KOVRR
Cyber Decisions. Financially Quantified.

CYBER'S *"SHIFT UP"* MOMENT

TOM BOLTMAN | VP, STRATEGIC INITIATIVES, KOVRR

Why Every Organization Needs to Develop a ***"Shift Up" Strategy*** to Manage Their Growing Exposure to Cyber Risk

www.kovrr.com

Summary

Today, cybersecurity is evolving into cyber risk management. The last few decades of immense technological and digital transformations have meant that, to a large extent, a business's ability to be resilient is dependent on a reliable, free flow of data and technology functioning without interruption. This shift has profound implications for the global economy's ability to remain stable.

The strategic importance of technology to a company's functioning means there is a growing need for CISOs to communicate their organization's cyber risk exposure in business language with the C-suite. In turn, there is a critical need for the C-suite and boards to be able to communicate to regulators and the market how they are managing their cyber risk exposure. As a result, there is a growing need for businesses and executives to adopt a "Shift Up" Strategy.

A strong "Shift Up" Strategy is specially designed to communicate with, convince, and unite executive stakeholders so they can strategically allocate the appropriate corporate resources (financial, staffing, technological) to maximize and manage a business's cyber resilience.

Introduction

Today, the world's largest economies are dependent on technology. Underlying that are critical companies that rely on technologies that are subject to hackers and vulnerabilities. This dependency is both direct through their adoption of cloud computing, payments systems, and digitized business operations and also indirect via dependencies on global networks of technology-enabled supply chains, third-party service providers,[1] and banking systems and through their reliance on critical national infrastructure. And for good reason.

The businesses and economies that have invested in digital transformation and the ability to quickly adapt over the last few decades have ushered in unparalleled global economic growth, productivity and scale.

This trend is certain to continue, especially when 40% of CEOs think that the very economic viability of their companies would be in doubt if they don't continue to adapt and change.[2] As the next wave of transformation, powered by the adoption of AI (McKinsey estimates that the impact on productivity that generative AI alone could add would be equal to $2.6 trillion to $4.4 trillion annually),[3] other advanced technologies will no doubt accelerate change even faster.

[1] The adoption is so profound that amongst Fortune 500 companies, 87% have adopted at least one public cloud platform, in SMEs which represent 99.9% of the worlds business number utilizing cloud services exceeds 90%.

[2] https://www.pwc.com/gx/en/issues/c-suite-insights/ceo-survey-2023.html#:~:text=Nearly%2040%25%20of%20CEOs%20think,%25)%20and%20manufacturing%20(43%25)

[3] https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-economic-potential-of-generative-ai-the-next-productivity-frontier#key-insights

The Challenge

> ***"Cybersecurity is essential to the basic functioning of our economy, the operation of our critical infrastructure, the strength of our democracy and democratic institutions, the privacy of our data and communications, and our national defense."*** [4]
>
> UNITED STATES, NATIONAL CYBERSECURITY STRATEGY, 2023

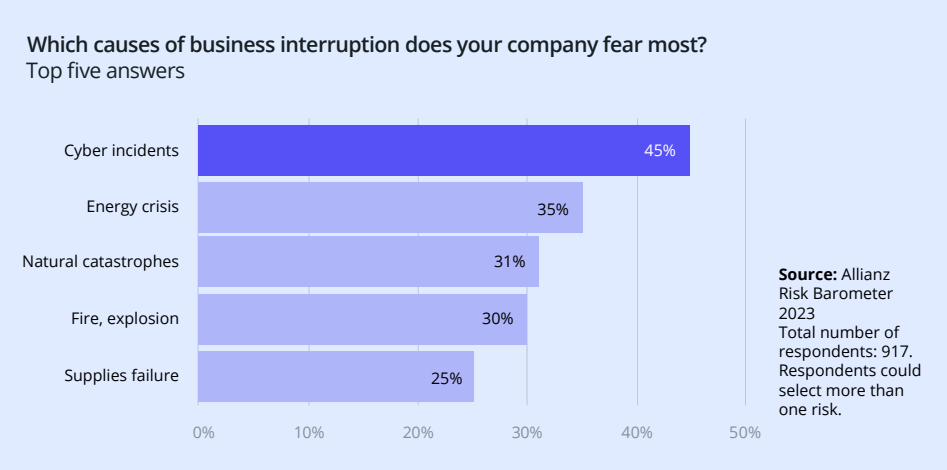
According to the US's 2023 National Cybersecurity Strategy,[5] "cybersecurity is essential to the basic functioning of our economy, the operation of our critical infrastructure, the strength of our democracy and democratic institutions, the privacy of our data and communications, and our national defense."

