Microsoft Security

Issue 1

CISO Insider

Welcome to the inaugural issue!

Explore

As attacks change, fundamentals still deliver valuable protection

The risk of doing business: Managing supply-chain threats

Innovative approaches to addressing the talent shortage

Letter from Rob

Welcome to the CISO Insider -- I'm Rob Lefferts, and I lead the Microsoft 365 Security Engineering team. At Microsoft Security, we're relentlessly focused on learning from our customers, particularly about the challenges they are facing and the choices they make about how to best run their businesses. As part of this pursuit, I speak with many CISOs about the latest security trends and issues impacting their companies, security teams and employees.

For the first time, we are releasing a public briefing in the form of the CISO Insider. We've heard from security leaders, especially as they face growing pressures, that they are looking for well-founded recommendations, grounded in peer experience and expert research.

Executive summary

Since the onset of COVID-19, security teams worldwide have adjusted, altered, and acclimated to the new realities of work, security, and life. Today, organizations are managing longer-term remote and hybrid work scenarios and continuing their migration to the cloud to support those work models—all while cyberattacks continue to increase. We all recognize this activity is on the rise—but some analysis points to a 17 percent increase year-over-year from Q1 of 2020 to Q1 of 2021.

Not surprisingly, the most pressing topics for security leaders right now are around preparing for major cyber breaches, defending their supply chain and managing the ongoing shortage of qualified security specialists. **Let’s dive in.**

Topics

Attack trends

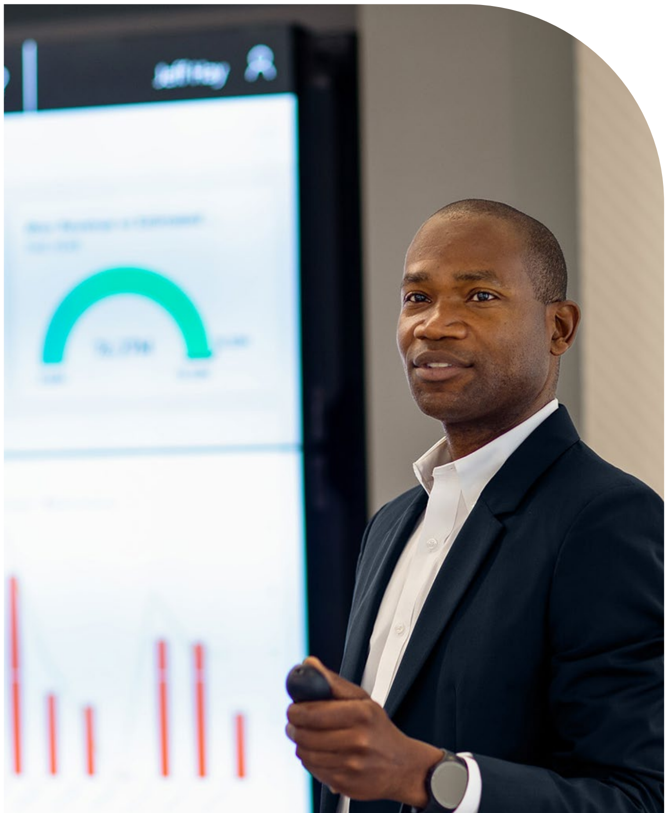
As attacks change, fundamentals still deliver valuable protection

COVID-19 has required organizations to increase reliance on workplace flexibility and accelerate digital transformation—and these changes have naturally required some changes in security tactics as well. The perimeter has expanded and is increasingly hybrid, spanning multiple clouds and platforms. Although new technologies have been a boon to many organizations, enabling productivity and growth even in challenging times, the shifts have also presented an opportunity to cybercriminals, who work to exploit the vulnerabilities found in increasingly complex digital environments.

The uptick in remote work–related phishing attacks is top of mind for the security professionals I talk with—and we see that reflected in our research as well. In a Microsoft survey of security leaders conducted in 2020, 55 percent told us that their organizations had detected an increase in phishing attacks since the beginning of the pandemic and 88 percent said that phishing attacks had affected their organizations. I also hear regularly about spiking ransomware attacks, how malware remains a consistent threat, and how identity compromise continues to be a major challenge that plagues security teams.

Added to that, we know that nation-state attacks are increasingly aggressive and persistent. The NOBELIUM supply-chain attack, leveraging the SolarWinds platform, was one of many novel attacks that have made headlines in the last year. While flashy new techniques are what often capture the news cycles, CISOs consistently tell me that even these advanced threat actors, like most cybercriminals, tend to focus on low-cost, high-value attacks of opportunity.

