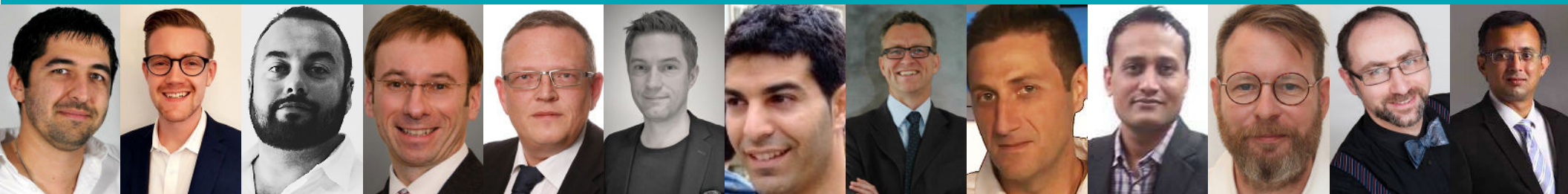
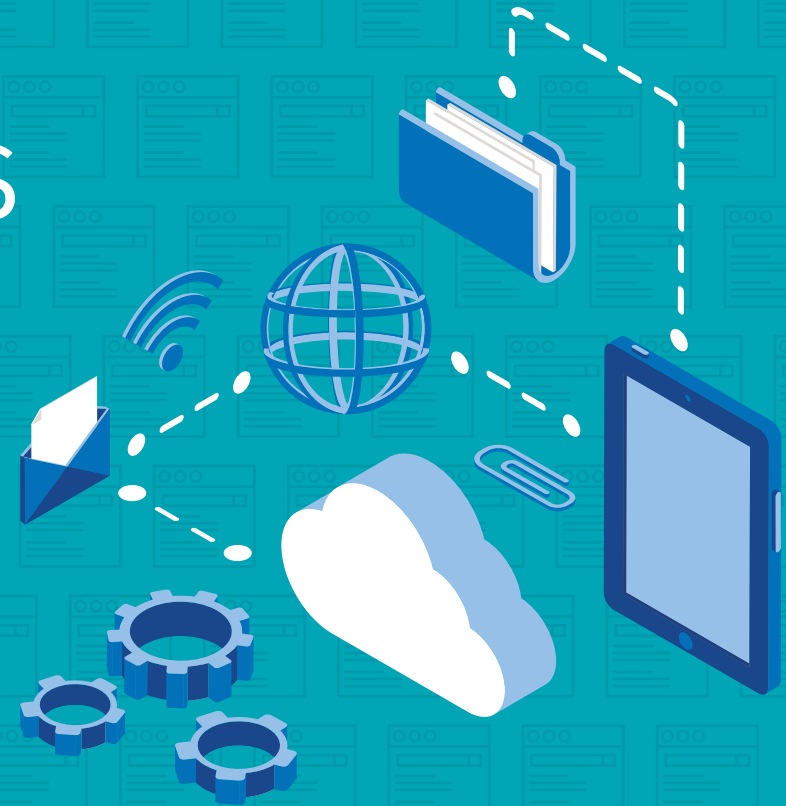


ECONOMIC, OPERATIONAL & STRATEGIC BENEFITS OF SECURITY FRAMEWORK ADOPTION

EMEA Industry Leaders Share Lessons Learned



FOREWORD

Security framework adoption is at an all-time high. According to research jointly sponsored by Tenable and the Center for Internet Security, 80 percent of organizations use one or more security frameworks. Over half the firms surveyed began their framework journey in the past year. Even so, 95 percent of all respondents report tangible benefits, from compliance with regulatory and contractual obligations to improved maturity and effectiveness of security operations.

Whatever the motivation, one thing is clear; basing your security program on an established framework gives you the controls, KPIs and vocabulary needed for building a structured, scalable, and effective practice. To learn more about how this practice plays out in the real world, Tenable collaborated with the team at Mighty Guides to interview 38 InfoSec leaders about the economic, operational and strategic benefits of security framework adoption.

As you read the brief essays in this ebook, you will gain insights from a diverse set of contributors, representing your peers from North America, Europe and Asia. Regardless of their location, industry or company size, these CISOs face the same cyber risk challenges you do: protecting an expanding attack surface from a growing array of threats, while translating the language of security for business leaders who must understand the organization's cyber risk.

Regardless of where you are on the road to security effectiveness, we hope this ebook inspires, motivates and accelerates your framework adoption journey.



Regards,
Brad Pollard
CIO, Tenable, Inc.



About Tenable

Tenable™ is the Cyber Exposure company. Over 23,000 organizations of all sizes around the globe rely on Tenable to manage and measure their modern attack surface to accurately understand and reduce cyber risk. As the creator of Nessus®, Tenable built its platform from the ground up to deeply understand assets, networks and vulnerabilities, extending this knowledge and expertise into Tenable.io™ to deliver the world's first platform to provide live visibility into any asset on any computing platform. Tenable customers include more than 50 percent of the Fortune 500, large government agencies and mid-sized organizations across the private and public sectors.

INTRODUCTION: SECURITY FRAMEWORKS

Not so many years ago, a standard security framework was something that large enterprises implemented. Most small and mid-sized organizations, particularly those in unregulated industries, cobbled together security strategies based on best practices that seemed important to them.

More recently, however, security frameworks have gone mainstream. This is driven in part by the growth of cybercrime, a more demanding regulatory environment, and the increased complexity of the IT infrastructure. With all this newfound enthusiasm for security frameworks, how have businesses actually benefited by adopting them?

With generous support from Tenable, we set out to discover the answers by asking 13 security experts from a wide range of industries and regions around the world the following question:

What are the business and security benefits that come from adopting a security framework?

