tenable™

Mighty Guides

ECONOMIC, OPERATIONAL & STRATEGIC BENEFITS

OF SECURITY FRAMEWORK ADOPTION

CISOs, PMs, and Others Share Success Perspectives and 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.

tenable™

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 midsized 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 30 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

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.

TABLE OF CONTENTS

A SECURITY FRAMEWORK COMBINES SECURITY AND BUSINESS GOALS

In this section...

LESTER GODSEY

Chief Information Security Officer,
City of Mesa, Arizona

Lester Godsey is the CISO for the City of Mesa, AZ. With over 24 years of public-sector IT experience, Lester Godsey has presented at the local, state, and national level on topics ranging from telecommunications to project management to cybersecurity. Lester Godsey has taught at the collegiate level for over 10 years in the areas of technology and project management. A published author, he holds a BA in Music and an MS in Technology from Arizona State University.

LinkedIn

Lester Godsey, chief information security officer (CISO) for the City of Mesa, says there are several distinct benefits to adopting a security framework:

- "A security framework is another way of establishing a baseline of what's acceptable in your organization," says Godsey. And if there's a request for a mitigating control, the framework gives you a context for discussing the value and impact of that control.
- If you don't have a framework in place, then you have no standards. "How can you enforce something that is unclear or people don't understand?" Godsey asks. "For example, when there needs to be an exception, what mitigating controls you are going to put in place to reduce a risk."
- Another benefit of a security framework is that it enables you to have security conversations with other business areas within your organization. "If management requests something that deviates from standards associated with the framework, then the framework is a good starting point for discussing that idea," he comments.

> *"If management requests something that deviates from standards associated with the framework, then the framework is a good starting point for discussing that idea."*

Selecting the right framework for your organization depends a lot on the type of business you are in. Godsey explains: "If you are in healthcare and most of your data is medical records, you will be governed by HIPAA. On the other hand, if you are a global conglomerate with many vertical industries, or if you are a city government, you may need to comply with multiple standards." Most municipal governments need to be PCI compliant, according to Godsey, but they also need to be HIPAA compliant, since the vast majority of calls for service from the fire department are medical in nature and not about actually putting out fires.

When your organization has to comply with multiple regulatory standards, count on having to customize your framework. In fact, most businesses use the framework as a guideline to decide which controls and practices are most important to their business. "Unless you have a very streamlined organization with straightforward needs, in the vast majority of cases you will have to tweak the framework so that it fits your specific business needs," he says.

> *"A good framework gives you the flexibility to adjust your security program to best serve the organization's needs."*

Once you have a framework in place, you can design security metrics that map to the important controls in your framework, a major benefit, because ultimately, the purpose of a security program is to serve the organization's business objectives. This means the security metrics you measure and that map to framework controls are really driven by top-down business considerations. "If a strategic mission is modified or updated, say a new product or service, or a fundamental change in your IT infrastructure, the cybersecurity program needs updating too," Godsey explains. "A mission change should automatically trigger a discussion about the security controls needed to support that mission, and the performance metrics need to validate that you are moving in the right direction from a security perspective."

Of course, all these discussions and determinations are more effective when you have a security framework as your baseline. "A good framework gives you the flexibility to adjust your security program to best serve the organization's needs. It's a process of continual evaluation and adjustment, driven from the top down," he concludes. ■

KEY LESSONS

1 **Most businesses use the framework as a guideline to decide which controls and practices are most important to their business.**

2 **The security metrics you measure and that map to framework controls are really driven by top-down business considerations.**

JEFF WILLIAMS

CTO and Co-Founder,
Contrast Security

Twitter

Website

Blog

LinkedIn

Cybersecurity is insanely complicated. People often compare it to securing houses or cars, but these analogies massively underestimate the challenge. For most organizations, a better analogy is securing an entire city. Think legislature, locks and guards, alarms, fire department, and social services. Adopting and customizing a cybersecurity framework is critical to achieving a balanced program, and can help with identifying gaps, budgeting, executives, etc... But remember, adopting a framework doesn't secure anything—it just helps you get organized.

A FRAMEWORK CAN ALIGN SECURITY OBJECTIVES WITH BUSINESS GOALS

LEE BAILEY

Director, IT Security & Operations,
ABC Fine Wines & Spirits

When he first joined the company in 2014, Lee Bailey formed ABC Wine & Spirits' first IT security organization to address escalating risks associated with Payment Card Industry Data Security Standards. He has served as director, IT security & operations, since 2016. His previous experience includes several security roles at Lockheed Martin, where he contributed to strategic planning and budgeting and managed 15 direct reports. A talented speaker, Lee Bailey has been president of Twilite Toastmasters and area director of Toastmasters District 84.

LinkedIn

In Lee Bailey's experience of having used security frameworks in businesses as varied as defense contracting and retail, one important value of implementing a security framework is growth in the maturity of a security practice. He says, "The framework allows you to go from asking, 'Do we need this?' to 'How do we get there?' and ultimately, 'These are our controls and processes.'" That journey forces you to make decisions about what your greatest risks are and what you need to protect most. "It's not always about putting the right framework in place," Bailey says. "It's about knowing what you're responsible for and making sure everybody in the organization knows what they're supposed to do."

In that respect, a framework makes it possible for security practices to become integral to the business—in the way you make security decisions based on business needs and risk, the way you talk to nontechnical people in the organization about security-related issues and processes, and how you make decisions about security expenditures. Embedding security in business operations enables you to align security benefits with business benefits.

Retailers spend a lot of time creating an experience for their customers, winning customer trust, and wanting customers to feel that the service they receive is excellent. The Payment Card Industry standard mandated by branded credit card issuers plays an important role in preventing the kind of breach that could cause customers, particularly online customers, to lose confidence in the business.

"The framework allows you to go from asking, 'Do we need this?' to 'How do we get there?' and ultimately, 'These are our controls and processes.'"

A FRAMEWORK CAN ALIGN SECURITY OBJECTIVES WITH BUSINESS GOALS

Bailey says, "It's a security framework, but it's also part of taking care of customers. If we don't take care of them and there's a breach, then we lose our credibility, and that can kill the business." If the customer experience is a core part of the business strategy, as it is for many retailers, then the framework becomes a way to align operations with business goals. "It helps drive alignment between the business's objectives and your security objectives," Bailey explains. "Ideally, they are one and the same."

- Securing an IT infrastructure can be a big, nebulous challenge. If you can't quantify what security means to the business, it becomes difficult to prove that whatever money you spend toward securing the business is effective. Bailey says, "Having the framework allows us to connect the dots between the money we invest in security and the return we expect from it. That's a critical part of knowing how best to allocate security resources."
- In many ways, having a framework simplifies budget and funding discussions, as well. Without a framework, you can spend a lot of time justifying an investment, showing why it's necessary, and demonstrating the cost of potential risks. Bailey says, "When everyone has agreed that yes, we are going to conform to a particular security framework, then the conversation shifts to, 'Okay, this is what we need to implement these controls or comply with this regulation.' We need this because it's what we've agreed to." ■

> *"The framework helps drive alignment between the business's objectives and your security objectives. Ideally, they are one and the same."*

KEY LESSONS

1. **Implementing a framework forces you to make decisions about what your greatest risks are and what you need to protect most.**
2. **Embedding security into business operations enables you to align security benefits with business benefits.**

LEE EASON

Director of DevOps,
Ipreo

Lee Eason started his career as a computer programmer. As his responsibilities grew, he learned that the secret of success in software development lies not in taking away responsibilities around infrastructure, monitoring, and deployment, but rather giving teams control and accountability around those areas, and ensuring that they are set up simply and reliably. Lee Eason truly believes that great leaders are servants first, and as a leader at Ipreo he serves his teams by enabling them to own those responsibilities.

