Auditing as a way to increase cyber security

Orkida Ilollari
Faculty of Economy & Information Technology, EUT

Manjola Islami
Faculty of Economy & Information Technology, EUT

Abstract

Nowadays, businesses are building bottomless real-time connections with their customers, suppliers, partners, and governments, collecting and selectively sharing huge amounts of data. The value of stored and in-transit information is rising rapidly, driving new markets and generating a need for securely connecting devices and delivering trusted data. Data integrity is a vital component in economy which can pertain to individuals, companies, governments and globally. It is a measure of the validity and reliability of a data. While internal audit has taken some steps toward keeping up with the dynamic changings and complex technology, recently survey indicate that it appears still a challenge to address technology risks as cyber-attacks have become more sophisticated and more complex. Cyber threats to economic security are increasing in frequency, scale, sophistication and severity of impact. The ranges of cyber threat actors, methods of attack, targeted systems and victims are also expanding. In Ernst and Young 2016 report "Creating trust in the digital world", the company warns that cyber security risks have been underestimated. Cyber security refers to the measures taken to protect company data in computer-based systems from loss, destruction, unauthorized access, or misuse by unintended parties. According to IIA's 2016 Global Perspectives and Insights, Internal Audit as Trusted Cyber Adviser: "Cyber security must be considered holistically and systemically, as the effects of failure can range from an inability to conduct basic transactions, to loss of intellectual property, to potentially significant reputational damage. It is not solely a technology risk; it is a business risk and, as such, internal auditors have a critical role to play." How can internal audit help in cyber security? Yet, most survey of board members rate technology risks, most notably cyber, *as high (if not at the very top) on the list of their concerns. A growing number of well-informed internal audit leaders are making steps toward positioning internal audit to be an organization's trusted cyber adviser by building competencies and demonstrating proficiency in IT issues such as cyber security and big data, and providing a full range of internal audit services related to those issues. The challenge of internal audit departments is not only to understand cyber security risks but to translate that understanding into action.*

***Keywords**: Internal audit, cyber security, cyber-attacks, data security, data integrity.*

1. Introduction

In less than a generation, we have passed from the industrial age to the digital age. Digital technologies related with digital era have an effect on every aspect of our daily lives such as our physiology, our identity and the way we built and manage relationships, our privacy and also on national issues such as economics and national defense. Companies collect, process, report and store large volumes of data in their normal course of business. The ability to examine, analyze and act on data is becoming more and more important to all companies. The Internet allows businesses to use information in a more effective way, by allowing the stakeholders such as customers, suppliers, employees, and partners to get access to the business information they need, how and when they need it. Consequently, internet and digital technologies are without a doubt one of the most influential and important inventions in the history of humanity. However, the technology has also undesirable consequences for our society.

The new digital technologies make companies more and more vulnerable. The technology evolves and the cyber-attacks have become more sophisticated and more complex. The increasing number of cyber-attacks and data theft cost to businesses and to the public sector several million each year. Consequently, cyber-security has captured the attention of businesses in all industries, which are investing more and more in information security. Preventing cyber-attack threats has become now a strategic priority for both private and public sector.

As awareness related to the cyber threat has increased, both public and private policymakers have developed ideas, prescriptions, technologies and advice in order to fight against cyber risks. Very often this large amount of information has led to confusion and uncertainty with a resulting paralysis of action just when clear and decisive policies are needed.

Cyber risk is not important at the same level for all companies and industries type since it can impact different fields from one sector to another (industrial systems in Industry sector, personal data and supply chain in Retail, etc.). In some sectors of activity, as Banks and Insurance, the managers are already very sensitive to this risk. However, other sectors, consider this risk as a real strategic risk. Consequently, the cyber risk must be treated, analyzed and well positioned on the scale of company's priorities, according to their business risk factors.

Internal audit is playing an important role in addressing technology risks. The role of the audit committee is crucial: it must monitor the level of management awareness and cyber threats. The Committee shall also monitor developments in business regulation and policies. Now, most of the businesses have placed technology risk and especially cyber-risk is in the top of their concerns. Internal audit managers are making steps toward positioning internal audit as an organization's cyber consultant through building competencies and demonstrating skills in IT issues such as cyber-security and providing audit services related to those issues.

The technology has changed our word and as a result the industry is developing strategies to meet these changes.

2. Data integrity

Data integrity refers to the accuracy, consistency (validity) of data over its lifecycle (Cucoranu et al, 2013). Compromised data is of little use to enterprises, not to mention the dangers presented by sensitive data loss. Consequently, data integrity is one of the most critical elements in any system (Subashini & Kavitha, 2010) and it is a core focus of many enterprise security solutions.

Data integrity defines the quality of information, which guarantees the data exist, is accurate, complete, and has a whole structure. Data integrity is preserved only if and when the data is satisfying all the business requirements and important rules and regulations. These requirements and rules might be how data is processed, linked, validity of details and content, etc. According to data architecture principles, functions such as data transformation and data storage, must guarantee the integrity of data, which means, data integrity should be maintained during input, transfer, storage and retrieval.

The data can be considered consistent and can be given the assurance to be accurate and reconciled if data integrity is well-preserved. In terms of data integrity in databases, should be ensured that the data stored in the database corresponds exactly to the real world details it reflects.

