Extreme weather events and the risk of armed conflict are characterized by periods of months or years when risk is fairly constant, interrupted only occasionally by a sharp spike. From the perspective of a board or CEO, some aspects of cyber risk need only be reviewed once a quarter or even once a year. But from the perspective of security operations, risk exposure can fluctuate significantly from one week, one day or one hour to the next.

The best way for security operations to keep risk down to the level targeted by a risk appetite statement is to engage actively and continuously with the chaos of an IT environment.

The best way for security operations to keep risk down to the level targeted by a risk appetite statement is to engage actively and continuously with the chaos of an IT environment. The goal has to be to quickly identify new risks amongst the constant blizzard of changes - and intervene to mitigate them. Without that, you leave the organization exposed for days, weeks or months. Recalling that risk is the cost of an incident multiplied by the probability of it occurring, the rest of this section explains how costs and probabilities can be managed by continuously monitoring and adjusting your attack surface and security controls as well as by committing to threat-informed defence.

Continuous monitoring and management of assets

As stated, an asset inventory should identify not just the assets themselves and requirements relating to their key attributes but also the highly complex matrix of paths and dependencies between them all. These constitute an organization's threat surface. The big challenge with getting this right in security operations is that an IT environment is inherently dynamic, if not chaotic – especially with the dynamic spinning up and down of software instances enabled in the cloud. Admin rights are constantly changing; software is updating; new vulnerabilities are disclosed; ports are opening and closing; botnets are taken down by law enforcement; new ones crop up in their place; and so on. Change events are triggered by employees, partners and vendors; not to mention cyber threat actors. Some events are automated while others are triggered manually.

So-called 'drift' in an IT environment is where continuous change causes the security posture of assets, or the relationship between them, to 'drift' from the state needed to meet cyber risk management targets. To be able to intervene and respond to constant change appropriately – to be able to fulfil the 'management' part of cyber risk management – requires that all the organization's assets, including security controls, be subject to continuous monitoring by security operations. It also requires being able to dynamically adjust the security posture of assets, and the relationships between them, to reduce or eliminate new risks that drift introduces.

This is one of the most important aspects of cyber risk management but it's also one of the most challenging. The rate of change is so intense that it can't be managed well manually. Continuous monitoring and continuous management necessarily require a lot of automation. Drift from the desired end state needs to be spotted quickly, policy needs to be validated, and remediation applied to ensure that any change in the environment aligns with the desired end state.

Security monitoring looks to put fires out by detecting and mitigating actual threats. Continuous monitoring and management of assets protects them from being vulnerable to fires in the first place. Regulation is also driving towards a more continuous model. For example, in the U.S, CISA Binding Operational Directive (BOD) 23-01 now requires that federal agencies run automated asset discovery every seven days & vulnerability enumeration every 14 days.

You can try to build up the required visibility by pulling data from a variety of siloed tools and running some correlation algorithms across them. But apart from being challenging in its own right, this ground-up approach will inevitably have gaps. For example, Endpoint Detection and Response (EDR) or XDR platforms can provide good insight into those endpoints that support their clients. However, they typically can't tell you which of your organization's endpoints are not supporting their client, or which of their clients are correctly configured and which aren't.

Effective cyber risk management requires a more universal and more granular view. It requires the ability to manage all assets including new entities that appear (or seem to appear); entities that disappear (or seem to disappear); and new relationships between entities. Graphical representations of the attack surface depicting the key context of dependencies between assets also suits a top-down cyber risk management perspective better than traditional asset lists that lack that critical context relating to business risk.

Threat-Informed Defence lengthens the odds on incidents occurring

If you're looking to understand which factors most impact the probability of suffering a cyber incident, then changes in the threat landscape – which cyber threat actors are targeting your organization, what they're targeting, how and why ? – is key.

A cyber risk management strategy has to aim for being increasingly threat intelligence-led or threat informed over time.

Change in the external threat landscape is as dynamic as with an organization's own environment. Old threat groups disband; new ones are formed. Groups that began as hacktivists targeting political opponents can morph into ransomware gangs targeting financial rewards. Malware is constantly changing - some of it driven by machine learning algorithms making the smallest of tweaks in code at machine speed to try and avoid detection. New vulnerabilities are disclosed. New exploits and dumps of stolen data appear for sale on the darknet for the first time. Worse, zero-day attacks exploit vulnerabilities out of nowhere, without any warning, before developers have even had a chance to fix them.

Hence a cyber risk management strategy has to aim for being increasingly threat intelligence-led or threat-informed over time. That means threat-informed management of your security controls – for example, adjusting your firewall configuration in light of new threat intelligence. But it also means threat-informed management of all your IT assets – for example, prioritizing fixing a vulnerability that impacts any of your critical assets because a threat group is actively exploiting it to attack organizations just like yours, triggering incidents that your organization considers a high risk. As depicted in **Figure 6**, becoming threat-informed is another capability that organizations should embrace in steps, either in-house or through reliance on trusted vendor partners.

