To Stay Relevant, InfoSec Must Strengthen Its Business Partnerships

The role of information security (InfoSec) originated to accommodate the need to protect and secure critical data and information technology assets. Since then, necessity has required InfoSec professionals to expand their scope of focus to include business operations as well. Digital transformation—largely accelerated by 2020's shift to remote work models—has altered the business from a visible set of centrally managed technology assets to a highly distributed, opaque set of digitally enabled processes, products and services.

The *2022 Security Risk Trends* survey conducted by AuditBoard in April and May 2022, found that traditional InfoSec approaches have become fragmented, labor-intensive and largely insulated from the business at large.[1] The survey findings reveal how changes in the business landscape have impacted the InfoSec profession and contributed to gaps in digital risk coverage across enterprises and their growing third-party ecosystems. These results also illuminate how the profession can prioritize limited resources to address relevant business risks and strengthen overall assurance efforts.

> The business areas experiencing the most digital transformation—business operations, finance, people, sales and marketing—are the ones with the least influence on building cybersecurity alignment.

Digital Risk Lurks in the Shadows

Today, data inform and drive areas of technology in an enterprise reaching beyond IT into operational processes, products and services. Robotics have become increasingly standard in manufacturing, while digitization is changing the delivery of healthcare—from telehealth visits to robotics-assisted surgery. Risk manifested by technology (both information technology and operational technology) in business operations is known as "digital risk." New technologies often fall under the category of shadow IT, the use of IT-related hardware or software without the knowledge of the IT or security group within the organization.[2] AuditBoard's 2022 *Security Risk Trends* survey found that more than 70 percent of organizations view shadow IT as a very important or important issue.[3]

Moreover, these digital technologies and risk areas are more difficult to manage from an IT perspective. Nearly 50 percent of survey respondents were relying on surveillance and monitoring software to manage shadow IT.[4] However, by definition, shadow IT lies outside the physical or digital domain of centralized IT. Therefore, digital risk fueled by shadow IT cannot be effectively monitored via surveillance software, which, ultimately, provides only a false sense of security.

The Role of Third Parties and Business Operations in Digital Risk

As organizations increasingly rely on outsourced or offshore digital products and services, the IT function may find itself ill-prepared to support the rapid innovation of third-party technology. InfoSec functions have struggled to adapt to the changing needs of the increasingly digitized business. Seventy-two percent of survey respondents felt their organization was not very well aligned on their largest cybersecurity risk areas and how to best manage them.[5]

The influx of both internal and external technology assets, such as hybrid cloud services, requires InfoSec professionals to link security impacts across an array of business processes. Yet the AuditBoard survey reveals the business areas experiencing the most digital transformation—business operations, finance, people, sales and marketing—have the least influence on building cybersecurity alignment,

JOHN WHEELER

Is senior advisor for risk and technology at AuditBoard and a former Gartner integrated risk management (IRM) analyst.

LOOKING FOR MORE?

- Read *State of Cybersecurity 2022. https://www.isaca.org/go/state-of-cybersecurity-2022*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

a significant area of digital risk impact[6] (**figure 1**). Without clear alignment on cybersecurity risk across the organization, InfoSec professionals simply do not have the ability to adequately manage digital risk.

Moreover, InfoSec teams spend the majority of their time coordinating activities with centralized corporate functions (IT, internal audit, and GRC) to promote a culture of information security. However, because digital risk emanates from the business itself, it is necessary for InfoSec to shift its primary focus from coordinating with similar functions to collaborating closely with its business partners.

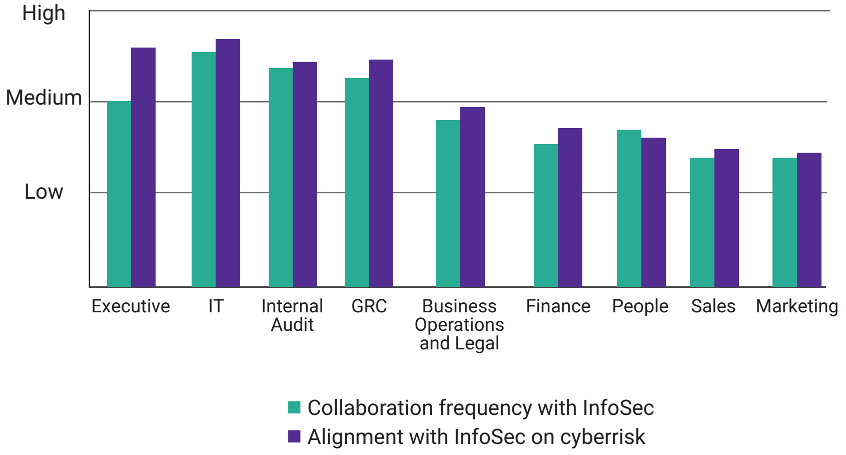
Three Imperatives for InfoSec Improvement in the Digital Era

The key to risk management success is to assign risk accountability to the ultimate risk owners. With this in mind, InfoSec professionals must tackle three imperatives to define relevant digital risk accountability with their business partners:

1. **Foster more communication and collaboration with business partners**. Because InfoSec has very little direct control over how digital risk is mitigated, a true partnership with the business is necessary to help business groups understand and own their risk on a day-to-day basis. The goal is to understand the business partners' purpose and what they are looking to achieve regarding the given digital product, service and markets. Also, rather than pushing the InfoSec agenda on the business, the InfoSec function should ask what it can do to make their business partners' lives easier. This can dismantle boundaries and improve efforts to increase digital risk accountability and ownership.
2. **Devote more time to strategic relationship-building activities to involve business partners in actively managing their digital risk**. It is beneficial for the team to understand how the business is changing and how IT is contributing to digital transformation. One relationship-building activity is to engage in business planning and design new digital products and services. By doing this on a regular or frequent basis, InfoSec positions itself as a proactive partner helping to weave security controls into the build, rather than retroactively applying controls.
3. **Leverage technology to enhance coordination with related enterprise functions and business partners**. Integrated risk management (IRM) technology can help InfoSec present security information in a business context, which helps foster understanding and collaboration with business partners. An IRM solution helps InfoSec teams communicate security impacts to business stakeholders and seek decisions on risk mitigation from them. This shifts risk accountability and ownership to the business and allows for a more targeted response. In addition, an IRM solution can aggregate security threats, vulnerabilities and incidents, which helps InfoSec link the overall security impact on technology assets to business processes and desired outcomes, improving overall reporting capabilities.

FIGURE 1

Other Departments' Influence on Building Cybersecurity Alignment



Using Digital Risk Management as a Competitive Edge

As organizations prioritize digitization, InfoSec professionals must keep pace with changes to the business. To effectively manage digital risk, InfoSec professionals and business leaders must work in tandem to increase their mutual risk understanding and mitigation efforts. Together, with the use of enabling IRM technology solutions, organizations can streamline digital risk management to gain a true competitive edge.

Endnotes

[1] AuditBoard, *2022 Security Risk Trends*, USA, 2022, *https://www.auditboard.com/resources/ebook/2022-security-risk-trends-infosec-must-transform-to-keep-pace-with-digital-business/*

[2] Cisco, "What Is Shadow IT?" *https://www.cisco.com/c/en/us/products/security/what-is-shadow-it.html*

[3] *Op cit* AuditBoard

[4] *Ibid.*

[5] *Ibid.*

[6] *Ibid.*