Data integrity can be compromised in a number of ways. Each time data is reproduced or transferred, it should remain unchanged and uncorrupted between updates. Error checking and detecting methods and data validation procedures are typically relied on to ensure the integrity of data that is transferred or reproduced without the intention of alteration.

The term data integrity may lead to confusion because it may refer either to a state or a process. Data integrity as a state defines a data set that is both accurate and valid. Furthermore, data integrity as a process, describes measures used to ensure validity and accuracy of a data set or all data contained in a database or other construct. For instance, error detection and data validation methods may be referred to as data integrity processes.

Maintaining data integrity is important and key to the companies for several reasons as data integrity ensures the accuracy of the information recoverability, searching ability, traceability connectivity and analysis. Protecting the validity and accuracy of data also increases stability, performance and drive decision-making considering the data can be maintained and reused when needed.

Data integrity drives enterprise decision-making, but it may undergo a variety of processes and organizing changes to transform from raw form to usable formats as needed and practical for reporting, analysis and facilitating the users' decisions. Therefore, data integrity is key and a top priority for all enterprises.

There are variety of ways which compromise data integrity making data integrity security practices an essential component of effective enterprise security procedures and actions. Data integrity may be compromised through:

- Transfer errors, including unintended alterations or data compromise during transfer from one device to another;
- Human error, whether unintentional or malicious;
- Viruses or malware, hacking, bugs and other cyber threats;
- Compromised hardware, whether a device or hard-disk crash;
- Physical compromise to computer or data storage equipment.

However, only some of the abovementioned compromises may be adequately prevented through data security. Consequently, data backup, duplication and storage become critical for ensuring data integrity. Other data integrity security best practices include input validation to prevent the entering of invalid data, error detection/data validation to identify and check errors in data transmission, and security measures such as data loss prevention, access control, data encryption, and more.

Most of the business debates and concerns regarding cyber threats have focused on the confidentiality, accessibility and availability of information. In the future, it is expected more cyber operations to change or manipulate electronic information in order to compromise its integrity in terms of accuracy and reliability, instead of deleting it or disrupting access to it. When corporate executives, investors, or other stakeholders cannot trust the information they are receiving, their decision-making will be impaired.

Successful cyber operations targeting the integrity of information would need to overcome any restrictions, data checks and balances designed to prevent the manipulation of the information.

One of the most significant new attack vectors is compromising the integrity of systems, networks and data. Confidentiality and accessibility attacks are loud and obvious. They break restrictions and expose data information causing embarrassment, inconvenience, and some losses. Data integrity attacks are stealthy, selective, and can be much more disturbing. Instead of doing damage or making off with huge amounts of sensitive data, they instead focus on carefully modifying particular elements within targeted transactions, communications, or data to gain a significant benefit.

Carbanak[1] was significantly different than previous banking malware, which focused on stealing account and login data. Carbanak stealthily compromised about 100 banks and enabled attackers to understand how internal operations were handled (Kam et al., 2015). The malware conducted reconnaissance for attackers who then began modifying selected transactions. When the attack ended, only a small number of accounts were targeted and $1 billion were stolen (Kam et al., 2015). Data integrity attack research is gaining momentum. The risk is data integrity attack in the financial sector in which large amounts of money may be stolen by cyber thieves who will modify selected information in the transaction stream, resulting in a significant redirection of payment to anonym or other designated accounts. The detection of that incident and others actions similar to it is becoming very difficult. Data integrity attacks can appear to be operational problems, accounting errors, audit issues, acts of hackers, or simply human errors. To compound matters, the existing tools, mechanisms, and processes currently available and in use are mostly blind to these types of attack.

Perhaps one of the most prevalent vectors for integrity attacks is in the rise of ransomware[2], which modifies only a few files. Ransomware, a permanent form of a denial-of-service attack, leaves the system working with all data present, but due to the integrity compromise certain files are no longer usable (Gazet, 2008). Attackers then demand a ransom to restore the original integrity. This attack path will also grow significantly in 2016 (McAfee Labs Threats Predictions, 2016).

[1] Carbanak is an APT-style campaign targeting (but not limited to) financial institutions that was claimed to have been discovered in 2015 by the Russian/UK Cyber Crime company Kaspersky Lab who said that it had been used to steal money from banks. The malware was said to have been introduced to its targets via phishing emails. The hacker group was said to have stolen 1BN dollars, not only from the banks but from more than a thousand private customers.

[2] Ransomware is a type of malware that prevents or limits users from accessing their system. This type of malware forces its victims to pay the ransom through certain online payment methods in order to grant access to their systems, or to get their data back.

3. Data integrity vs. data security

Data are the most important asset to any organization. Therefore, it must be made sure that data is valid, accurate and secure all the time.

Data integrity and data security are two different aspects that make sure the usability of data is preserved all the time. Main difference between integrity and security is that integrity deals with the validity of data, while security deals with protection of data. Backing up, designing suitable user interfaces and error detection/correction in data are some of the means to preserve integrity, while authentication/authorization, encryptions and masking are some of the popular means of data security. Suitable control mechanisms can be used for both security and integrity.

