The Third Question:

What CISOs aren't asking — and what's at stake.

The world's top cybersecurity innovators weigh in.

ABSOLUTE®

02

The role of Chief Information Security Officer (CISO) is one of critical importance — enabling business operations while defending organizational security in the face of ever-evolving threats.

And the stakes couldn't be higher. Failure to identify vulnerabilities and implement measures to address them can have catastrophic consequences — for the business, for customers, and for CISOs themselves.

Yet, balancing the demands of increasingly complex operating environments and rapidly changing priorities continues to challenge CISOs in their battle against sophisticated adversaries who are able to quickly adapt their techniques to the evolving threat landscape.

It seems that no sooner is a threat identified and addressed than another emerges, locking CISOs into a never-ending cycle of addressing two key concerns:

1. What security risks are we facing?
2. Do we have the necessary tools to manage these risks?

With security teams moving at breakneck speed to complete one project and move to the next, the third — and most important — question is often left unasked:

3. Once we've deployed these security tools — can we be certain that they're working as expected?

Without a continuous evaluation of their efficacy, CISOs risk over-investment in their security stack and, worse — overconfidence in their security posture — a surefire recipe for disaster.

We sat down with four globally recognized experts in cybersecurity — each of them experienced CISOs within the world's largest organizations — to gain insight into why, with so much at stake, this critical third question is frequently overlooked. How can organizations embed answering it into their security strategy? And, for those who do ask, what should be done when the answer is, 'no'?

Charles Blauner

Former Global Head of Information Security, Citi**; former CISO,** JP Morgan and Deutsche Bank**; Partner & CISO in Residence,** Teams8 Group**; President,** Cyber Aegis Consulting**; Strategic Advisor,** Absolute Software

Lou Klubenspies

CISO and Senior Director, IT Risk, PerkinElmer

Todd Inskeep

Former Commercial Cybersecurity Delivery Executive, Booz Allen Hamilton
RSAC Advisory Board Member

Malcolm Harkins

Former CISO, Intel
Chief Security and Trust Officer, Cymatic

Complexity is the enemy of security

Today's CISOs are charged with rapidly rethinking their security and risk strategies in the face of changing priorities and new demands of their role. Fast-evolving business environments, increasingly stringent compliance requirements, and ever-present budget and talent constraints mean that more is expected of them than ever before.

And all the while, new threats continue to emerge, with the solution often being to layer additional tools onto an increasingly complex security stack. Studies show that 86% of organizations use up to twenty security vendors[2], with many organizations managing solutions numbering into the hundreds. Predictably, 81% find this multi-vendor environment challenging.[3]

Charles Blauner knows these demands well. An internationally recognized expert on cyber resiliency, information security risk management, and data privacy, Blauner was most recently Global Head of Information Security at Citi, and previously held the CISO position at both JPMorgan and Deutsche Bank.

"CISOs tend to be responsible for very large, very complex environments," he explains, citing the 140 security tools and 500,000 devices under his purview across Citi's 100-country, 225,000-employee operation.

"But understanding operational integrity isn't just a challenge for global organizations — complexity impacts companies across the spectrum."

And, Blauner continues, in the face of this complexity, sometimes the most obvious questions can get overlooked.

"The CISO job can be so overwhelming, with so much to think about, that some of the follow-up gets left behind. And the question of, 'Is it still working?' is probably the biggest — not because you don't care, but because your attention has already turned to one of a thousand other things.

"When you finish a project or deploy a solution, you only have a moment to catch your breath. Another project is always waiting, another problem to solve or crisis to plan for. You're constantly jumping from one thing to the next. When looking across my world, there were 10 different program areas, with four or five scary projects happening at any one time. And there were always more on the horizon."

[2] 2020 Cisco CISO Benchmark Study, *Cisco.*
[3] ibid

An evolving, multifaceted role

As environmental complexity expands, so too does the role of CISO, with many now expected to contribute more directly to revenue strategies and customer experience initiatives.

With 30 years of innovation in cybersecurity, leading to his most recent position of Commercial Cybersecurity Delivery Executive at global consulting firm, Booz Allen Hamilton, Todd Inskeep has experienced the evolution firsthand.