Such ubiquitous use of technology has become a strategic imperative for all organizations. This strategic adoption and integration of technology has and will continue to deliver great opportunities and efficiencies. However, the dependency on it means each company now has potential vulnerabilities that can threaten its ability to operate.

In some cases, like that of Travelex such vulnerabilities will be critical factors in a company's very existence.[6]

C-Suite Interest

The 2023 Allianz Risk Barometer revealed that the single most significant concern of global executives when it came to their business being interrupted came from a cyber incident, reflecting "ongoing concern for the disruption caused by ransomware attacks, IT system and cloud outages and the threat of cyber war."[7]



The risk of ransomware attacks can inflict significant financial damage on organizations. According to Cybersecurity Ventures, the global cost of ransomware damage is predicted to exceed $265 billion annually by 2031.[8] The same source also predicted that there will be a ransomware attack on businesses every 11 seconds by 2021, up from every 40 seconds in 2016.

Another report from Statista mentioned that ransomware attacks were involved in 24% of all breaches, according to the Verizon 2023 Data Breach Investigations Report (DBIR).[9] Additionally, the "Coalition 2023 Cyber Claims Report" stated that the severity of ransomware claims reached a point where the average loss amount was more than $365,0005. Furthermore, 66% of

[4] https://www.whitehouse.gov-/wp-content/uploads/2023/03/Na-tion-al-Cybersecurity-Strategy-2023.pdf

[5] https://www.whitehouse.gov-/wp-content/uploads/2023/03/Na-tion-al-Cybersecurity-Strategy-2023.pdf

[6] https://www.ifsecglobal.com/cy-ber-security/travelex-hit-by-cy-ber-attack/

[7] https://commercial.allianz.com/-content/dam/onemarketing/com-mercial/commercial/reports/Allian z-Risk-Barometer-2023.pdf

[8] https://cybersecurityven-tures.com/global-ransom-ware-dam-age-costs-predicted-to-reach-250-billion-usd-by-2031/

[9] https://www.techtarget.com/-searchsecurity/feature/Ransom-ware-trends-statistics-and-facts

organizations reported a significant loss of revenue following a ransomware attack.[10] These statistics highlight the substantial and growing financial impact of cyber attacks.

The "Shift Up" Strategy

Responsibility for cyber events such as data breaches and ransomware attacks are no longer under the sole purview of the CISO and their teams. Because of the potential effects on a company's overall resilience and reputation, cyber risk has gained the attention of the C-suite, boards, and investors. Because of this, every organization needs to adopt a "Shift Up" Strategy for their cyber risk management. A "Shift Up" Strategy mirrors the evolution of cybersecurity into cyber risk management.

This shift is driven by technological, economic, and regulatory needs to involve and align a broader group of stakeholders internally within companies and externally with the investment community and regulators.

What's driving the need for a "Shift Up" Strategy?

1 Technology Drivers	Complete dependency on technology, supply chains, and third-party services in business and governments. This reliance magnifies the impacts should there be a severe breach, disruption, or destruction to any part of that ecosystem.
2 Economic Drivers	General austerity and efficiency demands driven by CFOs and the C-suite demanding companies 'Do more with less.' This reality necessitates data-driven approaches to prioritize investments and resilience objectives without sacrificing security.
3 Regulatory and Investment Drivers	Externalized pressure from regulatory and ratings agencies to optimize and report on cybersecurity. Examples include the new US SEC and EU NIS 2 requirements for cyber reporting and credit ratings and proxy reporting agencies' interest in cyber impacts on credit default probabilities calculations.

