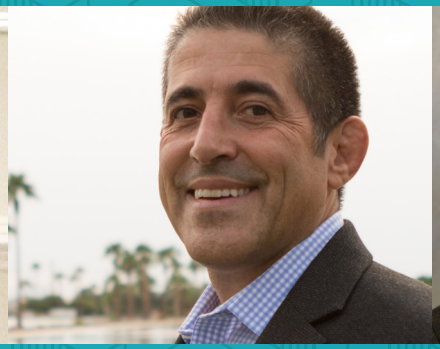
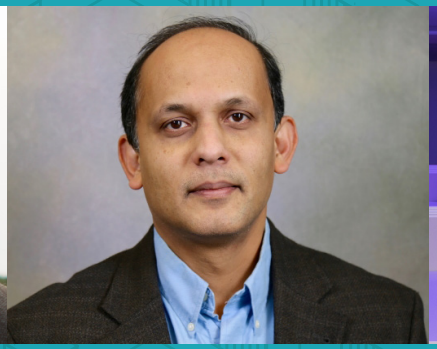
tenable

Mighty Guides®

REDUCING
CYBER EXPOSURE
FROM CLOUD TO CONTAINERS

5 Key Learnings from the CISO POV




INTRODUCTION

When it comes to IT infrastructure, it's fair to say the perimeter has left the premises. In fact, the perimeter has mostly disappeared. Consider:

- **The average organization uses 1,427 cloud services, but only 8.1% of them meet enterprise security and compliance requirements.[1]**
- **89% of companies now allow personal devices to connect to corporate networks.[2]**
- **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.**

We're living in a new reality, one crowded with new types of dynamic IT assets. 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 CISOs and security leaders looking to accurately understand and reduce their cyber risk.

To combat this challenge, a discipline called Cyber Exposure is emerging to help organizations manage and measure this risk. This ebook shares perspectives on how your peers are beginning their Cyber Exposure journey to protect their expanding attack surface – from cloud to containers and everything in between – and gain business insights. Read on for their key takeaways…

All the best,
David Rogelberg
Editor

Mighty Guides®

Mighty Guides make you stronger.

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

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

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

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 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.

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.

TAKEAWAY #1

The network perimeter is growing, thanks to technologies such as SaaS and IoT devices. How can you protect it?

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." ■

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 VP and 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."

Operating in this more fluid IT environment has required changing the way assets are protected.

TAKEAWAY #2

Having visibility into the digital assets you're trying to protect – whether in the data center or in the cloud – is critical to Cyber Exposure.

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.
- 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. ■

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

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

As executive director of the office of the 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."

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.

TAKEAWAY #3

Maintaining high-level security across all assets isn't only a resource drain – it's unrealistic. With Cyber Exposure, you can segment risk based on asset criticality and vulnerability.

"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 IoT 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." ■

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.

TAKEAWAY #4

Risks change, but whether it's in the cloud or on premises, you still have to encrypt data. So, only give access to those who need it.

"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.

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." ■

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."
- **IoT:** 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

TAKEAWAY #5

Automatic vulnerability scanning is commonly integrated into an agile app development process. But it doesn't end there. Many apps have built-in controls and self-validation routines.

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.

Norton describes two broad approaches to securing these infrastructure components:

- **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."
- **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. ■

Want to learn more about reducing Cyber Exposure?

Get more lessons learned by industry leaders in Mighty Guides'
"Reducing Cyber Exposure from Cloud to Containers" ebook

Take me to the ebook