In our discussions with the experts, we found that benefits relate to motivations for adopting a framework in the first place. Some businesses have legal requirements to show compliance with standards. For them, non-compliance is itself an important risk factor. Many businesses adopt frameworks to prove to their customers they are a safe business partner. But for all of them, the benefits typically run deeper and become embedded in the culture of their operation.

We identified many businesses that take creative approaches to framework adoption, along with some good tips on how to sell management on the need for a framework. And once you win that battle, then the real work begins.

Whether you are considering adopting a framework, or you have already implemented a framework and are facing an ever-changing security and regulatory landscape, I'm sure you will gain useful insights from these experts.



All the best,
David Rogelberg
Editor



Mighty Guides make you stronger.

These authoritative and diverse guides provide a full view of a topic. They help you explore, compare, and contrast a variety of viewpoints so that you can determine what will work best for you. Reading a Mighty Guide is kind of like having your own team of experts. Each heartfelt and sincere piece of advice in this guide sits right next to the contributor's name, biography, and links so that you can learn more about their work. This background information gives you the proper context for each expert's independent perspective.

Credible advice from top experts helps you make strong decisions. Strong decisions make you mighty.

© 2017 Mighty Guides, Inc. | 62 Nassau Drive | Great Neck, NY 11021 | 516-360-2622 | www.mightyguides.com

TABLE OF CONTENTS

Foreword	2
Introduction	3
The Framework Provides a Common Language for a Global Company Eric Bedell.....	5
Framework Benefits Tie Back to Reasons for Framework Adoption Paul Heffernan.....	8
Adapt the Framework to the Business, Not the Business to the Framework Russ Kirby.....	12
Even for Sophisticated Companies, Frameworks Help With Navigation and Priority Setting Daniel Cisowski.....	15
A Framework Enables a Consistent Security Practice in an Extended Global Enterprise Ole Frandsen.....	18
A Framework Can Streamline Vendor Onboarding Tero Lampiluoto.....	21
Security Frameworks Require High-Level Collaboration Oren Ben Shalom.....	25
Frameworks Can Play a Role in Building Customer Confidence and Transparency Erik Blomberg.....	28
The Framework as an Instrument of Change Nir Yizhak.....	31
Security Frameworks Require a Focused, Dedicated Approach Jayesh Patel.....	35

THE FRAMEWORK PROVIDES A COMMON LANGUAGE FOR A GLOBAL COMPANY



**ERIC
BEDELL**
CISO,
MUFG

A passionate information security professional with more than 19 years' experience in the field, Eric has occupied several roles ranging from technician to CISO. His credo is to make the security workable, user-friendly and not business blocking. He built his career mostly in the Luxembourgish bank industry, which has by its nature deep requirements in terms of information security.



LinkedIn

According to Eric Bedell, the greatest benefit of adopting a framework is that it provides a common language for talking to people about your security posture. “It is recognized by the customers and suppliers, partners, regulators, other offices in the company, pretty much everybody, and it provides a line of communication,” says Bedell, who is the chief information security officer (CISO) at Mitsubishi UFJ Financial Group (MUFG), one of the world’s largest financial services companies. Having a common security language is very important to a global company like MUFG, which has operations in more than 50 countries. Although each country has its own standards and regulations, and each region can adopt its own framework, everyone starts with the MUFG corporate standard, which is based on ISO 27001.

One good example of how a framework based on the ISO standard must be modified to meet local compliance requirements is MUFG’s European operations, which need to comply with the European Union’s GDPR (General Data Protection Regulation). “The ISO standard provides good controls to handle the technical side of data protection,” Bedell says. “But when you talk about compliance and the more legal side of GDPR, then you have to build on the ISO controls.”



“ The standard is recognized by the customers and suppliers, partners, regulators, other offices in the company, pretty much everybody, and it provides a line of communication. ”

THE FRAMEWORK PROVIDES A COMMON LANGUAGE FOR A GLOBAL COMPANY

For instance, the GDPR specifies that a company must fill the role of data protection officer (DPO), which is not a role specified in the ISO standard, and there are new processes that must be documented and overseen by the DPO. Those new processes are also not part of the ISO standard. “I will have two hats. In addition to my role in overseeing our corporate security program, I will serve as the DPO for GDPR compliance,” says Bedell.

That means he must maintain the security program based on controls drawn from the ISO standard. But he also has to perform the DPO functions of complying with legal requirements specified by the GDPR, such as how they respond to breaches and communicate with authorities. The DPO will also manage the customer-fulfillment side of the regulation, because based on GDPR, individuals will be able to request whatever data the company holds that relate to them, and individuals may request the deletion of data. In Europe, all of these new processes and functions need to be added to any framework based on the ISO standard.



“
The ISO standard provides good controls to handle the technical side of data protection. But when you talk about the legal side of GDPR, you have to build on the ISO controls.



THE FRAMEWORK PROVIDES A COMMON LANGUAGE FOR A GLOBAL COMPANY

While the GDPR is a legal requirement and a framework for responding to data-related events, ISO provides controls for securing the data. But implementing a framework based on ISO standards requires a lot of consideration. Whether you are a small business that just implements a framework or a very large global organization, you must make choices. “You shouldn’t focus on everything at once,” he recommends. “Start by focusing on goals and data that are most important to you. Review the scope so you can deliver on that. Then afterward, you can expand the scope of your program as needed.” Bedell also says you will need to be flexible in how you implement controls. “You really need to adapt controls to your own environment,” he says. ■

KEY LESSONS

- 1 One example of how a framework based on the ISO standard must be modified to meet local compliance requirements is European operations needing to comply with GDPR.
- 2 When implementing a framework, begin by focusing on goals and data that are most important, deliver on that, and then expand the scope of your program as needed.