“Today, CISOs get pulled in two directions: advancing how the enterprise thinks about security in everything it does and protecting it from attacks.”

Strategically, we’re closer to the business than ever, and that’s a good thing, because there’s a lot we can contribute to critical issues. Are we making money? How do we secure new business models? How do we secure our remote workforce? But this can also result in our attention being drawn away from the effectiveness of the tools and tactics already deployed.”

Threat landscape overload

With 86% of cyberattacks in 2019 motivated by financial gain[4], unprotected devices offer would-be attackers an appealing and, too often, successful target. In fact, the majority of breaches start at the endpoint[5].

In Inskeep's estimation, "99% of the time, endpoints are the source of entry. Adversaries gain access to a device and expand from there."

Malware and ransomware continue to be top threats, with phishing accounting for 80% of attacks[6]. And, with the average cost of a breach ringing in at $3.86M[7], the cost to businesses is staggering.

In response, organizations have shored up their endpoint defenses, layering on controls in a desperate race to remain one step ahead — despite all too often, lacking the visibility and tools to know if these controls are working, and to take action when they're not.

[4] 2020 Data Breach Investigations Report, https://enterprise.verizon.com/en-gb/resources/reports/dbir/
[5] IDC, 2018 , Securitymagazine.com, https://www.securitymagazine.com/articles/90388-endpoint-security-tools-eventually-fail-says-a-report
[6] CSO.com, https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html
[7] Cost of a Data Breach Report 2020, *IBM*.

Endpoint complexity is itself a vulnerability

As Blauner attested, managing endpoint complexity — driven largely by the increase in would-be solutions — is an ongoing battle.

In a 2020 study of six million endpoints, Absolute found that nearly one in three devices had an endpoint protection, client management, or VPN application that was not in compliance, and more than five percent of devices were missing one or more of these critical controls altogether.[8]

When antivirus or antimalware tools were installed, the majority of devices had more than one agent designed to do the same function. Multiple, sometimes duplicate, agents were causing controlss to collide and decay, leaving endpoints vulnerable.

Keeping devices up to date — particularly when securing a remote workforce may require deploying patches off-network — introduces its own set of challenges.

Since the beginning of the COVID-19 outbreak, the average time to patch has hovered well above two months. For organizations running Windows 10, the average delay increases to a startling 95 days.[9]

This, despite unpatched vulnerabilities remaining the most common attack vector for cybercriminals — another recent study found that 60 percent of breaches can be linked to a vulnerability where a patch was available, but not applied.[10]

[8] 2020 Endpoint Resiliency Report, Absolute.
[9] ibid
[10] https://www.darkreading.com/vulnerabilities---threats/unpatched-vulnerabilities-the-source-of-most-data-breaches/d/d-id/1331465

Taking matters into their own hands

The impact of multiple security agents on endpoints also impacts the user experience, and when employees get frustrated, their actions may inadvertently introduce new vulnerabilities.

Malcolm Harkins, former CISO at Intel, is a long-time advocate for minimizing risk through optimizing security controls — while maintaining a firm eye on business objectives and user experience. Says Harkins, "I see my role as a choice architect. We have to provide solutions that benefit the business, the CIO, and the end user. Key to that is creating a low-friction environment — where our security choices don't render devices more difficult to use. Knowing which controls increase friction is an essential component of threat management.

"When people start feeling pain, they'll disable or remove the source of that pain. Often, this is because the tools don't integrate well, and, quite frankly, the big security vendors are not incentivized to solve this integration problem."

Still, Harkins is quick to acknowledge that end users should not be held responsible for simply wanting their computer to work smoothly. "Too often, end users are blamed, when it's actually security, IT, and the management team that need to be accountable for providing a solution."

Only as strong as your weakest link

The importance of knowing if controls are present and working on every device could not be more clear with complexity resulting in their collision and decay, the probability that every endpoint protection agent will eventually fail is 100%.[11] This, acknowledges Harkins, is of major concern:

> **"An unprotected endpoint is the weakest link in the chain."**

Blauner highlights the need for security leaders to take action, stating, "CISOs are not thinking about the endpoint agent degradation problem. It just isn't in the inventory of risks, or, if it is, they don't know they have a way to actively manage that risk. If there is a whole category of risk that you are failing to manage, then there's a gap in delivery against what the Board expects of you. Closing that gap requires awareness of what's happening on the endpoint."

