Achieving Better Cybersecurity Posture

A Shared Mission Among Security Vendors and Insurers

Eric Skinner
VP of Market Strategy &
Corporate Development

An Executive Interview with Eric Skinner of Trend Micro

Eric Skinner is is a vice president of market strategy and corporate development at Trend Micro—a global leader in cloud and enterprise cybersecurity. In his 10 years with the company, Skinner has developed a detailed understanding of and passion for global security concerns, especially as they relate to digital identity, data protection and cyberthreats. Skinner provides a unique focus on advanced threat detection, endpoint and mobile security, detection and response approaches, machine learning, and identity and authentication technologies.

Skinner recently sat down with Advisen, a Zywave company, to discuss the current cybersecurity landscape, common mistakes organizations make when preparing for threats, ways organizations can bolster their risk management practices and the role insurers play when assessing organizations' exposures.

What is your take on the current cyberthreat landscape for businesses? Is this the riskiest time for companies that we've seen?

ES: We are seeing an acceleration in attacker activity. That doesn't necessarily mean it's worse for any particular business, but it does require a level of readiness that perhaps wasn't needed a few years ago.

Attackers are getting more specialized. For example, cybercriminals focus on breaking through an organization's cybersecurity protocols, others specialize in exfiltrating data, and so on.

So, while the tactics aren't changing dramatically, the way in which attacks are executed is much faster than it used to be. In the past, an attacker would spend a few days or even a week poking around a victim's system. What we see now is cybercriminals who are focused on gaining access to a system—and do so in short order. They then hand off critical information regarding the victim to other specialists who continue the infiltration and attack. As a result, organizations have significantly less time to detect suspicious activity and respond accordingly.

This is particularly true for attractive targets who store sensitive data and systems that can be easily compromised. It's important to think about cybercriminal activity as a business. These threat actors are trying to maximize their revenue and will have different strategies for prioritization and triaging targets. Effectively, the more appealing a target you appear to be based on an attacker's initial access, the more likely you are to be compromised by an experienced and knowledgeable cybercriminal crew.

That being said, ransomware activity across various segments continues to impact businesses of all sizes. So, while a smaller organization may not have a lot of money and is less likely to be targeted by sophisticated cybercriminals, they can still fall victim to threat actors who cast a wide net looking to make a quick buck.

How do organizations typically get into trouble from a cybersecurity standpoint? What are the top mistakes you're seeing?

ES: There's a lot of commonality concerning how businesses become victims of cyberattacks, and it typically boils down to two fundamental things.

Firstly, from what we see in our incident response practice, about 50% of serious incidents arise from phishing. It's a tactic that works again and again. This is despite an increased focus by organizations to prioritize employee cybersecurity training. If an attacker wants to phish an organization, they will find a way—it's become a much more sophisticated and easier-to-implement strategy than it was even a few years ago.

Secondly, the other 50% of serious events we see in incident response occur when attackers exploit internet-facing assets that are either unknown to an organization or poorly managed. Perhaps an organizational team implemented a cloud workload that the cybersecurity team was unaware of, or maybe a contractor opened a remote desktop port on an internet-facing host—there are a myriad of internet-facing services attackers can exploit.

Sometimes, businesses are aware of their internet-facing services but aren't managing them properly. For instance, these services could be misconfigured, creating potential vulnerabilities. Additionally, if services aren't regularly patched, cybercriminals often have an easy entry point when infiltrating the system.

Beyond these two trends, businesses that fail to update or adequately monitor their security products are often the victim of an attack. Some of these issues may stem from businesses that put all their faith in a cybersecurity product and, once they roll it out, don't actively engage with their vendors or implement supplemental internal processes to bolster their cybersecurity protocols.

What can organizations do to manage their exposures better and improve their cybersecurity posture?

ES: One newer and emerging strategy to focus on is attack surface management (ASM). Put simply, ASM encompasses the discovery, assessment and mitigation process when analyzing an organization's IT infrastructure.

There are three stages to ASM. Firstly, organizations need to get broad visibility of what assets they've got. Essentially, they need to have an understanding of and visibility over potential exposures, whether that be devices, servers, laptops or internet-facing applications. You can't protect what you don't know about.

Secondly, organizations need to assess the risk across those assets, prioritizing and addressing existing vulnerabilities and configuration problems. It's important to note that no organization will have a 100% risk-free cyber environment. All businesses will have misconfigurations, unpatched software or unchecked system privileges. And because you're never going to be able to patch 25,000 vulnerabilities in one day or even a week, triaging the risks that are most likely to impact core aspects of the business is so important. But certainly, many of those vulnerabilities are more critical to address than others—for example, those that are internet-facing or actively exploited.

Thirdly, organizations will want to analyze their risk assessment and execute mitigation strategies based on how they've prioritized their vulnerabilities. Depending on the exposures, organizations may be able to automate some of the mitigation strategies.

