KPMG

The role of internal audit in cyber security readiness

kpmg.com

Which of the following risks poses the greatest threat to your organization?

The rise in cyber risk to organizations

With the growing number of high profile cyber-attacks and data breaches, organizations across all industries have elevated cyber security to be a top priority in their business objectives. The costs associated with a data breach or cyber-attack have become so significant that organizations are focusing serious attention on how to protect their assets, especially industries and organizations that deal with sensitive data, such as personal identifiable information, bank or cardholder data, company financials, intellectual property, or material non-public information.

The serious risks involved have put organizations on alert, but many organizations do not feel prepared. According to the 2018 Harvey Nash/KPMG CIO Survey, only 22 percent of IT leaders feel that they are "very well-prepared" to defend a cyber-attack. However, 68 percent of IT leaders feel they have the support necessary from their board of directors to achieve their cybersecurity goals. So with growing support from organizational executive leadership, how do organizations and their internal audit functions bridge the gap in cyber security readiness?

At KPMG, we are here to help provide clarity on combating cyber security. Let's start by understanding data breaches. A data breach is generally defined as an event in which sensitive or confidential data is copied, viewed, stolen, or used by an individual or entity unauthorized to do so. Activities contributing to data breaches or other forms of Cybercrime include but are not limited to, human error, political or criminal intent, emerging technologies, or business change, to name a few.

The bad "actors" of yesterday have evolved from isolated criminals or "script kiddies" targeting identity theft, self-promotion opportunities, or theft of services to today's organized criminals, national states, hacktivists, or insiders targeting intellectual property, financial information, or strategic access to key resources. The methods used to exploit systems include, but are not limited to, phishing attacks, ransomware, denial-of-services attacks commonly due to poor system or process-level controls, unauthorized third-party software or poor security controls at third parties, or mobile devices, to name a few.

According to the 2017 Cost of Data Breach Study: Global Overview performed by Ponemon Institute and sponsored by IBM and The *New York Times*, cybercrime is one of the world's fastest-growing and most lucrative industries. 28 percent of most organizations will experience a material data breach in the next 24 months. The more records lost, the higher the cost of the data breach. The average cost incurred for each lost or stolen record was approximately $141 with costs exceeding $243 million in one instance of a larger-scale data breach. Compliance failures and the extensive use of mobile platforms were cited as new factors in the cost analysis for data breaches.

"68 percent of CEOs believe that a cyberattack is a matter of when and not if. 92 percent feel prepared in terms of their ability to identify new cyber threats, but only 41 percent consider themselves very well prepared."

As cyber-attacks become more sophisticated, board oversight of an organization's cyber response plan is no longer leading practice—it has become a requirement. So where do organizations begin and move from reacting to anticipating cyber-attacks?

KPMG

Cyber risk factors for internal audit to consider

Many organizations believe they are adequately protected on the basis of performing periodic penetration testing or having best-in-class technical tools. However, in reality, the boundaries of involvement to combat cyber criminals and minimize the risk of data breaches are widening to include broad operational processes and areas such as those mentioned below.

Emerging threats

The cyber threat landscape is continuously changing and evolving. Most cyber defense organizations within a company attempt to address and mitigate the emerging threat environment through a combination of controls and techniques. For example, organizations rely on subscription-based threat intelligence providers to provide real-time updates on new and emerging threats that are prevalent at any given time. In addition, organizations may perform their own reconnaissance by researching and accessing known social media discussion portals and searching for relevant items on the dark web. This intelligence is then actioned into remediation plans and preventative controls.

In one example case, an organization was made aware of an imminent denial of service attack unless certain ransom conditions were met. The organization immediately responded with additional controls around their denial of service mitigation approach as well as with increased monitoring of potentially affected systems.

Additionally, the SEC recently released an investigative report to make organizations aware that cyber-related threats of fraudulent electronic communications exist and should be considered in the system of internal controls. The SEC investigated nine organizations that were victims of such fraudulent communication schemes, which resulted in nearly $100 million worth of unrecovered losses.

Internal audit should assess the organization's overall strategy for dealing with emerging threats from a governance, architectural, operational, and technology perspective. Leading practice organizations will have a well-defined approach for dealing with the emerging threat environment.

Technology change

The current pace of change impacting organizations today with respect to technology innovation is increasing. Organizations, after many years, are increasing their spending on new technology to enable their businesses at an increased pace. The adoption of cloud, the increase in demand for intelligent automation, robotics, and the rise of the Internet of Things (IOT) have added new and more complex security risks to the business environment.

