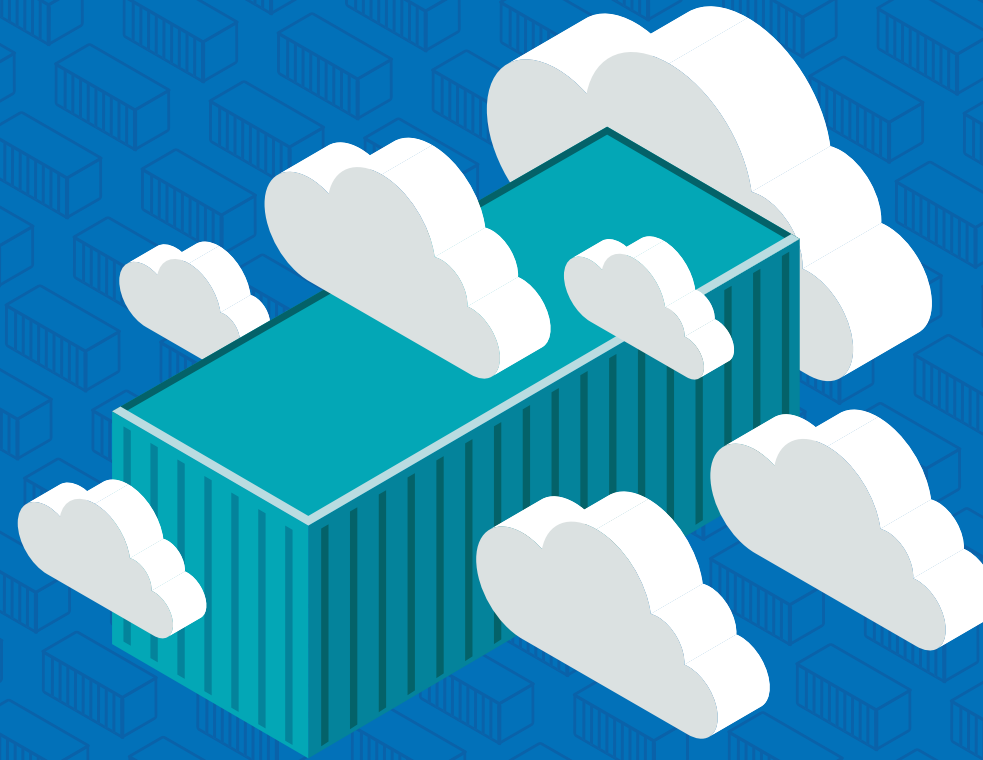


# REDUCING CYBER EXPOSURE FROM CLOUD TO CONTAINERS

EMEA Industry Leaders Share Lessons Learned



# FOREWORD

Digital transformation is putting pressure on every organizational function—especially IT Security. Whether it’s discovering short-lived assets like containers, assessing the state of cloud environments, or maintaining the security of web applications, today’s modern attack surface presents a growing challenge to security leaders looking to accurately understand and reduce their cyber risk. To combat this challenge, a new discipline called Cyber Exposure is emerging to help organizations manage and measure this risk. Cyber Exposure builds on the roots of traditional Vulnerability Management, expanding breadth of asset coverage and depth of insight, to provide a full, actionable picture of organizational risks.

This eBook shares perspectives on how your peers are beginning their Cyber Exposure journey to protect their ever-expanding attack surface—from mobile to cloud, IoT to containers, and everything in between—and gain business insight to reduce their cyber risk. Where do you begin? What are key factors for success? The first-hand experiences collected here represent a diverse array of industries and perspectives that we hope will offer valuable insight and best practices that you can use as you work to secure and reduce risk to your organization.



Regards,  
**Brad Pollard**  
CIO, Tenable, Inc.



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

When it comes to IT infrastructure, it's fair to say that the perimeter has left the premises. In fact, the perimeter has mostly disappeared. But what exactly does that mean?

Research by Skyhigh Networks<sup>1</sup> finds that the average organization uses 1,427 cloud services, but only 8.1% of them meet enterprise security and compliance requirements, and file sharing company Egnyte published data<sup>2</sup> showing that 89% of companies now allow personal devices to connect to corporate networks. Most analysts agree there are billions of connected IoT devices in use today, a number that is rapidly growing, yet there is no standard for securing them.

Security professionals face a rapidly changing IT landscape, one that is crowded with new types of dynamic IT assets. We decided to learn more about how they are adapting their strategies to meet these challenges. With the generous support of Tenable, we asked 11 cyber security experts the following question: **How have modern assets like cloud instances, web-based applications, mobile devices, application containers, and others affected your security and risk management program?**

It's a big question that lead to fascinating discussions and different perspectives from a variety of industry segments. Several themes emerged: more collaboration between security and app developers; growing emphasis on continuous scanning and detection; and some industries placing more emphasis on data-centric security strategies.

These essays are loaded with fresh insights into areas of security and risk management that are becoming more challenging and more critical to healthy business operations. Whether you are a security professional, a software engineer, or a business leader, I have no doubts you will find these essays useful and thought provoking.



