TRANSFORMED CYBER-RISK: A STRATEGIC GROWTH DRIVER FOR THE TRUSTED AND TRANSPARENT ENTERPRISE

Author:

Joel Stradling

September 2023

An IDC Spotlight sponsored by PwC

IDC #EUR151167723

Transformed Cyber-Risk: A Strategic Growth Driver for the Trusted and Transparent Enterprise

Introduction

- Cyber-risk has become a main priority for security and business leaders.
- A forward-looking risk approach encompasses:
  - **A Shift Left:** Risk management with real-time contextual intelligence drives positive business outcomes (leaving behind lagging point-in-time snapshots that are no longer fit for purpose).
  - **Risk Management for Business Agility and Success:** Understanding risk enables the taking of risk in an informed fashion — and thus quicker movement.
  - **Competitive Advantage:** Leveraging risk insights improves an organization's competitive position in the market.
- According to IDC's *Worldwide CEO Survey* of February 2023, security, risk, and compliance is the top technology priority for CEOs in 2023.
- Legacy cyber-risk audits are static, with the periodic checkbox exercise no longer fit for purpose.
- Market regulations are forcing cyber-risk programs to the top of corporate agendas. Certain sectors are now legally obliged to demonstrate cyber-risk frameworks and transparency or face a revoked license to operate.
- Regulations like the EU's Digital Operational Resilience Act (DORA) and the second Directive on Security of Network and Information Systems (NIS2) demand risk management approaches. These regulations require organizations to disclose cyber-risk and report cyber-incidents. At a recent IDC Security Summit, it emerged that even an ISV with less than the staff size required to comply with NIS2 still needed to raise the transparency level of its cyber-risk posture to play in its ecosystem of partners and customers. All businesses are thus motivated to strengthen and modernize their cyber-risk management programs.

AT A GLANCE

KEY STATS

What are your organization's top IT security priorities regarding technologies?*

- **34%:** Governance, risk, and compliance
- **30%:** Cloud security
- **26%:** Application and API security and vulnerability

What are your organization's top IT security priorities regarding operations?**

- **31%:** Data privacy and regulatory compliance
- **28%:** Cyber-resilience of systems and processes, remote work, and threat hunting
- **24%:** Internal security risk management, awareness
- **23%:** Third-party risk management

* Source: IDC's *European Security Annual Survey* (June 2023)
** Source: IDC's *European Security Annual Survey* (June 2023)

KEY TAKEAWAYS

Regulations and compliance are strong drivers of an efficient and thorough cyber-risk management program. Communicating cyber-risk to the C-suite and board as a business issue can enable cyber-risk to become a strategic growth driver and differentiator.

Main Trends

- **Dig-X and Cloud Expand the Attack Surface:** The rapid pace of digital transformation (e.g., the adoption of cloud computing, ecommerce, and connected things) across all industries is changing the way businesses approach cyber-risk. Progress in these areas means competitive differentiation. But cyber-risk can increase as new complexities and less well understood technologies expand the attack surface.
- **Cyber-Resilience:** The negative outcomes of unanticipated cyber-risk can be contained by the implementation of a cyber-resiliency framework.
- **Market Regulations:** The U.S. Securities and Exchange Commission and the EU (through DORA and NIS2) are requiring more transparency in terms of cyber-risk posture. Regional and national institutions like the European Union Agency for Cybersecurity (ENISA) and the U.K.'s National Cyber Security Centre emphasize addressing cyber-risk as a community or collective, as transformed cyber-risk management benefits society and global markets, including supply chains.
- **The Finance Sector's Maturing Approach to Cyber-Risk:** Regulations and fraud prevention objectives have tended to push the financial services sector further along the cyber-risk maturity path. Leaders in this sector understand that they need to identify, predict, and manage cyber-risk continually. Much work is needed to realize these goals, including the increased use of real-time data, advanced analytics, information governance, and monitoring systems for better insights and external reporting.
- **Data Telemetry Changes the Scale and Efficiency of Transformed Cyber-Risk:** Dynamic and real-time metrics provide a lens into the evolving security, risk, and compliance vantage point in real time. This means IT, security, and executive leadership can gain access to the necessary indicators to empower them in understanding and addressing cyber-risks in a proactive and continuous loop to meet the needs of digital-first and cloud-based operations and functions.