Data integrity and data security are two related items and important aspects each playing an important role in the successful achievement of the other of making sure that data is useable by its intended users. Data integrity makes sure that the data is valid. Data security refers to the protection of data against loss, unauthorized access or corruption and is necessary to ensure data integrity.

That said, data integrity is a desired result of data security, but the term data integrity refers only to the validity and accuracy of data rather than the act of protecting data. Data security, in other words, is one of several measures which can be employed to maintain data integrity, as unauthorized access to sensitive data can lead to corruption or modification of records and data loss. Whether it's a case of malicious intent or accidental compromise, data security plays an important role in maintaining data integrity.

For modern enterprises, data integrity is essential for the accuracy and efficiency of business processes as well as decision making. It's also a central focus of many data security programs. Achieved through a variety of data protection methods, including backup and replication, database integrity constraints, validation processes, and other systems and protocols, data integrity is critical yet manageable for organizations today. Fundamental data security requirements are confidentiality, integrity and accessibility.

A secure system ensures the confidentiality and privacy of data. This means that it allows individuals to see only the data or information categories which they are supposed to see. Confidentiality has several different aspects dealing with privacy of communications, secure storage of sensitive data, authenticated users and access control. Privacy is a very broad concept. According to Oracle Corporation[3], in the

[3] Oracle is a computer technology corporation developing and marketing computer hardware systems and enterprise software products.

business world, privacy may involve trade secrets, proprietary information about products and processes, competitive analyses, as well as marketing and sales plans.

Once confidential data has been entered, its integrity and privacy must be protected on the databases and servers where it resides, while authentication is a way of implementing decisions about whom to trust. Authentication methods seek to guarantee the identity of system users for data accessibility: that a person is who he says he is, and not a deceiver.

4. Cyber-security Problem and Policies to address it

Technological innovations have made it easy for attackers to exploit vulnerabilities from anywhere in a matter of seconds. The exploitation of such vulnerabilities at a smaller institution such as a community bank poses the risk of a domino effect across systemically important financial institutions, and possibly other industries and economies. Attacks against the financial and non-financial sectors have, for now, been very serious, including schemes resulting in hundreds of millions of dollars in losses. Phishing, or emails designed to trick users into giving sensitive information or to download malware, is an old-fashioned method that attackers have not yet abandoned simply because it is effective. According to a survey from cyber-security firm Cloudmark, "91 percent of companies' encountered phishing attacks in 2015, with the lion's share 84 percent of companies claiming attacks successfully snuck past their security defenses". Spear-phishing, which are emails that look like they come from a trusted source, have an even more harmful effect. The pattern of sending a message to the accounting department which looks like it is from the company's CEO has become quite popular, with 63 percent of companies having encountered the tactic. Phishing is a widespread and a low-cost technique that attackers use to infiltrate corporate networks. Phishing sites can generate tens of thousands of emails with the goal of getting just one attachment opened by a consumer or employee. Some 30 to 35 such sites per day are shut down by one of the Internet Security Alliance's financial sector members in collaboration with outside vendors.

In February 2015, James Clapper, Director of National Intelligence, resumed the effects of our current vulnerability: "We must be prepared for a catastrophic large-scale cyber strike. We've been living with a constant and expanding barrage of cyber-attacks for some time. This insidious trend will continue. Cyber poses a very complex set of threats, because profit- motivated criminals, ideologically motivated hackers, or extremists in variously capable nation-states, like Russia, China, North Korea, and Iran, are all potential adversaries, who, if they choose, can do great harm."

All the economic incentives in cyber-security favor the attackers. While hardware, software vulnerabilities, and technological standards are all-important when discussing cybersecurity, a little consideration is given to the economics of cybersecurity. Cyber-attacks are becoming more common and technology can help to illustrate how they occur. However, to address this issue in a more systematic and proactive way, it is also needed to investigate why they occur. From a private sector viewpoint, economics is concerned primarily with the why. Various independent studies from PricewaterhouseCoopers/CIO Magazine CSIS/McAfee have found the deciding factor in cyber-security is not technology, but economics. When one considers the cost and the value of cybersecurity, it becomes apparent that the economic balance is slanted in favor of the attackers.

5. Traditional mechanisms

Most of the modern communications are subject to cybersecurity attacks. Traditional mechanisms such as government regulation, independent regulatory agencies and consumer lawsuits are ineffective in making the security stronger in light of these threats. This is largely due to the fact that much of traditional regulatory and judicial enforcement were designed to address malfeasance and not the types of problems that the companies are facing today. The central problem with cyber-security, however, is that technology is under attack. Technology is constantly being constructed and many companies are willing to invest in reasonable security, but there are overwhelming incentives to attack them. In the case of Enron and WorldCom scandals of the 1990s, for instance, the independent agencies and regulators, took the right side of consumers to fight against corporate malfeasance. In the present cybersecurity environment, the side of the government, consumers and industry are opposed to the vast criminal syndicates and ever more nation states.

Cyber regulations should also be considered from a broader systems viewpoint. A slow pace of regulation will have an effect on investment, innovation and job creation. Major organizations find cybersecurity to be a complicated and costly undertaking, and ask to know how compliant their configuration will be before they can afford to make substantial investments?