> *"If nation states are going to attack me and my company, that's a lightning strike event. It can happen, I worry about it, but not as much as I worry about my day-to-day activities, my foundational security."*
>
> – Financial services CISO



Attack trends

To further illustrate this point, we've seen an uptick in nation-state attackers utilizing password spray attacks. Being a security leader is about managing risk and prioritizing—and many leaders tell me that strengthening their cyber hygiene to prevent the most common lines of attack, especially across their growing digital footprint, is their top priority. And our data and research support this sentiment—we estimate that basic security hygiene still protects against 98 percent of attacks (see page 124 in the Microsoft Digital Defense Report, October 2021).

As attacks change, fundamentals still deliver valuable protection

Most security leaders I speak with agree on the fundamental steps for a security strategy:

- Implementing multifactor authentication (MFA) and a registration policy
- Gaining visibility into their environment
- User education
- Staying on top of patching and vulnerability management
- Managing and protecting all devices
- Securing configurations of on-premises and cloud resources and workloads
- Ensuring back-up in case of worst-case recovery scenarios

> *"In the end, most of the time, it's...a dumb password on a privileged account, or it's that somebody didn't implement a certificate on a required particular endpoint."*
>
> – Healthcare CISO

Attack trends

As attacks change, fundamentals still deliver valuable protection

You may be thinking that it's easy to talk about fundamental security steps, but much harder to implement them in real life, especially when a team is overworked and understaffed. But I would argue that being a security leader is about managing both risk *and* prioritization —and that makes focusing on fundamentals a solidly pragmatic approach. All too often, security incidents aren't a matter of **IF** but **WHEN**. There are hundreds of alarming cybersecurity stats such as:

About 4,000 cybercrime attacks are committed every day in the United States alone

More than 30,000 websites around the world are hacked daily

I believe the best line of defense is taking a balanced approach and investing in incident detection and response alongside prevention.

Although it may seem difficult to invest in new levels of prevention while still trying to keep up with increasing demands on detection and response, finding the right balance between the two efforts is both essential and beneficial. A 2021 Ponemon Institute and IBM Security study found that organizations without an incident response team or a plan in place saw the average cost of data breaches go up by 55 percent. Security teams who can balance solid prevention with a strategy that includes an incident response and investments in detection and remediation tools will be well-positioned to weather the inevitable.

The bottom line?

Take a balanced approach—get your fundamentals in place and have a plan for possible breaches.

- Investing in foundational cyber hygiene and extending it to the growing digital environment is a critical strategy to help protect your company from an attack in the first place.
- Even though these major attacks aren't an everyday occurrence, it's important to be prepared and be ready. While the basics are crucial, forward-thinking organizations have their sights set on a well-documented and tested plan for what to do after a breach.

Supply chain

And on to our next top-of-mind topic for CISOs these days: supply chains and the intrinsic threats they expose. Expanding the security perimeter outside of the security organization and IT as a result of an increasingly connected and complex supply chain is a reality of today's business environment. A September 2021 report from Sonatype found a 650 percent year-over-year increase in supply-chain attacks from 2020.

Yes, you read that right—650%!

And new business realities—like hybrid work and supply-chain disruptions of all types, hitting all industries—have extended security and identity boundaries even further.

The risk of doing business: Managing supply-chain threats

It's no wonder security leaders are paying more attention to supply-chain risks—any and all links in the supply chain are not only vital to the operations of a company, but disruptions anywhere in the chain can be harmful in a myriad of ways.

As security leaders expand outsourcing to suppliers for apps, infrastructure, and human capital, they're looking for more effective frameworks and tools to help assess and mitigate risk across tiers of suppliers. Because that 650 percent number is scary—**and we're all susceptible.**

1,013 average number of vendors in a company's supply chain

Source: BlueVoyant,"CISO Supply Chain," 2020

64% of businesses claim to outsource more than a quarter of their daily business tasks to suppliers that require access to their business data

Source: (ISC)2, "Securing the Partner Ecosystem," 2019

Supply chain

The risk of doing business: Managing supply-chain threats

CISOs tell me that while traditional vetting measures can be effective at reducing risk during the selection process or during reviews, their teams are grappling with the inherent shortcomings of point-in-time reviews, including:

- Supplier review processes often include only a questionnaire or a "checklist" that doesn't address all the risks inherent in today's supply chains
- Once a supplier is onboarded, there is only a point-in-time review cycle, often annual or during contract renewal
- Often, different departments within the same company have different processes and functions involved, and no clear way to share information across internal teams

> *"Key suppliers are those which we have a large-scale reliance or those which support us most in achieving our vision. Any disruption to the wellbeing in either type of supplier will have a significant detrimental impact on our org."*
>
> – Scientific research CIO

These measures mean organizations are simply unable to enforce compliance and mitigate risk in real time. As a result, it's much harder for security teams to respond to anomalous behavior, such as quarantining compromised external software or blocking leaked admin credentials from accessing their networks. If recent attacks have taught us anything, it's that even the best cybersecurity hygiene and dedication to the fundamentals to identify, measure, and mitigate risk can't entirely remove the possibility of threats sneaking into supply chains.