[10] https://www.cyberea-son.com/blog/research/report-ran-somware-at-tacks-and-the-true-cost-to-business

A new wave of regulatory requirements for companies to have an understanding of what constitutes a material cyber incident and report it to regulators like the US Securities and Exchange Commission (SEC) further strengthens the need to rethink how cyber risk is communicated and managed across the board.

Technology Drivers

The International Data Corporation forecasts that 65% of the world's GDP will have been digitized, and investments in the digital transformation between 2020 and 2023 will have totaled $6.8 trillion, equivalent to the GDPs of France and Germany combined.[11] It's clear why. All efforts pouring into digital transformation and technology investments are driving profit or performance improvement uplift of more than 10 percent, up from 2.5 percent last year.[12]

The increasing dependence on technology is evident from recent statistics, with 77% of society relying on technology to succeed and 48% of the world's population owning a smartphone.[13] This overreliance on technology has significant implications for economic productivity and growth. Technological progress has been a critical driver of economic growth, allowing for more efficient production of goods and services, ultimately contributing to prosperity.[14] However, the reliance on technology has also exposed businesses to the risk of substantial financial losses in the event of technology failures.

Business interruptions caused by cyber events can result in substantial financial losses for businesses, with global cybercrime damage costs predicted to reach $8 trillion annually in 2023 and expected to grow to $10.5 trillion by 2025.[15] The average total cost of recovery and downtime from a ransomware attack increased from $761,106 to $1.85 million in 2021, with an average downtime of 23 days.[16] Technology outages cost organizations an average of $5,600 per minute.[17] Additionally, the global average cost of a data breach in 2023 was USD 4.45 million, representing a 15% increase over three years.[18]

Larger enterprises are particularly susceptible to these financial risks due to the scale of their operations and the potential ripple effects of a cyber-related business interruption on their customers and business partners.[19] The growing reliance on digital infrastructure has further heightened the vulnerability of businesses to cyber attacks, making the potential for widespread business interruption a critical concern.[20]

The Economic Drivers

The pressure on companies and CFOs to do 'more with less' is significant, impacting various aspects of business, including cybersecurity budgets. According to the PwC Pulse Survey, 77% of CFOs are adopting new cost-cutting measures due to economic pressures, even as 74% cite cyber attacks as a top risk to their businesses.[21] According to the PwC survey, one in five organizations are seeing shrinking or stagnating 2024 cybersecurity budgets.[22]

The threat of geopolitical tensions and the associated global economic volatility that comes with it could add further pressure on executives to review and reprioritize their overall spending and risk management plans. More than one-third of CISOs reported flat or shrinking cybersecurity budgets in 2023. While cybersecurity budgets grew 6% on average, that number was down from 17% the previous year. Recent research by Proofpoint states that over half (58%) of CISOs agree that recent economic events have hit their cyberse-

[11] https://www.thrivingtogether.eu-/analysis/148-the-transatlantic-digital-economy

[12] https://kpmg.com/xx-/en/home/insights/2023/09/kpmg-global-tech-report-2023.html?cid=ggl-cpc_ggl_all_xx_2023_kpmg-glb-tech_ad1&s_kwcid=AL!13704!3!682989594674!p!!g!!digital%20transformation&gclid=Cj0KCQiAtOmsBhCnARIsAGPa5yZHsLwqvew6grIqlab1CFvuDEpjT3WSAzdSfKgFq1ZMlqZQH9dAPFQaAq3ZEALw_wcB

[13] https://gitnux.org/dependence-on-technology-statistics/

[14] https://rcc.harvard.edu/knowledge-technology-and-complexity-economic-growth

[15] https://www.-forbes.com/sites/chuckbrooks/2023/03/05/cybersecurity-trends--statistics-for-2023-more-treachery-and-risk-ahead-as-attack-surface-and-hacker-capabilities-grow/

[16] https://www.insurancejournal.com/magazines/mag-features/2021/11/01/639581.htm

[17] https://gitnux.org/dependence-on-technology-statistics/

[18] https://www.ibm.com/reports/-data-breach

[19] https://www.insurancejournal.com/magazines/mag-features/2021/11/01/639581.htm

[20] https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide

[21] https://www.pwc.com/us/en/library/pulse-survey/business-growth-through-recession-uncertainty/cfo.html

[22] https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/global-digital-trust-insights.html

curity budget.[23] Finally, it's not simply that there is a need for more cybersecurity solutions. The proportional allocation to the different cybersecurity solutions being deployed. A recent PWC global digital trust report indicated that 19% of organizations say they have too many cyber solutions and need to consolidate.

