Thought Leadership INSIGHT CREATES VALUE
Leadership éclairé LA PERSPICACITÉ CONFÈRE DE LA VALEUR.

Effective Risk Mitigation: Internal Audit and Cyber Security & Privacy: Guidelines and a Checklist

May 2020

By Danny Timmins *CISSP*

The Institute of Internal Auditors
L'Institut des auditeurs internes
Canada

Effective Risk Mitigation
Internal Audit and Cyber Security & Privacy: Guidelines and a Checklist

Danny Timmins *CISSP*
May 2020

The areas of risk identification and mitigation have exploded for organizations since the turn of the new millennium. With data becoming an organization's most valuable asset, it has also become its most vulnerable. Cybercriminals are continually targeting potential weaknesses in your security stance. Cyber-attacks can culminate in an organization suffering costly or irreparable operational, financial and reputational damage.

As organizations move to digital to capitalize on new technologies and innovations to deliver business results, they also need to ensure that they build and maintain customer trust. Data privacy, financial impacts of cyber breaches, director and officer liability, are increasingly important areas stakeholders and regulators demand transparency on. Your audit committee should be up to date on when breaches have occurred, what's trending, how they are being addressed and what management is doing about ineffective controls.

An integrated risk-based approach, driven by internal audit and applied to governance, risk management and internal controls, delivers efficiency by supporting informed decision making and effective resource allocation. It helps to ensure the organization is focusing its assurance and audit efforts on either key risk exposures or key controls/mitigation strategies. Benefits include a clear view of vulnerabilities, opportunities and value drivers.

Just recently, we saw a large consumer financial information business suffer a major data breach, which impacted over 143 million people and resulted in both its CEO and CISO resigning. Pending results of ongoing investigations, there could be legal, legislative, financial and operational implications for financial institutions and other organizations alike. It is becoming extremely apparent risk management professionals, and internal auditors will need to help face the challenge of managing cyber risks.

Increasingly, organizations are recognizing the need for an independent review of security measures and performances.

"Internal audit is one of the few voices that is purposely positioned to go across the entire organization, and it is able to look at how the different parts work with each other and make sure the right information is getting to the right people."[1]

Internal audit activity can provide senior management with independent and objective assurance on governance, risk management and controls pertaining to cybersecurity. This includes assessing the overall effectiveness of the activities performed by the first and second lines of defence (management and information security, respectively) in managing and mitigating cybersecurity risks.

Focus areas for internal audit should include the relationship between cybersecurity, privacy and operational risk, prioritizing responses and control activities and performing audits for cybersecurity & privacy risk mitigation across the organization.

Are your organization's Cyber Security & Privacy Posture meeting the organization's expectations? Here are six principles Internal Auditors should live by.

Setting the Tone: Six Principles to Live By

1. ***Cyber & Privacy Risk is Enterprise Risk***
Technology is now embedded within every business. Incorporate cybersecurity planning and expertise into all enterprise risk planning to understand the likelihood, source and steps to avoid, or reduce the harm of a potential breach.

2. ***Cyber & Privacy Risk Require Expertise Perspective***
Invite cybersecurity experts to join the board and include cyber discussions as a regular agenda topic at board meetings. Create a technology committee where priorities, trends, concerns and emerging controls are discussed and evaluated.

3. ***Cyber & Privacy Risk Management Begins with Policy & Awareness***
Create and promote a culture of cyber incident prevention by emphasizing privacy protection, good technology hygiene and risk awareness throughout the organization.

4. ***Cyber & Privacy Risks Have Legal Implications***
Be aware of any legislative changes and legal cases pertaining to privacy, cybersecurity, reporting guidelines and repercussions of businesses who have experienced a cyber breach.

5. ***Cyber & Privacy Risks and Attacks are Always Evolving***
Focus on the fundamentals and strive for excellence in your cybersecurity maturity program while staying on the lookout for new breach techniques, incidents and risks; especially those occurring within your organization.

