CYBERSECURITY NEXUS

CISO Board Briefing 2017

Insights from the 2016 CISO Forums

ABSTRACT

In 2016, chief information security officers (CISOs) gathered in Las Vegas, London and Singapore for the ISACA annual CISO Forums. They met to tackle issues and share experiences as leaders in their profession. Throughout all discussions, one point was clear: communication between CISOs and business stakeholders is an absolute necessity to ensure the successful mitigation of risk and the security of enterprise data assets. This document presents to enterprise boards and executives high-level summaries of topics covered at the ISACA CISO Forums.

PURPOSE

The purpose of this briefing is to foster improved understanding of information security among boards, executives, CISOs and those in similar roles. Several information security leaders who participated in the CISO Forums agreed to be highlighted in this board briefing. Their testimonials follow each topic summary and are meant to be considered as guidance.

ISACA®
Trust in, and value from, information systems

Introduction

A chief information security officer (CISO) has chosen a role that, for many enterprises, is either new or changing. A senior-level executive with growing cross-functional teams, the CISO remains constantly alert to the state of security. He or she can simplify technical jargon to fit security priorities into overall business strategy. The CISO works with corporate governance players and is driven to enable growth by allowing the enterprise to afford higher risk and manage that risk within an acceptable appetite. But, depending on the enterprise information-security maturity level, a new security-focused culture may not have gained traction quickly, so the CISO is also a salesperson. The CISO's team dedicates itself to protecting the enterprise digital asset confidentiality, integrity and availability. The CISO wants to hire the right people to fill potentially long-standing information security job openings; however, the market lacks talented professionals, so the CISO wants to provide training to those currently employed. This training can also solve the retention problem, as the enterprise loses ambitious employees to the higher-paying competition. Decorated with several technical and managerial certifications, such as the CISM, CISA or CISSP, the CISO likely has an IT audit and risk background and moved to a cyber security role as enterprises made it a priority over the last decade. As a new and rapidly growing enterprise priority, cyber security is an unfamiliar path for the enterprise. The CISO is driven to succeed, and there is so much that he or she is working to change.

This briefing is a summary of observations made at the ISACA annual CISO Forum. In 2016, CISOs gathered in Las Vegas, London and Singapore to tackle issues and share experiences as leaders in their profession. The briefing summarizes the main topics of discussion from the forums and includes direct responses from the CISOs themselves.

Governance

Governance ensures that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives; sets direction through prioritization and decision making; and monitors performance and compliance against agreed-on direction and objectives.

> *"The word governance is derived from the Greek verb κυβερνάω [kubernáo], meaning to steer a ship. Like steering a ship, governance is the act of setting direction and monitoring progress towards the destination. A more complex situation, such as steering an enterprise, requires setting goals, assigning responsibilities, establishing structures, implementing processes and measuring outcomes. The same applies to information security governance and cyber security governance."*

MICHEL LAMBERT
CISO, Québec Ministry of Agriculture, Fisheries and Food

Roles, reporting structures and communication mechanisms are most commonly discussed when the topic of cyber security governance arises. Based on the discussions at the ISACA 2016 CISO Forums, it can be concluded that the success of the cyber security governance structure is determined by the skills of the information security executive, whom the information security executive reports to, and the information and how it is reported. Because of these influencing factors, there is not one correct organizational map, not one universal title and not even one universally applicable job description for the information security executive. Every possible combination has its ups and downs. There is one consideration that tops all others: Is the chosen cyber security governance structure the best option for the enterprise?

> *"The cyber security framework of an organization will depend heavily on the organization's culture, the risk appetite, principles and goals. Of course, the role of the CISO is to build the governance framework, taking into consideration all those aspects and leveraging them to get the necessary buy-in. The cyber security governance has to be coupled with the business strategy."*

RIZWAN JAN
CISO, Henry M. Jackson Foundation for the Advancement of Military Medicine.

▶ What is the ideal reporting structure for most enterprises?

> *"Each organization must identify what is the best for them; just be sure to prevent making the information security function an IT function. In my experience, this has been a bad decision. I would suggest to have the information security function report to the CEO, board of directors or maybe the chief risk officer. This function needs to be independent of IT."*

DOUGLAS BENCOMO
CISO, Maduro & Curiel's Bank N.V. (MCB-Group)

▶ What advice would you give executive teams about creating a governing structure that elevates cyber security priorities?