All the best,  
**David Rogelberg**  
Editor



## **Mighty Guides make you stronger.**

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

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

<sup>1</sup> "Cloud Adoption and Risk Report," Skyhigh, Q4 2016  
<sup>2</sup> Infographic - <https://www.egnyte.com/file-server/byod.html>

# TABLE OF CONTENTS

Foreword .....	2
Introduction .....	3
Applying a Data-Centric Strategy in a Vast IT Ecosystem   Eric Bedell.....	5
Life cycle Data Encryption Is Effective, But It Is Not a Magic Bullet   Paul Heffernan.....	8
Businesses Must Focus on Protecting Information   John Meakin.....	11
Digital Assets Provide Great Benefits, but Also Create Vulnerabilities   Mark Nicholls.....	15
Shifting to Software Driven Data Protection   Rory Alsop.....	18
Protecting Modern Assets Requires a Data-Centric Security Posture   Antonio D'Argenio.....	21
Protecting Modern Assets Requires a Proactive Approach   Isabel Maria Gómez González.....	24
Automate as Many Regularly Occurring Events as Possible   Russ Kirby.....	28
You Must Account for Entirely New Kinds of Risks   David Carvalho.....	31

# APPLYING A DATA-CENTRIC STRATEGY IN A VAST IT ECOSYSTEM



**ERIC  
BEDELL**

**CISO,**  
Mitsubishi UFJ Financial  
Group

An 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 Luxembourg bank industry, which has strict information-security requirements. Living in France, working in Luxembourg for International firms, Eric is definitely a traveler.



LinkedIn


As one of the world's largest financial services companies, Mitsubishi UFJ Financial Group (MUFG) operates in more than 50 countries and has a complex IT ecosystem that spans geographies, regulatory environments, and business drivers. In such an environment, Eric Bedell, MUFG's chief information security officer, says that trying to secure every device, every application, and every cloud instance is extremely difficult. Instead, he focuses his security strategy on the data. "We classify all our information and locate our most important data centrally," Bedell says. "Everything in that central location is classified. Removal of data from that vault is authorized based on data classification and where the data is going." Bedell says that it doesn't matter if the data is going to the cloud, a managed service, or a device: The move is authorized only based on the classification of the data and the person or process having the appropriate clearance. 

*“ Nobody can block a hacker who really wants to hack you. The most important thing is that that attacker shouldn't be able to gain access to business-critical assets. ”*



# APPLYING A DATA-CENTRIC STRATEGY IN A VAST IT ECOSYSTEM

Bedell prefers to focus resources on securing the data rather than every element of a global infrastructure. “Nobody can block a hacker who really wants to hack you,” he says. “The most important thing is that that attacker shouldn’t be able to gain access to business-critical assets. I’m a big fan of deception technologies.”

With so many assets moving into the cloud and onto mobile devices, implementing a data-centric security strategy requires more controls built into software. Bedell says, “It’s not a question of which person or what role has access to a control but rather a piece of code somewhere that has access to that control.” This approach changes the way you architect applications, but if your data is classified in the right way, it doesn’t significantly affect your overall strategy. Bedell explains, “We use a kind of vault that changes passwords frequently. We use an application programming interface (API) to access the vault. We have a server that generates one-time, complex passwords with short lives. This way, we focus more on protecting the API than protecting the identity of the caller. All this happens in the software.” 

“

*If you classify your documents or the database on which they reside correctly, it’s easy to say what data can leave the vault without controls and what data you need to control tightly.*

”

# APPLYING A DATA-CENTRIC STRATEGY IN A VAST IT ECOSYSTEM

Bedell emphasizes that it all comes back to data classification. “It really depends how you classify your documents. If you classify your documents or the database on which they reside correctly, it’s easy to say what data can leave the vault without controls and what data you need to control tightly.” This approach enables you to focus security resources on controls that lock down your most valuable data assets. Bedell says, “If this means leaving parts of the infrastructure unprotected, that’s fine because your most critical data assets will never be in those places, and nobody in those places can ever access them.” From an end-user perspective, users only ever see data they are authorized to see. This data-centric approach is an effective way to balance the costs of protection against the risk of damage, especially in a complex, ever-changing IT infrastructure with no clear boundaries. ■

## KEY LESSONS

- 1 With so many assets moving into the cloud and onto mobile devices, implementing a data-centric security strategy requires more controls built into software.
- 2 Data-centric security effectively balances the costs of protection against the risk of damage, especially in a complex, ever-changing IT infrastructure with no clear boundaries.

# LIFE CYCLE DATA ENCRYPTION IS EFFECTIVE, BUT IT IS NOT A MAGIC BULLET



**PAUL  
HEFFERNAN**  
Group CISO,  
Unipart Group

Paul is the group CISO for Unipart. With experience in the cybersecurity world, consulting for some of the world's biggest brands, he engages with the business at board level to enable trusted secure commerce. Paul 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

As chief information security officer (CISO) of the UK-based Unipart Group, a global enterprise that provides manufacturing, logistics, and consultancy services, Paul Heffernan likens old-world IT security to castle defenses. "You put up strong walls and big doors, and you keep all your valuable stuff inside where it's easy to find. But with modern computer systems and the way business uses them, the castle doesn't work anymore," he says.

