New Infrastructure, New Risks:
Managing Threats, Compliance and Fraud in an Era of Digital Transformation

In this issue

Managing Security, Compliance and Fraud Risks with Proofpoint
Research from Gartner: Managing Risk and Security at the Speed of Digital Business
The digital transformation is changing the way we work, collaborate and create. It’s changing our businesses processes, supply chains, our relationships with vendors, partners, and even competitors. And it’s changing the way we attract, nurture, and engage customers.

The back office is moving to software-as-a-service (SaaS) apps. Infrastructure is moving to the cloud. Endpoints are going mobile. And customer engagement is moving to new digital channels.

More than ever, your success hinges on your ability to transform your business. You need to be more efficient, agile, and responsive to customers. That’s why organizations are moving to infrastructure and channels that they don’t actively manage, own, or in some cases, even control.

**TRANSFORMING THE THREAT LANDSCAPE**

These flexible platforms mean new security, compliance and fraud risks. That’s because you own less and less of the infrastructure you rely on to keep workers productive, the business running, and customers engaged.

**Security risks**

Today’s attacks target people, not just technical flaws. That means even the best-secured cloud and SaaS apps are vulnerable to threats that target the weakest link in today’s mixed environments: the human factor.
Most data breaches start with an email. And most email attacks rely on a person to activate it, either by opening a boobytrapped attachment or clicking a link to malicious code. Email fraud, meanwhile, get through otherwise well-protected email systems because they rely on social engineering, not malware or malicious URLs.

And many of today’s attacks play out over multiple channels. They take advantage of businesses’ trusted connections with partners, vendors and customers.

**Compliance risks**

Keeping up with ever-evolving compliance rules was never easy. The digital transformation is only complicating the challenge.

Modern infrastructure is more complex and fragmented than ever, leaving potential compliance gaps. Regulated data may sit on dozens of different cloud and SaaS platforms, all with different discovery, protection, archiving and retention capabilities. And social media is often an afterthought in compliance programs.

**Fraud risks**

The internet’s open framework makes it fertile ground for fraudsters looking to cash in on your brand and the people who trust it. In digital channels you don’t control, anyone can create a domain, website, mobile app or social-media account that impersonates your company or brand.

Cyber criminals quietly spoofing your domain outside of your email gateway can hurt your reputation—and bottom line. Social media, too, is rife with impostors. These include fake accounts run by counterfeiter or attackers looking to steal customer credentials. Lookalike websites have become a growing problem for major brands as they try to engage customers online. And counterfeit apps can use your brand to spread malware, steal credentials or spam users with pop-up ads.

**TRANSFORMING YOUR SECURITY POSTURE**

In today’s digital economy, securing these platforms, infrastructure, devices and digital channels—which exist well beyond your internal network—is critical.

A modern security solution must offer broad, coordinated omnichannel protection against today’s most advanced threats. That means preventing, detecting, and stopping threats that exploit not just technical flaws, but human nature. The solution should work everywhere your organization does—email (where most threats still begin), the web, SaaS, social media, and mobile.

Your compliance solution must give you visibility and control over your data on and off premises. It should capture communications on the collaboration platforms your people use. It should empower workers by taking the guesswork out of compliance, free them up to do what they do best.

---

To protect your brand and the people who count on it, you need to find and stop fraudsters using email, social media, the web and mobile app stores to impersonate you.

Your solution should also bring all of these capabilities together, integrating threat intelligence from email, social, mobile, and network activity. In most cases, that means integrating into a larger ecosystem of threat detection and intel for complete, cohesive security, compliance and fraud prevention.

**How Proofpoint can help**

Proofpoint has appeared in Gartner’s Magic Quadrant for seven years running. We help you embrace Gartner’s six principles of trust and resilience (page 10 of this report) with blend of technology, threat intelligence, and dedication to your success.

Built on advanced intelligence and a cloud architecture, our security, compliance, and fraud platform enables today’s digital transformation. We help you secure the digital channels you rely on: email, the web, SaaS, social media, and mobile apps.

By closely checking and safeguarding these channels, we help stop attacks before they reach their targets. We detect and help you resolve hidden compliance issues. And we stop anyone trying to hijack your brand to defraud your customers or tarnish your reputation.

**Security**

We protect against advanced threats that exploit technical vulnerabilities and human nature to expose, steal, and damage critical data and resources. These include malicious links and attachments sent through email and social media, malicious and risky mobile apps, unauthorized access to your internal and external infrastructure, and social-engineering attacks designed to siphon money, user credentials, and sensitive data. No defense can prevent every attack. When something goes wrong, we give you the tools and insight you need to stop it before it causes lasting harm.

**Compliance**

We help you follow with complex and evolving regulations in industries and jurisdictions around the world. We help you find, manage, supervise, and secure information stored in internal networks and on external infrastructure. We also help you capture and retain communications across a wide range of internal and external platforms, including enterprise collaboration tools and SaaS platforms.

