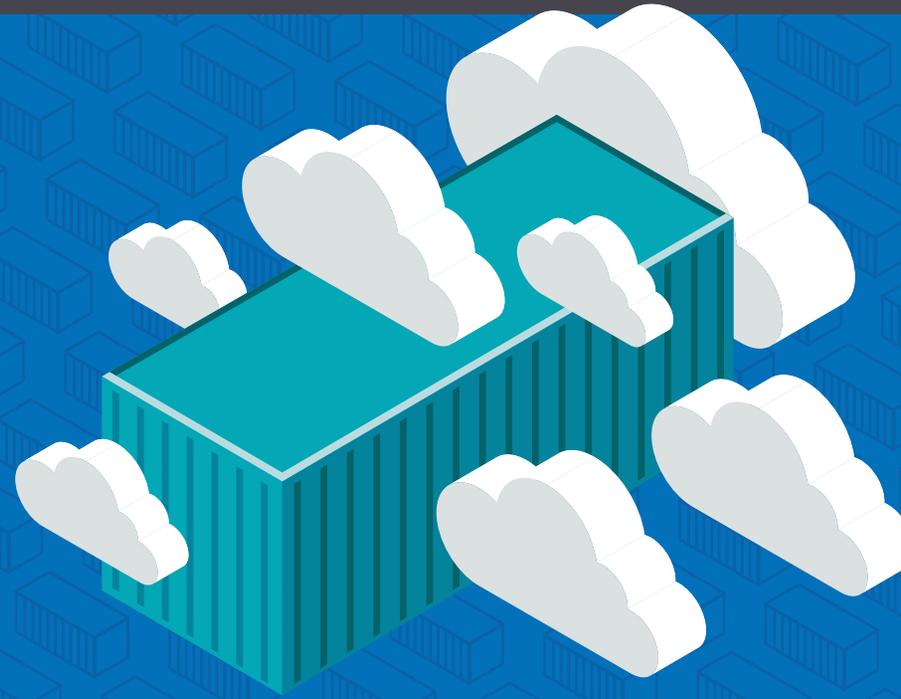


REDUCING CYBER EXPOSURE FROM CLOUD TO CONTAINERS

Lessons Learned by Industry Leaders



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 Networks¹ 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 data² 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 29 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.

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

TABLE OF CONTENTS

Foreword	2
Introduction	3
Securing a Dynamic IT Environment	
Digital Assets Provide Great Benefits, but Also Create Vulnerabilities Mark Nicholls.....	6
Collaboration Is Key to Securing a Dynamic IT Environment Carlos Lerma.....	9
You Must Account for Entirely New Kinds of Risks David Carvalho.....	13
Visibility into Your Entire IT Ecosystem Is Fundamental Floyd Fernandes.....	16
Managing Risk Requires New Levels of Visibility Lester Godsey.....	19
The Leap from Securing Static to Dynamic Assets Is a Management Challenge Mannie Romero.....	22
Innovative Identity Management Protects Modern Assets Cassio Goldschmidt.....	25
Maintaining a Love/Hate Relationship with Modern Assets Scott Estes.....	29
Rethinking Security for a Cloud Environment	
Cloud Services Force You to Reconsider Your Risk Model Javed Ikbal.....	33
Manage Security as a Shared Responsibility Andy Boura.....	36
You Must Recognize Hidden Costs and Hidden Risks Alex Wood.....	40
Securing Applications Is an Incredibly Complex Task Caleb Sima.....	42
A Segmentation Strategy Simplifies Securing Cloud Assets Chad Lorenc.....	45

Protecting Modern Assets Requires a Proactive Approach Isabel Maria Gómez González.....	48
Secure Your Assets, Wherever They Reside Arlie Hartman.....	51
Securing a Complex Ecosystem Requires a Layered Strategy Harshal Mehta.....	55

Moving Security to the Application Layer

Risk Management Decisions Must Be Made at the App Development Level Darwin Sanoy.....	59
You Must Manage Security Controls Differently When You Move Assets to the Cloud Lee Eason.....	62
A Fragmented Ecosystem Challenges a Coherent Security Strategy Avinash Tiwari.....	65
Shifting to Software Driven Data Protection Rory Alsop.....	69
Modern Assets Require a Disciplined, Step-by-Step Approach to Security Dilip Panjwani.....	72

Focusing on Data Security

Protecting Modern Assets Requires a Data-Centric Security Posture Antonio D'Argenio.....	76
Applying a Data-Centric Strategy in a Vast IT Ecosystem Eric Bedell.....	80
Businesses Must Focus on Protecting Information John Meakin.....	83
Life cycle Data Encryption Is Effective, But It Is Not a Magic Bullet Paul Heffernan.....	86

Automating Security Testing and Controls

Protect Modern Assets with Standards and Automation Michael Capicotto.....	90
Automate as Many Regularly Occurring Events as Possible Russ Kirby.....	94
Dynamic Assets Require Continuous Monitoring Jamie Norton.....	97
Automated Processes Become Your Configuration Items Joshua Danielson.....	101

SECURING A DYNAMIC IT ENVIRONMENT

In this section...



Mark D. Nicholls
Peabody.....6



Carlos Lerma
Beam Suntory Inc.....9



David Carvalho
OCS Group.....13



Floyd Fernandes
A Large Media Organization...16



Lester Godsey
City of Mesa, Arizona.....19



Mannie Romero
Optiv.....22



Cassio Goldschmidt
Stroz Friedberg.....25



Scott Estes
Major provider of construction services for the telecom industry.....29



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.**

COLLABORATION IS KEY TO SECURING A DYNAMIC IT ENVIRONMENT



**CARLOS
LERMA**

**Sr. Information
Security Architect,
Beam Suntory Inc.**

Carlos F. Lerma is a Sr. 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

For the past four years, Beam Suntory, one of the fastest-growing spirits companies in the world, has been moving more of its IT assets into a cloud environment. This has forced Carlos Lerma, its senior information security architect, to make many adjustments to his security practices. And as Lerma points out, "When we talk about the cloud, cloud is only one component. We are enabling many things to support business processes that we hadn't enabled before."

These include mobile devices and industrial controls. "Even though we're not heavily implementing open industrial controls at this time, SCADA ICS is the one that keeps me awake at night," he says, referring to Supervisory Control and Data Acquisition, and IP access to industrial controls. "That's the one that introduces the most complex challenges for any organization," says Lerma. "The traditional IT security triad of confidentiality, integrity, and availability now has to also consider the physical safety of electronic components."

So how is Beam Suntory adjusting to these new challenges? The very first thing involved gaining a better understanding of how these new systems really worked. "We had to learn how these services and connections were interacting with the outside world, but also with other internal applications and services, like SAP and web applications. >>>

“ When we talk about the cloud, cloud is only one component. We are enabling many things to support business processes that we hadn't enabled before. ”

COLLABORATION IS KEY TO SECURING A DYNAMIC IT ENVIRONMENT

With that understanding, they had better insight into the kinds of services they wanted to put on the cloud and how to make them available to users. “That’s how we started to understand the threats we were facing, and what we had to do to counter them from a security architecture perspective.”

From a process management perspective, Beam Suntory has changed several practices to gain better control of the new IT ecosystem:

- When it comes to introducing new technologies, IT Leadership has encouraged greater collaboration among IT project managers, business stakeholders, and the security practice. “A pure security architect is the one that gauges all the business drivers,” Lerma says. “When it comes to new IT initiatives, IT project managers know they have to get security involved during the design phase. I gauge the risks and security considerations. This is a process that we try to implement from the beginning of the project.”
- With mobile devices, Beam Suntory secures both BYOD devices and the company’s own devices that are managed through a third party. “We do lock down company-owned devices in terms of what they can and they can’t do,” Lerma says. “We’re moving to a policy-based scheme so we can be more nimble about deploying permissions into our devices.” 

“
The traditional IT security triad of confidentiality, integrity, and availability now has to also consider the physical safety of electronic components.
”

COLLABORATION IS KEY TO SECURING A DYNAMIC IT ENVIRONMENT

- Although Beam Suntory does not have its own DevOps shop and outsources much of its web app development, the company performs a review process before any app goes live. “Once we get the applications, before going live we scan them very extensively. If we find vulnerabilities, we kick it back to the developer to fix. It’s an iterative process that we drive in house. It’s been very successful in reducing risks and assuring the release of high quality applications,” Lerma says.

As the company grows and its IT infrastructure continues to change, Lerma sees collaborative involvement in the security process as key to successful security management. He says, “If we don’t have visibility into the purpose of new assets, if we don’t know what the main business goal is for those deployments, we’re pretty much in the dark when it comes to securing them properly.” ■

KEY LESSONS

- 1 When it comes to introducing new technologies, a more collaborative involvement of IT project managers, business stakeholders, and security architects results in better security.
- 2 One way to ensure security of outsourced web apps is to run vulnerability scans on them before going live. If they fail, keep kicking them back to the developers until they pass.



**JEFF
WILLIAMS**

CTO and Co-Founder,
Contrast Security



Twitter



Website



Blog



LinkedIn



It's way past time for organizations to realize how ridiculous it is not to expect web applications and APIs to be attacked. There is no perimeter, and there are no 'internal' applications. Application security isn't optional, it's the leading cause of breaches. The explosion of libraries and frameworks, APIs, containers, CI/CD, and other modern development practices have left traditional appsec practices and tools in the dust. Organizations should continuously inventory, assess, and protect every application and API in their portfolio.



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.

VISIBILITY INTO YOUR ENTIRE IT ECOSYSTEM IS FUNDAMENTAL



**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 and information security in a range of industries across financial, 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 and operations.



LinkedIn

Securing a large global network of heavily used digital assets is Floyd Fernandes' unique challenge. As vice president and chief information security officer (CISO) at a large media organization, Fernandes is responsible for securing a top 10 web property accessed by 190 million unique visitors each month, and assuring secure IT operations for the development of these sites. This all happens in an environment where IT assets are no longer hidden behind a defensible perimeter. Now they can be anywhere: They are mobile. They are in the cloud.