FRAMEWORK BENEFITS TIE BACK TO REASONS FOR FRAMEWORK ADOPTION



**PAUL
HEFFERNAN**

Group CISO,
Unipart Group

Paul Heffernan is the group CISO for Unipart Group. With experience in the cybersecurity world, consulting to some of the world's biggest brands, he engages with the business at board level to enable trusted secure commerce. Paul Heffernan is a regular international speaker at conferences such as the e-Crime Congress, GBI CISO Summit, and CISO360 Barcelona. Paul is proud to have been recognized by the Cybersecurity Awards as 'Highly Commended' CISO of the Year 2017.

"We use a range of security frameworks because of the diversity of our business," says Paul Heffernan, chief information security officer (CISO) of Unipart Group, which provides manufacturing, logistics, and consultancy services. "It's complicated because we have a number of different businesses, with operations in Europe, North America, Australia, and Japan, supported by over 7,000 employees." Heffernan explains that not all segments of the business need to operate under strict security regimes. "In some parts of our business, we operate with strict controls, and in others we have a more liberal approach that ensures a baseline standard but does not unnecessarily constrain the business" he says.

Unipart uses the UK Cyber Essentials framework, and also the IASME (Information Assurance for Small and Medium Enterprises) framework, as guidance in its security practices. IASME maps to ISO 27001, and offers a similar level of assurance to the internationally recognised ISO 27001 standard. It is especially designed to help small and medium-sized businesses adopt suitable controls for their operations, which makes it a good standard for enterprises that have complex supply chains made up of smaller vendors. Heffernan uses these frameworks in Unipart's security practices that cover their logistics and manufacturing operations, and also as a foundation for the cybersecurity consultancy that is one of Unipart's business groups. >>>

“The framework allows the customer to have a sense of trust, and that trust turns into business confidence, which turns into more new customers.”



Twitter



| Website



| LinkedIn

FRAMEWORK BENEFITS TIE BACK TO REASONS FOR FRAMEWORK ADOPTION

Heffernan believes the primary business benefit of these frameworks comes from customer assurance. “The framework allows the customer to have a sense of trust, and that trust turns into business confidence, which turns into more new customers,” he says. But it also plays an important role in discussing security with customers. “Cybersecurity is quite complex,” Heffernan says. “Although business customers say they value a company that has strong cybersecurity, in many cases they don’t understand or cannot articulate the specifics of their cybersecurity requirements.” The framework provides a way to hone down this complex issue to something that can be understood and appreciated.

From a security and risk-management perspective, the framework enables you to know what your partners and suppliers are doing in their security practice, and it makes it easier for suppliers to comply with your requirements. This is important if you have a complex supply chain. “For the supplier, they know exactly what they have to do to meet your security standard,” Heffernan explains. “It gives the supplier a to-do list to work through that will give them a tangible benefit.”



“
For the supplier, they know exactly what they have to do to meet your security standard. It gives the supplier a to-do list to work through that will give them a tangible benefit.
”

FRAMEWORK BENEFITS TIE BACK TO REASONS FOR FRAMEWORK ADOPTION

In Heffernan's experience, most businesses implement a framework either because a customer requires them to, or they have decided they need a framework to be competitive in demonstrating that they take security seriously. He also says that although a framework does not necessarily make a business more secure, it can be the basis for a culture of security within the organization, and that will make the operation more secure. "It begins with the very first question, which is why are you implementing a framework? Is it a regulatory requirement? A customer requirement? Is it to drive business? That starts the discussion about how it gets implemented, and how it gets sponsored in the organization. No framework will be successful without board support," he says. If it is taken seriously in the organization and given the proper resources, a security framework starts to become part of the organization's memory.

"Implementing a security framework gives you the control and the insight into how security is actually performing inside the organization so you can quantitatively and qualitatively describe its performance to board members, and ask for further investment," Heffernan concludes. ■

KEY LESSONS

- 1 The framework enables you to know what your partners and suppliers are doing in their security practice, and it makes it easier for suppliers to comply with your requirements.
- 2 If it is taken seriously in the organization and given the proper resources, a security framework starts to become part of the knowledge and systems thinking within the organization.



DANIEL DRESNER

Academic Coordinator for
Cybersecurity,
University of Manchester



Twitter



Website



Blog



LinkedIn



The popular understanding of security tends to ride on the crest of scares and fashions, ranging from regulatory fines to people-are-the-weakest-link slogans. A good risk-based framework (used well)—like the basic ‘Cyber Essentials’ through IASME to the more complex control toolkits from ISACA, ISO, NIST et al.—can build a maintainable and practical environment of resilience to assure information. The benchmark of using a framework well will remain the test of asset protection, business operation, and self-preservation.



ADAPT THE FRAMEWORK TO THE BUSINESS, NOT THE BUSINESS TO THE FRAMEWORK



**RUSS
KIRBY**
CISO,
CreditSafe

Russ Kirby is the Group CISO at Creditsafe, and former head of information security at HPE. Russ is passionate about implementing effective and relevant security into organizations and challenging conventions on how security and compliance are approached.

“I have a love-hate relationship with frameworks,” says Russ Kirby, chief information security officer (CISO) of Creditsafe, an international provider of business credit reports with offices in Europe and North America. “One problem with frameworks is that many are industry specific or preferred in certain industries. Another is they are slow to evolve.” ISO 27001, for instance, was first published in 2005 after years of development. Then it was not revised until 2013, which is its most recent incarnation. Kirby points out that changes in enterprise computing and regulatory environments are outpacing changes in security frameworks.

On the other hand, running a security program without a framework is not practical given the complexities of today’s IT ecosystem and compliance requirements. Having a framework provides specific advantages, such as a more methodical way of viewing and assessing your own security practice. “Once you establish a framework that suits your business and your business model, you gain visibility that enables you to anticipate what will be required for reporting to regulatory bodies,” Kirby says. »»

“ A framework facilitates an understanding of risk within the business, and those understandings allow you to identify the most critical projects that you must have. ”



Website | LinkedIn



ADAPT THE FRAMEWORK TO THE BUSINESS, NOT THE BUSINESS TO THE FRAMEWORK

Frameworks also help internally as you work to implement a security program at an operational level, and to justify priorities. “A framework facilitates an understanding of risk within the business, and those understandings allow you to identify the most critical projects that you must have,” says Kirby.