6. Cyber-attacks

Cyber threats to economic security are increasing in frequency, scale, sophistication, and severity of impact. The ranges of cyber threat actors, methods of attack, targeted systems, and victims are also expanding. Overall, the unclassified information and communication technology networks that support economic activities remain vulnerable to disruption. Cybercriminals are increasingly targeting midmarket companies and startups in hopes of easy access (PWC, 2015). The cost to a business can be high, ranging from financial loss to reputational damage. With heightened awareness, private companies can fight back. With cyber-attacks on the rise, technology experts worry about the looming threat to data integrity. In a data modification attack, an unauthorized party on the network interrupts data in transit and changes parts of that data before retransmitting it. An example of this is changing the euro amount of a banking transaction from €1,000 to €100,000. In a replay attack, an entire set of valid data is repeatedly interjected onto the network. An example would be to repeat, one thousand times, a valid €1,000 bank account transfer transaction. Data must be stored and transmitted securely, so that information such as credit card numbers cannot be stolen.

These quiet, insidious attacks may come in the form of planted malware or selective hacks that seize, modify or delete data or transactions in ways that benefit the perpetrators. For example, an attack could change a bank account's direct deposit setting to channel deposits to another account. High-profile attacks continue to increase in frequency.

James Clapper, Director of U.S. National Intelligence, last year warned of a growing number of low- to moderate-level cyber-attacks against private sector targets from a variety of sources, including several nations. These attacks resulted in stolen or deleted corporate data, compromised personally identifiable information and sizeable remediation costs to companies and consumers.

Like any business, most cybercriminal operations follow the money, looking for the easiest way to steal something of value. Payment systems used to be simple. To buy something, all we needed was enough cash. Today, however, the number of alternate payment methods is rather dizzying, from credit cards, and debit cards, mobile applications, to online payment services. Significant security focus is placed on vulnerabilities associated with credit and debit card transactions because most digital transactions use these forms of payment. With the growth in alternate payment methods, the number attack surfaces have multiplied, giving cyber thieves many, many targets from which to choose. The 2014 data breach at Home Depot exposed information from 56 million credit/debit cards and 53 million customer email addresses. Home Depot estimated the cost of the breach to be $62 million (Hawkins, 2015). Most attacks approach payment card theft in the same way they have for the past 10 years, by attacking payment mechanisms or the databases containing card data. Once the card data have been obtained, they sell it as quickly as possible and pocket the profit. Now, however, the things are changing. Given the abundance of payment methods, most of which still require usernames and passwords, credentials have become very valuable. To steal credentials, the cybercriminals are targeting the consumers directly because they are both the source of the credentials and the weakest link in the payment process. The studies (McAfee Labs Threats Predictions, 2016) predict that in 2016, payment system cybercriminals will increasingly focus on attacks that lead to the theft and sale of credentials. The experts think that they will leverage traditional, time-proven mechanisms including phishing attacks and keystroke loggers, but new methods will emerge too. They also predict that the number of payment system thefts will continue its relentless growth.

7. Cyber-security in the Banking and Financial Sector

In a digital world where the number of targets that could be hacked has grown exponentially, banks and other financial institutions remain a top target for cyber-attacks, whether for retaliation, financial gain, or data theft. State adversaries or activists disrupt the financial services industry in order to wound the interconnected global economy and the integrated nature of today's society. As cyber-attacks become more sophisticated, financial service firms are investing in cybersecurity to reduce vulnerabilities, according to a 2016 annual report by the Financial Stability Oversight Council. Financial institutions continue to be among the sectors that support above average cybersecurity programs. Nearly two-thirds of sector institutions have an overall security strategy. Forward-leaning firms are using innovative cybersecurity tools and emerging technologies to set high standards in security and privacy in the face of often redundant regulatory oversight. Yet despite the best efforts, the sector has been unable to fully counter sophisticated cyber-attacks ranging from distributed denial of service attacks to breaches of personal and financial data. The consequences of cyber-attacks are not limited to losses suffered by the attacked institution.

Financial services were one of the first industries to embrace information and communication technology, to automate inner workings and branch operations and develop innovations like credit cards and ATMs. This did not only help the sector to grow, but it also changed the behavior of retail and commercial banking customers. Consumers today have higher expectations about service, given the rapid increase of technologies available to them. Unlike

their predecessors, they are more likely to shop around for products and take an interest in direct and mobile channels. At the same time, new market entrants and established competitors in the retail banking business are responding with new and compelling offerings. New technologies, such as smartphones, realistic authentication and cloud computing are influencing change, particularly in the area of mobile payment applications and instant money movement. However, as more innovations become important for market differentiation and cyber protection, the exploitation of mobile devices and applications for consumer banking has rocketed.

Commercial banking, too, is expected to benefit greatly from technology as a new distributed ledger system known as blockchain moves into the mainstream. The application of encryption and algorithms has the potential to automate complex, multi-party transactions and improve the speed and accuracy of settlement systems.

In June 2016, a group of seven financial institutions used blockchain to move money almost instantaneously via a gross settlement system known as Ripple.

Since then, securities exchanges and record-keepers have enabled technologies for the formulation, processing, and settlement of highly complex trades that previously took hours or even days. High-frequency trading is now widely used by institutional investors, pension funds, unit trusts and other market participants in an effort to achieve higher returns for investors.