> *"I would advise executive teams on the fact that cyber security is not an IT issue; it is a business issue that requires enterprisewide buy-in to be managed successfully. IT will certainly be a component of the solution and the success. To be successful, CISOs need to either chair or be a key participant on committees responsible for managing enterprise risk."*

BRIAN NESGODA
SVP & CIO, Sikorsky Credit Union

Cyber security has a history of being a low priority on the list of governing bodies. With the help of the media, cyber security has quickly become a growing concern for many enterprises, giving CISOs a better chance of obtaining the resources and direction necessary to secure their enterprises. Even so, making security a top priority within necessary business processes causes typical concerns: cyber security initiatives will slow down the process, it will cost too much or it is not necessary at this stage. It is the job of the CISOs to use their specialized expertise and knowledge of the business to override these fears with the advantages that security will have on the business goals and objectives—essentially, that security does not benefit the enterprise for security's sake; security benefits the enterprise financial security, reputation, legal state, etc.

> *"Enterprises do not benefit simply just by being secure. That is expected. I hope we can emphasize that advanced cyber security capabilities will allow a company to embrace new business models and initiatives that were previously deemed to be of high risk. Hence, a board that empowers the CISO with adequate resources and support may, in fact, elevate the enterprise's competitive advantages."*

LEONARD ONG
Associate Director, IT Risk Management & Security, Asia Pacific & Japan, Merck & Co, Inc.

What strategies do you use to get buy-in from your board/executive team?

> *"A successful strategy used to gain buy-in from my board/executive team has been to align security initiatives with the organization's strategic goals, illustrating how implementing controls early in a process can reduce the likelihood of future audit findings. Express risk in terms that matter to the board (i.e., losses in units produced, losses in sales, etc.), and not the number of threats blocked or vulnerabilities patched. Leverage internal audit as an ally and collaborate to develop action plans to address risk. Cooperation fosters buy-in."*

BRIAN NESGODA
SVP & CIO, Sikorsky Credit Union

> *"Communication, communication and communication. While decisions are made in the boardroom, it took a lot of effort (outside of the boardroom) to understand each board member's perspective on cyber security, address their communication needs and convince them of necessary cyber security capabilities on an ongoing basis. Boardroom meetings just formalize the decision but are not enough to present and attempt to justify the buy-in required."*

JOHNNY MUNGER
CISO, TCW Group

What advice would you give other CISOs who are having trouble obtaining resources or pushing initiatives forward?

> *"Perform an in-depth and honest current-state analysis, and benchmark against the minimum baseline required by regulations, as well as to other enterprises in the same industry. If we are behind from the minimum required baseline or from other enterprises in the same industry, it is clear that the board would have fiduciary duty to ensure the right resources are provided to bring us to the right level."*

JOHNNY MUNGER
CISO, TCW Group

> *"Partner with departments and show them how they can gain traction on their project by being a part of strengthening the security program. Work with project managers to identify the hurdles and challenges they face in implementing their projects, and use security as a tool to solve those challenges (i.e., develop action plans that bake in security to solve obstacles). Leverage third-party entities like the DHS and the FBI to demonstrate how your organization is proactively improving the security program."*

BRIAN NESGODA
SVP & CIO, Sikorsky Credit Union

Through the progression of this discussion, it became clear that, in addition to a CISO's title, reporting structure and reporting methods, an often-unspoken piece of governance is the skills that a CISO must have. For successful governance, if the CISO has been strategically placed to report the right things to the right people in the right ways, soft skills are the most important skills to have, followed by technical credibility.

> *"On the board/executive levels you can't talk about firewall settings, malware names, etc. On the other hand, this kind of talk is very useful/credible in IT. It is also very helpful if you can establish nonformal relationships with others; it's amazing what you can learn in morning coffee meetings."*
>
> **ANTON BOJANEC**
> *CISO*

> *"Financial skills should be also considered. At the end of the day, a CISO's discussion with the CEO and CFO always prioritizes financial aspects. Understanding them and also being able to be part of the discussion is something I learned to be of high importance."*
>
> **JEAN-FRANÇOIS SIMONS**
> *CISO, Brussels Airlines*

What skills do you use most in your role?

