INTERNAL AUDIT PERSPECTIVES

CYBERSECURITY AND DIGITAL TRUST

IAI
Canada
Montréal

Introduction

Cybersecurity has become a major concern for businesses of all sizes and industries. Cyberattacks can cause significant financial and reputational losses by compromising the confidentiality, integrity, and availability of data.

In this context, the internal audit function can play a key role in helping businesses protect against cybersecurity risks. To learn more about this topic, we interviewed Alexandre Bercovy, who worked in internal audit for several years before taking on the responsibility of integrated risk management in his current company. In this interview, we discussed key elements of cybersecurity and digital trust, the role of internal audit in cybersecurity, and the challenges and opportunities in this critical field.

BIOGRAPHY

Biography

Alexandre Bercovy is an expert in integrated risk management. With 30 years of experience in professional services and operational roles, he focuses on analyzing technological risks. He has served numerous clients in banking, transportation, pharmaceutical, and service industries, leading complex and multinational audit and consulting mandates.

His experience includes addressing technological issues in cybersecurity, implementing the three lines of defense model, identifying and evaluating risks, associated controls and objectives, program and project management, and change management.

He is currently the Director of Integrated Risk Management at Investissement Québec. He is also the ex-officio president of the Montreal chapter of ISACA and holds the titles of Certified Information Systems Auditor (CISA), Certified in the Governance of Enterprise IT (CGEIT), Certified in Risk and Information Systems Control (CRISC), and Certified Data Privacy Solutions Engineer (CDPSE).

Interview

01 Before diving into the subject, I would like to start by defining the key terms and better understanding the conceptual differences between information technology, cybersecurity, and digital trust.

Information technology (IT) refers to the tools, systems, and infrastructure used to collect, store, manage, and exchange information. This includes hardware assets such as computers, servers, routers, disks, storage units, networks, and software such as applications, databases, etc., that provide capabilities for data processing, storage, transportation, and security. IT is essential for the functioning of organizations as it enables data management, process automation, and communication. Nowadays, dependence on IT has become critical.

Cybersecurity, on the other hand, focuses on protecting these information technologies against threats and malicious attacks. It aims to prevent unauthorized access, disruptions, data theft, and damage to computer systems. Cybersecurity involves technical, organizational, and human measures to ensure the confidentiality, integrity, and availability of data and systems.

Finally, digital trust is a broader and more human notion. It concerns the trust we place in digital tools and technologies that are ubiquitous in our daily lives, both professionally and personally.

Digital trust raises questions such as: Can we trust the security of our online transactions? Can we trust the operators to whom we entrust our personal data, whether for social interactions or storing them in the cloud? How can we be sure that our online interactions are authentic and legitimate?

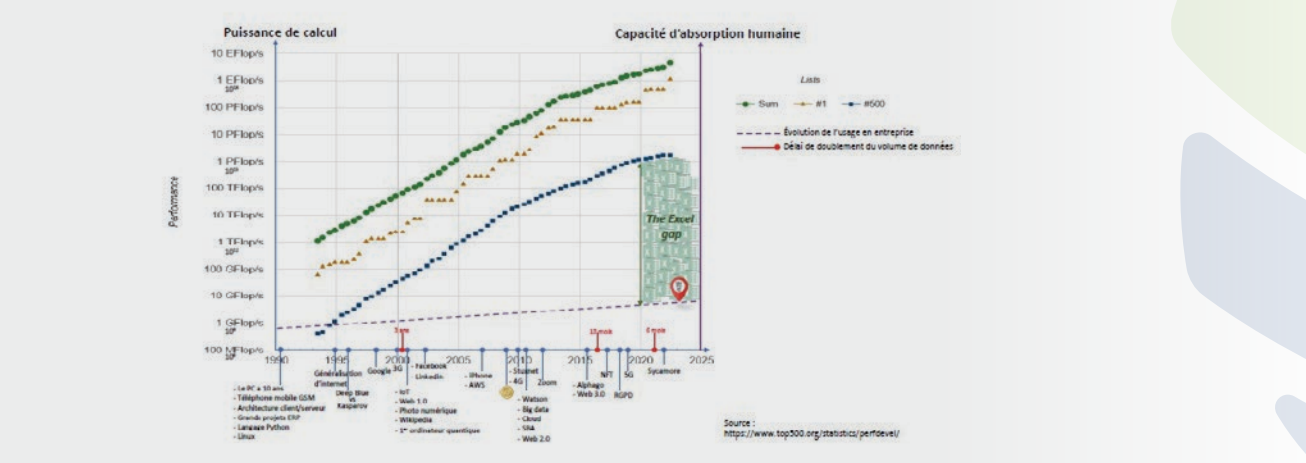
Digital trust encompasses the security of information technologies and goes beyond by including ethical aspects. For example, our data may be well protected by an operator who nevertheless sells it to its business partners. It is about ensuring that our daily online actions are protected and that we can trust the digital services we use by having effective visibility into how our personal data will be treated.