6. ***Cyber & Privacy Are Not all Equal***
Know which cyber & privacy risks you want to avoid, need to mitigate, and are willing to accept or transfer through insurance along with your strategy for each.

Setting the Stage: Six Steps to Secure the Business

You need to know which cyber risks you want to avoid, need to mitigate, and are willing to accept or transfer through insurance along with your strategy for each industry or sector.

Here are Six Steps to Secure your Business:

1. ***Establish Effective Policies and Procedures:*** Align your organization against an identified inventory of your applicable security, privacy and data protection laws, regulations, compliance and contractual obligations. Create a comprehensive cyber & privacy best practices for the organization.

2. ***Create (and Test) an Incident Response Plan:*** Ensure everyone understands how to identify a breach, who to communicate with about a known or suspected breach, how to contain the breach and what to do in the aftermath.

3. ***Conduct a Maturity Threat Assessment:*** Periodically, identify & review your inventory of controls (e.g. policies, technology) to determine whether they are suitable and effective for your enterprise risk profile. Best to use a known Cyber Security Framework.

4. ***Review Your Technology Infrastructure:*** Periodically assess your technology framework (e.g. firewalls, anti-malware, software versions) to determine whether they will protect against a breach.

5. ***Penetration Test Your Systems:*** Proactively hunt for vulnerabilities in your technology systems to understand the effectiveness of your cyber controls and the potential damage of a breach.

6. ***Manage Your Third-Party Vendors:*** Understand how any arms-length organizations protect your data, your liability and how they will protect you in the event their systems are breached.

Key Questions Internal Audit Should Ask

The following are key questions which internal audit should try to answer to gain an understanding of an organization's current security & privacy posture, risk appetite and its ability to manage and mitigate any potential cyber threats;

- ✓ Who has access to the organization's most valuable information?
- ✓ Which assets are most likely to be targeted?
- ✓ What is the financial impact of a cyber or privacy breach?
- ✓ For example, which systems would cause the most significant impact to the organization should they be compromised?
- ✓ For example, which data, if stolen, would cause financial or competitive advantage, legal ramifications and / or reputational damage?
- ✓ Is management prepared to react in a timely manner should a cybersecurity incident occur?
- ✓ Is senior management / board aware of risks relating to cybersecurity?
- ✓ Are cybersecurity policies and procedures in place, understood and followed?

- ✓ Has management performed risk assessments to quantify their risk exposure?

Audit committees are being held more accountable for their actions, giving stakeholders confidence the executive suite has oversight of the organization and the committee is actively involved in ensuring internal controls are in place and are operating effectively.

An effective audit committee has members with a broad range of experience pertinent to your organization, who understand the business and aren't afraid to hold executives, management and each other accountable.

GETTING THERE

A successful integrated approach starts with a robust organizational risk assessment. This enables internal audit to focus on areas of highest risk and greatest value to the organization when planning its risk-based internal audit plan.

BENEFITS

The key benefits of an integrated approach, focusing on the areas of highest risk and greatest value of an organization, are ultimately reduced risk, less stress on an organization's limited resources, and a clear view of how assurance is provided through various lines of defence (both internal and external assurance providers) within the organization. In doing so, internal audit furthers its reputation as a trusted advisor of senior management providing the analysis and insights needed to minimize risk, and more effectively deploy resources.

[1] Internal Audit Magazine - www.theiia.org/periodicals

About the Author

Danny Timmins, CISSP, is MNP's National Cyber Security Leader and a member of the firm's Enterprise Risk Services team. Drawing on more than 20 years of experience, Danny is responsible for leading and mentoring an experienced, highly skilled cyber security team in the delivery of customized, client-focused cyber security managed services, product solutions and professional services.

Danny's expertise includes working with executives and boards to assist with the development of prioritized and strategic cyber security strategies. By focusing on deliverables that fit clients' unique business needs and objectives, he helps organizations improve awareness and reduce and manage overall cyber risk.