And as Fernandes points out, "We extend that even further as we move to a paradigm of containers and immutable images and serverless computing. You're in a situation now where a service or a container may only live for 60 seconds. It comes up to do a task and then disappears." 

“ There is no way you could do this unless there was a high degree of automation built into your systems. ”

VISIBILITY INTO YOUR ENTIRE IT ECOSYSTEM IS FUNDAMENTAL

Operating in this more fluid IT environment has required changing the way assets are protected. Fernandes describes three particular challenges and ways to deal with them:

- Perhaps the most fundamental element in securing dynamic digital assets is visibility. “To understand your risk and protect your assets, you must have tools and applications that give you visibility into everything,” says Fernandes. This is not so easy, especially in public cloud environments where the service providers don’t allow you inside the infrastructure. Achieving the visibility you need requires new strategies, such as creating a virtual instance that can monitor the orchestration layer as short-lived assets come and go, and using APIs to capture the metrics you need. “We’ve gone from a hardware-centric approach to software-driven visibility to document our IT assets and activities,” says Fernandes.
- Automation is essential, and real-time provisioning and analysis depends on it. Whether you are reverting to golden images for short-lived assets, or tracking virtual machine (VM) and container formation in real time, or orchestrating a blue-green approach to patch management in complex environments, automation becomes hugely important. “There is no way you could do this unless there was a high degree of automation built into your systems,” he says. 

“
You’re in a situation now where a service or a container may only live for 60 seconds. It comes up to do a task and then disappears.”

VISIBILITY INTO YOUR ENTIRE IT ECOSYSTEM IS FUNDAMENTAL

- Only allow known things to connect to your network, Fernandes says. “With mobile devices, it goes back to visibility. Do I know what is connecting to my network? If I do, does it pass enough integrity for me to allow it to connect?” It’s easier to answer these questions in some cases than in others. For instance, in the case of consumers, you can create a secure mobile application that you put in an app store. That app will limit what that user or device can do in the network. Employee devices, especially bring-your-own-device (BYOD), are more difficult, and when these are connecting through unverified hot spots in an internet cafe or in a foreign country, you have to be especially careful. “From a vulnerability management perspective, you want to know that machine is in a certain state that meets your requirements before you allow it to connect,” Fernandes explains. “You’re specifying a minimum set of standards for allowing any device to connect.”

It all comes back to having visibility into the digital assets you are trying to protect, whether they are in the data center or in the cloud, plus visibility into your mobile footprint, and visibility into your customer footprint. ■

KEY LESSONS

- 1 It all comes down to having visibility into the digital assets you are trying to protect, whether they are in the data center or in the cloud.
- 2 Whether you are reverting to golden images for short-lived assets, tracking container formation in real time, or orchestrating patch management in complex environments, automation becomes hugely important.

MANAGING RISK REQUIRES NEW LEVELS OF VISIBILITY



**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 has presented at the local, state, and national level on topics ranging from telecommunications to project management to cybersecurity. Lester 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

In the seven years that Lester Godsey has been involved in IT and security at the City of Mesa, he has seen continual growth and expansion of the network perimeter. “One of the overarching themes from my cybersecurity program is that our network perimeter is constantly expanding in ways that are not always visible to us,” he says, adding that traditional cybersecurity tools and methodologies do a great job in identifying and protecting assets within the network environment.

“It’s those dynamic IT assets such as software as a service, platform as a service, infrastructure as a service, and the proliferation of IoT devices that are making everybody’s jobs in the cybersecurity realm so challenging,” he continues.

The essential problems of risk management do not change, regardless of your IT ecosystem. “You’re still applying the same methodology to answer questions about what’s in the environment, what’s the probability of something happening, and what its impact would be,” Godsey says. “You’re balancing probabilities of something happening against the impact of that thing. That’s the core of any risk-management plan.” The key is expanding these methodologies to cover the new and changing IT landscape. 

“You’re balancing probabilities of something happening against the impact of that thing. That’s the core of any risk-management plan.”

MANAGING RISK REQUIRES NEW LEVELS OF VISIBILITY

Godsey has seen changes in security technologies and practices that provide more visibility and control over activities involving new kinds of assets, especially those operating beyond the perimeter. There are numerous changes to consider.

More advanced endpoint protection with endpoint detection and response (EDR) solutions. “This has come about because traditional antivirus solutions are no longer adequate for protecting the diverse and dynamic endpoints that contact the IT ecosystem,” he explains.

“There has been a consolidation of security functions into higher power solutions,” says Godsey. “For example, we’re now seeing solutions out there where there’s firewall capability, deep packet inspection, VPN functionality, and multi-tenant capability, all built into a next-generation firewall that combines functions that were once performed by separate, stand-alone systems.” These capabilities enable greater flexibility and the kind of deeper inspection of network traffic that is necessary for the more context-based security strategies complex IT environments require. 

“
IoT devices can expand the perimeter of your network in ways that you may not even be aware of.”

MANAGING RISK REQUIRES NEW LEVELS OF VISIBILITY

There have also been changes in basic security practices to accommodate more dynamic IT environments. “Scanning is a good example,” Godsey says. “We were already doing that pretty frequently. To put this into perspective, to be PCI compliant, level 3 merchants must do a vulnerability scan on their systems once each quarter. For the past couple of years, we have been scanning once a week.”

“IoT devices are changing the cybersecurity game,” says Godsey. “In addition to traditional endpoints such as printers and PCs, cybersecurity professionals now need to be concerned with TVs, web cameras, or anything else that connects to the Internet.” He continues, “IoT devices can expand the perimeter of your network in ways that you may not even be aware of.”

Even with these kinds of changes, the fundamental security problems have not changed. “Most tried-and-true approaches are still good,” Godsey comments. “They just have to be expanded in such a way that they accommodate the new landscape, especially with new IoT devices, software as a service, and other kinds of more dynamic services.” ■

KEY LESSONS

- 1 The essential problems of risk management do not change. The key is expanding these methodologies to cover the new and changing IT landscape.
- 2 The network perimeter is growing thanks to technologies such as SaaS and IoT devices, yet still needs to be protected.

THE LEAP FROM SECURING STATIC TO DYNAMIC ASSETS IS A MANAGEMENT CHALLENGE



MANNIE ROMERO

Executive Director,
Office of the CISO,
Optiv

Mannie Romero has more than 20 years of technical and information security experience in multiple disciplines including incident response, offensive security, crisis management, forensics, vulnerability management, application security, network security, governance, risk, and compliance. Mannie holds several security certifications, including the OSCP, CISSP-ISSEP, GPEN, and GCFE. He has also earned degrees in electrical engineering technology from New Mexico State University and an MBA from the University of Phoenix.



Twitter | LinkedIn

As executive director of the office of the chief information security officer (CISO) for Optiv, one of the largest holistic pure-play cybersecurity solutions providers in North America, Mannie Romero has witnessed several content revolutions as companies struggled to figure out exactly which assets they needed to protect. “As an industry, we’ve historically not been that great at asset inventory and asset management,” he says. This was true even when most important assets were static and sat primarily in private data centers.

“And now we are reaching what a lot of people are calling the third platform’s computing revolution based on big data, social networks, mobile, and cloud computing with dynamic assets such as VMs (Virtual Machines) and containers that spin up and down at a rapid rate,” adds Romero. “That makes security a much bigger challenge.”



“Network people who are used to running discovery scans on the system now have to move up the stack to applications and start learning APIs in AWS, Azure, and other cloud infrastructures. It’s a struggle.”

THE LEAP FROM SECURING STATIC TO DYNAMIC ASSETS IS A MANAGEMENT CHALLENGE

This, according to Romero, has led many companies to take inappropriate steps to secure their data, especially if they don't have a hierarchy of assets or even a complete inventory. "Typically, when people don't have an idea of how important and where their data is," he says, "their usual reaction is to try to protect everything at the highest level." Because such high-level security is difficult to maintain and can affect revenue by investing too many resources in non-critical data, this approach is prone to failure.

"Where shadow IT in the past might have been a very small percentage," says Romero, "we've moved into a different model, which is continuous integration, continuous deployment, and a DevOps model, where that's no longer the exception but that's the norm. So now, when you ask 'what are your assets?' people point you to an API and say, 'this is what my assets are today.' What that's forced people to do is, everybody is kind of having to move up the chain. So people who were network people in the past and are used to running discovery scans and doing things on the network and the system, now have to move up the stack to the applications and start learning APIs in AWS, Azure, and other cloud infrastructures. It's a struggle."

The situation is only going to get more challenging, says Romero, as artificial intelligence, robotics, machine learning, and the Internet of Things become more prominent and widely deployed. "Although these dynamic assets are spinning up and spinning down," says Romero, "you can view it as an opportunity as well as a challenge—with the DevOps model, people are making updates and changes continually, so there's a lot of opportunities we didn't have before to fix security issues very fast." 

“If a container has a vulnerable piece of software, and the security team is in a DevOps model, they can work quickly, fix the container image, and the next time that container gets spun up, it is secure.”

THE LEAP FROM SECURING STATIC TO DYNAMIC ASSETS IS A MANAGEMENT CHALLENGE

So what is it about DevOps that puts these challenges into reasonable perspective? “If a container has a vulnerable piece of software, and the security team is in a security DevOps model,” says Romero, “they can work quickly, fix the container image and likely, the next time that container gets spun up, it is secure. That is a reaction time measured in days, and you don’t have to deal with thousands and thousands of systems. You only have to deal with the golden image of that container. So there are a lot of opportunities that security teams can take if they embrace the DevOps model.”

Finding the right talent to embrace this new model is not easy, according to Romero. “I think for the first couple of years, people went out and tried to find application security people and cloud security architects for this work,” says Romero. “And we quickly found out that there’s not a whole lot of them on the shelf—you actually have to make ’em. And so, creating pipelines where you’re getting software developers that want to direct their career into application security is important.