The old model doesn't work because of an explosion of new technology that lets people buy IT assets on credit cards, create shadow IT, enter a world of apps whose origins are uncertain, and adopt an Internet of Things that opens a whole new set of access points and data streams. "The big challenge is how to make assets visible to the IT security team so that they can monitor and secure them," Heffernan says.


Having policies and processes in place that take these new kinds of assets into consideration is important, but that often does not address all the visibility issues. One strategy that some organizations are increasingly adopting is to focus on following and protecting data as it moves through the changing infrastructure. "The idea is to protect data from the beginning to the end of its life cycle," Heffernan explains. "It doesn't matter where that information goes, whether it's somebody else's computer, or an employee's smartphone or my desktop—security needs to be pervasive." 

*“The big challenge is how to make assets visible to the IT security team so that they can monitor and secure them.”*



# LIFE CYCLE DATA ENCRYPTION IS EFFECTIVE, BUT IT IS NOT A MAGIC BULLET

Heffernan points out that the idea of securing data is nothing new. Methodologies like access management, vulnerability scanning, and monitoring data activities still apply, but using them in the new infrastructure requires new approaches. For example, doing this in the cloud is not so easy. “You’re on a computer system that you have limited ability to manage. You’re sharing it with other customers. The cloud provider may not give you the access you really need for meaningful assurance, because they must protect their other customers,” Heffernan says. This lack of visibility can be partly addressed by agreements with the cloud provider that it does the kind of vulnerability testing and monitoring you need, and it provides you with the results. This works, but it also means changing your risk considerations and how you evaluate service providers.

Other technologies are coming into play too. “Encryption is a great example of this,” says Heffernan. “If I encrypt my data throughout its entire life cycle, security of the cloud infrastructure that the data traverses is not so important.” However this approach still has its limitations. For instance, only some cloud providers allow customers to bring their own encryption keys into the environment. Heffernan says, “It is a challenge for cloud providers because if everyone brings their own encryption keys and encrypts data at scale, it erodes their ability to understand how customers are using the platform, hampering business intelligence.” 

“  
*When your data is decrypted, you still have to manage the security risk during that window of data decryption.*  
”

# LIFE CYCLE DATA ENCRYPTION IS EFFECTIVE, BUT IT IS NOT A MAGIC BULLET

There are other limitations to the encryption strategy. Heffernan notes that if you're using the cloud provider to do something with your data, like reporting, or business intelligence, or some other processing, you may have to decrypt using the cloud provider's service. "When your data is decrypted, you still have to manage the security risk during that window of data decryption," he says. "We are struggling, I think, as a security industry to come up with a good way to keep that data secure during processing, which is actually where the risk profile is the highest." As long as data is at greatest risk during processing, the use of vulnerability scanning and monitoring will be central to securing those data assets. ■

## KEY LESSONS

- 1 One strategy that some organizations are increasingly adopting is to focus on following and protecting data as it moves through the changing infrastructure.
- 2 To gain better visibility into cloud assets, work with your cloud providers to conduct the vulnerability testing and monitoring you need, and ask them to provide you with the results.

# BUSINESSES MUST FOCUS ON PROTECTING INFORMATION



**JOHN  
MEAKIN**


**Former Chief Risk and  
Security Officer,  
Burberry**

Dr. John Meakin has recently retired as a chief security and risk officer and now advises a number of businesses on cyber risk. He is a specialist in information security with more than 25 years experience. Previously, he has built and led security functions in Richemont SA, a range of banks, as well as BP plc and Reuters. He was a founding member of the Jericho Forum, and has served on the Customer Advisory Boards of leading security product vendors. He is a regular speaker at industry conferences. He has a Ph.D. in physics from Cambridge University.



LinkedIn

John Meakin believes the need to protect modern assets has led businesses to place a new focus on securing information rather than simply defending infrastructure. This is a result of companies capitalizing on the value of data insights by collecting more information and extracting greater value from it through analysis, explains Meakin, former chief risk and security officer at Burberry. In such a dynamic environment that places a high priority on customer engagement, a CISO must also adjust his or her mindset accordingly and craft tailored approaches that enable business strategy.

One reason for this change is that customers are using an increasingly wide variety of channels and entry points to engage with businesses. Using China as an example, Meakin notes, “customer transactions are taking place using infrastructure that is completely outside of a retailer’s control—on a smartphone app like WeChat, for example.” Naturally, in such a scenario the business will have to focus on securing the information rather than the underlying infrastructure. 