[11] ibid

You can't secure what you can't see

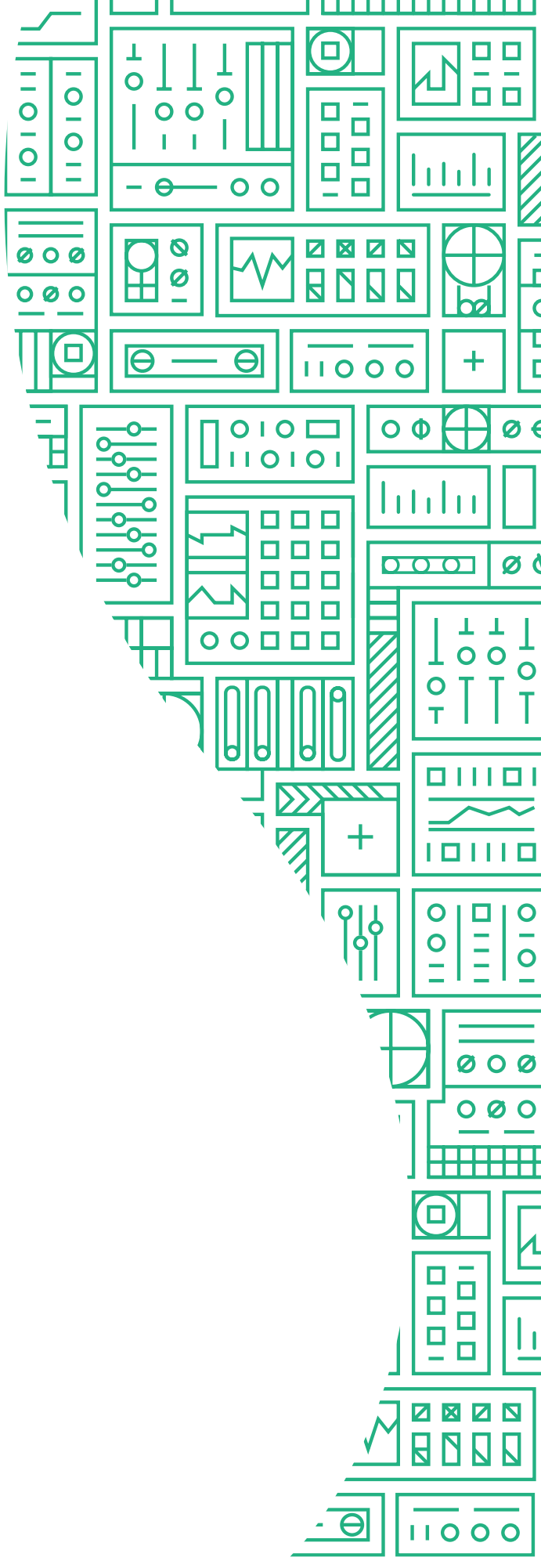
Of course, achieving that awareness means that devices must remain visible— never a greater challenge than now, in the face of a global pandemic. For CISOs tasked with maintaining business continuity for their newly remote workforces, keeping endpoints in sight is the first step toward knowing what's working.

"Asset visibility is my greatest worry," confides Lou Klubenspies, CISO at Fortune 1000-ranked genetic research firm, PerkinElmer.

"I inherited over 10,000 endpoints — that I'm aware of. But am I seeing every endpoint in my environment, and how do I know for sure? Now that people are working from home, they're staying off the VPN, too, and that compounds the issue."

Says Harkins: "It takes visibility to prevent vulnerabilities and compromises. Without it, detection becomes difficult, and in many cases, leaves response after the fact as the only option."

Klubenspies echoes the need for greater focus: "We have to work harder on gaining visibility. And we need the tools to make the experience seamless."



The risk tolerance trade-off

Klubenspies explains, “My job is risk management, not risk elimination. You’re never going to be able to fully eliminate risk, so you have to figure out what amount you’re willing to live with.”

