CIOs Should Manage Technology Risk and Cybersecurity Through the Lens of Business Value

Published: 3 November 2016 **ID:** G00314523

Analyst(s): Paul E. Proctor

CIOs should address technology risk and cybersecurity challenges through the lens of business value to deliver appropriate levels of protection that support business outcomes. Treat cybersecurity like a business function.

Key Challenges

- Cybersecurity and technology risk are perennial issues with board-level visibility.
- Check box approaches to cybersecurity create overspending in some areas and unacceptable levels of risk in other areas.
- As organizations transition to digital business, infrastructure and applications are less directly owned, and more services are outside of IT's control.
- Concern over cybersecurity and technology risk hinders innovation — the lifeblood of digital business transformation.

Recommendations

To better communicate the business value of IT, CIOs should:

- Create executive awareness and appetite to manage and accept appropriate levels of risk that support business outcomes. Use people-centric security to create behavior change, so that people move from being the weakest link in the security chain to the strongest.
- Build and formalize a risk-based approach and program that acknowledges the basic risk appetite shift when adopting digital business. Identify gaps and opportunities for improvement, stack-rank the resulting remediation projects and create multiyear remediation plans.
- Manage cultural change to create a risk-engaged culture. Help your non-IT counterparts to understand and consciously engage in good decision making related to technology risks.

- Transform technology risk and cybersecurity into a business function. Position accountability for security as a business unit issue, which allows business units to choose their level of investment and balance the needs to protect against the needs to run their business.

Table of Contents

List of Figures

Strategic Planning Assumptions

By 2020, 60% of digital businesses will suffer major service failures due to the inability of IT security teams to manage digital risk.

By 2020, 60% of enterprise information security budgets will be allocated for rapid detection and response approaches, up from less than 30% in 2016.

By 2018, 25% of corporate data traffic will flow directly from mobile devices to the cloud, bypassing enterprise security controls.

