KOVRR
Cyber Decisions. Financially Quantified.

www.kovrr.com

What Keeps a CISO Up at Night? Managing an Expanding, Evolving Attack Surface

APRIL 2022

The job of a chief information security officer (CISO) seems to only get more challenging. While controls to mitigate cybersecurity threats are emerging, cyber criminals continue to come up with new attack methods, and the setup that businesses rely upon is becoming more and more complicated. Even when CISOs think they have adequate defenses in place, the ways in which companies operate continually evolve, meaning CISOs need to develop strategies to protect new endpoints and new ways of working overall.

In this series on **"what keeps a CISO up at night,"** we'll be examining some of the most pressing issues that these security leaders need to deal with, starting with managing an expanding and evolving attack surface.

Specifically, the attack surface has changed due to factors like the following:

Work from anywhere

The COVID-19 pandemic seems to have accelerated a lasting shift in the way employees work. Your company might still be figuring out the best way forward, but in general, there's more of a "work from anywhere" mentality. Even if your company can't operate remotely, your third-party service providers and partners might be doing so, which can change the threat landscape.

For one, remote or hybrid work might cause you to re-evaluate bring-your-own-device (BYOD) policies. Before the pandemic, employees might have been using personal devices like smartphones for work email, so you may have already implemented protections like multi-factor authentication. Now, however, you may have to take another look at how employees are using — and should use — personal devices, especially if they're getting more access to company networks, systems and data so they can work remotely.

As it stands, however, many companies are struggling in this regard. For example, a global survey of cybersecurity professionals and business leaders by cybersecurity company Fortinet finds 59% "still don't have the ability to authenticate users and devices on an ongoing basis and are struggling to monitor users post-authentication."

Cloud computing

In a work-from-anywhere world, cloud computing has arguably become even more important. All types of enterprises are migrating on-premise services to the cloud for functions ranging from accounting to sales to HR. That means CISOs need to focus more on securing cloud environments, as opposed to just making sure that devices get protected on premise.

“In the context of remote working and online customer interactions, it’s little surprise that CISOs [in 2021] most often said that they are focused on network/cloud security and identity management,” notes a global survey from Heidrick & Struggles, an executive search firm. Heidrick adds that this priority marks “a shift from a focus on endpoint security.”

That’s not to say that endpoint security is no longer a concern for CISOs, but this demonstrates how the attack surface has expanded and changed. Now, CISOs likely need to develop a multi-pronged strategy to tackle endpoint, network and cloud security.

Having “full visibility of all users, devices and data across their network, endpoint and the cloud” is needed “to understand the context of an attack, enforce security policy across the network and endpoint, and correlate security events to improve the organization’s security posture,” notes cybersecurity company Palo Alto Networks.

IoT

In addition to getting a handle on more personal devices like employees’ laptops and smartphones, CISOs also need to help their enterprises navigate the growth of Internet of Things (IoT) devices.

From smart HVAC systems to sensors for manufacturing equipment, so many different types of IoT connected devices are in use across industries. IoT Analytics, an IoT market insights organization, projects the number of connected IoT devices globally to grow from 12.3 billion in 2021 to over 27 billion by 2025.

With so many internet-connected devices, that can easily keep CISOs up at night worrying about how to stay secure.

For one, cyber criminals might engage in spoofing, which “occurs when an attacker breaches a lower-level device with little or no security and gains access to a network with protected devices, which is then tricked into believing the intruder is encrypted,” explains Tulane University’s School of Professional Advancement Information Technology program. Cyber criminals can also launch denial-of-service attacks, such as smurfing, which “uses IP spoofing to overwhelm a server and prevent it from responding to legitimate requests,” adds Tulane.

Managing the Expanding and Changing Attack Surface

While this expanding and exchanging attack surface can be difficult to manage, it’s not as if CISOs have to just sit back and let their cybersecurity falter. CISOs might not be able to eliminate all risks, but they can use technologies and implement new strategies that help them reduce threat levels and focus on the most important areas.

For example, using a combination of technology and data analysis can potentially help manage IoT risks, as CompTIA, a non-profit IT trade association, explains:

“The use of an intrusion detection systems (IDS), as well as a security information and event management (SIEM) system can help – so can the practice of information sharing. Using cybersecurity threat intelligence (CTI), it is possible to profile attackers and more intelligently position security controls for IoT and ICS (industrial control system) devices.”

As it stands, however, many companies are lacking on the data front. A 2022 global PwC survey of business, technology and security executives finds that fewer than one-third of respondents have “integrated analytics and business intelligence tools into their operating model.”

As a result, these respondents have the least ability among those surveyed "to turn data into insights for cyber risk quantification, threat modeling, scenario building and predictive analysis — all critical technologies for smart cybersecurity decisions," notes PwC.

The good news is that enterprises can turn to relatively straightforward tools to start becoming more data-driven. For example, Kovrr's Quantum cyber risk quantification platform integrates technographic, global threat intelligence, and cyber insurance claims data to then help CISOs and other security leaders with financial quantification and risk management.

By gaining a better understanding of the threat landscape and how your organization's security posture translates into financial risk, you can then make more informed decisions about additional cyber security investments, such as technologies for improving authentication in this work-from-anywhere era.

Cyber risk quantification can also help in areas like prioritizing internal security strategies. If CISOs need to decide where to focus resources and training amidst the expanding and changing attack surface, then knowing the most expensive risks can help clarify those choices. Plus, financial quantification can help CISOs get buy-in from other executives who might be more focused on monetary issues and business risk than on technical ones.

> Want to see how Kovrr can help your company financially quantify cyber risk? **Book a demo** with our experts.

KOVRR
Cyber Decisions. Financially Quantified.

The Author

Shalom Bublil

CPO

About Kovrr

Kovrr's cyber risk modeling platform delivers global (re)insurers and enterprises transparent data-driven insights into their cyber risk exposures. The Kovrr platform is designed to help chief risk officers, chief information security officers, underwriters, exposure managers, risk professionals and catastrophe modelers understand, financially quantify and manage cyber risk by utilizing AI-powered risk models.
To learn more please contact the Kovrr team: contact@kovrr.com