Report

SKYBOX SECURITY

Reduce cyber risk with security posture management

Leaders in risk-based cybersecurity go beyond frameworks like NIST, applying proactive practices that significantly reduce business risk and improve the bottom line

SKYBOX SECURITY

Contents

A seismic shift in cybersecurity

Cybersecurity is at a crossroads. In the last few years, a convergence of forces has reshaped the industry in fundamental ways, and security teams are grappling with challenges on a scale never seen before.

The threat landscape has exploded. Threat vectors have multiplied and diversified. Threat actors are more numerous, organized, and capable—empowered by a vast ecosystem of providers, tools, and services (e.g., malware-as-a-service) that cater to experts and novices alike. Cyberattacks are more frequent, destructive, and insidious—and are increasingly targeting not just IT systems but also supply chains, third-party software, and operational technology (OT), including critical infrastructure. Zero-day exploits are on the rise, as are nation-state attacks, fueled by the Russia-Ukraine war.

Simultaneously, the rapid adoption of new technologies driven by digital transformation, cloud migration, the hybrid work culture, and the IIoT (industrial internet-of-things) boom has left security teams scrambling to manage an expanding attack surface and skyrocketing vulnerabilities. The situation is particularly perilous in OT, where many systems lack robust security protections and are exposed to attack as IT and OT environments converge and formerly air-gapped devices are hooked up to networks. As if that weren't enough to contend with, organizations have their hands full complying with a raft of new, more complex regulatory requirements.

All of this is happening at a time of severe resource constraints, made worse by an uncertain economy and chronic cybersecurity talent shortages aggravated by widespread burnout and the "great resignation." Functional silos within organizations—between IT and OT, for example, and between network, cloud, and security teams—further hamper efficient, coordinated action.

Cyber threats are surging, and so are risks

- **40%** of chief security officers say their organizations are not well prepared for today's rapidly evolving threat landscape.[1]
- Risk managers rank cyber threats as the **number-one** business risk in 2022, higher than business interruptions, natural disasters, or pandemics.[2]
- New cryptojacking and ransomware programs increased by **75%** and **42%**, respectively, in 2021.[3]
- The number of new vulnerabilities exploited in the wild rose **24%** in 2021.[4]
- OT vulnerabilities leaped **88%** in 2021.[5]
- Companies experienced an average of 270 attacks in 2021, up **31%** over 2020.[6]
- The number of data breaches broke records in 2021, jumping **68%** year over year.[7]
- Zero-day attacks nearly **doubled** in 2021.[8]
- The average cost of data breaches hit $4.24 million in 2021, up nearly **10%** from 2020.[9]
- The average time to detect and respond to cyberattacks grew to **280** days in 2021.[10]
- **36%** of CIOs say the shortage of skilled workers is their biggest cybersecurity challenge.[11]

[1] Cybersecurity Solutions for a Riskier World, ThoughtLab, May 2022
[2] Allianz Risk Barometer, Allianz, January, 2022
[3,4,5] Vulnerability and threat trends report 2022, Skybox, April 2022
[6] Elevating The Cybersecurity Discussion: Why CEOs Need To Get More Involved In Securing The Business, Accenture, 2022
[7] Data breaches break record in 2021, CNET, January 2022
[8] 2021 has broken the record for zero-day hacking attacks, Technology Review, MIT, September 2021
[9,10] 2021 Cost of a Data Breach Report, IBM, July 2021
[11] Cybersecurity Solutions for a Riskier World, ThoughtLab, May 2022

The soaring cost of insecurity

These threats are anything but hypothetical. They inflict real damage and take a growing toll on companies' bottom lines. The past year broke records not only for the number of breaches,[12] but also the cost. As IBM describes in their latest *Cost of A Data Breach Report*, "Data breach costs rose from USD 3.86 million [in 2020] to USD 4.24 million [in 2021], the highest average total cost in the 17-year history of this report."[13] And those averages were only for small-to-moderate breaches that compromised 2,000-101,000 records. For larger "mega-breaches" the costs run much higher—averaging $401 million for breaches of 50 million to 65 million records—and "can have an outsized impact on consumers and industries."[14] Examples of such catastrophic incidents include the 2017 Equifax breach, where the company eventually reached a settlement of up to $425 million with the Federal Trade Commission,[15] the 2019 Capital One breach, where the company agreed to pay $190 million in a class-action lawsuit,[16] and the 2021 T-Mobile breach, which is the subject of two ongoing class-action suits.[17]

As sobering as the average costs quoted above are, they may not reflect the full financial impact of breaches. In addition to the easier-to-quantify near-term costs (e.g., ransom payments, incident response and recovery expenses, downtime and lost productivity, legal settlements and regulatory fines, insurance premium increases, crisis management costs), there are less tangible effects that exact a heavy toll over the longer term. The damage to a company's reputation and brand, the loss of customer and employee confidence, the increased cost of capital, and other long-tail effects can drag down revenues and market share for years and even jeopardize the survival of the company.