Twitter | LinkedIn

Security frameworks are valuable tools for guiding the compliance-standards discussion with customers. Building an efficient way for product development teams to build solutions that comply with those frameworks is key to scaling your application development. If those teams are building for public cloud infrastructure, that becomes even more critical.

Unfortunately, it can be very difficult to simply hand a framework specification to your product development teams and have them be able to digest it. The terminology used can be obtuse and unfamiliar to software development teams, and it is difficult for them to translate a framework into actionable terms. Instead, one strategy gaining traction is the use of an internal development playbook.

Lee Eason, director of DevOps at Ipreo, a leading Financial Technology company serving the largest investment banks in the world, explains that their teams are adopting just such a playbook. "The playbook helps guide our development teams as they craft new solutions. It helps the teams build their solutions with confidence and know that the result of their hard work will be a product the market will accept."

Development playbooks are an opportunity to translate the security frameworks your industry requires you to achieve into an actionable plan for your development teams. Once development is finished, an internal certification process can ensure that the required bar has been hit. Once that has been achieved, the new solution should be able to pass third party certifications with minimal impact to the development team.

> *"We use standard frameworks as reference guides to build our own application development playbook."*

Another good example of how this helps is with something like the patching process. "Our customers are big on this right now because regulators are pressuring them, and they turn to us and say, 'We're required to patch these things within this timeframe. How are you doing it?'" Eason explains.

The team members responsible for rolling out patches have lots of things to consider besides the patching strategy, and they don't necessarily know what the ISO standard says about patching. But the team's approach to patching has been drawn from the ISO standard with help from the InfoSec team and built into the app development playbook. "Now the patching team understands how the patching process works in easy-to-consume terminology they understand," says Eason. "Then our information security team can take that documentation and process, and they can defend it. They can tell customers and regulators how it works and show that it's ISO 27001 compliant."

Eason says that by using the frameworks to build their own app development playbook, organizations are able to separate their internal process from the customer-facing label they need to put on it. They are able to do this in a way that assures compliance standards. ■

> *"Our information security team can take that documentation and process, and they can defend it."*

KEY LESSONS

1. **As more security controls are managed at the app level, developers take on primary responsibility for creating processes that manage those controls.**
2. **The development playbook, based on standards frameworks, presents security standards in a language developers understand.**

DANIEL MEISSLER
Director of Advisory Services,
IOActive

Twitter
Website
Blog
LinkedIn

The benefits of using a security framework mostly center around ensuring that you haven't missed key components of a program, and that you can clearly communicate your efforts to other groups, including peer organizations and auditors.

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.**

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.

Twitter | Website | LinkedIn

"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."*

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.**

LAURA BELL

Founder and CEO,
SafeStack

Twitter

Website

Blog

LinkedIn

Managing security for a large, growing, or innovative organization can be like visiting a restaurant and finding the menu has 500 items. As you stand there trying to decide what to choose, how much to spend... meanwhile the restaurant keeps moving. There are many things we have to manage in security... too many for most organizations to tackle. A framework lets you structure and prioritize so that you can get on with doing security, rather than staring at the menu.

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.**

BUSINESS BENEFITS OF A SECURITY FRAMEWORK

In this section...

A SECURITY FRAMEWORK MAKES THE BUSINESS VIABLE

SCOTT ESTES

Director, Site Reliability, Infrastructure, and Security, Dycom Industries

Scott Estes helps companies transition their traditional, onsite infrastructure and data into distributed cloud-based models that provide enterprise-level security and high availability. He has built and led teams that manage IT assets from single-site data centers to global, multi-site infrastructure. Along with IT security and site reliability, he focuses on building teams that live the DevOps culture required to provide five nines of high availability for the businesses he supports.

LinkedIn

Having most recently served as director of site reliability, DevOps, and security at a major provider of construction services for the telecom industry, Scott Estes comes to the discussion of security frameworks from the perspective of protecting critical infrastructure. He points out that the need for an organized approach to developing and maintaining a security posture is essential for any business. "Without an understanding of what your security posture is, how you're implementing and maintaining it, the entire business is at risk," says Estes. "Someone's going to repeatedly try and disrupt you. If you are considered critical infrastructure, then an effective security posture becomes an existential requirement."

All publicly traded critical infrastructure companies must comply with many regulatory requirements. These include Sarbanes-Oxley and government regulations pertaining to the telecom industry. "Those pass through directly to any businesses providing services to the infrastructure companies. Everyone goes through a quarterly and annual review of their controls and processes to ensure that they are meeting the requirements needed to do business with the telecom groups," says Estes. COBIT and ISO 27000 are two security frameworks that many companies use to help them create their security posture. "These standards provide guidelines for company-created controls and processes, which we can demonstrate complies with those standards," he adds.

> *"Without an understanding of what your security posture is, and how you're implementing and maintaining that, the entire business is at risk."*

A SECURITY FRAMEWORK MAKES THE BUSINESS VIABLE

As an example, Estes explains that there were multiple controls from the ISO 27000 standard his team used as a basis for processes to verify personal information and protect customer data. The processes show how they operationally assure those protections when they set up and tear down offices, and how to handle equipment before and after those operations. "All of that is very tightly managed under those controls," Estes says.

Having the security framework mapped out in this way affords key business advantages. One is that it provides structure for security reporting, whether that involves reporting to customers, quarterly reporting to the board of directors, or reporting to regulators. Another major advantage is that it streamlines a lot of operational activities that have a basis in security practices. "There is less conflict, less confusion about what needs to be done," Estes says. "Field technicians can do their jobs seamlessly without IT getting in the way." He describes this as a "prepare and response" approach. "If you've got your security posture adhering to those two tenets, it makes your depth of operations, from the back office to the middle office to the front office, run more smoothly," he says.

> *"The process of adopting controls to build your security posture is how you actually implement your strategy, and it's how you bring security awareness and value to your organization."*

A SECURITY FRAMEWORK MAKES THE BUSINESS VIABLE

One thing a security framework does not do is make you more secure. “A control is simply that,” Estes says. “All it does is verify that you’re doing what you say you’re doing. The process of adopting those controls to build your security posture is how you actually implement your strategy, and it’s how you bring security awareness and value to your organization.” This is true whether you are implementing a security practice entirely in-house, or whether you are working with third parties. In the case of third parties, such as cloud providers or other infrastructure service providers, the framework becomes a way to communicate your security needs and expectations to the service provider.

KEY LESSONS

1 **The need for an organized approach to developing and maintaining a security posture is essential for any business.**

2 **Mapping security practices to framework controls makes your depth of operations, from the back office to the middle office to the front office, run more smoothly.**

MATTHEW OTWELL

Cyber Solutions Architect,
JACOBS | Cyber Innovation

LinkedIn

In today's world, security and business form a symbiotic relationship. One cannot move forward without the other. By implementing an industry-recognized security framework you are building a security program with a solid foundation that will benefit organizational business units by enabling them to progress without having to circle back to consider security. Security is then 'baked in' to the business processes, allowing them to be more secure, efficient, and cost effective, which in turn can lead to even more funding for security programs and allowing the cycle to continue.

SECURITY FRAMEWORKS MUST SERVE BUSINESS OBJECTIVES

FLOYD FERNANDES

Chief Information Security Officer, A Large Media Organization

Floyd Fernandes is the chief information security officer for a large media organization. He has 20+ years of experience in information technology & information security in a range of industries across financials, software, and telco, having worked across the globe in Fortune 500 organizations. He currently leads the information security strategy for a top media organization's online content network & operations.

