

COHESITY

Strengthening Cyber Resilience: Tackling Threats and Gaps

Industry Leaders Discuss Proactive Measures to Strengthen Cyber Resilience

ISMG
INFORMATION SECURITY
MEDIA GROUP

COHESITY



Tom Gillis

Gillis previously served as the senior vice president and general manager of networking and advanced security at VMware. Prior to that, he founded Bracket Computing in 2011 and served as its CEO. Before that, he was president and general manager of Cisco Systems' security technology group and vice president of marketing and co-founder of IronPort Systems, acquired by Cisco in 2007.

Brian Spanswick

Spanswick has over 20 years of experience managing IT and cybersecurity organizations within high-growth companies, while also providing consulting services for large, globally dispersed blue-chip enterprises. Prior to Cohesity, he managed risk and information protection at Splunk, leading and rapidly expanding the organization responsible for managing cyber risk across the company.



In a world where cyberthreats loom larger than ever, organizations are facing a critical imperative: strengthening their cyber resilience. Industry leaders **Brian Spanswick**, CIO and CISO of Cohesity, and **Tom Gillis**, senior vice president and general manager of Security Business Group, Cisco, shared insights into the evolving landscape of cyberattacks and the proactive measures being taken to combat them. From boardroom concerns to front-line strategies, automation, AI and collaboration play pivotal roles in fortifying defenses and minimizing the impact of breaches, the duo agreed.

"The headlines speak for themselves. Cyberattacks have reached the boardroom level and have prompted a shift in strategy toward minimizing the impact of these disruptions on business outcomes," Spanswick said, emphasizing the prioritization of cyber resilience. "Timeliness is the most important thing. A combination of automation and AI tools will allow us to create more automated responses than were ever before possible, even six months ago. The industry is going through an explosive period of change," Gillis said.

In this video interview with Information Security Media Group at RSA Conference 2024, Spanswick and Gillis also discussed:

- Integration efforts to streamline security operations;
- Shifting focus from solely trying to prevent attacks to also minimizing their impact;
- The collaboration between Cisco and Cohesity.

THE NEED FOR CYBER RESILIENCE

ANNA DELANEY: Cyberattacks and ransomware attacks are becoming increasingly a board-level concern. What are IT leaders and security leaders doing about these growing threats?

BRIAN SPANSWICK: The headlines speak for themselves. Cyberattacks have reached the boardroom level and have prompted a shift in strategy toward minimizing the impact of these disruptions on business outcomes. It's different than just talking about how you protect your assets. It's talking about the sustainability of the organization. That's why it's becoming board-level.

TOM GILLIS: The ability to disrupt is self-evident. There are attackers whose motivation is financial. There are nation-state attackers who are looking simply to disrupt, and that's a growing concern in this geopolitical environment. Timeliness is the most important thing. A combination of automation and AI tools will allow us to create more automated responses than were ever before possible, even six months ago. The industry is going through an explosive period of change. Some of the work that we've been doing with Cohesity is a perfect example of what we can do to automate the response and recovery in the event – the inevitable event – that an attack occurs.

SPANSWICK: Two things have changed over the last five years. There's been a focus on: How do we minimize the impact of these attacks and not just try to stop them? We'll continue to try to stop them, but it's become an arms race with the attackers. Minimizing the impact if they're able to get through the defenses is key. It's all about time. How quickly can you recover your core processes, minimizing the disruption, and how quickly can you identify and respond to the attack? That's where you're seeing organizations invest.

ACHIEVING CYBER RESILIENCE

DELANEY: What are security leaders doing to prioritize building resilience into their security strategies?

> "It's all about time. How quickly can you recover your core processes, minimizing the disruption, and how quickly can you identify and respond to the attack? That's where you're seeing organizations invest."
>
> – Brian Spanswick

SPANSWICK: It's changing their strategy. Their strategy is becoming more balanced. They're making investments as much in resiliency as they are in trying to stop or create a wall to keep the attackers out.