Internal audit will be challenged with assessing the cyber risks of these new and emerging technology areas. It will be important to assess current business risk associated with these new or emerging technologies in terms of their impact on existing business. In addition, having a line of sight into new initiatives that might introduce risk into the organization as a result of emerging technologies should be considered. Has the organization embraced security-by-design principles, and is the security organization undertaking design or technology reviews prior to final adoption and implementation of the technology?

Business change

Business change is impacted by technology change; regulatory environment changes; new business models; and the impact of mergers, acquisitions (M&A), or divestitures. Internal audit functions have traditionally been proactive in addressing business risk associated with these changes. However, until recently, the consideration of cyber risk and its associated impact has not always been considered at the depth and breadth that it should be.

Key cyber risks for consideration should include such items as addressing the threat environment of the business and M&A cyber risk for the acquiring entity. For example, if an organization is in acquisition mode, cyber risk assessment and impact of known data breaches should be part of the broader due diligence assessment.

Regulatory change

In every industry, the changing regulatory landscape has an impact on the organization. The recent General Data Protection Regulation (GDPR) legislation and other data security and privacy laws have placed additional controls requirements on organizations. Some organizations have not been as prepared to address these new regulatory requirements and, as such, have opened themselves up to the possibility of regulatory sanctions or fines.

In the financial sector, the European Banking Authority (EBA) recently published Guidelines on major incident reporting under PSD2, Guidelines on the security measures for operational and security risks of payment services under PSD2, and Guidelines on outsourcing arrangements, and is about to publish Guidelines on ICT and security risk management. Furthermore, the European Central Bank (ECB) recently reaffirmed that it will continue to push for and request banks' resilience to and preparedness for cyber threats.

In other sectors, the Directive on security of network and information systems (NIS Directive) –transposed in Luxembourg law in May 2019 – establishes security and incident notification requirements for Operators of Essential Services (OES) in critical sectors such as energy, transport, health sector, drinking water supply, and digital infrastructure; and for Digital Service Providers (DSPs), including online market places, search engines and cloud services.

Internal audit can play a key role in assessing the impact of new or existing regulations, as well as assessing the readiness of their organization in dealing with the new regulation.

Third-party risk

Most organizations have an increasingly complex supply chain and have increased their reliance on third party vendors to provide goods and services to their organization. This increased reliance has increased cyber risk by allowing third parties to access their systems directly or through processing of their private or confidential information or those of their customers. All industries should have a solid handle on the nature of information being handled by the third party, how the information is transmitted, and how the information is stored and processed by the third party. In many instances, a fourth party may be involved (i.e. outsourcing "chains" where a service provider outsources part of its outsourced activities to other service providers). Internal audit can perform assessments of their overall third party programs as well as perform detailed assessments of high-risk vendors.

Internal audit's involvement in cyber security readiness

Every company is unique as are the threats that it faces. Accordingly, every cyber response strategy will be different. However, for internal audit functions, there are some common areas of focus for cyber that should be considered when scoping audit work in this area. For example:

1. Business goals and strategies

- Understand business environment, goals, stakeholders, and regulatory expectations
- Link cyber audit objectives to IT and enterprise goals
- Understand previous cyber deficiencies and management action plans
- Review prior audit plan coverage

2. Framework alignment

- Define cyber leading practices and industry frameworks
- Tailor frameworks to your organization's environment
- Align cyber audit plan to framework (e.g., ISO, NIST Cybersecurity Framework)

3. Emerging risks and threats

- Understand technologies adopted by the organization
- Understand the threats and vulnerabilities introduced by technology
- Address emerging risks in digital, cyber, automation, and cloud adoption, etc.
- Prioritize risk areas to establish the cyber audit focus areas

4. Talent and staffing

- Develop audit plan to identify talent requirements and skill sets to support cyber audits
- Define sourcing model to achieve cyber audit quality, performance, and value
- Recalibrate audit plan in response to evolving risk landscape, business priorities, and technology adoption

A thorough top-down understanding of the organization, its objectives, its risks, and its processes is needed to be able to fully address the cyber security challenges an organization may now face. Internal audit must be a student of its organization but must possess robust technical knowledge as well to marry the organizational goals with the execution of its processes.