> **KPMG's 67% say that in comparison to last year they are expected to do more with a smaller budget.[25]**
>
> KPMG, GLOBAL TECH REPORT, 2023

This pressure is also reflected in the need for CFOs to introduce new revenue streams, enter new markets, and balance price increases with long-term customer demand.[26] As a result, CFOs are seeking targeted investments to drive performance, including in areas such as cybersecurity.

The question then becomes - how can CISOs articulate the value and ROI of each solution and their overall strategy, set forth a budgetary justification for what is needed, and explain how any consolidation and expense reallocation will not diminish the cyber resilience of the company - or perhaps even improve it.

Regulatory and Investment Drivers

On June 26, 2023, US SEC Chair Gary Gensler announced, "Many public companies provide cybersecurity disclosure to investors. I think companies and investors alike, however, would benefit if this disclosure were made in a more consistent, comparable, and decision-useful way. Through helping to ensure that companies disclose material cybersecurity information, today's rules will benefit investors, companies, and the markets connecting them."[27]

The NIS 2 Directive is the EU's legislation on cybersecurity, which modernized the existing legal framework to keep up with increased digitization and an evolving threat landscape. It expanded the scope of cybersecurity rules to new sectors and entities, further improving the resilience and incident response capacities of public and private entities, competent authorities, and the EU as a whole.[28] On the other hand, the SEC has adopted rules requiring registrants to disclose material cybersecurity incidents they experience.

Indeed, the SEC cybersecurity rules and the European Union's NIS 2 (Directive on measures for a high common level of cybersecurity across the Union) are significant regulatory frameworks driving the need for a "Shift Up" Strategy. Naturally, having built-in capabilities to assess, define, and determine financial materiality will help both internal communication and strategy in addition to meeting the external requirements set forth by the regulator. These rules also require public companies to disclose their cybersecurity risk management, strategy, governance, and incident disclosure.[29]

The NIS 2 Directive and the SEC cybersecurity rules are aimed at enhancing the protection of critical infrastructure, improving incident disclosure, and strengthening the resilience of organizations and the overall cybersecurity posture. The importance of financially quantifying cyber risk has become increasingly significant due to the SEC cybersecurity rules and NIS 2.

Financially quantifying cyber risk is essential for fulfilling SEC cyber disclosure

---

[23] https://www.proofpoint.com/sites/default/files/white-papers/p-fpt-uk-wp-voice-of-the-CISO-report.pdf

[24] https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/global-digital-trust-insights.html

[25] https://kpmg.com/xx/en/home/insights/2023/09/kpmg-global-al-tech-report-2023.html?cid=ggl-cpc_ggl_all_xx_2023_kpmg-glb-tech_ad1&s_kwcid=AL!13704!3!682989594674!p!!g!!digital%20transformation&gclid=Cj0KCQiAtOmsBhCnARIsAGPa5yZHsLwqvew6grIqlab1CFvuDEpjT3WSAzdSfKgFq1ZMlqZQH9dAPFQaAq3ZEALw_wcB

[26] https://www.pwc.com/us/en/library/pulse-survey/business-growth-through-recession-uncertainty/cfo.html

[27] https://www.sec.gov/news/press-release/2023-139

[28] https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

[29] https://www.sec.gov/news/press-release/2023-139

requirements and providing shareholders and the investment community with a clearer view of the potential impact of cyber events. Additionally, assessing and managing systemic cyber risk is crucial for the financial system, as it involves analyzing cyber risk exposures, assessing cybersecurity and preparedness capabilities, and understanding the properties of cyber risk and various cyber risk scenarios.[30] Therefore, in the current regulatory and threat landscape, financially quantifying cyber risk and utilizing it to underpin a "Shift Up" Strategy is important not only for individual organizations but also for the stability of the financial system as a whole.