*“Customer transactions are taking place using infrastructure that is completely outside of a retailer’s control—on a smartphone app like WeChat, for example.”*

# BUSINESSES MUST FOCUS ON PROTECTING INFORMATION

How are businesses taking on this challenge? Meakin feels there's been a shift in posture from protection towards detection and response, for starters. "Improving the quality of my monitoring is at the top of my challenging work agenda," he says. "First, improving the quality of my intelligence about the threats that are outside my network so I know what I'm looking for when I'm monitoring. And then to make my security team and the rest of the business agile enough so that if we see something happening we can respond fast enough to limit the damage."

Although there are many different types of modern assets to keep track of such as the cloud, mobile devices, and application containers, Meakin considers them all equally challenging. "They're not separate things, really," he says. "If you're thinking about securing valuable business information that's in mobile devices, well, it's going to get to the mobile devices via some serving of apps through the cloud." That's why it's important to craft a strategy for securing the information while it's resident or transient through the cloud infrastructure as well as while it's being served in the applications, and on the mobile platform. "You've got to devise a strategy that recognizes whether your data is truly captive within the app, or if in fact it's exposed within the storage of the mobile platform," he adds.



*“Improving the quality of my monitoring is at the top of my challenging work agenda.”*



# BUSINESSES MUST FOCUS ON PROTECTING INFORMATION

This advice reflects Meakin's belief that businesses must concentrate their efforts on securing information as it travels from one point to another rather than simply locking down infrastructure. CISOs have an important role to play in crafting a tailored approach that enables companies to engage successfully with their customers. They can best protect modern assets, now and into the future, by using a more comprehensive approach that asks first what the business seeks to achieve and then takes active steps to make that possible. ■

## KEY LESSONS

- 1** As businesses place a greater value on maximizing data insights, they must adjust their security focus to protect information, not just infrastructure.
- 2** Security leaders have an important role to play in crafting a tailored security approach that protects information while enabling business strategy.



## DANIEL DRESNER

Academic Coordinator for  
Cybersecurity,  
University of Manchester



Twitter



Website



Blog



LinkedIn



*Innovation (not disruption) is delivering opportunities to assess better risk controls as technology opportunities arise. But they also bring the risk-albatross to hang around people's necks. Sociotechnical boundaries deserve more attention so that calls for awareness, and education won't leave 'users' open to the misanthropy of 'blaming human error' when applications (human-computer symbiosis) were not designed and built right in the first place. Risk assessments should never be made to turn green as an excuse to grab the bleeding edge.*







## MARK D. NICHOLLS

Head of Information Security & Governance, Peabody

Mark Nicholls is head of information security and governance at Peabody, one of London's oldest housing associations. He holds overall group responsibility for security management and related governance activities, ensuring that the organization puts appropriate safeguards in place to protect information and business operations. Before he worked at Peabody, he spent 15 years in academia, holding various senior information security roles.



Website | LinkedIn

As head of information security and governance at Peabody, one of London's oldest and largest housing providers, Mark Nicholls is responsible for keeping all the private data the nonprofit accumulates safe and secure. This is a unique challenge, as residents expect easy access to housing information and transactions through multiple devices and applications. Though Nicholls is realistic about the vulnerabilities that can result from assets such as Web apps, mobile devices, and the Internet of Things, he sees the tremendous value those can provide. "From my perspective I see the new stuff that's coming along as being of great benefit," he says. "It's something that we can't be cavalier about and just say, 'no, stop, we're not doing this because of x vulnerabilities, x security concerns, etcetera. But we need to be very acutely aware of the threats these assets do bring just by the sheer nature of the devices.'"

A good example, says Nicholls, is the Internet of Things. "These devices, like smart televisions, come on to our networks, often wirelessly, and we have to allow that, but we also have to remain conscious that they are quite vulnerable devices just by the sheer nature of the operating systems and lack of built-in protections. Fortunately, for Peabody, it is still possible to assert some company-wide controls, like restricting BYOD items and standardizing on certain operating systems and closed networks. That helps on one hand, but also requires monitoring and training to assure compliance," says Nicholls.



*“ Security is very much a knowledge-sharing exercise—we want to try and up-skill as many traditional IT folk in the world of security as we can, because we are a small team. ”*

# DIGITAL ASSETS PROVIDE GREAT BENEFITS, BUT ALSO CREATE VULNERABILITIES

“I’ve tried not to say no in the past,” he admits. “That’s not the way I like to do things. But things need to be done in a secure manner, and we do everything we can to accomplish that. For example, let’s take smart televisions. In our environment, we must segregate them and stick them onto dedicated networks that are appropriately protected. So they can still get information, still broadcast, but rather than going directly to the internet we manage that type of content as it comes in and take away the vulnerabilities. Most of the vulnerabilities I’ve seen on these types of devices seem to be exploitable as soon as they’re talking to the outside world. But you can’t do too much because it will restrict the usability factor of the technology.”

Tackling a challenging security environment must also begin early in every process, explains Nicholls, which requires a great degree of cooperation. “We’ve gone through a process of maturing our IT life cycle here so that security is embedded right from the start as part of the design process,” he says. “The security team is the same for the IT team, but they work very closely with the other teams like development teams, the infrastructure teams, the operations teams. And it is very much a knowledge-sharing exercise—we want to try and up-skill as many traditional IT folk in the world of security as we can, because we are a small team. We can’t be there for every meeting, every design, look at every document, etc. So the more that we can improve those teams’ knowledge the better.”



