Special Report: Cybersecurity at the Speed of Digital Business

FOUNDATIONAL **Refreshed:** 7 December 2017 | **Published:** 30 August 2016 **ID:** G00315580

Analyst(s): Paul Proctor, Ray Wagner

Cybersecurity is the foundation of digital business and innovation. It must address a new reality in which IT organizations have little direct infrastructure, and their biggest security concerns will come from services outside their control.

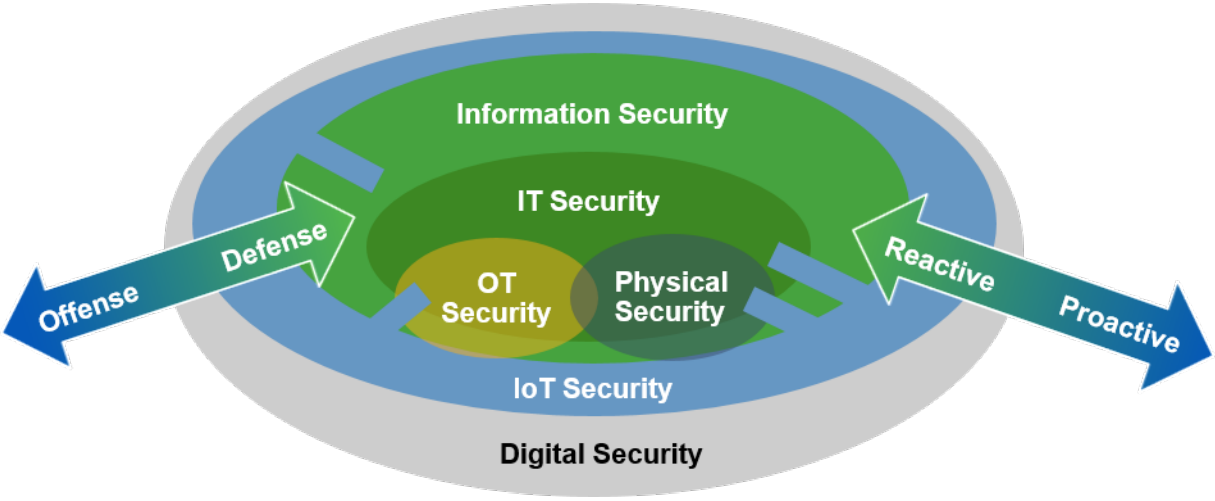
FOUNDATIONAL DOCUMENT

This research is reviewed periodically for accuracy. Last reviewed on **7 December 2017**.

Analysis

Cybersecurity is a critical part of digital business, with its broad external ecosystem and new challenges in an open digital world. The scope of cybersecurity is expanding and becoming digital security (see Figure 1). As organizations transition to digital business, cybersecurity will need to address the lack of directly owned infrastructures and the prevalence of services outside IT's control. 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 is accelerating to algorithmic speeds, as algorithms replace human intervention in business decision making. 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]

Figure 1. The Scope of Cybersecurity Is Expanding to Become Digital Security



Source: Gartner (August 2016)

Material shifts in culture, behavior and technology are required. As citizen and business unit IT becomes the dominant model, security officers will work more like intelligence officers and trusted advisors:

- 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, which is an increase 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.

As business units innovate to discover what security they need and what they can afford, organizations will learn to live with acceptable levels of digital risk. Digital ethics, analytics and a focus on people will be as important as technical controls.

Gartner has identified five key areas of focus for successfully addressing cybersecurity in digital business:

- Leadership and Governance
- The Evolving Threat Environment
- Cybersecurity at the Speed of Business
- Cybersecurity at the New Edge
- People and Process: Cultural Change

Research Highlights

Leadership and Governance

When addressing cybersecurity and technology risk in digital business, improving leadership and governance is arguably more important than developing technology tools and skills. Decision making, prioritization, budget allocation, measurement, reporting, transparency and accountability are key attributes of a successful program that balances the need to protect against the need to run the business.