Moreover, the harm caused by breaches goes beyond the impacts on individual organizations. It can affect whole supply chains, industries, and the broader economy, as well as public health and safety in the case of vital infrastructure and healthcare systems.

Impacts of breaches

In a recent survey, cybersecurity executives were asked to list the biggest impacts of breaches on their organizations. The most-cited impact was reputational loss, followed by business disruptions and the cost of responding to the incident.[18]

% citing as the main impacts of material breaches	All	Industry high
Reputational loss—reduced market share, higher capital cost, rating downgrade	**37%**	Life sciences **48%**
Business disruption—staff downtime, costs of business interruption	**31%**	Retail **40%**
Response costs—managing disruption, notifying customers/stakeholders	**27%**	Media and entertainment **39%**
Direct losses—financial theft, compensation to victims	**21%**	Technology **26%**
Opportunity costs—foregone gains due to diverted management attention	**19%**	Retail **26%**
Replacement costs—repair/replace capital assets, recover data	**19%**	Healthcare **29%**
Customer (or citizen) losses—lower client retention, sales	**14%**	Public sector **22%**
Fines and legal expenses—litigation, regulatory fines	**13%**	Telecoms **20%**
Intellectual property—loss of IP and confidential data	**13%**	Automotive **19%**
Supply chain/ecosystem losses—disruption, higher costs	**11%**	Consumer, manufacturing, retail **18%**

[12] Data breaches break record in 2021, CNET, January 2022
[13,14] 2021 Cost of a Data Breach Report, IBM, July 2021
[15] FTC Announces Final Settlement Over Equifax's 2017 Data Breach, Forbes, February 2022
[16] Breach Costs—Millions of Lost Revenue, Security Scorecard, March 2022
[17] T-Mobile Faces Two New Class Action Lawsuits After Data Breach Leaked User's Social Security Numbers, Birth Dates, and Other Personal Data, Top Class-Action Lawsuits, September 2021
[18] Cybersecurity Solutions for a Riskier World, ThoughtLab, May 2022

A tipping point

The trends described above have been underway for years, but they went into warp drive due to the pandemic and associated economic and geopolitical upheavals. As a result, cybersecurity has reached a tipping point. Traditional security approaches that rely on reactive, detect-and-respond measures and tedious manual processes can't keep pace with the volume, variety, and velocity of current threats.

The number of vulnerabilities (hundreds of thousands or even millions of instances in large organizations) is simply too great for conventional brute force tactics ("scan-and-patch-everything"). Many assets, particularly network devices and OT systems, are impossible or impractical to scan and patch in any case. And all too often, organizations don't even have full visibility into their attack surface. They can't see all their assets, environments, vulnerabilities, and exposures, let alone remediate them. In fact, 44% of cybersecurity executives cite "unknown assets" as one of the top causes of successful breaches.[19]

Cybersecurity teams who continue to depend on traditional methods and tools are losing ground as workloads swell and backlogs mount. While threat actors are moving ever more swiftly to exploit new vulnerabilities, the time it takes security teams to detect and address those vulnerabilities is lengthening.[20] So is the time to detect and respond to cyberattacks, which stretched to 280 days in 2021.[21]

> **"For executives around the world, data security risks are escalating faster than their ability to mitigate them."[22]**

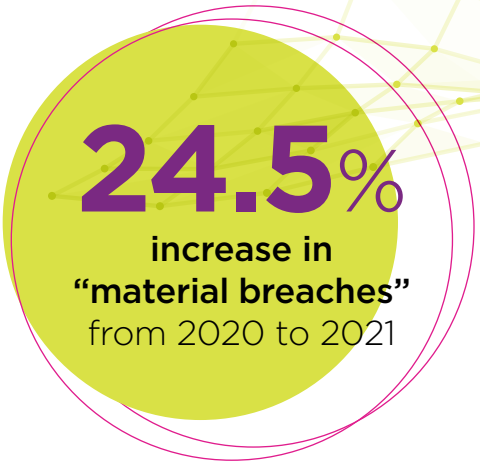
Reduce breaches with a risk-based approach

