DARKREADING
RESEARCH

JUNE 2025

Qualys State of Cyber Risk Assessment Report

Commissioned by Qualys

Qualys.

Executive Summary

Cyber-risk management is on the cusp of a new age in maturity. The security industry is still mired in trench warfare — spreading efforts far and wide but not deep. This won't stand against modern chaotic actors and adversaries armed with AI bent on infiltrating your ranks to target your most valuable assets. While some defenders are changing strategy — focusing their limited resources on what the business stands to lose — most remain stuck in a war of inches they can't possibly win.

Cybersecurity is moving beyond the era where vulnerability remediation and asset risks are managed solely based on the criticality of the flaw. Unfortunately, many organizations still do not excel at examining risk based on business context — that is, understanding the value-at-risk in terms of one's critical assets.

Results from the 2025 State of Cyber-risk Assessment report show that awareness is growing for business-focused cybersecurity risk management. Nearly half of organizations today have a formal program, and more are on the horizon. The majority of organizations today do some kind of periodic asset discovery. And the rate of those that use contextual factors beyond just vulnerability severity from scan results as a way to assess risk to those assets is on the rise.

These results are promising, but they also show that there's significant ground to cover in the cyber-risk management maturity journey for most organizations.

Many respondents said their risk levels are rising due to the increasing volume and sophistication of attacks, the growth in exposure from expanding asset portfolios, and the complexity of infrastructure from areas like cloud and AI/ML applications. At the same time, there's still a high reliance on manual work. Most businesses focus on vulnerability criticality informed by threat intelligence. However, they do so without considering business context around assets. This means they're still not prioritizing work in a way that meaningfully reduces business risk over time.

Just 18% of organizations use integrated risk scenarios that focus on business-impacting processes, showing how investments manage the likelihood and impact of risk quantitatively, including risk transfer to insurance. This is a key deficiency, as business stakeholders expect the CISO to focus on business risk.

Some highlights from the report findings include the following:

Momentum growing for formal risk programs

- 49% of organizations have a cyber-risk management program
- 43% of these programs are under 2 years old
- 19% of organizations plan to establish a program in the next year
- 71% of all organizations say their risk levels are increasing or holding steady

Risk prioritization a work in progress

- 70% of organizations use regular security assessments to identify cybersecurity risks
- Almost 1 in 3 organizations have a cyber-risk quantification strategy
- However, only 43% of organizations involve business stakeholders in the risk management process

Asset inventorying is common, but discovery frequency is still spotty

- 83% regularly conduct comprehensive inventories of IT assets
- But only 13% say they can do this continuously
- 64% of organizations use asset discovery tools
- But 47% say they also rely on manual asset inventory methods

Security data analysis still pretty tactical

- 54% of organizations say they use a centralized SIEM for tracking and compiling security risk data
- That's in contrast to just 32% that use GRC platforms or integrated risk management solutions
- Plus, almost 1 in 3 organizations say they rely heavily on manual spreadsheets to track security metrics

Many organizations are trying to layer in asset value as context to visibility

- 69% of organizations use asset value moderately to somewhat well to support risk management
- 19% of organizations say they use a single industry score like CVSS to rank risks across their assets

Reporting more frequent but without enough business context

- 90% of organizations today report cyber-risk findings to senior leadership and boards
- The most common reporting interval is quarterly
- Only 9% continually report with real-time dashboards and alerts

Risk Perceptions and State of Formal Programs

Even though most organizations today don't have anything close to real-time visibility or awareness across their IT asset portfolio, security and IT leaders seem confident in their ability to identify all of their most valuable IT assets. The study showed 84% of respondents reporting that they're very to somewhat confident of their capabilities on this front. As we dig deeper, we find indications that some of that confidence may be overstated.

While awareness is growing and work is being done to focus on business-impacting risk, the reaction to that awareness may lead to a 'worse than doing nothing' situation for many security teams. The appearance of sophistication can make security teams feel better about what they are doing without actually solving the problem.

Currently, the industry is at a point where organizations with a formal cyber-risk management program are still in the (slim) minority, which is concerning given the rapid expansion of cloud-native infrastructure and AI. Approximately, 49% of organizations said they have a formal program. However, a significant chunk of those said they have a program with a bit of a caveat.

Nineteen percent of organizations say they have a program, but it doesn't effectively manage cyber-risk in the context of broader business risk **(Figure 1)**. So, while we're seeing a growing interest and need for formal cyber-risk management programs, even among the one-fifth or so that do have a formal program, there still needs to be more understanding around prioritization as it pertains to business context.