Compared with the past 20 years, everything is different now for security officers and security departments. They have new levels of funding, but that comes with new expectations for execution. They have new visibility with executives, but that comes with new scrutiny. The organization has new delivery models, such as the cloud, mobility and the IoT to protect, but that requires new technologies. The organization has new ways of work (e.g., bimodal IT); however, this requires new skills and approaches. As the ways to create and consume IT services, such as business unit IT and citizen development, evolve, security departments have less control.

This special report addresses critical areas, such as the evolution of skills and the scope of responsibility for IT risk and cybersecurity leaders, the development and management of a mature cybersecurity and technology risk program, and reporting to non-IT executives, such as your board of directors. It also covers the transformation of cybersecurity and risk culture. The value delivery of cybersecurity programs is advancing from defense and protection only to support resilience and risk-based approaches.

- "Managing Risk and Security at the Speed of Digital Business" — Digital business challenges the basic principles of information risk and security management. Risk and security leaders must understand the risks associated with business unit innovation, and balance the imperative to protect the enterprise with the need to adopt innovative technology approaches.
- "Use Six Principles of Resilience to Address Digital Business Risk and Security" — Risk and security leaders' ability to steer their organizations through the intersection of digital business and increasing IT risk and cybersecurity threats will create resilience, differentiate their organizations, define their legacies and shape the ways that future enterprises apply technology.
- "How to Build an Effective Cybersecurity and Technology Risk Presentation for Your Board of Directors" — It is now common practice for a board of directors to require annual reporting on the state of IT risk and information security. Risk and security leaders must provide board-relevant and business-aligned content, and this sample board presentation can help.
- "Create a Digital Risk Officer Role in Your Organization" — Organizations will have to create the new role of digital risk officer to address the changing nature of risks and threats across IT, OT and IoT, as well as safety concerns in the era of digital business. Risk and security professionals should prepare now for the additional responsibilities they will be asked to assume.
- "Align Your IAM Program With Your CIO's 2016 Priorities — Building the Digital Platform" — Identity and access management (IAM) leaders spend most of their time and effort servicing the

IT legacy debt — nurturing and developing legacy assets and capabilities. CIOs remain key IAM stakeholders; however, CIOs are starting to focus on a cultural shift toward digital business and innovation. True innovation requires vision and new approaches, involves different stakeholder representatives, and happens on different fronts. In IAM, the most potential for innovation is on the edge (e.g., the cloud, mobile and consumers), sometimes driven by other IT teams, or sometimes even by other lines of the business (such as marketing).

- "How to Get Your CEO to Embrace Digital Risk Management" — Common risk management practices are often a barrier to achieving strategic business outcomes. By proactively assessing risk appetite and the value of the desired business outcome, CIOs and chief information security officers (CISOs) can transform digital risk management into a competitive advantage.
- "Using Storytelling to Bolster Your Security Communication Plans" — CISOs and CIOs looking to communicate risk management needs to decision makers should use the ancient techniques of storytelling, which can have contemporary relevance.
- "Developing Digital Risk Leaders for Digital Business Innovation" — With a more-complex and intertwined global technology environment, the number of digital risks facing companies continues to multiply. As a result, the demand for risk management leaders is increasing. CIOs must develop digital risk leaders to ensure successful digital business innovation.

The Evolving Threat Environment

Advanced threats continue to evolve, and Gartner provides a top-down analysis of the latest trends for addressing these targeted and pervasive mechanisms. We also explore the potential future of threats in 2020, where the blurring of the lines between physical and digital will make safety a primary concern of cybersecurity. Incident response must address recovery and resilience in the face of aggressive business disruption attacks.

- "Shift Cybersecurity Investment to Detection and Response" — IT risk and security leaders 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.
- "Prepare for and Respond to a Business Disruption After an Aggressive Cyberattack" — Awareness is skyrocketing in boardrooms around the globe of the rapid increase, breadth and depth of cyberattacks and their resulting financial and reputational impacts. Organizations must integrate security incident response processes with those used for business continuity management.
- "Cybersecurity Scenario 2020 Phase 2: Guardians for Big Change" — Changes in computing fabric, devices and services wrought by digital business continue to shape risk and security landscapes. Business transparency and digital value generation drive security and risk leaders to develop security and risk practices for business resilience.
- "Best Practices for Detecting and Mitigating Advanced Threats, 2016 Update" — Information security, network and communications practitioners are obligated to employ best practices to prevent, detect and mitigate advanced threats. These practitioners should leverage existing and emerging security technologies in their security architectures.