**Fraud prevention**

We protect brands and the people who trust them from impostors on email, the web, social media, and mobile apps. We stop domain spoofing, social media
account takeovers, fraudulent social media accounts, phony websites and counterfeit apps that tarnish your brand and put your customers at risk.

**Secure your digital transformation**

You shouldn't have to choose between enabling digital transformation and protecting your organization against the new security, compliance, and fraud risks it creates.

We give you complete visibility across all major threat vectors. That means you detect security, compliance, and fraud risks before they evolve into major threats. You stop threats before they cause lasting harm. And you get the insight you need to prevent and resolve future risks as they emerge.

We help protect you from these risks across email, the web, social media, mobile apps, and SaaS platforms.

With Proofpoint, you stop security threats before they reach their targets. You stay compliant with ever-evolving regulations. And you prevent fraud that hurts your brand and the people who trust it.

To learn more about how we can help secure your digital transformation, visit www.proofpoint.com.

*Source: Proofpoint*
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.

**Foundational Document**
This research is reviewed periodically for accuracy. Last reviewed on 14 August 2017.

**Key Challenges**
- Increasing adoption of digital business strategies is challenging conventional approaches to security and risk management.
- Risk and security programs must adapt to this new reality or face being sidelined by the digital business initiatives, ironically exposing the enterprise to even bigger risk.

**Recommendations**
- Develop a compelling vision for risk and security management based on establishing trust and resilience in your digital business.
- Adapt the strategic objectives of your risk and security program to encompass the new realities of digital business.
- Embrace the six principles of trust and resilience.
- Develop and evolve an adaptive, context-aware security architecture.
Implement and manage a formal, process-based risk and security management program to support the digital business.

**Introduction**

The increasing adoption of digital business approaches is changing the traditional IT governance and control landscape. Two key characteristics of digital business are challenging conventional IT control:

- As the business claims increasing autonomy in deploying new digital technologies, it degrades the authority of the central IT organization.

- The dramatic increase in the number of elements (e.g., systems, devices, things, data and dynamic relationships) exposes scalability issues with many traditional security control solutions.

This reality challenges the status quo in information risk and security management. Many conventions and technologies on which risk and security practices have been based do not scale in the new reality. For example, the principle of least privilege is being challenged by new approaches that support business agility. IT risk and information security leaders must assess and transform their programs to become digital business enablers rather than obstacles to innovation.

Gartner has developed a series of foundational research that conveys risk and security practices appropriate for the digital business era (see Figure 1). We will continue

---

**Figure 1. The Foundations of Risk and Security in the Digital Business World**

**Vision:** "Trust and Resilience: The Future of Digital Business Risk"

**Objectives:** "Cybersecurity Scenario 2020 Phase 2: Guardians for Big Change"

**Principles:** "Use Six Principles of Resilience to Address Digital Business Risk and Security"

**Architecture:** "Designing an Adaptive Security Architecture for Protection From Advanced Attacks"
to develop applicable research on this topic (see the Gartner Recommended Reading section).

Analysis

**Develop a Compelling Vision for Risk and Security Management Based on Establishing Trust and Resilience in Your Digital Business**

The starting point for any risk and security program is to develop a compelling vision that the rest of the business can comprehend and that will act as a target state for strategy planning activities. The typical objective of an information security and risk management program is to establish a continuous, iteratively improving regimen of planning, building and running security solutions that are aligned to business requirements. Most organizations will develop an initial vision of such an information security management system (ISMS) from existing standards and frameworks, such as ISO/IEC 27001.

However, it is crucial that the vision is customized by complementing the basic ISMS model through articulating the business, technology and risk drivers that are unique to the enterprise. Within the context of digital business, it is important to acknowledge that the digital business environment comes with unprecedented risks that go beyond IT operations, encompassing the enterprise and its ecosystem.

Hence, the vision for risk and security in the digital business must be based on establishing an ecosystem that enables trust and resilience. The vision must:

- **Make the people, processes and technology more resilient.** The transformation to full-scale digital business extends well beyond the IT organization, impacting the design and staffing of nearly every business function. Its sheer scale underscores the importance of applying resilience to people, processes and technology. It emphasizes the need to focus beyond IT risk to operational risk. As digital business takes hold, digital risk becomes increasingly synonymous with operational risk. More and more enterprise business functions, including IT, are now architected for agility and convenience. In the next decade, the trade-offs between convenience and resilience will be difficult, and significant investment will be required throughout the enterprise.

- **Increase awareness among stakeholders to build trust and resilience.** Technology alone will not protect the individual and the enterprise, whether from their own carelessness or malicious actors. Increased personal awareness and responsibility with respect to safety and propriety must come into play. Enterprises should replace once-a-year training with ongoing awareness campaigns. Given that the lines between personal and business technology are blurring, enterprises should also consider extending protections to employees at home.