Enabling C-suites and boards to internalize the importance of cyber risk during mergers and acquisitions (M&A) activities is an additional dimension. As exemplified by the data breach at Yahoo, a lack of cyber due diligence can significantly impact investment decisions. The failure to disclose the breach in 2014 in a timely and accurate manner led to a $35 million penalty imposed by the SEC on Yahoo. This penalty was the first of its kind and highlighted the importance of proper cyber-disclosure procedures. The breach, which compromised the personal data of millions of users, had far-reaching consequences, including a potential $1 billion reduction in Yahoo's value and impacting its acquisition by Verizon. Such incidents can lead to charges of material omissions and misstatements in public filings, resulting in regulatory enforcement, litigation, and loss of investor trust. Therefore, investors need to consider the potential financial and reputational fallout of cyber incidents when making investment decisions.[31] [32] [33] [34]

A near-universal challenge is communicating cyber risk to the C-Suite and board is often too technical and hard to articulate. Reliance on red, amber, green traffic light risk systems makes it difficult to compare against each other, rarely change and don't convey the level of potential loss to the business.

The Challenge of Communicating Cyber Risk Today

Most CISOs and executives will generally agree with the need to take cyber risk seriously. They readily acknowledge the drivers above and the enhanced cyber threat landscape that they and their companies operate in. However, establishing a strategic and validated view of cyber risk from which one can secure and prioritize the right resources to manage it is still elusive for many organizations. While cyber is no doubt taken seriously, the growing requirement and desire for executives and boards to get more actively involved in managing cyber risk means that the traditional CISO approach of working 'down' is no longer enough. In other words, they can no longer focus on what they and their team of security specialists are working on). Creating a "Shift Up" Strategy requires getting and keeping CISOs and the C-suite on the same page and speaking a common language.

This strategy will help meet the growing need for businesses to have more strategic discussions that enable the business as a whole to be resilient, and these involve conversations between the CISO and the C-suite. However, a near-universal challenge is communicating cyber risk to the C-suite and board is often too technical and hard to articulate. Reliance on red, amber, and green traffic light risk systems makes it difficult to compare against each other, rarely changes, and doesn't convey the level of potential loss to the business. Security ratings, while a more nuanced and trackable heuristic, still fail to convey the threat on the business's ability to operate, prescribe the level of financial exposure that the business has, and what qualitative level

[30] https://carnegieendowment.org/2019/09/30/cyber-risk-scenarios-financial-system-and-systemic-risk-assessment-pub-79911

[31] https://www.jonesday.com/en/insights/2018/05/sec-announces-yahoo-will-pay-35-million-for-failur

[32] https://www.paulweiss.com/practices/transactional/capital-markets/publications/yahoo-agrees-to-35-million-sec-penalty-for-failure-to-disclose-cyber-incident?id=26363

[33] https://www.cybereason.com/blog/yahoos-potential-financial-fallout-shows-the-unexpected-impacts-of-a-data-breach

[34] https://www.whitecase.com/insight-alert/sec-fines-yahoo-35-million-failure-timely-disclose-cyber-breach

and mix of investments should be made or even prioritized.

Without that, organizations are left setting critical thresholds about important risk governance items like appetite, materiality, and insurance without the information necessary to make a proper decision.[35]

Therefore, we see there is a growing need for businesses to define a data-driven "Shift Up" Strategy. One that unites all executive stakeholders and delivers on a plan to allocate resources that maximize a business's cyber resilience strategically.

Qualitative	Quantitative
Subjective View	Evolving Data Driven View
Traffic Lights	Financial ROI-Based Prioritization
Security Ratings	Financial Loss Insights
Operational and Tactical Actions	Strategic Resources Allocation

By moving from a more qualitative type of analysis to a more quantitative form of analysis, the entire chain of stakeholders is able to both align, plan and justify, based on the gross and net benefit to the business and market what they are doing to reduce the financial impact of a cyber risk event to the organization.

