OLIVER WYMAN | SIG
the network for sourcing executives

CYBER SPEND TRENDS,
OPPORTUNITIES, AND IMPLICATIONS FOR PROCUREMENT

CONTENTS

OVERVIEW OF CYBER SPEND TRENDS

In our interconnected and digitized world, cyber risk is increasing, and the nature of cyber-attacks evolving. If the recent attacks and resulting media attention are any indication, various threat actors who can precipitate cyber-attacks have ambitions which can be harmful in severe ways. These factors along with the pace at which technology is evolving are compelling companies and their Board of Directors to have a clear understanding of the cyber risks they face and to determine the level of spend they are willing to dedicate to cybersecurity.

An effective, measurable, and actionable cyber investment strategy provides institutions with a risk management capability to set and communicate strategic boundaries for cyber risk-taking across the institution.

CYBER THREATS ARE BECOMING MORE SOPHISTICATED FORCING COMPANIES TO ACT

Several elements are contributing to today's heightened cyber threat level. As the world becomes more interconnected by leveraging newer technologies, it is also becoming more exposed, with a myriad of entry points for threat actors to target. Recent cyberattacks have left companies with millions in damages and exposed the need for companies to strengthen their cyber defenses.

In addition, international tensions have stimulated large-scale efforts to enhance national cyber defenses to improve readiness for response and recovery. The emergence of AI driven cyberattacks and targeted tampering of machine learning systems are only some of the latest cybercrime innovations.

As a result, Boards of Directors are increasingly expecting a coherent and accurate articulation of their company's cyber defense that are linked to their business model and strategy and integrated into their enterprise risk management strategy. More advanced institutions have been on the journey for several years to actively protect, detect, respond, and recover business services and underlying IT capabilities. Others are now playing catch-up.

In our experience, commitment to a cyber risk management or information security strategy and the associated funding is critical. Therefore, it is essential to engage senior management and the Board of Directors to use a structured design approach covering the following:

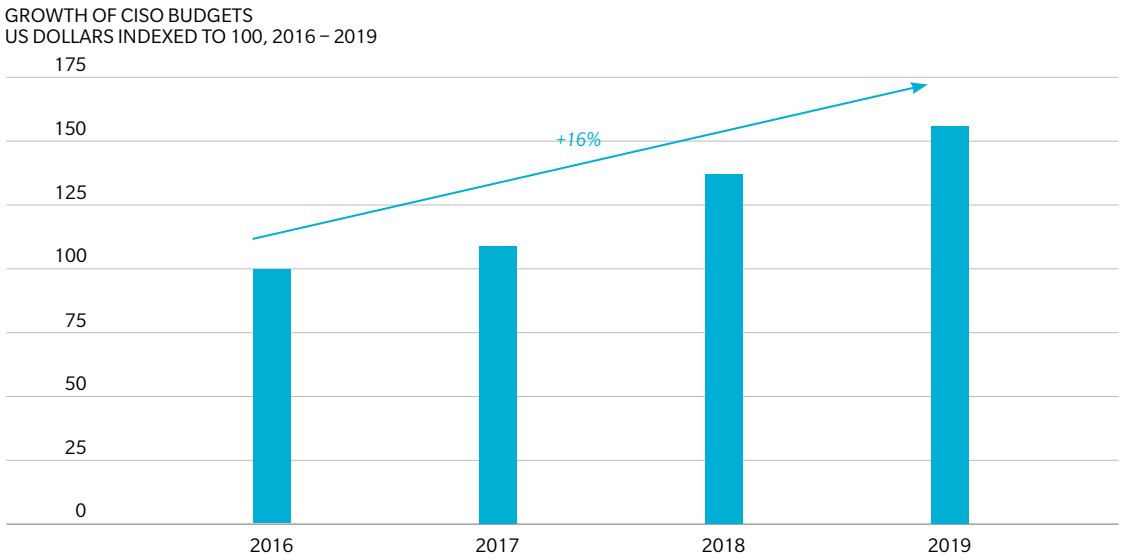
- Ongoing Board engagement
- A clear articulation of the cyber risk management strategy
- Operational preparedness for cyber defense and resilience
- A clear Three Lines of Defense organization model
- Timely and effective management information regarding cyber
- A funding strategy with checks and controls, for example the extent to which investments have changed the nature of cyber risk for enterprise

In a world of limited resources there are always trade-offs to be made: how to diversify investment, how much risk to tolerate, and how much to mitigate or insure against. In considering these factors, the customer experience, and the modern digital business models of today and tomorrow, zero appetite for cyber risk is not realistic.