Kirby stresses the importance of choosing a framework that is flexible enough to adapt to your business. That often means borrowing from different standards and adapting those to an operational framework designed to serve your business objectives. “It’s more difficult to take these hybrid approaches when you have to deal with compliance-based rigorous frameworks like PCI, but overall as a business objective, you need to adopt something that serves your business, rather than hammer your business into a compliance framework,” Kirby comments.

“My strategy has always been to take up relevant aspects from multiple frameworks,” he continues. “We are certified to ISO 27001. We benchmark our business functions to that, and then we add other policies and controls on top of that to meet higher business requirements like GDPR and regulation.”



“
My strategy has always been to take up relevant aspects from multiple frameworks.
”

ADAPT THE FRAMEWORK TO THE BUSINESS, NOT THE BUSINESS TO THE FRAMEWORK

In Kirby's experience, most businesses adopt frameworks to put them in a better position to win business by demonstrating the security of their operations. "I would say 80 percent of adoptions are being driven by sales and marketing, in order to gain more business," says Kirby. Even so, it's important to borrow from standard frameworks and apply their principles in a context that is relevant to your own business. In this way you will establish a more holistic view of your security program, which will improve the maturity of your practice. ■

KEY LESSONS

- 1 Choosing a framework often means borrowing from different standards and adapting those to an operational framework designed to serve your business objectives.
- 2 Adopting a framework that suits your business gives you visibility that enables you to anticipate what will be required for reporting to regulatory bodies.



**DANIEL
CISOWSKI**
CISO,
Vorwerk Group

Daniel Cisowski is a CISO with the Vorwerk Group, a German, internationally successful family enterprise known for its superior household products. He has been in security for more than 10 years, consulting for multinational businesses on security and risk management and helping organizations improve their security maturity. He holds an MA in Computer Science from the University of Kaiserslautern.



LinkedIn

“The more mature a company is, the less dependent it probably is on standards,” says Daniel Cisowski, chief information security officer (CISO) at Vorwerk Group, a large German consumer-products company. “I believe this is because they already know what needs to be done.” However, according to Cisowski, this does not diminish the value of or need for frameworks. “I believe having a framework that you can align to is a very, very good thing—especially for small and medium businesses. They profit from having a framework or a standard that they can use, and frameworks help companies of all sizes to navigate through the security jungle,” he says.

“Frameworks [Vorwerk follows ISO 27000 primarily, and Cisowski has experience with many others] simplify and reduce complexity because they restructure all the areas,” he continues. “You can take out certain sections or certain areas and work on them one at a time, or divide and conquer. By the end, you have covered everything, but in small steps, guided by the framework—this can be very helpful.”

Frameworks also help everyone in the organization and external partners properly identify and communicate risks. “Frameworks give you something everyone can align on and are an appropriate way to assess and communicate risks,” says Cisowski, “and then you can identify and prioritize the appropriate measures to increase security maturity and reduce the residual risk using reusable components.”



“ Frameworks simplify and reduce complexity because they restructure all the areas, so you can take out certain sections or certain areas and work on them one at a time, or divide and conquer. ”

This same adherence to common standards is essential in evaluating suppliers and other providers of critical services. “There is a lot of need to use services outside of our organization, supporting our business,” says Cisowski. These are cloud-based and raise questions about security, he explains. “Having a certain framework that the supplier is certified against helps me and helps our organization understand how our information will be secured. This is really a great help—let’s say our payment service provider complies with the Payment Card Industry Data Security [PCI DSS] standard. Then a lot of questions are already answered and we can reduce our effort assessing the supplier’s security.”

According to Cisowski, thanks to frameworks there is a certain type of “security consensus,” which tends to help all parties focus, communicate with common language, and benefit from reproducibility that may not be possible without the framework. “There is a structure,” he says, “so if you assess certain things or you have to do something multiple times, you can rely on it—it is repeatable.”



“
Frameworks give you something everyone can align on and are an appropriate way to assess risks so then you can identify the appropriate measures to increase the maturity of your security.
”

When it comes to advice about picking a security framework, Cisowski is a bit more philosophical. “I don’t think there is a process for choosing a framework,” he says, “because it’s a very, very high level. Using a framework generalizes a lot and makes it independent of products and services. I believe your experience and knowledge about the frameworks combined with asking the question ‘what do I need to do?’ will help identify the best suited framework. There’s no process or checklist that perfectly matches your needs with a specific framework—I don’t think that something like that exists.” ■

KEY LESSONS

- 1** Mature companies tend to know what they need to do, but frameworks add an element of standardization and discipline that helps bring order and reproducibility to security processes.
- 2** Choosing an appropriate framework requires experience and familiarity combined with a detailed business assessment and consideration of what partners may be doing.



OLE FRANDSEN

Group CISO,
ISS World Services A/S

Ole Frandsen is a CISO with 22 years of experience, the last seven years at C-level. His mission is to embed information security into the very foundation of the companies he works for. He partners with CFOs and CIOs to make sure innovation progresses, with the proper security procedures in place, and enables the business to gain market share, delivering information-security services superior to those of the competitors.



Website | LinkedIn



For a large facilities-management company with operations in 80 countries and over half a million employees, securing infrastructure is a daunting task. Without the right framework, it would not be possible to implement any kind of coherent security strategy across the enterprise. Ole Frandsen, group CISO and head of information security at ISS, has chosen the ISO 27000 family of frameworks as the standard for ISS's security operations. "It is the most used framework in the industries we serve around the world," says Frandsen. "In most cases, our clients use the same framework, which gives them assurance from both a business and security perspective."