The status quo is unsustainable. The threat landscape has evolved dramatically while cybersecurity practices have lagged behind. **In fact, the number one cybersecurity challenge is inadequate identification of key risks.[23]** It is not simply a matter of tweaking the existing paradigm or spending more money while maintaining business as usual. Traditional methods are far too little, too late in an era of exponentially increasing risks. **No wonder 27% of all executives and 40% of chief security officers say their organizations are not well prepared for today's rapidly shifting threat landscape.[24]**

As worrisome as that may sound, there is cause for optimism. A landmark new study, *Cybersecurity Solutions for a Riskier World*,[25] reveals how a select group of organizations is flipping the narrative, jettisoning the old scattershot, reactive model, and turning cybersecurity into a rigorous, precise process that can successfully identify and reduce risks proactively, with demonstrably better outcomes.

The study surveyed executives and analyzed the cybersecurity investments, practices, and performance of 1,200 companies and public-sector organizations in 16 countries and a wide range of industries. It's one of the largest cybersecurity benchmarking studies with C-level decision-makers ever undertaken. What makes it so significant is that it not only shows how conventional cybersecurity approaches are falling short but also how some organizations are bucking the trend.

[19] Cybersecurity Solutions for a Riskier World, ThoughtLab, May 2022
[20] Average time to fix critical cybersecurity vulnerabilities is 205 days: report, ZDNet, June 2021
[21] 2021 Cost of a Data Breach Report, IBM, July 2021
[22,23,24,25] Cybersecurity Solutions for a Riskier World, ThoughtLab, May 2022



The researchers found that, on average, organizations experienced 15% more cybersecurity incidents in 2021 than in 2020, and “material breaches”—defined as “those generating a large loss, compromising many records, or having a significant impact on business operations”—jumped 24.5 percent.[26]

The top four causes of breaches as reported by the affected organizations were:

- Human error
- Misconfigurations
- Poor maintenance/lack of cyber hygiene
- Unknown assets

What’s notable about this list is that all of these conditions result from mistakes or inadequate processes inside organizations—which means they are all in principle avoidable. The clear implication is that, however pernicious external threats have become, cybersecurity teams still have the power to repel them. And that’s the good news: With the right practices and tools, the probability of breaches can be sharply reduced.

The study bears this out. One of its most eye-opening findings is that though organizations on average saw a big uptick in incidents and material breaches in the past two years, a distinct subset had few or no breaches at all. What sets these exceptional organizations apart? The researchers found that firms with fewer breaches were different from the rest of the pack in two fundamental respects.

For starters, they tended to rank higher in cybersecurity progress as measured by the NIST framework. The framework, developed by the National Institute of Standards and Technology, provides guidelines that help companies evaluate and improve their cybersecurity maturity in activities such as detecting and responding to incidents.[27]

Beyond the NIST framework, organizations with no breaches took what the researchers call “a risk-based approach” to cybersecurity. This second step is crucial. While NIST and similar frameworks help companies assess their cybersecurity maturity and identify gaps, they don’t specify how to close those gaps and mitigate risks. **As the FAIR Institute (a non-profit that promotes risk management best practices) puts it, “Risk frameworks from organizations such as NIST, ISO, OCTAVE, ISACA, are useful for defining and assessing risk management programs. They all prescribe the need to quantify risk, but for the most part, they leave it up to the practitioners to figure it out.”[28]**

“Figuring it out” is exactly what the risk-based approach does. As the benchmarking report explains, “A risk-based approach is key to achieving cybersecurity proficiency: it enables organizations to identify, measure, prioritize, and manage the cyber threats they face in line with their enterprise risk management framework.”[29]

> “Combining a risk-based approach with a maturity model **boosts cybersecurity results**. Our research shows that organizations that excel in the areas of risk-based management saw **fewer incidents** and material breaches than others in both 2020 and 2021.”[30]

[26] Cybersecurity Solutions for a Riskier World, ThoughtLab, May 2022
[27] NIST Cybersecurity Framework, National Institute of Standards and Technology
[28] What is FAIR?, The FAIR Institute
[29,30] Cybersecurity Solutions for a Riskier World, ThoughtLab, May 2022