In summary, information technology refers to the tools and systems used to manage information, cybersecurity focuses on protecting these technologies against threats, while digital trust encompasses the trust we place in digital tools and interactions as a whole.

02 What are currently the most significant challenges that businesses face in terms of cybersecurity?

Cybersecurity is an ongoing concern as cyber-attacks have become more frequent (if not daily), sophisticated, and diverse. It is essential to recognize that the question is not whether an object or system will be hacked, but rather when, by whom, how many times, and how it will happen.

The graph below, developed based on public data, explains the gap between technological evolution and human absorption capacity. It highlights the key milestones in cybersecurity and several major challenges related to cybersecurity.



One of the major challenges is targeted cyber-attacks. Companies are constantly targeted by attacks aimed at stealing sensitive data, disrupting operations, or compromising their reputation. These attacks can come from cybercriminal groups, nation-states, or malicious internal agents (employees).

There is also the vulnerability of critical infrastructure, such as power grids, transportation systems, or healthcare services, which are increasingly interconnected and dependent on information technologies. Attacks at this level can have devastating consequences on society. Examples include the attack suffered by the STM in November 2020, the Colonial Pipeline in the United States in 2021, or the disruption of Air Canada planes by fake GPS signals in March 2024.

The emergence of new technologies such as the Internet of Things (IoT), artificial intelligence (AI), and blockchain has created new opportunities but also new challenges in cybersecurity. These technologies introduce new attack vectors and require adapted security measures.

Furthermore, businesses must comply with a growing set of data protection and privacy regulations, such as the General Data Protection Regulation (GDPR) in Europe or Law 25 in Quebec. Non-compliance with these regulations can result in significant financial penalties.

Lastly, I think of employees who are often considered the weakest link in cybersecurity. Companies need to invest in raising awareness and training their staff to help them recognize threats and adopt good security practices. For example, the use of Excel is widespread. However, it is important to note that using Excel does not guarantee increased security for stored data. Specifically, users are not sufficiently aware of the risks associated with sharing Excel files containing sensitive or even confidential data. I do not believe that humans as the weakest link are inevitable, but raising awareness is an ongoing effort.

03 What are the key roles in an organization regarding cybersecurity?

Operations, including IT, and business lines are responsible for implementing security controls and managing risks at the operational level. They are the first actors to face threats and must therefore be aware of risks and good security practices. This includes, for example, protecting infrastructure, raising employee awareness and training, implementing security policies, effective access and authorization management, and monitoring activities to detect security incidents.

Working in collaboration with business lines is key. For example, identity and access management are not, or rarely, a technical topic. It is not IT who decides who has access to what, but rather the operational teams, so the first line. The implementation of these rules, on the other hand, falls under the responsibility of IT. In this context, the second line can - and should - play its role in identifying, assessing, and analyzing cybersecurity risks to provide them to IT teams along with their perspective. It should also test mitigation measures and propose action plans when necessary. This is very close to the audit approach, but with a different positioning.