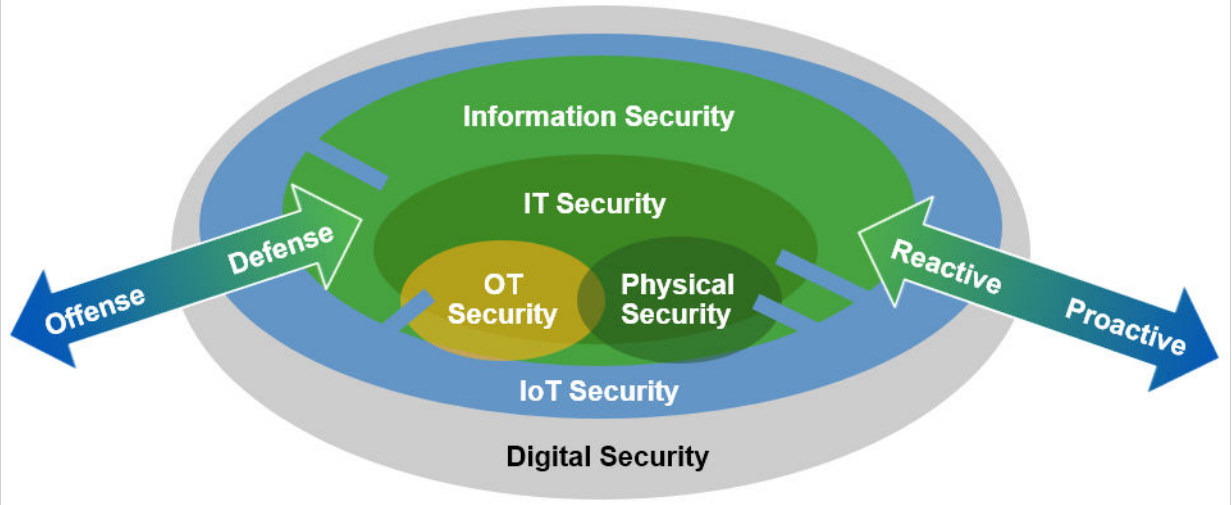
Introduction

Business value is the best lens for CIOs to appropriately manage technology risk and cybersecurity. This lens is best described as better understanding the dependencies business outcomes have on technology. Doing so improves risk management decision making, while also improving corporate performance though improved risk management. Cybersecurity today is often thought of as a technical problem, handled by technical people, buried in IT. As cybersecurity becomes a risk-based discipline, corporate performance is a great foundation for prioritization of resource against business outcomes. Also, CIOs engaging their peer executives to better understand the business value of IT will have more rigor and defensibility when their business case is tied to corporate performance dependencies on technology.

Digital Business Changes Everything About Technology Risk and Cybersecurity

CIOs need to understand the current context and trajectory of managing technology risk and cybersecurity in a modern enterprise. Cybersecurity is a critical part of enterprise value delivery with today's broader external ecosystem and new challenges in an open digital world. As organizations transition to digital business, externally owned infrastructure and services must be addressed by cybersecurity. Digital trust must be established with customers, and partners will be required to effectively compete in the digital business world (see Figure 1).

Figure 1. The Elements of Digital Security



Source: Gartner (November 2016)

Safety becomes an issue with the intersection of technology and the physical world (IT/operational technology [OT]/Internet of Things [IoT]). The pace of business accelerates to algorithmic speeds as algorithms take over business decision making from human intervention. Digital risks and digital adversaries will continue to challenge organizations, and more losses should be expected. In a 2016 study of non-IT executives, 71% said that concerns over cybersecurity are impeding innovation in their organizations.[1]

Material shifts in culture, behavior and technology are required to effectively address technology risk and cybersecurity. In the future, security officers will work more like intelligence officers and trusted advisors as citizen and business unit IT become the dominant model:

- By 2020, 60% of digital businesses will suffer major service failures due to the inability of IT security teams to manage digital risk.
- By 2020, 60% of enterprise information security budgets will be allocated for rapid detection and response approaches, up from less than 30% in 2016.
- By 2018, 25% of corporate data traffic will flow directly from mobile devices to the cloud, bypassing enterprise security controls.

Organizations will learn to live with acceptable levels of digital risk as business units innovate to discover what security they need and what they can afford. Digital ethics, analytics and a people focus will be as important as technical controls (see "Special Report: Cybersecurity at the Speed of Digital Business").

Leadership and Governance

Improving leadership and governance is arguably more important than developing technology tools and skills when addressing cybersecurity and technology risk in digital business. Key attributes of a successful program that balances the need to protect with the need to run the business are:

- Decision making
- Prioritization
- Budget allocation
- Measurement
- Reporting
- Transparency
- Accountability

Accountability is non-negotiable in the digital business world.

The expectation and management of cybersecurity is very different now compared to the past 20 years. Security has new levels of funding, but that comes with new expectations for execution:

- Security has new visibility with executives, but that comes with new scrutiny.
- The organization has new delivery models like cloud, mobility and the IoT to protect, but that requires new technologies.
- The organization has new ways of work, like bimodal IT, but that requires new skills and approaches.

The security department has less control as the ways to create and consume IT services evolve, such as business unit IT and citizen development.

Cybersecurity program value delivery is advancing from defense and protection-only to support resilience and risk-based approaches. This requires a shift in culture and skills.

The Evolving Threat Environment

Advanced threats continue to evolve through targeted and pervasive mechanisms. The blurring of the lines between physical and digital have made safety a primary concern of cybersecurity. Incident response must address recovery and resilience in the face of aggressive business disruption attacks.

Cybersecurity at the Speed of Digital Business

Digital business moves at a faster pace than traditional business, and traditional security approaches designed for maximum control will no longer work in the new era of digital innovation. Business opportunity, development, decision making and expectations will have to be addressed in

a timely and efficient manner, requiring new skills and practices. Programs will evolve. Bimodal IT and the emergence of Mode 2 projects in mainstream management will require a new approach to cybersecurity.

