Synoptek

May, 2019

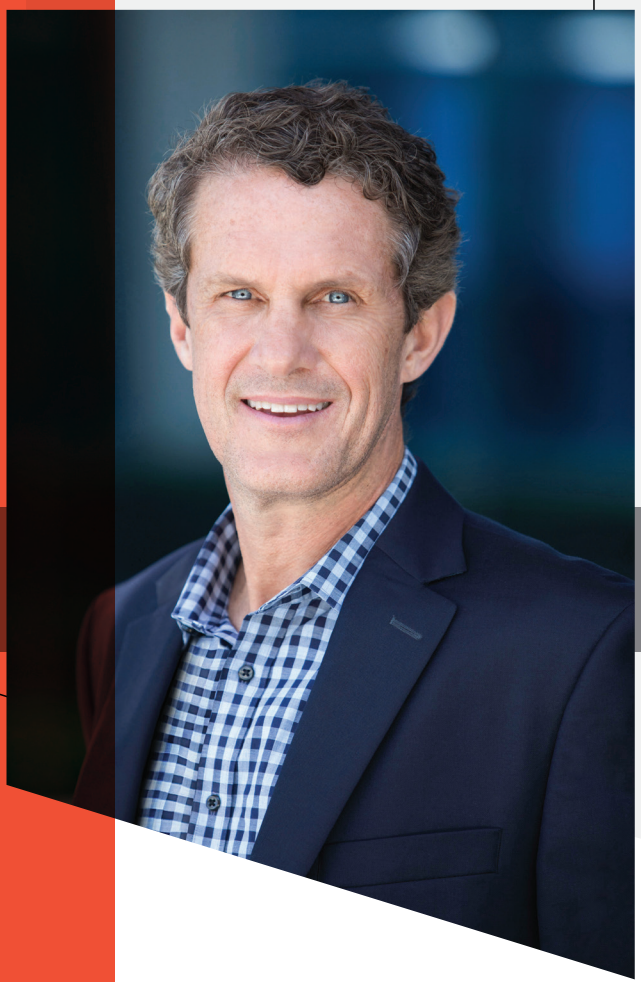
Cyber Security: Companies Need to Hop On Board and Invest

Business risks: compliance, cyber security threats

Nothing changes faster than the cybersecurity landscape. Just as businesses divert one security threat, several more take its place and test cyber protections at every turn.

And it shows no signs of slowing down. The cyber underworld continues to evolve and consolidate and there's greater coordination among cybercriminals using the underground market. This has allowed them to become more effective.

IT leaders know they need to ramp up their cyber security and several reasons are pushing this mindset — from numerous headline-worthy data breaches, ransomware strikes and malware attacks to strict government regulations. As efforts heighten to improve security — cost is another factor — which can soar into the millions. So even if change is needed, it's not happening everywhere because cyber-security can get expensive quickly. Many companies are still under threat, ill-equipped and vulnerable.



Let's look at what's happening out there:

01 The attack surface is gargantuan

Organizations are still modifying their efforts to improve cybersecurity practices — a constantly moving target that seems to demand more every year. IT leaders used to have just a perimeter problem and companies simply needed the ability to hold down that perimeter. Now the playing field has widened — from employee devices and remote workers to access by third-party vendors and contractors.

02 Targeted attacks

Aimed at a precise target, this type of attack is organized and continuous and is achieved by combining "phishing email" with "malware," like viruses and worms. Emails are sent under the guise of normal business communications either from known or related people and organizations to the target, and then infection spreads with malware when the recipient opens the file.

03 The attacks are becoming increasingly complicated and the attackers are more focused and better funded

The criminal's aim is to make money and create disruption — from cyber terrorism aimed at governments to organized cybercrime attempting to take funds from financial institutions and corporations. What's more, digital warfare is becoming an important tool of government control. In 2016, NATO expanded its definition of "war domains" beyond air, land and sea to include cyberspace and its members are now co-operating here in the U.S. Still, cyber protection in private business has been slow to evolve, with many organizations simply resigned to the fact that their infrastructure will be breached and instead, focus on minimizing the ensuing damage.

04 **Business leaders recognize that modern-day threats are not only expensive but also debilitating**

A cyberattack significantly damages consumer and employee trust, hurts a company's market share, eats away at profits and returns, and stops operations. Companies need to improve cybersecurity, compliance and risk mitigation — they know these threats can kill their businesses.

05 **The Government is throwing around their weight**

With the General Data Protection Regulation, regulations are pushing companies to improve cybersecurity, compliance and data privacy practices. These laws are demanding that companies invest in certain cyber priorities which means increased spending, hiring and investment in cybersecurity-related technology projects. Not surprisingly, security and security-related topics are at the forefront of the boardroom and the C-suite.

06 **There's a challenge finding highly trained people to protect companies from threats**

The tight IT labor market has many CIO's admitting a lack of talent is holding their organizations back from keeping pace with technological change.

What's being done?

Ultimately, there are two main elements needed to maintain operational readiness against a cyber security threat:

Visibility

Being able to find, identify and see "into" all of the endpoints (devices) on your corporate network in real-time

Control

Assessing the situation and have the staff, skills, and tools to react and respond

One overarching trend is that organizations — particularly those with more mature cybersecurity operations — are investing heavily in next-generation cybersecurity technologies that use artificial intelligence and automation to analyze security-related data points and pinpoint the activities that are the most threatening. On the flip side, cybercriminals see the opportunity in the technology as well, particularly when it comes to evasion techniques, which enable the criminals to avoid detection and circumvent security.

> "IT leaders know they need to ramp up their cyber security."

Enter AI-based and other next-generation cybersecurity tools, which are taking advantage of emerging technology to detect and ward off increasingly sophisticated threats. To improve security capabilities, tools that use artificial intelligence to monitor device and user behavior and flag anything suspicious will be arriving on the forefront in the next few years, if not sooner.

> Companies want the assurance someone is 100% focused on having their back.

> As another way to combat the attacks, more organizations are coordinating between different business areas, consolidating cybersecurity, data privacy and risk/compliance activities into information lifecycle management, with the hopes doing this will deliver the best results throughout the business.

They're also looking for outside resources and expertise. In an area that changes at the blink of an eye, companies want the assurance someone is 100% focused on having their back. Partnering with a company that specializes in cyber security, the end goal is always quick remediation and should include not only a dedicated security staff, security training the latest cyber-security analysis and defense tools but also constant assessing and current awareness of trends and emerging threats.

52% featured hacking

43% involved small business victims

32% involved phishing

56% took months or longer to discover

29% involved use of stolen credentials

69% were perpetrated by outsiders

Source: Data Breach Investigations Report, Verizon, 2019

All told, consumer data is a digital gold mine. So, if you suffer a loss, your customers not only want to know what you'll do going forward, but what safeguards you already have in place. Data can always be recovered — trust can't. When you put all the necessary steps in place to strengthen your cyber security, you'll help protect your customers valuable information and, ultimately, your brand.

About the Author

Tim Britt, CEO

Tim Britt is founder and CEO of Synoptek, a Global Systems Integrator (SI) and Managed IT Services Provider (MSP) offering Comprehensive IT Management and Consultancy Services to organizations worldwide. An entrepreneur at heart — Tim leverages technology to squash the status quo and create solutions for his clients — a mission he's been on for more than 20 years.

About Synoptek

Synoptek is a global systems integrator and managed IT services provider offering comprehensive IT management and consultancy services to organizations worldwide. Founded in 2001; headquartered in Irvine, CA, we have offices and resources across North America and delivery centers in Europe and India.

Learn more at www.synoptek.com