Shifting Up at Every Level

As CISO Christine Bajarasco notes, "Transforming the organizational mindset to recognize cybersecurity as a fundamental business function is imperative. To create the right security outcomes, CISOs must consider the strategic goals the business wants to achieve, as well as the associated risks. Without this synchronization, security endeavors might not significantly contribute to the business's triumphs."[36]

To do this, all stakeholders will need to acknowledge the current limitations of the view of risk they are working with today and adopt new mindsets, methods, and tools so they can meet the evolving needs of the business and those managing and regulating it.

A "Shift Up" Strategy would propose that during the budgetary process or before a major technology investment, there is a clear understanding of the impact to the business and what the potential material financial losses may occur.

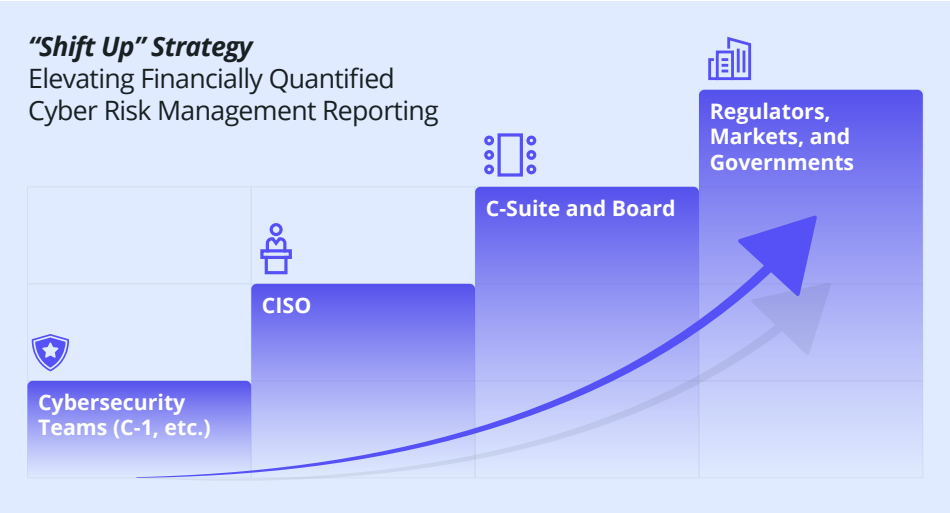
A "Shift Up" Strategy means:

- Treating cyber risk as a strategic business priority.
- Elevating and aligning those stakeholders primarily responsible for it to meet its increased importance.
- Ensuring those stakeholders have the right tools and resources to communicate potential financial losses and manage them as a dynamic and evolving business risk.

By enabling each stakeholder at each level to focus on the financial risk, they are more connected to the security of the systems that deliver value to the organization.

[35] https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2024/volume-1/emotional-cyberrisk-management-decisions

[36] https://www.helpnetsecurity.com/2023/11/22/cisos-business-security-goals/



A "Shift Up" Strategy would propose that during the budgetary process or before a major technology investment, there is a clear understanding of the impact on the business and what potential material financial losses may occur. Such a move would require a focus on what and how these different stakeholders think about cyber risk—moving from a more tactical "CVE and Open Ports" way of thinking to a more strategic "how do we reduce the key drivers of financial exposure" way of thinking. In essence, it would re-frame the conversation and those taking part in it from a cybersecurity discussion to a cyber risk management discussion.

Roles	Current View	Shift Up View
Cybersecurity Teams	Operational and security-focused	Risk and business-focused
CISO	Narrow view of preventing breaches of security	Financially quantified business impact
C- Suite and Board	Abstract and constrained risk impact	Financially quantified business and market impact
Capital Markets	Historically informed, abstract view of risk	Evolving view of critical individual risks and systemic economic impact
Regulators and Governments	Historically informed, abstract view of risk and statistically driven stress tests	Evolving view of critical individual risks and systemic economic impact

What Questions Does a "Shift Up" Strategy Answer?

