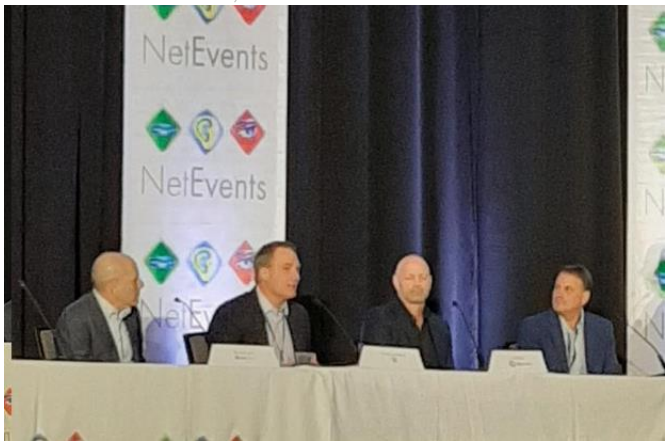
UPGRADE

http://www.upgrademag.com/web/2019/10/04/change-culture-to-deal-with-cybersecurity-threats-say-it-experts/
Change the culture to deal with cybersecurity threats, say IT experts
04/10/19

By Michael David Tan

Posted on October 4, 2019



COMMENTS

SAN JOSE, CALIFORNIA – Security is harder than everyone thinks, according to Vikram Phatak, founder of NSS Labs, here at NetEvents 2019: Global IT Summit. This is not surprising because the global cost of cybercrime reached $600 billion in 2018, and is expected to reach $3 trillion by 2020. Current top targets for cybercriminals include government agencies, healthcare industry, and financial industry – where, according to Phatak, "there's money."

Thomas Edwards from the US Department of Homeland Security noted that "cybercrimes are driven by profit." Cybercriminals, for instance, are after personal identification, and then turn this into profit; or are after credential theft, but then again eye to monetize this (credential).

Surprisingly, cybersecurity spending is pegged at only $124 billion in 2019, and only growing to $188.4 billion by 2023.

Phatak noted that there continues to be various issues affecting how companies respond to cyberthreats. There is skills shortage, for instance, with "not enough trained cybersecurity experts", and labor-intensive solutions requiring these experts. Also, "new attack vectors (force) us to compromise ourselves (since) situational awareness is lacking." And then "we have to consider where we're headed – e.g. cloud, IoT, 5G, and what happens when attacks jump from the virtual world to the physical world?"

But exactly because of the layers of issues that coalesce when tackling the cybersecurity landscape that IT experts say cultural change needs to happen to effectively deal with cyberthreats.

ZERO-TRUST CULTURE

According to Michael Levin, CEO and founder of Center for Information Security Awareness, "We're not training our people about cybersecurity until there's a problem." For him, therefore, "how do we create a culture (that is aware of cyberthreats)?"

This is because for him, "when you think of cybercrimes, you also need to think of social engineering." This means that the crime can be done in many ways – e.g. it could be over the phone, over social media, or over emails. "There are so many ways (for cybercrimes to be done), so that you have to come up with mechanisms for employees to be always on the lookout. We need to come up with simple mechanisms to deal with these crimes."

Threats could come from various sources, but Levin said that it doesn't matter where these come from. In the end, "you still have to train your people (how to deal with the threats)."

Ted Ross, CEO and co-founder of SpyCloud, recommends the establishment of a "zero-trust culture".

"People underestimate cybercriminals' ability to innovate," he said, noting that cybercrimes have long been associated with emails. But "fairly sophisticated criminals can access data" so there is a need to teach employees to "treat everyone as an adversary."

OPEN-DOOR POLICIES

Some of the cyberthreats are actually easy to discern if employees “take it slow.”

Levin, for one, said that people need to heed the “sense of urgency” of an act (e.g. an email). “This forces people to think quickly, and this results in fraud. For instance, we click links and attachments (when we think they’re urgent).,” he said. “Now how do you get people to think, and to slow down.”

For Levin, there is a need to create policies and procedures for this.

Edwards added that “employees need to know that it’s okay to commit mistakes (by having an) open culture.” This way, employees are “transparent with their cyber hygiene.” With the transparency, they are therefore empowered; which will prove beneficial to the company in the long run.

REALISTIC ASSESSMENT OF CAPABILITIES

Paul Kraus, VP for engineering of NetScout Systems Inc., said that companies need to know what they have (their assets). “(It starts with) gathering of inventory of what you have. How valuable is the asset? Secondly, can you monitor? Does the security team even understand what’s out there?”

Edwards from the US Department of Homeland Security similarly noted that without sharing of information between the private and public sectors about cyberthreats, “we’d lose the battle eventually; so information sharing is important.”

Nowadays, “security is like a gym membership,” Phatak said. “You join, but do you really use it?” And in the end, to really deal with cyberthreats, “you need to use this membership.”