> *"We have annual check-ins with key vendors, and depending on the tiering of vendors, we may come back every two years, every three years and redo an assessment. But an assessment only provides you with point-in-time information. It doesn't validate the year-round controls environment."*
>
> – Microsoft Supply Chain Management Customer Advisory Board Member

Supply chain

So how can you manage your supply-chain risks while remaining agile and productive? It turns out that many security leaders are approaching supply-chain threats much the same as they do cyberattacks—focusing on strong fundamentals and improving visibility.

Because there are so many different types of risks associated with the supplier ecosystem, there is no clear standardization, "best practices," or even technology to manage them. However, many security leaders are leaning into a Zero Trust model as their approach to help reduce their risk exposure and protect against the vulnerabilities that are consistently behind supply-chain threats—like compromised credentials of third-party users, malware-infected devices, malicious code, and more.

Zero Trust is a proactive, integrated approach to security across all layers of the digital estate that explicitly and continuously verifies every transaction, asserts least privilege, and relies on intelligence, advanced detection, and real-time response to threats.

We've been consistently hearing from security leaders that they've been able to decrease the impact of major supply-chain attacks and improve the overall efficiency of supply-chain operations by implementing robust Zero Trust strategies. In fact, according to a recent study by the Ponemon Institute and IBM Security, organizations with mature Zero Trust deployments saw about a 40 percent lower average cost of a breach compared to those without Zero Trust deployed.

> *"Zero Trust enabled us to create a framework and build access modalities to protect all the critical assets in our organization."*
>
> – Healthcare security decision maker

Let’s take a look at how security leaders employ Zero Trust principles to protect their supply chains.

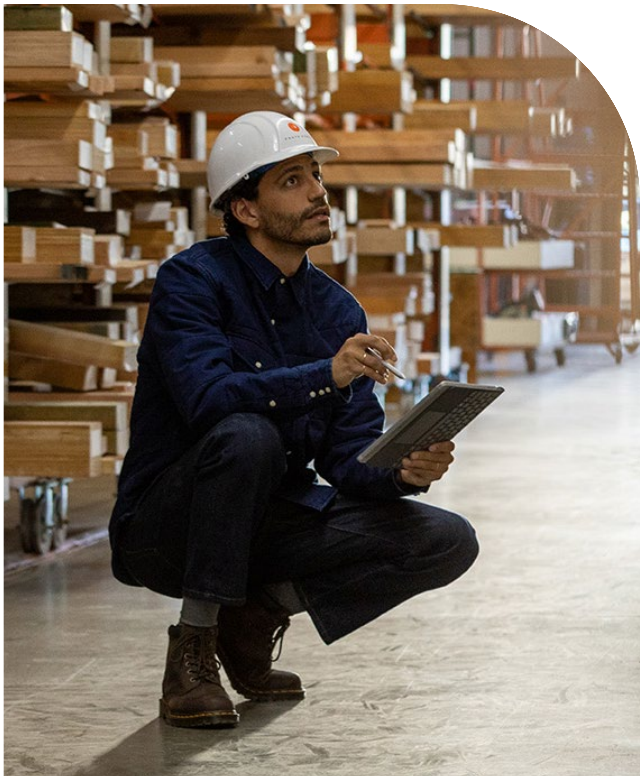
Verify explicitly

Verifying explicitly means we should examine all pertinent aspects of access requests instead of assuming trust based on a weak assurance like network location. In the case of supply chains, attackers typically exploit gaps in explicit verification—such as finding highly-privileged vendor accounts that aren’t protected with multifactor authentication or injecting malicious code in a trusted application. Security teams are strengthening their verification methods and extending security policy requirements to their third-party users.