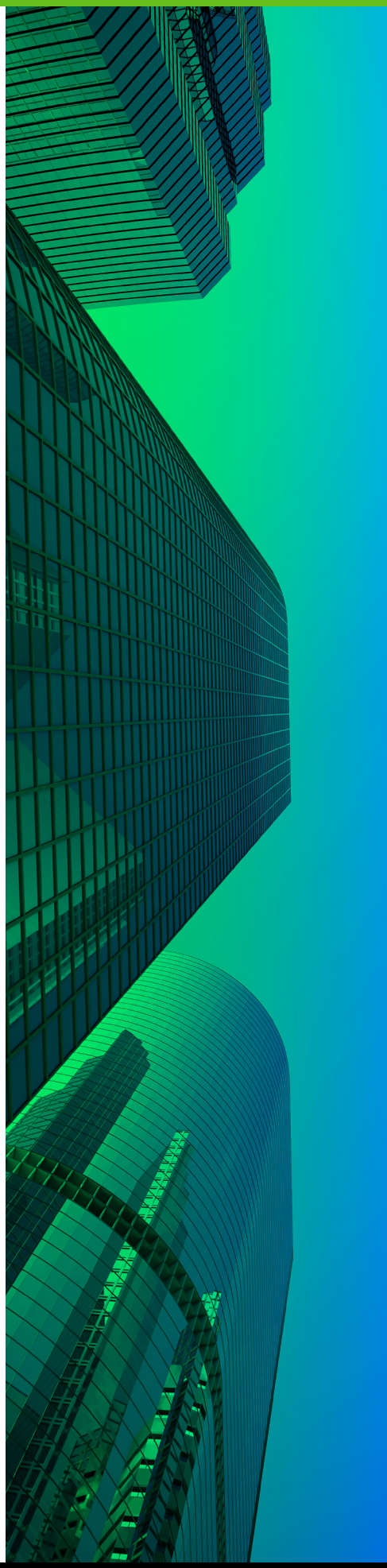
GILLIS: If we get our head around the idea that we want to focus on resilience and accept that an attack is going to come, it opens up some super interesting possibilities that we've been working on together. If you look at most of these attack profiles, attackers make several moves in the infrastructure that are detectable, but at a very low-fidelity detection, meaning a very high false-positive rate.

So, attackers quite deliberately hide in the noise of legitimate behavior. It's not practical to block or disrupt a connection or movement at that early stage of the attack. But using some of the automation techniques that we've been developing together, you can take a non-invasive passive response, such as trigger a snapshot. That can allow the response to move much earlier in the attack chain and therefore minimize potential damage and dramatically enhance security resilience. It's not an incremental change.

SPANSWICK: You're packaging the ability to rapidly recover or restore from the disruption as close to the disruption as possible, and that changes the game, especially in today's world where the attackers are exploiting some vulnerabilities within hours of that vulnerability being announced as opposed to days. How do you build a defense against that? Your best defense is to quickly respond and recover.

AN EXAMPLE OF CYBER RESILIENCE

GILLIS: Let's walk through a real scenario that we've worked on together. Imagine an email comes to one of your employees, and there's just something funny about that email. The sender doesn't accept mail in return – other than that, the email looks totally clean. There's a 5% probability it's



> "When a vulnerability is announced, within hours, we see it being exploited. That's a huge problem because … patching an application takes time. Having automated responses that can mitigate the damage in that window of exposed vulnerability is important."
>
> – Tom Gillis

malicious. The email has a link. The user clicks on that link, and it goes to a photo-sharing site that looks totally clean. We don't see any malware except it's new, and we've never seen it before. There's a 7% probability it's malicious.

Then all of a sudden on that machine, we see PowerShell spawn a new process we've never seen before. We talk to the EDR running on the machine. Windows Defender says, "No, I've never seen it before; it's new." At that point, there's a 10% probability that this is malicious. When that process goes to make a connection on the network, Cisco is able to see this in real time because we are in the network.

