


5 CRITICAL QUESTIONS YOU NEED TO ANSWER CONCERNING YOUR CYBERSECURITY STRATEGY

 **51%** of IT decision makers indicated 'security and compliance concerns' as a top driver for digital transformation.¹

It seems every month that goes by is yet another confirmation of what a scary place the world is from a cybersecurity point of view. In just the course of a few weeks prior to creating this document we've witnessed a major oil pipeline being shut down as well as the ransomware attack on the police department of our Nation's capital. It seems that there's nothing too brazen for cybercriminals to pull off today, and there is little ability to stop them.

But that's enough scary talk. The purpose of this technical brief isn't to scare you any further, it's to inform you. Yes, the digital world can be a forbidding place. That's why it's time to be proactive. A famous American general once told his staff out of utter frustration, "I'm tired of hearing what the other army is going to do, I want to hear about what we're going to do." So what are you doing to protect against the omnipresent cyberthreats of today? Below we have provided 5 questions that every IT leader needs to be asking themselves in order to evaluate whether they are on the right course, and what the correct course should be.

1. ARE YOU SPENDING TOO LITTLE OR TOO MUCH ON CYBERSECURITY?

According to a news article in 2018, cybersecurity spending is to exceed \$1 trillion over a five-year period ending in 2021.² That constitutes a growth rate of 12% to 15% a year. However, the same news site also predicts that the cost of cybercrime around the world will rise to \$6 trillion over that same period. Obviously, there seems to be a disconnect.³

We are spending more money to protect against threats that are in turn costing an increasing amount of money. You don't have to be a financial advisor or CFO to know that the ROI on that \$1 trillion isn't very good. A Deloitte 2019 study showed that financial institutions spend an average of 10 percent of their IT budget on cybersecurity,⁴ while a 2019 State of the CIO Survey showed a mean of 15 percent.⁵ While there is no hard answer to how much a company should spend on cybersecurity, companies should be getting some type of return on their investment like any other IT acquisition.



It seems that there's nothing too brazen for cybercriminals to pull off today, and there is little ability to stop them.

2. ARE YOU FOCUSING YOUR CYBERSECURITY SPENDING ON THE WRONG THREATS?

A 2017 survey involving some 1,100 cybersecurity executives showed a blaring disconnect between the security solutions their organizations spent money on and



the solutions they actually needed to address their most pertinent threats.⁶ While 30 percent of the respondents classified their organizations as “very or extremely vulnerable to data attacks, 62 percent listed network security as their top spending priority while 56 percent cited an endpoint solution. As it turns out, data-at-rest security solutions ranked last. One possible explanation for this quandary is that companies continue to purchase what they are comfortable with or what has worked in the past. The problem is that threats are continually evolving, therefore your required solution sets must evolve as well. Another contributing factor is that too many organizations implement security measures without first assessing what their digital estate truly compasses.

3. ARE YOU STUCK IN THE “BEST OF BREED” ARMS RACE?

Anyone involved in purchasing IT solutions is familiar with the term “best of breed.” A best of breed solution denotes a designation of the best option available. A solution with the true answer to your problem. In theory, best of breed sounds wonderful. Who doesn’t want to purchase the best in its class? At WEI, we stand behind solutions that we can attest are best of breed.

The problem is that cybersecurity is a little bit different than other facets of IT. That’s because there’s a seemingly endless stream of newly discovered attack methodology or uncovered vulnerability. Vendors then address each new threat with a new “best of breed” solution. This ambulance chaser mentality creates a flood of security programs offered by a multitude of vendors that IT teams must then grapple with and make work in their environment. The fact is—you cannot afford to address every new problem with a new solution regardless of its stature of excellence. Best of breed purchasing is a process for the weary. According to a 2020 study, 40 percent of security professionals say that purchasing from a multitude of security vendors adds cost and purchasing complexity to their organization.⁷ In fact the 2020 CISO Benchmark Survey underscored a direct correlation between the number of security vendors a company had with the amount of downtime they

experienced as a result of a security incident.⁷ More vendors equated to more downtime and compromised data records. Complexity is a hacker’s ally.