Beyond ASM—and specific to the endpoint space that Trend Micro and many other vendors are involved in—there are substantial risks when products are not fully deployed (e.g., a discovery process was not completed appropriately) or kept up to date. In terms of the latter issue, if you're running a 3-year-old product, it doesn't matter what vendor you've got; you're going to be exposed to cyberattacks. Essentially, what was effective against ransomware back then with an endpoint product will not be effective today, so it's critical to stay current, both from a software and strategy standpoint.

What should insurers look for when assessing an organization's cybersecurity posture?

ES: Cybersecurity is and always has been a complex risk to navigate. In general, the approach we've seen insurers take when assessing an organization's cybersecurity posture relates to information gathering. Whether it's from questionnaires or live collection, insurers often rely on data science to determine the factors contributing to an organization's risk. It's not too dissimilar to the approach cybersecurity vendors such as Trend Micro take.

A trap that insurers tend to fall into, however, is they focus too heavily on an organization's vendors and the cybersecurity features they offer on a surface level. Obviously, partnering with a cybersecurity vendor can go a long way toward improving cybersecurity. But, the fact that a business has invested in these solutions doesn't tell insurers a lot when taken at face value.

As an example, insurers can ask an organization if they have endpoint detection and response (EDR) solutions in place. And while it's helpful to have EDR solutions, insurers have no idea if the organization is leveraging these solutions, actively monitoring EDR alerts or utilizing a managed service provider to stay on top of EDR-related processes.

Put another way, the mere presence of a control doesn't necessarily allude to a strong cybersecurity posture. Still, that doesn't mean these types of questions aren't necessary. For example, if an organization indicates they don't have multifactor authentication, that's a red flag. But, insurers need to go deeper in some cases, and focusing on how the organization is utilizing, monitoring or configuring their cybersecurity tools can be just as important as identifying whether these tools are in place.

From an insurer's standpoint, continuous monitoring as it relates to how security controls are deployed is crucial. In general, insurers should consider measuring an organization's response time to a potential threat. It's also vital for insurers to know how often security measures are updated and who monitors the system as a whole.

There's also more room for cybersecurity vendors and insurers to work more closely together, as they both have a common goal. Insurers don't want a claim, and the cybersecurity vendor doesn't want a breach, which presents more opportunities for cooperation between insurance vendors and security vendors.

How quickly does the cybersecurity landscape evolve? What does the future of cybersecurity look like?

ES: When it comes to preventing cyberattacks, the detection logic is constantly evolving. It's a cat-and-mouse game, and cybercriminals continue to find ways around defense strategies.

Often, cybersecurity vendors are playing catchup. For example, suppose a cybercriminal finds a new way to use a Windows system utility. In that case, it will take some time before a vendor has the behavioral logic to look for that particular activity.

We're certainly in a very active period where every cybersecurity vendor needs regular updates to their detection logic. While machine learning can help with this process, those models still require frequent updates.

So, essentially, all cybersecurity vendors are constantly improving the detection capabilities they have in their products—and organization want to stay current. However, this doesn't mean a full product update is required on a regular basis, especially in the case of software-as-a-service (SaaS)-based products that get updated automatically by the vendor or receive regular over-the-air updates. The organizations that end up in the most trouble are typically the ones running on-premises software and not updating it frequently.

Thankfully, as quickly as the attack strategies change, so do the protection methods. Organizations in the best position are the ones doing what they can with respect to detection. That includes leveraging managed services, as well as technologies such as EDR and extended detection and response (XDR) solutions. XDR extends the EDR approach beyond the endpoint to correlate threat activity across endpoints, emails, networks and other areas—and that's something Trend Micro has been investing in heavily.

And given the pace at which cybersecurity issues and protection strategies evolve, organizations need to prioritize what they learn. You get an avalanche of data when you execute a discovery of vulnerabilities, catalog your assets, examine threat activity in your environment and analyze user activity. At that point, you have to determine what your most serious problems are.

Notably, there's a ton of innovation right now around helping organizations better prioritize their findings. Essentially, cybersecurity vendors are working closely with organizations to determine and address their most significant risks. That kind of prioritization is tremendously valuable when it comes to reducing exposures. It all feeds into strong ASM practices, which we touched on earlier.

In terms of what's on the horizon, there's significant hype around the "zero-trust" approach. Zero trust is essentially a security framework mandating that—before granting or maintaining access to applications and data—all users (inside and outside an organization) must authenticate, authorize and undergo ongoing security configuration and validation.

Fundamentally, with zero trust, you're getting your business into a state where, by default, you say no when new connections or access requests come in. Then, you're making a dynamic, automated decision on a granular level about what to do with those requests. Should this access take place? Should this laptop be able to talk to this other part of the network? This approach has tremendous benefits with respect to slowing down attackers.

Overall, ASM and the zero-trust framework are two areas to pay attention to in the current market. •

About Trend Micro

Trend Micro, a global cybersecurity leader, helps make the world safe for exchanging digital information. Fueled by decades of security expertise, global threat research, and continuous innovation, our unified cybersecurity platform protects hundreds of thousands of organizations and millions of individuals across clouds, networks, devices, and endpoints

With 7,000 employees across 65 countries, and the world's most advanced global threat research and intelligence, Trend Micro enables organizations to simplify and secure their connected world.