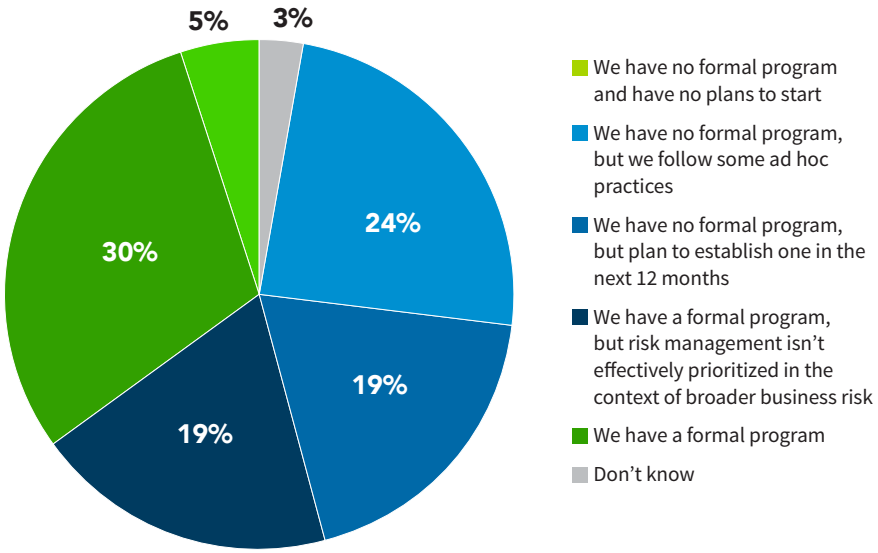
This is understandable considering that many programs are in their infancy, with 43% of those with programs stating that they've only been running them for two years or fewer. The results indicate that these newly minted programs are building momentum, as questioning revealed there are more new programs in the works at other organizations. Close to 1 in 5 organizations say they've got plans to establish a cyber-risk program in the next 12 months.

Whether they've got programs or not, the risks levels reported by respondents across all of their assets are rarely receding. A majority (51%) of respondents reported that their total risk level is increasing, and another 20% said it is holding steady. Just 6% reported their risk levels as decreasing. Of course, the big question to ask those

Figure 1

FORMAL RISK PROGRAM

Does your organization have a formal cyber risk management program that consistently identifies, prioritizes, manages and monitors risks to information systems in the context of business risk?



Data: Dark Reading survey of 108 IT and cybersecurity managers and executives, October 2024

without a fully functional program predicated on identifying and protecting assets based on value-at-risk is how they truly know what their risk levels are?

The top five biggest perceived threats that add risk to organizations' internal and external digital assets were:

- Phishing and social engineering (66%),
- Ransomware attacks (60%),
- Insider threats (44%),
- Cloud security risks (36%) and,
- Advanced persistent threats (33%). **(Figure 2)**

One thing that jumped out about these results was the "Layer 8" or impact of human behavior on the operation and security of a system. With the top risk being phishing and social engineering, it was clear that people are seen as the weak links in an organization's security controls.

While 66% of respondents felt phishing and social engineering was a top threat, all this has to be understood in the context of business risk. Where does the organization have controls, and how much of a risk do these attacks pose to the crown jewel assets that are most valuable to a company? In other words, phishing or ransomware attacks may or may not be significant, depending on which asset it is impacting. Therefore, organizations first need to have a good understanding of their risk factors in relation to their business critical assets, and then figure out what kinds of threats those assets might be overly exposed to. This should be understood in terms of regulatory data loss, business disruption, wire fraud, and other major impacts to the business.

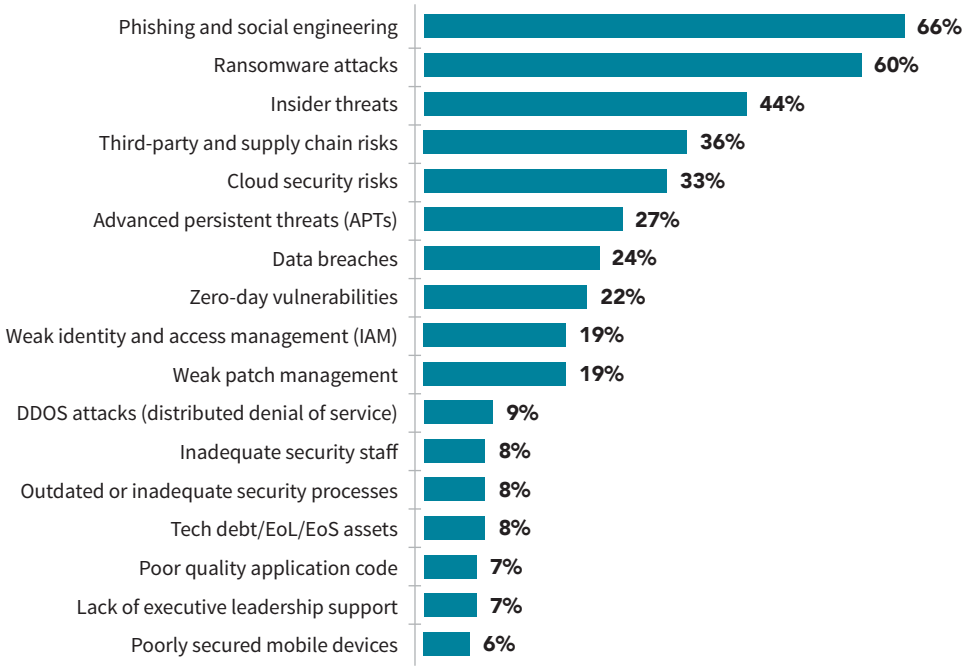
When we asked that plurality of respondents who said their risk levels are rising about why they think they're increasing, the common themes that came up time and again were around the increasing volume and sophistication of attacks, the growth in exposure from expanding asset portfolios, and the complexity of infrastructure from areas like cloud and AI/ML applications.

