KOVRR
Cyber Decisions. Financially Quantified.

www.kovrr.com

What Keeps a CISO Up at Night? Managing Cyber Supply Chain Risk

JUNE 2022

From managing an expanding, evolving attack surface to trying to secure enough budget, chief information security officers (CISOs) have plenty to deal with internally. The problem is that cyber threats aren't contained within the four walls of an organization. Your supply chain also carries risks, including the IT vendors that support your cybersecurity strategies and tactics. Weaknesses in their own cybersecurity could end up affecting your organization.

"Like other types of goods, a global supply chain exists for the development, manufacture, and distribution of information technology (IT) products (i.e., hardware and software) and information communications technology (ICT). As with other goods and services, risks exist to this cyber supply chain," notes the U.S. Congressional Research Service.

Indeed, your suppliers could be creating more cyber risk than anyone within your organization.

"Third party risk is probably the greatest threat any company faces today when dealing with cyber security threats. Instances of sub-tier suppliers or ancillary vendors with poor cyber hygiene who inadvertently allow for the breach of a much larger company are well documented," notes the Cybersecurity and Infrastructure Security Agency, part of the U.S. Department of Homeland Security.

That said, CISOs aren't relegated to sweating out this problem. There are steps you can take to better manage cyber supply chain risk. In this third installment of our series on "What keeps a CISO up at night," we're looking at the top issues that CISOs and other IT leaders face. Here, we'll examine the challenges and strategies around managing cyber supply chain risk.

Identify Your Supply Chain

To get a handle on cyber supply chain risk, you need to know what your supply chain looks like. Even if that sounds obvious, the reality is that organizations might not have this information readily available at the C-Suite level.

Start by making a list of all the third parties such as suppliers and distributors to your organization, advises the Australian government's Australian Cyber Security Centre (ACSC). "While an exhaustive list of such businesses, especially their subcontractors, may not be possible, the identification of those responsible for products or services with security enforcing functions, privileged access or handling particularly sensitive information should be prioritized," adds ACSC. The Kovrr approach starts with performing an automated mapping for the organization infrastructure, and the location of the different assets, whether their on-perm or managed by other third party service providers. This allows a more streamlined, easier mapping process that can serve as a baseline to the discussion.

© 2022 Kovrr All Rights Reserved

The Kovrr output can help your organization kickstart the journey by mapping the different IT providers, such as PaaS, Email and Email Security Services, CDN services, CRM Services.

Analyze Risks

Once you have a better understanding of who your suppliers are, you can start to address cyber supply chain risk. Doing so means analyzing risk in its many forms.

Ransomware may seem to be everywhere nowadays, but that's not the only threat you need to look out for. IT hardware suppliers, for example, could be putting your organization at risk if manufacturing deficiencies cause outages that then increase your internal cyber risk. If a corporate network experiences downtime, for example, employees might use their personal devices and networks for professional purposes, thereby creating shadow IT risks.

"Cybersecurity is never just a technology problem, it's a people, processes and knowledge problem," says the U.S. National Institute of Standards and Technology (NIST).

From there, CISOs also need to prioritize risk management. You can't always solve every risk at once, and the real value of some cybersecurity measures might pale in comparison to others.

Perhaps instead of switching vendors — where the net result for your cyber supply chain risk might remain about the same given the pervasiveness of cyber threats — educating employees about supplier risks might have more impact. Or, maybe you need to work with your IT team to adjust permissions to manage the risk that comes with employees using certain software vendors.

Cyber risk quantification tools can help you calculate the financial impact of cyber supply chain risks so that you can then prioritize your mitigation steps.

© 2022 Kovrr All Rights Reserved

Improve Cyber Governance

Getting a better handle on cyber supply chain risk and being able to effectively prioritize risk management strategies can also require improved cyber governance. CISOs shouldn't be the only ones overseeing cyber risk. Instead, organizations should take more of a shared accountability approach.

Leaders need to set the tone from the top regarding the importance of cybersecurity, and boards and other executives should align with CISOs on reducing cyber supply chain risk.

"Effective governance will also ensure that cyber security activities help to support the organization's strategic goals," says PwC.