CISOS ARE SPENDING MORE THAN EVER ON CYBER SECURITY

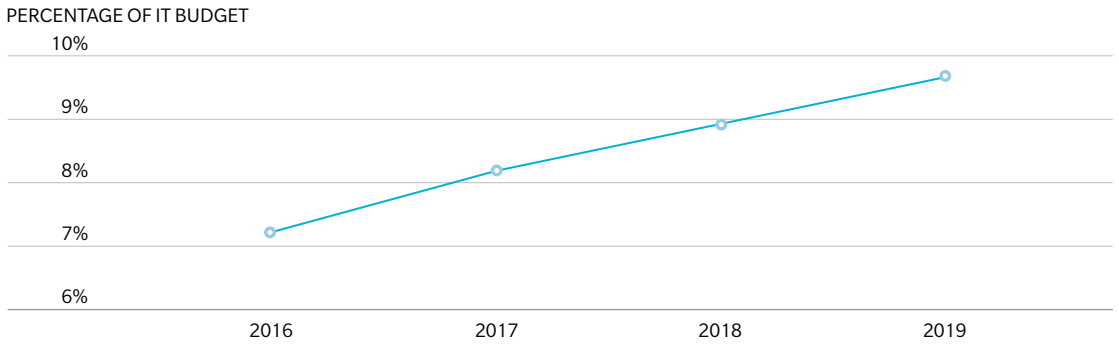
As a result of new and elevated threat levels and heightened scrutiny from board members, CISO budgets

Exhibit 1: Growth of CISO budgets – US dollars indexed to 100, 2016 – 2019



Source: Oliver Wyman cyber spend benchmark study

Exhibit 2: Growth of CISO budgets – as a percentage of overall IT budget, 2016 – 2019



Source: Oliver Wyman cyber spend benchmark study

have seen a significant uptick in recent years, up 16% annually between 2016 and 2019.

Compared to the overall IT budget evolution, cyber related budgets have grown faster than other spend categories.

A recent cyber benchmarking study by Oliver Wyman with national and global corporations, highlighted that many firms are still lagging in the cyber security space. These firms are typically redoubling their efforts in cyber defense to ensure that they do not appear to be "the weakest player on the street" thus avoiding becoming prime targets for hackers.

Other key factors driving increased investment in information security and strong cyber defenses, include:

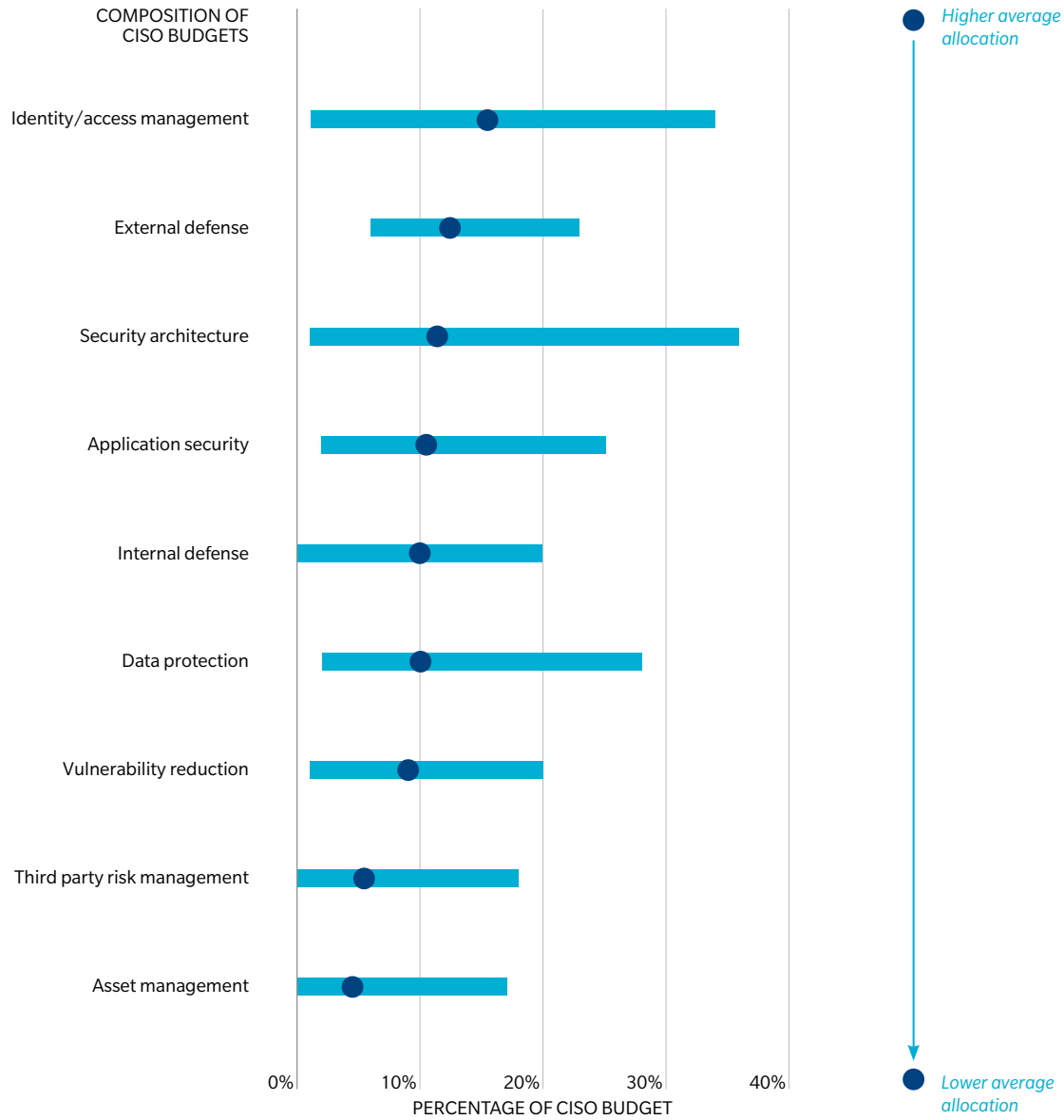
NEW REGULATION AND LAWS

(e.g., GDPR, The SHIELD Act, California Consumer Privacy Act and CCPA-like laws across many States) have increased the regulatory expectations for data security and potential penalties for firms found to be non-compliant.

MEDIA COVERAGE

of high-profile cyber breaches has been a significant driver in recent years (including its associated fines). Reputational damage to the firms can be significant. In addition, there has been an increased appetite for directors to take responsibilities and be liable for these events.

Exhibit 3: Composition of CISO budgets by type



Source: Oliver Wyman cyber spend benchmark study

SHAREHOLDER SCRUTINY

(e.g., new ratings methodologies) has also picked up as rating agencies factor in the firm's cyber posture and preparedness as part their rating approach.

BUDGET ALLOCATION VARIES BY TYPE

A typical CISO budget is made up of a broad array of key defense and preparedness initiatives.

Identity/access management and external defense command the highest shares of the overall budget, yet the budget spread is similar for most categories, with a few outliers:

- Wider ranges in categories that make up a larger share of the budget (e.g., security architecture, identity/access management)
- Narrower ranges among categories that represent "evergreen" spend (e.g., external defense, asset management)

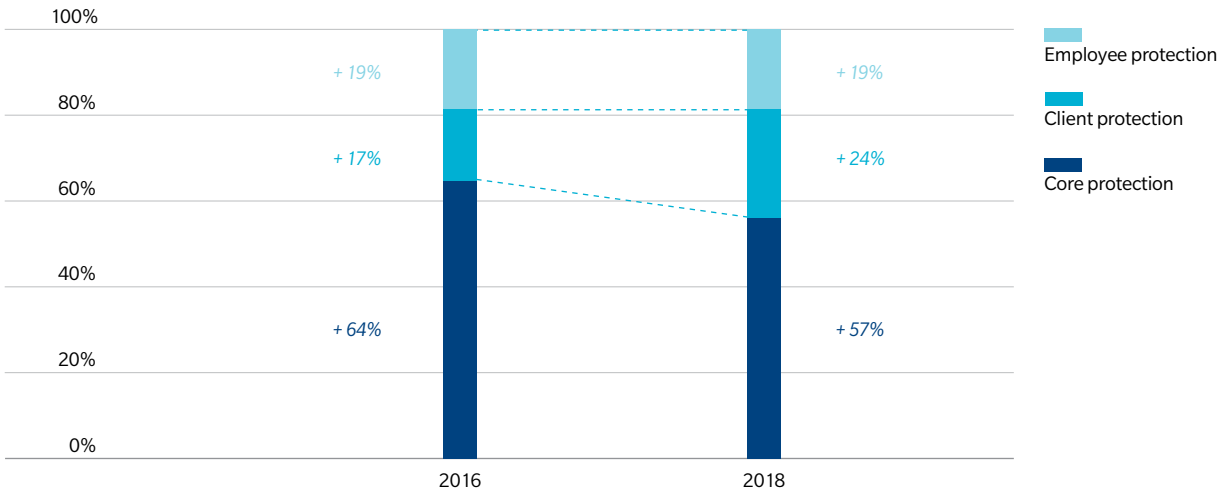
Companies on the lower end of spend across the identity/access management and security architecture categories have likely reached an acceptable level of maturity. Companies on the higher end of the spectrum are typical playing catch-up or have recently completed acquisitions in process of creating a common cybersecurity platform.

Over time, the composition of CISO budgets has also shifted from Core protection in favor of increased client protection.