The following are some highlighted causes detailed by those worried about their perception of increased risk:

Figure 2

RISK TO DIGITAL ASSETS

Which of the following pose the biggest risk to your organization's internal and external digital assets?



Note: Maximum of five responses allowed
Data: Dark Reading survey of 108 IT and cybersecurity managers and executives, October 2024

- "Expanding business with increasing number of owned assets, as well as supporting customer offerings."
- "Expanding criminal activity in our vertical. Changing customer demands stretching capability and capacity to adapt to new IT systems and business practices."
- "Threats are increasing, assets and systems are increasing, but security team size has flat lined. Leadership pushes back on adding resources. Employee burnout is a major risk."

Among those who report their risk is neither rising nor falling, we asked them to explain why that is. The consensus was that they're investing significantly to mature their risk management capabilities, but they're still treading water with their risk management practices in the face of all those headwinds described above.

There were only a handful of high-performers who believe they're really moving the needle on controlling true business risk exposure. The refrain there is that they're programmatically assessing risks to their assets and using data-driven methods to manage the biggest risks.

Asset Discovery and Scoping Risk Assessment

One result that shows how far cyber-risk assessment has come in the last decade is that nearly all organizations today conduct some kind of comprehensive inventorying of their IT assets. And over half of organizations conduct these exercises at least quarterly. Some organizations are very mature in this discovery process, with a little over 1 in 10 reporting they do it continuously in real-time.

At the same time, there's still work to do at many organizations. Over a third of organizations only inventory their assets once or twice a year, on an ad hoc basis or aren't sure of the frequency of these exercises. Plus, the punctuated regularity of discovery of these assets at most organizations — be it monthly, quarterly, or annually — indicates that a lot of the inventory work remains tied to manual and point-in-time methods.

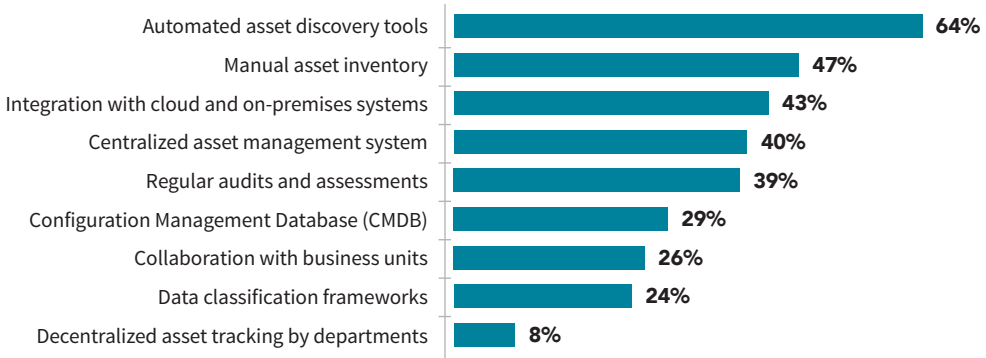
When asked about all of the different tools they use to identify, classify, and track the location of their most valuable IT assets, 64% of organizations did report that they do use automated asset discovery tools. However, the second-most common method and tooling was manual asset inventory, named by 47% of organization (Figure 3). Interestingly, this implies that manual asset inventory is still being leveraged by almost half of all respondents, and that some companies are probably using some combination of the two in order to keep track of all their assets.

While clearly, this situation isn't ideal, it also brings up a second implication. **Figure 3** shows again that we do not see enough business context — that is, understanding the value-at-risk in

Figure 3

TRACKING IT ASSETS

Which tools and processes does your organization use to identify, classify, and track the location of your most valuable IT assets?