Use least privileged access

Once you’ve achieved the first principle, least-privileged access helps ensure that permissions are only granted to meet specific business goals from the appropriate environment and on appropriate devices. This helps minimize opportunities for lateral movement by limiting how much any compromised resource (user, endpoint, app, or network) can access others in the environment. Security leaders tell us they are prioritizing providing vendors and third parties with only the access they need, when they need it, and continuously vetting and assessing access requests and policies within the organization’s supply chain to minimize contact with important systems and resources.

> *“I would say we’ve looked at our North Star and at least from a control perspective, it’s kind of leaning more towards Zero Trust. Instead of potentially asking all these questions, and then trying to deal with ‘how do I control everything for this specific scope,’ just go with the opposite and start with nothing, and only open up exactly what’s needed. So, I think that…Zero Trust is getting a new life in the industry.”*
>
> – Manufacturing consumer packaged goods CISO



Supply chain

Assume breach

While the first two principles help reduce the likelihood of a compromise, assume breach helps organizations prepare to quickly detect and respond to a breach by building processes and systems like it's already happened. In practice, this means using redundant security mechanisms, collecting system telemetry, using it to detect anomalies, and wherever possible, connecting that insight to automation that allows you to prevent, respond and remediate in near-real-time. CISOs tell me they're investing in robust monitoring systems that can help them detect changes in the environment—such as a compromised IoT device attempting to open unneeded connections to other devices—in order to quickly identify and contain an attack.

The risk of doing business: Managing supply-chain threats

Leaders I talk with about Zero Trust agree that it's a great framework for creating foundational cyber hygiene—and that includes supply chain management.

> *"The goal is to improve our security posture overall, but it's all about reducing friction in the end-user experience and making life easier for them."*
>
> **– Hospitality security decision maker**

The bottom line?

The vast number of vendors and array of challenges inherent in distributed supply chains make it even more important to manage proactively. With recent global data breaches, security leaders are eager to find ways to mitigate supplier risk and Zero Trust principles are providing a solid strategy and framework for managing the supplier ecosystem.

- A Zero Trust approach helps ensure that only the right people are getting the right level of access across your organization, while still elevating both security and end-user productivity.
- While there are many ways to get started with Zero Trust, instituting multifactor authentication should be the top priority from a supplier ecosystem and risk management standpoint.
- Assess the Zero Trust maturity stage of your organization and get targeted milestone guidance plus a curated list of resources and solutions to move forward in your Zero Trust journey.

Developing security talent

We've all heard about the great resignation. Over 40 percent of the global workforce is considering leaving their employer this year—and security leaders and their teams already feel under-staffed. I often speak with CISOs about how things are going overall, and affording, finding, and retaining top talent is one of their top concerns. And if top talent does leave, they are then faced with either finding new top talent or up-leveling the skills of those remaining. More efficient, integrated, and automated technology can help, but it's not nearly enough.

Innovative approaches to addressing the talent shortage

Security buzzwords have become part of the everyday vernacular as cyberattacks show up in the news regularly—and these attacks (and the news about them) can deeply impact a company. But guess what? That isn't all bad news. Given that cybersecurity has become a familiar topic across all areas of an organization, we are hearing that the concept of "security is everyone's job" is beginning to resonate across organizations. Especially with new hybrid work models and security perimeters being pushed in all kinds of new ways—security leaders are increasingly relying on innovative ways to keep everyone safe, even as they are facing talent and skill gaps. Not "doing more with less," but "doing more with different" is what innovative security leaders are all about these days.

> *"It's a challenge that everybody's facing, it's hard to find talent, it's hard to keep talent. There's a double-edged sword, when you develop talent, you make them too expensive to keep so there's definitely some challenges there."*
>
> – Legal services CISO

Developing security talent

Innovative approaches to addressing the talent shortage

While talent and skills shortages are definitely not a positive, there is a tiny ray of light here—creating a culture of security is becoming a reality. Many CISOs are telling us that one of the most effective ways to address their security challenges amidst staffing challenges is to build a culture of security where security is everyone's job. CISOs are increasingly advocating for this notion that the entire organization can take on the responsibility of security, especially as they are facing staffing shortages or funding challenges.

Development teams, system administrators, and yes, end-users, must understand the security policies that relate to them. Sharing information is fundamental and security teams are increasingly finding new ways to work with developers, administrators, and business process owners to understand risks and develop policies and procedures that benefit the entire organization.

Talent shortages and gaps in skills (especially in the ever-changing cybersecurity profession) have CISOs looking for new and innovative ways to stay ahead. One strategy we continue to hear about is an evolving "deputization" of employees outside of the security team. CISOs are looking to leverage the entire organization, with particular focus on training end-users to be part of the solution and building support from adjacent teams.