While 'Protect the core' investments dominate budgets, representing more than half of spend, CISOs have reduced allocations to core investments. The shift away from core spend represents a positive progression as cyber programs mature since:

- CISOs achieved efficiency gains and saw diminishing risk mitigation in additional infrastructure oriented investments
- CISOs have repositioned budgets to support broader mandates (e.g. Resilience, Privacy, GDPR/CCPA like regulation)
- CISOs have launched preventive measures, including:
  - Phishing and spoofing protection
  - Third party risk management
  - AI capabilities
  - Insider threat

Exhibit 4: Composition of CISO budgets



Source: Oliver Wyman cyber spend benchmark study

THERE ARE DIFFERENT WAYS TO DESIGN AND ALLOCATE CYBER SECURITY SPEND

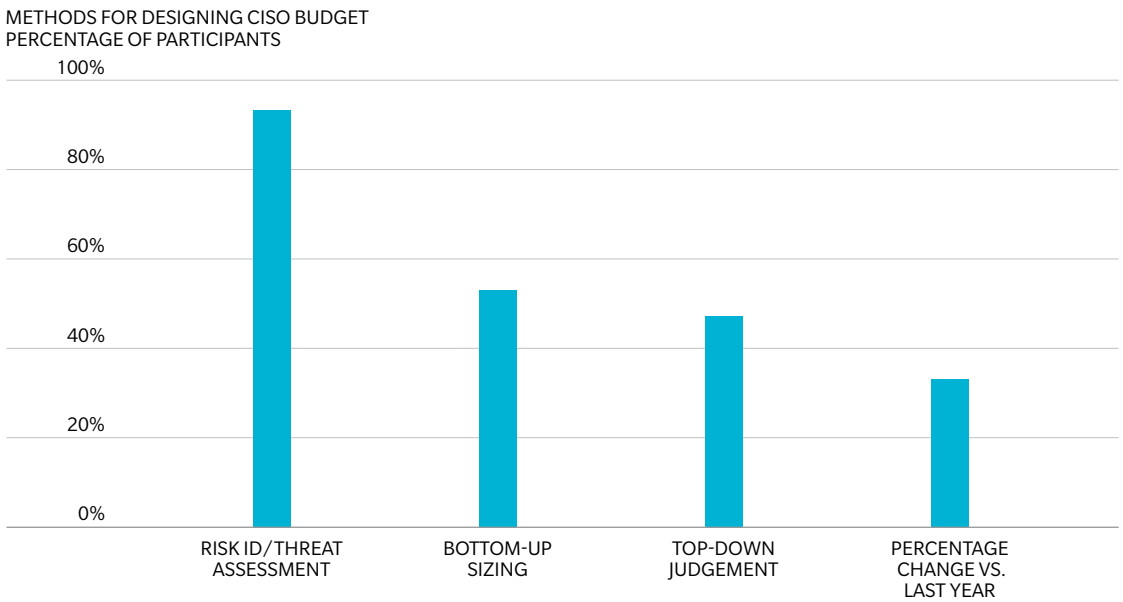
MOST CISOS USE RISK IDENTIFICATION AND THREAT ASSESSMENTS TO DESIGN AND JUSTIFY THEIR BUDGETS

When designing their budgets, CISOs overwhelmingly use risk identification and threat assessment as one of the methods. According to Oliver Wyman's recent benchmark study, 93% of the CISOs interviewed used a form of risk identification and threat assessment.

This does not necessarily mean that the risk identification and threat assessment is the primary way CISOs design their budgets. In fact, many companies use other methods such as bottom-up sizing, top-down judgement, or percentage change from the previous year as their primary budgeting tool.

To justify their budgets, CISOs also rely on the risk identification and threat assessment. However, it is difficult to link a program or an initiative to a cost/benefit analysis, given the challenges that companies have at measuring the value of a cybersecurity program.

Exhibit 5: Methods for designing CISO budget – as a percentage of respondents



Source: Oliver Wyman cyber spend benchmark study

When delving deeper into the risk identification and threat assessment method, this is even more evident, since CISOs adopt two fundamental approaches: a framework driven approach or a multi-pronged approach, usually in line with the maturity of their cyber programs.

FRAMEWORK DRIVEN APPROACH

This approach is driven by a program maturity assessment using industry frameworks, benchmarks, and tools, such the NIST Cybersecurity Framework or ISO/IEC 27002.

Prevalent in firms with developing cyber programs, the maturity assessment is often not the primary justification for their cyber budget request.

Instead, CISOs typically rely on other primary justifications such as proven track record, in which they point to the success of previous cyber-related investments to justify the planned investments for the upcoming year.

