DXC.technology

Managing Enterprise Risk in a Connected World

Transforming to a Digital Enterprise

In a connected world, disruptions can be devastating.

A single business in one small corner of the planet can be impacted by geopolitical events and weather disasters thousands of miles away, supply chain issues, vendor failures and more. And as sharing information becomes more prevalent, important and complex, organizations must work even harder to prevent exposure and respond effectively to cyberrisk.

With digital transformation, information technology has moved to the heart of the enterprise. This shift has expanded the need for security, continuity and resilience. Today's business must embrace an enterprise risk management strategy that includes legal, regulatory and political considerations. All levels of the organization should be involved in the discussion. Decision makers should include not only the chief risk officer but also the CIO, CEO and line-of-business executives.

The benefits of protection are well worth the commitment. Beyond keeping a business safe, strong resilience delivers strategic advantages and greater confidence in the pursuit of new business opportunities.

Digital transformation changes business models by enabling new types of interactions across the enterprise and with customers, partners and suppliers. While boosting the business, these new connections can profoundly raise a company's exposure to risk.

Research has shown that it's far cheaper to design for security at the start of a technology implementation than it is to "bolt on" a solution at the end. Yet the need to secure technology up front can create a challenge akin to launching an airplane while it's still being built. There are just too many moving pieces and time constraints.

Adding to this challenge is the need for organizations — especially large, complex, multinational ones — to comply with new and ever-changing legal and regulatory requirements. When combined with a shortage of skilled security personnel, the result is a perfect storm of risk.

And that storm grows bigger by the day. Organizations now face a constantly growing range of enterprise risks and cyberthreats. While some attacks make headline news, others are subtle enough to go undetected for considerable periods of time. And many of these incidents do immediate and lasting damage to affected businesses and their reputation in the marketplace.

An enterprise that fails to protect itself from these security risks may experience the following:

- **Instant brand damage:** A well-publicized data loss or major business disruption can lead to brand damage. With the rise of social media sites and sharing applications, dissatisfied customers can post a video or tweet a complaint, making their feelings known to millions of people around the world almost instantly.
- **Data loss and disruption:** Cyberbreaches often affect the confidentiality, integrity and availability of financial data, customer data, intellectual property, and production and control systems. This can result in widespread business and financial risk.
- **Enterprise embarrassment:** Malicious actors use "doxing" — the act of collecting and sharing damaging information about a person or organization — to harm an enterprise, undermine its goals and embarrass its stakeholders.

A company that mismanages enterprise risk could face a wide range of negative impacts, including a drop in stock price and market cap, an increase in operating costs and legal liability, and a tarnished reputation. Operations could be compromised by a disruption to the supply chain or another adverse event.

The unfortunate reality is that most organizations will be unable to block every risk and cyberattack. This new norm requires them instead to compromise, and focus their efforts on detection, response and recovery.

Gaining stakeholder support

While many supervisory boards are aware of enterprise risk, they often lack a common set of guiding principles.

Governance should start at the top and involve directors, risk committee members and C-level executives. For example, the finance industry uses a three-tier model. The top level provides independent oversight (including audit and regulatory), the middle level provides the enterprise governance, and the bottom level defines how to address risks.

[1] "Advancing Cyber Resilience Principles and Tools for Boards." World Economic Forum, 2017. http://www3.weforum.org/docs/IP/2017/Adv_Cyber_Resilience_Principles-Tools.pdf