LinkedIn

For Floyd Fernandes, vice president and chief information security officer (CISO) at a large media organization, one of the greatest values of a security framework is that it enables him to more strategically bridge the difference between security requirements and business needs. "The industry has historically come from this attitude of 'let's lock everything down,'" Fernandes says. But that is changing. Now businesses and security experts recognize that security must also serve as a business enabler. "You need to take more of a guardrail approach," he says. "This means using some of the frameworks as best practices, but also applying the framework controls that are essential for your business, and using automation to drive many of those controls."

In his current role, Fernandes draws from both the BSIMM Framework and the NIST Cybersecurity Framework. In addition to providing a more holistic view of a security practice, Fernandes finds that frameworks offer guidance that can be applied differently in different situations. If you engage in certain business practices, you must comply with certain security processes. How you do that depends on your physical infrastructure. "Regardless of whether your assets are mobile or in the cloud or onpremises or in virtual containers, you've still got the controls for identity management, vulnerability management, patch management, and encryption.

> *"Use some of the frameworks as best practices, but also apply the framework controls that are essential for your business, and then use automation to drive those controls."*

SECURITY FRAMEWORKS MUST SERVE BUSINESS OBJECTIVES

The security process is the same but the technology changes," says Fernandes. Those technology changes can be tricky, and in some cases, it's not always clear how to interpret the framework in different technical contexts.

For example, there are many unanswered questions with regard to General Data Protection Regulation (GDPR) compliance as it relates to cloud services. The regulation is designed to protect personal data of members of the European Union, and it specifies how that data can be handled and exported. Yet businesses are moving more assets to the cloud, and cloud service providers are global.

"At any given time, you could have an instance sitting anywhere in the world. From a compliance perspective, it might be overseas, which presents a problem if data is not allowed to leave the country," Fernandes says. Considering the global nature of web-based apps, there is uncertainty about what happens when data moves outside of Europe. "The GDPR is becoming a big factor in setting up certain data controls," he adds.

> *"Begin by understanding the requirements you need to meet. Then implement controls and fill in the gaps from a compliance perspective. Always bring in a third party for auditing."*

SECURITY FRAMEWORKS MUST SERVE BUSINESS OBJECTIVES

But ultimately, frameworks serve as guardrails for being secure and compliant in a way that serves business goals. Fernandes believes that to be sure your security strategy is properly serving your business strategy, it's best to rely on your own in-house expertise when adopting and implementing a framework. "In most cases, you know your environment best," he explains. "Begin by understanding the requirements you need to meet. Then implement controls and fill in the gaps from a compliance perspective. Always bring in a third party for auditing." Fernandes advises that unless you are simply turning the management of your security and compliance over to a third party, you need to drive the program and decisions of which frameworks you want to use. A third party may implement a framework more quickly, but you understand your business best, which is the key to having a security program that serves strategic business objectives. ■

KEY LESSONS

1 **One of the greatest values of a security framework is it helps to more strategically bridge the difference between security requirements and business needs.**

2 **A third party may implement a framework more quickly, but you understand your business best. That's the key to having a security program that serves strategic business objectives.**

SECURITY FRAMEWORKS PROVIDE A COMMON LANGUAGE

CURTIS LETSON

Director, IT Operations & Security,
SANS

Curtis Letson is an IT services and security executive with 20 years' experience in delivering solutions within diverse corporate environments. He is a trusted leader and mentor with a focus on team development and improvement to drive quality program success.

LinkedIn

There are many benefits to adopting a security framework, believes Curtis Letson. On the business side, there are the standard replicable processes that you can drive from instant management alerting and overall environment awareness. From a security standpoint, you understand the world you're living in and how to scale up and out from that world because you have that framework to grow out of. "A security framework helps you understand where you are and where you need to be," he says. "It makes it easy to have a conversation with the business because you're both talking about the same thing."

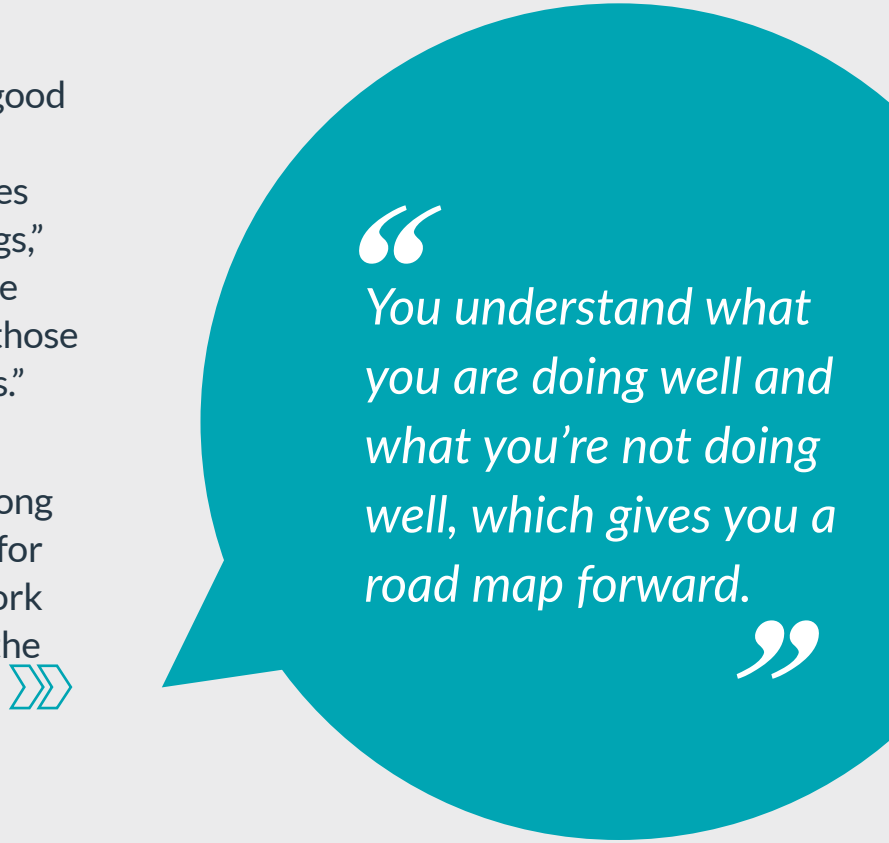
In Letson's view, this common frame of reference that a security framework provides is also useful when engaging with potential clients. "For instance, if I'm in the private sector and I'm selling an offering to a healthcare company, if I don't have a security framework that I follow for my own business, it makes it harder for me to speak the same language as my customers," he explains. "On the other hand, if I go to the government and I say, 'Hey, I'd like to sell you this product that I have and oh by the way, I'm NIST 800-53 compliant,' then they'll say, 'Oh, great. I understand what that means.'"

> *"A security framework helps you understand where you are and where you need to be."*

SECURITY FRAMEWORKS PROVIDE A COMMON LANGUAGE

Businesses that adopt a security framework can also evaluate their effectiveness in improving their security practices. "If you're doing a good job of complying with the standard, doing replicable assessment and analysis on how you're implementing the controls, and making changes when you need to, it gives you a very good understanding of two things," says Letson. "You understand what you are doing well and what you're not doing well, which gives you a road map forward. You can then fix those things you're not doing well and continue to scale out for the business."

For this reason, a security framework may also be able to help the business obtain additional funding for its cybersecurity program. Among the frameworks in use today, Letson notes that CIS Controls (Center for Internet Security Critical Controls) and NIST Cybersecurity Framework are often particularly worth considering depending on the nature of the business and the industry in which it operates.