Frandsen points out that without a framework, you have no basis for establishing controls in a consistent way across the organization. You also have no way of measuring your security practice against contracts or client requirements, and you can't provide evidence of compliance. "Without a framework, security operations become much more difficult, and in some cases, impractical," he says.



“ Without a framework, security operations become much more difficult, and in some cases, impractical. ”

Frandsen sees several distinct advantages to applying a security framework across a large global organization:

- It simplifies security-related discussions as part of client contracts and service agreements. “When clients ask how we approach security in our systems, we can point to the framework,” says Frandsen. “In most cases they use the same framework, so they can compare our framework with theirs, and they can look at it chapter by chapter to quickly see differences in compliance levels.”
- From an operational perspective, it provides a set of “off-the-shelf” operational controls that they can use to evaluate their own posture. “We can look at the framework controls and ask ourselves if we are doing those things. We can apply a scale indicating the level of maturity for each control,” Frandsen says. Having that maturity measurement makes it much easier to determine where they are in relation to client requirements, and what they must invest to support a client’s service agreement.
- Risk management is important for ISS, whose business activities include facilities management for critical infrastructure, military installations, power plants, financial services, and other critical operations. “It’s an uneven landscape with different security and compliance requirements,” says Frandsen. “We have to understand risks, including penalties, for not living up to certain contractual requirements. With the framework, we can be sure we’re not missing anything.”



“
We have to
understand risks,
including penalties,
for not living up to
certain contractual
requirements. With
the framework, we
can be sure we’re not
missing anything.”

”

When Frandsen joined ISS, they had developed a policy framework that was based on a subset of the ISO standard. His mission was to work with the many businesses under the ISS umbrella to strengthen and mature their security practices, to make sure they were using the right framework and standards. “I was lucky in that we had already started with a subset of the ISO framework. If we had not, I would have begun with the full framework from day one anyway, because so many of our clients already used it,” he says. ■

KEY LESSONS

- 1 Without a framework, you have no basis for establishing controls in a consistent way across an extended enterprise.**
- 2 Having a maturity measurement makes it easier to determine where you are in relation to client requirements, and what you must invest to support a client's service agreement.**

A FRAMEWORK CAN STREAMLINE VENDOR ONBOARDING



TERO LAMPILUOTO

Chief Information
Security Officer,
Outokumpu Oyj


Tero Lampiluoto is CISO for Outokumpu Oyj, a global leader in stainless steel. While leading cybersecurity and IT risk management, he is always seeking a business-driven approach towards security. Before joining Outokumpu, he worked in security consulting providing advisory, improvement, and audit services for many verticals including financial services and Payment Card Industry, retail, telecommunications, online gaming, logistics, and manufacturing.



Website | LinkedIn



“In manufacturing, the industry regulation for cybersecurity is still quite immature” says Tero Lampiluoto, chief information security officer at Outokumpu, a global stainless steel manufacturer headquartered in Finland and with offices in 30 countries. Nevertheless, information security plays an important role in the company’s operations. Lampiluoto points out that Homeland Security considers primary metals manufacturing as part of critical infrastructure. As a publicly traded company, Outokumpu is subject to financial regulation and must also protect personal data, especially sensitive employee data. Lampiluoto says, “I take a business-orientated approach to security. Cybersecurity is not only an IT matter: It must encompass human resources, communications, finance, and other operations across the organization.”

To accomplish those goals, Lampiluoto draws from several standard frameworks, using ISO 27000 as an essential reference. Outokumpu is a member of the Information Security Forum, relying in part on its standard of good practice for information security. The CIS Critical Security Controls by the Center for Internet Security also provide prioritized and practical actions to improve security in any environment. Lampiluoto says that he also refers to ISO 27005 for risk management as well as ISACA’s Control Objectives for Information and Related Technologies framework. “These risk management frameworks give us a range of good practices from different perspectives. Some are higher level and some are more granular,” he says. 

“If you are outsourcing services, whether it’s cloud or other third-party services, security frameworks become great tools for controlling the end-to-end supply chain.”

A FRAMEWORK CAN STREAMLINE VENDOR ONBOARDING

One of the most important benefits of these frameworks for his operation is not having to constantly reinvent the wheel as he adapts the business' security practices to changing operations and different regions. Lampiluoto says, "We're benefiting from good practices, the best practices really, whether it's related to people or processes or technologies. These are practices others have thought through and agreed to."

Another advantage a standard framework provides is that it establishes a common structure, language, and baselines. "It's much easier when you can reference a well-recognized framework and specific controls," explains Lampiluoto. "Even if a company is using some other framework, it can usually map its processes to something like ISO 27000 quite easily."

Having that common language provides many operational advantages. For instance, outsourcing can be complex from a risk management perspective. You need to set an expectation about your own security needs and receive reasonable certainty from the vendor that it can meet your requirements. Lampiluoto says, "If you are outsourcing services, whether it's cloud or other third-party services, security frameworks become great tools for controlling the end-to-end supply chain." In some cases, frameworks can streamline vendor onboarding. "If a vendor can show that they have an ISO 27001 certification, then maybe we don't need to ask them so many security-related questions," he says.



“Frameworks give good guidance and direction, but of course you need to be realistic and definitely not approach security as a checkbox assessment.”

A FRAMEWORK CAN STREAMLINE VENDOR ONBOARDING

Frameworks also serve as a different kind of communication tool for internal discussions related to security strategy. Lampiluoto says, “They provide good metrics and a way to show our overall current state, which is important for deciding where we want to be, our desired target state, and what kind of maturity are we trying to achieve.”