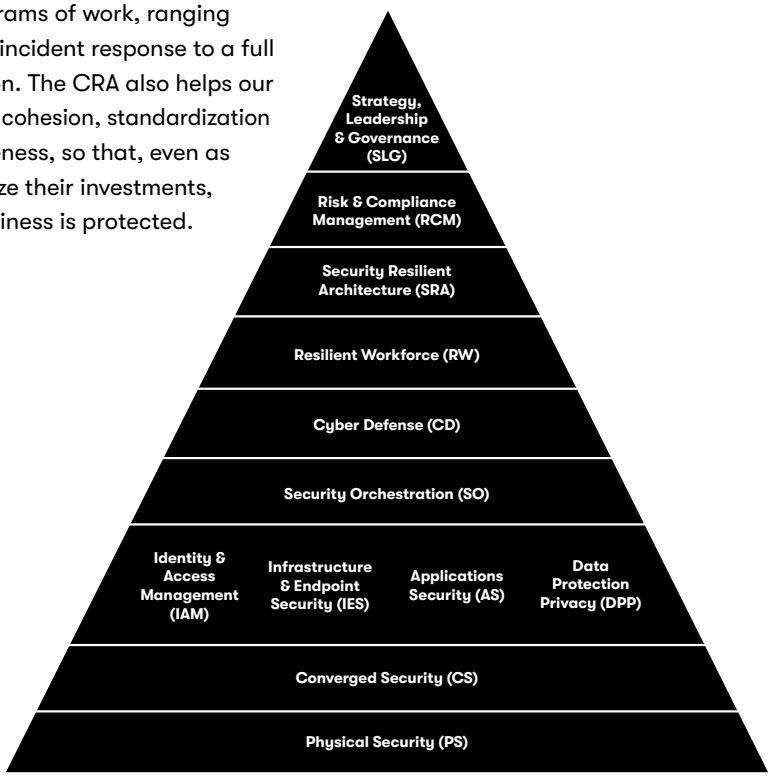
For True Cyberresilience, Take a Structured Approach

A structured approach to cyberresilience can help your organization ensure that all operational functions are clearly defined and deliver the levels of protection required for your overall strategy.

In a clearly defined model, risk becomes the cornerstone for cyberresilience, ensuring that cyberresilience is embedded in every function. This approach provides vital transparency for executives and stakeholders alike.

DXC Security has developed just such a structured model, the DXC Cyber Reference Architecture (CRA). This model is based on work we've done to transform and secure some of the world's largest organizations.

Our structured CRA describes how to manage risks, as well as how to protect, detect, respond and recover information assets. In this model, security capabilities are clearly defined and can provide the basis for blueprints used by programs of work, ranging from a single incident response to a full transformation. The CRA also helps our clients ensure cohesion, standardization and completeness, so that, even as clients optimize their investments, the entire business is protected.



DXC Cyber Reference Architecture

Investments in cybersecurity vary by region: 50% of respondents in Asia-Pacific say they will increase or start using cybersecurity tools, a figure that jumps to 56% in North America and 61% for EMEA, where privacy concerns are paramount.

Source: Global Digital Enterprise Survey 2016-2017, conducted by the Economist Intelligence Unit and sponsored by DXC Technology.

The World Economic Forum has developed a toolkit for implementing these best practices.[1] The organization recommends the following 10 steps, which we have expanded beyond cyberthreats to address additional business risks:

1. **Create a board:** Members will collectively take responsibility for enterprise-wide risk oversight.
2. **Get smart:** Board members should have a good command of the resilience subject. Get them started with a cyberresilience orientation, and keep them informed of new significant threats with regular updates, both in cyberspace and in the physical, economic and geopolitical world.
3. **The buck stops here:** Assign one corporate officer the responsibility of reporting on the board's capabilities and progress. And ensure that this officer has the necessary access, authority, subject matter knowledge, experience and resources.
4. **Get integrated:** Risk assessment and resilience should be integrated into the organization's overall business strategy, risk management and budgeting. This is best led by the board.
5. **Annual checkup:** Have the board define the organization's risk tolerance on an annual basis, and ensure that it aligns with the corporate strategy (for more on measuring your risk appetite, see below).
6. **Reporting framework:** Make executives responsible for reporting on cyberrisks, threats and events during all board meetings. Also, provide the board with a framework for validating these assessments.
7. **More planning:** Have the board lead the creation, testing and implementation of resilience plans.
8. **Don't go it alone:** Collaborate with other enterprise stakeholders (when appropriate) to ensure systemic resilience.
9. **Clean sweep:** Conduct an annual, independent review of your risks as new partners, services and information sources come online and as strategies shift.
10. **Get better:** Have the board periodically review its own performance and seek advice for improved effectiveness and digital awareness.