MULTI-PRONGED APPROACH:

The Multi-pronged approach is more commonly used among more mature cyber programs and generally uses a combination of assessments, including:

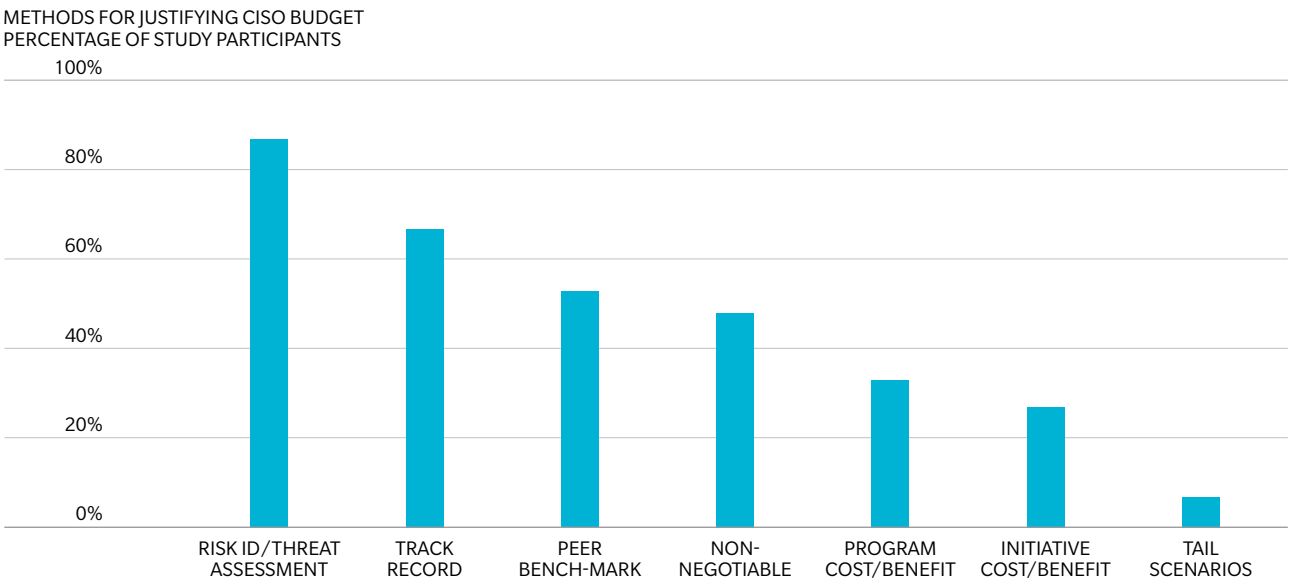
- Linking cyber risk to operational and/or technology risk assessments
- Measuring the impact of specific threats for specific businesses and processes
- Leveraging independent program reviews

A COMPREHENSIVE RISK-ORIENTED INVESTMENT APPROACH WILL BETTER ENSURE THAT INVESTMENTS BRING DOWN CYBER RISK

As firms become more mature on their cyber risk programs, they will need to invest time and effort to gain more clarity on how their investments will bring down cyber risk.

- Industry frameworks such as NIST provide a detailed cyber assessment and tend to use an audit-driven, "tick-the-box" process as a starting point before overlaying evaluation frameworks to capture the materiality of threats and risks. Unfortunately, this controls-oriented investment approach tends to lack the forward-looking and strategic component of the risk assessment, which limits the measurability and impact of the investments on a company's cyber risk exposure.

Exhibit 6: Methods for justifying CISO budget - as a percentage of respondents



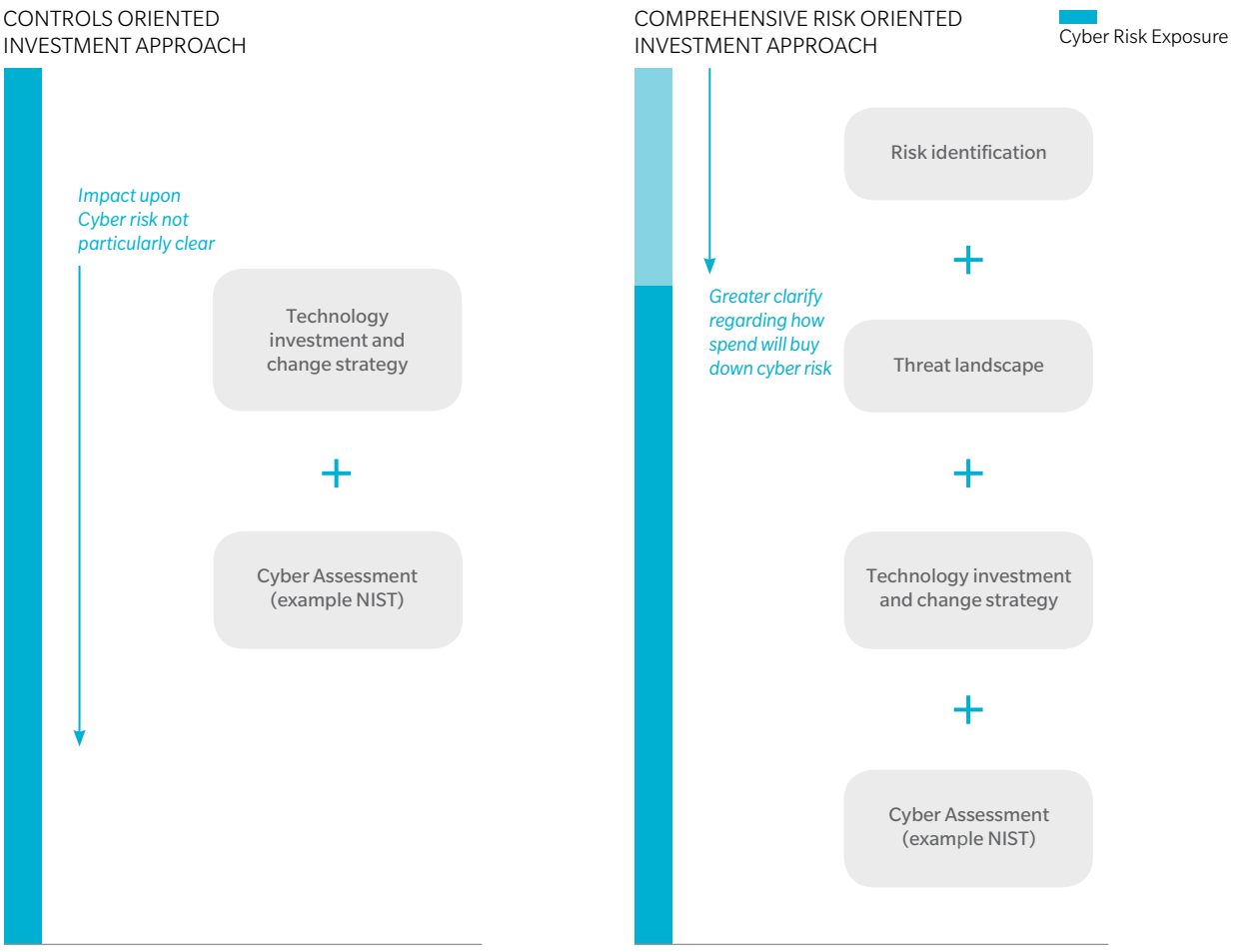
Source: Oliver Wyman cyber spend benchmark study