The growing exposure and the need to elevate cybersecurity to a strategic level requires a shift in communication strategies. As such, it is important to evolve corporate cyber risk reporting into one that's in line with the dynamic nature of risk and is capable of uniting all executives and stakeholders - irrespective of their understanding of technology or cybersecurity so that

they can deliver on a plan to allocate resources that maximize a business's cyber resilience strategically.

It's also important to mention that the questions answered by a robust "Shift Up" Strategy need to be answered by a broader constellation of stakeholders. In the "Shift Up" paradigm, while the CISO is foundational and largely responsible for helping make the company cyber resilient, they must also be able to align and communicate with others that also increasingly share this responsibility, for example, with the CRO, CIO, CFO and the board.

Strategically Aligning Decision Makers and Decisions

Ultimately, every organization has a set of cyber "jobs to be done" or, perhaps more precisely, cyber 'decisions to be made.' A financially quantified "Shift Up" Strategy will not only level the playing field when it comes to understanding risk. It will also mean that cyber can be treated similarly to other business risks.

While each organization differs, there are executive roles responsible for corporate risk management. The CEO is ultimately responsible, but to varying degrees, the CFO, CRO, CIO, and CISO will be charged with looking over governance, risk, compliance, security, and regulatory issues.

The CISO is foundational and largely responsible for helping make the company cyber resilient, they must also be able to align and communicate with others that also increasingly share this responsibility, for example with the CRO, CIO, CFO and the board.

Cyber risk decisions that are most relevant to business will be centered around the following outcomes. A financially quantified view of cyber risk can unite all relevant stakeholders across all major operational, risk and security responsibilities to drive better decisions on where to mitigate, transfer and accept cyber risk.

The Role of Financially-Focused CRQ (Cyber Risk Quantification)

An effective cyber risk quantification capability can deliver a comprehensive view of a business's cyber risk exposure and give evolving, measurable and actionable insights into how best to reduce it.

As mentioned above, the dynamic nature of cyber risk means that organizations need to be able to capable of constantly assessing the impact of changes in the:

Enterprise Intelligence

- Corporate structure and business units (E.g., Overall structure as well as M&A and divestiture changes)
- Business profile (E.g., Revenue, number of employees, locations, and industries served)
- Sensitive data records and IP
- Past incidences

Cyber Intelligence

- Cyber threat intelligence landscape
- Internal assets
- External attack surface
- Technological footprint and critical service provider dependencies and aggregations
- Security posture and maturity
- Vulnerabilities