Cybersecurity at the New Edge

It used to be easy to protect data because we knew where it was — in the data center. The new edge has pushed far beyond the data center into OT, cloud, SaaS and things. Organizations need to address cybersecurity and risks in technologies and assets they no longer own or control. Business unit IT is a fact in most modern enterprises, and it will not be shut down by cybersecurity and risk concerns. It must be embraced and managed to deliver appropriate levels of protection.

People and Process: Cultural Change

It has been a platitude for years that cybersecurity requires people, process and technology, but the people and process have not received the same attention as the technology. Cybersecurity in many organizations has been written off as a technical problem, handled by technical people, buried in IT. With the acceleration of digital business and the power technology gives individuals, it is now critical to address behavior change and engagement — from your employees to your customers. Cybersecurity must accommodate and address the needs of people through process and cultural change.

Analysis

Create Executive Awareness and Appetite to Manage and Accept Appropriate Levels of Risk That Support Business Outcomes

Introduce Your Non-IT Executives to the Notion That There Is No Such Thing as Perfect Protection

Non-IT executives believe that risk protection is a technical problem, handled by technical people, buried in IT. They believe that with sufficient money and people they will be OK. This must be addressed directly to avoid the common pitfall of firing the people in charge when there is an inevitable hack or data breach. Once the narrative is shared, you can turn your attention to transforming risk and security into a business function with far more manageable expectations (see "Board-Ready Slides for Cybersecurity and Technology Risk: Sample Narrative — First-Time Presentation").

Risk acceptance is well understood in business where trade-offs for risk and reward happen with every decision. Corporate performance benefits when technology also exists on a sliding scale of risk and reward. Business outcomes dependent on technology should be considered at risk, so appropriate decisions and investments can be made to accept or lower risk.

Identify Opportunities to Use People-Centric Security to Address Behavior Change

People are commonly understood to be the weakest link in the security chain, but they can be the strongest. Also, with all the power of technology and the rise of delivery models like business unit IT, security is in the hands of decision makers and regular employees (think email on your personal phone) very frequently. Centralized control is no longer sufficient. Posters and mouse pads that say security is important are not effective. What is needed is an approach that is designed to directly impact behavior. Gartner's research in people-centric security is the intersection of security and the social sciences to use techniques known to change behavior (see "Consider a People-Centric Security Strategy").

Most organizations recognize the value and necessity of their people in the achievement of business performance goals. A people-centric approach to the use of technology should be integrated with the human capital investments made in the normal course of business. As organizations create whole business models on technology, a people-centric approach delivers on the business value of IT.

Build and Formalize a Risk-Based Approach and Program

Formalize and Measure a Risk and Security Program That Delivers Variable Levels of Protection

Identify gaps and opportunities for improvement, stack-rank the resulting remediation projects and create multiyear remediation plans. Define security service levels that provide gold, silver and bronze levels of risk, and work with each business unit to deliver their desired level of protection with conscious recognition and acceptance of residual risk. Maturity models provide a good abstraction of technology choices and risk levels in conversations with non-IT executives (see "Assess Program Risk Posture and Set Priorities Using Process Maturity" and "CISOs Need to Understand the Components of Their Information Security Programs").

Measurable programs and measurable outcomes are necessary to make the linkage between corporate performance and the business value of IT. Creating variable levels of protection further supports the ability to choose investments and make conscious business decisions around the acceptance of risk to achieve business outcomes.

Formalize Risk Assessment Capabilities to Avoid a Paper-Pushing Exercise That Delivers No Value

The most common failure of risk programs today is that they have become paper pushing exercises where many executives are surveyed about risks, many resources assess risk, many reports are written, but very few decisions are influenced or value-delivered. Risk assessment methods should be short and practical to deliver just enough information and defensibility to support specific decision making. Beware of complex and sophisticated methodologies that are not understandable by non-subject-matter-experts. Identify specific audiences and the decisions to be influenced by any risk assessment activity (see "Six Required Elements of Effective Risk Management").