“  
*We’ve gone through a process of maturing our IT life cycle here so that security is embedded right from the start as part of the design process.*  
”

# DIGITAL ASSETS PROVIDE GREAT BENEFITS, BUT ALSO CREATE VULNERABILITIES

On the asset front, Nicholls is particularly concerned about web apps, but deploys the same “act early and involve everyone” approach as with all security concerns. His team, he says, “will be there with the developers looking at things and doing the vulnerability scans on these applications throughout the development process to see where they are and what they can do to fix it. Sometimes there are things you can’t seem to fix because it will destroy the functionality of the application. In those cases we put in other compensation controls.”

Nicholls is disciplined about his security, but a bit more philosophical about the real challenge facing the 155-year-old nonprofit. “I think it’s more about new ways of working as the next generation of workers comes in. They’re going to want to work differently. They’re going to want to work more out and about in the Starbucks or at the station. They’re going to want access to information instantly, they’re not going to want to be prevented from doing x, y, and z just because the company says that’s the way you’ve got to work. They want to work flexibly, and I think that’s going to cause the challenges. And I don’t have the answer to that.” ■

## KEY LESSONS

- 1 Embed security at every level of the organization and rely on cooperation and good training to supplement a small team.**
- 2 Work with development teams throughout the development process to solve problems and incorporate other compensation controls.**

# SHIFTING TO SOFTWARE DRIVEN DATA PROTECTION



**RORY  
ALSOP**

**Head of Information  
Security Risk Oversight,  
Royal Bank of Scotland**

Rory Alsop, CRISC, CIPM, CISM, C|CISO, M.Inst.ISP has led infosec, risk, privacy, and governance teams for the past 17 years in FTSE100 companies and Big-4 consultancies, and has founded two smaller security consultancies. As a director of the ISF, deputy Scottish chair of the IISP, research director of ISACA Scotland and co-founder of B-Sides Scotland, he provides industry leadership and guidance, both globally and locally. He moderates the Security.StackExchange.com question-and-answer site in his spare time.



Twitter




Website



LinkedIn

In the world of banking, there can be many connections between the bank's systems and those of clients, service providers, and even customers. Rory Alsop, head of information security risk oversight at the Royal Bank of Scotland, explains the challenges involved in keeping data safe and ensuring systems are reliable. "Enterprises use public, private and hybrid clouds, applications that sit partially with third parties, and third parties who are part of supply chains that might be five or six companies long, each providing part of the service," he says. "At that scale it's not so easy to manage an information asset inventory."

As IT systems have become decentralized, Alsop has seen a shift in security strategies that focus more on information asset classification and securing the actual data. "A critical starting point is implementing an asset inventory," he says. "You've got to know what you have in terms of information type, classification and life cycle so you know exactly what you're doing with our assets." This must be a risk-based approach: some must be secured as if they are the crown jewels, while others are less important. Not knowing the difference makes everything else more difficult. 

*“ We can simply put our security wrapper around our information assets, regardless of the client environment. ”*

# SHIFTING TO SOFTWARE DRIVEN DATA PROTECTION

Once you have a detailed asset inventory, securing it becomes easier. “My preferred approach, especially when dealing with cloud, is to assume any client service could be compromised, so I don’t need to rely on trust. You can simply put a security wrapper around your information assets, regardless of the client environment,” Alsop says. Exactly what controls go into that security wrapper may vary, depending more on the data classification than its physical location.

Another change is the growing importance of app security, because the apps themselves are being configured to automate various controls that govern authentication, access, and encryption. Yet for many organizations, apps are created in an Agile or DevOps process designed to accelerate development, testing, and deployment. “You can focus more on securing the building blocks,” says Alsop. “Validating pieces of architecture that have already been vetted. When developers use building blocks that are already approved, you can run a much more straightforward set of tests.”



“  
*We’re seeing development groups embracing the concepts of validation modules and building an architecture security from the start.*  
”

# SHIFTING TO SOFTWARE DRIVEN DATA PROTECTION

But still, you have to vet the building blocks, and if these things come from third parties or open source, they can change. “It is essential to carry out frequent module scanning, and assess every single one against risk, depending on what the application does, where it is going to sit, the sensitivity of data going through it, and the customer base.” Once the app goes live, it should become subject to regular scanning, and there are a lot of tools that will run all the time to complement assurance testing. “You can use tools to make sure the code hasn’t changed where you didn’t expect it to,” he explains. It becomes almost a continuous scanning process. Part of that continuous scanning that is particularly prevalent in financial services is done by behavior assessment tools that scan metadata in search of strange activity. “It’s the strange behavior that sends up a flag. At that point, we won’t know if it’s coming from an attacker or a valid user, but the alert means it can be checked.”