Leading
risk-based organizations

EXPERIENCED **fewer incidents**

48% had no breaches

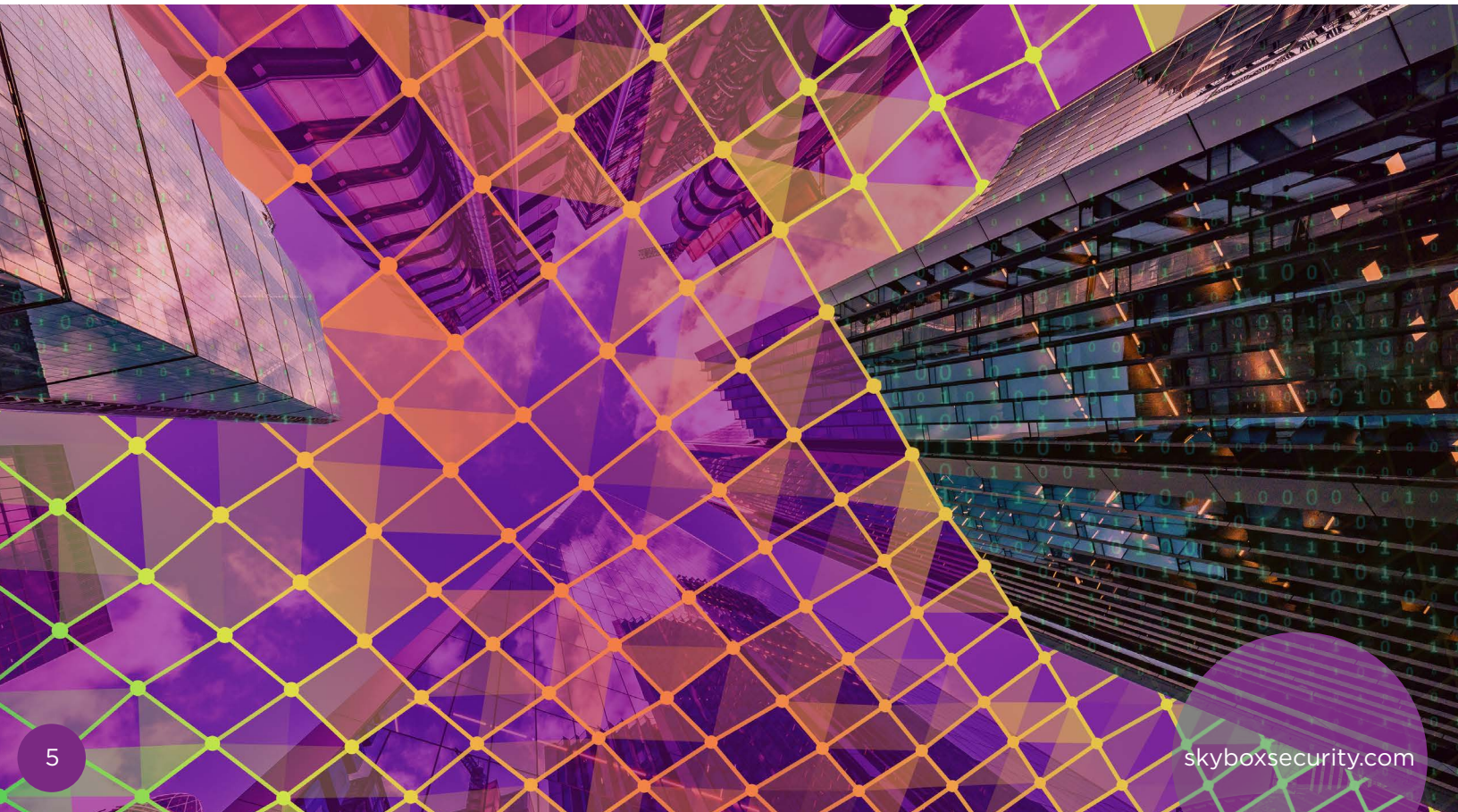
50% were top performers in time to mitigate

46% were top performers in time to respond

The benefits of a risk-based approach are clear in the benchmarking report. Leading risk-based organizations—which comprised 23% of the 1,200 organizations studied—experienced fewer incidents and fewer material breaches in 2020 and 2021. Forty-eight percent of organizations with no breaches in 2021 were risk-based leaders. Not only were risk-based leaders less likely to be breached, but they were also better at mitigating and responding to breaches that did occur. The study found that 50% of the top performers in time to mitigate a breach and 46% of the top performers in time to respond to a breach were risk-based leaders. The report adds that "given that today's risk leaders have still more progress to make on implementing risk-based management, these performance correlations understate the full potential of applying this discipline."[31]

The study also found that when it comes to applying a risk-based framework, some industries are further along than others. Life sciences, financial services, and automotive companies are the most mature, and healthcare, manufacturing, and media/entertainment are the least.