> *"Both soft and technical skills: my soft skills help me to convey my message to a nontechnical audience and to understand the requirements; my technical background supports my translation of business needs into technical language and technical solutions."*
>
> **DOUGLAS BENCOMO**
> *CISO, Maduro & Curiel's Bank N.V. (MCB-Group)*

> *"Soft skills are what I use most in my role. They allow me to connect to people at a personal level and gain a common understanding of the importance of cyber security."*
>
> **RIZWAN JAN**
> *CISO, Henry M. Jackson Foundation for the Advancement of Military Medicine*

What certifications and/or degrees do you hold? Which ones do you find most applicable to your role?

> *"I hold the following certifications: CISA, CISM, CRISC, CGEIT, CISSP, GCCC, GMON, GCIH. I think that CISM and CISSP are the most important; however, I think that in some way or another the knowledge that I have gotten with each one of them has helped me to fulfill my role."*
>
> **DOUGLAS BENCOMO**
> *CISO, Maduro & Curiel's Bank N.V. (MCB-Group)*

> *"CISM, CISA, CRISC, CISSP, ISSMP. The CISM is the most applicable."*
>
> **JOHNNY MUNGER**
> *CISO, TCW Group*

> *"CISSP, CISM, GCIH. CISM is probably the most relevant one to interact with the senior management, while CISSP and GCIH are relevant to understand and interact with the information security technical people."*
>
>
>
> **JEAN-FRANÇOIS SIMONS**
> *CISO, Brussels Airlines*

General governance advice that CISOs give to their boards of directors and executive management consists of the following:

- Incorporate security early in the process.
- Include CISOs in the hiring process of their teams. They require a more advanced and technical assessment of prospective hires.
- The financial cost of security does not outweigh the value of mitigating risk. Risk is a shared responsibility.
- Enterprise priorities should determine reporting structures for CISOs. Often, a CISO's job should not be considered as only an IT function.
- The CISO role is evolving. The CISO is not solely responsible for security, because security is a risk management function that is shared across the enterprise.

Cloud Security

Public cloud almost always involves infrastructure outside of an organizations' direct control. The term cloud was created to describe a paradigm by which business-enabling functionality is transported and stored. Cloud computing is defined by the US National Institute of Standards and Technology (NIST) as, "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[1] It seems that the term cloud is used to simplify the large pool of network resources that a CISO is required to secure and provision.

Many enterprises are transitioning to cloud services, making it necessary for CISOs to build cloud security models. For CISOs whose enterprises rely on cloud service providers, their concern is securing the data over which they could potentially lose control. The management of these cloud services must happen within the enterprise; even when services are completely in the cloud, the risk responsibility is still on the enterprise, and the business units involved are still accountable.

What do most CISOs think about cloud security policy? Many agree that, like most policy, it is useless unless it can be enforced. For many IT departments, cloud security policies fail because other business units acquire their own cloud services with little regard for cloud security. Total transparency into cloud service audit reports and action plans should be given to the CISO, as well as the ability to mandate specific audit items.

What advice would you give to your colleagues or other enterprises on securing their clouds?

> *"Public cloud computing, to be successfully utilized, requires that enterprises, especially CISOs, understand how the business works. Understanding details of workflows and data movement will help assess the risks that need to be managed. Security controls and audit reports for nonrelevant aspects add little value towards protecting your enterprise."*
>
> **PHORAM MEHTA**
> *Head of Information Security-APAC, PayPal Pte Ltd.*

> *"Consider them as the extension of their networks. Make sure to monitor usage and security the same as it's done in-house when they are using PaaS or IaaS. Ensure sound and efficient access control and high privileges access management. Enforce security configuration and hardening. Protect your sensitive data by enforcing encryption. Make sure you have efficient vendor management control and sound exits for the hosted data."*

> **FAIZA KACEM**
> *Senior Director Security Architecture and IAM, National Bank of Canada*

> *"My advice would be to find ways of implementing your existing security policies and controls to the cloud providers and avoid creating separate specific cloud controls and exceptions. This is easier said than done and has spawned a new category of controls: the cloud access security brokers (CASB). They offer a solution at the technical level, but will only be effective if their use is a requirement for implementation, and not seen as something to be circumvented by departments and project managers. Their use can further be ensured, as well as other aspects of cloud security, by a strong vendor management process."*
>
> **BRIAN NESGODA**
> *SVP & CIO, Sikorsky Credit Union*

What do you want your board/executives to understand about the cloud?