- "Building a Strong Advanced Threat Defense Posture" — The ongoing episodes of high-profile security breaches in today's environment are inspiring a shift in security strategy. Most CISOs accept that all attacks cannot be prevented; malicious activity is now too frequent, too well-disguised or too innovative for an organization to rely on a perfect prevention strategy.
- "Understanding Insider Threats" — Risk and information security practitioners struggle to understand and address insider threats. Gartner did an in-depth survey with 186 participants to understand insider threats through current incidents. Here, we summarize the results and identify steps for addressing different kinds of threats.
- "How to Plan and Execute a Threat Assessment" — The threat assessment process makes use of threat intelligence to determine which threats are relevant to an organization. It identifies relevant threat types, specific threats and explicit threat actors to include in risk management processes.
- "Use These Five Backup and Recovery Best Practices to Protect Against Ransomware" — Ransomware is on the rise, and its perpetrators are effectively evading countermeasures. Infrastructure and operations and business continuity management leaders should plan for the inevitable limited or widespread ransomware incident.
- "CISO Playbook: Master Wireless Technology Security Risks" — Wireless communications are growing in variety in every company. To prioritize wireless security investment, CISOs should consider the potential risks and develop mitigating best practices, including restricting enterprise wireless communications by limiting accessible networks and services.

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.

- "Managing Risk and Security at the Speed of Digital Business" — Digital business challenges the basic principles of information risk and security management. Risk and security leaders must understand the risks associated with business unit innovation, and balance the imperative to protect the enterprise with the need to adopt innovative technology approaches.
- "The Four Steps to Manage Risk and Security in Bimodal IT" — CISOs and risk management leaders must re-evaluate and develop the capabilities of their teams to ensure that they maintain appropriate security when engaging in more-agile development approaches as part of a digital transformation.
- "Master Bimodal IAM Capabilities to Build Digital Business Success" — Organizations preparing for digitalization need IAM leaders to provide a different set of basic services and capabilities, or look elsewhere. IAM leaders must assist and empower bimodal approaches by focusing on efforts to enable software developers through new APIs and agile methodologies.

- "Maverick* Research: Your Smart Machine Has Been Conned! Now What?" — Smart machines and artificial intelligence (AI) pose huge future risks that derive from malicious humans using or abusing them to achieve their goals. Here, we focus on identifying and managing those risks.
- "Unsanctioned Business Unit IT Cloud Adoption Will Increase Financial Liabilities" — As various business units move toward using data for revenue growth, the unsanctioned adoption of cloud services (SaaS and business process as a service [BPaaS]) is increasing the risks of data breaches and financial liabilities. CIOs and CISOs can use this research to manage these risks.
- "Good Citizen IT App Development Security Depends on Good IT Citizenship" — Individuals everywhere in your company can write their own programs with minimal programming knowledge, thanks to easy-to-use and powerful tools. IT security teams must embrace and add value to user-led business processes.
- "Six Paths to Operational Resilience for Digital Business"— Technology-only responses to service disruptions do not provide adequate resilience and can lead to further failure. A healthcare digital business example shows how CIOs and digital risk officers must reach beyond technology to involve all stakeholders in operational resilience planning.
- "How to Make Cloud IaaS Workloads More Secure Than Your Own Data Center" — The automation and programmatic infrastructure of leading infrastructure as a service (IaaS) providers enables enterprises to significantly improve the security protection of public cloud workloads to the extent that, when best practices are followed, they can be more secure than those in traditional data centers.

Cybersecurity at the New Edge

It was once 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 operational technology, the 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.

- "Clouds Are Secure: Are You Using Them Securely?" — CIOs and CISOs need to stop obsessing over unsubstantiated cloud security worries; instead, they need to apply their imaginations and energy to developing new approaches to cloud control. This will enable them to securely, compliantly and reliably leverage the benefits of this increasingly ubiquitous computing model.
- "Securing the Internet of Things" — The IoT creates a pervasive digital presence connecting organizations and society as a whole. New actors include data scientists, external integrators and exposed endpoints. Security decision makers must embrace the fundamental principles of risk and resilience to drive change.
- "How the Internet of Things Will Impact Cybersecurity" — The impact of the IoT will result in a pervasive digital presence that changes both business and the social fabric. Marketing managers must plan for opportunities that scale, with the diversity and function of IoT devices demanding expanded protection and control requirements, due to legal imperatives.