Challenges

- **Managing cyber-risk** as an organization transforms at scale and pace is difficult to achieve. Objectives may include adopting cloud compute, cloud storage, integrated digital customer experience platforms, thousands of connected IoT endpoints, and more supply chain partners and web APIs. Coordinating the cyber-risk posture with these new initiatives and aligning them with legacy IT poses a major challenge.
- **A mindset evolution** is required before business leaders perceive the cyber-risk domain as a key business performance indicator rather than a reactive lagging performance indicator. More holistic and transformed cyber-risk tooling, and a shift of the business leadership's overall understanding of the value of the modern approach to cyber-risk, drives positive business outcomes. The CISO and risk management roles can seek to increase the relevance of a transformed cyber-risk program to executives to make sure it is more prominent on the agenda.

- **Cyberthreats** continue to escalate in terms of frequency, intensity (e.g., DDoS), and sophistication. Businesses must understand in real time how cyberthreats and attacks are evolving and unfolding against critical infrastructure and services and thus continually impacting business risk.
- **Nation-state actors** have very powerful cyberattack capabilities. Generative AI (GenAI) is meanwhile making it easier for criminals who have little or no knowledge of cybersecurity to conduct attacks, including ransomware attacks.
- **A lack of confidence or full buy-in from executive leadership** can be a barrier to effective cyber-risk. A March 2023 IDC Survey Spotlight reported that just 53% of organizations have a cyber-risk management program in place.

Benefits

- Businesses that are able to understand cyber-risk in a more holistic and continual sense can leverage these capabilities to carve out **competitive advantage** with clients, prospects, partners, and internal staff.
- A proactive cyber-risk management program should **strengthen cyber-resilience and business operational resilience** over time. This will give supply chain partners confidence and inspire trust in the organization's digital services and customer experience.
- Businesses that can report their cyber-risk posture in a real-time visualization based on data feeds will face **less risk of costly fines or worse, loss of license**, from regulatory bodies and/or cyber-legislation (e.g., DORA and NIS2).
- Cyber-insurance underwriters are likely to insist on **demonstrable actions that address cyber-risk posture** and ongoing management. Failure to implement such measures may increase premiums and lead some underwriters to decline to offer cover.
- An effective program for understanding and visualizing cyber-risk, including an alignment and allocation to the business or initiative that owns the risk, leads to **better remediation of known risks**. Cyber-resilience and zero trust initiatives can be laser-focused on clear objectives to reduce cyber-risks to an organization's digital assets.
- A solid cyber-risk management platform helps organizations identify which risks are acceptable — and thus **accelerate digital product development, partnering, and product/service launches.** Such platforms enable resilience and zero trust initiatives/investments to be assessed in a balanced way. Efforts and funds can then be allocated to limit the potential damage of a worst-case scenario (e.g., a serious cyber-breach, ransomware, DDoS, or data exfiltration).

The Impact of NIS2

- The EU's NIS2, which came into force in January 2023, expands the scope and coverage of the first NIS directive. It is aimed at addressing pan-European fragmentation in cybersecurity approaches. The mandate specifies stricter adherence to strengthening supply chain security and streamlining reporting. Businesses that fail to address requirements will face sanctions and fines. EU member states have until October 2024 to integrate the directive's articles into national legislation.

- The updated legislation applies to more vertical sectors and subsectors, expanding the remit beyond critical infrastructure entities. It applies to all organizations in the designated sectors with 50 or more employees, extending its reach into the midmarket.
- Chapter 4, Article 21 of the directive sets out 10 minimum cybersecurity risk management areas for all organizations. Identity security controls play a significant part, from access control policies and advanced authentication to security of the supply chain.