Figure 6: The Cyber Threat Intelligence Taxonomy

Category of cyber threat information	Examples of Information Conveyed	Intended Audience	Decision Example	Timeframe of Use
Technical	Indicators of malicious activity (e.g., malware hashes or IP addresses)	Cyber security vendors and network providers	Should the network security tool allow this packet through?	Immediate
Tactical	Details related to a specific threat actor	Network defenders (i.e., relevant staff and decision-makers)	Do we need to change a security setting today?	Short term
Operational	Malware types; software vulnerabilities	Senior-level security personnel/ managers	How often should we patch our networks?	Medium Term
Strategic	High-level information on changing cyber risk	Executives/ senior decision-makers	Should we change our risk calculation because a new adversary is targeting our industry?	Long Term

Source: Cyber Threat Alliance

Repeatability matters more than rigour

To conclude, the fundamentals of cyber risk management are that it is a continuous process. Over time, rigour certainly matters – but not at the expense of repeatability. Focus on building out a limited, imperfect, set of repeatable processes. Then progressively scale those processes up, increase the level of automation, and make it increasingly threat intelligence-led over time. ■

About the Sponsors

About Cyber Threat Alliance

The Cyber Threat Alliance (CTA) is a 501(c)(6) non-profit organization that is working to improve the cybersecurity of our global digital ecosystem by enabling near real-time, high-quality cyber threat information sharing among companies and organizations in the cybersecurity field. We take a three-pronged approach to this mission:

1. Protect End-Users: Our automated platform empowers members to share, validate, and deploy actionable threat intelligence to their customers in near-real time.

2. Disrupt Malicious Actors: We share threat intelligence to reduce the effectiveness of malicious actors' tools and infrastructure.

3. Elevate Overall Security: We share intelligence to improve our members' abilities to respond to cyber incidents and increase end-user's resilience.

CTA is continuing to grow on a global basis, enriching both the quantity and quality of the information that is being shared amongst its membership. CTA is actively recruiting additional cybersecurity providers to enhance our information sharing and operational collaboration to enable a more secure future for all. For more information about the Cyber Threat Alliance, please visit www.cyberthreatalliance.org

About Noetic Cyber

Noetic Cyber is a market leader and innovator in Cyber Asset Attack Surface Management (CAASM). Noetic delivers a proactive approach to attack surface and exposure management, giving security teams the visibility and context to uncover coverage gaps, improve their security posture and reduce cyber risk. Our goal is to improve security tool and control efficacy by breaking down existing siloes and leveraging those insights to support broader use cases.

Noetic's award winning platform is successfully deployed in customers across Pharmaceutical, Telco, Financial Services and Energy sectors. Founded in 2019, Noetic is based in Boston and London. For more information, visit www.noeticcyber.com, or follow us on LinkedIn or X.

About Palo Alto Networks Unit 42

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. We help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration.

By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the forefront of protecting tens of thousands of organizations across clouds, networks, and mobile devices. Our vision is a world where each day is safer and more secure than the one before. For more information, visit www.paloaltonetworks.com

Palo Alto Networks Unit 42 brings together world-renowned threat researchers, elite incident responders, and expert security consultants to create an intelligence-driven, response-ready organization that's passionate about helping you proactively manage cyber risk. Together, our team serves as your trusted advisor to help assess and test your security controls against the right threats, transform your security strategy with a threat-informed approach, and respond to incidents in record time so that you get back to business faster. For more information visit www.paloaltonetworks.com/unit42.

About HardenStance

HardenStance provides trusted research, analysis and insight in IT and telecom security. HardenStance is a well-known voice in telecom and enterprise security, a leader in custom cyber security research, and a leading publisher of cyber security reports and White Papers. HardenStance is also a strong advocate of industry collaboration in cyber security. HardenStance openly supports the work of key industry associations, organizations and SDOs including NetSecOPEN, AMTSO, The Cyber Threat Alliance, The GSM Association, ETSI and TM Forum. To learn more visit www.hardenstance.com

HardenStance Disclaimer

HardenStance Ltd has used its best efforts in collecting and preparing this report. HardenStance Ltd does not warrant the accuracy, completeness, currentness, non-infringement, merchantability or fitness for a particular purpose of any material covered by this report.

HardenStance Ltd shall not be liable for losses or injury caused in whole or part by HardenStance Ltd's negligence or by contingencies beyond HardenStance Ltd's control in compiling, preparing or disseminating this report, or for any decision made or action taken by user of this report in reliance on such information, or for any consequential, special, indirect or similar damages (including lost profits), even if HardenStance Ltd was advised of the possibility of the same.

The user of this report agrees that there is zero liability of HardenStance Ltd and its employees arising out of any kind of legal claim (whether in contract, tort or otherwise) arising in relation to the contents of this report.