FROST & SULLIVAN

Visibility, Measurability, and "Securability": Achieving Resilient Cloud-to-edge Security

By Toph Whitmore, Industry Director, Cybersecurity Frost & Sullivan

Sponsored by

TECH mahindra

IBM Platinum Partner

FROST & SULLIVAN VIRTUAL THINK TANK

Enterprise security leaders face a myriad of operational challenges: They must secure operations, manage risk, and—in a world of constrained budgets—find ways to do more with less. Meanwhile, threat actors attack with seeming impunity, targeting vulnerable organizations with cyberattacks that grow more frequent, more sophisticated, and more damaging.

In the first in a series of Virtual Think Tanks, Frost & Sullivan Industry Director Toph Whitmore moderated a panel of enterprise cybersecurity leaders driving cloud initiatives in their respective organizations. They discussed their experiences establishing transparency, understanding resilience, and even measuring "securability."

Panelists included Joshua Copeland, cybersecurity director at AT&T; Dr. Shri Kulkarni, advisor to and head of the Cybersecurity Governance, Risk & Compliance program at Bombardier; Shannon Lietz, VP of Product and Software Security at Adobe; Jeff Nagle, information systems security manager at Stanley Black & Decker; and Sundeep Kumar, executive director at Morgan Stanley.

The Challenges of Securing a Multicloud, Remote-Access-Enabled, Device-Agnostic World

In the last decade, technology has shifted to the cloud, employees have shifted away from the office, and work has shifted onto any and every type of device. It's a cloud-prioritized, remote-access-enabled, device-agnostic world: Employees connect from a coffee shop, at headquarters, or on an airplane. They use resources on the internet, in the cloud, and in the corporate datacenter. They work on company-issued laptops, shared operational systems, even their own smartphones.

Enterprises have adapted—well, *are* adapting—to accommodate the new ways of work. In a recent poll, nearly three-quarters of enterprise cybersecurity leaders identified cloud as the most critical part of their digital transformation. And more than half of the enterprises included in the survey are prioritizing hybrid and multicloud environments.[1]

This rather dramatic shift to hybrid workspaces has extended defensible territory for most enterprises. In doing so, it has also created new blind spots. And threat actors are taking advantage. Cybersecurity attacks increased tremendously in 2020 and 2021, primarily in the frequency and sophistication of attacks. Worse, those **threat actors are using artificial intelligence (AI) and machine learning (ML) to scale up their attacks.**[2]

Thieves go to where the money is. And that lucre is easy to find. The average cost of a data breach to an enterprise based in the United States has grown to $9.4 million—nearly $5 million higher than the global average.[3]

1 Frost & Sullivan. (2021, December 15). The State of the Cloud 2021: The Hybrid, Multicloud Forms the Foundation to Digital Organizations.

2 Frost & Sullivan. (2022, January 18). Increasing Sophistication of Attacks and Evolving Threat Landscape Powering Global Industrial Cybersecurity, Outlook 2022.

3 IBM. (2022). Cost of a data breach 2022.

Achieving Resilience in the Face of Unyielding Threats

This Virtual Think Tank session's panelists noted the difficulties of securing the modern enterprise against an ever-evolving threat landscape. And though perspectives may have differed by geography or vertical, several key insights emerged:

- Visibility is a mandate, and it starts with documenting the enterprise universe of apps and resources.
- Measurability makes enterprise risk management not just possible, but practical.
- Resilience—in all its forms—is achievable…but only with good strategy coupled with AI-enhanced cybersecurity.
- Industry frameworks offer a compliance starting point, not the finish line.
- Integrating artificial intelligence and machine learning into security workflow can strengthen enterprise cyber defenses.
- Justifying cybersecurity investment requires business context and alignment with enterprise strategy.

Visibility is a mandate, and it starts with documenting the enterprise universe of apps and resources.

Panelists concurred that visibility starts with knowing enterprise assets—**what they are, where they are, and how they are used**.

> **"Ninety-nine percent of the CIOs or the CTOs, if we walk into their boardroom and ask them, 'Can you tell me you have an exact count of your inventory?' I don't think anybody would say, 'Yes,' to it," commented Dr. Shri Kulkarni.**

Kulkarni prioritized three transparency objectives "buckets" to reduce blind spots in an organization: "visibility into accurate configuration," "visibility into the identity and access management," and "adoption of technology to identify a malicious insider."