- In fact, only 6% of CISOs interviewed believe they have established a robust process for substantiating the benefits of cyber investments. Many CISOs expressed difficulty quantifying the reduction in cyber risk directly attributable to investments by the enterprise and still largely rely on anecdotal or lagging indicative evidence (e.g., no major breaches, no reputation damage in media).
- More mature companies will combine cyber assessments with a detailed view of upcoming technology investments, a comprehensive assessment of the threat landscape, as well as emerging risks, to adopt a more comprehensive risk-oriented investment approach and obtain a greater clarity on how the investments will reduce cyber risk.
- CISOs with more sophisticated approaches demonstrate improvement using a combination of quantitative and qualitative data:

QUANTITATIVE DATA ACTS AS THE ANCHOR

40% of CISOs track operational metrics such as malicious traffic, dwell time, or patching and leverage financial and business metrics to demonstrate the value of their investments through cost savings or time-to-market metrics.

Exhibit 7: Evolving risk assessment approach



Source: Oliver Wyman cyber spend benchmark study

QUALITATIVE DATA ACTS AS AN OVERLAY TO QUANTITATIVE METRICS

Risk reduction is often analyzed qualitatively (e.g., shift from "high" to "moderate" cyber risk in a specific area) and several CISOs are exploring new technologies and modeling methods to improve the quantification of cyber risk.

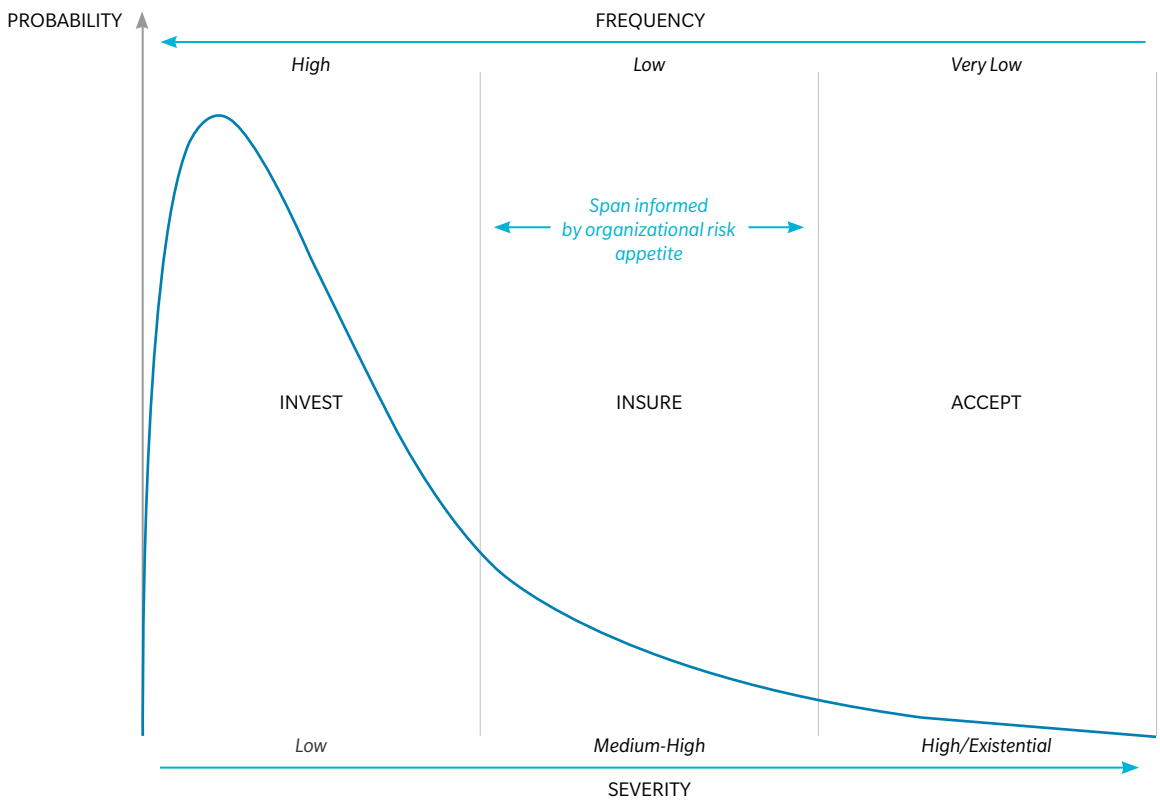
ORGANIZATIONS NEED TO DETERMINE WHERE TO INVEST, INSURE, OR ACCEPT THESE EVER-EVOLVING CYBER RISKS

