Cybersecurity: Form a Foundation of Trust

Acquiring and storing private information, and operating systems, are not just processes – they also are commitments. An industry expert offers his insight on maintaining and protecting their security.

Publish Date:

February 10, 2025

By:

John Iekel

Acquiring and storing private information, and operating systems, are not just processes – they also are commitments. And maintaining and protecting their security is key.

A foundation of trust between a service provider and employees and clients is essential when sensitive information and processes are part of the relationship. That was the message of Joshua Cook, an attorney who specializes in cybersecurity-related matters who is of counsel at the Wagner Law Group. In a Feb. 5 webinar, he offered his insights on establishing and maintaining that trust through steps to ensure cybersecurity.

Indeed, cybercrime is a widespread concern, Cook suggested, observing that in 2024, almost 900,000 cybercrime complaints were filed with the FBI. “The threat is ubiquitous – everyone is under threat,” warned Cook.

Consequences of Cyber Attacks

Cook spelled out in stark terms what is at stake in cyberattacks.

“Cybersecurity and privacy are cost centers,” said Cook. That’s not just because the steps by which one can protect a business from cyberattack involve expenditures; the crimes themselves can exact a heavy financial cost.

Further, the threat cyberattacks pose is more than financial – it can be existential. Cook noted that 60% of small businesses are out of business within six months of one.

What Imperils Cybersecurity?

Cook identified a variety of threats to cybersecurity:

- business email
- impersonation of people who are in the c-suite
- re-use of credentials
- vendors
- phishing and related actions, including smishing, vishing, and spearfishing

- ransomware
- offshore remote workers

Business email is fraught with peril, Cook suggested, remarking that it's "shockingly easy" for email to be compromised. Also, almost 70% of U.S. organizations are victims of ransomware attacks, he said, remarking, "that number is startling to me." Further, 74% of those attacks were aimed at small and medium-sized businesses in the first quarter of 2024.

Action Steps

"Cybersecurity is not something you should have to worry about in order to stay in business," said Cook, adding, "Being ready is the difference maker."

Cook argued that "putting a plan in place is far cheaper" than what a business will have to do to deal with a cyberattack that happens. He outlined some proactive steps to obviate such worries and attacks.

First of all, it is important to understand what data an organization has, Cook said. Then it can start thinking about the threat landscape, and try to figure out what the risks to the organization are.

Cook stressed the importance of having an incident response plan (IRP). But it's not enough to simply draft an IRP, Cook said – one also must work with the people who will help in implementing the response to a cyberattack. And he added that an organization should practice the IRP so all players know what to do if a cyberattack happens.

Even small steps to establish and maintain cybersecurity are worthwhile, Cook suggested, remarking that "small things can have an outsized effect on readiness."

"Get ready. It is going to happen to you," Cook warned.

But Be Careful

In taking steps to establish and maintain cybersecurity an organization should be careful, Cook cautioned. For instance, he said, some firms are too quick to outsource the effort.

Cook also cautioned against overreliance on cyber insurance. One reason he cited is that such insurance sometimes doesn't cover what organizations think it does.

But the biggest reason Cook posited for not relying too heavily on cyber insurance is that it doesn't prevent an attack. Cyber insurance is "after the fact" and "is not helpful in mitigating an issue right out of the gate," he said.

The Bottom Line

"Achieving resilience and bouncing back is what it's all about" in preparing for and preventing cybercrime, Cook said.

Comments

Please log in or create a free account to comment on this article.

Log In or Create Account

Contact Us

4401 Fairfax Drive
Suite 600
Arlington, VA 22203

703-516-9300

703-516-9308

customercare@asppa-net.org

Resources

Discover ASPPA

News

Education

Events

Webcasts