The failure of risk assessment capabilities could be likened to the impacts of failed due diligence in a business decision such as merger and acquisition activity. Poorly informed technology decisions through the lens of corporate performance are bad business decisions with similar impacts as bad due diligence.

Develop a dashboard of leading indicators linked to business outcomes. One of the most common questions today in risk and security is "What should we report to our board of directors?" There is no one common answer to this or a list of metrics that work for every organization. Mapping business outcomes to supporting business processes and technology dependencies creates a foundation to develop the five to nine metrics necessary to show both the business value of IT and the appropriate status of risk and security to executives and the board of directors (see "Develop Key Risk Indicators and Security Metrics That Influence Business Decision Making").

Metrics and reporting are key to business decision making in corporate performance. Effective technology metrics linked to business outcomes improve corporate performance. Businesses have leading indicators that drive material investment and resources. Technology should be no different.

Shift Security Investment to Detection and Response

CIOs must move from trying to prevent every threat, and acknowledge that perfect protection is not achievable. Organizations need to detect and respond to malicious behaviors and incidents, because even the best preventative controls will not prevent all incidents. By 2020, 60% of enterprise information security budgets will be allocated for rapid detection and response approaches, up from less than 30% in 2016 (see "Shift Cybersecurity Investment to Detection and Response").

This shift has a direct impact on budget and the acceptance of certain risks. The impacted business processes and outcomes should similarly be identified to create resilience and response plans. This manages and protects corporate performance and demonstrates the business value of IT.

Address new IT delivery models. The evolution of IT services and how they are consumed continues. Traditional security models do not work for most of these and must also evolve. These realities must be formally addressed as part of the security program and the evolution of IT itself:

- Cloud delivery models have come a long way, but many organizations are just getting started. Understand that cloud provider security is not the problem, it is your organization's inability to engage and use cloud services appropriately and securely (see "Clouds Are Secure: Are You Using Them Securely?").
- Mobile apps are emerging as a primary delivery model for many field operations from claims processing in insurance to factory floor operations in manufacturing to mobile marketing in multiple industries (see "The Gartner Risk Treatment Model for Mobile Marketing").
- Bimodal IT is an approach being adopted by many Gartner clients to address the reality that traditional approaches to development and delivery activities are not appropriate in all cases. These fail-fast, iterative approaches to development require a new approach to security (see "The Four Steps to Manage Risk and Security in Bimodal IT").

- Business unit/Citizen/Shadow IT is also emerging as a legitimate delivery model because of the power and access to technology and technology services outside of traditional channels. CIOs need to gain visibility into these activities and appropriately manage risk with new approaches more focused on contract SLAs and the acceptance of risk by the executives who engage in these services (see "Unsanctioned Business Unit IT Cloud Adoption Will Increase Financial Liabilities").

Each of these delivery models comes with not only risk, but also business benefit. Those business benefits should be considered and measured just as the risk and security requirements are considered. Each of these has a direct impact on corporate performance and the value of technology.

Manage Cultural Change to Create a Risk-Engaged Culture

Accountability is broken today because it means identifying who to fire when something goes wrong. This is exceptionally problematic as we transition to a risk-based world where non-IT executives understand the impact of technology dependency, and fund both IT and security efforts appropriately based on their support for desired business outcomes.

Develop a Risk-Engaged Culture to Socialize the Idea of Consciously Accepting Risk

It is necessary to improve executives' engagement in specific levels of risk that are consciously chosen. This will have the beneficial effect of improving executive decision making when it comes to controlling IT spend as they connect business outcomes to technology and risk levels (see "The Gartner Risk Treatment Model for Digital Business").

A risk-engaged culture is one of the most important shifts for a CIO. Business decisions are never made without a consideration of their risk. Traditionally, technology dependencies and security are just expected to be managed by the non-IT executives. CIOs need to help their non-IT counterparts to understand and consciously engage in good decision making related to technology risks.