SECURITY FRAMEWORKS PROVIDE A COMMON LANGUAGE

As we've seen, a security framework can offer your company multiple business and security benefits. It provides a road map for creating standardized operational processes for managing security within an organization, highlighting successful areas as well as specific aspects of security that need to be improved. A security framework also improves communication by providing a common frame of reference that is especially useful for discussions with internal leadership as well as potential clients. In this way, a business can enhance its security effectiveness while simultaneously boosting its business prospects. ■

KEY LESSONS

1 **A security framework provides a common frame of reference that is valuable for conversations with leadership as well as potential clients.**

2 **A business can leverage a security framework to understand its current environment and continually enhance its own security processes.**

DAVE SHACKLEFORD
CEO,
Voodoo Security, LLC

Twitter
Website
Blog
LinkedIn

Adopting a security framework may provide structure and measurable goals and metrics to a security program. While no framework is a guarantee, taking an ad hoc approach to building a security architecture and controls model will likely lead to an immature program in the long run.

CHAD LORENC

Senior Security Architect, Keysight Technologies

Chad Lorenc is a passionate security professional with broad experience. He's been a Cisco pre-sales engineer, large credit union ISO, Fortune 500 security architect, managed his own ISP, run his own security consulting company, been president of an ISC chapter, and deployed security solutions all over the world. However, he's more likely to talk to you about his time working in inner-city Denver or the 3-month sabbatical he took with his family to do humanitarian work in Haiti, where he trained locals in IT security.

LinkedIn

As a supplier of products and services to a wide range of industries and manufacturers, Keysight Technologies must demonstrate compliance with the standards its customers and partners require. To that end, it must show compliance with many frameworks. "We use ISO 27000 as a broad standard," says senior infrastructure security architect Chad Lorenc. "As a collection of security best practices that have been tested over time, it covers most of our requirements." However other customers have other requirements, so Lorenc must also show compliance with Payment Card Industry (PCI), Defense Federal Acquisition Regulation Supplement (DFARS), Personally Identifiable Information (PII) Security Policies, and other requirements.

The segmented approach Keysight has taken in its security strategy simplifies the process of compliance with many standards. "We use both a risk-based segmentation, where you put all your high-risk, medium-risk, and low-risk things together in their own groups, and functional segmentation, where you isolate functional groups down to the app level," says Lorenc. This enables the company to create an operational security matrix that lays low-, medium-, and high-risk "columns" over "rows" of traditional functions such as admin, tools, apps, database, web, and other categories. Each cell in this matrix becomes a "container" or zone with its own controls and security configurations. Activities happening in one container cannot leave that container.

> *"We can now quickly configure and provision a partner's security requirements by simply assigning their resources to an appropriate zone."*

"We can now quickly configure and provision a partner's security requirements by simply assigning their resources to an appropriate zone," Lorenc adds. "Once you're assigned to a zone, you get built into that zone, and you automatically inherit all the controls for that zone."

By overlaying specific controls on this security matrix, Keysight is able to use this segmentation approach to map security framework standards to specific risk zones. "If we have a customer with specific compliance requirements, such as PCI, we can assign them to a high-risk zone that is PCI-compliant," explains Lorenc. "If their compliance requirements are less demanding, we can provision them to a medium- or low-risk zone." The segmentation strategy also enables Keysight to build custom protections that are required by some customers.

Lorenc says that as they developed their segmentation strategy, they knew what kind of controls they needed for their risk- and function-based segments. They didn't need ISO 27000 to tell them what controls to build into their security matrix. "Using segmentation, you very quickly find that you can pretty easily define the controls or show how they overlay the zones," says Lorenc. "Once we built our secure data center using our segmentation model, we were able to use ISO to show others how we are meeting those security objectives."

"Once we built our secure data center using our segmentation model, we were able to use ISO to show others how we are meeting those security objectives."

KEY LESSONS

1. **Compliance with many standards is simplified by using a segmented security strategy.**
2. **Each cell in the segmented security matrix becomes a "container" or zone with its own controls and security configurations.**

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.**

BEN CHUNG

Chief Information Security Officer,
NTT Communications ICT Solutions

Twitter

Website

LinkedIn

"A security framework can be invaluable in providing a structured and consistent way of thinking about the protection of your organization.

For many organizations starting out on their journey to securing their organization and maturing their capabilities, a reliable and tested reference for thinking about their environment is an important road map.

For the emerging security department this adoption can help build trust in the security group and more importantly, for the business to build trust for the community."

FRAMEWORKS PROVIDE MANY BENEFITS, BUT IMPLEMENTATION IS KEY

AVINASH TIWARI

Senior Manager, Information Security,
A United States–based Financial Services Company

Avinash Tiwari is an information security and privacy professional whose career reflects his extensive experience in India, the United States, the United Kingdom, and France in banking, financial services, and insurance companies. His strong leadership qualifications are coupled with his sound knowledge of information security and hands-on expertise in risk governance, IT controls, application security, and user access management.

LinkedIn

Avinash Tiwari, who oversees information security and risk management at a financial services company based in the United States, says, "People are benefiting from several standard frameworks in the market today. If you are implementing a framework, there's no need to reinvent the wheel."

He speaks from his own experience over many years of working in security environments without a standard framework, convincing an organization to adopt one, and then successfully implementing it. Tiwari has worked with many frameworks, including ISO 27001, the National Institute of Standards and Technology (NIST) 800 series, and the Control Objectives for Information and Related Technologies (COBIT).

In his experience, organizations benefit in many ways from adopting and implementing a framework:

- Any framework helps an organization identify essential practices, implement them, and improve its overall security operation. Part of this comes from creating a common security language. Tiwari says, "If I want to communicate something internally, I know what should be communicated because we are following a standard. Similarly, if we are following a standard recognized outside the organization, everyone understands what they must do."

> *"With a framework, you can industrialize security governance across the entire organization."*

FRAMEWORKS PROVIDE MANY BENEFITS, BUT IMPLEMENTATION IS KEY

- A framework helps industrialize security governance and standard procedures. “It should not be that each person or each team or each vertical business line uses its own practices,” says Tiwari. “With a framework, you can industrialize security governance across the entire organization.”
- By providing a standard against which you can measure, a framework enables a more scientific approach to security governance. Tiwari says, “With a framework, you can be quantitative. You can use data to convince people why they should do something one way and not another. That’s the scientific way.”
- The framework provides a better understanding of all the risks a business faces. “Frameworks help a business have more transparent, accountable operations,” says Tiwari. “These are known risks and practices that many people have documented and tested.”

However, Tiwari emphasizes that realizing these benefits depends on effective implementation, which is not always so easy. He cites his experience at a company that was operating with security guidelines that varied from one geographic region to another. Over time, the business realized that it was spending money on security in each division and would be better off combining all the security expenditures into one budget that funded an enterprise-wide strategy. When it came to adopting a framework, however, there was resistance. Tiwari describes how the argument went. “We had built a bigger team, but when we presented the initial requirement, management said ‘No. Our main priority should be to earn money for the business, not to pay for a security standard. IT is a cost center, not a profit center.’”

> *“I can say I follow ISO or NIST or the SANS Institute or COBIT. But how thoroughly and effectively am I really doing it? We have to bring these things together.”*

Eventually, Tiwari and his team were able to convince management of the importance and value of implementing a standard, and they won their budget. Then, the real work began. Tiwari explains, "Guidelines were in place, but they didn't properly map to any standard. Our first job was a mapping exercise. We used International Organization for Standardization (ISO), COBIT, and NIST standards to map our controls to framework controls." He and his team started with 37 controls; by the time they were finished, they had a list of 90 controls they needed to apply in the organization.

The next job was implementing the controls. Tiwari says, "We divided those controls across three implementation phases. It took us three years to push everything out."

Tiwari says that implementing a framework is a balancing act between documenting your use of standard controls and using them effectively. "I can say I follow ISO or NIST or the SANS Institute or COBIT," he says. "But, how thoroughly and effectively am I really doing it? We have to bring these things together." ■

KEY LESSONS

1. **By providing a standard against which you can measure, a framework enables a more scientific approach to security governance.**
2. **Realizing the benefits of a standard framework depends on effective implementation, which is not always so easy.**

SECURITY BENEFITS OF A SECURITY FRAMEWORK

In this section...