Cybersecurity is "perhaps the single most important new risk to market integrity and financial stability," Commodity Futures Trading Commission Chairman Tim Massad told attendees of a 2015 futures industry conference (Meyer, 2015).

Indeed, more than half of those surveyed by the International Organization of Securities Commissions and the World Federation of Exchanges in 2013 reported experiencing a cyber-attack during the previous 12 months (Rohini & Naacke, 2013).

The insurance industry is also subject to the changes in how business is conducted in today's interconnected society. The richness of the insurers' data about credit cards, medical and other information makes them a prime target.

In its annual "Global State of Information Security Survey", Pricewaterhouse Coopers noted financial services companies saw a "striking year-over-year increase in incidents attributed to highly skilled adversaries in 2015." Not only is the involvement of nation-states (and their proxies) becoming more common, but organized criminal attacks on the financial services sector jumped 45 percent in 2015. Evidence is beginning to accumulate that nation-states and well-resourced, organized criminal syndicates are partnering to perpetrate cyber-crime, sometimes engaging insiders for assistance.

The impact of cyber-attacks is not confined to losses suffered by the attacked institution. A 2015 study for the Centre for the Study of Financial Innovation highlighted the threats to the financial system itself, noting that "we may at some point see a cyber-attack so powerful on an individual bank that it could bring down the institution necessitating a state bailout." A cyber-attack on key institutions could paralyze key activities such as interbank payments for several days, which could put the entire interconnected, global financial system into chaos.

8. Challenges in financial institutions and the three lines of defense

Cyber technology and attack methods are constantly changing and the regulatory process is time consuming. Furthermore, financial institutions are required to respond to duplicative cybersecurity inquiries from different regulators, or from different offices of the same regulator. In the United States, the SEC is becoming ever more insistent in monitoring and testing the cybersecurity controls of broker-dealers and registered investment advisers.

Mobile banking is very helpful for consumers, but opens up a window of opportunity for attackers to exploit. Cyber thieves code malicious applications targeting banking data, but it's not just banking applications that challenge cybersecurity.

Business units can integrate information technology (IT) to manage cyber risks in day-to-day decision making and operations. This makes up an organization's first line of defense. The second line includes IT risk managers who provide governance and oversight, monitor security operations, and step in as needed when instructed by the chief information security officer (CISO). Increasingly, many companies are realizing they may need a third line of cyber defense, independent review of security measures and performance by an internal audit. Internal audit of an enterprise should play a key role in identifying opportunities to strengthen security. At the same time, they have a duty to inform the audit committee and board of directors that the controls under their responsibility are in place and functioning correctly, to avoid potential legal and financial liabilities.

The why and how of cyber-risk assessment and defense-To explore an organization's cyber risks an answer is required to following questions:

Who might attack? Are they criminals, competitors, third-party vendors, disappointed insiders, hackers with an agenda of their own, or someone else?

What business risks need to be taken into account? Are they asking for money or intellectual property? Do they intend to disrupt the business or ruin our reputation? Could health and safety risks be created?

What tactics might they use? Will they test for specific system vulnerabilities, go phishing, use stolen credentials, or attack through a compromised third party?

Deloitte Advisory has identified a three-point approach to help clients address the threats identified through examining these questions:

Secure: Most organizations have established controls such as perimeter defenses, identity management, and data protection to guard against known and emerging threats.

Risk-focused programs prioritize controls in areas that align with top business risks.

Vigilant: Threat intelligence, security monitoring and behavioral and risk analyses are used to detect malicious or unauthorized activity such as application configuration changes or unusual data movement, and help the organization respond to the shifting threat landscape.

Resilient: Incident response protocols, forensics, and business continuity and disaster recovery plans are put into action to recover as quickly as possible and reduce impact.

Exploring the who, what, and how questions posed above in the context of a secure, vigilant, and resilient organization provides the foundation for a broad internal audit cyber-security assessment framework that will be an integral component of the organization's cyber defense initiatives.

9. Audit as a mean to address cybersecurity

According to IIA, cyber-security refers to the measures taken to protect company data in computer- based systems from loss, destruction, unauthorized access, or misuse by unintended parties. As explained in The IIA's 2016 Global Perspectives and Insights: Internal Audit as Trusted Cyber Adviser, "Cyber -security must be considered holistically and systemically, as the effects of failure can range from an inability to conduct basic transactions, to loss of intellectual property, to potentially significant reputational damage. It is not solely a technology risk; it is a business risk and, as such, internal auditors have a critical role to play."

Fortunately, the vast majority (93 percent) of them report that the risks associated with cyber-security are understood by their internal audit department. In contrast, in its 2016 report, "Creating trust in the digital world." Ernst and Young warned that cybersecurity risks had been underestimated and that too many organizations aggravated their vulnerabilities by taking an ad hoc approach to risk. Global Pulse also confirms that a little more than half (55 percent) of internal audit assert their organization uses a framework that is meant to address cybersecurity. A similar percentage of respondents (58 percent) say they provide cybersecurity-related internal audit services to their organization, either exclusively (16 percent) or through co-sourcing (42 percent). We should consider cybersecurity holistically and systemically, as the effects of failure can lead to an inability to conduct basic transactions, to loss of intellectual property, and to potentially significant reputational damage. Even though most internal audit departments may claim to know cybersecurity risks, only a few fully translate that knowledge into action by providing all of their needed organizations' cyber-security internal audit services. Yet one in four (25 percent) internal audit leaders indicate that no cybersecurity-related internal audit services have been provided to their organization because of lack of skills or knowledge and tools to audit cybersecurity, others 16 percent, report that all cybersecurity-related internal audit services are fully outsourced.

