PURESTORAGE®
Uncomplicate Data Storage, Forever

SUMMARY REPORT

Perfecting Cyber Resilience

The CISO Blueprint for Success

In the security world, no news is good news. But success on the job for the Chief Information Security Officer (CISO) can be a double-edged sword. When everything is going right, it can be easy to forget all that goes into keeping threats at bay. And that's precisely when vigilance within the organization can falter.

Recently, Pure Storage® hosted a roundtable discussion with four CISOs to uncover the biggest InfoSec challenges facing enterprises today, debunk old myths, and reveal the solutions they believe actually work. Read on for insights from the conversation.

Contents

Part 1: A Day in the Life of the CISO

From the liability felt in the wake of incidents like the SolarWinds hack to the intricacies of managing ultra-low-latency systems without compromising security, it's safe to say CISOs today are under a lot of pressure on a daily basis. And their jobs are never done. To stay ahead of evolving risks (and out of the headlines), CISOs must constantly assess the world around them—and within their enterprises' four walls. During the roundtable discussion, the CISOs identified three common challenges:

Third-Party Software Breaches Increase the Threat of Personal, Not Just Professional, Responsibility

CISOs feel the pain of third-party software risk management deeply. And they take it personally. There are ways to minimize this burden through "risk transfer"—for example, buying cyber insurance to mitigate the financial impact of a breach. But there would still be loss of brand reputation and customer trust to manage.

If a breach results from hacked third-party software, the company is liable, and that, from the company's perspective, may mean they're the ones to blame. That's a heavy responsibility: If CISOs are aware of infrastructure weaknesses and don't order them fixed in a timely way, they're the ones on the hook, having to explain what happened to stakeholders, as well as to investigators.

Reliance on open-source software exacerbates "inheritance risk" and issues with visibility. Choosing open-source or other third-party software means you're also taking on its risks as well—without the visibility you'd have into software created in-house. And when the enterprise is the one supplying popular third-party software, the worries pile up, since no CISO wants customers to be impacted by a coding flaw.

The Need to Beg for Resources—despite the Magnitude of Their Task

CISOs may not own the risk, but they do have to manage it. And while every business function wants more budget, CISOs can feel like they're at the end of the list when funds are handed out—especially when it seems like everything is going smoothly. They want to do more—advanced microsegmentation, for example—but they don't have the means or the headcount. CISOs often see opportunities to get creative with security approaches, matching the ingenuity of hackers, but lack of resources gets in the way.

The Human Element Is Ever-present and Unavoidable

Are CISOs juggling personnel, BYOD best practices, egos, and corporate culture? Absolutely. There's no dodging the fact that people are inextricably linked to privacy and security. Rogue VPN use, engineers creating backdoors to boost productivity, and poor password management can thwart even the most effective security controls. This means training, awareness, and a culture of shared responsibility and reporting are on CISOs' plates.

Awareness is key to letting the humans know the power they wield in allowing a security event to occur. Training has to be role-based and focused to avoid fatigue. And it should clearly communicate all of the ways that people can become attack vectors. The minute they lose sight of the risks they pose, they become risks themselves.

While low-level access users can still compromise systems, CISOs should hone in on higher-level access users. One recommended that engineers be brought to the table and made a part of the plan. Learn their processes and implement security controls for those processes, so they stop creating workarounds—and creating risk. Consequence management should be part of the mix.

Part 2: Emerging Challenges CISOs Are Facing

CISOs find themselves juggling the expectations of diverse stakeholders, having to simultaneously balance compliance requirements, board directives, customer trust, and market dynamics. Managing these multifaceted expectations is no simple feat, especially with new challenges popping up, including:

Balancing Security with Performance

"Protect my data, but keep it accessible and available." It's a common conundrum, as data fuels more enterprise operations—especially AI, where data has to be lightning-fast, frictionless, and secure. CISOs increasingly have to answer for the side effects of safer data, like lagging performance.

Here's where traditional security measures often come with significant trade-offs, including technical debt, difficulty upgrading, and performance degradation. CISOs are tasked with finding solutions that deliver security without compromising on ultra-low-latency requirements—especially in sectors where performance to the nanosecond is critical, such as financial services.

IoT Security Skirts Traditional Controls

The proliferation of IoT devices introduces numerous security challenges, primarily due to their limited capacity for updates and their exclusion from traditional asset management frameworks. Specific strategies to mitigate IoT risks are imperative, given the devices' vulnerabilities and their increasing integration into critical business processes.