- **Support a bimodal IT strategy.** Risk and security specialists must get a seat at the bimodal table and work with business and IT stakeholders to get visibility into Mode 2 projects. While not neglecting the risks inherent in Mode 1 operations, they
must use a risk-based approach that is cognizant of the unique risk appetite associated with Mode 2 initiatives rather than trying to enforce conventional standard controls.

- **Plan for the unprecedented.** Digital business is an unprecedented era. To assume that tomorrow will be just like today, or only slightly different, is a risk in itself. At this early stage, there are precious few best practices for digital business (risk management included), and most of these are only “next” practices. To succeed, enterprises will have to blaze new trails. To be resilient, they will need to go beyond the ordinary, imagining responses to unprecedented but plausible circumstances.

- **Address the need to protect assets that IT no longer owns or controls** (e.g., cloud-based services or new mobile-based applications). In digital businesses, more technology is being procured and operated outside of the visibility or control of the IT department. Decentralized IT spend implicitly puts more control in the business units for deciding how much risk they will accept and how much they will spend to address risk.

The objective is to provide an ecosystem that balances the imperative to protect the enterprise with the need to adopt innovative, risky new technology approaches to remain competitive.

---

**Adapt the Strategic Objectives of Your Risk and Security Program to Encompass the New Realities of Digital Business**

The digital explosion is reshaping organizational security and risk management. The traditional model ascribed to for decades has been based on the objectives of confidentiality, integrity and availability (CIA). However, in the digital business world, the CIA model isn’t enough.

Digital business is pushing the environment for protecting data and infrastructure into the physical world, merging functions focused on data and information with functions that make actual changes to people and their surrounding environments. Protecting information alone isn’t enough, and ensuring the confidentiality, integrity and availability of that information isn’t enough. Leaders in risk and cybersecurity must now assume the responsibility of providing safety for both people and their environments or, at minimum, participate in providing that safety with other security practices (see Figure 2).

As digital business transforms the way in which technology and information are used in the enterprise, it is prudent to investigate the effectiveness of the current risk and security leadership function and organization. In many organizations, the existing risk and security roles are constrained by the limits of their scope, authority and experience. A digital risk officer can potentially provide the authority (and attract the requisite skills) to deal effectively with digital business risks.
Embrace the Six Principles of Trust and Resilience

Digital business is challenging key security conventions such as the principle of least privilege or that prevention is always better than cure. In this dynamic environment, successful risk and security requires adopting a new set of key principles.

Principle No. 1: Stop Focusing on Check-Box Compliance, and Shift to Risk-Based Decision Making

Risk-based thinking is about understanding the major perils a business will face and prioritizing controls and investments in IT risk and security to achieve business outcomes. As technological complexity increases, leaders won’t have enough money to address all threats equally. Risk-based thinking allows cybersecurity investments to be targeted where the greatest risk resides — but risk according to the business itself, not IT’s view of risk. While many organizations believe they have already achieved this transition, Gartner still observes many compliance-driven behaviors.

Principle No. 2: Stop Solely Protecting Infrastructure, and Begin Supporting Business Outcomes

The infrastructure must be protected; however, leaders must elevate the risk and security strategy to protect desired business outcomes. For businesses, this means corporate performance, such as profitability. For government, this means public service delivery and citizen welfare. For the military, this means protecting the mission.

Principle No. 3: Stop Being a Defender, and Become a Facilitator

As part of the transition to supporting a business outcome mindset, IT risk and security leaders must move from being the righteous defenders of the organization to acting as the facilitators of a balance between the need to protect the organization and the need to achieve desired business outcomes. Organizations must continue to invest in legacy technology, traditional cybersecurity and availability operations activities, where they are still appropriate. However, rapid innovation to facilitate digital business requires IT risk and cybersecurity programs to adopt a different approach to developing new controls that is more fluid, agile and adaptable.
Principle No. 4: Stop Trying to Control Information, and Determine How It Flows

IT risk and security leaders must move from trying to control the flow of information to understanding how information flows. This understanding will improve organizational resilience and support the achievement of desired outcomes. Digital business will introduce massive new volumes and types of information, and business processes that must be understood and appropriately protected.

Principle No. 5: Accept the Limits of Technology and Become People-Centric

IT risk and security leaders must understand the limits of security and availability solutions and recognize that properly motivated people can be the strongest links in the chain. It is necessary to shape behavior and motivate people to do the right thing; it’s not enough to just try to force people to do what they are told.

Gartner has pioneered a strategic approach to information security known as “people-centric security”. This emphasizes individual accountability and trust, and it de-emphasizes restrictive, preventive security controls. People-centric security is all about individual trust and accountability.