Governance, risk management, and compliance functions play a crucial role in overseeing and coordinating cybersecurity. These assurance functions establish security policies and procedures, conduct risk assessments and tests, monitor compliance with regulations and security standards, and provide advice and guidance to operations to strengthen the organization's security posture. They also ensure coordination with internal and external stakeholders, including regulatory bodies and business partners.

Internal audit and risk management functions are responsible for the independent assessment of the effectiveness of security controls and cybersecurity governance. Risk management produces frameworks (policies, guidelines, procedures) and identifies mitigation measures (security controls). Internal audit and risk management provide recommendations to improve the organization's security posture. They also play a role in advising and verifying that security measures are adequately designed and effectively operated.

A key success factor is for all these roles to work together. To remain relevant in terms of cybersecurity, training and change management must be fundamental elements, and each actor has a role to play in promoting a security culture within the organization and raising employee awareness of risks and good security practices. Specifically, I believe it is essential for the governance, risk management, and compliance functions to convey this message to operations in their language.

04 Specifically for internal audit functions, how can they prepare to address the challenges of cybersecurity?

The standards have been recently updated. I paraphrase, but audit is now defined as a value vector for the company to achieve its objectives. It bridges the gap between operations and the audit committee to whom it reports. It is a powerful tool that has its legitimacy to participate in significant challenges such as cybersecurity and has a privileged position within the company.

In my opinion, internal audit faces several challenges. First and foremost, it needs to have competent professionals in cybersecurity. This may involve recruiting cybersecurity specialists or providing ongoing training to existing internal auditors to develop their skills in this field. In a competitive market, this is not always easy.

Once equipped with competent staff, internal audit needs to be able to understand and document the complex cybersecurity requirements in order to assess them properly. We can take the example of the Risk Assessment (RA) domain of NIST 800-53. This may require close collaboration with cybersecurity teams and access to detailed information on controls and required or implemented security measures. Only clear and comprehensive documentation can enable internal audit to conduct effective tests and make relevant recommendations.

I also think of timely access to data. Internal audit may encounter obstacles when it comes to accessing the necessary data to assess cybersecurity. Ironically, this can sometimes be due to security rules. However, it is only by analyzing the data that audit can produce accurate results. It is therefore important for the internal audit charter to provide unrestricted access and for it to be applied in practice.

Furthermore, it is important to work closely with operations to understand their security concerns and find solutions that meet both audit recommendations and do not suffocate business sectors. Too much control kills control. Cost-benefit trade-offs must be omnipresent in discussions and decisions. This may include discussions on data protection measures and the establishment of protocols to facilitate secure access to relevant data.

Finally, internal audit must adopt a holistic and comprehensive view of cybersecurity rather than focusing on specific aspects. Understanding current cybersecurity issues and trends is essential for assessing risks, putting them into perspective, and advising on measures to strengthen the organization's security posture. Let's take the concrete example of the average cost of a data breach, which is estimated at $4+ million USD and continues to increase. It is also important to note that cyber insurance companies are becoming increasingly reluctant to insure businesses. These trends highlight the need for organizations to strengthen their security posture and implement effective prevention and protection measures. We should not be resigned or disillusioned, but we need to be realistic. Until the pandemic, ransomware attacks were seen as a matter of money. They are now a business continuity issue, and that changes a lot of things.

In the face of the constantly evolving cybersecurity risks, one must be prepared to act quickly and effectively in the event of an incident. We cannot have definitive opinions, and we are unable to imagine future risks and their magnitude. We need to be agile and know what to do to ensure business continuity. We need to have good reflexes, and that requires training. For all of this, internal audit must be ready to assume an advisory role.

05 I would like to go back to the concept of digital trust. To ensure that I understand it well, could you give me a concrete example?

We could take the example of surge pricing used by some ride-sharing or taxi booking platforms to understand the trust factor beyond technical aspects.

During an exceptional event, such as the London bombings in 2017, crisis management led to a high demand for travel outside dangerous areas. In this situation, traditional taxis responded by offering free rides to help people get to safety. However, Uber's algorithm, which operates on the basis of surge pricing, increased prices due to high demand. The algorithm detected an increase in demand and adjusted prices accordingly, as programmed. This sparked a scandal as users perceived it as exploiting the emergency situation and questioned their trust in Uber.