JOSHUA DANIELSON

CISO,
Copart

With a decade of experience in both the public and private sector, Josh Danielson has served in a variety of industries throughout his security career, from academia and government contracting to the financial sector. Josh has an MS degree in Information Management from Syracuse University, and currently holds multiple certifications including CISSP-ISSAP and CISM.

Twitter | LinkedIn

With a large portion of its revenue-generating activities directly tied to online processes, Copart depends on an IT infrastructure that is perfectly adapted to its needs. "For us, it's all about availability and reliability, because that's critical to the business," says Joshua Danielson, the chief information security officer (CISO) at Copart. When he joined the company, which is a provider of online vehicle auction and remarketing services, it had an effective security program that was adequately serving the IT infrastructure, but part of the challenge was justifying it to non-technical business stakeholders. "There's no way you can throw a 50-page security program document at the C-level folks and expect them to absorb it," he says.

One thing Danielson did was to revamp executive-level security reporting. He did that by using the NIST Cybersecurity Framework as a starting point and adapting its controls to suit the Copart organization. "We use the NIST Cybersecurity Framework because of its adaptability, which made it easier for us to describe our program from the data-center level to the boardroom level," he says. He also overlaid Carnegie Mellon University's Capability Maturity Model Integration (CMMI) to rate the maturity of a key aspect of their practice on a scale of one to five. "With the CMMI, it's very clear as far as what managed and developing mean. So it provides a much more defined structure," Danielson explains.

> *"It gives you a basis for describing the same risk whether you are talking to IT people or boardroom decision makers."*

Danielson says the security practice has realized several key benefits from applying the NIST framework to their program:

- Its principal value is that it enables you to build a process for making cyber risk decisions based on a collective body of knowledge. "It gives you a basis for describing the same risk whether you are talking to IT people or boardroom decision makers."
- He believes that working from an industry standard security framework not only helps defend your practice within the organization, but can also provide legal cover in the event the organization is challenged on a security-related matter. "It provides a baseline, based on a standard used by many organizations in many industries, that you can use to show how you know you're managing risk."
- Danielson also says using the framework as a guide when reviewing your practices gives you a broader perspective. "When it comes to managing security, you often find that people really aren't as objective as they think they are, and they can overlook things," he says. "NIST pulls together the best security knowledge into one document. This collective knowledge is deeper than even the smartest person on your team."

"NIST pulls together the best security knowledge into one document. This collective knowledge is deeper than even the smartest person on your team."

Danielson believes that one of the key elements in selecting a security framework is its ability to adapt to the business at hand. Flexibility is important. For instance, some controls in the framework may not be relevant, and you may want to strengthen others. "There are references to industrial control systems and critical infrastructures that we don't need, so we leave them out of our program," he says. "But I feel the current version of NIST lacks some controls around authentication, so we added them in ourselves." ■

KEY LESSONS

1 **A security framework enables you to build a process for making cyber risk decisions based on a collective body of knowledge.**

2 **One of the key elements in selecting a security framework is its ability to adapt to the business at hand. Flexibility is important.**

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.

FRAMEWORKS STRENGTHEN A COLLABORATIVE SECURITY PROCESS

CARLOS LERMA

Sr. Information Security Architect, Beam Suntory Inc.

Carlos F. Lerma is a senior information security architect at Beam Suntory Inc, based in Chicago, IL. He holds a bachelor's degree in Accounting from Universidad Autónoma de Tamaulipas (Ciudad Victoria, Mexico) and an MS in Telecommunications and Network Management from Syracuse University. His research interests are cyberintelligence, threat management, SIEM systems, and strategic intelligence in InfoSec management. The rest of his spare time is spent playing beer-league softball and as lead singer for the metal cover band "The Fat Vampires."

LinkedIn

As one of the fastest-growing spirits companies in the world, Beam Suntory's IT infrastructure has been in transition in recent years, and so has its security strategy. "Growth has been the big driving force," says Carlos Lerma, the company's senior information security architect. "We need to be able to think more broadly and be more nimble in how we apply technology. That's the main reason we are trying to do so much so quickly."

Part of the changing IT security strategy includes adopting a framework to help manage the growing challenges that come from having an increasingly complex infrastructure. "We're currently going through a security assessment by an external firm. Our goal is to use that assessment to adapt our security processes to something we can manage through a framework like NIST 800-53 or ISO 27001:2013," Lerma says.

Lerma and his boss, Justin Metallo, Beam Suntory's Senior Manager - Information Security, have been champions of a collaborative security practice where IT managers, business decision makers, and security are engaged in the process. "We try to engage every single business stakeholder, from the application owners and platform administrators, to leadership," he says. "For things like vulnerability management in the platform, we understand what the main business drivers are."

> *"We try to engage every single business stakeholder, from the application owners and platform administrators, to leadership, so we understand what the main business drivers are."*

In that way, security enables everyone to do their work while providing them with the necessary tools that work in the background. To do this, Lerma depends on good relationships and input from IT system administrators and business managers. "Why do we do this? Because, I've always believed they know more than us about what the infrastructure is and what it needs to do. They will always know more, because they live and breathe the infrastructure 24/7," he says. With this collaborative approach to security, Lerma can take cues from business and IT managers when deciding how the company should manage vulnerability, what is the best way to categorize and prioritize vulnerabilities, and how best to remedy them.

Lerma believes adopting a security framework and building an effective road map that is aligned with business objectives will strengthen this collaborative approach to securing Beam Suntory's growing IT infrastructure. "The assessment we are currently doing will give us security objectives that we will map into business objectives," he says. "Then we'll use the framework and our road map to describe security objectives, areas where we need to improve, defenses we need to strengthen, and things we need to monitor more closely."

> *"Our goal is to use the assessment to adapt our security processes to something we can manage through a framework like NIST 800-53 or ISO 27001:2013."*

FRAMEWORKS STRENGTHEN A COLLABORATIVE SECURITY PROCESS

Lerma's role as information security architect is to provide IT managers with the security they need to run the infrastructure properly. He says, "What I've been doing ever since I took over this position is to get them involved in the design process, to include them in a very immersive way, so they can actually get their hands dirty and understand what security is and how it ties to their own objectives." Adopting a framework and road map will be another step along that path, an important one that must be taken as the company and the IT infrastructure grow. ■

KEY LESSONS

1 **Adopting a security framework and roadmap helps manage the growing security challenges that come from having an increasingly complex infrastructure.**

2 **The adoption of a framework and a roadmap strengthens a collaborative security process in which business and IT managers contribute to decisions about how the company should manage risk derived from IT Security.**

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.**

CHRIS WYSOPAL
CTO,
CA Veracode

Twitter
Website
Blog
LinkedIn

For too long security was an afterthought—reactive, not proactive—but large-scale breaches and attacks have pushed security into the spotlight. However, many companies are still overwhelmed by all that needs to be done. Security frameworks can help them prioritize their efforts around the most impactful activities. But in today's ultra-competitive global economy these policies can't interfere with innovation.

FRAMEWORKS PROVIDE AN EXCELLENT WAY TO UNDERSTAND RISK

GARY HAYSLIP

VP, Chief Information Security Officer, Webroot

Gary Hayslip is chief information security officer at Webroot. He is responsible for the development and implementation of all information security strategies, including Webroot's security standards, procedures, and internal controls. Previously, he was CISO of the City of San Diego, and held various CISO roles with the U.S. Navy (Active Duty) and US Federal Government. In these positions, Gary founded security programs, audited large disparate networks, and consolidated legacy infrastructure into converged virtualized data centers.