> *"The cloud is far from meaning cheaper, highly flexible IT; cloud solutions are IT tools, and the IT department should always be involved in evaluation of solutions; and it is okay to rapidly go for a cloud solution in order to meet business needs, as long as we understand and accept the risks related to the solution."*
>
> **JEAN-FRANÇOIS SIMONS**
> *CISO, Brussels Airlines*

[1] Mell, Peter; Timothy Grance; *The NIST Definition of Cloud Computing*, US National Institute of Standards and Technology (NIST) Special Publication (SP) 800-145, USA, 2011

"First, boards/executives need to prioritize what they want their employees to focus on: managing IT infrastructure or building innovative products. Cloud computing is reaching a stage where businesses really do need to understand and discriminate between technology infrastructure versus engineering. Second, boards need not fear the cloud. In the early years, a lot about how cloud achieved its efficiencies and the compromises, if any, made on the security front were unknown. As standardization and transparency increases, evaluating assets on the cloud becomes much easier."

PHORAM MEHTA
Head of Information Security-APAC,
PayPal Pte Ltd.

"Clouds belong to cloud service providers and hold critical data of the enterprise. There is always a risk to lose control, not only of the critical data, but of the businesses that rely on the cloud infrastructure."

ALEXANDER KHOMKO
Director of Information Security, JS Electronic Moscow

What are your best cloud solutions? What factors do you consider?

"All solutions have their pros and cons. The large-scale solutions, such as AWS or Azure, offer better stability, more geographical distribution, standardized implementation, several tenancy options, scalability, security compliance to industry standards such as SAS 70 and PCI DSS, etc. However, it may be difficult to customize them to specific needs. The choice of cloud provider must be led by the business needs and risk exposure and appetite."

FAIZA KACEM
Senior Director Security Architecture and IAM,
National Bank of Canada

"The best solution saves money on infrastructure while being secure to the required level. I consider the following factors: geographical data center placement, origins of the cloud service stakeholder, certifications, responsibility transfer in agreements, and the service provider's current insurance."

LIUDAS ALISAUSKAS
CISO, Lietuvos Energija

What is your view on encryption?

"It depends on where [encrypted data] is used (in transit, at rest, in memory, etc.), who holds the keys and how they are protected. At minimum, encryption should be used at least when data is in transit and at rest."

ANTON BOJANEC
CISO

"To encrypt all data in the cloud is almost the only way to neutralize the risk of data leakage from the cloud. At the same time, there is high risk to lose it because of improper and unconfident implementation of the encryption policy."

ALEXANDER KHOMKO
Director of Information Security, JS Electronic Moscow

In summary, a CISO's advice to the board of directors on cloud security includes the following:

- The cloud is not one product, but instead it is a network of resources often managed by (often) outside service providers.
- Business units should not acquire new cloud service providers without consulting with the IT department first. Many cloud failures result from doing otherwise.
- Public and hybrid cloud models can erode the borders between inside and outside the enterprise network. Although risk is more flexible and expandable, it should be assessed before implementing any solution.
- CISOs often want to deploy encryption universally, but it is an extremely difficult task, especially for small or medium-sized enterprises.

Annual Priorities

Data presented from Foote Partners, LLC. predicts that enterprises need to be ready to change dramatically to keep up with competition in 2017.[2] The change must do with where and how an enterprise innovates—where they place their bets. Big data is phasing out as an emerging trend in security, but how enterprises use big data intelligently in 2017 will determine their continued success.

How do you identify your priorities for the new year?

> *"We have aligned our cyber practices with the NIST Cybersecurity Framework, following the tier range (1 partial - 4 adaptive; risk management practices). The tier selection process considers our current risk management practices, threat environment, legal and regulatory requirements, business/program objectives, and organizational constraints. We then determine the desired tier, ensuring that the selected level meets our goals, is feasible to implement, and reduces cyber security risk to critical assets and resources to levels acceptable. This assists us in prioritizing our initiatives."*
>
> **RIZWAN JAN**
> *CISO, Henry M. Jackson Foundation for the Advancement of Military Medicine*

> *"I identify our sets of priorities using threat intelligence. Paying attention to what other enterprises in the same sector are experiencing helps to identify what needs to be done on our side to prevent the same issues. We are really paying close attention to the development of new threats and trends."*

> **DOUGLAS BENCOMO**
> *CISO, Maduro & Curiel's Bank N.V. (MCB-Group)*

> *"We look at our enterprise business objectives and corresponding global IT objectives before identifying and prioritizing IT risk management and security divisionwide objectives. It is important that we have a strong alignment according to the best corporate and IT governance practices."*
>
> **LEONARD ONG**
> *Associate Director, IT Risk Management & Security, Asia Pacific & Japan, Merck & Co, Inc.*

What trends do you foresee for the new year?