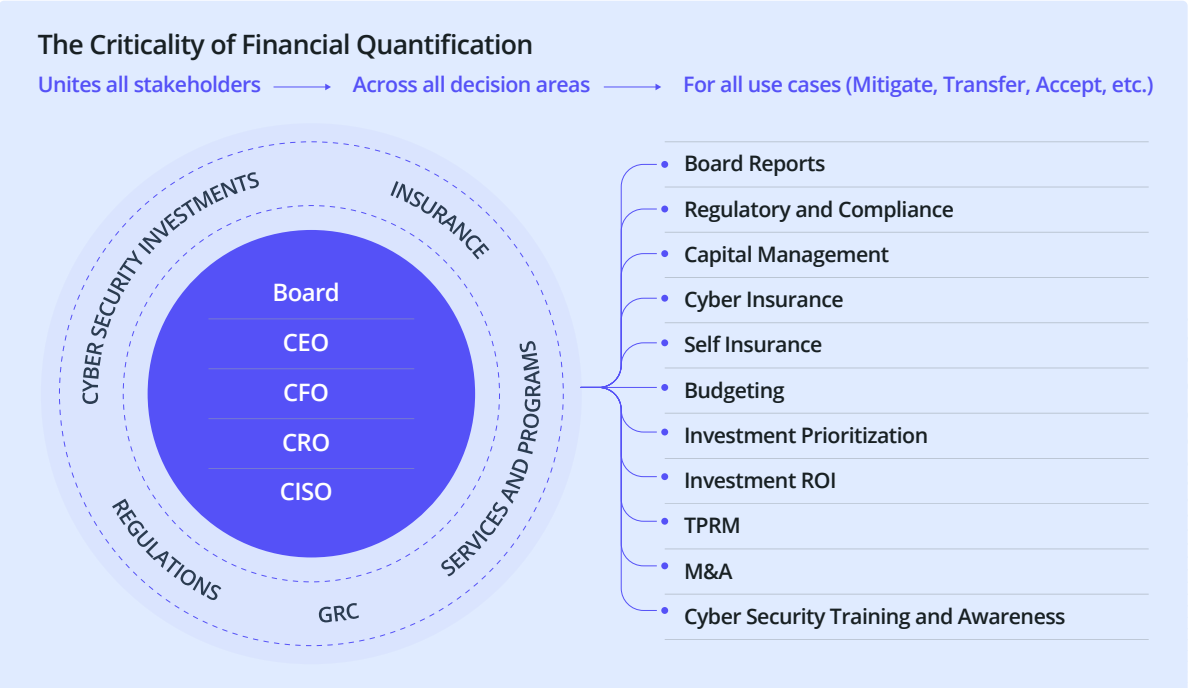
Market Intelligence

- Regulatory landscape
- Compliance landscape
- Insurance and market landscape (E.g., the cost of insurance coverage and cyber claims)

Such a wide array of evolving data points lends itself to an integrated technology led approach, as it's often beyond the capability of most teams to track and compute.

A robust technology-driven CRQ approach is able to integrate and fuse these elements and provide a clear analysis of a company's overall cyber risk exposure as well as that of any subsidiaries and business units that it has.

By creating a common language of financially quantified cyber risk, the variety of executives and board stakeholders can be more confident that they both understand the magnitude of the risk to which they are exposed and be more aligned in how they will all jointly ensure that continuity of operations will be ensured.



Benefits of Utilizing CRQ to Drive Your "Shift Up" Strategy
1 Ensures cyber risk is managed a strategic issue.
2 Enables the CISO to communicate effectively with the C-suite and the board.
3 Enables all relevant stakeholders to make more strategic decisions around cyber resilience. For example, the what, why, and ROI of cybersecurity control investments, risk transfer, and risk acceptance decisions.
4 Enables the company to communicate to the market, investors, and regulators (in line with emerging regulatory developments around cyber and reporting on materiality – e.g., the US SEC, the EU's NIS 2, and APRA.

Example Questions to Consider When Designing a "Shift Up" Strategy

What is our financial exposure to cyber risk?
What is the primary driver of cyber risk? Are we prioritizing our investments and activities to focus on the main potential losses we might suffer?
How much cyber risk can we attribute to each part of the business?
Does this analysis reflect our current use of technology and service providers, security posture as well as market and threat intelligence trends?
Are we able to refresh or seek an updated analysis on demand?
How is our financial exposure changing over time?
What are the optimal investments to make in cybersecurity?
What is the ROI of cybersecurity control investments?
What opportunities are there to transfer risk to insurers?
How much coverage do we really need? Which coverage should we prioritize, and at what price?
What is our risk appetite? How much can we afford to lose?
How much risk could and should we retain?
How do we define material risk? Do we have the ability to report it credibly to regulators?
How does the investment community view our cyber risk exposure?
Is the CISO being given the right access, support, and representation in the C-suite?
Do we have the right cyber expertise on the board?

Conclusion

In an increasingly evolving technological, economic, and regulatory environment, adopting a financially quantified “Shift Up” Strategy is essential to help organizations, institutions and governments elevate cybersecurity into a strategic cyber risk management issue.

By elevating CISOs and the issue of cyber risk and implementing a cross-stakeholder “Shift Up” Strategy, organizations will be able to manage and communicate their cyber risk exposure more effectively, ensuring operational resilience and strategic decision-making that will meet and surpass the company's needs and those of the capital market’s and regulators.

KOVRR's cyber risk quantification platform empowers enterprise decision-makers to manage cyber exposure more effectively by providing an in-depth risk analysis that drives actionable, financially justified decisions.

For more information about how your organization can develop a financially quantified **"Shift Up" Strategy** to manage its cyber risk exposure, contact the Kovrr team or schedule a free demo today.

KOVRR
Cyber Decisions. Financially Quantified.

www.kovrr.com