For Adobe's Shannon Lietz, manageability of that visibility into corporate systems is paramount. "The biggest challenges that we face in moving forward as an industry, moving forward with technology…really is about complexity," commented Lietz. "[T]ransparency helps us with figuring out what specifically we care for."

AT&T's Joshua Copeland echoed Kulkarni's "bucket" list priorities but provided his perspective on reaching those ideals.

> **"[U]nderstanding what your actual network contains, what is within that boundary, is ultimately the first and hardest part of the equation," said Copeland. "'Do I have shadow IT sitting here? [A]m I running some OT stuff on my IT infrastructure because they didn't realize that that really should be segregated? Have I done the appropriate segmentation and microsegmentations?' But the first thing you have to do is figure out where that boundary is, what's included, what is not included. And that is extremely hard."**

As employees have embraced remote work, such security boundaries have been extended to accommodate work-from-anywhere connectivity. And that has greatly expanded the external attack surface, introducing new vulnerabilities, risks, and management complexity. Attack surface management has become so important to large enterprise security leaders that they cite it as their number one investment priority.[4]

Measurability makes enterprise risk management not just possible, but practical.

How does an enterprise measure security posture? It's a difficult question, but according to Adobe's Lietz it is one that enterprise cybersecurity leaders must (and can) answer.

> **"We can take away [threat actors'] advantage by focusing on the most important tactics and procedures that they're working through, thinking about the vectors that are critical from the perspective of those adversaries," explained Lletz. "Chasing an actual measurement is going to give us a lot more power against adversaries."**

4 Randori, an IBM Company (2022). The State of Attack Surface Management 2022.

Lietz proposed a "securability-as-a-metric" risk measurement, one that positions enterprise assets "in scope for those adversaries" as the numerator and "exploitable opportunities" as the denominator. The resulting metric can be used to benchmark risk and threat posture.

"[With a "securability" metric,] you can focus your effort on the most critical elements of the problem with adversaries," said Lietz. "And then, from there, [be] really transparent about what your escapes are…Getting to the point where you're doing root cause on those escapes and really driving down your exploitable opportunities over time has the most impact on taking away the possibility of adversaries getting there first."

Resilience—in all its forms—is achievable…but only with good strategy, practices, and commitment.

Sundeep Kumar of financial services firm Morgan Stanley described his sector's perceived "lack of understanding about cloud and security," noting that "the first misconception that almost everyone in the financial industry has is that the cloud is insecure." For Kumar (and, for that matter, for the banking industry as a whole), faith in the institution is the basis of secure cloud transformation.

> **"We are actually resilient because we believe in our system," commented Kumar. "As long as we secure our systems, we are actually in very good shape. [W]e are a big believer that cloud is the direction and not only private cloud, public cloud for us, and the main problem that we see is people understanding what their footprint is and what is their threat parameter."**

For Stanley Black & Decker's Jeff Nagle, cybersecurity resilience requires discipline. "Everything that we've been talking about really builds on establishing good resilience," said Nagle. "And the word or phrase that comes to my mind is cyber hygiene."

Kumar noted that involving all stakeholders in cloud transformation planning was a step towards greater resilience and oversight: "When we move to the cloud, we want it to be secure. We have to understand it and then make everyone aware of it. The main thing for getting transparency is moving towards understanding what is our entire inventory."

Industry frameworks offer a compliance starting point, not the finish line.

Nagle, Kulkarni, and Copeland all spoke of the importance of structural cybersecurity frameworks, citing as examples the Cybersecurity Maturity Model Certification (CMMC), NIST 800-53 (Security and Privacy Controls for Information Systems and Organizations), NIST 800-171 (Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations), and Center for Internet Security Controls (CIS) among others. But whatever the baseline, cybersecurity frameworks are meant to be built upon.

"[At Stanley Black & Decker,] we work towards accomplishing and achieving NIST 800-171 and all the controls," said Nagle. "It basically gives you a really solid framework when fully implemented to address everything that we've been talking about."