The explosion of the Internet of Things has presented us with a major cyber security challenge. Connected devices might be small, but they contain complex software that wasn't designed to be connected to the Internet. Where there is Internet connectivity and software, there is exposure. The software on IoT devices—firmware—has not been developed with security in mind, and, therefore, the IoT is essentially an unmanaged invitation for the adversary.

[2] Foote, David, "Cyber Security "People Architecture": The difference between success and failure", Foote Partners, LLC, USA, 18 October 2016

> *"We are also seeing increased consideration of cyber security in regulatory circles. There are mounting calls for regulation of IoT devices, and information related to cyber security events may be considered material information that must be publicly disclosed under SEC regulations. These shifts will introduce a level of transparency that some CISOs may not be comfortable with."*

JUSTINE BONE
CEO, MedSec

> *"Cyberthreat intelligence sharing, threat analysis, cyber security capability (leading indicator) and maturity (lagging indicator), new technologies (virtual reality), back to basics (firmware security, effective monitoring of new threats, etc.)."*

LEONARD ONG
Associate Director, IT Risk Management & Security, Asia Pacific & Japan, Merck & Co, Inc.

> *"Malware (ransomware, etc.); more risks for critical infrastructure; new attack vectors on virtual infrastructure and cloud service providers; enforcement of government requirements and legislation in the field of information security."*

ALEXANDER KHOMKO
Director of Information Security, JS Electronic Moscow

> *"Increase user awareness, enhance data-owner accountability, review/update key security processes (such as incident management and IAM), increase depth and frequency of pen testing, and the full support of new business initiatives."*

MICHEL LAMBERT
CISO, Québec Ministry of Agriculture, Fisheries and Food

▶ How do you encourage innovation in your workplace?

> *"Hire people who are passionate about their work and have different backgrounds and capabilities. This will bring a diverse set of ideas and approaches to solving a problem or bring innovation."*

JOHNNY MUNGER
CISO, TCW Group

> *"We institute innovation as one of our core objective domains every year. It is an official scope of work. There is a process where an innovation idea can be proposed, assessed and funded accordingly. Managers are encouraged to ensure that employees have the bandwidth to ideate and pursue a good idea into proof of concept before full implementation."*

LEONARD ONG
Associate Director, IT Risk Management & Security, Asia Pacific & Japan, Merck & Co, Inc.

The Skills Gap

According to the ISACA report, *State of Cyber Security 2017*, 48 percent of enterprises get fewer than 10 applicants for cyber security positions, and 64 percent say that fewer than half of their cyber security applicants are qualified. To solve this problem, many CISOs point to the need for accelerated cultural change for an array of demographics. For young students, cyber security education needs to start at an early age and needs to be a part of the standard curriculum.

What does the skills gap mean to you, and how do you feel the effects of it?

> *"The lack of expertise and knowledge for cyber security functions either internally or in the hiring market is one of the signs of a skills gap. Another sign is that the educational system does not concentrate on developing skills that are/will be needed to face current and future challenges in the market. Lastly, the resource shortage when trying to hire competencies is a clear presence of a skills gap. The most significant effect is the impossibility to fill open positions with the appropriate skill level, the lengthy duration of job postings, and, most importantly, the changing of the hiring strategy during the job posting in order to better match the market, instead of the other way around."*
>
> **FAIZA KACEM**
> *Senior Director Security Architecture and IAM, National Bank of Canada*

What are you doing to hire and retain the right people?

> *"I am constantly monitoring the HR market (salary and additional benefits) and trying to keep our personnel salary current to the market. Challenging talented people is also necessary."*
>
> **LIUDAS ALISAUSKAS**
> *CISO, Lietuvos Energija*

> *"If someone shows a gap in knowledge, skill or experience that is needed in the near future (for example, passing certifications exams), but, if that individual is loyal in attitude to the company, I would hire this applicant. To retain the right people, you need to make achievable goals for them, rotate responsibilities, encourage training, and stimulate them."*

ALEXANDER KHOMKO
Director of Information Security, JS Electronic Moscow

What do you think we need to do as a society to solve the skills gap?

> *"Start promoting the information security/cyber security field in schools, colleges and universities. Try to make this field attractive. In my case, I am giving the CSX Cybersecurity Fundamentals workshop to university students and young professionals."*
>
> **DOUGLAS BENCOMO**
> *CISO, Maduro & Curiel's Bank N.V. (MCB-Group)*

What should CISOs be doing to fill the skills gap?