Lampiluoto appreciates that frameworks provide a structured way to approach security practices while giving organizations the flexibility to adapt the practices to their needs. However, that flexibility also leaves open the possibility that a company’s implementation may not be what it should be, which could leave gaps. He says, “Frameworks give good guidance and direction, but of course you need to be realistic and definitely not approach security as a checkbox assessment. When you’re self-evaluating a security practice, you need to be critical of your own work.” ■

KEY LESSONS

- 1 One of the most important benefits for his operation is not having to constantly reinvent the wheel as he adapts the business’ security practices to changing operations and different regions.
- 2 Frameworks give you flexibility to adapt the practices to your own needs, but that leaves open the possibility that your implementation may not be what it should be.



**DANIEL
SEID**
CISO,
Svenska Spel



One of the many benefits with a systematic security framework is quality, or what to be expected from the organization's agreed security controls and deliverables. A certified framework should be preferred, such as ISO 27001 certification, after being audited by an independent third party, including the documented management commitment for the business security. Such certification will serve as proof that the business takes its own, and its customers', security seriously and also result in a business advantage over its non-certified competitors.



SECURITY FRAMEWORKS REQUIRE HIGH-LEVEL COLLABORATION



**OREN BEN
SHALOM**
CISO,
Tel Aviv University

With 10 years of experience in IT systems and information security, Oren Ben Shalom is currently CISO at Israel's Tel Aviv University. His previous positions include information security manager at Shomera Insurance Company and network/systems administrator at payment services company Payoneer. As well as being a team leader and building and implementing long-term projects, Ben Shalom's accomplishments include creating continuous work plans, managing security surveys, and raising awareness of security risk throughout his career.



Website | LinkedIn


According to Oren Ben Shalom, the success of a security framework depends on who is responsible for it within the organization. “When you have a structure that says the chief executive officer [CEO] is responsible for the security framework, the chief information security officer [CISO] should also sit at the C level,” Ben Shalom explains. “Otherwise, the CISO’s voice doesn’t carry enough weight within the company, and security may be overlooked.”

Ben Shalom implemented several security frameworks, such as Payment Card Industry Data Security Standard, Sarbanes-Oxley Act (SOX), and IT General Controls, within a strict regulatory environment while working at an insurance company. Upon learning that Israel’s Ministry of Finance had announced that it was requiring insurance companies to comply with a particular framework such as ITGC, Ben Shalom had to inform his company’s board of the news. After a high-level discussion, the board provided the funding necessary for Ben Shalom to implement the framework. The work continued well after implementation, of course. “I partnered closely with the financial team to implement SOX and review it with them every year,” he explains. >>

“ When you have a structure that says the CEO is responsible for the security framework, the CISO should also sit at the C level. ”

SECURITY FRAMEWORKS REQUIRE HIGH-LEVEL COLLABORATION

Although his company was required to adopt new security frameworks such as ITGC, SOX, or PCI-DSS for compliance purposes, Ben Shalom notes that it was ultimately beneficial both from a top-level business perspective and from the vantage point of his role as CISO. “I had a security steering committee comprising of C-level executives, including the CEO. If I needed to implement a particular framework, I had to come to this steering committee for authorization. So, I presented the procedure, told the committee members that we were required to use it according to our industry regulations, and then I received the necessary funding and buy-in to proceed,” he explains.

In the process of adopting security frameworks at the insurance company, Ben Shalom learned the importance of balancing security with the needs of the business. “When I implement a requirement like this, security has to be set at the right level. At the same time, I cannot make my colleagues’ work more difficult or interfere with their everyday business processes. If I don’t provide them with the right tools, they will find another way to send sensitive data,” he explains. That kind of shadow IT can create even more risks for the business. 

“
I partnered closely with the financial team to implement SOX and review it with them every year.
”

SECURITY FRAMEWORKS REQUIRE HIGH-LEVEL COLLABORATION

Ben Shalom also stresses that although it may be tempting to think of adopting a security framework as a one-time initiative, the reality is that the work is never done. “When you have implemented a security framework and you think that you have finished creating all the tools you need, you shouldn’t sit comfortably and say, ‘Okay, my work is finished. There’s nothing more I have to do,’” he says. Attackers are constantly devising new ways to steal sensitive data, as we saw with the Equifax hack, so you have to be alert and stay up to date on emerging threats.

Although many businesses adopt security frameworks because they must demonstrate compliance with regulations, doing so can ultimately be beneficial from a CISO’s point of view. The business collaborates at a high level to achieve an important goal, but the company gains tools and best practices with which to defend itself against potential attacks in the future, as well. ■

KEY LESSONS

- 1 High-level internal collaboration is necessary for a business to successfully adopt a security framework.
- 2 The work of improving your security is never done. A CISO must always stay up to date on new threats.



**ERIK
BLOMBERG**

**CISO,
Svenska Handelsbanken**

Erik Blomberg is senior vice president and the CISO of Svenska Handelsbanken. He is an experienced leader who specializes in enterprise risk management, business alignment, international coordination, and information and IT-security governance. Erik has worked for 20 years in different management positions in Handelsbanken IT, most recently as head of UK IT. Erik has a master's degree in computer science and worked as a consultant at Capgemini before joining Handelsbanken.

As head of information and security for Handelsbanken, a large Sweden-based financial group operating in multiple countries, Erik Blomberg is familiar with security frameworks. Indeed, the banking sector is one in which both regulation and best practices require adherence to multiple standards. Handelsbanken goes beyond viewing frameworks as must-have protocols to structure internal operations. They also serve as customer-facing tools that help clients understand the security efforts and risks involved in international banking. Blomberg breaks the important role of frameworks into five distinct areas.


The first and most obvious area in which frameworks provide value is that, for many industries, they fulfill legal or industry compliance requirements. “Obviously, regulators expect you to have appropriate frameworks in place,” says Blomberg, “especially in industries like banking.” Because Handelsbanken operates in Sweden, Denmark, the Netherlands, United Kingdom, United States, and other countries, frameworks provide common standards and practices and, depending on each country’s regulations, may also fulfill a direct requirement.