Twitter | Website | Blog | LinkedIn

A practical approach to security, according to Gary Hayslip, chief information security officer and vice president of Webroot, is first to understand and quantify risk. "To me, frameworks are just a way to understand your risks," he says, "because you must have a place to start. What do you actually have? What's important? What are you doing that's good? What are you doing that you probably need to change? Are you totally missing things? Many times, you don't know until you start asking questions. The typical driver of such questions is someone who has made a conscious decision to follow some type of best practice, a framework. Every framework I've used in the cyber domain has focused on answering two questions: How much risk do we have, and what's the impact to the business?"

In its own implementation of ISO 27001, Webroot is discovering that questions matter a great deal. "We started working with our DevOps teams," says Hayslip. "We started working with our network teams, with my information security team. You start to ask a lot of core questions, such as 'Where is all our data? What type of data do we have? Who has access to the data? With which third parties do we have contracts? From a data governance perspective, what are those parties doing?'

> *"Every framework I've used in the cyber domain has focused on answering two questions: How much risk do we have, and what's the impact to the business?"*

To answer such questions, says Hayslip, companies must prioritize: Doing everything at once is rarely possible. "When you follow a framework, you start asking these questions. The answers give you the idea that yes, there is risk here. Now, how do we want to handle it? Here are all the pieces: Let's prioritize them. What is critical that we must protect lest it significantly affect the business? These pieces here? Okay, let's focus on those first. What resources do we need? Do we need people? Contractors? Professional services? Should we purchase some type of technology? Do we just need to make changes in our business processes?"

Frameworks also provide a structure for which steps to take and when. "Often, when I talk to business unit stakeholders in my company," says Hayslip, "I explain to them that we're not just doing this for the fun of it. We're doing this because we've selected a specific framework, a specific best practice, that we're going to use as our reference methodology to protect ourselves. This methodology has a list of things that we need to look at, to assess and be aware of. It just happens that one of those components, one of those recommendations, deals with your piece of the business and how you work."

> *"The typical driver of such questions is someone who has made a conscious decision to follow some type of best practice, a framework."*

FRAMEWORKS PROVIDE AN EXCELLENT WAY TO UNDERSTAND RISK

"Cybersecurity is intertwined with all the different departments and business processes," says Hayslip, "and everything we do can have a significant impact—a negative impact—if you don't do it correctly." This is why the step-by-step implementation of frameworks works so well, he explains. You can easily identify the highest priorities, and then measure against best practices as you implement changes in a disciplined manner. ■

KEY LESSONS

1 **Frameworks provide a central gathering point for important questions about the business that must be answered before moving forward.**

2 **Adherence to a framework helps everyone in the organization see why their part is critical and that the actions they must take are not random but part of a disciplined plan.**

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."*

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.

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.**

DANIEL SEID
CISO,
Svenska Spel

LinkedIn

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.

JAVED IKBAL

VP, Information Security & Risk Management,
Bright Horizons

Javed Ikbal is the CISO and VP of information security, risk management, and compliance at Bright Horizons, a global provider of childcare and educational services. He has 25 years of IT & Security, experience with financial services, industrial research, and education. He also teaches graduate-level information security courses at Brandeis University in Waltham, MA. Javed specializes in building or re-engineering security programs.

LinkedIn

As a leading provider of early education, preschools, and employer-sponsored childcare, Bright Horizons is expected to protect sensitive information about clients' employees and their children. Javed Ikbal, who is the chief information security officer (CISO) and VP of information security, risk management, and compliance, says, "We are audited by our financial-services clients as if we are providing financial services to them. We are audited by our defense clients as if we are another defense contractor. Part of this is about securing client data, and part of it is about complying with regulations. We're not simply complying with regulations that apply to us. Clients expect us to comply with the same regulations that apply to them."

Some years ago, Bright Horizons made the strategic decision to adopt a security framework. "It was really driven by our clients," says Ikbal. "Our financial services and federal government clients were increasingly asking us to comply with regulations specific to their industries."

After reviewing a number of frameworks, the firm adopted a blend of the NIST Cybersecurity Framework and the ISO Security Management Framework. "Our US customers are more familiar with NIST, and our European clients are more familiar with ISO," he continues. "There is a 90 percent overlap between those two, and there is acceptance of those as the gold standards."

> *"When we say we use a hybrid of the NIST Security Framework and the ISO Security Management Framework, we don't have to explain anything more."*

Adopting these frameworks has resulted in three key business benefits for Bright Horizons:

- Adopting a recognized security framework that has been tested and vetted has enabled the company to develop a security posture that translates directly to client requirements. "When we say we use a hybrid of the NIST Security Framework and the ISO Security Management Framework, we don't have to explain anything more," Ikbal says. "They know what that means. That's the marketing side of the security framework."
- Another benefit of adopting these standards is they get everyone on the same page in a security discussion. "Everyone knows what I'm talking about," Ikbal says, "and if they ask me a question, I know what that means. If they ask me for a piece of evidence I know what evidence I need to produce." It also helps translate client expectations into accepted standards. For instance, if a client asks for one piece of evidence, but the documented standard requires something different, the framework becomes a way of bridging that understanding. "It gives me a basis for pointing out that we follow the published standard, and asking anyone to follow a standard is a powerful argument. Having the framework makes a lot of disagreements go away," Ikbal explains.

> *"When you adopt a framework that has been developed over the years, and vetted by many experts, it's highly unlikely that a new standard can trip you up."*

- The framework serves as a basis for quickly complying with new regulatory requirements. For example, New York recently changed regulatory requirements for financial-services companies, and those clients came back requesting compliance with a new list of regulations. "We spent half a day mapping those to our framework controls, and we were able to get back to them quickly and tell them how we were in compliance and how their controls mapped to specific NIST controls," Ikbal says. Whenever clients request compliance with a new security framework they don't have to start from scratch. They start mapping controls from the client security framework to the standards in their hybrid framework. "When you adopt a framework that has been developed over the years, and vetted by many, many, many experts, it's highly unlikely that a new standard can trip you up," he says. "I feel confident in telling clients that most of their requirements will map to our existing framework."

KEY LESSONS

1 **Adopting a recognized security framework that has been tested and vetted enables a security posture that translates directly to client requirements.**

2 **A framework serves as a basis for quickly complying with new regulatory requirements without having to start from scratch.**

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.**

IMPLEMENTING A SECURITY FRAMEWORK

In this section...

A FRAMEWORK IS A FOUNDATION

KALPESH DOSHI

CISO–APAC, Group IT,
Capgemini

Kalpesh Doshi is an information security specialist who has more than 16 years of experience in business continuity management, information risk management, security management, and consulting across industry segments. He is currently the chief information security officer of Capgemini as CISO–Asia Pacific, GroupIT, and helps his organization and its clients protect their information assets against threats. He is CISA, CRISC, and CEH certified.

LinkedIn

As the chief information security officer for Group IT covering Capgemini's Asia Pacific region, Kalpesh Doshi oversees the security of internal infrastructure, internal applications, and client deliverables, which includes ensuring that the deliverables are fully compliant. Part of this work involves tracking security certifications. "We use ISO 27001 for information security and the ISO 22301 framework for business continuity," says Doshi.

Doshi sees five key benefits that come from adopting a security framework:

1. Benchmarking. "The foremost benefit is benchmarking," Doshi says. "When I deploy a framework, I know that I'm deploying widely accepted industry best practices." This framework helps the business because there is always concern about whether the organization is pursuing the correct strategy, whether it's making the right investments and the best recommendations for its clients, and whether an alternate approach exists to managing a risk. Doshi says, "The framework is a benchmark in which the direction is clear, even if you make judgements about how to follow it."
2. Measurement. By serving as a security benchmark, the framework also provides a way to measure how secure the organization actually is. Doshi points out that without a framework, it would be difficult to explain to customers that the business's operations are secure. "With a framework, I can say we are compliant with ISO 27001 and have these specific controls in place," he says.