“And there are computer scientists and computer engineering folk that have an affinity for security—they have all the base elements and technical knowledge that they need, now they just need to familiarize themselves with the cybersecurity world and get those security skills. So we see a lot of the most successful security programs attracting and training the security talent they need.” ■

KEY LESSONS

- 1** Maintaining high-level security across all assets is a resource drain in large enterprises. Security leaders need to analyze cyber exposure so they can segment risk based on asset criticality and vulnerability.
- 2** The shortage of security talent in this new world of modern assets means that security pipelines will rely more on DevOps and cloud engineers with security skills acquired on the job.

INNOVATIVE IDENTITY MANAGEMENT PROTECTS MODERN ASSETS



**CASSIO
GOLDSCHMIDT**
Vice President,
Stroz Friedberg

As VP in Stroz Friedberg's Cyber Resilience practice, Cassio Goldschmidt leads engagements that help clients proactively identify, validate, and prioritize information and cyber risk. With almost 20 years of experience, Goldschmidt brings a balanced technical and business perspective to aid organizations in managing both product and program-level security. Outside work, Cassio is known for his contributions to the Open Web Application Security Project, Software Assurance Forum for Excellence in Code, the Common Weakness Enumeration (CWE)/SysAdmin, Audit, Network, Security (SANS) Top 25 Most Dangerous Software Errors, and his contributions to security education.

Cassio Goldschmidt believes that identity management is a crucial factor that must not be overlooked when protecting modern assets. Whether an organization is facing a phishing attack, a brute force attack, or a website breach, insecure passwords often make the exploit more likely to succeed. "Mobile devices, phones, and other types of devices require multifactor authentication. Internet assets also require some type of authentication. People always think about these kinds of things using passwords but, truth be told, passwords are in the process of being phased out," explains the vice president, cyber resilience practice, at Stroz Friedberg, a risk-management firm.

So what forms of authentication are being used in conjunction with passwords or replacing them altogether? Biometrics is one, according to Goldschmidt. If, for example, you call a financial institution for help with your account, it may no longer request your social security number to verify your identity. "Some companies are using a voice-recognition system, where they'll ask you to say a phrase aloud as a form of authentication. They can actually see that it's you because of the way you pronounce words and the manner of your speech," he says. 

“Some companies are using a voice recognition system, where they'll ask you to say a different phrase aloud each time you call as a form of authentication.”

INNOVATIVE IDENTITY MANAGEMENT PROTECTS MODERN ASSETS

Another form of biometric authentication that Goldschmidt is familiar with involves cameras, whether in a smartphone or located elsewhere at a company. “A phone camera can look at the veins in a person’s eyes and tell who they are. Like fingerprints, they are unique for each person,” he says. Such biometric identification methods like this, of course, require you to be close to a device you own—which makes it harder for hackers to gain access to it remotely because it requires both something the user is and something the user has.

Of course, protecting modern assets also requires careful attention to other aspects of security. Goldschmidt, who consults for a number of businesses at Stroz Friedberg, feels that it is important to make your attack surface as small as possible—that is, to take a close look at what you have in place and disable what you don’t need. You may also have to segregate certain assets from the main corporate network so as to make it harder for a hacker to compromise one device or instance and then leverage it to stage a broader attack within the company. 

“
A camera can look at the veins in a person’s eyes and tell who they are. Like fingerprints, they are unique for each person.
”

INNOVATIVE IDENTITY MANAGEMENT PROTECTS MODERN ASSETS

Creating a centralized monitoring and alerting system, particularly one that monitors the data leaving your network—since a breach typically involves data getting out rather than coming in—is also critical for a business that wants to protect its sensitive information. “For some companies, it may make more sense to engage the professional services of people who are doing this for a living so that they can focus on their core business. Just like we treat electricity today, it’s a service that somebody else can provide,” he adds.

Protecting modern assets is challenging, Goldschmidt acknowledges, but identity management is a great starting point. By taking advantage of advanced authentication methods such as biometrics and applying multiple authentication methods, an organization can build more resilient defenses against an attack. This is one powerful way to guard the business amid a complex and evolving threat environment. ■

KEY LESSONS

- 1 Authentication is often key to protecting modern assets, regardless of the type of attack.
- 2 It is important to make your attack surface as small as possible—that is, to take a close look at what you have in place and disable what you don’t need.



**DANIEL
MESSLER**

Director of
Advisory Services,
IOActive



Twitter



Website



Blog



LinkedIn



Significant risk is introduced through the disconnect between expectation and reality. The center of vulnerability for most organizations today is the lack of asset management. Having so many web apps, so many cloud apps, and so many shadow assets raises the risk in an organization to extraordinary levels for the simple reason that you can't defend what you don't understand.



MAINTAINING A LOVE/HATE RELATIONSHIP WITH MODERN ASSETS



SCOTT ESTES

Director, Site Reliability, Infrastructure, and Security,
Major provider of construction services for the telecom industry

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 5+ nines of high availability for the businesses he supports.



LinkedIn

“There is always a vulnerability somewhere,” says Scott Estes, director of site reliability, DevOps, and security for a major provider of construction services for the telecom industry. “If you incorporate new technologies into the business without carefully planning for attacks, you’re going to open up the company to liability.” This is especially true when it comes to dealing with modern assets such as the cloud infrastructure and mobile applications. “As technology becomes a bigger part of our lives, and businesses take their non-technical audiences and start injecting their jobs with technology, they don’t always understand the consequences,” he comments.

To demonstrate his point, Estes cites two examples. “I’ll give you a technical example and a non-technical, human-factor example. The technical areas that really concern me are container and serverless computing. I love containers and I love serverless computing – they’re great technologies, but I believe they are forcing us as a community and as an industry to up our game. Applications deployed via containers are easy to deploy. They can be efficiently deployed, decommissioned, redeployed, without affecting other containerized applications that may be running on the same host. But if a hacker manages to gain control of the host operating system, all the containerized applications are at risk of being compromised. »»»

“If everyone is thinking about security, (think neighborhood watch) as they go about their daily routines, the overlooked, “little” things that can lead to some of the massive data breaches we’re seeing today can be accounted for properly.”

MAINTAINING A LOVE/HATE RELATIONSHIP WITH MODERN ASSETS

For the non-technical, human factor, Estes explains that something seemingly as harmless as watching movies on a company-sponsored device during your lunch hour can expose the system to vulnerabilities if someone gets hold of the employee's password through the application that is providing the video stream. "Vulnerabilities are everywhere and getting the non-technical audience to understand not just the importance of, but the absolute requirement for, security of their work devices and the technology that they use, that's a huge challenge," he says.

He adds: "Modern assets have forced businesses to acknowledge that security is not some esoteric religious thing that we put off in a place somewhere and that we only talk to employees about when we absolutely have to. We've got to take this seriously and collaboratively. You have to look at security completely differently now," he says. "You have to budget differently, you have to plan differently, and everyone has to be involved, from developer to manager to supervisor to receptionist." 

"You have to look at security differently now. You have to budget differently, plan differently, and everyone has to be involved, from developer to manager to supervisor to receptionist."

MAINTAINING A LOVE/HATE RELATIONSHIP WITH MODERN ASSETS

For example, says Estes, “You still have to do security reviews, but you don’t wait until the end of the project to do them. Ongoing security training, (tailored for the audience) is a must for everyone. If everyone is thinking about security, (think neighborhood watch) as they go about their daily routines, the overlooked, ‘little’ things that can lead to some of the massive data breaches we’re seeing today can be accounted for properly.”

When you have successfully built what Estes calls “a security culture,” you start to see a more pragmatic, inclusive, and successful approach to security. ■

KEY LESSONS

- 1** Modern assets are forcing a new way of approaching security, whereby everyone in the organization must take security seriously and understand the potential consequences of even the simplest action.
- 2** Security teams are no longer the gating factor they once were. Security needs to be built in at every level and as early in each process as possible.

RETHINKING SECURITY FOR A CLOUD ENVIRONMENT

In this section...



Javed Ikbal
Bright Horizons.....33



Andy Boura
Senior security architect.....36



Alex Wood
Pulte Financial Services.....40



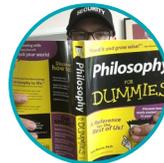
Caleb Sima
Capital One.....42



Chad Lorenc
Keysight Technologies.....45



Isabel Maria Gómez González
Bankia.....48



Arlie Hartman
KAR Auction Services.....51



Harshal Mehta
Carlson Wagonlit Travel.....55

CLOUD SERVICES FORCE YOU TO RECONSIDER YOUR RISK MODEL



**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 and security experience in financial services, industrial research, and education. He also teaches graduate-level Information Security courses at Brandeis University in Waltham, MA. Javed Ikbal specializes in building or re-engineering security programs.



LinkedIn

Moving IT assets into the cloud creates new security challenges, but what is the exact nature of those challenges, and how do you best manage them?

“I don’t see this as a new security problem. I see this as a governance problem,” says Javed Ikbal. He compares it to the earlier days of mainframe computing when people logged in at a terminal, did their work, and got billed by the hour or minute. The mainframe itself may have been located far away and shared by other users. This model mostly went away with the arrival of powerful desktop computers.

“Now with cloud services, we are going back to a common platform model,” Ikbal explains. “We don’t know where the computer is, and we only pay for the capacity we use. We need to rediscover how to minimize those risks, but people have done that work before, so we don’t have to start from zero.”

One thing that changes is how you manage risk tradeoffs. For example, Bright Horizons used to back up all its data every night to another data center. Now they back up to the cloud every few minutes, reducing exposure in a worst-case data loss scenario. That’s a clear risk management advantage, but it also poses a new risk. “The risk is putting that data where we have no idea what goes on in the building,” Ikbal says. “We are relying on somebody else’s audit, and we have no idea what that person does. It introduces new risk models we need to address.” He points out that even though there are new risks, you’re still dealing with the same principles covered in your existing framework. 

“It’s not even a question of controlling access. It’s a question of knowing what’s happening.”