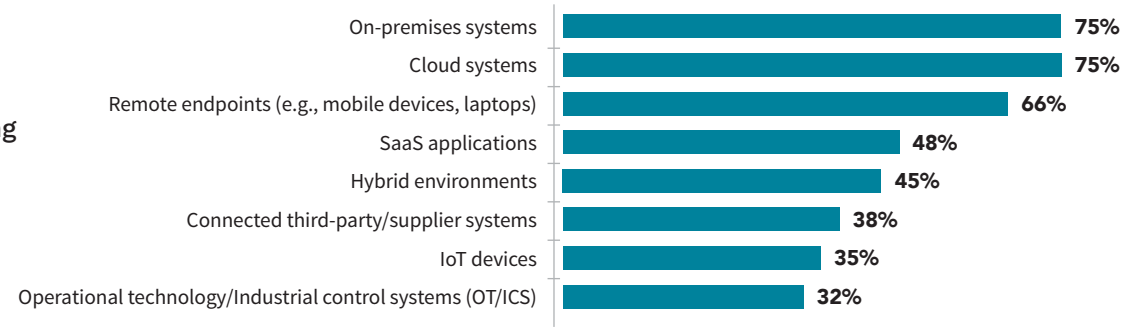


Note: Multiple responses allowed
Data: Dark Reading survey of 108 IT and cybersecurity managers and executives, October 2024

Figure 4

RISK MONITORING

Which of the following are in scope for cybersecurity risk assessment and risk monitoring?



Note: Multiple responses allowed
Data: Dark Reading survey of 108 IT and cybersecurity managers and executives, October 2024

terms of one's critical assets. While some of the options here could provide some of that broader enterprise context for what assets would be most valuable, such as a CMDB (29%), collaborating with other business units (26%), and data classification frameworks (24%), that grasp of business context to help prioritize and understand one's enterprise risk is still nascent at best.

When asked about which assets in their inventory are in scope for risk assessment and risk monitoring activities, the top three most common categories were on-premises and cloud systems (both 75%), and remote endpoints (66%) (**Figure 4**). Just a little under half of organizations reported that SaaS applications (48%) and hybrid environments (45%) were in scope. With digital transformation and the massive adoption of SaaS, it was surprising to see only 48% of respondents having SaaS applications in scope for risk monitoring. While most of those surveyed seem to be doing a good job of monitoring their on-premises and cloud systems, dependencies on a SaaS provider can be a huge area of risk exposure that enterprises are not paying enough attention to. SaaS-related compromise and loss can sometimes cause existential damage to a company's operations, through business disruption or loss, making your first- and third-party systems crucial to protect.

On the promising side, approximately a third of organizations continuously assess the risks to all of those internal and external assets that are in scope. However, another third either don't do comprehensive risk assessments at all, aren't sure how often they do them, do them only when they suspect a problem, or conduct these assessments annually. Another 27% say they only do them monthly or quarterly at best. There is certainly room to grow and improve in this area.

Using Asset Value to Fuel Risk Management

One thing that the results of this survey have made abundantly clear is that cybersecurity is moving beyond the era where vulnerability remediation and asset risks are managed solely based on the criticality of the flaw.

Increasingly, organizations are striving to find ways to — at a minimum — consider the business criticality and value-at-risk of an asset, the data it touches, and the role it plays in an organization's infrastructure as they prioritize risk management action around the asset.

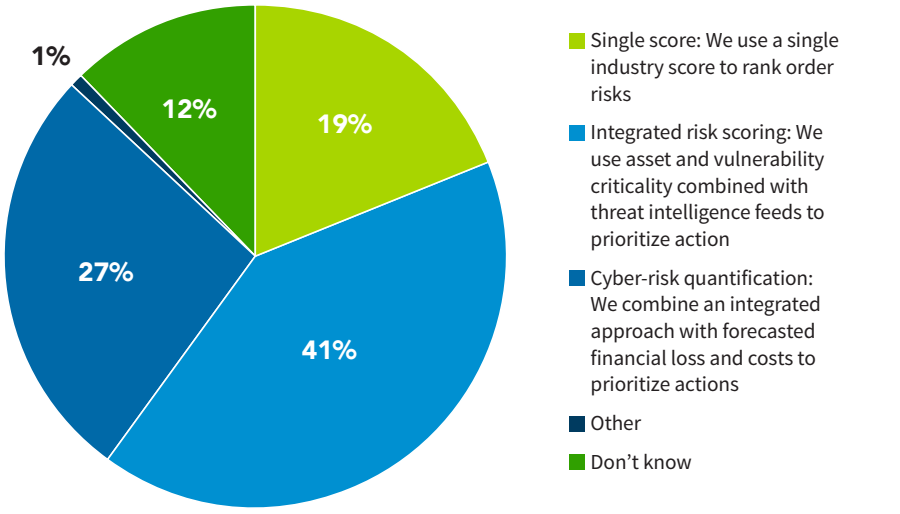
When asked about how they prioritize risks, only 19% of respondents said they use a single industry score like CVSS to rank order risks (**Figure 5**). Approximately, 68% use some form of integrated risk scoring that's combined with threat intelligence feeds to prioritize action.