> **"I look at NIST 800-53, NIST 800-171, and CIS benchmarks as the minimum bar," commented Copeland. "[But] you need to tailor it based on your unique security requirements because no standard's going to be the right fit for everyone across the board. A lot of folks see meeting one [or more] of these criteria as the goal, and really it should be just the starting point."**

Kulkarni observed that complying with industry-standard security requirements isn't flexible and has become a business leadership priority. "Either you have implemented everything, or you have not done everything," he explained. "[You can't say,] 'I've just discovered 50% of my systems, but the other 50% is still in process.' You don't get a score for that. That level of visibility is at the board level right now. So, they're pressuring, pushing the technical teams to a 'T' on this."

Integrating artificial intelligence and machine learning into security workflow can strengthen enterprise cyber defenses.

As threat actors adopt more menacing tactics, enterprise cybersecurity leaders must employ their own advanced technologies to thwart attacks. AI and ML offer promise in data analysis, threat detection, and behavioral assessment.

Panelist Kumar detailed how Morgan Stanley uses AI/ML to identify individual fraudulent transactions, detect potential breaches, and reduce risk.

> **"We always have a problem with insider threat," explained Kumar. "So we have systems which track how people are actually using the system. If someone from HR connects to a development repository and kit, you know that's a problem. We need tools which recognize that there's an anomaly, something that we have not seen before. And that's where AI's predictability basically comes into place. We are now looking at using AI in every single aspect of our security monitoring."**

In fact, a recent survey found that organizations using security AI and automation detected and contained an incident on average 74 days faster versus organizations that didn't deploy security AI and automation.[5]

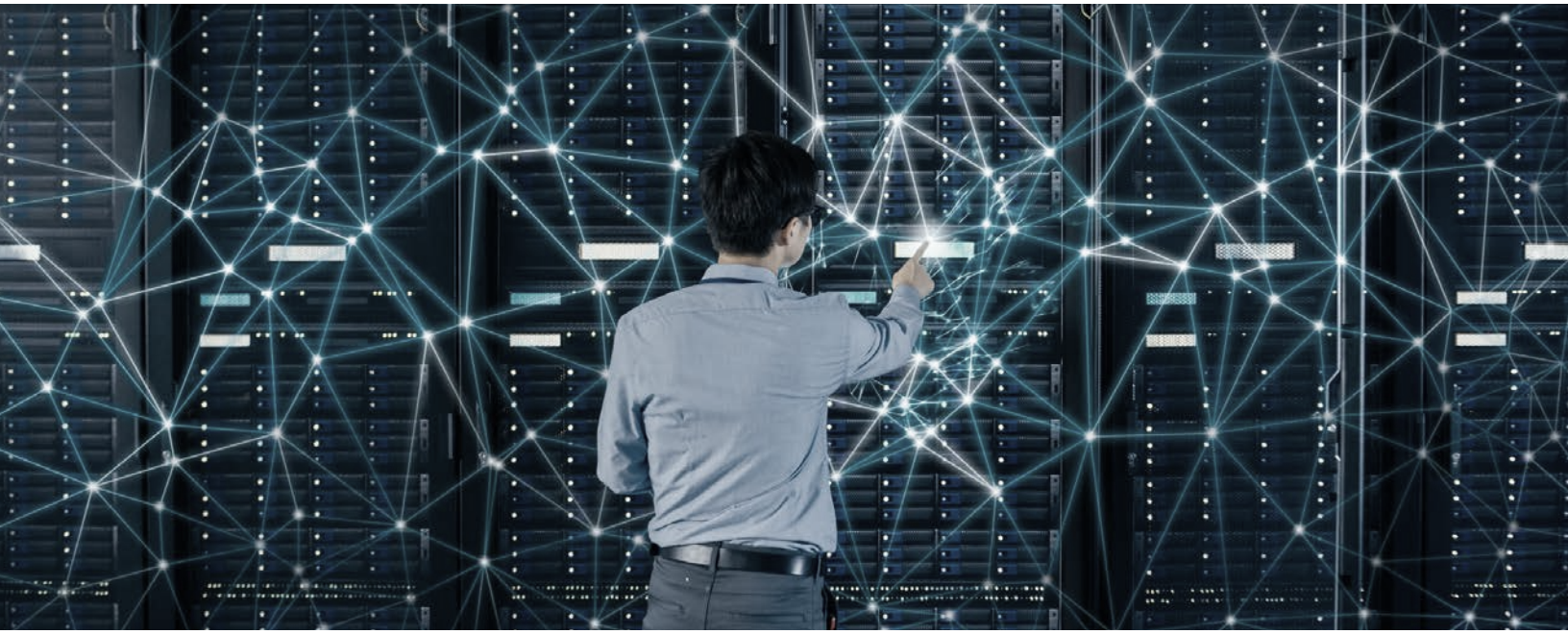
5 IBM. (2022). Cost of a data breach 2022.