So, we can see a funny-looking process on a funny-looking machine wants to connect to this server, which is a customer database. At a 10% probability of being malicious, there's no way we're going to block that connection. If we sent that alert to the SOC, they would turn it off because 90% of the time, it's wrong. But a snapshot with Cohesity takes up almost no space.* We say, "Let's allow the connection, but let's take a copy of it, trigger a snapshot." We mark it. We don't make an alert or bug anybody, and then we watch.

If it turns out that the new process was just a Windows update , we throw the snapshot away. With Cohesity, that's almost no consequence. But if it turns out that it's a ransomware attack, we just automated the recovery process to use, in storage parlance, an RPO recovery point of zero. That means, "Dear customer, I'm so sorry to inform you that you had a ransomware infection. Here's the good news. You didn't get sick. It's like a vaccine for ransomware. You may have an infection, but it's not going to have impact on your business operations." That is security resilience.

SPANSWICK: It's super exciting. You've got the capability to recover in the snapshot that you got from Cohesity, but it's triggered and identified quickly through the insights and the automation through the Cisco solution. It's a powerful combination.

GILLIS: And as we bring Cisco and Splunk together, we're going to flow that same functionality up into

* edited for clarity



the Splunk console. This is going to become part of the playbook of every security operations center everywhere, thanks to Cohesity.

CYBER RESILIENCE CHALLENGES

DELANEY: Where are the most significant gaps in resilience plans right now?

GILLIS: It's the speed at which attackers are responding to new vulnerabilities. When a vulnerability is announced, within hours, we see it being exploited. That's a huge problem because no matter what you do, patching an application takes time. You don't just patch – you don't just throw new code into a running application and hope it works. It takes days, sometimes even weeks, and sometimes you can't patch because you don't even control the app. It's a third-party piece. Having automated responses that can mitigate the damage in that window of exposed vulnerability is important.

Something like Log4j creates a significant, scary threat for the security community. The flip side is: With automation, we have the ability to create graduated responses. We can turn on a packet capture, trigger a snapshot and follow the attackers in a way that allows us to back them out without having any business impact. That's magical.

SPANSWICK: That helps you action the recovery. The other gap that I see in a lot of security organizations is that their recovery capabilities are based on old ideas around disaster recovery. They've got legacy backups that would be very similar to you backing up your iPhotos to make sure that you don't lose the data, but you haven't considered what it's going to take for you to be able to recover those core systems. That capability combined with the ability to action that quickly against an attack is the gap that needs to be bridged.



THE CISCO-COHESITY APPROACH

DELANEY: How are you helping your customers with their cyber resilience plans?

GILLIS: At Cisco, we're focusing on automated response. We introduced Cisco Hypershield, where we have the ability to put a little compensating control in front of a vulnerability in a highly automated fashion. Perhaps within minutes of a vulnerability being announced, we can put in a little protection. It doesn't alleviate the need for patching, but it automates the response. It's very consistent with the work we've done together to automate the snapshot. We plug the hole, take a snapshot, and now if an attacker got through, we can contain the damage and minimize or eliminate business impact.

SPANSWICK: From a recovery perspective, our solution has the ability to recover quickly at scale based on the way that the product is architected. You don't have to go through multiple steps of hydrating the data, which would add time to your recovery time objective. It enables recovering large business processes at scale.

GILLIS: That's one of the things that Cohesity does particularly well in our view. We're not storage people, but they're able to define these protection groups so that it's not only the recovery point but the recovery time. When I trigger that snapshot, I know that Cohesity has figured out all the stuff that has to be captured so that I can restore back and make the thing run. It's a good combo.

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 36 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

(800) 944-0401 • sales@ismg.io

BANK INFO SECURITY® · CU INFO SECURITY® (Just for Credit Unions) · GOV INFO SECURITY® · HEALTHCARE INFO SECURITY®

infoRisk TODAY · CAREERS INFO SECURITY® · Data Breach TODAY (Prevention. Response. Notification.) · CyberEd.io

CIO.inc · DeviceSecurity.io · PaymentSecurity.io · FraudToday.io

CYBER THEORY · CyberEdBoard · Xtra mile LIFECYCLE MARKETING · GREYHEAD

ISMG
INFORMATION SECURITY
MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismg.io