NIS2: 10 Risk Management Areas

- **Advantages and Disadvantages of GenAI:** GenAI can assist with risk management (e.g., augmenting and automating manual assessment processes), provide clearer root-cause insights, and offer recommendations for risk remediation optimization. Transformed cyber-risk management can be designed, implemented, and fine-tuned to give security leaders and risk managers better insights on root-cause analysis post breach, while also optimizing risk remediation. On the downside, GenAI lowers the entry barrier for criminals to mount cyberattacks, resulting in a greater volume of attacks initiated by actors who may have little technical cybersecurity knowledge. GenAI is also boosting the sophistication of phishing attacks.
- **Zero Trust:** IDC believes zero trust models can deliver robust security and strengthen the cyber-resilience of a business if correctly implemented as part of a holistic and multi-layered defense strategy. Fundamentally, zero trust seeks to ensure that only a verified and identified user, using only an authorized device, has appropriate (e.g., role-based or attribute-based) access to defined resources (e.g., applications and data) in the correct context always (i.e., with the above controls reassessed continuously). Correct implementation of zero trust controls drives data security and privacy and improves overall security posture.

Vendor Profile

- PwC has unveiled a new brand strategy and announced a PwC Global Risk Services division. The initiatives are aimed at helping clients address a broad of array of geopolitical, regulatory, cybersecurity and other risk challenges, and cost pressures.
- PwC has built a comprehensive and robust suite of risk tooling, based on expertise. Its offerings combine a modern approach to risk, including cyber-risk and IT technology risk components for new digital businesses. The components of the Global Risk Services portfolio include Cybersecurity, Risk and Compliance, Internal Audit, Risk Modelling and Data Analytics, Forensics-FCU, Enterprise Technology Solutions, Trust and Transparency Solutions, and ESG Risk.
- PwC began its journey to its new Global Risk Services brand and go-to-market strategy several years ago. Initial steps included aligning capabilities under the Risk and Regulatory Platform and reconstructing the internal organization to align risk services and capabilities according to a “One Firm” principle.
- The Risk and Regulatory Platform was formed to address the most significant risks faced by organizations, including cybersecurity, regulatory, and technology risks, and related organization complexities. Progress and market recognition led to the development of the global Cybersecurity, Regulatory, and Risk brand that was brought to the market by the U.S. firm and deployed throughout the PwC network of firms with flexibility for territory-unique strategies.
- Today, the company's primary purpose is to connect and address risk challenges by leveraging PwC Group synergies, which include a worldwide network of local feet-on-the-ground firms, global priority accounts, training and awareness programs, a strategic ecosystem of technology partners, risk technologies offered through multiple delivery models, shared R&D, and thought-leadership credentials.
- To support delivery, PwC has 25,000+ risk professionals, a vast spread of applied technology for risk tooling, a growing basket of XaaS options that can be licensed, and an ongoing commitment to invest billions of dollars to upskill/reskill PwC staff. Additional credentials include a partner (joint business relationship) ecosystem of leading technology providers, academic institutions, and industry groups, all aligned and collaborating on global risk topics.
- PwC's Managed Cyber Risk (MCR) solution consists of a platform with a number of modules, and a complementary suite of optional services to help operationalize and automate cyber-risk management processes (see figure below).

- MCR comes pre-built with industry-standard control frameworks that are pre-mapped to threats, risks, and metrics, all of which can be configured. MCR can be integrated with existing client tools (e.g., GRC, XSMP, CCM, or TIP) to enable a more real-time view of risk.
- PwC has built MCR using extensive practical experience developing cyber-risk models and reports for hundreds of clients across all industries. Two years ago, a major European banking organization contracted PwC for support with risk reporting. The client understood that this new way of reporting was having a positive effect on communicating risks, threats, and metrics to executives and was a better way of prioritizing weaknesses and addressing them.

Recommendations

- Organizations can address internal skills development by preparing cyber-risk professionals and by investing in, and developing, cyber-risk tooling and solutions.
- Businesses can apply cyber-risk assessments to recognize areas where increased resiliency would have the most significant impact on preventing the compromise of confidentiality, integrity, or availability.
- Organizations can increase collaboration with trusted partners to understand the impact of cybersecurity mandates on procurement templates, staff skills, and training needs.
- Supply chain risk can be overly opaque and difficult to manage. Businesses should proactively and thoroughly search for security gaps in the technology ecosystem. They should implement processes within an overall cyber-risk management capability to identify high-risk supply chain partners that may pose unacceptable risk levels.