Areas of focus for internal audit

Choosing the right approach to assess your cyber security program can be challenging, especially since skilled cyber talent remains a challenge for many audit functions.

KPMG can work with you to identify your gaps; help augment your existing workforce with the right skills, behaviors, and competencies; and help determine a path forward to remediate gaps and demonstrate both corporate and operational compliance with your regulators, investors, and the members of the board.

How mature is your cyber security program?

KPMG's Cyber Maturity Assessment (CMA) provides an in-depth review of an organization's ability to protect its information assets and its preparedness against cyber-attacks. The advantage of such a review is to provide the board and management with an independent view of holistic security risk to the organization and how well the organization's overall security program has matured to meet that risk. Several industry frameworks such as ISO 27001/02 or the NIST cyber security framework can be used as the basis for assessment, along with KPMG's benchmarking models by industry. Such assessments provide an effective framework for internal audit to consider follow-up deep dives into areas of higher risk.

KPMG's CMA is distinct in the market in that it looks beyond pure technical preparedness against cyber-attack. It takes a rounded view of people, process, and technology to enable clients to understand areas of vulnerability and identify and prioritize areas for remediation, turning information risk to business advantage. Many of KPMG's clients' Internal Audit functions have engaged KPMG to perform the CMA as a first step in their annual cyber audit program.

Through a combination of interviews, workshops, policy and process reviews, and technical testing, KPMG's CMA rapidly:

- Identifies current gaps in compliance and risk management of information assets
- Assesses the scale of cyber vulnerabilities
- Sets out prioritized areas for a management action plan.

The assessment provides the flexibility to assess the level of cyber maturity on a site-by-site basis or at a company level. It helps to identify leading practices within an organization and provides comparator information against peer groups and competitors.

In short, it provides executives with a rapid assessment of their organization's readiness to prevent, detect, contain, and respond to threats to information assets.

How can internal audit evaluate cyber security risks?

Internal audit functions can execute a variety of technical and process driven assessments to help cyber security risks are identified, assessed, and mitigated. The following table provides a selection of such audits, as well as example scope items to be considered:

Technical assessments

Operations and technology	Vulnerability scanning and penetration testing
	Network logging and monitoring/threat assessment
	Device configuration reviews (infrastructure devices, firewalls, routers, etc.)
	Wi-Fi – Scanning for unauthorized Wi-Fi/ and Wi-Fi configurations and vulnerability/ exploitation testing
	Remote access/VPN points – Technical assessment of the remote access points and configuration to help ensure they are protected
	Application/database assessment – e.g., vulnerability scanning, penetration testing, and DB configuration reviews
	Security by design
	Architecture reviews and analysis
	Operating system/database security configuration
	Patching process/remediation procedures
	Code reviews

Process and controls assessments

Operations and technology	Identity and access management: — Centralization versus decentralization — Single sign-on — Identify access management procedures — Remote access management and authentication — Privileged access management
	Physical and personnel security: — Logical and physical access controls — Security awareness training—commonly referred to as social engineering
	Mobile device security
	Security operations assessments
Information risk management	Vendor risk management and security
	Cyber threat analysis and risk management process: — Threat identification, assessment, and update process — Including integration with change management and software development lifecycle
	Cloud computer security and ongoing assessment
	Data classification, protection, and encryption Enterprise-wide training and awareness programs
Human factors	IT talent management and training
Leadership and governance	Cyber governance, roles, and responsibilities
	Cyber and enterprise risk management integration
Legal and compliance	Regulatory considerations and integration into cyber framework
Business continuity and crisis management	Security incident response and communication: — Crisis communication plan — Team roles and responsibilities — Notification procedures (legal, regulatory, etc.) — Shutdown process — Maintain controls during an incident — Investigation — Training and awareness
	Integration with security
	Disaster recovery/resilience
	Business impact assessment process
	Testing strategy

How we can help your internal audit team

As noted above, cybercrime is one of the fastest growing risks, and audit committees and executives are rushing to understand their company's position as it relates to cyber risk management. KPMG has a dedicated team who can work with internal audit to help challenge their thinking or provide an on-demand agile workforce with deep industry knowledge to successfully deliver technical, process, or control assessments.

Contact us

Anne-Sophie Minaldo
Partner
T: +352 22 51 51 7909
E: anne-sophie.minaldo@kpmg.lu

Laurent de la Vaissière
Associate Partner
T: +352 22 51 51 6038
E: laurent.delavaissiere@kpmg.lu

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia