Title Tag: Cybersecurity Unscripted Conversation | 2Secure Corp (52 chars)

Meta Description: Engage in a cybersecurity unscripted conversation tackling AI, security risks, and more with industry experts on this episode of The Cybersecurity Insider. (155 chars)

Kw: cybersecurity unscripted conversation

Cybersecurity Unscripted Conversation

The CybersecurityInsider - Yigal Behar
Steve Magnani
Seth Melendez
THE CYBERSECURITY INSIDER

In this unscripted The Cybersecurity Insider episode, Yigal is joined by guests Seth Melendez, owner of WareGeeks Solutions, and Steve Magnani, cybersecurity consultant at Altria for a candid dialogue about cybersecurity issues, AI, client compliance, and more.

The 800-pound Gorilla in the Room

Steve starts by talking about the 800-pound gorilla in the room, which is AI (artificial intelligence). “AI seems to be perched to be able to come in and do a great deal of many things that a lot of programs today require, you know, diligent knowledge and understanding to configure to make the right settings, and so forth.”

He believes AI will handle many manual network tasks. He cites CrowdStrike as an example. Crowdstrike already uses AI. He adds that companies not using AI could fall behind, especially if smaller companies find cheaper AI options.

Steve stresses that using AI well means giving it the right instructions to get the results you want. They think there will be more resources to help people learn how to give these instructions unless they're already IT experts.

Seth observes, “I think this stuff is overblown.” He compares it to past technological advancements like the web, which were also predicted to cause widespread job losses. He believes that the technology will eventually find its place and that people will be tempted to buy software with features they won't use, similar to how most people only use a fraction of Microsoft or Google software's capabilities.

Seth highlights the challenge of integrating AI into existing systems, particularly in cases where businesses are hesitant to change and still rely on outdated technology. “Most people won't even realize what is AI-driven and what isn't, and the bosses aren't knowing. You see, you've talked to these, some of these bosses, where they're like, 'Well, I don't want to, I don't want to change this or I don't want to change that,' and they're running on 10-year-old computers, and now all of a sudden they're going to put AI on that 10-year-old computer.”

He adds that while some people will be negatively affected by AI, others will approach it more tactically and “a little smarter”.

Steve suggests that instead of focusing on unused features, AI will bring the most relevant features to users. “I'm just thinking that instead of looking for all of those 80% of the features that they're not using, I think AI is just gonna bring it right to them.”

However, Seth points out that AI has been around for a while, gradually integrated into tools like spell checkers. The recent explosion of AI, particularly with the introduction of ChatGPT, has made it more accessible to the average person, similar to how AOL made email more accessible.

Debate on AI

Yigal disagrees that spell check was an early form of AI. He says that true AI capabilities were introduced to Microsoft products, particularly Microsoft 365, only within the past six months.

Although some AI-powered virus checks were present in Microsoft Defender earlier, the full integration of AI into various Microsoft applications has been more recent.

He also highlights the subtle signs of AI integration in desktop Office applications, noting the appearance of new software and features indicating the use of AI. He mentions SentinelOne's efforts to include more AI in their offerings.

The discussion then turns to the distinction between AI and machine learning (ML). While ML has been used in cybersecurity for some time, as seen in spam filters, the rise of ChatGPT has made AI more accessible to the general public.

Yigal points out that AI applications no longer require powerful PCs and can be accessed easily through web browsers.

Seth counters by emphasizing the numerous business applications that have integrated AI locally. He acknowledges that some companies prefer local AI solutions over cloud-based options, even if their hardware might not be fully optimized for it.

"What I'm saying [is] there are a ton of applications that are out there now that have AI integration in them that are locally based. If you look at, uh, there's software that's financial software, there's, um, database, there [are] different databases that are having them," he adds. "So what I'm saying is that there are people who want certain softwares [sic] out there, they don't want to get the cloud one, but then now they want to move to a local version, but they don't have the equipment yet so they're gonna have a bad experience."

Bridging the AI Gap

Yigal remarks that many companies are clueless about what to do with AI and have no idea how to implement it. He believes companies are not using AI as much as they should or could be. This observation sparked a conversation about how AI is being used in different industries.

Seth, for instance, shared that he uses AI in his writing software a couple of times a week, while Yigal uses it multiple times daily. This points to the varying degrees to which users and companies are adopting AI into their workflows.

The conversation then turns to the broader applications of AI. They discuss how AI is being used for virus and malware checks. They mention that many third-party software companies have integrated AI into their products. For instance, Microsoft and Google have integrated AI into many of their products. Nvidia recently released a new GPU chip called Blackwell, which is more advanced than previous versions (ref).

Yigal clarifies that he's using AI specifically for marketing purposes, not for network or software checks.

Seth again reiterates that a lot of the AI hype is overblown, with companies selling features that customers likely won't use. He claims that some companies are making poor decisions to implement AI in-house when it would be easier to use cloud-based solutions, but they don't have the right equipment.

Yigal offers his two cents on why companies might choose internal AI solutions: **privacy** and **proprietary concerns** as the main motivators. There's a fear that sensitive data could leak out if used on the cloud.

People don't need to Google anymore, they can just ask AI assistants like ChatGPT. ChatGPT is limited to 2022 data; however, Yigal prefers Google's Gemini (formerly Bard) because it's more up-to-date.

AI's Impact & Privacy Concerns

Seth repeats that marketing is overblown. People are worried about how much information AI collects and how it's used. Companies often oversell AI, making big promises without fully explaining the risks.

This led to a broader conversation about how companies use buzzwords, like "active persistent threat" (APT), to sell their products. But the heart of the matter lay in the probable impact of AI on technology, with the recent release of Microsoft's AI-powered Surface laptops serving as a prime example.

Privacy concerns quickly took center stage, as Seth voices his worries about the sheer amount of data AI could collect. He cites a chilling story about how Amazon seemingly knew about a woman's pregnancy before she had even told her mother.

“Privacy is pretty much going to go out of the window in general because it's going to be able to correlate different things. If you start searching for cars, you talk about cars. It's picking up your audio about cars now. It's going to present you a whole bunch of stuff on cars,” he asserts.

The conversation then shifts to the possibility of using AI as a defense mechanism against cyber threats. Steve argues that even giants like Google and Amazon haven't been able to protect users from their own data collection practices.

While Seth argues that users should have the right to demand privacy and AI could help enforce it, Steve is still skeptical of AI tools and their ability to protect user privacy by choosing not to use voice assistants like Alexa.

Yigal prefers the Google Nest for its physical button to disable audio recording, jokingly calling the red "off" light a placebo for privacy concerns.

Why Companies Don’t Do What They Need to Do

In this part of the discussion, Seth observes that the industry seems to be stuck in a cycle of repeated cyberattacks despite the availability of solutions. He questions whether the stagnation is due to a lack of training or care within the industry.

He mentions the issues that arose when less experienced technicians were promoted to networking roles during the Linux boom. He notes that hackers continue to use the same old tactics, exploiting unpatched vulnerabilities, and taking advantage of carelessness. Then, he asks if they see any change in this pattern.

Steve attributes the problem to a combination of factors, including **money** and **tolerance to change** in large organizations. He explains that large organizations often have to balance the risk of disruption against the need to apply patches. He also points out that bad actors are aware of these vulnerabilities and will exploit them over time. “Big organizations—they have to live with the risk. That's the problem. The bad guys know that they [the organizations] have it [the risk] on board, and they're [the bad guys] just going to look for it.”

Seth then shares an example of a company that has repeatedly experienced outages but refuses to change its outdated practices.