In that class — a further 27% say they combine that integrated approach with forecasted financial

Figure 5

PRIORITIZING RISK

How do you currently prioritize risk with your business stakeholders?



Data: Dark Reading survey of 108 IT and cybersecurity managers and executives, October 2024

loss to refine their prioritization even more. This shows that many organizations are still getting prioritization backwards — they're engaging in trench warfare of cybersecurity. Organizations shoud prioritize what they stand to lose first. Everything else is a distraction, leading to spreading limited resources thinly across the attack surface.

Only about a quarter of organizations say they have an extremely mature asset discovery and classification program that uses those financial loss calculations to drive sophisticated risk prioritization. But another 69% say that they do use asset value moderately or somewhat well to support risk management.

The most common factors considered when classifying assets and determining their value to the business are:

- Criticality to business operations (70%)
- Sensitivity of the data (63%)
- And estimated value of the systems themselves (52%)

The frequency with which assets are reviewed and adjusted for their value is still relatively intermittent, though. An even half of organizations say they only update risk profiles biannually or annually or only after a significant system change. Just 18% say they do this adjustment monthly.

The results show that this frequency of reviews has a strong correlation with businesses' confidence in their risk management practices. A strong 67% of those who update their risk profiles on a monthly basis believe they prioritize risk management based on the value of their IT assets very well, eighty-two percent of those who only make profile updates after significant changes say they do this not very well at all or only somewhat well.

When asked what the most common methods used to prioritize mitigation of risks to IT assets, the top five answers in order of prevalence were: vulnerability severity (55%), potential business impact (45%), asset value and criticality (44%), regulatory compliance (42%), and likelihood of compromise (23%) (**Figure 6**). It's no surprise here that vulnerability severity was the top choice among respondents, as most risk scoring methodologies use heuristics such as vulnerability severity as their underpinnings. It's encouraging to see the industry now starting to take into consideration broader business context in their risk prioritization now, too. This is evident from how organizations are increasingly incorporating factors like likelihood of compromise, cost-benefit analysis, cyber-risk quantification and business stakeholder

Figure 6

METHODS TO PRIORITIZE RISK

What are the most common methods your organization uses to prioritize mitigation of risks to its most valuable IT assets during incidents and day-to-day security work?

Note: Maximum of three responses allowed
Data: Dark Reading survey of 108 IT and cybersecurity managers and executives, October 2024

input (9%) into their decision-making process on risk prioritization. Truly, any comprehensive risk scoring methodologies needs to take into account other contextual value like asset value-at-risk and business impact.

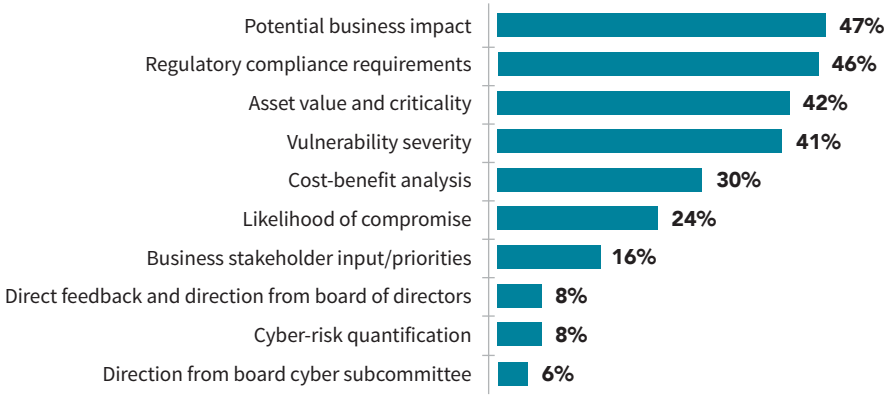
Notably, the results showed that only 13% of those surveyed are currently using cyber-risk quantification in their organizations to prioritize risks. Anecdotally, we have observed a desire from organizations and CISOs to do cyber-risk quantification more effectively — that is, using financial models and simulations to predict the likelihood of seeing a certain level of loss, mapping that probability to dollars as a measure of impact, and using that to make strategic decisions on accepting, mitigating or transferring risk. However, cyber-risk quantification can prove challenging to do well. The easiest approaches may provide incorrect or misleading results, while more complicated methods can take a lot of time or be cost-prohibitive.

Interestingly, when asked which methods influence long-term prioritization of investments and implementation of security controls potential business impact (47%) ranked first, followed by regulatory compliance (46%), asset value and criticality (42%), vulnerability severity (41%), and

Figure 7

METHODS FOR LONG-TERM PRIORITIZATION OF INVESTMENTS

What are the most common methods your organization uses to direct long-term prioritization of security investments and implementation of security controls?