> *"Ensure that: (1) lean, yet effective, organizational structure for information security is designed; (2) appropriate funding is planned, meeting requirements based on organization strategy and evolving threat trends; (3) information security and all company personnel are trained continuously; (4) emergency contracts with third-party cyber security experts are in place."*

LIUDAS ALISAUSKAS
CISO, Lietuvos Energija

In summary, a CISO's advice to the board of directors on closing the skills gap includes the following:

- Invest in developing people to increase retention and build much-needed skills; leverage tools to maximize efficiency of the personnel you already have.
- CISOs need to work closely with HR teams to make the most progress in filling job openings and retain the right candidates after they are hired.
- Cyber security professionals often require different benefits than professionals in other business units.
- Support for minority demographics must start at the top of every enterprise.

Vendor Risk Management

Often, the most exciting moments at the CISO forums happened when participants went off topic and discovered critical, underlying issues through the conversations. One topic that was not primarily highlighted in the agenda, but was brought up numerous times in all three countries, was vendor risk management. Whether the cases discussed cloud security, priorities or interdepartmental communications, they all sparked insights and germane discussions about vendor management and supply chain risk management. Some conversations led further into considerations for supply chain risk management. It is clear that CISOs are involved in the risk assessment and mitigation of their enterprise vendors and should continue to be, if not even more so than they are now.

Third-party vendors and business partners can introduce new risk. Furthermore, vulnerabilities can continue to be introduced over the life cycle of a product or service. CISOs and risk management teams need to be involved in the beginning and throughout these life cycles to get to know the vendors and ask the right questions to mitigate risk and assure information security.

What third-party vendor services does your enterprise typically encounter? To what extent are you involved in their procurement?

> *"Services, infrastructures and software/solutions vendors. A vendor risk assessment and security requirements are included in every agreement. The CISO team is involved in the assessment of the security posture of the vendor."*
>
> **FAIZA KACEM**
> *Senior Director Security Architecture and IAM,*
> *National Bank of Canada*

> *"Software as a service (SaaS) vendors are most common and are considered because they offer solutions without the overhead and capex. Vendor management is owned by the risk management department, which provides the benefit of having security-focused staff involved in the evaluation of third-party vendors. SLAs, SSAE 16 reports, contracts, etc. are reviewed, risk rated and reported to a vendor management committee. Issues are identified and ultimately reported to the board of directors, providing further metrics and supporting the enterprise risk management program."*
>
> **BRIAN NESGODA**
> *SVP & CIO, Sikorsky Credit Union*

Do you have a process or policy in place? How would you define the overall purpose of your process/policies?

> *"We have a process and policy in place. We have established specific standards, guidelines and procedures necessary to ensure that any information provided to our third party is kept safe and reduces the risk of unauthorized use, disclosure, modification or destruction, whether accidental or intentional. The amount of due diligence required is specific to the risk associated with the services that the third party performs."*
>
> **RIZWAN JAN**
> *CISO, Henry M. Jackson Foundation for the Advancement of Military Medicine*

> *"Yes, policy and processes are in place. The purpose is to ensure that the third party complies with the corporate information security requirements and that the company resources and data are properly managed, protected and controlled/monitored."*
>
> **FAIZA KACEM**
> *Senior Director Security Architecture and IAM,*
> *National Bank of Canada*

> *"Yes, both a vendor management policy and standard exist that define roles and responsibilities as well as criteria by which the vendors should be evaluated. The purpose is to identify critical vendors to the organization so that they can be appropriately risk assessed and residual risks reported."*
>
> **BRIAN NESGODA**
> *SVP & CIO, Sikorsky Credit Union*

What are your vendor risk management pain points?

> *"Some vendors do not always come through the procurement process and we (security) capture them after the fact. No centralized onboarding process causes us to have an incomplete picture of our risk posture."*
>
> **RIZWAN JAN**
> *CISO, Henry M. Jackson Foundation for the Advancement of Military Medicine*

> *"Vendor relationships change over time and so does the threat landscape based on the industry and geopolitical activities. However, most vendor risk management programs are still an annual exercise. One of the key challenges/priorities for us is to make the vendor risk life cycle a more dynamic and real-time process."*
>
> **PHORAM MEHTA**
> *Head of Information Security-APAC, PayPal Pte Ltd.*

What is necessary to ensure the success of your vendor risk management efforts?