He airs his frustration that the company continues to rely on an internal network and resists cloud-based solutions. "It's like, are we in 2012? It's like these problems could be solved much more easily if you had, let's say, a [sic] cloud backup, offsite stuff, or anything like that that they could be using to help them mitigate some of these issues, but they're not doing any of those things. And they're not following—every time I speak to people over there or speak to people that know people over there—they're not following standard protocols."

Seth speculates that the company's older administration may be averse to spending money and embracing change. Yigal agrees and adds that a lack of education might also be a factor. He says that the company will likely claim to have learned from their mistakes when they're hit with another cyberattack.

IT Security Dilemma & Working With Clients

Yigal continues to share his experiences with IT security. There’s this one client who, after experiencing a cyber attack, gave the IT guy complete control to fix the issues but they don’t call him anymore.

He mentions another person who experienced identity theft and no longer trusts their IT company. Trust can be the reason “why they don't do anything is because they see that the IT company, the IT guy—you know, whoever he is—they don't do their job. They don't understand security.”

He then shares a specific example of a client's IT person who gave everyone admin access, potentially to avoid dealing with help requests. “I'll tell you a story with that specific client. They created... he created account email accounts, and he gave everybody admin role on Office 365. In addition, he made all the users on the computer admin.”

Seth questions Yigal about how he handles such situations, implying that he is more lenient than others. He asks if there is a point where Yigal would refuse to work with a client due to their lack of security practices.

Yigal clarifies that the IT person gave admin roles, not passwords, and this would make troubleshooting difficult as any issues could be blamed on the security team.

He explains his approach, which involves taking control and fixing issues without asking questions. He mentions another issue with the client: employees using Gmail for business purposes, which was then disallowed.

Steve jokingly asks if Yigal even allowed the client to print from their own devices at home.

The discussion then turns to whether there is a limit to where they would refuse to work with a client. Yigal says it depends on the situation and the client's willingness to change. He suggests using compensating controls as a way to improve security while allowing the client to function.

He also advises to think outside the box to find solutions. "Maybe I can find a different way to allow them to function without reducing security, but actually you're adding security, and it's better than the status now—a little bit better than it was before."

Balancing Security & Business Needs

Seth shifts the conversation to his role in security assessments of third-party vendors. He explains that his current focus is on reducing the number of findings from these assessments to avoid overloading the GRC (Governance, Risk, and Compliance) system.

There is a need for compensating controls and mitigating factors to drive down the risk level. He notes that even when a risk is categorized as "low" and automatically accepted, it doesn't mean the risk has disappeared.

Yigal says there is a need for flexibility when dealing with clients who may have budget constraints or require significant system changes.

He advises against forcing solutions on clients, as they might have established business processes that cannot be changed quickly.

He proceeds to use the example of asking a client for documentation of their systems and processes, which they might not have. Seth interrupts to ask about the threshold at which Yigal would walk away from a client.

Yigal states that he wouldn't walk away from his current clients, as he has been working with them for years and feels a sense of responsibility towards them. He emphasizes compassion and understanding the client's perspective while trying to find solutions.

When to Fire a Client

Faced with a different situation, Seth provides an example of a client his company worked with for years on various projects. He explains that despite user training and follow-up calls, the client would often make unauthorized changes to systems that caused issues.

Instead of addressing the root cause of the problems (lack of understanding of the training), the client would take shortcuts like giving users admin access. He mentions that the client would deviate from the agreed-upon protocols and documentation whenever there was an issue, opting for quick fixes that would create more problems later.

This led to a cycle where Seth’s team would fix problems, only to find more problems caused by the client's actions. The client became upset about the increased billing, not understanding that the extra work was a result of their own changes.

Seth eventually decided to terminate the client relationship stating that there's a point where he has to protect his company's reputation and walk away from such clients.

To ease Seth’s plight, Yigal advises that he give the client a document. This document will specify that “I'm removing [sic] myself from and responsibility for all these projects because you keep changing [sic] things. Sign off this document that you recognize the responsibility, and that you're going to acquire this responsibility from me. You, as a business owner—I don't know who you talked to, maybe the manager—said okay, sign this document. Uh, I'm not responsible anymore for what's going on because you are not following what we have agreed upon before.”