10. Auditing Culture

History shows that culture can directly and negatively affect an organization's reputation, operations and finances. Board members, executives and other corporate stakeholders should be able to look to internal audit to provide assurance and advisory services that help an organization to monitor and strength its culture and generate an alert when things may go wrong.

Internal audit has been assessing soft controls and an organization's general ethical climate for quite some time. However, while some are taking the steps to formally audit organizational culture, a number of factors are impeding the majority's ability to progress. Culture is established at the top, embodies the organization's believes and values, and dictates acceptable and unacceptable behavior. Unacceptable or unethical behavior puts an organization at risk and may contribute to toxic organizational cultures associated with fraud, corruption, and other types of malfeasance.

Some extreme events have even led to economic crises and eroded public trust. In 2015, a series of high-profile incidents were potentially indicative of major culture missteps, including an accounting scandal at Toshiba, allegations of bribery and corruption at FIFA, evidence of modified emissions tests at Volkswagen, and questionable reports on the impact of climate change from ExxonMobil. These examples should be a wake-up call for internal audit to guarantee on whether an organization's culture is consistent with the core values it advocates and whether it complies with laws and regulations. However, less than 28 percent of internal audit leaders state that they do audit culture.

11. Cybersecurity related internal audit services

All cybersecurity-related internal audit services that the internal audit department provides are co-sourced between internal audit and outside providers. According to a 2016 IIARF CBOK report IT and analytics are two of the seven skills that chief audit executives (CAEs) are building within their internal audit departments. CAEs also compensate for the lack of competencies and tools through co-sourcing and outsourcing arrangements.

FIGURE 1: Organizations cyber-security-related internal audit services providersSource: Issue 5, Global Perspectives and insights

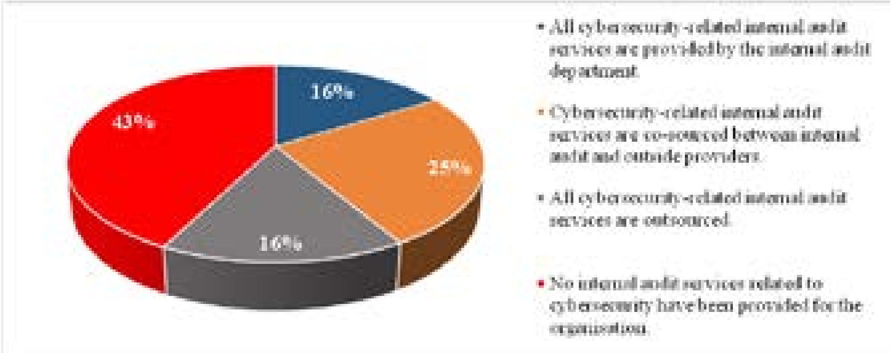
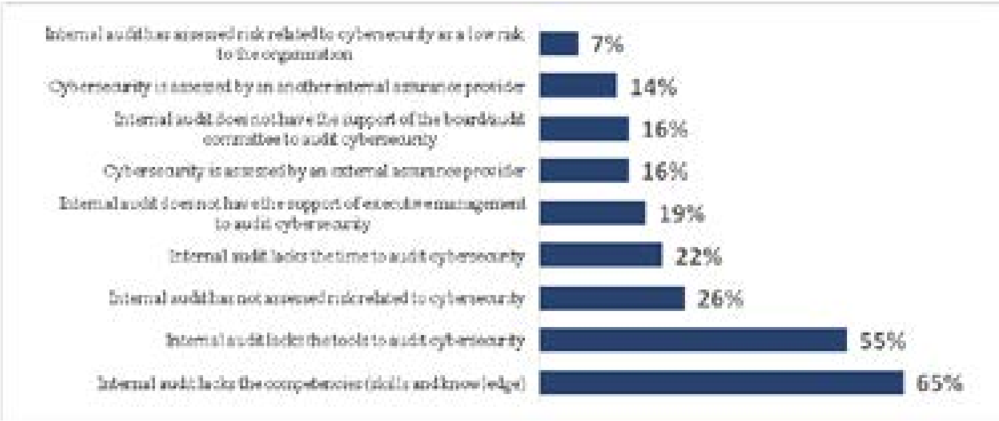


FIGURE 2: Reasons why internal audit departments do not audit cybersecurity Source: Issue 5, Global Perspectives and insights



12. The Audit Committee's Role in Cyber-security

Cyber risks are becoming more frequent and varied, and the potential harm they can cause to companies, their trading partners, and customers continues to grow. While most businesses take these risks seriously, more can be done both to combat the dangers and to inform company leaders about cybersecurity readiness. Internal audit has a critical role in helping organizations in managing cyber threats. They play it by providing an independent assessment of existing and needed controls, and helping the audit committee and board understand and address the diverse risks of the digital world.