Transform Technology Risk and Cybersecurity Into a Business Function

Security programs today are perceived as cost centers with a purpose to protect the organization from cybersecurity threats. This leads to poor investment decisions and improper expectations. It is possible to create a set of sustainable security services that deliver defined levels of risk at defined cost. At the highest levels of maturity, it is even possible to create chargeback for the business units. Doing this properly positions accountability for security as a business unit issue that allows the business units to choose their level of investment and to balance the needs to protect against the needs to run their business. This is a three- to five-year journey for most organizations, but the clock doesn't start until a decision is made to pursue this approach.

Corporate performance and the business value of IT are fully integrated into this concept of treating security as a business function. Today, most businesses understand that they pay for infrastructure, laptops and applications, but very few think about the cost of security against a variable level of protection.

Case Study

The Dutch national police have developed an efficient and effective risk-based approach and methodology. This approach engages and delivers value to senior executives, and creates the balance between the needs to protect information and the needs to achieve the organizational outcomes of a 65,000-person national police force.

In 2003, the Amsterdam police used traditional risk matrixes and workshops that were limited by traditional check box approaches, which were not meeting the organization's needs. Management supported discarding check boxes, but they needed clearer outcomes in management language that solved operational, not IT, problems. The immediate challenge was to convince the management board of the added value of a risk analysis that would be delivered within a week with an outcome that was handed off to non-IT executives.

The outcome formulated the business consequences in plain language. This had two effects:

- Non-IT management understood the options and the necessary decisions in the context of the effects on the core business.
- Non-IT decision makers could no longer plausibly deny that they were just following the guidance of the technical experts.

Management was quick to embrace and support the method for risk-based security. It even gave them a broader perspective; since the analyses weren't limited to security, they focused on operational risks — even to the point that the chief of police and the management board are defending the method and its value against external pressure from auditors to apply check boxes (see "CIOs Must Implement a Risk-Based Approach to Improve Business Outcomes").

Gartner Recommended Reading

Some documents may not be available as part of your current Gartner subscription.

"Special Report: Cybersecurity at the Speed of Digital Business"

"Measure, Report, and Improve Enterprise Risk Culture"

"CIOs Must Implement a Risk-Based Approach to Improve Business Outcomes"

"Board-Ready Slides for Cybersecurity and Technology Risk: Sample Narrative — First-Time Presentation"

"Consider a People-Centric Security Strategy"

"Six Required Elements of Effective Risk Management"

"Develop Key Risk Indicators and Security Metrics That Influence Business Decision Making"

"Clouds Are Secure: Are You Using Them Securely?"

"The Four Steps to Manage Risk and Security in Bimodal IT"

"The Gartner Risk Treatment Model for Digital Business"

Evidence

[1] "Cybersecurity as a Growth Advantage."

More on This Topic

This is part of an in-depth collection of research. See the collection:

- Cybersecurity and Digital Risk Management: CIOs Must Engage and Prepare

GARTNER HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Regional Headquarters
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations,
visit http://www.gartner.com/technology/about.jsp

© 2016 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates. This publication may not be reproduced or distributed in any form without Gartner's prior written permission. If you are authorized to access this publication, your use of it is subject to the Gartner Usage Policy posted on gartner.com. The information contained in this publication has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information and shall have no liability for errors, omissions or inadequacies in such information. This publication consists of the opinions of Gartner's research organization and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice. Although Gartner research may include a discussion of related legal issues, Gartner does not provide legal advice or services and its research should not be construed or used as such. Gartner is a public company, and its shareholders may include firms and funds that have financial interests in entities covered in Gartner research. Gartner's Board of Directors may include senior managers of these firms or funds. Gartner research is produced independently by its research organization without input or influence from these firms, funds or their managers. For further information on the independence and integrity of Gartner research, see "Guiding Principles on Independence and Objectivity."