CISOs not only have to live in a world in which the impact of investments is difficult to measure but also acknowledge that zero risk is simply an impossible reality. While most Board of Directors and senior management start with a close-to-zero risk position, it quickly becomes evident that it would be prohibitive cost-wise and would essentially mean that the company cannot be "online".

As a result, CISOs must pick their battles using an Invest – Insure – Accept framework. High frequency items with low severity are prime candidates for companies to invest in cyber-protection. These may range anywhere from phishing to firewall breach attempts. Lower frequency cyber risks would be candidates for insurance while very rare risks would have to be part of CISOs' margin of acceptance, given the extremely high insurance premiums these would otherwise incur.

Given the difference between organizations, the invest – insure – accept investment curve can vary significantly from one organization to the next and is dependent on the organization's risk appetite.

Exhibit 8: Invest – Insure – Accept risk appetite curve



Source: Marsh

KEY TAKEAWAYS

A FORWARD-LOOKING CYBER RISK ASSESSMENT FRAMEWORK INCREASES ORGANIZATIONS' VISIBILITY INTO FUTURE THREATS AND ABILITY TO PROACTIVELY MITIGATE THEM

Conventional cyber risk assessments tend to be "point-in-time," considering an organization's current infrastructure and threat actors' current capabilities.

A forward-looking view is essential to ensure that organizations are prepared for tomorrow's threats, in addition to today's.

Forward-looking cyber risk assessments can be broken down into external and internal risk assessments:

EXTERNAL RISK ASSESSMENT

The external risk assessment identifies how threat actors might use emerging technologies and techniques to launch new attacks or bypass existing controls.

Key inputs include:

- Industry reports: External reports identify candidate emerging technologies to consider for assessment
- External SMEs: Discussions with external SMEs identify new attack methods and vulnerabilities due to emerging tech
- Threat intelligence: Threat intelligence provides insight into whether/how adversaries are adopting new technologies

From that external risk assessment, organizations prioritize their risk mitigation efforts by determining how urgently the enterprise needs to address the cyber related risks and threats before identifying the specific types of controls that must be strengthened or replaced.

INTERNAL RISK ASSESSMENT

The internal risk assessment identifies changes to an organization's risk exposure due to changing business landscape and internal operations – including launching new products, adopting new technology or a different mix of third-party service providers.

Key inputs include:

- Business process SMEs: Business process SMEs identify processes affected and potential impacts due to compromise
- Cyber SMEs: Support functions determine the most likely attack methods, as well as the suite of controls available and their effectiveness in mitigating risks
- Prioritization of emerging threats: Forecasts of emerging attack methods offer additional input for consideration

From the internal risk assessment, organizations determine the strategic business changes and the associated cyber risks, before they develop mitigation strategies and options. These mitigation actions identify the specific types of controls that can be strengthened that are consistent with the organization's cyber risk appetite.

Exhibit 9: Challenges with conventional, "point-in-time" cyber risk assessments

THREAT ACTORS ARE RAPIDLY INNOVATING

Cyber threat actors are rapidly increasing the diversity and sophistication of their attacks

Conventional risk assessment findings and mitigation efforts may be rendered obsolete in a short timeframe due to new attack methods made possible by emerging technologies

ORGANIZATIONS ARE ADOPTING NEW TECHNOLOGIES

Conventional risk assessments identify existing vulnerabilities in an organization's IT defenses, but do not take into account future vulnerabilities due to adoption of new technologies

Risk profile may change significantly as an organization's technology infrastructure changes

PROCUREMENT HAS AN IMPORTANT ROLE TO PLAY IN REDUCING CYBER RISK

Cyber risk increases with the proliferation of systems and suppliers, given the complexity and effort it takes to secure each system, across geographies and business units.