- "Market Guide for Operational Technology Security" — This research provides a definition of the OT security market, its market dynamics and a view of OT market participants. The OT security market is now mature enough to begin evaluating and ranking vendors, as client interest and impact demand coverage.
- "Mind the SaaS Security Gaps" — Although enterprises have focused on the adoption of SaaS applications, they have often ignored the security governance principles that would normally be applied on-premises.
- "Understanding and Implementing Security in Office 365: Exchange Online, SharePoint Online and OneDrive for Business" — Organizations about to implement Office 365 have concerns about the product's security. This research gives an overview of Office 365 security capabilities for email and collaboration, and their effectiveness. This will help to select the appropriate mix of Microsoft and third-party controls.
- "Roundup of Cloud Application Security and Governance Research" — Gartner's research on cloud computing governance examines how CIOs and their leadership teams can take full advantage of the public cloud, while avoiding regulatory compliance and security complications.
- "Innovation Insight for Trusted Execution Environments on Mobile Devices" — Enterprises can now leverage hardware-based Trusted Execution Environments (TEEs) to secure workforce and consumer apps running on Android devices, but adoption is limited. We present key concepts and illustrate when and how security leaders and digital channel leaders should implement TEE-enabled apps.
- "Address Cybersecurity in Assets You Don't Control or Own" — In the world of digital business, every enterprise is a link in a global chain. Data flows through and is with third parties outside the organization's ownership and beyond its control, requiring enterprise risk and security teams to alter their cybersecurity strategies.

People and Process: Cultural Change

It has been a platitude for years that cybersecurity requires people, process and technology; however, 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 and 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.

- "Connect People-Centric Security to the Digital Humanist Manifesto by Starting and Ending With People" — Digital humanism is a system design philosophy centered on human interests and values. It is ostensibly at odds with conventional security principles that treat humans as the weakest link. Digital risk officers, technology strategists and CISOs must treat people-centric security as an integral part of digital humanism.

- "Connect People-Centric Security to the Digital Humanist Manifesto by Embracing Serendipity" — The essence of the digital humanist principle of embracing serendipity is to enable users to change the ways their systems and applications are used. Security policies that damage the innovative, adaptive use of systems can't be established.
- "Identity and Access Management Scenario 2020: Powering Digital Business" — Digital business is driving major changes to enterprise IT. Business transparency, openness and IoT's enablement at the organization's edge affect IAM markets and the ways that IAM leaders manage their programs.
- "Three Ways to Support CRM While Ensuring Customer Data Privacy" — The consequences of mismanaged customer data privacy include litigation and diminished company reputations. Application leaders supporting CRM must ensure customer data privacy to make customers feel confident enough to provide accurate data, which will improve data quality and reduce the likelihood of abnormal customer churn.
- "Kick-Start the Conversation on Digital Ethics, 2016" — Every business and IT leader should prioritize digital ethics. The unintended ethical consequences of digital business are a challenge to every industry, and guidelines on how to avoid these consequences are emerging.
- "Transform Your Security Team to Deal with Digital Business Risk" — Security organizations cannot remain static in an age of digital change. Organizations must build adaptive and resilient digital security practices to address new demands from digital business.
- "Staying Secure in the Cloud Is a Shared Responsibility" — Although public cloud providers typically have strong control attestations, numerous compliance certifications and their own security features, CSPs cannot offer complete security. CISOs and security leaders must understand the scope of their responsibilities for security in the cloud.

Evidence

[1] "Cybersecurity as a Growth Advantage." Cisco.

"M-Trends 2015: A View From the Front Lines." Mandiant, A FireEye Company.

"Understand What You're Up Against." Verizon.

Note Additional Resources

Analyst Webinar: "Special Report: Cybersecurity Is a Foundation for Digital Business"

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