Blauner agrees. “As a CISO or CIO/CTO, you have a responsibility to your stakeholders around the operational integrity of the environment. The expectation is that you can say with confidence: I understand our risks. I measure our risks. And I manage them against a set of risk tolerances that, as a CISO, I have agreed upon with the Board of Directors.”

Answering the third question

Mitigating risk by addressing endpoint complexity can be the difference between knowing that users are accessing the network from devices that are secure, encrypted, and up-to-date, or exposing the organization to attack when preventative controls are compromised.

Faced with an evolving threat landscape, rapidly shifting priorities, and security agents failing at predictable rates — despite heavy investment — CISOs that pause to embed 'Is it still working?' into their success criteria will inevitably improve their security posture — and realize the value of their investments.

"We need to find out if the product actually solved the problem we intended it to, and if it's still doing its job," says Blauner. "The first step is making sure this is measured.

"There will be three sets of outcomes when we start asking the question. One: there's no problem — although this is unlikely. Two: there is a problem, but it's product-specific and we can exit or replace the product to solve the issue. Or, three: there's a problem created by interaction between products or the environment itself. In this case, the consequences of removing a product may make it worse, so instead we need to manage the risk by making that environment resilient."

Resilience is the solution to complexity

With massive complexity endangering today's endpoint environments, it's clear that simply relying on solutions such as encryption, VPN, antivirus, and antimalware for protection is no longer enough.

According to Gartner, Inc., "Boards and senior executives are asking the wrong questions about cybersecurity, leading to poor investment decisions. It is well-known to most executives that cybersecurity is falling short. There is a consistent drumbeat directed at CIOs and CISOs to address the limitations, and this has driven a number of behaviors and investments that will also fall short."[12]

Today's CISOs must increase the rigor around measuring the effectiveness of the investments they've made. They need to ask the third question — 'Is it working?'— and have strategies in place when the answer is 'no.'

The proven approach is a strategy of endpoint resilience. At its center is a hardware Root of Trust that is embedded in device firmware and immutable, allowing organizations to maintain connectivity and control through an unbreakable digital tether. Endpoints must be able to recover from any incident to a secure operational state automatically, without user intervention.

As to security solutions that deliver true endpoint resilience, Blauner has only one recommendation, asserting, "Absolute is the only solution that can answer the question, 'Is it still working?'. They are the company best positioned to solve the endpoint resilience problem and create a self-healing environment."

Absolute is the only undeletable endpoint defense platform. Using patented Persistence® technology embedded in the firmware, it allows organizations to maintain a continuous, secure connection to every device — even off the corporate network.

It is this unbreakable connection that powers endpoint resilience — enabling devices to heal themselves, with autonomous capabilities for repair and reinstallation. And because this ability to self-heal is also extended to critical applications, Absolute is uniquely able to answer 'the third question,' and give CISOs peace-of-mind that their endpoints are protected.

[12] Gartner, The Urgency to Treat Cybersecurity as a Business Decision, Paul Proctor, 12 February 2020. (Gartner subscription required)

Living up to the role

"We have a responsibility to the business, to our customers, and to society to secure the endpoint," says Harkins. "A CISO's goal in answering 'Is it still working?' is not only the impact on the company's bottom line, but on lives."

For Klubenspies, every CISO must know the answer to feel confident they've done their job. "You need to be able to look your CEO in the eye and tell them that the organization is secure. If you can state with confidence that your security tools are working, you're in a good place."

ABOUT ABSOLUTE

Absolute Software is a leader in Endpoint Resilience™ solutions and the industry's only undeletable defense platform embedded in over a half-billion devices. Enabling a permanent digital tether between the endpoint and the enterprise who distributed it, Absolute provides IT and Security organizations with complete connectivity, visibility, and control, whether a device is on or off the corporate network, and empowers them with Self-Healing Endpoint™ security to ensure mission-critical apps remain healthy and deliver intended value.

EMAIL:
sales@absolute.com

SALES:
absolute.com/request-a-demo

PHONE:
North America: 1-877-660-2289
EMEA: +44-118-902-2000

WEBSITE:
absolute.com