STRATEGIES FOR CISOs: KEEPING UP WITH THE PACE OF CHANGE

Sponsored by Cyber Talk

Cyber security leaders are racing to keep up with the fast and furious pace of technological change. As new tools, applications and architectures emerge and are integrated into the tech stack, CISOs are struggling to secure them efficiently and effectively.

Cloud computing, IoT, AI and block chain, for example, all require specialized cyber security risk mitigation skills. Across the past few years, as the aforementioned tools were integrated into ecosystems, teams needed to quickly build the right skills or to urgently hire.

On account of the pace of change, 94% of CISOs feel stressed out in their roles, 74% feel that they are facing unreasonable job expectations, and 76% believe that their organization is unprepared to cope with a targeted cyber attack.[1,2]

In a landscape that moves at lightspeed, how can CISOs not only keep up with, but also excel, in spite of continuous security evolution?

Actively Participating in Digital Transformations

By actively participating in digital transformations, CISOs can ensure that new technologies are secured when they're first introduced to the organization — not days, weeks, months or even years later.

To effectively participate in transformation initiatives, CISOs need to forge relationships across the organization. As CISOs familiarize themselves with technology stakeholders, they should join discussions surrounding large-scale infrastructure changes.

Organizations derive limited value from infrastructure changes if the changes blindly heighten risk exposure. Thus, the CISO's active involvement in digital transformations simplifies security management and accelerates genuine business growth.

At present, Chief Information Security Officers are now measured on how security preempts new initiatives and enables faster service or application delivery.

---

[1] CISO stress levels are out of control, SC Media, June 21, 2023
https://www.scmagazine.com/perspective/ciso-stress-levels-are-out-of-control

[2] CISOs' confidence in post-pandemic security landscape fades, Help Net Security May 12, 2023
https://www.helpnetsecurity.com/2023/05/12/cisos-elevated-cyber-threat-concerns/

Staying Innovative and Agile

Cyber criminals have embraced agility within their operations, shifting tactics to exploit global events, unpatched vulnerabilities and to evade new forms of detection. In response, CISOs must make agility an end-goal. In so doing, CISOs must invest in agile network access controls, device visibility and high-caliber management solutions.

CISOs also need a multi-cloud strategy that allows them to easily scale up or scale down cloud security services and capacity in conjunction with operational needs. To put this into play, CISOs must integrate a unified cloud security approach across their applications, workloads, and network.

In addition, CISOs should set aside time to speak with vendors about the latest technologies, must experiment efficiently, review emerging guidelines, and continuously enhance incident response playbooks to stay agile. In the long run, it'll all be worth it.

Failure to innovate and iterate can come at a high cost. While time or dollars might be saved, at the macro-level, innovation ultimately supports business resilience, continuity and growth. However, the real secret to success is enabling innovation and adaptation to occur automatically.

Automation

Security automation is critical in keeping up with the pace of change and in preventing cyber attacks. However, automation tools and approaches should work together, otherwise you will be left with blind spots and vulnerabilities in your solution.

For CISOs and teams dealing with growing workloads, implementing a Cloud Native Application Protection Platform (CNAPP) approach allows effective security automation; from code to cloud. Today's organizations are giving special attention to building security around and incorporating automation within the following key areas:

Least Privilege Access to Cloud Workloads and Resources:
Gain visibility into the effective permissions of users and assets. Reach least privilege roles enforcement to eliminate over-permissions with auto-identification of identity and entitlement threats.

ShiftLeft Security:
Integrate with developers' tools to detect code vulnerabilities and to identify secrets and misconfigurations in the code before deployment, preventing unauthorized use to nefarious ends.

Risk Management and Prioritization:
Proactively reduce risks by taking all of the security and contextual factors into account and automate prioritized remediation.

Prevention-First

A prevention-first cyber security approach enables CISOs to not just keep up with hackers, but to actively stay ahead of threats. In the absence of a prevention-first approach, CISOs are continuously overseeing investigations — where adversaries have already infiltrated systems, potentially compromising the "crown jewels" — and containment.

When it comes to prevention-first, experts emphasize the importance of leveraging comprehensive, consolidated and collaborative cyber security solutions.

In an environment where stress, threats, and workloads are increasing everyday, a prevention-first approach can keep cyber security teams calm and in control.

Cyber Resilience

To not only keep pace with change, but to cultivate a thriving security environment, CISOs must embrace a holistic approach to cyber resilience; ensuring that resilience is a core element of the cyber security strategy. To address cyber resilience, your organization may need to integrate new solutions into the enterprise lifecycle.

An effective resilience approach will include artificial intelligence and machine learning, identity access management solutions, SIEM, SOAR and other tools that can prevent and assist your organization in 'bouncing back' from advanced threats at-scale.

> "As the digital landscape continues to evolve, businesses must stay vigilant, adapt to emerging challenges and prioritize resilience above all else.[3]
>
> Deryck Mitchelson, Check Point Field CISO

[3] How Does Your Board Measure Cyber Resilience? Cyber Security Intelligence, June 6, 2023
https://www.cybersecurityintelligence.com/blog/how-does-your-board-measure-cyber-resilience-7044.html

Strategic Planning

There are additional methodologies that can help leaders keep up with the pace of change. VP of Cloud Security at Check Point, TJ Gonen suggests using the "1-3-2" method for strategic planning. This method involves predicting where you want to be in two to three years and then working backwards to figure out how to get there.

The process is simple:

- "1" represents where you are currently
- "3" represents your future goal
- "2" is the series of actions that will take you from "1" to "3"

For instance, Step 1 could look like a combination of adopting cloud security, such as: lifting and shifting, going cloud native and losing the power of saying no to the speed of development. The trick is in the ability to give an honest, unbiased and realistic opinion of where your organization sits within this spectrum. Assess what it is, where you are and what you do.

Step 3 is an aspiration of where an organization hopes to be; it's a visualization of the landing spot. The work is in Step 2. What can we do as a series of 2's so that value is created, so that you learn through your results and get to the 3? Actions can be vetted in Step 2.

It's important to note that this process is a cycle. As soon as you reach your "3" goal, you need to start working on your next goal.By using the "1-3-2" method and visualizing the end goal, it becomes easier to think strategically and plan for the future. Learn more about this method here.

In Conclusion

To keep up with the pace of change and to excel in the CISO role, Chief Information Security Officers must actively participate in digital transformations, stay innovative and agile, embrace automation, adopt a prevention-first approach and prioritize cyber resilience.

Implementation of these strategies will increase abilities to adeptly navigate the threat landscape, and will drive rapid business growth while establishing, maintaining and strengthening an organization's cyber security posture.

For more related insights, please see our whitepapers here. Put cutting-edge cyber security into action.

Worldwide Headquarters
5 Shlomo Kaplan Street, Tel Aviv 6789159, Israel | Tel: +972-3-753-4599

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 1-800-429-4391

www.checkpoint.com

© 2023 Check Point Software Technologies Ltd. All rights reserved.