Principle No. 6: Stop Trying to Perfectly Protect Your Organization, and Invest in Detection and Response

Compromised IT environments are inevitable. IT risk and security leaders must move from a singular focus on trying to prevent compromise to acknowledge that perfect prevention is not achievable. The organization needs to be able to detect a compromised IT environment and react quickly. In the digital world, the pace of change will be too fast to anticipate, and it will be impossible to defend against every type of attack. IT risk and security leaders must invest in technical, procedural and human capabilities to detect when a compromise occurs. They must provide the tools for first responders to react quickly and investigate the source and impact of breaches, compromise and incidents.

Embracing these six principles predicates a willingness to deviate from perceived security conventions and best practices. This requires not just a willingness to change on behalf of incumbent staff, it also impacts the hiring of new risk and security resources. Hiring leaders should not just look for digital business technology skills, but also for people willing to move beyond conventional thinking.

Develop and Evolve an Adaptive, Context-Aware Security Architecture

Most conventional security efforts and products have traditionally focused on blocking and prevention techniques (such as antivirus) as well as on policy-based controls (such as firewalls) to block threats (see the upper-right quadrant of Figure 3). However, perfect prevention is impossible. Advanced targeted attacks are easily bypassing traditional firewalls and signature-based prevention mechanisms. All organizations should now assume that they are in a state of continuous compromise. However, organizations have deluded themselves into believing that 100% prevention is possible, and they have become
overly reliant on blocking-based and signature-based mechanisms for protection. As a result, most enterprises have limited capabilities to detect and respond to breaches when they inevitably occur (see the bottom half of Figure 3), resulting in longer dwell times and increased damage.

To enable a comprehensive, adaptive security protection architecture, we believe that 12 specific capabilities are necessary to augment the ability to block and prevent attacks, as well as detect and respond to attacks (see Figure 3).

**Figure 3. Twelve Critical Capabilities of Gartner’s Adaptive Security Architecture**

Implement and Manage a Formal, Process-Based Risk and Security Management Program to Support the Digital Business

Effective risk and security management requires an integrated approach in which risk and security are made part of the core fabric of business processes and become key components of the organizational culture. This requires infusing the key components of risk and security management (i.e., policies, processes, behavior and technology) across all the dimensions.

Source: Gartner (February 2016)
### Table 1. Elements of a Risk-and-Security Program

<table>
<thead>
<tr>
<th>Component</th>
<th>Purpose</th>
<th>Content/Deliverables</th>
<th>Foundational Gartner Research</th>
</tr>
</thead>
</table>
| **Enterprise Security Charter** | Executive Mandate | - Business Need Scope  
- Accountability Statement  
- Mandate for CISO  
| **Security Program Framework** | Terms of Reference/Reference Model | - Vision Statement  
- ISMS Description Principles  
- Program Components  
- Capabilities/Functions Taxonomy  
“Five Golden Rules for Creating Effective Security Policy” |
| **Annual Strategy Plan** | Plan of Action | - Target State  
- Current State  
- Gap Analysis  
| **Governance Model** | Implementation of Accountability and Decision Rights | - Policy Framework  
- Steering Committees/Bodies  
- Organization Model  
- Executive/Assurance Reporting Framework | “Best Practices for Establishing an Information Security Steering Committee” |
| **Process Model** | Operational/Maturity Improvements; Foundation for Organization Model | - Process Catalog  
- Maturity Model | “The Security Processes You Must Get Right” |

Source: Gartner (February 2016)
of IT — business processes, applications, technology infrastructure and, most importantly, people.

In larger enterprises, this predicates the establishment of a strategic, process-based risk-and-security program. Such a program is a complex ecosystem consisting of multiple elements (see Table 1).

To support digital business initiatives, this program must support a bimodal IT strategy. As Mode 2 projects will require increased agility, existing formalized security programs might need refinements, principally in supporting the plan and budget phases of Mode 2 projects. Organizations without a formalized security program might mistakenly think they can be more flexible, but security for bimodal IT requires more, not less, rigor to effectively balance risks with necessary agility.

To support bimodal initiatives, risk and security leaders must:

- Take steps to prepare security and risk management teams for bimodal IT. Learn about bimodal IT, evaluate where your organization is on the bimodal journey, and identify the primary skills and technology gaps.
- Build additional organizational capabilities to support increased agility and defend against new digital risks.
- Understand the higher-risk appetite represented by Mode 2 projects.
- Adapt security practices to the pace of Mode 2 projects, with laser focus on low interferences during early stages and continuous monitoring of security debt.
- Maximize effectiveness with a bimodal security program. Start before you are ready with small scale, autonomous projects to lead cultural change toward increased agility.

Source: Gartner Research Note ID: G00296694, Refreshed: 14 August 2017 | Published: 24 February 2016, Tom Scholtz