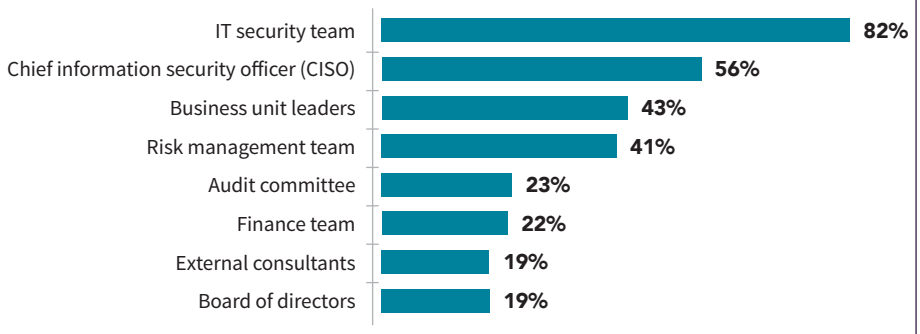


Note: Maximum of three responses allowed
Data: Dark Reading survey of 108 IT and cybersecurity managers and executives, October 2024

Figure 8

STAKEHOLDERS INVOLVED IN RISK MANAGEMENT

Which of the following stakeholders are involved in the risk management process for IT assets?



Note: Multiple responses allowed
Data: Dark Reading survey of 108 IT and cybersecurity managers and executives, October 2024

cost-benefit analysis (30%) (**Figure 7**). It was interesting to see that business impact was the primary factor that influenced long-term investment decisions, but it was not the main method for prioritizing the mitigation of risks as shown in the results for the previous question. This suggests that operationally, companies are taking a more tactical approach to deciding how to prioritize risk mitigation by choosing business continuity over everything else. Whilst when faced with a longer term, strategic investment decision, business context is the primary deciding factor.

The bottom line is that forward-leaning enterprises are adding more business impact into how they score their risks and make strategic investment decisions. It's still early days, but we forecast that the use of business risk as context for how organizations operationalize their security programs will continue to grow.

How Risks Are Judged and Prioritized

The most common approaches used by organizations to measure cybersecurity risks are qualitative risk assessments (58%) and risk scoring tools (54%). But 53% said they use expert judgment, indicating that many organizations still pin a lot of their assessment work on 'gut instinct' to determine risk levels. Far fewer are using quantitative risk models, which was only named by 32% of organizations.

While there is growth in the effort to use asset value to determine risk priorities, fewer than a third of organizations (30%) employ a defined cyber-risk quantification strategy when scoring risks. Among those, the most common methods employed are threat assessment and remediation analysis, probabilistic risk assessment, and threat modeling. Other methodologies like loss distribution, crown jewel analysis, value at risk analysis, and FAIR assessments are still relatively rare.

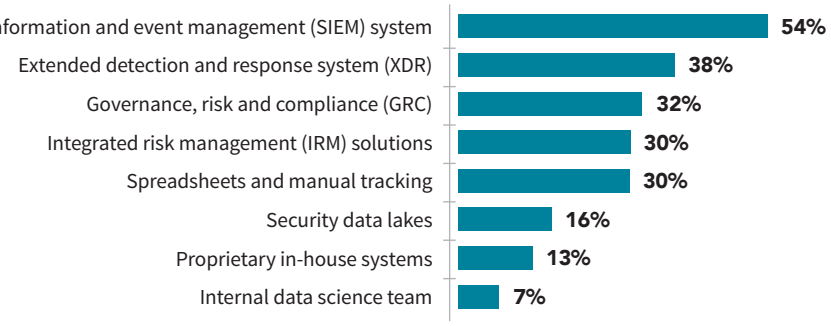
A lack of sophistication in tying business risk and business value to cybersecurity may stem from the relative isolation with which most cybersecurity practitioners are determining risk. Respondents were asked to name all of the stakeholders involved in the risk management process and 82% said the IT security team is involved, but only 56% said the CISO is involved, indicating that many teams still take a very tactical approach to evaluating risk (**Figure 8**). However, it may also be that CISOs are left with the technical elements of cyber while the risk assessment bubbles up to a broader risk team as 41% of respondents reported that they have a risk management team involved.

Meanwhile, just 43% of organizations say business stakeholders are involved, and a scant 22% say the finance team is involved — which makes us wonder how those majority of organizations that don't involve these stakeholders are able to effectively determine the criticality and value of assets to the business without that input.

Figure 9

PROCESSING SECURITY ANALYTICS

How do you primarily compile, organize, and process security analytics and risk information collected from different security tools?