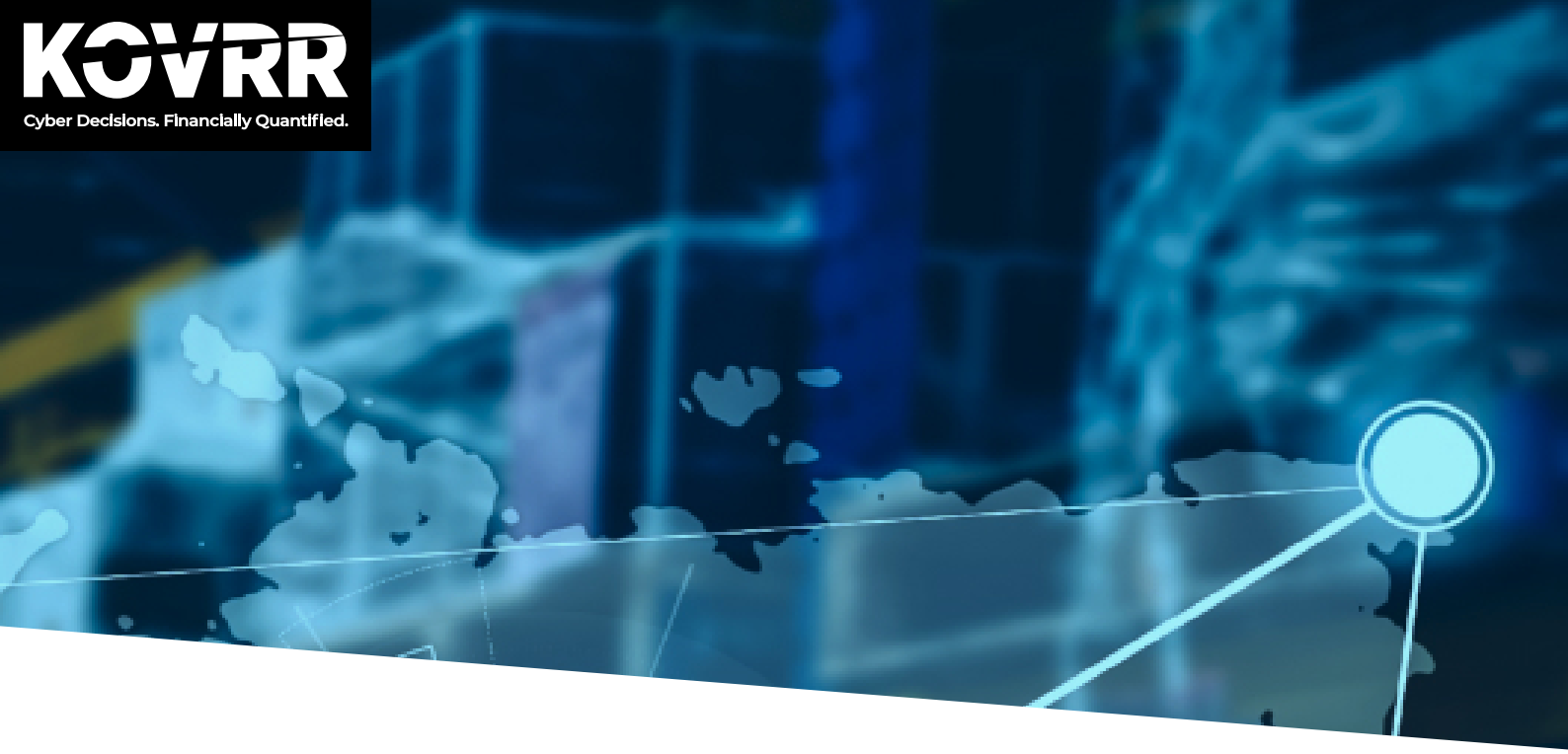
For example, suppose your company is deciding between two customer relationship management (CRM) platforms. They both have similar features, yet one has a slightly lower price. However, when considering the cyber risk that both vendors have, you might then take a closer look at their data security policies.

From there, you might determine that the higher-priced vendor has lower cyber risk, which could help you avoid future costs stemming from a cyber attack. So, you can achieve your goal of choosing a CRM vendor that limits your long-term risk from both a financial and cybersecurity standpoint.

Overall, organizations need to realize that cyber risk comes in many forms. By looking into your cyber risk both internally and externally, you can reduce the likelihood and potential fallout from an attack. Getting there requires executives and boards to find alignment and prioritize cybersecurity, including cyber supply chain risk management.

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

© 2022 Kovrr All Rights Reserved



The Author

Shalom Bublil

Chief Product Officer

About Kovrr

Kovrr's cyber risk modeling platform delivers global enterprises and (re)insurers 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

© 2022 Kovrr All Rights Reserved