This example highlights the importance of ethics in digital trust. Users expect companies to take ethical values into account both in everyday situations and during exceptional circumstances.

Another common example of digital trust concerns the use of a VPN. Users trust a VPN provider to protect their privacy by securing their data and masking their IP address. However, there are concerns about whether the VPN provider itself may sell users' data to third parties, which goes against the very service requested. Yet, this is a widespread practice, especially among operators that provide a free service.

To simplify, digital trust manifests itself in situations where users must trust algorithms, platforms, and practices of digital service providers to protect their data and act ethically. The law now requires free and informed consent from users, but in practice, there is still progress to be made.

06 What is the future of risks and controls when thinking in terms of digital trust?

It is very complex and constantly evolving. Regulatory compliance is an important anchor point for creating an ethical framework, but it often lags behind emerging risks. And even so, human nature is constantly balancing between the cost of compliance and the cost of non-compliance penalties. This is the basis of risk management. However, adhering to an ethical framework goes beyond this trade-off as it defines the true values of the company. A recent study has shown that companies that build and adhere to an ethical framework are better valued than those that do not.

A major challenge for the future of controls is the velocity of change. Technological advancements, including artificial intelligence, create new risks. For example, «deepfakes,» which were initially used for humorous videos, are now being used in fraudulent activities, including voice fraud for identification.

We saw a spectacular example of fraud using «deepfakes» during a Teams meeting in Hong Kong in February 2024 (costing $25 million USD). This rapid and unpredictable evolution of technologies makes it difficult to predict what the future will look like in terms of risks and controls.

What we can do is stay up to date with new technologies, cybersecurity trends, and best control practices. It is a period of uncertainty and stimulation.

Internal auditors face significant challenges in supporting organizations in the face of cybersecurity and digital trust issues. These challenges are also accompanied by exciting opportunities to advance the profession and bring value to organizations.

07 To wrap up, do you have any recommended sources of information for internal auditors who would like to delve deeper into what we have discussed?

The Institute of Internal Auditors (IIA) offers a wide range of resources to deepen understanding of cybersecurity concepts. I particularly recommend their new GTAG titled «Auditing Cybersecurity Operations: Prevention and Detection,» which helps auditors better understand cybersecurity control objectives. This guide is essential for enhancing the value of audit and advisory missions and includes complementary resources for further exploration.

IAI Montréal offers various training programs related to cybersecurity, such as «Cybersecurity Audit,» «Financial Compliance Testing to CGTI: How to Navigate the Transition,» and «SOC Reports: Demystifying and Maximizing Their Value.»

ISACA is an international organization focused on governance, risk, and compliance in cybersecurity. They also provide valuable resources for internal auditors. I recommend exploring their website for access to these resources.

Interview conducted by
Maelle Gillet for the Institute of
Internal Auditors – Montreal Chapter

About ISACA

ISACA is an international association that brings together over 150,000 members in 188 countries, with over a thousand professionals in Montreal alone. Its mission is to help organizations leverage information systems to support their strategy and manage technological risks. Our chapter specifically focuses on training professionals, preparing them for international professional certifications offered by ISACA in the areas of governance and control of information systems, including CISA, CRISC, COBIT, ITAF, Val IT, Risk IT, and BMIS. We also provide training in governance, management of information systems, and cybersecurity risk management.

About IAI Montréal

Founded in March 1945, the Institute of Internal Auditors, Montreal Chapter (IAI Montréal), is a non-profit organization incorporated under the Quebec Companies Act. It brings together nearly 900 members and is governed by a board of directors supported by committees.

Our chapter's mission is to support and develop internal audit professionals throughout their careers, as well as promote the role and value of the profession. Our vision is to be recognized as a preferred partner by the business community, ensuring relevance and innovation within the profession.

Our slogan? The ultimate partner for the growth of our members!

IAI
Canada
Montréal