Note: Maximum of three responses allowed
Data: Dark Reading survey of 108 IT and cybersecurity managers and executives, October 2024

Tracking and Compiling Risk Data

When we questioned respondents about the logistics of compiling, organizing, and processing security analytics and risk information, answers were fairly evenly distributed, indicating that there are a wide range of methods in play.

We asked them to give a top three ranking of how they track and compile relevant security and risk data and the top answers were still very heavily focused on security operations rather than risk management type platforms. Fifty-four percent of organizations say they lean most heavily on a centralized SIEM, and 38% said they leverage XDR platforms on this work (**Figure 9**). Ask any risk manager and they will tell you that these are telemetry tools and not even risk telemetry tools at that. Third, fourth, and fifth place were fairly evenly split with 32% reporting they use GRC platforms, 30% reporting they utilize integrated risk management solutions, and 30% saying they favor the familiar but very manual method of tracking things in spreadsheets.

The reality is that spreadsheets are still a core application, suggesting organizations may not be able to find commercial solutions in the market that can help them achieve the same outcome. Taking internal data science teams (7%), proprietary in-house systems (13%), security data lakes (16%), and manual tracking (30%) together, it becomes clear that two-thirds of respondents (66%) are relying on in-house solutions to compile and aggregate their security and risk data. This suggests a strong need for a context-rich commercial solution that can help organizations automate this process of measuring, communicating, and eliminating their cyber-risk more effectively.

The good news is that the majority of organizations today collect and analyze security performance metrics to track how well their program is reducing risks: Only 12% of organizations say they don't have set performance metrics. However, among those that do, the population is evenly split between those with simplistic risk KPIs and those with more mature sets of metrics. Some 41% say they only track the coverage and configuration of key security capabilities across enterprise assets with specific KPIs. Meanwhile, 36% say they use coverage and configuration metrics as table stakes and build on that by also tracking the operational efficiency of controls in terms of risk elimination, including mitigation and remediation.

Communicating Risk

Effective risk management requires good communication of risk factors to all of the relevant stakeholders in a way that speaks to value at risk versus threat scores, security KPIs and, so on. The business should be able to understand what they stand to lose and they can't gain that understanding when security leaders focus on vulnerability counts and such.

Figure 10

CYBERSECURITY RISK REPORTS

Which of the following are typically contained in the cybersecurity risk report or risk register presented to the company's senior leadership/ board of directors?

Note: Multiple responses allowed
Data: Dark Reading survey of 108 IT and cybersecurity managers and executives, October 2024

Fortunately, the number of companies who never report cyber risk findings to senior leadership and boards of directors is exceedingly rare — just 3% of firms admit to this. The most common reporting interval is a quarterly update, named by 40% of firms. Almost 1 in 5 of organizations do it more frequently, on a monthly basis or continually through real-time dashboards and alerts. In the meantime, 14% of organizations are only reporting up to the board once or twice per year.

These rates of reporting are promising. A decade ago, the numbers would have been very different.

The content of that reporting contained in a risk report is usually multifaceted, though often lacking implications around business impact. When asked about all of the elements in their risk register or risk report, the answers were very evenly distributed. The most common element was overall organizational risk level, named by 56%, followed by an outline of current cybersecurity plan (54%) (**Figure 10**). The next four choices were at nearly a dead heat with one another, including roster of significant, outstanding threats (48%), new technologies required to mitigate risks (47%), relevant regulatory compliance issues (46%), and risk quantification/risk scoring (42%).

Finally, while it didn't rank as highly as other elements, a significant 35% of the population also reports on their estimates of potential costs of security breaches when having those board-level discussions.

When communicating risk levels and risk scoring (and risk resolution) to the board, the most common method is KPIs and KRIs in terms of their progress quarter over quarter using PowerPoint, which was named by 29% of organizations. Approximately 1 in 5 companies use heat maps or risk registers that either use a 5x5 matrix or top N list of risks that qualitatively communicate what is important and how risk control is progressing. While again, these are commonly used methods, they fall short of providing quantitative context around risk in dollars and cents.

On the other hand, just 18% of organizations use integrated risk scenarios that focus on business-impacting processes, showing how investments manage the likelihood and impact of risk quantitatively, including risk transfer to insurance. Finally, another 14% use cyber-risk quantification that ties together integrated risk scenarios with financial quantifications.

In terms of reporting structures, a significant ratio — 36% of companies — have some kind of formal risk committee in place and an equal proportion say they don't have a committee but are meeting informally. This shows positive signs that collaborative decision-making is occurring around how to allocate security resources to protect business value. Additionally, a solid 60% of respondents say that the collaboration is ongoing, and that they also meet members of the board outside of board meetings.

Finally, that communication is a two-way street, with 80% of respondents saying that they get feedback from the board through formal meetings and reviews, written feedback and reports, and other forms of feedback. When they do receive it, this feedback helps risk leaders prioritize their projects and it influences their budget allocation.