“ We think that communicating about security will, over time, build trust and strengthen our brand—something that will be important in the future. ”

Second, Handelsbanken actively presents framework compliance as a customer offering. “Frameworks are helping us create awareness programs for customers,” says Blomberg. “We believe that our brand is our strength, and so we are generous with the cybersecurity guidance we offer our customers.” Blomberg suggests that Handelsbanken doesn’t directly market security to customers; rather security “has become part of the natural dialogue and communication with our customers, either in customer events or in our day-to-day language and messaging.” Blomberg adds that “we think that communicating about security will, over time, build trust and strengthen our brand—something that will be important in the future.”

Third on Blomberg’s list is the role that frameworks play in product development, which he says is significant. “The framework has to be integrated into the development cycle,” says Blomberg, “either in DevOps or when working with suppliers.” He adds that “it should be integrated transparently, as well, all with the aim of keeping customers happy and confident.”

The fourth area of importance for frameworks is that they can reduce the impact on and cost of cyber incidents. “The framework helps us proactively ensure that we have a robust and reliable infrastructure,” says Blomberg. “Of course, incidents will happen: You must have the mentality that you’re always being targeted for attack. The security framework provides guidance and controls that enable an organization to have a focused and sustainable response to incidents when they happen.” 

“
The security framework provides guidance and controls that enable an organization to have a focused and sustainable response to incidents when they happen.
”

“And the fifth area,” says Blomberg, “is that our frameworks are identifying risks and vulnerabilities in our infrastructure. Those risks are then fed into our normal risk-management governance at the bank and treated the same way as other risks we encounter. Frameworks are a way of identifying risks and making management aware of those risks. We have a risk-based view of things. Sometimes, we might be prepared to take a risk, but mostly we need to mitigate them.”

Each framework provides distinct value, depending on the industry, says Blomberg. For the banking sector, however, it's membership in the Information Security Forum that is top of mind. That member-driven organization, which has close to 500 participating financial institutions, has created standards of good practice—a set of best practices embodying nearly 4,000 rules. These rules and best practices consider many of the country-by-country standards such as International Organization for Standardization, the U.S. National Institute of Standards and Technology, Control Objectives for Information and Related Technologies, and Payment Card Industry. “Each country might have specifics that we then need to treat uniquely,” says Blomberg, “but we have selected the standard good practice of the Information Security Forum as the foundation of our internal information security rules.” ■

KEY LESSONS

- 1** Security practices can become important customer-facing communications, instilling brand confidence and awareness.
- 2** Frameworks provide the foundation for a security strategy that builds on best practices, with added, specific requirements on a country-by-country or industry-specific basis.

THE FRAMEWORK AS AN INSTRUMENT OF CHANGE



**NIR
YIZHAK**

SaaS CISO,
Micro Focus
International plc

Nir Yizhak, chief information security officer at Micro Focus Software as a Service, is a highly experienced information security architect with an extensive background in information security practices and solution development. Other than being a visionary in security strategies, Nir Yizhak is especially interested in compliance and risk management.



LinkedIn

Software as a Service (SaaS) plays a key role in Micro Focus' business model, not only as a method of delivering existing software products but also as a channel for introducing new products and services. With a global customer base that includes some of the world's largest organizations across all industries, Micro Focus must fulfill many security and compliance requirements. Nir Yizhak, chief information security officer for the SaaS organization, says, "One of my challenges comes when we negotiate a deal with a big global customer. That customer may be subject to one set of regulations in Europe, another in Asia Pacific, and another in the United States. We have to adhere to each and every one of our customer's requirements."

Security frameworks play a key role in fulfilling those requirements. Yizhak says that his organization has standardized on ISO 27001 and ISO 27018, but there are cases when it must support SOC Type 2 reporting or Payment Card Industry certification for a specific location. "We are also in the process of analyzing and adapting key technologies and controls to demonstrate compliance with soon to come European Union's General Data Protection Regulation," Yizhak says.



“ When we agree to deliver service levels related to security and compliance, customers inherit our security practices. In turn, we take on some of their risk management and compliance obligations. ”

THE FRAMEWORK AS AN INSTRUMENT OF CHANGE

From Yizhak's perspective, security frameworks provide several benefits, including:

- Building a culture of security. By providing a structured set of guidelines and controls that everyone in the organization agrees are important, the framework enables Yizhak to more effectively manage the security practice. He says, "The framework gives me a tool that I can use to provide security leadership across the entire organization and at all levels, including our senior management."
- Customer assurance. "We utilize well-known and respected security standards to drive our program to ensure the selection and implementation of adequate controls that provide confidence to interested parties. We can point to specific standards and controls to show how we meet a customer's specific requirements. This gives customers confidence in us, which supports our sales team and becomes a business accelerator," says Yizhak.
- Building stronger security. "Regardless of which framework you adopt, it becomes the basis for your risk management workflow," says Yizhak. He explains that this becomes clear as you implement a framework and discover gaps in your practice, but also when the market changes or there are new requirements, such as GDPR. Having a framework in place enables you to adapt with minimal business disruption. He adds, "The framework also gives you better visibility and control over business-related risks, which better protects the company, its assets, and its stakeholders."



"The framework gives me a tool that I can use to provide security leadership across the entire organization and at all levels."

THE FRAMEWORK AS AN INSTRUMENT OF CHANGE

It's not just the business that benefits from adopting a security framework, however. Micro Focus customers benefit too, because the framework helps them meet their own legal and risk management obligations. Yizhak says, "When we expose them to our security statements, policies and processes on incident and change management, and when we agree to deliver service levels related to security and compliance, customers inherit our security practices. In turn, we take on some of their risk management and compliance obligations."