[31] Cybersecurity Solutions for a Riskier World, ThoughtLab, May 2022



Leading organizations embrace risk-based cybersecurity

Looking more closely at the ingredients of a risk-based approach and the specific practices that distinguish risk-oriented organizations from their less proficient peers, the benchmark study found that risk-based leaders excelled in seven key areas beyond the NIST framework:[32]

- **Attack surface visibility and context**
- **Attack simulation**
- **Exposure analysis**
- **Risk scoring**
- **Vulnerability assessments**
- **Research (threat intelligence)**
- **Technology assessments and consolidation**

This makes sense. Risk-based cybersecurity is fundamentally about accurately assessing (identifying, measuring, and prioritizing) and effectively managing (eliminating or mitigating) risks, and all of the processes on this list contribute to those ends.

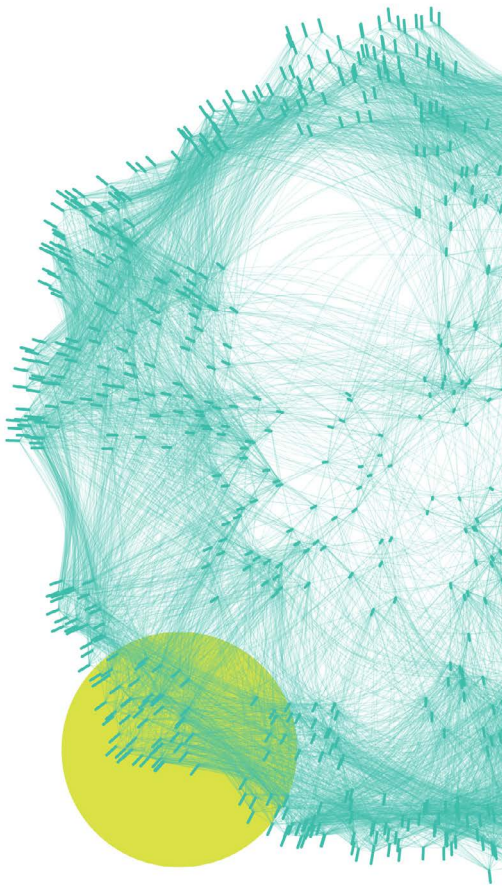
Putting these processes into practice in a way that markedly improves cybersecurity performance and achieves the goals of risk-based management requires a set of advanced capabilities—capabilities missing from traditional tools and practices:

+ **Comprehensive discovery and network model**
+ **Simulation and analysis**
+ **Cyber risk quantification and prioritization**
+ **Vulnerability remediation**
+ **Security policy management**
+ **Proactive security policy management**

> **You must take a risk-based approach because you can't secure everything a hundred percent.** There are a lot of questions to ask: What is the business of the business? What does the risk profile look like? What are the threats? What are the implications? And what is the governance process that an organization goes through to make risk-based decisions? Today, risk assessment is mostly subjective, but there are start-ups out there with new tools that will allow a much more quantitative model—the cyber world isn't there yet, but it's heading there."
>
> – Gary McAlum, Board Director, National Cybersecurity Center[33]

[32] The researchers note that, when measuring risk-based maturity, "we also incorporated the progress that respondents have made on risk assessment, risk management strategy, and supply chain risk management as prescribed by the NIST framework. In addition, we adjusted our rankings to reflect their investments in conducting regular risk assessments, audits, stress tests, and penetration tests, as well as investments in cyber risk modeling and assessment platforms."

[33] Cybersecurity Solutions for a Riskier World, ThoughtLab, May 2022



Comprehensive discovery and network model

The breakneck adoption of new technologies, the growth of shadow IT, and the heterogeneous nature of today's digital environments have made it increasingly hard for organizations to visualize their entire attack surface and track vulnerabilities. Active scanning, the traditional go-to method for detecting vulnerabilities, leaves many blind spots (where assets are unknown or unscannable) and gaps (between scan events).

Organizations need a unified 360-degree view across their entire IT and OT environments, including cloud and multi-cloud domains. That's only possible using advanced solutions that:

+ **Collect information on assets, configurations, and vulnerabilities from a wide variety of sources:** network and security infrastructure, public and private clouds, configuration, patch and asset management systems, EDR solutions, threat intelligence feeds, OT passive scanning solutions, and more. Non-intrusive scanless detection techniques can address blind spots in active scanning solutions by providing a continuous view of vulnerability risk and exposure in network and security infrastructure.
+ **Aggregate and normalize the collected information to create a holistic network model.** The model is a dynamic representation of the connectivity and configurations across the entire hybrid environment. It provides a comprehensive understanding of all security controls and network configurations in place.