Determining risk appetite

Risk appetite or tolerance can be difficult to measure, in part because business units in an organization may view the same risk differently. This can lead to inappropriate levels of risk control.

Fortunately, models are available to help enterprises navigate this terrain. The World Economic Forum has established guidelines to help boards define and quantify their organization's risk tolerance, ensuring consistency between its corporate strategy and its risk appetite. These include:

- Understanding the potential business impact of risk on both individual projects and business lines, as well as on the organization as a whole
- Agreeing on risk appetite in light of shareholder, regulatory, customer and external perspectives, such as legal and regulatory considerations
- Understanding how the balance between meeting business objectives on the one hand, and the operational cost and impact of cybersecurity on the other, is determined by risk appetite
- Clarifying how the agreed-upon risk appetite should be applied to business decision making
- Presenting the difference between agreed-upon risk appetite and actual risk tolerance on an annual basis

Creating a risk framework and matrix

A risk framework and matrix are essential tools for discussing and managing risk. These guidelines take into account the risk appetite parameters discussed above and align them with actions that must be taken to manage or mitigate threats.

Within the matrix, organizations should outline the complete portfolio of risks they face, taking into account all relevant legal, operational, financial, reputational and strategic considerations. Identified risks can be assessed across two dimensions:

- The potential impact on the confidentiality, integrity and availability of assets that may include intellectual property, infrastructure and personally identifiable information
- The likelihood that threats and vulnerabilities to people, processes and technology could put those assets at risk

Over the next 2 years, 80% of consumers in developed nations will defect from a business because their personally identifiable information is impacted in a security breach.

Source: IDC FutureScape: Worldwide Security Products and Services 2017 Predictions, Doc #US41866116, November 2016

In Risky Times, Try Antifragility

We live in risky times.

Consider the 2008 financial crisis, devastating terrorist attacks, the European migration crisis. Think about the cyberattacks on corporate, national and international infrastructures that have dominated the news. And the possibility of trade wars, geopolitical conflicts and civil disorder that challenge global stability.

Today, nearly everything is hyperconnected, subject to inspection and controllable. That's true for vehicles, nuclear power plants, factories, fridges, hospital equipment, wearable devices and so much more.

This connection has brought ease and efficiency to our daily lives, but it dramatically increases the risk. Making matters worse, we often design fragility into our systems and processes, particularly in search of efficiency and cost cutting opportunities.

The Leading Edge Forum contends that many businesses and governments have essentially sleepwalked into the 21st century world of VUCA — short for volatility, uncertainty, complexity and ambiguity. What's needed instead is an evolution in the way we approach risk — how we think about it, sense it, manage it and monitor it.

Unfortunately, most traditional approaches to risk management suffer from two major flaws:

- They neither fully protect the organization, nor help it take intelligent, value-creating risks in a world of increasing VUCA.
- Many businesses, in their quest for profit growth and efficiency, have built engineering fragility into their organizations, often accidentally.

A powerful alternative is the relatively new concept of "antifragility," an approach that not only gains from chaos but also requires it in order to survive and flourish. The term, coined by author Nassim Nicholas Taleb, offers several benefits:

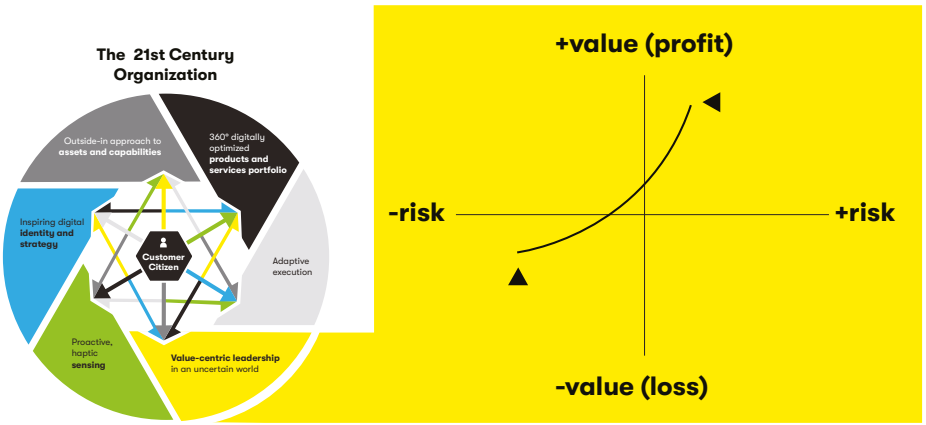
- A new perspective focused on "bending luck" that guides organizations to win more than they lose when hit by shocks, stressors and risks
- The fusion of value creation with risk management in high-VUCA environments
- The ability to be applied at all levels of component, process and business models where traditional statistics-based correlations still regularly miss unexpected events