CLOUD SERVICES FORCE YOU TO RECONSIDER YOUR RISK MODEL

Another area of change is that IT is no longer the gating factor for IT infrastructure. In the past, if you needed a new server or a new application, you went to IT. Now business groups can launch cloud-based services, and employees can easily leak or send sensitive information over cloud-based document sharing services or email. All of those resources are outside the traditional perimeter with limited controls over access. But, adds Ikbal, “It’s not even a question of controlling access. It’s a question of knowing what’s happening.”

He speaks from experience, having once learned about plans to adopt a new cloud CRM product when one of the business groups was ready to sign a big contract with a CRM service provider. Ikbal immediately realized this presented a security problem. His company made promises about how they secured client information, but now a business unit was signing up for a service without thinking about how it affected the security of client data they planned to put into the CRM. Ikbal says, “One danger of the cloud is that with IT no longer the gatekeeper and with security watching over things, data in the cloud may mean data in the wrong hands: a data breach. As the security guy, I have to step in and stop it, which makes me the preventer of information services.” Of course Ikbal needs to be an enabler, not a preventer. 

“
One danger of the cloud is that with IT no longer the gatekeeper and with security watching over things, data in the cloud may mean data in the wrong hands: a data breach.
”

CLOUD SERVICES FORCE YOU TO RECONSIDER YOUR RISK MODEL

To avoid this problem, Ikbal implemented a rule that any cloud expense over a certain amount now has to be approved by security in advance, and any service contracted with a new service provider requires automatic security review. These rules helped eliminate surprises. But regardless of where the asset is located, it still comes back to fundamentals, says Ikbal. “Whether it’s in the cloud or on-prem, you have to do the same things—encrypt data, only give access to those who need it, and make sure nobody can break in.” ■

KEY LESSONS

- 1 With business groups launching and using cloud-based services, IT is no longer the gating factor for IT infrastructure.
- 2 Risks change, but whether it’s in the cloud or on premises, you still have to encrypt data, only give access to those who need it, and make sure nobody can break in.

MANAGE SECURITY AS A SHARED RESPONSIBILITY



**ANDY
BOURA**

**Senior Information
Security Architect**

Andy Boura, who has held technical and security positions at a large information systems and services company since 2007, is currently a senior information security architect at the media corporation. He employs a top-down approach to handling structure and security challenges, empowering organizations to manage technology risk proactively. Boura has provided security leadership on high-profile projects and has contributed to many of the foundational standards of the company's products and data center network infrastructure. Previously, he worked as a technical team leader at AVT, a financial software start-up.



Twitter



LinkedIn

One of the biggest changes to security and risk management that comes from moving IT assets to the cloud is the shift from an IT stack to a compositional model of application building. The move doesn't change what you need to secure, but it completely changes how you manage security and risk.

Andy Boura, senior security architect for a large information systems and services company, explains the significance of this change. "It used to be that you maintained layers in a stack. You had an operating system in your data center. Perhaps you ran some middleware, your app ran on top of that, and you'd link in some libraries. With a cloud architecture, there's a shift to a compositional model where you actually decompose the application into separate modules. Those modules could be running in different data centers, different organizations, and different clouds." Boura says that this compositional or microservices architecture changes risk management from focusing on security life-cycle activities and governance to focusing more on a complicated supply chain with third-party risk management. 

“ You actually decompose the application into separate modules. Those modules could be running in different data centers, different organizations, and different clouds. ”

MANAGE SECURITY AS A SHARED RESPONSIBILITY

He cites the example of a simple experimental app that he built. He uses one company for user authentication, another for a real-time NoSQL database, Amazon Simple Storage Service to store the static content for a web page, Amazon's Domain Name System and Secure Sockets Layer services, and its content distribution network. His app also has federated authentication so that users can sign in with their Facebook or Google ID. Boura says, "I've got five companies underpinning one simple experimental web application. To the end user, it looks like one app."

In this kind of ecosystem, managing security and risk becomes a responsibility shared among the companies buying those services and the third parties that provide them. Service level agreements (SLAs) must spell out exactly which security controls and protections the purchaser expects from the third party and the evidence the vendor must provide to demonstrate that it is meeting those expectations. One might think that this creates a level of complexity that makes managing security more difficult, but that's not necessarily the case:

- Each modular component of the system has a specific role. A vendor supplying one component is 100 percent focused on getting that piece right from a security and availability perspective. Boura says, "Because these components are often commodity offerings, you can switch suppliers reasonably easily. That gives the third party a lot of incentive to deliver a high level of service."



“Working with third parties and their teams rather than in-house teams forces you to spell everything out in SLAs. It becomes much clearer how responsibilities are carved up.”

MANAGE SECURITY AS A SHARED RESPONSIBILITY

- The microservices model provides an opportunity to more clearly enforce good practices. Boura points out that if you had a monolithic application you had built entirely in house, you'd actually still have the same attack surface and the same amount of functionality to worry about. You would still have all the security controls and monitoring and access to resources to troubleshoot or respond to anything related to availability or security. "You always had to do everything that you have to do in the new model," he says. "But now, you're working with third parties and their teams rather than in-house teams, and that forces you to spell everything out in SLAs. It becomes much clearer how responsibilities are carved up."

Boura says that one key to successfully applying a shared-responsibility approach to IT security and risk management is to clearly understand where your vendor's capabilities and responsibilities end and where yours begin. "Vendors can make sure that no one can access your data without proper credentials, but they're not responsible for making sure you've correctly configured permissions," Boura says. "Perhaps they have the capability to warn you if it looks like you're making a mistake, but that may just be their added value rather than part of the service level they've agreed to deliver." In that case, you would be responsible for your own processes and controls to assure proper configurations. "It's critical to understand what that breakdown is and make sure that you are fulfilling your own responsibilities," says Boura. ■

KEY LESSONS

- 1 Moving to the cloud doesn't change what you need to secure, but it completely changes how you manage security and risk.
- 2 Successfully sharing responsibility for IT security and risk management means clearly understanding where your vendor's capabilities and responsibilities end and yours begin.



**LAURA
BELL**

Founder and CEO,
SafeStack



Twitter



Website



Blog



LinkedIn



Gone are the days when we just have one border. Our politely defined corporate networks are now expanding and evolving to form a distributed mesh of risks. From the large increase in technology variety, to the difficulties in protecting, tracking, and consistently configuring this mess of tools and devices...it's no wonder risk management has to evolve. If our technical environment is evolving this quickly, our security and risk management must be equally agile.



YOU MUST RECOGNIZE HIDDEN COSTS AND HIDDEN RISKS



**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.

As chief information security officer (CISO) at Pulte Financial Services, a homebuilding company that also provides a variety of financial services and online customer engagement, Alex Wood oversees the security of all financial services systems, including cloud-based assets. Like many companies, Pulte Financial Services has increased its use of cloud services and web applications. Because of the way cloud services work and the fact that you generally don't have direct administrative access to cloud infrastructure, it's necessary to approach security differently in this environment.

Wood says, "If you traditionally had all of your infrastructure in your own data center, and now you're moving some or all of that to a cloud provider or some other external service, some security controls will remain under your management, and some you will hand off to the service provider." This does not mean you need to scrap your security program and start over, or throw out your security framework. In fact, having more mature security processes in place puts you in a better position to define who's responsible for what in this extended infrastructure. "Your existing program or framework becomes the starting point of a discussion about what controls you need the provider to manage, and what additional services you will need to implement to manage the risks in the extended infrastructure," says Wood. He adds that it is important to recognize your service provider may not have those controls working the way you have implemented them. You may need to be creative in working with the provider to figure out how to meet your security objectives.



“ Your existing program or framework becomes the starting point of a discussion about what controls you need the provider to manage. ”

YOU MUST RECOGNIZE HIDDEN COSTS AND HIDDEN RISKS

Wood believes there are two areas that people often overlook when they are moving assets off premises:

- Companies often think they are moving to the cloud because it's cheaper. But some of the controls they currently use to manage risk aren't built into the cloud provider's base cloud service. You need to rethink how you are going to achieve the level of security you need. "That may mean you actually have to increase your budget for cloud security controls to have the same level of security as you get from your own infrastructure," Wood explains.
- There needs to be a clear understanding of where security liability lies. If you are collecting customer data or providing a service to your customers, no matter who your cloud provider is, you are still responsible for making sure there's proper regulatory compliance. "You need to be sure, through contractual obligations, that you're on the same page with your provider. For that very reason it's important that the security team be involved in selecting service providers handling your IT assets," he says.

Woods points out that while a service provider may be attractive from a business perspective, there are other considerations. If engaging them increases your risk on the security side, you might have to offset that in some other way with additional security investments. It's important that the business understands the change in risk so it can fully account for it. ■



KEY LESSONS

1 Having more mature security processes in place puts you in a better position to define who's responsible for what in this extended infrastructure.

2 Any time you collect customer data, regardless of who your cloud provider is, you are still responsible for making sure there's proper regulatory compliance.

SECURING APPLICATIONS IS AN INCREDIBLY COMPLEX TASK



**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 and 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 start-up, where he was CTO and founder of SPI dynamics.



Twitter



LinkedIn

Protecting modern assets can be a particularly challenging task when many organizations are still dealing with a lack of ownership in security, says Caleb Sima. Not long ago, in an on-premises world, a business could enjoy complete control of its environment—from the servers and the operating systems to their implementation, configuration, and management. But now, Sima explains, “when we move into this new cloud-based infrastructure, it’s a challenge because these dynamic instances are owned and operated by a separate entity.”

At this point, organizations start losing some of their controls as well as some of their visibility, and that poses difficulties from a security perspective. For example, if a business is looking at taking advantage of Elastic Block Storage and other enterprise services offered with Amazon Web Services (AWS), Sima says, “We just don’t have the visibility or the ability to configure an asset like this properly. It might be our EBS for instance, but it’s stored somewhere else, shared among millions of other customers in a data store somewhere in AWS.”