> *"It is necessary to have a central onboarding process when dealing with vendors. Also (along with procurement), legal should be engaged. Cyber security language should be added to any contract language, which is then aligned with the third-party security self-assessment. Legal language should always include the right to audit as well to hold your vendor accountable to the controls they are attesting to."*

> **RIZWAN JAN**
> *CISO, Henry M. Jackson Foundation for the Advancement of Military Medicine*

> *"Training and accountability. Technical solutions can be used but are not necessary. Simple spreadsheets will suffice if a strong vendor management workflow and process exist and are understood by the contract owners. Holding contract owners accountable for their vendors is critical to ensuring risks are identified."*
>
> **BRIAN NESGODA**
> *SVP & CIO, Sikorsky Credit Union*

In summary, a CISO's advice to the board of directors on vendor risk management includes the following:

- Departments procuring vendors should involve information security managers from the beginning and through the vendor's life cycle.
- One centralized onboarding process is an efficient way to mitigate risk.
- Create a vendor risk management program that is dynamic enough to keep up with real-time changes in vendor relationships or the threat landscape.

European Regulations and Compliance

As a champion of personal privacy, the EU is known for having strong regulations around data security and personal privacy. In 2016, the EU passed the Network and Information Security (NIS) Directive to "provide a high-level network and information security throughout EU member states, not just against network breaches by hackers, but also against technical failures and natural disasters."[3] By 2018, companies that fall under the directive's purview are expected to be compliant. In addition to the NIS Directive, there are other new—and not so new—compliance pain points to which CISOs are working toward adherence:

- General Data Protection Regulation (GDPR)
- Payment Services Directive (PSD2)
- Solvency II
- EU Network and Information Security (NIS) Directive
- Corporate governance
- Payment Card Industry Data Security Standard (PCI DSS) v3.2

What are your compliance pain points?

> *"The main pain point of compliance is time. GDPR, Russia's new regulation and China's new privacy law all request to be compliant in a relatively short period of time (EU GDPR being the most flexible one)."*
>
> **JEAN-FRANÇOIS SIMONS**
> *CISO, Brussels Airlines*

> *"GDPR – determining GDPR real requirements in practice, identifying the current gap and implement the minimum necessary steps."*
>
> **ANTON BOJANEC**
> *CISO*

What advice would you give your peers for complying with security regulations for 2017?

> *"Start as soon as possible, get management understanding and active support, involve business areas into activities."*
>
> **ANTON BOJANEC**
> *CISO*

> *"Complying in 2017 is definitively not on my agenda; I'm aiming for 2018! Most important to me is having a clear road map towards compliance so that if you are not able to be compliant on due time, you can report efforts being done so far and ongoing initiatives to reach full compliance (with target dates)."*
>
> **JEAN-FRANÇOIS SIMONS**
> *CISO, Brussels Airlines*

[3] Allison, Peter Ray, "What the EU's cyber security bill means for UK industry," Computer Weekly, USA, January 2016, *http://www.computerweekly.com/feature/What-the-EUs-cyber-security-bill-means-for-UK-industry*

Featured in This Board Briefing

Liudas Aliauskas

CISO

Lietuvos Energija

Douglas Bencomo

CISA, CRISC, CISM, CGEIT, GCCC, GMON, GCIH

CISO

Maduro & Curiel's Bank N.V. (MCB-Group)

Anton Bojanec

CISM, CISSP

CISO

Justine Bone

CEO

MedSec

Rizwan Jan

CISSP, PCIP, CTPRP

CISO

Henry M. Jackson Foundation for the Advancement of Military Medicine

Faiza Kacem

CISM, CRISC, ISO27KLA

Senior Director Security Architecture and IAM

National Bank of Canada

Alexander Khomko

CISM

Director of Information Security

JS Electronic Moscow

Michel Lambert

CISA, CRISC, CISM, CGEIT

CISO

Québec Ministry of Agriculture, Fisheries and Food

Phoram Mehta

CRISC, CISM, CISSP, ISO27K

Head of Information Security-APAC

PayPal Pte Ltd.