"A great wealth of knowledge is created around a framework."

3. Faster time to compliance. When a business adopts a framework, it's walking a road that many have walked before it, and they have all shared their experience. Doshi says, "A great wealth of knowledge is created around a framework." Some of that knowledge is in the form of tools that enable the business to meet compliance obligations. "Standardized tools that help with compliance and drive automation enable you to complete your programs more quickly," he says.
4. A framework is a foundation. "The framework provides a foundation on which you can build to meet client requirements," says Doshi. "Once everyone understands the client requirements, you generate a comparison between what clients have asked for and the controls you have deployed as part of your framework." Based on this analysis, the business can quickly determine whether it meets the requirements already or must implement additional controls from its or another framework. Doshi says that sometimes, certain clients have special compliance requirements, such as Payment Card Industry or Health Insurance Portability and Accountability Act. In those cases, the organization may need to adjust its operating framework, adding controls. He says, "If you have a framework, your job is easier because when you create a map, you realize that 70–90 percent of the controls are common between various requirements." Although the level of rigor may differ between frameworks, many of the controls map from one framework to another.

> *"The framework provides a foundation on which you can build to meet client requirements."*

5. Prioritization. In some cases, a framework can help make implementation decisions. Doshi cites examples. "A framework might say that you need to have encryption no matter what. Now, that's a clear mandate for the business that you must invest in encryption technology. A framework might require backups. That will drive your investments in appropriate backup solutions." But there are other cases where security investments are more incident driven. Doshi says, "You might give something a lower priority based on a risk assessment. Then, an incident takes place, and suddenly that thing moves to the top of the list."

In addition to these benefits, Doshi says that frameworks help clients interpret the results of third-party assessments. He says, "Security assessments include a lot of focus on compliance. If an assessment finds any deviation, that deviation appears in the report. Client then have the freedom to determine whether that deviation has any material impact for them." ■

KEY LESSONS

1 **When you adopt a framework, you're walking a road that many have walked before you, and they have all shared their experience.**

2 **Frameworks help clients interpret the results of third-party assessments. If an assessment finds a compliance deviation, the client can decide whether that deviation has any material impact for it.**

RUSS KIRBY
CISO,
CreditSafe

Russ Kirby is a 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.

Website | LinkedIn

"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.

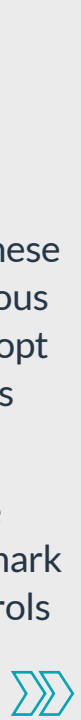
On the other hand, running a security program without a framework is not practical given the complexities of today's IT ecosystem and compliance requirements. Having a framework provides specific advantages, such as a more methodical way of viewing and assessing your own security practice. "Once you 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."*

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."

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.**

MAPPING RISK DIRECTLY TO FRAMEWORK CONTROLS

ALEX WOOD

CISO,
Pulte Financial Services

Alex Wood is the CISO for Pulte Financial Services and has over 18 years of experience in information security and risk management. Alex is a former director for ISSA International and is a co-host of the Colorado = Security podcast. Alex holds a CISSP and has a MAS in Information Security from the University of Denver.

Twitter | Website | Blog | LinkedIn

"I like to think of a security framework as the road map for your security program," says Alex Wood, chief information security officer (CISO) at the Pulte Group, a home-building company that also provides a variety of financial services. "The map is not the only thing you'll need to get from point A to point B, but it helps you find the best route."

After managing the security program based on a variety of best practices culled from various standards, Pulte decided to consolidate its security practices around the ISO 27000 standard. Since Wood joined the company, it has been migrating to the NIST Cybersecurity Framework. "NIST takes the same sort of controls that you have in the ISO framework and makes them a little more user friendly," he says, which is a big advantage when talking to people in the organization who are not so familiar with the technical details of security controls.

Another advantage of the NIST framework is the way it organizes controls into categories based on the maturity of your security practices. "This makes it easy to decide where you need to be and then quantitatively look at those areas where you have weaknesses and strengths," says Wood.

"I like to think of a security framework as the road map for your security program. The map is not the only thing you'll need to get from point A to point B, but it helps you find the best route."

He sees several key advantages to having a security framework in place. For one thing, it provides a way to both qualitatively and quantitatively discuss security within the organization, whether it relates to operational practices, budget discussions, or regulatory issues. "We can pull out specific controls that relate to the standard, and we can map metrics to those things as a measure of how well we were doing in meeting the security standard," Wood says. Measuring the practice in this way becomes a valuable communication tool for explaining to executive leadership and other stakeholders how well the security program is doing. It also provides a frame of reference for comparing your company's performance to others in the industry or to industry benchmarks.

Another advantage of having a security framework is that it becomes possible to map specific IT risks to framework controls. "Any security program needs to start with a risk assessment," he says. "That's how you figure out the likelihood of something bad happening to your data and technology infrastructure, and the impact of that on the business."

"We can pull out specific controls that relate to the standard, and we can map metrics to those things as a measure of how well we were doing in meeting the security standard."

MAPPING RISK DIRECTLY TO FRAMEWORK CONTROLS

Once you know your risks, you can look at the framework and decide what controls to implement to reduce your greatest risks, and then implement those specific controls. And once you've implemented the controls, you can apply a metric and make a quantitative measure of risk reduction. "My metric tells me if I'm really doing it the way that I expect it to be done, and does it really reduce the risk that I was trying to reduce in the way that I would expect it to be reduced."

Wood's advice to those who are just beginning a framework implementation: Do the simplest things first. If you look at the NIST Cybersecurity Framework or even the Sans Top 20 controls (CIS Controls), they can be pretty complex. "But they also have the ability to be really simple," Wood says, "and they give you guidelines on which areas you should look at first. If you're brand new to this, you should focus on those things first." ■

KEY LESSONS

1 **A security framework provides a way to qualitatively and quantitatively talk about security, whether it relates to practices, budget discussions, or regulatory issues.**

2 **With a security framework, it becomes possible to map specific IT risks to specific framework controls.**

ASHISH RAJAN
Director,
DevOps Principal,
Cognizant

Website

LinkedIn

Security standards must inform every aspect of operations, including app development. If your development process is secure and all of the right standards have been followed, then it becomes easier to adapt a process to the company-wide framework.

CALEB SIMA

Managing Vice President, Cybersecurity,
Capital One

Caleb Sima is currently working at Capital One serving as the managing VP of cybersecurity. In his past, he was CEO & co-founder at Bluebox Security (acquired by Lookout) and previously operated as CEO of Armorize (acquired by Proofpoint), and prior to that CTO of application security at Hewlett-Packard via acquisition of his first startup where he was CTO & founder of SPI dynamics.

Twitter | LinkedIn

Caleb Sima believes that security frameworks are valuable because they create an understanding across the organization of what is expected from not only the security team, as well as the risks they must manage, but how the entire company must be involved. "Security is embedded in every single part of the organization from application developers, to IT, to the business functions, to customer support. Security is everywhere," he says. "A security framework builds the understanding that security goes across the board and that every person has a piece that they're responsible for." Accordingly, it shows how all of those pieces play a role in making the business more secure.

For example, if an organization needs to adjust the way it responds to a security threat, it might look at its security framework and notice that there are threats coming in from social engineers—people who are calling into the company in an attempt to extract its customers' data. "We know that rolls down into the framework to who is responsible for our customer interactions," Sima says. "From there, we look at how we can turn the dial up for our customer support team so that they can become more secure. We'll likely tighten certain restrictions and let them know about the threat so they can do their part to keep that customer data safe." Among the security frameworks being adopted by organizations today, he feels that NIST and PCI are often particularly useful depending on the business and the industry in which it operates.