“ When we move into this new cloud-based infrastructure, it’s a challenge because these dynamic instances are owned and operated by a separate entity. ”

SECURING APPLICATIONS IS AN INCREDIBLY COMPLEX TASK

When attempting to protect assets in the midst of these constraints, important questions arise. “What happens to that data? Who has access? How do we do our jobs effectively if, for example, we don’t have access to this type of information?” Sima asks. An organization may take different measures to secure its mission-critical data depending on its size, its industry, and other unique characteristics. At Sima’s company, where regulation is a factor, they take what he calls a hybrid approach. “We store the really sensitive data that we want in our control on-premises. Everything that’s not as critical can be placed in the cloud infrastructure. That allows us both to abide by regulations more easily and at the same time get greater assurance as to our sensitive data—what we can control on-premises versus externally.”

Another type of business might adopt a different method for securing its assets, however. “If you’re a start-up, for example, I would say you might not necessarily need to store some of your data on-prem as we do, and the cloud might be fine. But you just have to be careful about how you secure that data. You will probably want to take advantage of methods like encryption and tokenization so that you can store it somewhere else and still take full advantage of a hundred percent cloud.” In that scenario, says Sima, “It is the CISO’s job to say, ‘Okay, that’s where you’re going, let me figure out what I need to do on my end to help you do that in a more efficient and safe manner.’” 

“
It is the CISO’s job to say, ‘Okay, that’s where you’re going, let me figure out what I need to do on my end to help you do that in a more efficient and safe manner.’
”

SECURING APPLICATIONS IS AN INCREDIBLY COMPLEX TASK

By taking a careful, considered approach to protecting its modern assets, one that takes into account the organization's unique security requirements, a business can ensure that its most sensitive data is secured even within a dynamic, evolving technology landscape. ■

KEY LESSONS

- 1 While the cloud offers many benefits, businesses face challenges in securely managing and obtaining visibility into their assets.
- 2 Organizations that adopt a hybrid approach to keep their most valuable assets on premises will need to seamlessly protect assets across on-prem and cloud infrastructures.

A SEGMENTATION STRATEGY SIMPLIFIES SECURING CLOUD ASSETS



**CHAD
LORENC**

Senior Security Architect,
Keysight Technologies

Chad is a committed 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 three-month sabbatical he took with his family to do humanitarian work in Haiti, where he trained locals in IT Security.



LinkedIn

As a company providing test equipment and services for a variety of industries, Keysight Technologies has been shifting more of its operations into the cloud. “A lot of my work has focused on how we redesign the network in an intelligent way to protect our assets while leveraging new transformational technologies we are able to deliver,” says Chad Lorenc.

Keysight faces some interesting challenges, not the least of which involves converting hardware products, such as test equipment, into software products. Lorenc says, “One of our big risks used to be competitors reverse engineering our hardware to steal our intellectual property. But now our intellectual property is starting to be software, and that dramatically changes our risk profile.”

Several years ago, when Lorenc’s team was designing a new data center, the staff decided to step back and take a hard look at their long-term needs. “Cloud services were emerging,” says Lorenc, “so we sat down and worked to boil out that impossible IT goal of defining our 10-year strategy.” Much of this work was done with the idea of moving to a software-defined networking environment. Although SDN was not mature enough to meet their needs at that time, they successfully developed a security strategy that would be “SDN” ready. 

“ We can now quickly configure and provision security requirements by simply assigning resources to an appropriate zone. ”

A SEGMENTATION STRATEGY SIMPLIFIES SECURING CLOUD ASSETS

To do this, they extensively researched different approaches to security and found that many enterprises segmented their security needs. “We found there are two basic approaches to segmentation,” Lorenc says. “One segments by risk, where you put all your high-risk, medium-risk, and low-risk things together in their own groups. The other segments by functionality, where you isolate functional groups down to the app level.”

This enabled them to create an operational security matrix that laid 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 became a “container” or zone with its own controls and security configurations. Activities happening in one zone could not leave that zone.

This strategy has made it possible for Lorenc’s team to manage the different security needs of customers, partners, and data assets more easily through modular access controls, auto provisioning, and more efficient use of resources such as firewalls and other security tools. “We can now quickly configure and provision security requirements by simply assigning resources to an appropriate zone,” says Lorenc. “Once something is assigned to a zone, it’s built into that zone, and it automatically inherits all the controls for that zone.”



“
Once something is assigned to a zone, it’s built into that zone, and it automatically inherits all the controls for that zone.
”

A SEGMENTATION STRATEGY SIMPLIFIES SECURING CLOUD ASSETS

Segmentation also enables Lorenc to overlay specific controls for things like vulnerability scanning and patch management based on whether something is in a low-, medium-, or high-risk zone. And Lorenc points out that this segmented approach helps quickly determine if unusual events are benign or threatening. “If we see something kick off 500 admin requests from the tools zone, that’s probably legitimate. But if we see the same request coming out of the high-risk app zone, now we know it’s a high-priority incident.”

An additional big benefit of this segmentation strategy is that it has enabled Keysight to seamlessly migrate security controls into the cloud environments where they are increasingly delivering their products as software solutions. ■

KEY LESSONS

- 1 **Micro-segmentation simplifies the use of modular access controls and auto-provisioning to more easily manage security needs of many different customers, partners and assets.**
- 2 **With micro-segmentation, you can overlay specific controls for vulnerability scanning and patch management based on whether something is in a low-, medium-, or high-risk zone.**

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.
”

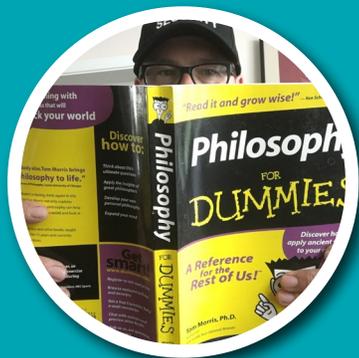
PROTECTING MODERN ASSETS REQUIRES A PROACTIVE APPROACH

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.

SECURE YOUR ASSETS, WHEREVER THEY RESIDE



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

Since joining KAR Auction Services as information security architect, Arlie Hartman has worked to transform the company's vulnerability management across an infrastructure that is constantly changing through growth and acquisition. As one of the largest providers of remarketing services to the wholesale used-car industry, KAR has extensive partner relationships with banks, insurance companies, and auto manufacturers. It offers auction sales that are streamed online, and financial services. "We have very large customers, our networks are connected to theirs, and they have stringent security requirements," says Hartman.

Hartman spends about 20 percent of his time transitioning IT security from acquired businesses so those infrastructures comply with KAR's requirements. He spends the other 80 percent managing vulnerabilities in their on-premises assets and transitioning some of those assets to the cloud. "In addition to improving availability and scale, we must create standards that maintain or improve the security of those assets," he says. 

“ Anybody with a corporate credit card can set up an instance, and the next thing you know, you're finding sensitive information in S3 containers on Amazon. ”

SECURE YOUR ASSETS, WHEREVER THEY RESIDE

These activities are complicated by the fact that ongoing operations generate constant changes to the infrastructure. “We have several hundred developers working within three different public cloud environments, standing up instances, using API keys, and all those things that make security people stay up at night,” Hartman explains.

“This challenges the question of where your traditional application security ends and your vulnerability management begins.”

To address these issues, Hartman uses several strategies that attack the visibility problem around cloud-based activities and address human behaviors that are the source of many security issues.

- It’s not enough just to rely on security certifications of cloud services providers, because that doesn’t protect you against the things people do and short-term transitional instances. You have to rethink operational and configuration management. “Anybody with a corporate credit card can set up an instance, and the next thing you know, you’re finding sensitive information in S3 containers on Amazon without proper controls around them,” says Hartman. You can never know everything that might be out there, he adds, so you need to develop new rules and practices. For instance, Hartman looks at cloud service procurement card purchases for anything unusual. “We track it back to the instance through the billing cycle, and in that way we can apply administrative controls and technical controls. We can also remind people how they are supposed to set things up,” he says. >>>

“
*It becomes a practice
that combines
connecting the tools,
continuous scanning,
and automation.*
”

SECURE YOUR ASSETS, WHEREVER THEY RESIDE

- Hartman also relies more on automated controls. For example, they may put an agent within an operating system on a platform, or leverage API calls to cloud environments to understand what's new and if it belongs. If something looks out of place, it automatically triggers a scan. Or the system alerts a scan engine that it just gave an IP address to a device. The scan engine either recognizes the device or it does not, and if it does not recognize the device, that triggers a scan. "It becomes a practice that combines connecting the tools, continuous scanning, and automation," Hartman says.

Hartman sees vulnerabilities being driven by discrepancies, regardless of where in the infrastructure that occurs. "There's the way you architect it, design it, and document it; and then there's the way you build it. The gap between these is your vulnerability. My goal is to drive consistency so we reduce that gap between the designed and actual state," he says.

KEY LESSONS

- 1 It's not enough just to rely on security certifications of cloud services providers, because that doesn't protect you against the things people do.
- 2 Vulnerabilities are driven by discrepancies. The gap between the designed intent and the actual state is your vulnerability.



**DAVE
SHACKLEFORD**
CEO,
Voodoo Security, LLC



Twitter



Website



Blog



LinkedIn



Risk management has been forced to adapt much more rapidly than it ever has before, as more technologies are adopted more quickly, and development and deployment cycles accelerate. Many security professionals are somewhat behind the curve on new technologies, and need to learn new skills and technologies that complement these rapid cycles of development and operations.



SECURING A COMPLEX ECOSYSTEM REQUIRES A LAYERED STRATEGY



**HARSHAL
MEHTA**

**Senior Director -
Information Security,
Carlson Wagonlit Travel**

Harshal is a seasoned information security professional with more than a decade of experience spread across risk management, security governance, compliance management, payment security and incident management. He has held various consulting and leadership roles across the globe delivering high-value security consulting projects. He is currently senior director of information security at Carlson Wagonlit Travel, managing regional security initiatives interfacing with business and stakeholders for aligning security with the business and delivering a sustainable and secure environment.



Blog |



LinkedIn

In managing enterprise travel programs, companies like Carlson Wagonlit Travel (CWT) handle a lot of personal information, including financial and passport information. “There are many interfaces,” says Harshal Mehta, senior director of security. “Travel management companies extract data from multiple sources such as GDS, suppliers, partners, etc., and consolidate them to have a seamless experience for the end user.” Because much of this relates to global travel, both employees and client users rely heavily on mobile apps. “Such a complex environment needs agile delivery and secure performance of the applications, which relies heavily on the cloud and mobile environment,” says Mehta.