The level of the audit committee's involvement in cyber-security issue differs according to company type and industry category. In some organizations, the audit committee is directly in charge of cyber-security risk, while in other organizations, there is a separate risk committee. Companies, for which technology is the core tool of their activity, in most of the cases have a cyber-risk committee which is entirely dedicated to cyber-security.

Audit committees should be always aware of cyber security trends, policy developments and main threats that affect their company, as the risks related to information and data theft can have an economic and reputational impact that can significantly affect the shareholders of the company. Despite of the formal structure in place, the fast change of technology, data growth and risks demonstrate the growing importance of understanding cyber-security as an independent business risk.

In order for audit or risk committee to better understand where they should be focused they have to be always in touch with Technology Department employees.

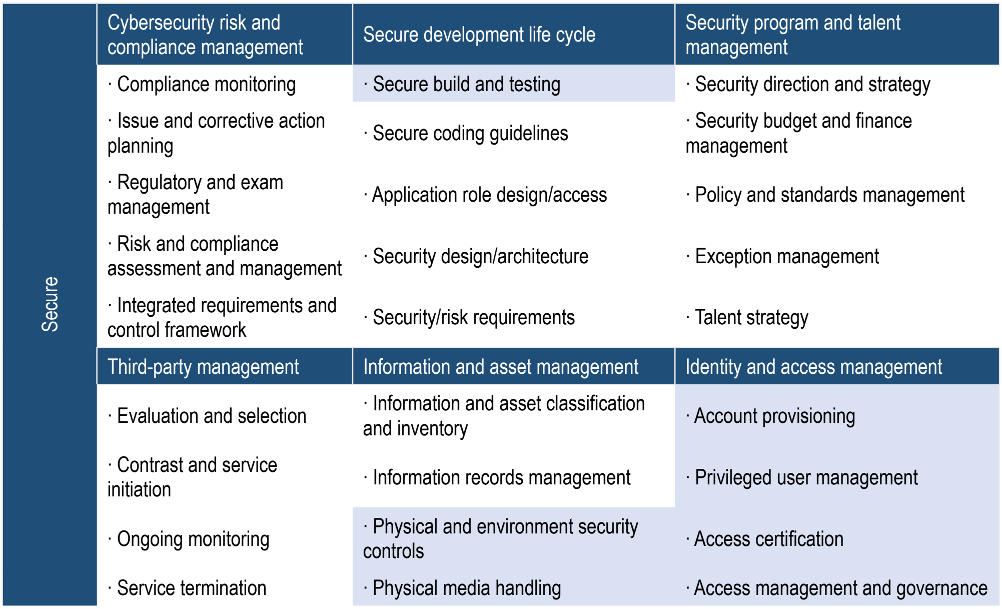
Audit committees members during cyber-security risks monitoring might be focused on two main streams:

1. The kind of data which is leaving the company and the related monitoring activities which are in place.
2. If a response plan exist for cyber-attacks, if it is up to date and the company have practiced it in the past.

13. Cyber-security assessment framework

Attack and penetration procedures that evaluate components of the organization's cybersecurity readiness, are valuable, but do not provide assurance across the spectrum of cybersecurity risks. For internal audit to provide a comprehensive view of cybersecurity, and avoid providing a false sense of security by only performing targeted audits, a broad approach should be employed. Table 1 portrays a cybersecurity assessment framework built on the Secure; Vigilant; Resilient. TM concept. As shown, multiple security domains support each of the three themes. In assessing cybersecurity readiness, internal audit can benefit from understanding the capabilities within each of the 12 domains, how they are addressed today, and gaps that may exist within the organization.

TABLE 1: Representative cyber-security framework



Secure	Cybersecurity risk and compliance management	Secure development life cycle	Security program and talent management
	· Compliance monitoring	· Secure build and testing	· Security direction and strategy
	· Issue and corrective action planning	· Secure coding guidelines	· Security budget and finance management
	· Regulatory and exam management	· Application role design/access	· Policy and standards management
	· Risk and compliance assessment and management	· Security design/architecture	· Exception management
	· Integrated requirements and control framework	· Security/risk requirements	· Talent strategy
	Third-party management	Information and asset management	Identity and access management
	· Evaluation and selection	· Information and asset classification and inventory	· Account provisioning
	· Contrast and service initiation	· Information records management	· Privileged user management
	· Ongoing monitoring	· Physical and environment security controls	· Access certification
	· Service termination	· Physical media handling	· Access management and governance

Vigilant	Threat and vulnerability management	Data management and protection	Risk analytics
	· Incident response and forensics	· Data classification and inventory	· Information gathering and analysis around:
	· Application security testing	· Breach notification and management	- User, account, entity
	· Threat modeling and intelligence	· Data loss prevention	- Events/Incidents
	· Security event monitoring and logging	· Data security strategy	- Fraud and anti-money laundering
	· Penetration testing	· Data encryption and obfuscation	- Operational loss
	· Vulnerability management	· Records and mobile device management	
Resilient	Crisis management and resiliency	Security operations	Security awareness and training
	· Recover strategy, plans and procedures	· Change management	· Security training
	· Testing and exercising	· Configuration management	· Security awareness
	· Business impact analysis	· Network defense	· Third-party responsibilities
	· Business continuity planning	· Security operations management	
	· Disaster recovery planning	· Security architecture	
SOX (financially relevant systems only)		Penetration and vulnerability testing	BCP/DRP testing

Source: Deloitte, 'Cybersecurity: The changing role of audit committee and internal audit'

The framework in Table 1 aligns with industry standards including National Institute of Standards and Technology (NIST), International Organization for Standardization (ISO), Committee of Sponsoring Organizations (COSO) and Information Technology Infrastructure Library (ITIL).