A software-driven data protection strategy depends heavily on tight integration between DevOps and security professionals. This requires individuals from different teams to work with each other, from security representatives to developer scrums. “We’re seeing development groups embracing the concepts of validation modules and building an architecture security from the start. It’s all the concepts we’ve discussed for years, but I think DevOps gives you an opportunity to actually do it. And I see a greater uptake of developers wanting to understand security,” Alsop says. ■

## KEY LESSONS

- 1 As IT systems have become decentralized, there has been a shift in security strategies that focus more on information asset classification and securing the data.
- 2 Once the app goes live, it becomes subject to continuous scanning, and there are a lot of tools that will run all the time.



# PROTECTING MODERN ASSETS REQUIRES A DATA-CENTRIC SECURITY POSTURE



## ANTONIO D'ARGENIO

Security Architect,  
Tech Data Corporation

Antonio D'Argenio is an expert information security professional with over 25 years of experience. As a pioneer of information security in southern Europe, D'Argenio has managed information security governance, telecommunication risks and operations, intelligence/law enforcement, information technology security for government departments, and entertainment companies. He has covered key positions in renowned consulting firms that support customers in their effort to attain an optimal security status. Currently, D'Argenio holds the position of information security architect for Tech Data Corporation.



Twitter |



LinkedIn

Antonio D'Argenio has seen firsthand the impact the transition to the cloud has had on security, especially for B2B and B2C companies. His company, Tech Data, is grappling with these challenges as well. “At the moment, we are moving our own core business from older technologies to the cloud,” he says. “The cloud definitely offers more flexibility, but most of the time this flexibility will come with a relaxed security posture.”


It's difficult for security professionals to provide the same level of physical and logical security in a cloud scenario that they can guarantee in a classic, on-premises setting. At the same time, with the popularity of social media and consumer technology, users don't necessarily appreciate the business risks involved in lax security practices. In this environment, it can be an arduous task to secure sensitive corporate information and prevent it from being accessed by an unauthorized third party.

D'Argenio and his colleagues are responding to these challenges by moving from a classic security posture to a data-centric security structure, proactively protecting sensitive information. “This means, for example, that we are talking about encrypted databases and secure communication at every level. We are also talking about intensive use of encryption via public and private key methodologies to limit the transit of data between applications,” he explains. To minimize risk, it's important to limit the number of sites where such data can live in the cloud. And, crucially, a business must start thinking about security by design. »»

“The cloud definitely offers more flexibility, but most of the time this flexibility will come with a relaxed security posture.”

# PROTECTING MODERN ASSETS REQUIRES A DATA-CENTRIC SECURITY POSTURE

A business should begin by identifying the critical data it needs to secure. “If you are applying an information-centric security policy, you need to classify the data that you have to protect,” D’Argenio says. Also, consider that any measures you take will require a security infrastructure. “For example, encryption needs a security infrastructure—the public interface to protect and encrypt the data,” he says. Very likely, the data you decide to safeguard will be associated with the core value that your company provides. In the case of an insurance company, it might be policyholder information. Whatever your business model, the most valuable data will likely need special attention.

Of course, some businesses are required by law to take such steps—particularly in Europe. “If you are a CISO, normally you are legally responsible for the data that your company’s exposing,” D’Argenio notes. “It’s a lot of risk, and in Europe there are hefty fees associated with noncompliance.” With Europe’s GDPR law about to come into effect, companies doing business in Europe will have even more stringent regulations to contend with. He notes that the GDPR has even been proposed as a global regulation, potentially impacting more businesses worldwide in the future. 

“  
*If you are applying an information-centric security policy, you need to classify the data that you have to protect.*  
”

# PROTECTING MODERN ASSETS REQUIRES A DATA-CENTRIC SECURITY POSTURE

Businesses face formidable challenges in protecting their modern assets, particularly if they face strict regulatory requirements. One way they can prevent damaging attacks is by assuming a data-centric security posture. Through identifying their most valuable information and taking proactive measures to protect it, they can ensure that the business is secure and well positioned to flourish in today's technology landscape. ■

## KEY LESSONS

- 1 **Businesses can protect their modern assets by adopting a data-centric security posture.**
- 2 **To minimize risk, a business must start thinking about security by design.**

# PROTECTING MODERN ASSETS REQUIRES A PROACTIVE APPROACH




## ISABEL MARIA GÓMEZ GONZÁLEZ

Group Information Security Manager, Bankia

Isabel is a certified executive manager with cross-functional expertise in risk management specialized in information security, cybersecurity, data protection, compliance and digital transformation. She has a career of more than 18 years of experience managing and leading projects that involve different legal, normative, technical, and financial areas. She is an expert contributor and participant in forums, articles, and discussions on issues related to new technologies and regulations.


Isabel Maria Gómez González believes businesses must proactively adapt to the changing IT environment in order to successfully protect their modern assets. “We are currently undergoing the Fourth Industrial Revolution, so of course the IT environment has changed a lot,” she explains. “We must protect not only applications and mobile devices, but our brand and our legal requirements as well.” While in the past a business might have used a security methodology that focused almost solely on IT security risks, that mindset must change now. “We must also factor in legal and regulatory requirements—like information security, like cybersecurity, like data protection and so on,” Gómez González says.