Simulation and analysis

The network model enables several types of simulation and analysis needed to identify risks:

+ **Attack simulation** emulates potential attacks that could be used by malicious actors.
+ **Path analysis** maps all possible network paths that packets can take across a hybrid network, uncovering potential attack vectors.
+ **Exposure analysis** identifies exploitable vulnerabilities and correlates them with an organization's unique network configurations and security controls to determine if they're exposed to attack. Exposure analysis has become such an important part of risk reduction that it has given rise to an emerging discipline called **exposure management**.

These simulations and analyses provide a critical understanding of the security protections in place as well as the exposures, gaps, and misconfigurations that create openings for attacks. This understanding—which traditional tools don't provide—is necessary to accurately assess risks.

Cyber risk quantification and prioritization

It's not enough to merely identify vulnerabilities; it's crucial to measure the actual risk that vulnerabilities pose to an organization. This enables teams to focus remediation efforts on those vulnerabilities with the potential to do real harm and avoid wasting precious resources on non-issues. Conventional risk management approaches that focus primarily on the severity of vulnerabilities (as measured by CVSS, the common vulnerability scoring system) miss the mark because severity alone is a poor guide to risk. Severe vulnerabilities may actually be low-risk because they're not exposed to attackers, or because there are no active attempts to exploit them, or because they don't affect important assets; the opposite may be true for lower-severity vulnerabilities.

It's therefore essential to apply advanced multi-factor scoring that evaluates not only severity but also exploitability, asset importance, and exposure. Exposure analysis, which is absent in most risk-scoring solutions, is especially vital since it can distinguish the small subset of vulnerabilities that are exposed from the typically much larger number of vulnerabilities that aren't. Exposure analysis can reduce remediation workloads by several orders of magnitude (from hundreds of thousands of vulnerabilities to a few thousand in larger organizations).

Some cutting-edge solutions have gone even farther, incorporating the financial impacts of an asset's loss into their risk-scoring algorithms and allowing security teams to articulate cyber risk in terms that resonate in the boardroom. This new level of cyber risk quantification (CRQ) gives businesses an objective methodology for prioritizing risks and investments, allocating resources, and demonstrating the ROI of their cybersecurity budgets.

> **"Even with unlimited budget and resources, it would be impossible and impractical for the security organization to address every single threat. The fast-moving and evolving nature of cyberattacks requires CISOs to act quickly and decisively to mitigate those risks with the greatest impact on the business. By quantifying assets and expressing the dollar value at risk from cyber events, CISOs can target their risk mitigation strategies on the most significant risks with most consequence to the firm."**
>
> – Forrester Research[34]

Vulnerability remediation

After risks are identified and scored, advanced tools can recommend a range of practical remediations. The options go well beyond patching (since patching may not be possible or feasible in many cases, especially in network and OT devices) and include adjusting configurations, enforcing appropriate policies, applying IPS signatures, implementing network segmentation, and more. In addition to recommending remediations, solutions can help facilitate their implementation (via integrations with IT service management solutions) and ensure that they are properly maintained (via change management systems).

[34] Transform Cyber Risk with Cyber Risk Quantification, Forrester Research, Inc., January 2022

Security policy management

Vulnerability management is a big part of effective risk-based cybersecurity, but it's not the only part. Security policy management also has a vital role to play, reducing risks by minimizing weaknesses in security configurations and ensuring that organizations adhere to best practices set by regulatory bodies and company policies. The benchmark study found that network security policy management was one of the top five technologies that organizations with no breaches invested in, and that optimizing security policy management is one of the top cybersecurity investments executives plan to make in the next two years.[35]

"The presence of a high level of compliance failures was associated with breach costs that were $2.30 million higher than breach costs at organizations without this factor present."[36]

Automated compliance verification can substantially improve and streamline compliance processes. Such solutions use a network model to check network and asset configurations against regulatory frameworks and company policies.

Smart automation

The labor-intensive, manual methods still used by many organizations and tools are no match for today's complex cybersecurity challenges. Intelligent automation is an absolute must for a modern, risk-based approach. Automation can be applied to all key phases of risk-based cybersecurity, including holistic discovery, network modeling, analysis and simulation, cyber risk quantification, remediation workflows, policy management, change management, and tracking and reporting.

> **Automation will become even more critically important going forward. The war for talent is tough in our discipline, and automation can help you fill in the gaps when you don't have all of the people that you need all of the time. Automation also helps you retain talent, because they can avoid working on lower-level tasks. Work becomes less monotonous."**
>
> – Curley Henry, VP and CISO, Southern Company[37]

By automating these processes, advanced solutions can speed the time to identify and mitigate risks and shrink the window of exposure. Automation saves labor costs, eliminates repetitive tasks, and reduces burnout. It also reduces human error and captures and preserves institutional knowledge by systematizing best practices.