4. ARE YOUR CYBERSECURITY SILOS INCREASING YOUR VULNERABILITY?

As an enterprise manager, you’ve heard it many times. You need to break down the IT silos in your enterprise. We often associate silos with management systems or data storage solutions in which individual components or pools of data operate in disparate fashion with one another. Each security tool logs data that is then analyzed in isolation, inhibiting the ability to see the big picture or detect more subtle and hidden attacks. While companies have made great headway over the years in breaking down these silos, the average cybersecurity estate remains plagued with them. Rather than working in unified collaboration, these tools work independently of another. This forces IT professionals to perpetually bounce back and forth between tools, creating both visibility and attention gaps. It also creates a deluge of unfiltered alerts. According to the 2020 CISO Benchmark Study, 44 percent of organizations see more than 10,000 daily alerts, of which only half are addressed.⁸ The same study showed that 82 percent of CISOs acknowledged that orchestrating alerts from multiple vendor products was challenging.

5. DO YOU KNOW THE ADVANTAGES OF A SECURITY PLATFORM?

There is no doubt that cybersecurity is a problem and it is growingly obvious that we can’t spend our way out of it. We also can’t hire our way out of it either. According to MIT, fewer than one in four cybersecurity applicants are even qualified to apply.⁹ In fact 74 percent of cybersecurity professional report that the cybersecurity talent shortage has impacted their organization.¹⁰

What companies need today is a security platform that enables a more holistic and collaborative approach to combat threats. While many are familiar with the concept of solution based platforms such as an endpoint protection platform or the platform of tools conglomerated in a next



generation firewall appliance, portfolio-based platforms allow you to integrate the products you already use now with the products you may want to use in the future. They also integrate with other third-party products either out of the box or through APIs at a depth that SIEMs and SOARs fall short. These agnostic security platforms such as Cisco SecureX can unify visibility across all parts of your infrastructure through a combined console that vastly increases operational efficiency. These platforms provide actionable automation when it comes to workflows in order to better hunt and remediate threats. Cisco's security platform enables better decision making through comprehensive threat detection, powerful analytics and security policy management. In addition to its security offerings, a modernized security platform provides value through greater efficiency and ROI metrics that can greatly accelerate time to value.

Yes, it's a whole new approach to security and a whole new way of doing things. It's one that you cannot afford not to learn more about. Let our security platform experts at WEI educate you on this this new methodology that is proving as cost effective as it is in protecting the vast hybrid network architectures of today.



TALK TO WEI TODAY

Questions about enterprise security? Contact the security engineering team at WEI today!

Sources:

1. IDG Research commissioned by WEI, January 2021.
2. Cybersecurity Ventures projects \$1 trillion will be spent globally on cybersecurity from 2017 to 2021. (Cyber Defense Magazine)
3. Cybercrime cost to double due to Coronavirus; uptick in attacks predicted (eccouncil.org)
4. Financial services firms spend 6% to 14% of IT budget on cybersecurity – survey (pionline.com)
5. How much should you spend on security? (CSO Online)
6. Are businesses spending their money on the wrong IT security? (Help Net Security)
7. ESG Research Insights Paper: Toward Enterprise-class Cybersecurity Vendors and Integrated Product Platforms
8. 2020 CISO Benchmark Study (Cisco)
9. A cyber-skills shortage means students are being recruited to fight off hackers (MIT Technology Review)
10. The cybersecurity skills shortage is getting worse (CSO Online)

ABOUT WEI



WEI is an innovative, full service, customer centric IT solutions provider.

Why WEI? Because we care. Because we go further.


At WEI, we're passionate about solving your technology problems and helping you drive your desired business outcomes. We believe in challenging the status quo and thinking differently. There are a lot of companies that can take today's technology and create a great IT solution for you. But we do more. We go further. And we have the customer, vendor and industry awards to prove it. WEI is a premier technology partner, who always puts our customers first while providing the most innovative solutions for over 30 years.



 info@wei.com

 www.wei.com

 43 Northwestern Drive | Salem, NH 03079

 800.296.7837