An increasing number of organizations have turned towards the procurement function to drastically reduce the number of third parties to ensure that the company can manage cyber risk efficiently. Given the complexity of cyber risk assessments, the fewer third parties an organization have, the easier it is to manage.

In parallel, the number of vendors providing cyber security services has exploded. While this does not make the lives of Procurement easier, it improves the bargaining power of organizations looking to purchase such services.

Procurement functions also play critical roles as the gatekeepers for the firm. Procurement serves to ensure that vendors effectively and consistently will meet the cybersecurity requirements to be considered for the job. Once a vendor is approved, the Procurement function is responsible for defining the key contractual terms and ensuring vendors (and their vendors) adhere to the same stringent cyber security standards as their organization. By revisiting/re-assessing contractual terms, starting with the vendors whom the organization has the biggest reliance on and hence pose the greatest threat, procurement functions act as cyber risk managers. They ensure vendor background checks are performed, that vendors share the responsibility in case an attack should occur and more importantly, proactively collaborate with the cybersecurity team to define the steps to be taken in case of an attack to remediate the situation.

In the case of an attack, procurement functions can work with third parties to ensure that emergency responses are prepared for and that emergency protocols are clear and executable. The procurement function should also ensure that the negotiated contractual terms oblige third parties to inform the organization of any breaches and their remediation strategy, in the case that the third party is compromised.

Cyber risk is not going anywhere and can at times be daunting due to its unpredictability and rapid evolution. What is predictable is that an attack will happen, and it is only a matter of how and when. Luckily, organizations can take steps to mitigate these and the procurement function has an active role to play in this, serving as the first line of defense of the organization.

Exhibit 10: Emerging Procurement practices in Third Party Risk Management

EXTENSION OF BUYER POLICIES TO PROVIDERS

- Worker background checks
- Data privacy and protection
- Secure coding practices/assurance
- Cyber insurance

CYBERSECURITY VENDOR RATIONALIZATION

- Consistent with an intended cyber defense architecture

CYBER INCIDENT RESPONSE STRATEGY

- Collective planning and preparedness
- Tabletop, drills and exercises
- Intelligence sharing

THIRD PARTY PORTFOLIO SIMPLIFICATION

- De-complex, access efficiency or pricing improvements
- Have more understandable/ manageable third-party risk surface

ROLLING ASSESSMENT OF VENDORS

- Risk/criticality based rolling assessment of vendors regarding their cyber policies, posture and preparedness

CONTRACT REPAPERING

- To be fully cognizant of cyber risks, responsibilities, and liabilities

EXAMINATION OF FOURTH PARTIES

- Risk assessment of vendors.

KNOWLEDGE OF ALTERNATE SUPPLIERS

- Having contingency plans ready

AUTHORS

Paul Mee – Partner, Oliver Wyman
paul.mee@oliverwyman.com

Karina Swette – Partner, Oliver Wyman
karina.swette@oliverwyman.com

Mike Matheis – Partner, Oliver Wyman
mike.matheis@oliverwyman.com

Dominique Brieger – Engagement Manager, Oliver Wyman
dominique.brieger@oliverwyman.com

ABOUT OLIVER WYMAN

Oliver Wyman is a global leader in management consulting. With offices in 60 cities across 29 countries, Oliver Wyman combines deep industry knowledge with specialized expertise in strategy, operations, risk management, and organization transformation. The firm has more than 5,000 professionals around the world who work with clients to optimize their business, improve their operations and risk profile, and accelerate their organizational performance to seize the most attractive opportunities. Oliver Wyman is a wholly owned subsidiary of Marsh & McLennan Companies [NYSE: MMC]. For more information, visit www.oliverwyman.com. Follow Oliver Wyman on Twitter @OliverWyman.

SIG CONTACTS

Dawn Tiura – President and CEO
dtiura@sig.org

Stephani McGarry – Vice President, Global Events
smcgarry@sig.org

ABOUT SIG

SIG (Sourcing Industry Group) is the premier global sourcing association, founded in 1991 that provides thought leadership, networking and training opportunities to executives in sourcing, procurement and outsourcing from Fortune 500 and Global 1000 companies. It has served these professionals and opened dialogues with their counterparts in finance, HR, risk and other business functions throughout its 28-year history. The organization is unique in that it blends practitioners, service providers and advisory firms in a non-commercial environment. With a 75:25 ratio of buy-side to sell-side, and over 68% of delegates holding decision-making titles, SIG events are collegial, memorable and senior-level. For more information, please visit: www.sig.org.

OLIVER WYMAN