Journal of Forensic and Investigative Accounting
Volume 14: Issue 3, Special Issue 2022

Cybersecurity and Data Privacy: The Rising Expectations Within Internal Audit

Liahona R. Hepworth
Cindy Greenman
Derrick Esplin
*Ross Johnston**

Introduction

Cybersecurity and data privacy are serious issues in this modern age where most information is now digitally stored data. Security of that data includes protecting it from unauthorized exploitation of the structure, the network, the applications, and the cloud. This can include threats from humans as well as natural disasters. Consequences of breaches in security can result in a poor company image, as well as financial losses for customers and companies. As proven in the SolarWinds and Colonial Pipeline cyber-attacks. Stolen data could also lead to identity theft. Internal auditors are increasingly expected to step up and be more involved in ensuring security measures will effectively protect data. These rising expectations mean that the internal auditors will need to foster relationships with other departments, acquire new skills, and pay particular attention to controls meant to detect risks that make it past preventative controls. They also need to broaden their scope to include the protection of privacy in the business use of social media.

Literature Review

Internal Audit—Traditional Role and Expectations

The internal audit is a critical part of a company. Their central role is to keep the other business functions on track by evaluating their processes and procedures to make sure they are carrying them out both efficiently and effectively and complying with set standards. The Institute of Internal Auditors (IAA) provides the following definition:

> Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes. (The Institute of Internal Auditors, n.d.)

An internal audit function protects the effectiveness of business processes by assessing how well the processes are meeting the objectives of the firm and pointing out where there are inefficiencies that need to be improved. These objectives include operating efficiency, compliance with rules and regulations, and reliable financial reporting. To meet these objectives, companies put in place internal controls designed to meet these objectives. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) has established a widely accepted framework as the standard for the design and operation of internal control systems. Internal controls consist of control activities, risk assessment, information and communication, monitoring, and the control environment (COSO Framework, 2019). The COSO model defines internal control as follows:

> Internal control is a process, effected by an entities board of directors, management, and other personnel, designed to provide reasonable assurance (not absolute assurance) regarding the achievement of objectives relating to operations, reporting, and compliance (COSO Framework, 2019).

The original COSO model, developed in 1992 was a pyramid. In following their mission, the COSO Board instituted new guidelines in what is now referred to as the 2013 COSO Framework. The 2013 COSO model is often represented by a

***** The authors are, respectively, Graduate Student, Associate Professor, Assistant Professor, and Associate Professor at Utah Tech University.

cube with rows, slices, and columns. The rows are the five components on internal control, the slices are the three organizational objectives (operating, reporting, and compliance), and the columns are the entity's organizational structure:

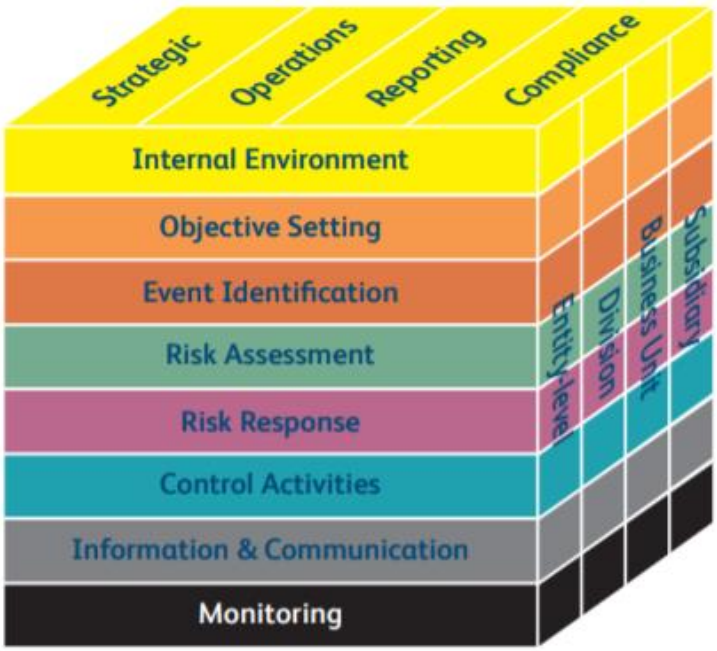
Figure 1: COSO Cube (COSO Framework, 2019)

Audits are performed on the effectiveness of controls at all business levels to see if they are supporting the objectives. Unlike external auditors, who are hired by shareholders and report to stakeholders, internal auditors are employees of the company and give their reports to management.

The definition above mentioned three processes in which internal auditors have a role. These were risk management, control, and governance. Risk management is the process of identifying and responding to business risks. Internal auditors are expected to assess the effectiveness of risk management activities as well as understand the source of the risk and give guidance on how to reduce it (Messier, Glover, & Prawitt, 2018). Controls are procedures put in place to provide reasonable assurance that the organization is achieving its objectives of efficient operations, compliance with laws and regulations, and reports that are useful for stakeholder decision making. Internal auditors review the "adequacy and effectiveness" of controls and provide "consulting and advisory" services to improve controls (COSO Framework, 2019). Essentially, the governance process is everything and everyone involved in governing the organization and meeting business objectives.

The COSO Board commissioned an integrated framework in 2004 that applied more toward an Enterprise Risk Management (ERM) system. The complexity of risk and the ever-changing landscape of risk management enhanced the awareness of the need for an improved approach and guidelines. This supplement was developed from industry practices in efforts to manage risk. This framework is now being used around the world to assist in designing and implementing ERM processes throughout their organizations. The original COSO ERM Cube from 2004 focused on "what can be audited rather than identifying threats and opportunities, which is where the real value in ERM lies" (Williams, 2019).

Figure 2: COSO ERM Cube 2004 (Williams, 2019)



Organizations utilized this model for many years, but soon realized that there was a disparity within the framework. While it assisted in reducing fraud risks and regulatory issues, it lacked the ability to identify and assess those risks the entities needed more controls around. It also focused solely on what can be audited rather than identifying threats and opportunities within the organizations. With this feedback, COSO in partnership with PriceWaterhouseCooper (PWC), updated the framework in 2017 (Williams, 2019).

The structure itself is much different. Rather than a cube to demonstrate the link among the four categories and eight components of risk management, the 2017 framework utilizes a ribbon-type diagram that crisscrosses five categories (Williams, 2019).

Figure 3: COSO ERM Framework 2017 (Williams, 2019)

Cybersecurity

Along with the increase in the use of computers and networks in businesses, there are many new opportunities for fraud against which businesses must learn to defend themselves and their customers. The response to these new digital risks is called cybersecurity, which is defined as the "art of protecting networks, devices, and data from unauthorized access or criminal use …" (Cybersecurity & Infrastructure Security Agency, 2019). Today nearly everything is digital, which brings

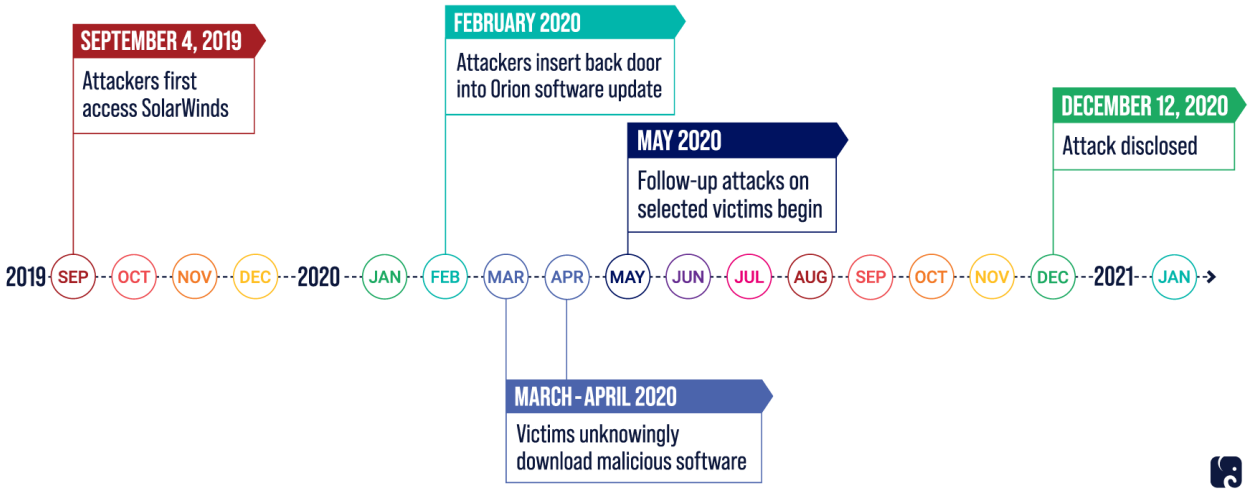
with it many time saving conveniences and efficiencies, but also causes more challenges to secure information since hackers do not have to physically access an entity. Rather, they can hack into an entity's network or database from a remote location. Some examples of cybercrime include theft of data, such as credit card information or social security numbers, ransomware, and viruses that could be destructive to the computer system.

For example, in August 2021 T-Mobile announced that 48 million of their customers were affected by a data breach. The hackers accessed the social security numbers, drivers license ID information as well as phone numbers, addresses and dates of birth. T-Mobile had to file a new, updated 8-K with the Securities and Exchange Commission (SEC) due to the breach and pending lawsuits that may occur (Fletcher, 2021).

FireEye, a cybersecurity consulting firm, uncovered and disclosed in December 2020, what is now called the SolarWinds operation. Hackers inserted malicious code into an update for SolarWinds' popular network management platform, known as Orion. Customers who routinely updated their Orion software unknowingly downloaded the embedded virus into their systems. Once inside, the attackers could choose which areas to access and were able to move through systems and conduct their operations undetected. SolarWinds' current understanding is that the operation began in September 2019, when attackers first breached the system. How the attackers gained access is still unknown. The malware was deployed in February 2020, and customers downloaded the Orion update through March and April. Attackers to move within the targeted systems in May, reading emails and other documents. Their activity remained undetected for the next eight months.

The agencies noted that while there were approximately 18,000 private and public sector victims that downloaded the infected Orion software, "a much smaller number have been compromised by follow-on activity on their systems." Government agencies confirmed to be affected by the attack include at least the Departments of Commerce, Defense, Energy, Homeland Security, Justice, Labor, State, and Treasury, as well as the National Institutes of Health. The economic damage from the operation is likely to be immense. Some experts estimate it may cost as much as $100 billion over many months to root out malicious code and ensure systems are not compromised. From an espionage perspective, the damage is impossible to calculate but is likely to be substantial. Federal agencies and global companies may spend years determining whether they were breached, what information was accessed, and what communications were read. The federal government spends billions of dollars each year on cybersecurity. Yet for months, none of the government's defenses, spread across dozens of federal agencies, detected the intrusion (Senate RPC).

Figure 4: SolarWinds Operation Timeline (WWW.rpc.senate.gove/policy-papers/the-solarwinds-cyberattack)



The Colonial Pipeline was the victim of a ransomware attack in May 2021. The Colonial Pipeline hack is the largest publicly disclosed cyberattack against critical infrastructure in the U.S. The assault began when a hacker group identified as DarkSide accessed the Colonial Pipeline network. The attackers stole 100 gigabytes of data within a two-hour window.

Following the data theft, the attackers infected the Colonial Pipeline IT network with ransomware that affected many computer systems, including billing and accounting.

The attack involved multiple stages against Colonial Pipeline IT systems. Colonial Pipeline was not clear how widespread the intrusion was or how long it would take to restore the compromised systems. This uncertainty prompted CEO Joseph Blount to pay the ransom, hoping it would speed up the recovery time. Fortunately, the pipeline's operational technology systems that actually move oil were not directly compromised during the attack.

Hackers gained entry into the networks of Colonial Pipeline Co. on April 29 through a virtual private network (VPN) account, which allowed employees to remotely access the company's computer network, said Charles Carmakal, senior vice president at cybersecurity firm Mandiant, part of FireEye Inc., in an interview. The account was no longer in use at the time of the attack but could still be used to access Colonial's network, he said. The account's password has since been discovered inside a batch of leaked passwords on the dark web. The VPN account, which has since been deactivated, did not use multifactor authentication, a basic cybersecurity tool, allowing the hackers to breach Colonial's network using just a compromised username and password.

The hack caused Colonial to shut down the entirety of its gasoline pipeline system for the first time in its 57-year history, Blount said. "We had no choice at that point," he said. "It was absolutely the right thing to do. At that time, we had no idea who was attacking us or what their motives were" (Turton and Mehrotra, 2021).

There was significant and immediate effect when the Colonial Pipeline hack occurred. The problem affected the airline industry, where there was a jet fuel shortage for many carriers, including American Airlines. There were also limited disruptions at airports, including Atlanta and Nashville. The uncertainty of a gas shortage caused panic-buying and long lines at gas stations in many states, including Florida, Georgia, Alabama, Virginia, and the Carolinas. Panic-buying did lead to some real shortages in certain areas as consumers bought more gasoline than usual.

Colonial Pipeline paid DarkSide hackers to get the decryption key, enabling the company's IT staff to regain control of its systems. The DarkSide attackers asked for a ransom of 75 bitcoin, which was worth approximately $4.4 million on May 7 (Kerner, 2021). After Colonial Pipeline paid the ransom, the Federal Bureau of Investigation followed the digital money. Over the next 19 days, court records show, a special agent watched on a publicly visible bitcoin ledger as hackers transferred the 75 bitcoins to other digital addresses. A May 27 transfer of nearly 64 bitcoins landed at a virtual address to which the FBI gained access, providing an opportunity to get a warrant and pounce. The Justice Department recovered some of the cryptocurrency, equal to about $2.3 million of Colonial's initial ransom (Uberti, 2021).

Data Privacy

Data privacy is a crucial issue closely related to cybersecurity. Now, more than ever, firms collect enormous amounts of data from their customers, some of which is very sensitive. So much data is collected that there is a term for it: big data. Customers trust these entities to keep their data private and secure, but this is not always the case. Cybercrime make it difficult to protect sensitive data because it is harder to limit access. There are many examples of security breaches. One popular example of this is the data breach at Target in which the information of millions of shoppers was stolen. This information included their credit card numbers which can be used to make unauthorized purchases on customer accounts. Although an extreme example, even smaller data breaches can impact privacy and expose customers and businesses to financial fraud. In addition to the difficulties caused customers, organizations themselves could be faced with lawsuits that could be detrimental, especially to smaller companies.

Confidentiality

Data confidentiality has to do with the secrecy of information. This involves authorizations to view the data, to share the information and to utilize the information. Data confidentiality is protecting information from those who do not have the authority to possess that type of critical materials. The most straight forward and common method of maintaining confidentiality includes data encryption. This provides an effective method to safeguard data confidentiality but also involves its own limitations and weaknesses.

Rising Expectations of Internal Auditors—Cybersecurity

In this age of digitalization and data, companies need to be increasingly vigilant regarding cybercrime threats. Technology is continually changing and with that comes new cyber threats that businesses must enhance their systems

ability to meet. Many firms are realizing that internal auditors need to play a larger role in cybersecurity. In a publication on the role of internal auditors, Deloitte called cybersecurity "an urgent call to action" (Deloitte., 2017). One-way companies are meeting increased cyber threats is by placing more responsibility on the internal audit function when it comes to the detection of risks. Internal auditors are expected to build good working relationships with other functions to audit the effectiveness of the controls and processes more fully within these functions. Of course, to understand these processes, internal auditors need new skill sets that allow them to make recommendations on improvements. Internal auditors must have a better understanding of information security, automation, artificial intelligence, and how all these IT functions integrate into the cyber risk management of their day-to-day operations.

Internal auditors can assist in the control process for cybersecurity by supporting the organization in its efforts to achieve its objectives by adhering to the five components of internal control (control environment, risk assessment, control activities, information and communication, and monitoring). A useful memory aid for the five COSO components of internal control is, "Controls stop CRIME" (COSO Framework, 2019):

C	Control Activities
R	Risk Assessment
I	Information and Communication
M	Monitoring
E	Control Environment

Internal auditors can assist management in evaluating the adequacy and effectiveness of internal controls in response to risks in the entity's oversight, operations, and information systems. For example, internal auditors could help evaluate internal controls in the following ways (COSO Framework, 2019):

1. Achievement of the organization's strategic objectives
2. Reliability and integrity of financial and operational information
3. Effectiveness and efficiency of operations and programs
4. Safeguarding of assets
5. Compliance with laws, regulations, standards, policies, procedures, and contracts

Although management is ultimately responsible for the design and operation of the system of internal controls regarding cybersecurity, a properly running internal audit department can certainly help the organization in achieving its goals and objectives by taking on a consulting and advisory role.

Information security controls are methods used to lessen the risks in information security breaches, data theft, and unauthorized differences to digital information or systems. These controls are meant to assist in protecting the confidentiality, integrity and accessibility of the records and network overall. They are typically put into effect after a risk assessment has been performed. Information security controls consist of preventive controls, detective controls and corrective controls. The preventive controls are typically designed to prevent cyber breach events. Detective controls are meant to detect a cyber breach attempt (unsuccessful) or incident (successful) while it is taking place and to alert the appropriate security personnel. Corrective controls are utilized after a cyber incident to minimize the loss of information and any damage done to the system or network, as well as to restore crucial business processes as quickly as possible (Reciprocity, 2019). These are all controls that internal auditors should familiarize themselves with so that when working with IT they have a better understanding of the overall risk to the organization.

Trust Services Criteria (TSC)

The American Institute of Certified Public Accountants (AICPA) established a task force with the responsibility of ensuring the technical accuracy of the Trust Services Criteria (TSC). TSC include principles that are utilized in attestation

or consulting engagements to assess and report on controls over data and systems. The AICPA identified five areas under the TSC umbrella:

Security: Information and the systems are protected from unapproved use, access, modification, inspection, disruption, disclosure, or anything that could interrupt the system and the entity's ability to conduct their business.

Privacy: information that is collected that can be used to personally identify any stakeholder should be utilized and retained only to meet the organizations goals; disclosed, and then destroyed in the proper manner.

Availability: the information and structures should be available for processes and procedures to attain the organization's goals.

Confidentiality: the material that is designated as confidential is secured to accomplish the organization's goals.

Processing integrity: assuring that the system administration and processing is extensive, thorough, authorized, effective, timely, and acceptable to achieve the entities goals (AICPA, 2022).

Lines of Defense

Companies have three lines of defense that make up their risk management. Each of these three lines has a unique role in the protection of an organization. According to the article "The Future of Cybersecurity in Internal Audit," the three lines of defense for cybersecurity are: (a) information technology, which maintains the entity's hardware, software, and systems, (b) information security, which carries out risk management activities, and (c) the internal audit function, which makes sure risks are being addressed effectively and gives advice on how to improve risk management processes. Jamison (2018) points out that these three lines of defense are no longer clearly defined. With responsibilities beginning to overlap, internal auditors are expected to perform objective assessments of efficiency and effectiveness in areas other than their traditional role. This assessment includes auditing IT or Information security procedures meant to detect risk rather than those meant just to prevent negative events from occurring in the first place.

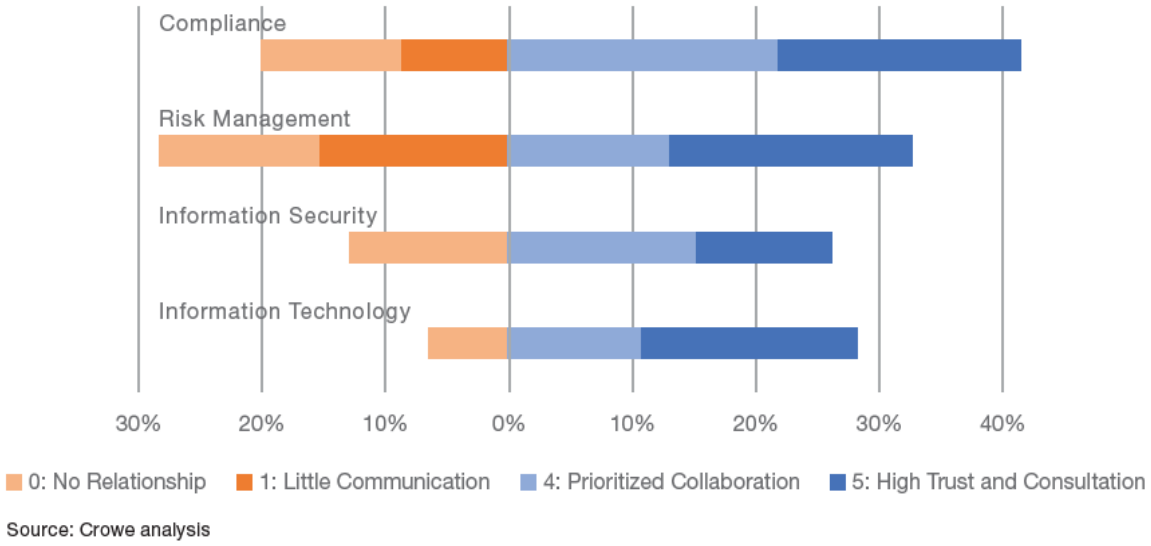
Prevent, Detect, and Correct

Internal auditors have mostly worked diligently to make sure controls are effective enough to stop security breaches from occurring, or in other words, to prevent them. In an external audit, auditors make it clear they can only provide reasonable assurance, not absolute confidence, that control procedures are effective. There comes a point when the costs of doing a more in-depth audit outweigh the benefits. The costs of implementing and following the controls should never be greater than the benefit. Because of this need, internal auditors can only provide 'reasonable assurance' as well to prevention of risks. As it has been explained, "preventing all attacks is simply not feasible" (Jamison, 2018). If a company cannot prevent everything, then they must at least stop it before it can do serious damage. This need for containment leads to the increasing expectations for internal auditors to audit processes and controls meant to detect cybersecurity risks (Jamison, 2018). The internal audit is expected to ensure the efficiency and effectiveness of controls meant not only to prevent cybersecurity risks, but also the processes put in place to detect threats that enter the company. If a cybersecurity event has occurred, corrective actions must take place to repair any damage that has transpired or to restore resources and capabilities as soon as possible.

Relationships with Other Functions

To perform more in-depth audits of detection procedures, internal auditors must work closely with other functions. In a study performed on the effects of a relationship between the internal audit function and the information technology function, it was found that personnel at four organizations agreed a good relationship between these two functions increased the detection of cybersecurity risks. As the article declared, "a better relationship between the information security and internal audit functions increases the detection of incidents both before and after they cause material harm" (Steinbart, Raschke, Gal, & Dilla, 2012, p. 23). In a second article, these authors said a "good relationship" between internal auditors and IT give auditors more access to information they need to make a more in-depth dive into the adequacy of controls and procedures over risk detection (Steinbart, Raschke, Gal , & Dilla, 2018). Any effective relationship requires trust and respect. Such a relationship requires a great deal of trust between the two functions for the internal audit to take a deep dive into the detection processes of information technologies. Internal auditors are expected to foster relationships of trust with other functions to carry out their expanding role.

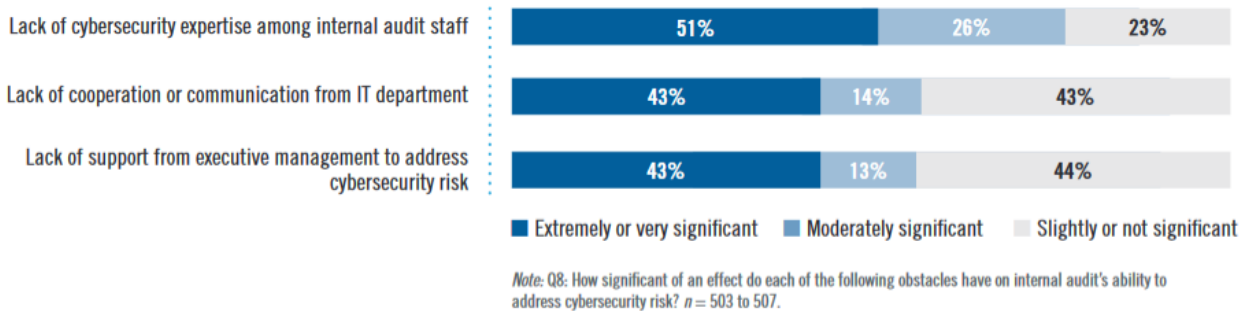
Figure 5: Weak and Strong Relationships with Internal Audit (Jamison, 2018)



According to a survey by Crowe Analytics (Jamison, 2018), most companies report stronger relationships between internal auditors and compliance and risk management than with information security or information technology (see Figure 5). This emphasis on compliance and risk management show how the traditional focus of internal auditors has been on preventative procedures. As internal auditors work to meet the rising expectations regarding cybersecurity, more companies must report relationships of "high trust and consultation" between the internal audit function and both the information security and information technology functions.

The chart below further illustrates the importance of the relationship internal auditors are expected to have with IT. As seen in the chart, one of the main obstacles to an internal auditor's ability to address cybersecurity is a poor relationship with the IT function. The results shown on Figure 5 come from the responses of Certified Association Executives (CAEs). A CAE is a person who has "demonstrated the wide range of knowledge essential to manage an association in today's challenging environment" (The Center for Association Leadership, 2019). Forty-three percent of CAEs agreed that a poor relationship between the internal audit function and IT hindered the internal audit's ability to tackle cybersecurity risks.

Figure 6: Obstacles to Addressing Cybersecurity Risk (The Institute of Internal Auditors , 2019)



Although the articles mentioned address internal audit's relationship with IT, the same principles apply to the internal audit's relationships with other business functions (marketing, shipping, receiving, sales, production, etc.), as well as information security, risk management, and compliance. IT is, however, considered one of the most important relationships that the internal audit must maintain to meet rising expectations.

New Skills

If internal auditors are increasingly expected to give objective guidance on the detection of cybersecurity risks, they must understand how these risks are detected. "Cyber assessments require a deep understanding of the applications, systems, and technologies involved" (Jamison, 2018). Figure 6 shows that more than half of the CAEs felt internal auditors were

impeded in their ability to audit cybersecurity controls and procedures because they did not have the knowledge required to understand the field. This lack of knowledge means internal auditors need to learn about information technology so they must be able to assess whether the systems are detecting risks. Another reason internal auditors need to better understand information technology is to identify what risks are most threatening to the organization. Gaining IT knowledge not only helps auditors understand processes, but also helps to improve relations with other departments throughout the organization. An exploratory research project completed in 2012, found that organizations agreed that the relationship between internal audit is positively related to the amount of IT knowledge of the internal audit (Steinbart, Raschke, Gal, & Dilla, 2012). As discussed previously, a good relationship allows internal auditors to provide better consulting as they have access to more resources.

Maintaining Independence

Despite the expectation that internal auditors need to work more closely with other business functions and departments, they must remain independent and objective. In fact, it is even more imperative than ever. As it has been so eloquently stated, the internal audit and other business functions must be "independent but integrated" (Jamison, 2018). When working with other functions, they need to be careful that they do not become involved in the design or implementation of internal controls, policies, or procedures. Because they will be working closely and fostering relationships with other functions, internal auditors could easily become entangled in a project. Assisting with the creation of a control or process, rather than remaining in a consulting position, could lead to loss of objectivity. They should also be very careful about exchanging favors as remaining independent requires that the internal audit have no obligations to other functions or conflicts of interest.

Rising Expectations of the Internal Auditor—Data Privacy

With the increase in cyber breaches and how it is constantly evolving, the cyber risk landscape is important for all size companies to understand. Proper oversight is essential to mitigating risk and this oversight relates directly back to the rise in expectations of the internal auditors within the organizations. But what is being done to reduce the impact or the ability of hackers to breach company's security and IT systems? EY conducted a survey and established a tier of six cyber questions challenging boards of directors to be able to answer "yes" to each of these questions:

1. Has your organization conducted a recent enterprise-wide cyber risk assessment?

Having a clear and documented understanding of the impact and likelihood of cyber risks to your organization is a critical data set to properly manage and report on risk, yet it is something that many companies lack. EY professionals see this lack of knowledge consistently while working with their clients across the globe, especially in industries where operational, health or environmental risks are present. These companies, mistakenly, often view cyber risks as secondary.

2. Has your organization implemented a data governance program beyond basic classification?

Data privacy is a facet of cybersecurity where we've seen more confusion and immaturity than nearly any other. Just as Sarbanes-Oxley (SOX) emerged from trouble in the world of financial reporting, data privacy regulations are emerging from identity theft, rampant cybercrime, blithe sharing of information by companies and malicious use of that information. Almost in partnership with those troublesome realities is the lack of uniformity in national or provincial data privacy regulations.