> *"A security framework builds the understanding that security goes across the board and that every person has a piece that they're responsible for."*

A security framework can also be beneficial in terms of demonstrating due diligence and limiting an organization's liability, particularly if the business is in a regulated industry. As Sima noted, "Regulators are checking to ensure that you've got the right policies and processes in place. They're also confirming that you are following and acting on these policies and processes so that you can manage risk effectively. If you can hand a sheet over to them that shows exactly what that security framework looks like, how you manage it, and that you're executing on it well, then that makes their job a lot easier."

To ensure the greatest likelihood of success, a security framework must be messaged in such a way that employees can understand it and put their support behind it. As Sima explains, "It's got to be simple enough that people get it, but yet comprehensive enough that clearly demonstrates its value and effectiveness." This is how businesses can bring everyone together toward the common goal of making the business more secure now and into the future. ■

> *"Regulators are checking to ensure that you've got the right policies and processes in place."*

KEY LESSONS

1. **Building a security framework must be a collaborative, organization-wide initiative, demonstrating how each person can do their part to ensure better security.**
2. **A security framework also demonstrates due diligence and limits liability by making the regulatory process more efficient.**

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.**

ARLIE HARTMAN

Security Architect,
KAR Auction Services

Arlie Hartman is a security architect specializing in Payment Card, Healthcare, cloud computing, privacy, security, and compliance. He develops and implements information security programs including policies, procedures, awareness training, data classification, and controls designed to protect data and mitigate risk. He is a SANS Mentor and lectures at schools for the ISC2 Safe and Secure Online program. Arlie holds the ISA, CISSP, CCSP, and HCISPP certifications.

Twitter | LinkedIn

The main reason Arlie Hartman, information security architect at KAR Auction Services, is using a security framework is to satisfy the security requirements of KAR's customers. "We use the NIST Cybersecurity Framework here to measure our security program," says Hartman. "We may leverage NIST controls from that framework, or we may use our own. Whatever framework you use, the key question you have to ask is, does it meet the needs of the organization from a complexity and risk standpoint?"

Hartman, who joined the company to transform KAR's vulnerability management across an infrastructure that is itself in a state of change, is grappling with this question. Rapid growth through acquisition and business development has forced many changes, including moving more IT infrastructure to the cloud. In addition to having a complex IT infrastructure, part of the security challenge comes from the nature of KAR's business activities, which involve running large online wholesale auctions for the used-car industry, and also providing financial services. KAR has extensive partner relationships with banks, insurance companies, and auto manufactures, and one of the big drivers behind its security strategy is complying with the requirements of these partners. "We've got very large customers, our networks are connected to theirs, and they have stringent security requirements," Hartman says.

"Whatever framework you use, the key question you have to ask is, does it meet the needs of the organization from a complexity and risk standpoint?"

The NIST Cybersecurity Framework is not the only one they are considering: Hartman is also taking a close look at PCI controls. The goal is to map controls from these frameworks to their own operational security framework. "We're mapping our operational controls to the Cybersecurity Framework so we can show how we're driving consistency in our program," Hartman says. This is critical to the success of their business because of the expectations of customers and partners. "The most important business value comes from our use of the framework to demonstrate that we're doing due diligence in a way that can be measured and that drives trust, and trust drives business," says Hartman.

The framework also plays an important role in internal security and budgeting discussions at the executive level. The security team discusses five broad areas within the Cybersecurity Framework with a more detailed breakdown of control areas under those five, and they use spider graphs to illustrate their maturity in each of these areas. "We rate our posture on a scale of one to five for each of the critical areas, and we use that to decide where to best allocate resources," says Hartman. A number of factors can be considered in this kind of discussion, including weighing risk against the cost of achieving a five in each critical area, and peer comparisons to see where they are compared to the competition. "It's an effective tool for communicating to the board without getting caught in the technical details of specific controls," says Hartman. ■

"It's an effective tool for communicating to the board without getting caught in the technical details of specific controls."

KEY LESSONS

1. **Business value comes from using the framework to demonstrate that you are doing due diligence in a way that can be measured and that drives trust, and trust drives business.**
2. **Many factors can be considered with a framework, including weighing risk against the cost of achieving a certain posture, and seeing where you are compared to your competition.**

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."*

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.**

FRAMEWORKS NEED TO ADAPT

LUIS BROWN

Chief Information Security Officer, Central New Mexico Community College

As CISO at Central New Mexico Community College, Luis Brown's responsibilities include risk monitoring and analysis, incident investigation, consultation, collaboration with leadership to formalize processes, and implementing methodology to build and enhance security function. Prior to working at the college, Brown was IT infrastructure manager at Little and Dranttel, a manager in several positions at Wall Colmonoy Corporation, computer specialist at Village of Los Luna, and senior developer at Legend Information Systems. Since 2001, he has run a boutique service firm that remotely manages networks for small businesses.

LinkedIn

Like many education institutions, Central New Mexico Community College must manage the cybersecurity challenges of an IT environment shared by students, faculty, and staff. It is an environment that enables the sharing of ideas, research, and connections with the community while protecting a wide range of personal and proprietary information. A security framework plays an important part in the overall security practice, but to be effective, it must adapt to the college's needs. "We follow standards like the NIST Cybersecurity Framework to some degree," says Luis Brown, chief information security officer (CISO) for Central New Mexico Community College, "but there are aspects of that framework, and a framework like ISO 27002, that are not applicable to a college environment."

Brown sees two significant business advantages in adopting a security framework:

- A framework helps manage liability. Brown says, "If you're a business running an eCommerce website, by saying you meet ISO 27002 standards, you're telling an auditor or a cyber-insurance company that you should be secure and you're doing everything right." In the event of a breach, you can show that based on compliance with the framework, you made a serious effort to have the proper controls in place.

> *"Once an organization adopts a framework, the discussion is no longer about whether you need a control. It's about the cost of implementing the control everyone agrees they need."*

FRAMEWORKS NEED TO ADAPT

- A framework helps administer the security practice. Frameworks tell you what you need to be secure, but they don't tell you how to secure your system. "They're primarily based on protection level standards," says Brown. "For instance, you have a firewall, you have patching, you have a password policy, and you can verify you've put all of these things in place." It also facilitates the internal discussion about security needs and priorities. "Once an organization adopts a framework, the discussion is no longer about whether you need a control. It's about the cost of implementing the control everyone agrees they need," says Brown.

A framework provides security advantages too, but Brown cautions against assuming that implementing a framework makes you more secure. "Most frameworks focus on protective solutions," Brown says, "but we're not investing enough on detection and response. If you don't actively find the holes in your security, the hackers will do it for you." One area where a framework can provide a security benefit is in its implementation phase. "If you're a fledgling organization with little security background, you can take a framework or a list of protections like the SANS Critical Security Controls (CIS Controls), and in working through that, discover weaknesses in your current security practices," he adds.

"Most frameworks focus on protective solutions, but if you don't actively find the holes in your security, the hackers will do it for you."

FRAMEWORKS NEED TO ADAPT

For an organization implementing a framework, Brown recommends contracting with a consultant who can come in, audit your systems, look at your data, and make recommendations about the kinds of controls you need. They can also suggest a framework that is appropriate to your business. "It's much better to know these things going into the game, and if you don't have that expertise in-house, you need to go hire a consultant before you spend hundreds of thousands of dollars on protections you don't need," Brown concludes.

KEY LESSONS

1 **Frameworks tell you what you need to be secure, but they don't tell you how to secure your system.**

2 **Organizations implementing a framework should contract with a consultant who can come in, audit the systems, look at the data, and recommend the kinds of controls they need.**

About Tenable

Tenable™, Inc. 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.

To learn more, visit Tenable.com