Yigal relates a similar experience where a client questioned the need for both email security and endpoint protection. The client felt that the combined cost was excessive. He explains the distinct roles of email security and endpoint protection noting that both are necessary for comprehensive security.

He disagrees with the client's assessment and firmly asserts the importance of both layers of protection. Finally, he stood his ground on the issue, despite wanting to end the relationship with the client for reasons he did not disclose.

A Different Perspective from the Security Assessment Side

Seth asks Steve if he has a limit when it comes to client compliance and whether he's diplomatic about it like Yigal.

Steve mentions that his role is different as he assesses specific findings in security assessments. He gives an example where a vendor might claim to have cryptographic key management but only provides evidence of using BitLocker.

He discusses that while BitLocker provides encryption, it doesn't fulfill the requirements of a cryptographic key management solution. He says that in such cases, the decision to accept the risk falls on the business and potentially the CISO (Chief information security officer).

Steve admits that his situation is different from dealing with retail customers, where the limit would be anything that could negatively impact his company's reputation. He would require the client to sign off on the decision that they are accepting the risk.

Stories From the Field

Seth then shares his past experience working for a pharmaceutical company where they were constantly pressured to bypass security protocols. He describes being asked to turn off the firewall to work on projects more easily, which he refused to do due to security concerns.

He expresses his firm stance on not compromising security, even if it meant being arrested, and reiterates his refusal to disable the firewall. His refusal attests to his commitment to security principles.

Steve also shares his experience working at Citigroup, where he spent a portion of his time dealing with information security. He recounts conversations about their development environment being internet-facing despite the numerous security rules for production environments.

Steve explains that the company couldn't afford to build a separate development environment that wasn't exposed to the Internet. So he suggests that they should have had two development environments: offline and online with a proxy for security.

He then rattles off his concerns about the vulnerabilities and risks this situation posed, which were being ignored. According to him, this is a common problem, as most application development environments need to be tested on the Internet, which exposes them to potential threats.

Still Developing on Production Environments Despite Virtualization

Yigal observes that many software development companies still develop directly in production environments that lack separate environments for development and testing. He explains the difference between production, testing, and development environments.

Production is hardened for public use, testing is similar to production but allows for application testing, and development is where developers can freely experiment.

Seth expresses surprise that this issue still persists despite the advent of virtualization, which could easily create separate development environments.

Steve also confirms that Citigroup did not use virtualization for their development environment.

At Johnson & Johnson, Seth shares that his team replicated the production environment in development, using virtualization to easily create and delete virtual machines. They used actual production data, which was common in the early stages of virtualization (2006). Over time, companies began to prioritize risk analysis and use dummy data instead. “Some didn't care about the production data, some did over time,” he says.

Windows Server Hiccups

As the podcast nears its end, Yigal attempts to wrap up the discussion but encounters technical difficulties while trying to showcase the new Windows Server 2022.

This leads to a brief chat about the upcoming 2023 demo and some confusion about future versions, with speculation of a potential 2025 release.

Yigal shows his screen displaying the Windows Server features, including Active Directory, data storage, Hyper-V, and AI before technical issues forced him to stop.

Steve recounts a story about a China-based company plagued with security issues. Their audit found 43 issues. The company submitted action plans and deadlines to fix most issues, except for one: they still operate on "end-of-life", unsupported servers and exchange servers.

Steve doubts the fixes will work on the old systems and suggests talking to management about getting new ones. Yigal finds this story relatable and sees it as a possible explanation for why companies fail to take necessary security precautions. "Maybe that actually gives the answer for the first question that was introduced: why companies don't do what they need to do."

Catch every episode of The Cybersecurity Insider podcast—available on YouTube, Apple Podcasts, and Spotify.