In the travel world, mobile apps play a central role in handling itineraries and bookings, tracking travel and providing detailed information such as airport gate numbers, and delivering alerts from various external agencies. Securing the mobile applications involves a layered approach. “Principal approach is with basic authentication at the mobile device, and having single sign-on integrated with centralized infrastructure,” says Mehta. “Tracking activities on the device, and from a containment perspective, knowing how traffic is originating from mobile devices and interfaces with the internal network is a key priority.” This requires an intermediary between the mobile traffic and the internal network. “This layer monitors and manages security controls, and it makes sure that proper handshakes happen between the network and mobile devices,” he explains.



“Whether it’s a cloud-hosted environment or a co-located environment, the fundamental principle of any secure environment is to have control over what is happening.”

SECURING A COMPLEX ECOSYSTEM REQUIRES A LAYERED STRATEGY

In addition to these controls, we rely on monitoring to detect unusual activity. “It’s basically monitoring against a baseline and then looking for deviations,” Mehta says. “If you see something that is not baseline, you need to have trigger points that create alerts that go out to appropriate security and application teams for proper response.”

Mehta suggests using the same layered approach to securing online tools as well. He says, “Whether it’s a cloud-hosted environment or a co-located environment, the fundamental principle of any secure environment is to have control over what is happening. So even if you use a cloud environment where they host the application or infrastructure for you, there are multiple layers. You need to break down the layers and look at the various bits and pieces.”

This begins at the basic level of how to provision an image. “You should have a secure image for creating an instance which is used for provisioning multiple instances of those images or servers,” Mehta continues. Then you must have a secure process for creating apps that run inside the image or environment. “This would include ensuring you do validation testing as part of the coding process, and if it’s a web application, you perform an application security test (static or dynamic).”



“
It comes back to your monitoring system, and having a baseline of day-to-day operational activities. Then you continuously monitor for variations that will trigger alerts.
”

SECURING A COMPLEX ECOSYSTEM REQUIRES A LAYERED STRATEGY

At the operations level, you must have policy controls in place for managing administrative access, user access, and controls that clearly segregate the test and development environment from the production environment. And then overlaying all this structure there are tools for monitoring and detection. “It comes back to your monitoring system, and having a baseline of day-to-day operational activities,” Mehta says. “Then you continuously monitor for variations that will trigger alerts.”

Much of this strategy is based on risk related to end users, both end users and employees engaging with mobile and online apps. “Many attacks target end users, who are the most vulnerable actors in the whole ecosystem,” says Mehta. “Organizations need to work hard to cover risk factors associated with end users rather than having a total reliance on only security tools and technologies.” ■

KEY LESSONS

- 1 While security begins at the basic level of creating trusted secure images, you also must have a secure process for developing applications that run on those images.
- 2 Because end users are often targeted, work with them to help them understand risk factors associated with mobile and online apps.

MOVING SECURITY TO THE APPLICATION LAYER

In this section...



Darwin Sanoy
Major SaaS company.....59



Rory Alsop
Royal Bank of Scotland.....69



Lee Eason
Ipreo.....62



Dilip Panjwani
FIS Global.....72



Avinash Tiwari
A US-based financial
services company.....65

RISK MANAGEMENT DECISIONS MUST BE MADE AT THE APP DEVELOPMENT LEVEL



**DARWIN
SANOY**

Senior Cloud Architect,
Major SaaS company

Darwin Sanoy is a senior cloud architect who builds shared tooling for automating platform provisioning and continuous delivery. Darwin has been loving coding up automation for over 20 years. He is a PluralSight course author, open source Chocolatey packager, CIS AWS Benchmark contributor, and was awarded the "PowerShell Open Source Projects Top Contributor for 2017." When Darwin isn't on the trail trying to break his mountain bike, he is in his garage tuning or repairing it.



Twitter



Website



LinkedIn

One of the great challenges of securing assets beyond the perimeter is building apps designed to run securely in that environment. Darwin Sanoy, a senior cloud and automation architect at a major SaaS company, attributes this challenge in part to the difficulty of overcoming traditional app development practices. "Traditional on-premises development that happened within a 'secure perimeter' philosophy didn't worry a lot about security," he says. "Whenever you're dealing with something legacy, such as adapting existing code to the cloud, there are legacy habits in which security is not a first-class citizen as far as application design."

Sanoy notes that when it comes to security, new "born-in-the-cloud" app development has big security advantages as it embraces the cloud and DevOps practices that include continuous integration, testing, and automation through the entire process. "A true DevOps process gives you the possibility of accounting for security in a much more holistic way," he says. 

“ A true DevOps process gives you the possibility of accounting for security in a much more holistic way. ”

RISK MANAGEMENT DECISIONS MUST BE MADE AT THE APP DEVELOPMENT LEVEL

This may mean developers have to work differently, but it also involves developers having a clearer understanding of how to put together, and leverage, cloud-service components to deliver a level of security required by a business or an application. Containers—small, stripped-down aspects of the operating system that are useful for isolating a process or creating a microservice—provide a good example. But they are limited: For example, web services included in typical containers have limited security. Productionized containers require other platform components as fronting technologies, such as an API gateway, a load balancer, or a firewall. “With assemblable cloud technologies that are cloud native, this all becomes possible,” says Sanoy.

But developers also have to consider tradeoffs. For instance, building in greater resiliency and fault tolerance may impact performance and increase costs related to the components used to strengthen an app. Now developers are making decisions about risk-cost benefits that may have risk-management implications for the entire business. How does the app-development process prepare itself to make these kinds of decisions at the application level? 

“
Now I assume a breach from the very outset, and I am protecting against someone who's gotten in. This is not the old perimeter security method and it's one of the hardest perspectives to shift to.

RISK MANAGEMENT DECISIONS MUST BE MADE AT THE APP DEVELOPMENT LEVEL

Sanoy believes the answer to this question lies in several places:

- Developers need to make sure they understand how to translate security requirements into practical value and day-to-day security functions. “You have to take the development team through a security standard and really dig into what the policies and controls mean for the systems,” Sanoy says. “Even simple things like password policies become complex when there are 50 different types of authentication in your organization.”
- Developers also need to see a clear connection between business and technical objectives. “You have to rely on very clear security directives from strategy, policy, architecture, and ‘security built-in’ development time estimates. And then you have to have developers who are engaged in delivering those things for the benefit of the company,” he says.
- Sanoy believes that a DevOps methodology is essential, and it needs to have automation and testing throughout the process. This can include static code analysis as part of the DevOps automation scheme. “You can use static code analysis to test for security as well as performance and best practice,” says Sanoy.

Sanoy offers one other piece of advice that addresses the change in mindset of cloud-based app development. In a traditional infrastructure with a supposed “secure perimeter,” developers assumed they worked in a safe place, inside the perimeter. “Now I assume a breach from the very outset, and I am protecting against someone who’s already gotten in. This is not the old perimeter security method and it’s one of the hardest perspectives to shift to,” he concludes. ■

KEY LESSONS

1 Developers must have a clear understanding of how to put together, and leverage, cloud service components to deliver a level of security required by a business or an application.

2 DevOps methodology is essential, and it needs to have automation and testing throughout the process.



**LEE
EASON**

Director of DevOps,
Ipreo

Lee 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. Rather, giving teams control and accountability around those areas, and ensuring that they are set up simply and reliably, affords a much greater chance of success. Lee 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

Lee Eason, director of DevOps at Ipreo—which develops software used in all aspects of financial markets—says that in recent years, the industry has been moving more assets into the cloud. “Before, we relied exclusively on co-located data centers,” says Eason. “Over the past two years the trend has been to start building new services on public cloud.” This has forced Eason and others in the Financial Technology space to address directly the security of cloud-based assets.

Prior to the shift toward public cloud, security of co-located data centers was largely controlled by the network layer. “Many organizations primarily relied on infrastructure engineering for information security; things like switch configurations, firewall configurations, access control, and processes for auditing and changing those things,” Eason remarks. “There wasn’t so much focus on application layer security.”

But as the industry has moved more assets into the cloud, two things have happened. First, physical access controls are now entrusted to a third party. The other major change relates to who has access and can make changes to those pieces of infrastructure. “There’s still a switch somewhere,” Eason says. “There’s still a firewall somewhere. We still have security groups, but the question of who can access and operate security controls has changed. The definition of those things is now in code. Now it’s the development team accessing those security functions.” 

“ The question of who could access and operate security controls changed.... Now it’s the development team accessing those security functions. ”

In this new environment, there is often no central team controlling changes to security settings. In effect, the number of people who can make those kinds of changes has increased. That makes security conversations with customers more complicated, because the customers still need to answer regulators' questions about who controls the controls. "We will spend more time educating customers, but increasingly, controlling security at the application layer is becoming the norm," he says.

Eason believes this shift to application layer security actually improves the overall security of IT assets. Before you would rely on the fact that there was a network engineer who knew what they were doing and would not make a change that would be detrimental to the business. "Now we can be more transparent," says Eason. "We have the ability to put much more automation into our change-control process than we had before. And we have a complete record of every change at the code level, which can easily be audited."

This enables all kinds of automated review processes to be added to the code, build, and deploy process. "It's not a question of whether I can find when a certain change is introduced. It becomes very easy to do that. If I want to know when a security group setting or networking configuration was changed, for example, that's in the code history of the application, right along with the business logic. It's in the same repository." 

*“
Good visibility is
essential to effective
security.”*

Eason also believes the DevOps process itself, with its incremental code releases, improves security. “If you are releasing big pieces of functionality with thousands of lines of code changes, it’s difficult to review all that,” he explains. “Even an automation system might flag hundreds of things you need to check. What we want to do is push out changes once a week or once every couple of days, non-breaking database changes, and small incremental changes that are easier to review and control.”