Challenges

- Vendors and managed security service providers with cyber-risk management solutions should be ready for new opportunities offered by the EU's NIS2.
- Conducting data collection and analysis in real time across fragmented IT systems and sprawling estates that combine on-premises systems with multicloud is technically complex and difficult to achieve.
- Cyber-risk requires foundational steps to enable businesses to progress to more mature and thorough cyber-risk management programs and platforms. Organizations may build foundational elements in a future-proof cyber-risk management program for longer-term benefits.
- Businesses face an uphill task to define a risk taxonomy that matches what risk quantification and management service providers can offer alongside security vendor tooling. Time and effort spent up front to develop a common cyber-risk taxonomy will reap rewards down the line.
- Legacy business risk approaches tend to be overly reliant on checkboxes that do little to give a real-time, current snapshot of cyber-risk, especially where supply chains are involved.
- A critical obstacle is natural resistance to organizational change. Just over half of organizations now have cyber-risk programs in place. A lack of resources, education, and/or skills can result in cyber-risk laggards. It may be challenging for PwC's prospective customers to accelerate their maturity standing in a modern cyber-risk context.
- There are multiple cyber-risk quantification tools available on the market, but these products may be very theoretical and offer a limited point-in-time visualization. It can be easy to assess cyber-risk posture, but communicating this companywide and addressing known risks in a balanced and effective manner is more challenging.

Conclusion

Cyber-risk management is rapidly becoming a top priority for European security leaders and a key consideration for the broader C-suite. PwC is leveraging its risk management experience to support cyber-risk management with improved visualization and reporting to give ongoing, actionable insights into a business's cyber-risk position.

More than one-third (34%) of organizations polled in IDC's Annual European Security Survey cited identity security governance, risk, and compliance as a top IT security technological priority for 2023.

MESSAGE FROM THE SPONSOR

The cybersecurity industry has spent the last 10+ years trying to improve the way it represents cyber-risk. There are no established industry good practices for cyber-risk reporting. PwC is looking to set the benchmark.

Our approach is based on the principles of pragmatism, flexibility, and explainability. We recognize both the scrutiny that cyber-risk attracts and the wide variety of maturity in risk management practices that exist across the industry.

Unlike many other technology products in this space, PwC's MCR solution includes an extensive catalogue of pre-loaded content and optional services led by our cyber-risk experts. They are passionate about this topic and can partner with you to make the process of end-to-end cyber-risk management easy.

Contact us to learn more about our solution.

About the Analyst

Joel Stradling, Research Director, European Security

As research director for IDC's European Security Practice, Joel Stradling leads the content and analyst team for tracking the European security segment. His main focus areas include zero trust network architecture, managed security services, and cyber-risk and cyber-resiliency.

Joel has 22 years of experience as an analyst of cybersecurity and international managed enterprise network and IT services. He is a regular speaker at major industry conferences that address security and privacy and digital trust and managed security services in B2B enterprise services. He is a well-known and highly regarded expert in the industry who offers insight and advice to C-level executives on security technology competitive landscapes and evolving market segments, including managed security services, zero trust network access, cloud security, risk and compliance, IT/OT security, secure IoT and 5G, secure operations, and endpoint, identity, and access management.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets.

With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives.

Founded in 1964, IDC is a wholly-owned subsidiary of International Data Group (IDG, Inc.), the world's leading tech media, data and marketing services company.

IDC UK

5th Floor, Ealing Cross,
85 Uxbridge Road
London
W5 5TH, United Kingdom
44.208.987.7100
Twitter: @IDC
idc-community.com
www.uk.idc.com

Global Headquarters

140 Kendrick Street,
Building B
Needham,
MA 02494
+1.508.872.8200
www.idc.com

IDC Custom Solutions

This publication was produced by IDC Custom Solutions. As a premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets, IDC's Custom Solutions group helps clients plan, market, sell and succeed in the global marketplace. We create actionable market intelligence and influential content marketing programs that yield measurable results.