This has created a compliance nightmare directly connected to cybersecurity risk. The trouble is most organizations outside of retail and healthcare typically adopt only basic data classification policies to govern internal handling/sharing if that. Even more disturbing is the number of companies that are unaware of the type and location of sensitive information within their environments. Budget and cost are often cited as obstacles to implementing a more robust data governance strategy.

3. Have cyber risks and responses been incorporated distinctly into your crisis management program?

The most requested cybersecurity or IT internal audits seen by practitioners are for IT disaster recovery or cyber incident response. These audits have identified that cybersecurity is often not included in organizations' overall crisis management plans. Lacking a formalized plan can greatly reduce an organization's ability to respond and recover from such an event.

Most companies have disaster recovery programs that lead their board to believe their organization would recover quickly from a cyber incident. This misplaced confidence in IT disaster recovery or cyber incident response is an example of board

misalignment on major risks. Indeed, overall board misalignment on risk was one of the key findings in the IIA's 2020 OnRisk report.

4. Has your organization conducted a recent third-party and/or joint venture cyber risk assessment?

Third-party contracts are a normal part of business but once they are signed, they are rarely looked at again, and compliance to terms is not routinely checked unless mandated by a compliance-driven factor such as SOX reporting. Rarer still are routine checks to see if any new regulations, such as the ever-changing data privacy regulations mentioned in question two, should be incorporated into them. In addition, engaging third parties is often department specific, and IT is not always involved. This can lead to concerning gaps in cybersecurity. The 2020 EY Global Consumer Privacy Survey reports 36 percent of organizations have had a data breach caused by a third party over the past two years with this trend on the rise in the remote working model. Fortunately, there is plenty of guidance on this topic. The NIST CSF is a good place to start, specifically ID. GV-4, ID.RA, ID.RM, and ID.SC-1.

5. Is cybersecurity included in the audit plan and/or is internal audit being leveraged as a tool to help your organization manage cyber risk?

The group of practitioners involved in writing this article report they have seen cybersecurity-related audits grow from a rarity to a fixture. Just five years ago, only a select few organizations were doing such audits, but in the group's current portfolio of global clients, every single one has cyber built into its audit plan in some way or another. With IT audit-related expertise required in internal audit groups, boards are starting to recognize the crossover of skillsets applicable to some of the more non-technical cyber needs within organizations—and using it to build their understanding of their organization's cyber resiliency.

Leveraging internal audit as a tool to understand and help manage cybersecurity risk is an enabler that helps organizations answer "yes" to all six of the questions.

6. Is the effectiveness of cyber controls measured and reported in a consistent, meaningful manner?

According to EY's 2020 Global Information Security Survey results, only 7 percent of organizations report they can financially quantify the impacts of breaches, and few can quantify the value of effort spent managing the risk. If neither are quantified, neither are reported with much granularity.

While the new expectations of internal auditors regarding cybersecurity also protect an entity's data privacy, there are specific areas related to data privacy an auditor must address. These areas include the storage and disposal policies of an organization as well as the organizations use of social media. Auditing these areas includes ensuring that access to data, and the use of data is appropriate (Lovejoy et al., 2021).

Data Safekeeping/Confidentiality

Internal auditors are playing larger roles in the protection of data by assessing controls and procedures related to the use and storage of data. Maali and Hrubey (2019) indicate that internal auditors are in an "excellent position" to advise on the proper storage and disposal of data, particularly on the proper length of time to retain data, security measures in place, and the security of third parties hired to process data. The storage and disposal of data is very important for two reasons. First, organizations would be wasting resources to spend the money storing data that is no longer useful. Second, the longer data is stored, the greater the risk that company or customer data privacy will be violated. The security measures for data storage relate back to the internal audit's role in cybersecurity, which protects against unauthorized access. Internal auditors can assess whether procedures in place allow for proper disposal of data. As for third party data processing, companies often outsource the processing of their data to companies specialized in analytics. Companies are responsible for the data handled by third parties, so internal auditors should make sure the hired company can properly protect the data. As data is used at an ever-increasing pace, internal auditors will be held to higher expectations in this area.

Social Media

Another area where internal auditors are expected to devote more attention is social media. Social media platforms are being used more and more often in business for marketing and communication with customers. Internal auditors should make sure controls and procedures for social media use are adequate to protect customers privacy and company data. Steps internal auditors can take to audit social media use include assessing the risks to the company, especially reputational risks, and understanding how the organizations use social media (Cain, 2012). The risk to an organizations reputation when using

social media include the loss of business image if employees and other company representatives behave improperly on social media. This loss of image also could involve a loss of trust if private information shared with a company on social media is disclosed. Business use of social media is expanding to communication with customers regarding complaints or other issues, which means there is sensitive information exchanged through companies' social media platforms. Internal auditors must be ever more vigilant.

Future Research

The idea of a correlation between cyberattacks and effective internal audit procedures was not a focus of this study, however, future research could focus on the idea of the roles of internal auditors and a correlation between the strength of the audit function and risk management of cybersecurity.