Eason says, “Good visibility is essential to effective security.” He believes that from a tooling and DevOps automation perspective, having more security controls at the app layer makes for stronger IT security. ■

KEY LESSONS

- 1 **There is no central team controlling changes to security settings. In effect, the number of people who can make those kinds of changes has increased.**
- 2 **The shift to application layer security actually improves the overall security of IT assets.**

A FRAGMENTED ECOSYSTEM CHALLENGES A COHERENT SECURITY STRATEGY



**AVINASH
TIWARI**

**Senior Manager, Information
Security,**
A United States-based
financial services company

Avinash is an information security and privacy professional with a pioneering career reflecting strong experience in various parts of the globe (India, the US, the UK, and France) in BFSI industries. He boasts strong leadership qualifications coupled with sound knowledge of information security and hands-on expertise in various information security domains, including risk governance, IT controls, application security, and user access management governance.



LinkedIn

Avinash Tiwari, who oversees information security and risk management at a US-based financial services company, sees the modern IT ecosystem as a complex security challenge that requires different but coordinated approaches to achieving a desired security posture. A coherent strategy affects how companies secure applications they develop and how they secure the environments in which those applications run.

When it comes to application development, many companies are building a DevOps methodology into their process. DevOps provides an opportunity to integrate security and app development more tightly; when that happens, the role of the security team changes. In a traditional approach to app development, several levels of code testing would take place, including various functional tests, before the app went to the security team for security testing. Tiwari says, “The process had many steps and used to take a long time.”

In the DevOps approach, security testing becomes integral to the process. “Instead of sending the source code to the security team, we implemented online vulnerability scanners. So, we integrated the scanners into the development environment,” says Tiwari. Doing so has changed the way the security development teams relate to one another. “Now, my job is more of a tutor to teach developers about security awareness and the framework,” he says. “Our job is to translate the security framework requirements into a language that developers understand.” 

“ My job is more of a tutor to teach developers about security awareness and the framework. Our job is to translate the security framework requirements into a language that developers understand. ”

A FRAGMENTED ECOSYSTEM CHALLENGES A COHERENT SECURITY STRATEGY

By building security into the DevOps process, it's easier to ensure that the apps have necessary and appropriate security controls for the environments in which they run—an important point because the modern computing ecosystem is a fragmented, hybrid landscape in which every environment has its own security challenges. For instance, smartphones, tablets, and other mobile devices are essential tools in today's workplace. At any time, they can access company data. Tiwari says, "We have controls in place through a mobile device management (MDM) solution and containers in which apps run and data reside. Any apps that download data will operate fully within that container: Nothing goes outside it." This containerized MDM solution becomes a tool for provisioning users' devices with apps and services appropriate to their role. In short, the provisioning itself becomes an automated security function.

Cloud environments provide a similar but unique challenge. For instance, certain processes in the shared cloud environment must often be isolated, with controls for data access. However, an additional layer of security consideration exists for the cloud service providers. "If the cloud is a vendor-managed environment, you have to consider many things when signing a contract," Tiwari says. "You need to keep in mind where your data resides, which regulations apply, and who will have access to the cloud-hosted apps. You must specify the kind of testing and scanning the provider will do, the kind of reports they will deliver, and how they'll respond if you see something they need to address. You must keep all those things in mind when designing your contract with the vendor." 

"In a vendor-managed environment, you must specify the kind of testing and scanning the provider will do, the kind of reports they will deliver, and how they'll respond if you see something they need to address."

A FRAGMENTED ECOSYSTEM CHALLENGES A COHERENT SECURITY STRATEGY

Tiwari points out two key elements that tie all these security pieces together:

- Many decisions related to app controls and service provider contracts map back to requirements laid out in a security framework.
- Many of these decisions regarding app controls, tools, containers for mobile devices, and cloud services have associated costs.

Thus, the security and risk management team has an essential role to play in balancing security requirements and risk-cost benefits across all aspects of the extended IT ecosystem. ■

KEY LESSONS

- 1 **By building security into the DevOps process, it's easier to ensure that apps have the security controls required for the environments in which they run.**
- 2 **The security and risk management team has an essential role to play in balancing security requirements and risk-cost benefits across all aspects of the extended IT ecosystem.**



**BEN
CHUNG**

Chief Information
Security Officer,
NTT Communications ICT
Solutions



Twitter



Website



LinkedIn



“Technology and its uses are always evolving and as a consequence so are the security attack surfaces. Traditional security and risk management programs must evolve to understand what controls can be applied. Reviewing first principles such as understanding the data and how it is being handled, who has access to the data and what can they do to it, and how we track and trace what is happening in the environment will focus your ability to assess your use.”



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.

MODERN ASSETS REQUIRE A DISCIPLINED, STEP-BY-STEP APPROACH TO SECURITY



DILIP PANJWANI

Director, Information Security and CISO, India, FIS Global

Dilip Panjwani—director, information security and CISO for FIS Global (India markets)—is responsible for information security compliance and governance for FIS India. Prior to working for FIS Global, Panjwani was associate vice president and head of information security services and ATM management at DBS Bank, India. He was included in the list of “Top 100 CISOs” by CISO Platform and as one of the “InfoSec Maestros” by InfoSecurity group. He is also a member of various thought leadership forums involving select CISOs and CIOs.



Twitter



Website



LinkedIn

Because FIS Global, where Dilip Panjwani serves as director of information security, provides various solutions and services to the financial industry, there is a large amount of customer information at risk, much of which needs to be accessed from mobile devices or the cloud. As a result, the company has implemented an extremely high level of security, especially around modern assets such as containerized applications. The process, says Panjwani, requires discipline and structure, particularly when it comes to interconnected devices.

There are three main areas Panjwani focuses on. “First, we need to ensure that our application programming interfaces (APIs) are programmed to allow only specific services to be exposed to third parties,” he says. “Secondly, they should only be able to provide limited information as required for the service integration, and not an open API, which can be exploited further. The APIs should be authenticated and then accessed, as this allows much more controlled access to the systems, as well as the data that has been input internally. The third aspect would be any external third parties that we work with. There needs to be a strong vendor risk-management and governance program, right from the time of pre-assessment to onboarding and continual assessments.” 

“ We need to ensure that our APIs are programmed in a manner that allows only specific services to be exposed to third parties. ”

MODERN ASSETS REQUIRE A DISCIPLINED, STEP-BY-STEP APPROACH TO SECURITY

And when it comes to third parties, Panjwani says there are two levels of auditing. “One is where we insist that they comply to certain policy and procedure compliance requirements as an organization in general,” he says. “And secondly, we check the entire data flow architecture as well as the connectivity architecture for services engaged. Whatever interconnected and stage-two systems, which provide support to applications, are used, they must be connected to our systems in a manner that keeps vulnerabilities to a minimum.”

Even with such requirements in place, there are certain assets that trigger deeper investigation and a multi-check approach that takes place right from the initiation or conceptualization stages. “First,” says Panjwani, “new applications or new product requirements are assessed by the security team to analyze the product and data flow, and to understand what interfaces will be connecting to the application. These are both internal and external considerations. Secondly, we ask what kind of protocols and what kind of systems these applications work on. And third, we determine the kind of connections and ports that will be required to connect to these APIs and how the data would be secured right from the storage to transmission and eventually processing at both our systems as well as the third-party-provider systems.”



“

One of the common issues that we see among many of the service providers or the partners we connect with, or any service organization, is the need for vulnerability management and remediation within a defined period of time.

”

MODERN ASSETS REQUIRE A DISCIPLINED, STEP-BY-STEP APPROACH TO SECURITY

After all these steps are analyzed and security is considered, there is still a need for regular, or continuous, vulnerability management, which Panjwani sees as a weakness in many organizations. “One of the common issues that we see among many of the service providers or the partners that we connect with, or in any service organization, is the need for vulnerability management and remediation within a defined period of time. And putting enough compensating controls and monitoring controls in place to be able to proactively detect any threat that could be coming towards them.”

And as far as the future is concerned, Panjwani sees two asset areas that concern him, both revolving around lack of technology standards for interoperability and security. “One would be around mobile payments where customers buy using smart devices and smart systems for their homes and offices. But there is no defined technology standard for these Internet of Things devices.”

In addition, there are issues around the use of mobile wallets. “Today your mobile payment solutions are wallets that typically link with your mobile phone or your sim number,” he says. “So that’s something that also needs to be looked into—how we can strengthen the process to have your mobile number secured along with your bank account.” ■

KEY LESSONS

- 1 **Modern assets require extra diligence, especially around interconnected devices.**
- 2 **Even with careful control over data access, there is still a need for regular, or continuous, vulnerability management, which is a weakness in many organizations.**

FOCUSING ON DATA SECURITY

In this section...



Antonio D'Argenio
Tech Data Corporation.....76



John Meakin
Burberry.....83



Eric Bedell
Mitsubishi UFJ Financial
Group.....80



Paul Heffernan
Unipart Group.....86



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.**



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.



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.

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.**

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.

AUTOMATING SECURITY TESTING AND CONTROLS

In this section...



Michael Capicotto
Two Sigma.....90



Jamie Norton
NEC Australia.....97



Russ Kirby
CreditSafe.....94



Joshua Danielson
Copart.....101

PROTECT MODERN ASSETS WITH STANDARDS AND AUTOMATION



**MICHAEL
CAPICOTTO**
Security Architect,
Two Sigma

Michael Capicotto studied computer engineering at the University of Toronto, and then moved to New York and began a career in cloud computing. He has spent the past several years designing and building scalable, secure cloud architectures, and giving public talks about the latest cloud security topics. Michael's passion and focus lie in the intersection of security, automation, and machine learning.



LinkedIn

Michael Capicotto has witnessed massive shifts in the security landscape over the past decade. Businesses once had physical control over all of their assets and could rely heavily on techniques like perimeter security, inspecting everything that flowed in and out of their data center. Now, Capicotto explains, “You have teams deploying web applications in the cloud and people using mobile devices to access their work email, and that drastically changes how we should approach security. You have almost no physical control over the assets you’re using, and you have a lot less physical control over the data and where it flows.”