Yizhak also points out the value of applying security frameworks in a modern computing ecosystem. He says, "The world is changing. More and more companies are adopting Platform as a Service and Software as a Service models, which can introduce new threats and a new attack landscape." It is important to establish some kind of framework that integrates security into everything you do, he believes. This includes the development life cycle, the human resources recruitment life cycle, operations, new technology adoption, and the technology lifecycle. "To identify and mitigate risk early, you must have a comprehensive set of security controls that encompass design, review, threat modeling, and testing."

With security embedded into so many aspects of the business, a framework can actually become a tool that facilitates change. Yizhak says, "Maybe it's a new set of regulations that forces operational changes or a new DevOps policy that changes processes and controls. The framework becomes the basis for building in new controls that accommodate these kinds of changes." ■

KEY LESSONS

- 1** It's not just the business that benefits from adopting a security framework. Customers benefit too, because the framework helps them meet their own legal and risk management obligations.
- 2** With security embedded into many aspects of the business, a framework can actually become a tool that facilitates change.



**ANSHUL
SRIVASTAV**

Chief Information Officer
and Digital Officer,
Union Insurance



Twitter



LinkedIn



Adopting a framework gives you the basic hygiene of threat avoidance and a kind of process excellence. But it's up to the organization to implement the framework in day-to-day operations in a way that meets business and security goals.



SECURITY FRAMEWORKS REQUIRE A FOCUSED, DEDICATED APPROACH



**JAYESH
PATEL**

**Head of Information
Security,
Save the Children
International**

Jayesh Patel is a seasoned Information Security professional with experience in managing information security change and transformation initiatives for leading global organizations across different industry segments including banking, oil & gas and speciality chemicals. He has worked both within the consulting sector and within large international InfoSec functions working with IT and non-IT teams across Asia, Africa, Middle East, Europe, and USA. He currently heads the global information security function at one of the biggest non-profit organizations.



LinkedIn

According to Jayesh Patel, every security framework should be closely aligned to the business. “A security framework helps information-security experts achieve their own objectives while also aligning them with business objectives,” he says. As chief information security officer (CISO) at Save the Children International, Patel and his team concentrate on providing cost-effective information-security solutions so that they do not cut into the funding for the organization’s core mission of promoting children’s well-being. Using this approach, they can still provide the essential IT resources to staff who are charged with delivering programs.

With these goals in mind, Patel’s organization has adopted a combination of information-security controls from ISO 27001 as well as the NIST Cybersecurity Framework (CSF). “NIST CSF provides a framework for planning and implementation,” he says. “ISO 27001 provides a methodology for continuous improvement and looks at controls for information protection beyond cybersecurity. That’s why we’ve adopted a mix of both approaches.” Since the nonprofit relies on funding and must work within resource constraints, Patel says, “we can’t have too many things going on at one time and try to address each and every issue at once. So we customized those two frameworks to meet our needs.”



“ A security framework helps information security experts achieve their own objectives while also aligning them with business objectives. ”

SECURITY FRAMEWORKS REQUIRE A FOCUSED, DEDICATED APPROACH

Patel began with limited funding for the first phase of a campaign that addressed defining security practices they would use. “We started with information security training in different languages, and now we are going all-out with that training effort,” he explains. As a result of these efforts, staff has gained a greater understanding of how to defend the organization against the phishing and social-engineering attacks that are on the rise and are one of the reasons behind most information security breaches. “I believe the ability to identify such exploits in the first place will help us keep away from almost 80 percent of the attacks,” he adds. He has since been able to propose targeted funding for a two-year plan to proceed with further phases of security initiatives for the organization.

Given that every business is going through a complete technological transformation, security is an ongoing and evolving challenge. “You see the rise of the cloud, mobile, smartphones, and social media being leveraged by many organizations,” Patel says. Security frameworks are especially important in this changing environment because they allow the organization to develop its business programs effectively and proactively manage the need for information security. For this reason, he says, “businesses that adopt information security frameworks have a competitive advantage over the others that do not.”



“
*Businesses that
adopt information
security frameworks
have a competitive
advantage over the
others that do not.*
”

SECURITY FRAMEWORKS REQUIRE A FOCUSED, DEDICATED APPROACH

At the end of the day, Patel believes, security frameworks are similar to a relationship: you get out what you put in. “If you adopt a security framework and follow it properly, it gives you the ability to put in place effective controls. For me, simply having information security controls in place is not enough. Having those controls be effective is what’s important,” he notes. To be effective, the controls have to be actively integrated, known, and used within and outside of IT environment. They must become an integral part of the business and security practice. Organizations also need to develop measures that will tell them if the controls they are using are improving their security posture. ■

KEY LESSONS

- 1 Security frameworks should always be aligned with the business, particularly when an organization is working with limited resources.
- 2 To be effective, the controls have to be actively integrated and used in the IT environment. They must become an important part of the business and security practice.



Tenable is the pioneer of Cyber Exposure, an emerging discipline for managing and measuring the modern attack surface to accurately understand and reduce cyber risk. Built on the roots of Vulnerability Management designed for traditional IT, Cyber Exposure transforms cybersecurity from identifying bugs and misconfigurations and expanding it to live discovery into every asset in any environment. Cyber Exposure also delivers continuous visibility into where assets are secure versus exposed, and to what extent, and prioritizes remediation based on the asset's business criticality and the severity of the exposure. The adoption of Cyber Exposure will ultimately empower organizations to translate raw security data into a metrics driven program where every business decision factors in Cyber Exposure in the same way as other business risks, to make more proactive and better decisions.

To learn more, visit [Tenable.com/cyber-exposure](https://tenable.com/cyber-exposure)

Learn more about Tenable, our solutions and our global office locations, at www.tenable.com.