Historically, IoT security is the last piece that vendors consider before bringing products to market. User-friendliness is generally high on the list for IoT products, while security is not.

As IoT devices proliferate in the enterprise, the risks rise as well. Voice conferencing systems, AV systems, card access solutions, and even products like printers and refrigerators can all connect to corporate networks with very weak or even nonexistent security. Even if the devices have security, IoT devices tend not to be patched and are often ignored by asset management tools. CISOs and security teams have to rely on IoT vendors to disclose security protections and patching needs, assuming such notification even occurs.

All Security Strategies May Be Compliant, But Not All Compliance Strategies Are Secure

"As long as you can demonstrate compliance, how do you justify the extra $3 million needed for security? If they get a report that ticks all of the boxes, they won't see past that. So that is a huge challenge."

The consensus: Compliance and security are not the same thing. In fact, well-executed compliance can deliver a false sense of security and even put some CISOs in a bind.

Say a CISO is facing the challenge of securing funding for security measures. A buttoned-up compliance report won't help to make their case. Instead, it may paint a rosy picture that everything is under control, offering a false sense of security.

While compliance is certainly necessary, it should not guide the security conversation, nor is it a sufficient gauge of a comprehensive security program. Most importantly, a compliance report represents a point in time, but the dynamic nature of cybersecurity threats requires ongoing vigilance and adaptation. A CISO is responsible for staying on top of holes that constantly arise and need fixing, long after a compliance report is submitted.

Bottom line: Cyber criminals aren't deterred by your compliance, and the market won't care that your compliance report was clean if you get hacked.

State-sponsored Groups Have All the Time and Budget to Keep Hacking

The groups behind state-sponsored attacks aren't slowing down, especially when it comes to financial institutions facilitating crypto trading. Sophisticated, state-sponsored hackers can devote plenty of time to developing specific attack techniques to target financial assets and critical infrastructure, as well as find opportunities for Trojan horses to exploit, in case of economic chaos or armed conflict. Crypto assets run 24×7, putting significant pressure on security teams to keep up with patching or identifying vulnerabilities in a way that outpaces the attackers.

Part 3: The Future for CISOs

Identity Is the "New Perimeter"

"If you look at the breaches that are out there, everything is identity-focused."

Organizations need better orchestration for identity—not only to control access and understand what people are doing but in hopes of truly thwarting threat actors. Because traditional security tools, such as firewalls, weren't built to tackle the new network perimeter, CISOs and their teams seek out process-focused solutions like privileged access management. They also see the value in adding tools like multi-factor identification, so they don't rely solely on trust or authentication.

Hygiene Should Be Security's Job—Not IT's

"Hygiene is a hugely missed point in security. A lot of times in the past, we would have pushed it away and said, 'That's not our job, right?' It was IT's job to keep systems patched and managed. But really, it all flows back to security."

Data hygiene is critical in protecting against data breaches, mitigating the risk of data corruption or loss, and enhancing the overall integrity of an organization's data assets. Given its strategic importance, it's easy to make the case that this responsibility should fall within the purview of the CISO rather than the IT department. This shift reflects a broader understanding that data security is not just about technology management but is inherently tied to the organization's risk management, compliance, and governance frameworks.

If the CISO team owns hygiene as part of their remit, they can more directly control the cleanliness, accuracy, and security of data throughout its lifecycle through the regular updating and patching of software and systems, access controls, encryption, and backup and recovery plans. That includes taking a stronger stance on how quickly patching should occur, rather than being reliant on another team to do it—one with less skin in the game.

This ensures practices are aligned with the broader cybersecurity strategy, allowing CISOs to be more proactive and enforce stringent data hygiene protocols.

Targeted Attacks Require CISOs to "Get Creative"

"Threats are changing and evolving. You can prevent some—but then new ones arise. The main item to focus on is the reaction; because sooner or later, each company will be in some way attacked and breached."

The rise in targeted cyberattacks demands that CISOs employ creative, tailored strategies beyond conventional defenses. Techniques like perimeter or conditional access controls and "honeypots" have been discussed, but the consensus was that innovation in defense mechanisms is crucial to head off the many different ways these groups find to attack an environment—ransomware included. For example, honeypots, which are decoy computing systems that are intended to trap attackers, can't be equipped with firewalls that would deter attackers.