In light of these changes, he believes that organizations must update their security strategy by defining standards and taking advantage of automation to enforce them. “Today, it’s more about setting standards and saying, ‘No matter what type of asset we use and no matter which cloud provider is hosting it, these are the security standards to which it’s going to adhere,’” Capicotto says. “The security team will be useful only if it can keep pace with the business and the rest of the IT organization. Now, anyone with a credit card can go to a cloud provider, sign up for a service, and deploy a virtual server in a matter of minutes,” he explains. Unless the security organization can keep up with that pace of innovation, it will be difficult to protect the business. 

“The security team will be useful only if it can keep pace with the business and the rest of the IT organization.”

PROTECT MODERN ASSETS WITH STANDARDS AND AUTOMATION

Security automation is beneficial because it addresses some of these critical challenges while also increasing an organization's security posture. A business can build a continuous security system that automates many of the checks the security team would typically complete by hand. "If you build an automated security system correctly, it's a lot less likely to make mistakes than humans are," says Capicotto. "That automated security check can keep happening over and over, with much less chance of error than when humans are performing that work."

Once a large part of an organization's security practice is automated, the security team is free to build value-added systems that go above and beyond the baseline level of security with which the company is comfortable. For example, they could build more robust security controls with which to defend the organization's networks and assets, using techniques such as anomaly detection and machine learning. "I think that's one of the main reasons why automating security is so important in the changing IT landscape, and in the heavy cloud usage we see in a lot of organizations today," says Capicotto. 

“
If you build an automated security system correctly, it's a lot less likely than humans to make mistakes.
”

PROTECT MODERN ASSETS WITH STANDARDS AND AUTOMATION

Businesses face complex and growing security challenges as they move to better protect a range of modern assets. They can create a more responsive and resilient approach to security by setting clear standards that can be applied to modern assets, while also taking advantage of the efficiencies automation offers, clearing the way for security professionals to raise the bar on the company's security practices even farther. That way, businesses can not only respond to today's formidable challenges, but surpass them, ultimately arriving at a proactive security posture. ■

KEY LESSONS

- 1** Businesses can better protect their modern assets by setting standards that apply to a range of technologies and providers.
- 2** Security automation helps a business keep up with a changing landscape while also increasing its overall security posture.



**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.

DYNAMIC ASSETS REQUIRE CONTINUOUS MONITORING



**JAMIE
NORTON**

Head of Cybersecurity,
NEC Australia

As head of cybersecurity for NEC, Jamie helps clients identify and optimise their cyber risk and resiliency. Jamie is a strong advocate for improving “situational awareness” within modern technology environments, helping clients understand that improved visibility is critical to discovering and responding to modern threats.

Jamie was formerly CISO for the World Health Organization and has led security teams across the Asia Pacific region. Jamie holds CISA, CISM, CISSP, and CGEIT certifications and sits on a number of boards related to security.



Twitter



Website



LinkedIn

Jamie Norton, head of cybersecurity at NEC Australia, explains that many pieces of a modern IT infrastructure present similar security challenges: lack of control over, and visibility into, infrastructure components. For example:

- The cloud. “In a cloud environment, you don’t have ownership of the building blocks that make up that environment,” Norton says. “You can’t just peel back the layers and see how the operating system is built, or see how the gateways or firewalls are working. You don’t have that level of access.”
- Mobile devices. Norton says, “Mobile devices are similar in that you have very limited control over what is on the device, in terms of the operating system and what lies beneath it.”
- Internet of Things (IoT). The IoT presents a new kind of challenge in which there is an explosion of connected devices that have little or no cybersecurity protections, each offering a potential path of least resistance into a larger network. “It’s almost like security by obscurity,” Norton explains, “particularly with regard to sensing equipment in critical infrastructure like power grids. In these situations, it’s difficult because these are often high-risk networks where you can’t be proactive without risk of damaging a sensor and possibly causing a catastrophic failure.” Another problem with IoT devices is they often run on old operating systems with known vulnerabilities. But in many cases the OS is “baked” into the devices, with no possibility of installing patches.



“ *In the cloud, you may have passive monitoring or continuous monitoring of an environment where you’re looking for indications of compromise.* ”

DYNAMIC ASSETS REQUIRE CONTINUOUS MONITORING

Norton describes two broad approaches to securing these infrastructure components. One consists of a variety of containerization strategies used to isolate, monitor, and control critical processes. The other is a more aggressive approach to network monitoring and the use of analytics and even artificial intelligence to identify anomalous activity.

- **Containerization.** The use of containers has become a common method for creating isolated, controllable environments in the cloud and on some mobile devices. “You’re virtualizing an environment,” says Norton. “Now you can actually look at that environment and see what’s going on, rather than trying to look at the underlying infrastructure which you cannot access. Even if there is compromise in the underlying environment, you’ve got controls around your virtual environment.” Containerization becomes especially important in the cloud where complex applications dynamically use layers of virtualization to run critical processes or load critical data for short periods of time. “We’re seeing orchestration becoming a lot more complex and automated,” says Norton. “When a container gets stood up, it’ll automatically get scanned and compared to a known good version of that container so the process knows it’s all correct and can move on.” 

“
IoT devices are often in high-risk networks where you can't be proactive without risk of damaging a sensor and possibly causing a catastrophic failure.
”

DYNAMIC ASSETS REQUIRE CONTINUOUS MONITORING

- **Scanning and Monitoring.** Vulnerability scanning and activity monitoring become continuous processes running inside the IT ecosystem. “In the cloud, you may have passive monitoring or continuous monitoring of an environment where you’re looking for indications of compromise,” says Norton. Automatic code scanning to test for errors and vulnerabilities is now commonly integrated into an agile app development process, but it does not end there. Many apps have built-in controls and self-validation routines. “Applications are starting to build in more self-checking or self-verification, and even APIs where other modules and other software guests plug in to verify that the process is working the way it should,” he explains.

Norton believes that scanning and monitoring is destined to play an even greater role in securing the IoT. With billions of poorly secured connected things plugged into networks all over the world, analyzing the data they produce will be an essential part of detecting compromised devices. “The way to address this is through risk governance, making sure you’ve identified those systems as being potential risks, and then monitoring continuously, and having sensors in those networks, so if you see something unusual, you can jump on it.” ■

KEY LESSONS

- 1 **Automatic vulnerability scanning is commonly integrated into an agile app development process, but it does not end there. Many apps have built-in controls and self-validation routines.**
- 2 **With literally billions of thinly secured connected things plugged into networks all over the world, scanning and monitoring is destined to play a great role in securing the IoT.**



**CHRIS
WYSOPAL**
CTO,
CA Veracode



Twitter



LinkedIn



An ever-growing percentage of our daily lives takes place digitally. The convenience and efficiency of systems we collectively use, like Windows, Google apps, and other applications with big user bases is also a common point of failure that can topple countless users like dominoes. If we want to continue to grow and live in a digital world we need to shore up the two weakest points—the software and the identities of those who access it.



AUTOMATED PROCESSES BECOME YOUR CONFIGURATION ITEMS



**JOSHUA
DANIELSON**

CISO,
Copart

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



As is the case for many businesses, cloud applications and mobile devices play an important role in Copart's operations, which involve receiving totaled cars, assessing their condition, preparing them for resale, and conducting online sales in the wholesale market. For Joshua Danielson, who as chief information security officer (CISO) is responsible for securing Copart's IT infrastructure, the top security challenge is high availability and high reliability. "If the systems aren't running, we're not making money," he says.

So how does he secure this distributed infrastructure? For Danielson, it begins in two places:

- Finding the right people, and that does not necessarily mean looking for people with "security" in their title. "When building out a cloud strategy, we hire cloud architects and DevOps engineers because right now, there just isn't much security talent that understands cloud. This will change as the industry matures."
- The next essential question is to answer what business objectives you expect to accomplish by moving to the cloud. "For us it's high availability and reliability, because that's critical to the business," Danielson says. "It might be something else for another business, but you need to know what it is, because this leads you to what kind of cloud partners you look for, and what kind of services you need from them." 

“If you build your assets off an automated process, or OpenStack, or AWS CloudFormation templates, those things become your configuration items from an auditing perspective.”

AUTOMATED PROCESSES BECOME YOUR CONFIGURATION ITEMS

Danielson says that many of the security principles you apply to cloud assets are the same as for on-premises infrastructure, but you implement them differently. For instance, in an on-premises data center you might do a quarterly audit to verify that your resources do not have vulnerabilities that could result in public exposure. In an AWS implementation, you achieve the same security function with an automated process that runs continuously. For instance, you might have a process that checks that none of your S3 buckets are exposed at any time, and if one is, the process might send an alert or simply delete the object. “If you start building your assets off an automated process, like with AWS CloudFormation templates, those things become your configuration items from an auditing perspective,” Danielson says.

When it comes to auditing and reporting on how effective your controls are, you will be more dependent on the cloud service providers and third parties to validate them. “If you want your service provider to have SOC 2 certification to ensure the security controls you need are actually in place, that’s fine. But the certification is actually provided by a third-party auditor.”



“
There are new preventative controls that are really helpful, but the piece I focus on most is looking at the data that is passing to those mobile devices.
”

AUTOMATED PROCESSES BECOME YOUR CONFIGURATION ITEMS

In Danielson's view, securing mobile devices presents a similar challenge in the sense that you need to decide what they are being used for, and then configure them accordingly. "People are bringing their own devices. We really need to get past that debate," he says. "There are new preventative controls that are really helpful, but the piece I focus on most is looking at the data that is passing to those devices." Danielson believes that with mobile devices, you need to start with your own policy and the standard you want to impose. Then permit data connections based on those standards and the classes of data you are allowing through those devices. ■

KEY LESSONS

- 1** First identify business objectives you want to meet by moving to the cloud. This will lead you to the kind of cloud partners you should look for, and the services you need from them.
- 2** In an on-premises data center you might do a quarterly vulnerability audit. In a cloud implementation, vulnerability testing becomes an automated process that runs continuously.



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

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

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