Gómez González’s most difficult challenge is to protect the services that are provided via third-party vendors and providers. “There are a lot of services, for example within Amazon or Google, that those vendors are using to protect my information. In this case, I am not just dealing with my vendors—I’m dealing with their vendors too.” Her dilemma is to find a way to make these third-party vendors understand that it’s not enough for Amazon or Google to implement her security rules; the third-party vendors must also implement them in order for her company’s information to be truly protected. 

*“ We must protect not only applications and mobile devices, but our brand and our legal requirements as well. ”*

# PROTECTING MODERN ASSETS REQUIRES A PROACTIVE APPROACH

Of course, this is not an easy task. On one hand, the third-party vendors may be reluctant to implement her security rules. But on the other hand, Gómez González must comply with certain European security requirements, such as those originating from the European Central Bank and new requirements related to GDPR, PDS2, etc. Gómez González and her colleagues address this challenge proactively. “Since 2011, my bank has conducted what we call ‘third-party homologations.’ It’s a process that all my providers and vendors must go through. They must specify the security measures they will implement to protect our information,” she explains. This doesn’t just apply to the first level of an agreement. It must also be extended to all the vendors and providers that have access to her bank’s information—encompassing those third-party vendors and providers as well. If they don’t obtain the authorization, they won’t work with my group.

Beyond taking such security compliance measures such as these, Gómez González and her team are working hard to implement an awareness plan that accurately reflects changes in the overall security landscape and within the business as well. She also considers it especially urgent for young people, whether employees or clients, to understand the importance of privacy in their lives. With that in mind, she recommends that all companies consider implementing an awareness program that teaches digital natives how to protect their information better. 

“  
*In this case, I am not just dealing with my vendors and providers—I’m dealing with their vendors and providers too.*  
”

# PROTECTING MODERN ASSETS REQUIRES A PROACTIVE APPROACH

Protecting modern assets is a complex challenge in today's digital age, but a vigilant posture and firm, proactive due diligence can go a long way toward helping a business secure its vital information. By adopting an evolved security methodology that includes factors such as legal, regulations and brand requirements, a company can successfully adapt to the quickly changing security landscape and thrive within it. ■

## KEY LESSONS

- 1** Conduct a "third-party homologation" process that all providers and vendors must pass. They must specify the security measures they will implement to protect your information.
- 2** Consider implementing an awareness program that teaches digital natives how to better protect their information.





**DANIEL  
SEID**  
CISO,  
Svenska Spel



LinkedIn



*With any new technical solution it should be understood that one of the risks is that the same solution can also be misused, with either malicious or non-malicious intent. Thus, assume that anything you can use, someone else can misuse and abuse. If this is true, then any and all new technology, from a strictly security standpoint, should be viewed with initial mistrust, until the opposite is proven, i.e that the solution is safe, secure, and robust.*



# AUTOMATE AS MANY REGULARLY OCCURRING EVENTS AS POSSIBLE



**RUSS  
KIRBY**  
CISO,  
CreditSafe


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 is approached.



Website | LinkedIn



As chief information security officer (CISO) of Creditsafe, an international provider of business credit reports with offices in Europe and North America, Russ Kirby is responsible for cybersecurity, regulations, and compliance, including GDPR compliance which is currently rolling out in Europe, and risk management. “I cover everything,” Kirby says. “It’s a very holistic security operation.”

An important part of his security work involves securing cloud-based assets. “Some organizations treat cloud security as the service provider’s problem. I think of outsourced, leveraged services as a risk asset in themselves,” Kirby comments. He sees two broad areas of security activity that require special treatment when cloud assets become part of the IT ecosystem. One involves ensuring that the service providers themselves are delivering a secure service. This is a third-party risk-management problem. The other is ensuring that the data you put into that environment and the processes you run there are secure, which may require some new security practices. 

“ You can ask to see redacted details of vulnerability scans, and remediation plans associated with them. You can ask to sample and check on key controls. ”

# AUTOMATE AS MANY REGULARLY OCCURRING EVENTS AS POSSIBLE

Managing vendor risk involves verifying that vendors are actually delivering the security you need. “At the very least,” says Kirby, “you are looking for third parties that adhere to industry best practices and can show you the program they have in place to manage risks, vulnerabilities, and threats.” This should be more than a current certification. For instance, although service agreements should and typically do have a right-to-audit clause, many organizations do not actually audit their service providers. He points out that you don’t need to do full audits to evaluate your service provider. “You want the ability to see evidence of what the service provider is doing. You know they have to do a vulnerability scan as part of your certification. You can ask to see redacted details of those scans, and remediation plans associated with them. You can ask to sample and check on key controls.” This is not always so easy, especially when many service providers are themselves subcontracting their services to other services providers. >>>

“  
*Regularly occurring events become security requirements in your architecture stage.*  
”

# AUTOMATE AS MANY REGULARLY OCCURRING EVENTS AS POSSIBLE

In addition to making certain the vendor is delivering a secure service, you need to be sure that the processes you run and the way you provide access to your cloud assets are also secure. For instance, Kirby says, “you must properly use internet security and event management, monitoring, and configuration management. This is especially true when doing things like spinning up servers on an ad hoc basis.” Whether it’s validating the server image or enforcing proper view and function states, you need to adopt a process to automate this through configuration management controls.