How the organization views risk matters. Instead of taking only an engineer's view of risk, organizations should also consider a financial viewpoint. Seen this way, risk is an inherent (and not always negative) feature of all business, process and value flows.

Companies can therefore choose activities that offer attractive risk/return profiles or yield curves. They can also bend those yield curves in ways that make them even more attractive.

— Dave Aron, global research director, Leading Edge Forum

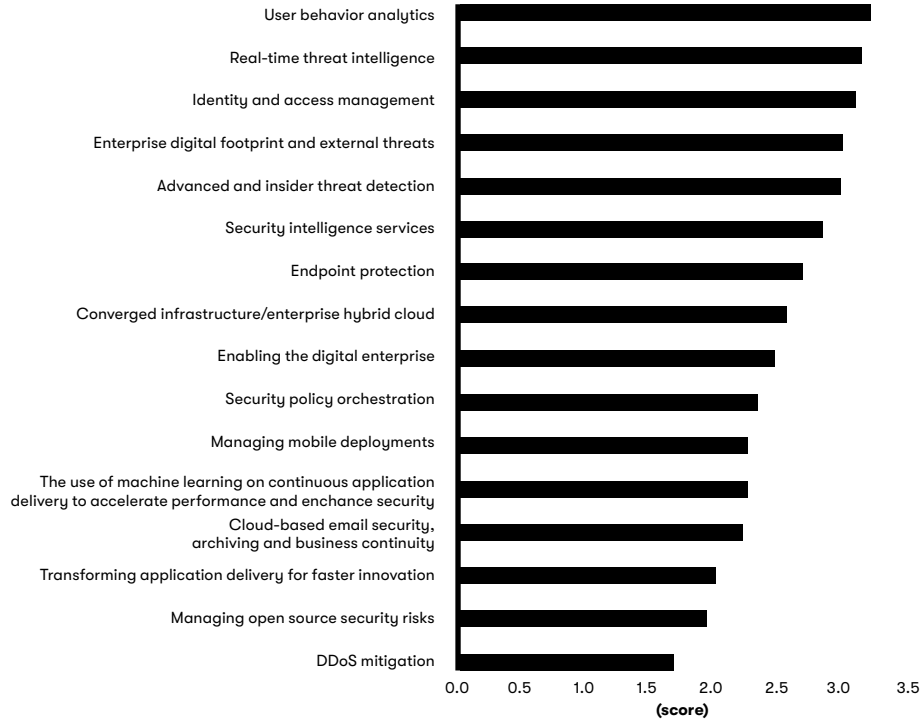
"Bending Luck" with Antifragility



For example, retailers may note the risk of customer credit card information being stolen by hackers. This act could lead to financial losses, unhappy customers and serious reputational damage, making it a high-impact event. And, as recent headlines have demonstrated, this type of theft is all too common, making it highly probable as well.

Organizations should use the risk framework to highlight possible events, their potential effects and reponse options. By separating this discussion from business desires, such as the need to simplify transactions and increase customer satisfaction, it's possible to focus on the agreed-upon risk appetite.

CIOs and CISOs' Security Technology Priorities for the Next 12 Months



Note: Scores are based on a scale of 0-4, with "0" being "not a priority" and "4" being "high priority"

Source: IDC Market Snapshot: CIOs and CISOs' Security Technology and Service Priorities, Suya Xiong and Pete Lindstrom, Doc #US41881216, November 2016

The end state

To become resilient, both IT and business leaders must engage in ongoing dialogue about the balance of risk versus opportunity. Incorporating discussion about cyberrisk and other threats into the overall business strategy is much more effective than simply reacting to the latest "cyberscare." In fact, it normalizes the topic of risk.