Zero Trust Isn't the Be-all and End-all

Not a day goes by when zero trust isn't praised as the silver bullet to all security worries. But CISOs, who are in the trenches, are skeptical. ***"I tend not to focus on network controls as much as I used to,"*** said one CISO. ***"Zero trust is overplayed. It means a lot of different things to a lot of different folks."***

Zero trust is widely advocated but equally misunderstood. The truth is, it should be thought of more as a long-term objective, not an immediate solution or an endpoint. Implementing zero trust will also require a fundamental shift in how access and trust are managed within an organization's network.

For this CISO, better orchestration of identity is certainly necessary, but not the only security fix to focus on.

Part 4: When the Attacks Happen (and They Will), What Will You Do?

"You can write as many things as you want down, you can practice as often as you can, and you need to. But when it comes to the heat of battle, different personalities pop up, and things that you rehearse tend to get tested."

CISOs fully understand that networks are going to get breached. There's no such thing as 100% security. The good news? Most organizations tend to recover. But if getting compromised is, unfortunately, to be expected, all eyes are on the aftermath: how the organization identifies the threat, communicates its impact, and addresses the weakness that led to it.

In keeping with the CISO mantra of "It's not if attacks will happen, but when," organizations need to be ready to manage situations where they're under attack and under pressure. They can't take the chance that they'll lose sensitive data, damage customer loyalty, and disrupt the business. CISOs not only need to put procedures in place for managing the outcome of an attack but also be assured that the procedures will work under high-pressure circumstances like a ransomware attack. Do people know what to do and how to do it in the minutes and hours after a serious attack, or are they trying to find the file or notebook with the instructions?

When everything's on fire, security teams and their CISOs need to also manage egos and possible infighting. If the head of your SOC and the deputy head aren't in agreement about procedures, the minutes will tick by while the attackers escalate their damage.

CISOs and security teams need to test their scenarios under real-life scenarios, where decisions need to be made in a matter of seconds, not minutes. Technology safeguards such as immutable snapshots of data are invaluable, too.

Part 5: The Modern CISO Stack/Strategy

What capabilities and technologies will CISOs need most moving forward? What should be retired—or, at least, relied on less than it used to be? As one CISO noted, ***"DLP (data loss prevention) platforms were designed for a world that doesn't exist anymore."*** DLP systems are also expensive and complicated to run. So where do DLP platforms fit into the modern CISO security stack—or what should be taking their place?

1. **Immutable backups.** This provides forensic readiness and a reliable recovery point—for example, a clean image to recover to that's not affected by the attack.
2. **Security controls for a new data landscape.** With data spread across cloud services, SaaS products, and various other digital platforms, controls will only get you so far. Modern strategies should encompass data classification, robust asset management systems, data discovery exercises, and stringent access control at the network level. This requires a unilateral, layered suite of tools to provide redundancy and mitigate reliance on a single authentication method.
3. **Encryption of classified, sensitive, personal, critical, or industrial data.** Implementing encryption techniques that can provide access level to that data, and of course, to back up and save the copy of data without affecting replication.
4. **A tiered backup architecture with "data bunkers."** Offline copies of data, not reachable from operating infrastructure.
5. **Anomaly Detection.** Automation and threat monitoring are invaluable, but how do you determine what is abnormal in all the noise? This task becomes even more complex when multiple SaaS-based systems talk to one another on a many:many basis. While it can be time-consuming and resource-intensive, the CISOs suggest microsegmentation coupled with monitoring logs and tailored access can help.
6. **Role-based controls**. Passive monitoring can help identify the level of access needed between systems, then roles can be restricted as much as possible until adjustments are needed.

The Pure Data Storage Platform Gives CISOs Peace of Mind

This enlightening roundtable discussion has highlighted the complex, critical role CISOs play in delivering resilience, privacy, and trust to enterprises, healthcare organizations, governments, and private citizens across the globe. Given the magnitude of this responsibility, it's easy to make the case for CISOs to get a seat at the table—and to get strategic decision-making power when it comes to the technologies that support their operations.

At Pure Storage, we empower CISOs to choose a data storage platform that has their backs and enables them to sleep at night. Pure Storage helps mitigate the risk associated with cyber attacks by building the most resilient infrastructure and eliminating the uncertainty and need for long-term storage planning. Unlike legacy storage products, Pure combines built-in, multi-level ransomware protection with AIOps management to deliver fast, guaranteed clean recovery to minimize disruption to your evolving business needs.

The quality of a recovery is contingent on the quality of the response, which means CISOs need the best possible data storage platform in their corner in the heat of battle. Visit PureStorage.com to learn more.

purestorage.com

800.379.PURE

PURESTORAGE®
Uncomplicate Data Storage, Forever