Conclusion

Technology risks related to cybersecurity and big data occupy the most attention for many boards. Given the risks, however, the number of internal audit departments that are providing internal audit services to their organizations appears to not be at the level it needs to be. The departments that do provide these services are often helping the organization to direct its attention to the critical risk and control issues associated with cybersecurity and big data. The challenge will be for internal audit to ensure it has access to the skills, knowledge, resources, and tools in a dynamic risk environment. Leveraging co-sourcing arrangements by bringing in the appropriate subject matter expertise may prove to be imperative to many internal audit functions going forward.

Steps that will help internal audit progress toward excellence in this area include: The number of internal audit departments that are providing cyber-security and Big data related internal audit services to their organizations appears to not be at the level it needs to be given the risks.

- Fully understanding technology-related risks and their possible impact on the achievement of operational and strategic objectives.
- Leveraging the organization's technology investments to obtain the necessary tools to audit cyber-security and big data.
- Developing necessary internal audit competencies.
- Helping to foster cooperation between technology and business operations.
- Providing a comprehensive suite of technology-related internal audit services, from participation in project management teams to providing technology- related risk management and internal controls assurance to the board.

References

Center for Strategic and International Studies and McAfee, 2014: Net Losses: Estimating the Global Cost of Cybercrime. [https://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf]

Centre for the Study of Financial Innovation (CSFI) and PricewaterhouseCoopers (Pwc): Banking Banana Skins 2015.

[http://www.pwc.com/gx/en/financial-services/pdf/Banking-banana-skins-2015-final.pdf]

Clapper James R 2015. Opening statement to Worldwide Threat Assessment Hearing Senate Armed Services Committee. [https://www.dni.gov/files/documents/SASC_Unclassified_2016_ATA_SFR_FINAL.pdf]

Cloudmark: 2015 Annual Security Threat Report. [https://www.cloudmark.com/en/register/threat-reports/report-annual-2015]

Cucoranu I.C., Parwani A.V., West A.J., Romero-Lauro G., Nauman K., Carter A.B., Balis U.J., Tuthill M.J. & Pantanowitz L. (2013). Privacy and security of patient data in the pathology laboratory. J Pathol Inform, 4:4.

Deloitte: Cybersecurity: The changing role of audit committee and internal audit. [https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-cyber-security-changing-role-in-audit-noexp.pdf]

Deloitte Advisory: Cybersecurity and the role of internal audit. An urgent call to action. [https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-risk-cyber-ia-urgent-call-to-action.pdf]

Ernst and Young: 2016 report "Creating trust in the digital world". [https://webforms.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2015/$FILE/ey-global-information-security-survey-2015.pdf]

FSOC: 2016 Annual Report. [https://www.treasury.gov/initiatives/fsoc/studies-reports/Documents/FSOC%202016%20Annual%20Report.pdf]

Gazet, A. (2008). Comparative analysis of various ransomware virii, J Comput Virol (2010), 77–90.

IIA: PULSE OF INTERNAL AUDIT Navigating an Increasingly Volatile Risk Environment. [http://flbog.edu/about/_doc/cod/igoffice/Pulse-of-Internal-Audit-March-2015.pdf]

IIA: The IIA's 2016 Global Perspectives and Insights: Internal Audit as Trusted Cyber Adviser. [https://www.iia.nl/actualiteit/nieuws/cybersecurity-and-the-role-of-internal-audit]

IIA: Issue 5 Global Perspectives And Insights: Emerging Trends Powered by Global Pulse of Internal Audit

https://global.theiia.org/translations/PublicDocuments/GPI-Emerging-Trends-English-British.pdf

IIARF: CBOK report 2016. [https://na.theiia.org/iiarf/Pages/Common-Body-of-Knowledge-CBOK.aspx]

Kam, H-J. Goel, S. Katertannakul, P. and Hong, S. (2015). Organizational Security Norms in the Banking Industry: The United States vs. South Korea. WISP 2015 Proceedings, Paper 5.

McAfee. McAfee Labs 2016 Threats Predictions. Available at: http://www.mcafee.com/tw/resources/reports/rp-threats-predictions-2016.pdf

Meyer, G 2015. NYSE Owner Warns of Cyber Risk to High-frequency Trading. Financial Times.

PricewaterhouseCoopers: Global State of Information Security Survey, 2015. [http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html]

PricewaterhouseCoopers: The Global State of Information Security, 2008. [http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html]

Subashini, S. & Kavitha, V. (2010). A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications 34, 1–11.

Tendulkar, R. & Naacke, G 2013. Cyber-crime, Securities Markets and Systemic Risk. Working paper no. SWP2/2013. IOSCO Research Department and World Federation of Exchanges.