Conclusion

In many ways, the cybersecurity and cyber-risk management community is failing to scale with the rate that the business is exposing value to the world via digital and AI transformation. Cybersecurity's lack of focus on value has spread limited resources too thin. This is a dire problem, and leaders need to focus on protecting what the business stands to lose in an economically and operationally efficient manner.

The following are some important ways businesses can make improvements on this front:

1) Business risk is all about context. In order to have a good understanding of organizational risk, a business first needs to understand what their business critical assets are, then understand their risk factors or threats as it relates to those crown jewel assets. Without this context, vulnerabilities or threats are just information.

2) If everything is critical, nothing is. Prioritizing risks is paramount as organizations do not have unlimited resources. In order to be capitally efficient, companies need to spend as little as possible to avoid the largest possible amount of risk. Whatever is not mitigated through technology represents risk that needs to be accepted, or transferred to cyber insurance. There are two types of prioritization:

a. Operational prioritization (tactical): where security teams rank order the vulnerabilities and misconfigurations that need their attention to be patched, mitigated or isolated

b. Business prioritization (strategic): determining whether or not to make capital investments based on business priorities, such as which security tools to buy to best suit their cyber-risk profile.

3) To get a good read of the cyber-risks across the enterprise, you need a diverse telemetry of risk signals. Organizations can't rely on just one — such as scanning for vulnerabilities — instead, companies need visibility into their application security, identity security stack, and more, every part of the enterprise that is exposing your attack surface.

4) Instead of focusing on reactive incident response — for example with a SIEM or a SOC — organizations need a better system that proactively looks to predict risks and works to reduce the likelihood of an event happening by implementing a Risk Operations Center (ROC). This approach to risk management helps leaders make better, more informed decisions based on their unique business context.

5) We need to overhaul the way we are communicating cyber-risk to the board. There is a need to communicate cyber-risk in quantifying dollars and cents to the board of directors, as money is the language of business. It is data- and time-intensive to be able to bring that information together in a consumable way, and remains a top need and critical issue. We foresee that integrated risk scenarios that focus on business-impacting processes, such as how investments and insurance impact risk, will be the future of "business-oriented" risk reporting, and much more effective at the purpose of communicating to board members.

About Qualys

Qualys, Inc. (NASDAQ: QLYS) is a leading provider of disruptive cloud-based security, compliance and IT solutions with more than 10,000 subscription customers worldwide, including a majority of the Forbes Global 100 and Fortune 100. Qualys helps organizations streamline and automate their security and compliance solutions onto a single platform for greater agility, better business outcomes, and substantial cost savings.

The Qualys Enterprise TruRisk™ Platform leverages a single agent to continuously deliver critical security intelligence while enabling enterprises to automate the full spectrum of vulnerability detection, compliance, and protection for IT systems, workloads and web applications across on premises, endpoints, servers, public and private clouds, containers, and mobile devices. Founded in 1999 as one of the first SaaS security companies, Qualys has strategic partnerships and seamlessly integrates its vulnerability management capabilities into security offerings from cloud service providers, including Oracle Cloud Infrastructure, Amazon Web Services, the Google Cloud Platform and Microsoft Azure, along with a number of leading managed service providers and global consulting organizations. For more information, please visit www.qualys.com.

Learn more about the Risk Operations Center (ROC) powered by Qualys Enterprise TruRisk™ Management at qualys.com/etm.

Methodology & Firmographics

Qualys commissioned Dark Reading to research the current state of cybersecurity risk, including identifying and assessing the risks to internal and external digital assets. The survey asked 108 cybersecurity and IT professionals who were familiar with their organization's cybersecurity risk governance.

The survey was conducted online in October 2024. Respondents were recruited via emailed invitations containing an embedded link to the survey. The emails were sent to a select group of Dark Reading's qualified database.

The survey queried respondents including IT and cybersecurity executive-level titles such as CIO/CTO (14%), CSO/CISO (11%), chief privacy officer (1%), chief risk officer (3%), VP of IT or security (3%). Other titles included cybersecurity director/head (15%), IT director/head (13%), and other manager-level respondents from application development, cybersecurity team, and general IT roles.

One-quarter of respondents (25%) worked at companies with under 100 employees, 29% at companies with 100 to 999 employees, 23% between 1,000 and 4,999, 11% between 5,000 and 19,999, and 12% at the largest-sized companies with 20,000 or more employees.

Respondents' organizations represent more than 19 vertical industries, including technology manufacturing, banking and financial services, consulting/business services, healthcare/pharma, non-computer manufacturing, and government, to name those cited by 6% or more.

Dark Reading was responsible for all survey administration, data collection, and data analysis. These procedures were carried out in strict accordance with standard market research practices and existing U.S. privacy laws.