While it may be difficult at first for enterprises to gain a transparent view of threats, especially in organizations that have little to no experience in cybersecurity, it can be done, in part by adopting the structured approach outlined above and by getting all organizational leaders speaking the same risk language.

To start, leaders must identify their current position on the risk-versus-opportunity continuum; that is, where they want to be on the continuum now, given the current view of overall strategy and opportunities. They may also consider where they want to be in the future, as new business opportunities emerge or fail to materialize. Will the organization be compelled to take on more risk? Will it be less willing to accept risk?

For instance, a move to the cloud might expose the organization to new cyberrisks, but it can also deliver huge gains, such as increased capacity, greater flexibility and reduced capital expenses. To balance these risks and rewards, stakeholders will need to take into account the organization's overall strategy, risk appetite, new business opportunities and current challenges.

Improved resilience can deliver other benefits as well. Organizations that gain a better understanding of — and response to — risk can adapt and change more quickly than their competitors. Business agility can lead the way to new projects, beneficial acquisitions and other fruitful opportunities.

Ready to manage your enterprise risk in the digital economy? Follow the guidelines outlined above, take initial steps to assess your risk status and determine where immediate improvements are needed. Then consider partnering with an expert in security management to implement the cutting-edge tools that can ensure success.

How DXC and Partners Can Help You

Managing enterprise risk is a major undertaking. Fortunately, you don't have to go it alone. DXC has deep expertise and experience in risk, digital transformation and industry optimization.

Our risk solutions and services include risk reporting, risk data aggregation, security risk management and more. Our governance services can help you manage risk, discuss risk up and down your organizational hierarchy, and provide individual risk profiles for further discussion.

And our Cyber Reference Architecture, developed with our clients, draws on leading threat research to help you increase your cyberresilience and address your company's unique challenges using a set of defined industry and technical blueprints (see sidebar, "For True Cyberresilience, Take a Structured Approach").

You can also turn to DXC for software-based risk solutions, including our Riskmaster Accelerator software that supports risk and claims management in all industries, including education, energy, government, healthcare, manufacturing, retail and transportation.

Partners help, too. DXC's Partner Network features more than 250 industry-leading strategic and solution providers, including Amazon Web Services, HPE, IBM, Microsoft, Palo Alto Networks, SAP and ServiceNow. We work with our partners to create and deliver the right solution to address your top risk-management challenges.

For more details, visit **www.dxc.technology/security.**

Authors

Chris Moyer is the chief technology officer of Security at DXC Technology. He is responsible for technical strategy and innovation for advisory services, security operations, threat management, identity management, endpoint security, data protection, cloud security and enterprise risk management. Previously, Chris was CTO for Hewlett Packard Enterprise Services and vice president for Mobility and Workplace, bringing technical thought leadership to clients and delivering market-leading workplace and user support services globally. He incubated new services and built strategic technical alliances for HPE-ES across its offering portfolio.

▶ **chris.moyer@dxc.com**

Art Wong is senior vice president and general manager of Security at DXC Technology. He is responsible for the company's security offerings, including advisory services, managed security services, identity management and monitoring, and information assurance. Prior to this role, Art served as senior vice president and general manager of Enterprise Security Services at Hewlett Packard Enterprise, where he worked with large global clients across industry sectors to help manage their information security risk, protect their assets and improve business performance.

▶ **art.wong@dxc.com**

DXC Technology's ResearchNetwork contributed to this paper.

DXC.technology

Learn more at
www.dxc.technology/digital_enterprise

DXC Technology (DXC: NYSE) is the world's leading independent, end-to-end IT services company, helping clients harness the power of innovation to thrive on change. Created by the merger of CSC and the Enterprise Services business of Hewlett Packard Enterprise, DXC Technology serves nearly 6,000 private and public sector clients across 70 countries. The company's technology independence, global talent and extensive partner network combine to deliver powerful next-generation IT services and solutions. DXC Technology is recognized among the best corporate citizens globally. For more information, visit dxc.technology.