Future research also could highlight the area of independence and objectivity of internal auditors working within the different business functions of a company. There are also significant research opportunities in artificial intelligence being utilized in internal audit and the effectiveness of internal controls.

Conclusion

Internal auditors face many new and rising expectations related to technology, cybersecurity, and data privacy. Companies need their internal audit functions to step up and objectively advise on the improvement of controls, procedures, and processes put in place for the security of data. This requires internal auditors to have relationships of trust with the functions such as IT and information security, that design, implement, and maintain these controls and procedures. To be successful in these expanding roles, internal auditors need to foster new skills, specifically those related to information technology and the technology systems used by a company. Internal auditors need make sure the use of social media is not negatively affecting data privacy. Because of the serious implications of potential breaches in security, these increasing expectations of internal auditors are critical to privacy, cybersecurity, and the continuation of an entity.

References

American Institute of Certified Public Accountants (AICPA). (2022, January). Trust Services and Information Integrity. Retrieved from AICPA Assurance and Advisory: https://us.aicpa.org/interestareas/frc/assuranceadvisoryservices/trustdataintegritytaskforce

Cain, A. (2012, August). The Social Media Scene. *Internal Auditor* , pp. 44–49.

COSO Framework. (2019). *CMA Review Part 1: Financial Reporting, Planning, Performance, and Control.* Gainesville: Gleim.

Cybersecurity and Infrastructure Security Agency. (2019, November 14). *Security Tip (ST04-001)*. Retrieved from Cybersecurity and Infrastructure Security Agency: https://us-cert.cisa.gov/ncas/tips/ST04-001

Deloitte (2017). *Cybersecurity and the role of internal audit An urgent call to action.* Retrieved from Deloitte: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-risk-cyber-ia-urgent-call-to-action.pdf

Jamison, E. A. (2018). *The Future of Cybersecurity in Internal Audit.* Inernal Audit Foundation, Crowe Analytics.

Kerner, S. (July 2021). Colonial Pipeline hack explained: Everything you need to know. *WhatIs.com.* Retrieved 01/21/2022: Colonial Pipeline hack explained: Everything you need to know (techtarget.com)

Lovejoy, K., Hartkopf, L., Randolph, M., George, A., Chambers, R., Petrisky, D. (2021). The Risky Six: Key questions to expose gaps in board understanding of organizational cyber resiliency. *Ernst & Young and The Institute of Internal Auditors.* Retrieved 02/18/2022 from: ey-the-risky-six.pdf

Maali, M., and Hrubey, P. (2019, April). A Matter of Privacy. *Internal Auditor*, pp. 64–65.

Messier, W. F., Glover, S. M., and Prawitt, D. F. (2018). Internal Auditing. In W. F. Messier, S. M. Glover, and D. F. Prawitt, *Auditing & Assurance Services* (p. 730). McGraw-Hill.

Reciprocity (2019, November). What are Information Security Controls. *Reciprocity.* Retrieved 02/18/2022 from Reciprocity: https://reciprocity.com/resources/what-are-information-security-controls/

Senate RPC: Policy Papers. (January 29, 2021). The SolarWinds Cyberattack. Retrieved 02/21/2022: The SolarWinds Cyberattack (senate.gov)

Steinbart, P. J., Raschke, R. L., Gal, G., and Dilla, W. N. (2018). The Influence of a Good Relationship Between the Internal Audit and Information Security Functions on Information Secruity Outcome. *ScienceDirect*, 15–29.

Steinbart, P. J., Raschke, R. L., Gal, G., and Dilla, W. N. (2012). The Relationship Between Internal Audit and Information Security: An Exploratory Investigation. *ScienceDirect*, 228–243.

The Center for Association Leadership. (2019). *CAE Certification*. Retrieved from The Center for Association Leadership: https://www.asaecenter.org/programs/cae-certification

The Institute of Internal Auditors . (2019). *2019 North American Pulse of Internal Audit*. Lake Mary, Florida, United States: The Institute of Internal Auditors.

The Institute of Internal Auditors. (n.d.). *Definition of Internal Auditing*. Retrieved from IIA: The Institute of Internal Auditors: https://na.theiia.org/standards-guidance/mandatory-guidance/Pages/Definition-of-Internal-Auditing.aspx

Turton, W., and Mehrotra, K. (June 2021). Hackers breached Colonial Pipeline using compromised password. *Bloomberg Technology/Cybersecurity*. Retrieved 01/21/2022: Colonial Pipeline Cyber Attack: Hackers Used Compromised Password - Bloomberg

Uberti, D. (June 2021). How the FBI got Colonial Pipeline's ransom money back. *The Wall Street Journal*. Retrieved 01/21/2022: How the FBI Got Colonial Pipeline's Ransom Money Back - WSJ

Williams, C. (March 2019). COSO ERM Framework – background and overview. *ERM Insights.* Retrieved 02/21/2022: https://www.erminsightsbycarol.com/coso-erm-framework/