Justifying cybersecurity investment requires business context and alignment with enterprise strategy.

Cybersecurity risk is business risk, and—according to panelists—managing it properly can set an organization up for growth. So how do industry security leaders justify continued investment in cybersecurity technologies?

> **"I try to focus on showing ROI through security," noted Stanley Black & Decker's Nagle. "Reducing our cybersecurity risk will increase our ability to bid on contracts. And that's a direct income generator which shows value…showing I secure your network equals more money."**

Adobe's Lietz concurred. "Risk management is very much a set of processes, capabilities," said Lietz. "We have to, as a community, get to the point where we use metrics to drive the conversation of what is the risk. Are we all on the same page across the company? If you don't understand what you're trying to drive, you won't get the maximum investment you're trying to get out of it. ROI is going to be based on what you're doing with your processes."



Ongoing Continuous Improvement, Measurable Progress, and Carrying a Big Stick (of AI and ML):

The present and future of securing the modern enterprise

IT leaders must secure both cloud-friendly and cloud-unfriendly devices. The changing threat landscape demands new security architectures that:

- Provide full visibility into employee work, whether it is on the network, the open Are measurable—in security risk posture, business impact, and asset "securability"
- Deliver fast, secure connectivity for employees, whether they are working at headquarters, in a branch, or at a coffee shop
- Employ advanced technologies (e.g., XDR, AI/ML) to detect and thwart cyberattacks

The challenge of thwarting cyberattacks is one that requires boundaries, controls, and a new way of thinking about threat actors, cautions Adobe's Lietz. "If you look at the total universe of folks that come to your websites and whatnot, adversaries are in there," said Lietz. "They're part of it. How do we think about customer-focused and adversary-focused and being able to create finite controls around how we think about and talk about the problem space? If you think about most cybersecurity, it's unbounded. These adversaries could do anything! [But with controls in place,] it's actually a boundable way that we can move forward."

Kulkarni advises enterprise security leaders to take a long-term outlook. Kulkarni concluded: "[T]here is still a humongous room for [cybersecurity] improvement in all the companies. And that is a never-ending journey."

IBM's Mary O'Brien adds that "the security fraternity is talking about adopting AI and automation. I think we have finally reached a point where AI has become sophisticated enough to be demonstrating some real value to the SOC analysts," she said. "At IBM, what we're using AI and automation for is to take the noise out of the system, to allow machines to do what machines do. We have taught the machine how an analyst would handle low-security risks."

Tech Mahindra is IBM's Platinum Business Partner, and this global partnership spans over two decades. We have dedicated centers of excellence across IBM products and co-invested labs. Our strategic initiatives on IBM Cloud, Watson IoT, Security and Blockchain has enabled us to deliver more innovation and value to customers. Our deep expertise in IBM technologies have made us preferred partners for many global organizations that employ IBM technology and solutions and have bagged us multiple awards. The synergy has resulted in several unique solutions and cutting-edge accelerators that have empowered our customers to comprehend quicker, act smarter and grow faster by unlocking data to actionable insights.

Source: https://www.techmahindra.com/en-in/alliance/ibm-partnership/

THE GROWTH PIPELINE COMPANY

For over six decades, Frost & Sullivan has provided actionable insights to corporations, governments and investors, resulting in a stream of innovative growth opportunities that allow them to maximize their economic potential, navigate emerging Mega Trends and shape a future based on sustainable growth.

Contact us: Start the discussion