Kirby says to do that, you may have to adjust your whole DevOps approach so that you can automate as many regularly occurring events as possible. “Those things become security requirements in your architecture stage,” he says. “They need to become part of your security operations, and they must be monitored and checked.” ■

## KEY LESSONS

- 1 With cloud assets in the infrastructure, you must ensure that service providers are delivering a secure service, and the processes you run there are secure.
- 2 Whether validating the server image or enforcing proper view and function states, you need to adopt a process to automate this through configuration management controls.

# YOU MUST ACCOUNT FOR ENTIRELY NEW KINDS OF RISKS



**DAVID  
CARVALHO**


Global CISO,  
OCS Group

The youngest global CISO in Europe, David Carvalho is heavily involved in several blockchain-based projects and other crypto-related innovations. Leveraging hands-on skills with strategic thinking, and currently leading a group of global organizations with more than 100,000 employees, David has worked in cybersecurity since he was 15 years old, and has over 18 years of direct cybersecurity experience. He focuses on looking at problems through an innovative lens, providing actionable cybersecurity strategy.



LinkedIn

David Carvalho, group chief information security officer (CISO) for OCS Group UK and a self-described hacker with board-level acumen, warns that in a modern IT ecosystem designed more for ease of use than for security, companies must recognize that hackers will gain entry. “The hacker always wins against the defender,” he says. “As a defender, I have to leverage real-world tools and budgets, and my liability is absolute. Hackers leverage their imagination, and their liability is zero.” Companies must build security strategies based on realistic risk assessments and practical risk-management decisions, Carvalho notes.


For example, the cloud presents certain risks, regardless of service-provider assurances and certifications. “The argument in favor of moving to the cloud is that it saves you money and they have all these controls and certifications. But still, there’s a lack of visibility, and an inability to do real pen testing, and there’s the fact that clouds are breached all the time. You can have service-level agreements in place, but providers will not be liable for your losses or for your non-compliance,” says Carvalho. 

“ *As a defender, I have to leverage real-world tools and budgets, and my liability is absolute. Hackers leverage their imagination, and their liability is zero.* ”

# YOU MUST ACCOUNT FOR ENTIRELY NEW KINDS OF RISKS

He points out that risks run even deeper than that, because cloud providers often don't tell you where they keep your data. Some outsource to other providers who then outsource to others. "You have what I call the spaghetti cloud, and you don't know where the spaghetti ends," says Carvalho. "It could end up in Russia, or Iran, or Pakistan, or in other locations where new data centers are springing up. Your data could be intercepted in transit, or a local government could look at it."

Carvalho stresses the importance of vulnerability scanning when moving assets into the cloud. "Have vulnerability scanners look at your assets from the inside out and also scan from the outside in, to give you the hacker's view," he says. The internal scan will be both authenticated and non-authenticated, to see if anyone can subvert processes. The external scan will let you see what the hacker sees and what vulnerabilities he or she might subvert. "You should check one scan against the other, and patch vulnerabilities quickly," Carvalho says.

The Internet of Things (IoT) represents another area of emerging vulnerability. "IoT is everywhere, smart cameras, dumb cameras, all sorts of sensors, SCADA devices, and companies that use PLCs [programmable logic controllers]. The whole world is producing IoT devices with few or no regulations at all," Carvalho says. He points out that the risks are great. For instance, if a phone uses facial recognition to enable a banking app, your face image is data that can be hacked. "You can change a password," Carvalho says, "but you can't change your face." 

*“Have vulnerability scanners look at your assets from the inside out and also scan from the outside in, to give you the hacker's view. Check one scan against the other, and patch vulnerabilities quickly.”*



# YOU MUST ACCOUNT FOR ENTIRELY NEW KINDS OF RISKS

Although there is no standard way to secure the vast array of existing and new IoT devices, Carvalho suggests a promising strategy. “You can use a blockchain approach where an entire set of devices of a particular type creates a baseline. Then if one device in the set is changed from the others, and the change is not authorized, that device is either automatically patched to match the others, or it is shut down.” A hacker would need to change all the devices at once in order to compromise one device, which would be practically impossible. This method would require continuous scanning to verify the devices. “It would be a kind of polling or heartbeat,” says Carvalho. “The scanner is continuously asking every device if it is still safe.” ■

## KEY LESSONS

- 1 You can have a provider with many certifications and service-level agreements in place, but providers will not be liable for your losses or for your non-compliance.
- 2 The network perimeter is growing thanks to technologies such as SaaS and IoT devices, yet still needs to be protected.



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

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

**Learn more about Tenable, our solutions and our global office locations, at [www.tenable.com](https://www.tenable.com).**