Johnny Munger

CISA, CRISC, CISM, CISSP, GWAS, ISSMP

CISO

TCW Group

Brian Nesgoda

CISSP

SVP & CIO

Sikorsky Credit Union

Leonard Ong

CISA, CRISC, CISM, CGEIT, CPP, CFE, PMP, CIPM, CIPT, CISSP, ISSMP-ISSAP, CSSLP, CITBCM, GCIA, GCIH, GSNA, GCFA

Associate Director, IT Risk Management & Security, Asia Pacific & Japan

Merck & Co, Inc

Jean-Francois Simons

CISM

CISO

Brussels Airlines

Trust in, and value from, information systems

3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA

Phone: +1.847.660.5505

Fax: +1.847.253.1755

Support: *support.isaca.org*

Website: *www.isaca.org*

Provide feedback:
www.isaca.org/ciso-board-briefing-2017

Participate in the ISACA Knowledge Center:
www.isaca.org/knowledge-center

Follow ISACA on Twitter:
https://twitter.com/ISACANews

Join ISACA on LinkedIn:
http://linkd.in/ISACAOfficial

Like ISACA on Facebook:
www.facebook.com/ISACAHQ

ISACA®

ISACA (*isaca.org*) helps global professionals lead, adapt and assure trust in an evolving digital world by offering innovative and world-class knowledge, standards, networking, credentialing and career development. Established in 1969, ISACA is a global nonprofit association of 140,000 professionals in 180 countries. ISACA also offers the Cybersecurity Nexus™ (CSX), a holistic cybersecurity resource, and COBIT®, a business framework to govern enterprise technology.

DISCLAIMER

This is an educational resource and is not inclusive of all information that may be needed to assure a successful outcome. Readers should apply their own professional judgment to their specific circumstances.

RESERVATION OF RIGHTS

ACKNOWLEDGMENTS

ISACA would like to recognize:

Expert Reviewer

Michel Lambert,
CISA, CRISC, CISM, CGEIT, Québec Ministry of Agriculture, Fisheries and Food, Canada

ISACA Board of Directors

Christos K. Dimitriadis
Ph.D., CISA, CISM, CRISC, INTRALOT S.A., Greece, International Chair

Theresa Grafenstine
CISA, CGEIT, CRISC, CIA, CGAP, CGMA, CPA, US House of Representatives, USA, Vice-chair

Robert Clyde
CISM, Clyde Consulting LLC, USA, Director

Leonard Ong
CISA, CISM, CGEIT, CRISC, CPP, CFE, PMP, CIPM, CIPT, CISSP ISSMP-ISSAP, CSSLP, CITBCM, GCIA, GCIH, GSNA, GCFA, Merck, Singapore, Director

Andre Pitkowski
CGEIT, CRISC, OCTAVE, CRMA, ISO27kLA, ISO31kLA, APIT Consultoria de Informatica Ltd., Brazil, Director

Eddie Schwartz
CISA, CISM, CISSP-ISSEP, PMP, WhiteOps, USA, Director

Jo Stewart-Rattray
CISA, CISM, CGEIT, CRISC, FACS CP, BRM Holdich, Australia, Director

Tichaona Zororo
CISA, CISM, CGEIT, CRISC, CIA, CRMA, EGIT | Enterprise Governance (Pty) Ltd., South Africa, Director

Zubin Chagpar
CISA, CISM, PMP, Amazon Web Services, UK, Director

Rajaramiyer Venketaramani Raghu
CISA, CRISC, Versatilist Consulting India Pvt. Ltd., India, Director

Jeff Spivey
CRISC, CPP, Security Risk Management Inc., USA, Director

Robert E Stroud
CGEIT, CRISC, Forrester Research, USA, Past Chair

Tony Hayes
CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA, Queensland Government, Australia, Past Chair

Greg Grocholski
CISA, SABIC, Saudi Arabia, Past Chair

Matt Loeb
CGEIT, FASAE, CAE, ISACA, USA, Director

CISO Forums Working Group 2016

Vilius Benetis
CRISC, CGEIT, NRD CS, Lithuania

Justine Bone
MedSec, USA

Thomas Borton
CISA, CRISC, CISM, CISSP, San Francisco Airport, USA

Ken Hendrie
CISA, CRISC, CISM, CGEIT, Cordelta, Australia

Michel Lambert
CISA, CRISC, CISM, CGEIT, Québec Ministry of Agriculture, Fisheries and Food, Canada

Brian Nesgoda
CISSP, Sikorsky Credit Union, USA

Jamie Norton
CISA, CISM, CGEIT, CISSP, NEC, Australia

Rolf von Roessing
CISA, CISM, CGEIT, CISSP, Forfa AG, Switzerland

James Seaman
CRISC, CISM, Croda International