As the benchmarking study explains, "Automation helps to deliver better results: it reduces mundane work, drives efficiencies, frees up staff, and enables a more blanket approach to cybersecurity: fighting machines with machines. One CEO notes that companies are embracing automation at record levels to optimize workflows, implement changes, validate network security policies, and accelerate detection and response time."[38]

[35] Cybersecurity Solutions for a Riskier World, ThoughtLab, May 2022
[36] 2021 Cost of a Data Breach Report, IBM, July 2021
[37,38] Cybersecurity Solutions for a Riskier World, ThoughtLab, May 2022

Proactive security posture management

It's clear from the benchmarking study that risk-based management can't be done in a reactive, piecemeal manner. The old patchwork approach to cybersecurity, with its siloed teams, disparate functions, and disconnected tools, is a non-starter in today's hyperconnected and interdependent digital world.

> **"Those advanced in NIST are moving to a platform approach rather than using many individual solutions, and more than a third of entities with no breaches plan to consolidate their tools."[39]**

For instance, vulnerability management, security policy management, and change management have typically been treated as completely separate functions, but they're actually interlocking pieces of an overall risk-reduction strategy. Vulnerability management is necessary to identify, prioritize, and remediate weaknesses. Policy management is required to ensure that security controls and network segmentation are set properly to minimize exploitation and associated risk. And change management helps ensure that proper remediations, controls, and configurations are maintained over time while not exposing the organization to new risks.

As these examples illustrate, organizations must take a unified approach to cyber risk management. It should encompass everything from security planning, deployment, and remediation to compliance and change management. There's a name for this holistic approach: security posture management. The goal is to ensure overall security efficacy and reduce risks across an organization's entire estate by harnessing the best people, practices, and technology.

Just as processes need to be integrated, so should tools. Vulnerability management and security policy management solutions, for example, should interoperate—ideally as part of a single platform leveraging a common network model.

CISOs' expanding roles reflect a greater focus on reducing risk

As modern cybersecurity programs shift toward a risk-based approach, the job of the CISO is broadening accordingly. In the benchmarking study, CISOs were asked how their roles have changed over the last two years. Nearly half of respondents cited their growing responsibility for compliance and privacy—a result of proliferating new regulations and policies that are raising the risk of non-compliance. A large number of CISOs likewise reported greater involvement in OT security as those systems come under increasing threat. CISOs are also doing more to fight fraud, reduce vendor and supply chain risk, and improve resilience and business continuity. A number of respondents said that their duties now extend beyond IT and now encompass security posture management as a whole.

[39] Cybersecurity Solutions for a Riskier World, ThoughtLab, May 2022

SKYBOX SECURITY

How the CISO role has shifted across industries

In the benchmarking research study *Cyber Security Solutions for a Riskier World*, 1,200 C-level cybersecurity decision makers were asked: "How has the role of the CISO changed in your organization over the last two years?" The chart below depicts the top three answers per industry.

	Aerospace & defense	Automotive	Consumer goods	Energy & utilities	Financial services	Healthcare	Manufacturing	Insurance	Life sciences	Media & entertainment	Public sector	Retail	Technology	Telecoms
Expanded responsibility relating to data privacy and compliance	●	●	●	●	●		●	●	●	●	●	●		●
Greater management of operational technology						●	●							
Greater focus on security posture than IT	●			●				●						
Greater management of customer and insider fraud	●	●	●	●	●	●	●		●	●	●	●		●
Growing role in vendor, third-party, and supply chain management			●		●							●		●
Greater role in operational resiliency and business continuity						●				●	●			
Increasing interaction with the board of directors and senior management														
Greater involvement in enterprise and geopolitical risk management								●						
Greater influence over the organization's strategy and operations		●							●					
Partnering more closely with other functions and departments														
Increasing involvement in product development								●						

● Indicates one of the top three options chosen by industry

A risk-based approach delivers major business benefits

The combined effect of these risk-based techniques is transformative. Powered by next-generation automated solutions, risk-based management puts cybersecurity on an entirely new and stronger footing. It enables organizations to get out of firefighting mode and get ahead of threats, shifting the dynamic:

FROM	TO
+ Partial awareness	+ Holistic visibility
+ Guesswork	+ Certainty
+ Manual labor	+ Automated efficiency
+ Intermittent	+ Continuous
+ Reactive	+ Proactive

Adopting a risk-based approach can unlock a host of benefits for cybersecurity teams and businesses as a whole.