Boosting and enhancing end-user knowledge of security threats—like ensuring they understand phishing and the signs of subtle attacks—go a long way to increasing the eyes and ears of the security team, especially as a "tip of the spear" strategy, where end-users are often an entry point for an attack. I'm not saying end-users can magically be trained to catch everything but having prepared and alert users can dramatically reduce the load on security teams.

> *"You may have heard the phrase that 'security is everybody's responsibility.' When it comes to IT, what we've done is we deputized members of IT as representatives of security. We have appointed members of different teams, specifically development teams, architecture teams, infrastructure teams where they get extra security training. They get to sit down at some of my security meetings, and they get to be representative for their group in security as well as representatives of security back to their group."*
>
> – Legal services CISO

Developing security talent

Innovative approaches to addressing the talent shortage

"So, if you look at the world of security, the security personnel, they don't do a lot of the stopping of attacks, it's the IT people. Security people don't patch, for example. The people on the IT side of things (are who) patch. Security doesn't manage the asset management inventory, IT does that.

And there's a lot of things and depending on what org you're in, firewalls are usually managed by a networking team, not necessarily a security team. So a lot of what we're doing is we're helping the people that are tasked with actually doing the protective types of things, and we're upskilling them, we're giving them tools to automate some of the work that they're doing.

We're giving them the why, and not just the what, and sometimes understanding the why will influence and inspire to do the what."

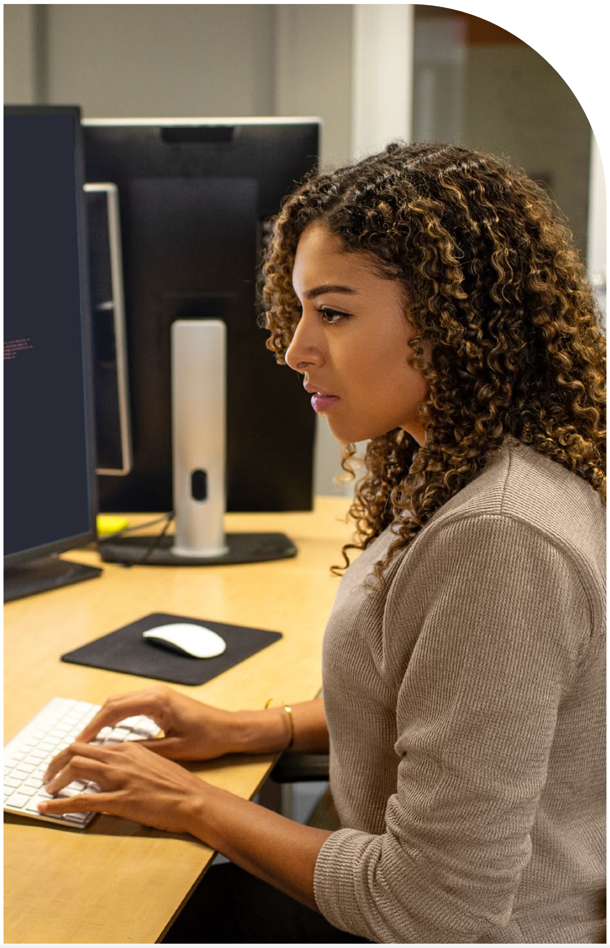
– Legal services CISO

Developing security talent

Innovative approaches to addressing the talent shortage

Another strategy is to deputize IT as part of security. Keeping the IT team closely connected to the security team and ensuring that IT is briefed on security strategies is helping many security leaders extend their mission to all areas of the organization.

Providing guidance and help on automation and other proactive workflow and task management strategies is a fundamental way CISOs are extending their teams and leveraging IT teams to help ensure solid security posture.



The bottom line?

Getting creative with resources isn't new. But developing a wider team through systematic training and engaging with teams adjacent to security is an innovative way that CISOs are easing some of the pain of talent shortages and gaps in key skills.

- Creating synergy with other teams and deputizing employees outside of the security team helps to expand the sphere of influence and keep the company safe.
- Training users to recognize phishing and commonplace security issues is a strategy that most security leaders agree is worth the time and effort.

Look to our next issue for more security analysis and insights.
Thanks for reading the CISO Insider!

Learn more

Explore the latest cybersecurity insights and updates at Microsoft Security Insider. www.microsoft.com/security-insider

All cited Microsoft research uses independent research firms to contact security professionals for both quantitative and qualitative studies, ensuring privacy protections and analytical rigor. Quotes and findings included in this document, unless specified otherwise, are a result of Microsoft research studies.