Fortified security posture

With its unprecedented ability to detect, measure, and stem cyber risks wherever they reside (whether in IT, OT, public cloud, or private cloud environments), risk-based management enables organizations to preemptively shore up defenses, improve resistance to attacks, and prevent misconfigurations and other forms of human error. That not only helps companies avert the potentially enormous financial losses and other damage that breaches inflict but can also yield immediate dividends in the form of reduced insurance premiums, greater customer confidence, improved reputation, and greater predictability and resilience.

Precise quantification

The new discipline of cyber risk quantification brings greater precision to cybersecurity risk management through practical application of investment theory principles. The ability to measure the actual financial impacts of risks enables leaders to make better-informed decisions, fine-tune spending, and demonstrate the ROI of their programs.

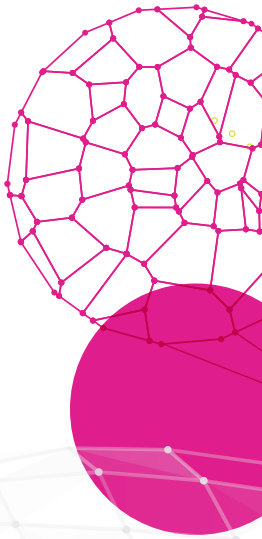
Greater productivity

Best-in-class risk-based solutions can boost productivity by automating laborious manual processes, by slashing the number of vulnerabilities that need to be remediated (thanks to better risk scoring), by speeding the time to remediate, and by enabling teams to better allocate limited resources. Cybersecurity organizations can do much more with less, managing complex heterogeneous environments with lean teams. Freed from menial tasks and no longer stuck playing catch-up, cybersecurity practitioners can go on the offensive, pursuing strategic initiatives that further improve processes and business resiliency.

Improved compliance

Automated policy management lets organizations efficiently navigate an increasingly complicated maze of regulations. It dramatically improves the efficacy of security controls, speeds and improves compliance processes, reduces human error, improves audit readiness, and unburdens overworked staff. Automated change management solutions can help maintain continuous compliance.

> **Security is all about the management of risk,** and the key element in any risk assessment is the business impact—your risk profile has to map to what you are trying to do as an organization. Generally, across the enterprise, you will probably be doing qualitative-based risk assessments, but in some areas a quantitative approach will be the way to go because your board or finance director will want to know the numbers. Because the threat landscape changes so very quickly, forecasting threats—particularly when they will come to pass—is increasingly difficult, even though mature organizations are getting very good at forecasting what those threats might be. Many large companies already have competency in risk assessment in the enterprise risk management group, but often it may not be accessible to the cybersecurity group because of internal politics and corporate silos—that needs to change."
>
> – Steve Durbin, CEO, Information Security Forum



Making the business case for security posture management

The business impact of successful risk-based security posture management—versus the old status-quo, detect-and-respond approach to cybersecurity—is hard to overstate. By preventing or mitigating breaches, risk-based methods and integrated security posture management can save companies many millions of dollars per year and prevent untold damage to reputation, customer trust, company morale, market standing, and competitiveness. In extreme cases, it may make the difference between the survival and extinction of the company itself. By improving efficiencies and reducing workloads, automated risk-based solutions can help companies trim costs while accomplishing more—boosting productivity in a time of tight resources and economic instability.

In addition, techniques like cyber risk quantification eliminate the guesswork of traditional cybersecurity and support improved, data-driven decision-making, prioritization, and forecasting. CRQ can also help demonstrate the benefits and justify investments in risk-based cybersecurity to CEOs and boards. Armed with hard numbers, CISOs can make a powerful business case. They can communicate the organization's risk exposure—and potential losses if breached—in financial terms. And they can document the costly inefficiencies of traditional scattershot security practices and quantify the enormous savings that are possible with precise, prioritized, proactive security posture management.

About Skybox

Over 500 of the largest and most security-conscious enterprises in the world rely on Skybox for the insights and assurance required to stay ahead of dynamically changing attack surfaces. At Skybox, we don't just serve up data and information. We provide the intelligence and context to make informed decisions, taking the guesswork out of securely enabling enterprises at scale and speed.

Our security posture management platform delivers complete visibility, analytics, and automation to quickly map, prioritize, and remediate vulnerabilities across your organization. The vendor-agnostic platform intelligently optimizes security policies, actions, and change processes across all corporate networks and cloud environments. With Skybox, security teams can focus on the most strategic business initiatives while ensuring enterprises remain protected.

Interested in speaking with an expert to help solve your greatest security challenges?

Contact us.
skyboxsecurity.com

SKYBOX SECURITY