www.pipelinepub.com
Volume 18, Issue 1

Technology Can't Save You from Cyberattacks

By: Kirsten Bay, Corey White

The cybersecurity industry was founded to prevent people and organizations from being breached, yet hacks have grown more visible and virulent over the last three decades.

Put simply, the security industry has failed to keep pace with the adaptability of today's cyber criminals, leaving buyers in the unenviable position of continually scrambling for the latest security tools in an attempt to keep confidential information safe. They spend more money and they buy more security tools without knowing if they're spending in the right places or on the right things. It's the foundation of a vicious cycle resulting from the failure to prevent attacks in the first place, which is the primary job of cybersecurity.

Consider the Equifax breach, where more than 148 million consumer records were exposed. Human error and a reckless approach to security were at the root of this notorious hack, according to former CEO Richard Smith. Poor data hygiene, permissive access controls, and an open network architecture gave hackers all the help they needed to pilfer the crown jewels of U.S. consumer data. This entirely preventable breach was caused by the failure of Equifax's IT team to implement a critical patch and exacerbated by internal security systems that failed to flag the suspicious traffic that followed. Worse, six of the 11 remedial recommendations given to Equifax by a top consulting firm included increased security and technology investments, despite the failure of many similar tools to prevent, detect, or contain the original breach.

As long as security providers continue to make money off their own failures, it will always be in the industry's best interest to sell using fear tactics. But this doesn't mean buyers have to play along. Organizations can evolve from approaches favored by the industry to new methods that

© Pipeline Publishing, L.L.C. All Rights Reserved.

Not for reproduction or distribution. © Pipeline Publishing, L.L.C. All Rights Reserved.

serve buyer needs first. To succeed, organizations must know what to protect, how best to protect it, and how to keep it protected over time.

Embracing the basics

Whatever the industry's shortcomings, we all have a hand in why security solutions fail. Whether our focus is on decreasing overall risk, reducing technology complexity, supporting faster sales cycles, speeding time to market, achieving better compliance, improving customer retention, or just doing a better job preventing data breaches, we must understand our own environments. There are three basic steps that form the foundation of a winning strategy.

Secure your assets

What assets do you have? Servers? Cloud infrastructure? Laptops? BYODs? If you're not sure, make a list. Seventy-nine percent of organizations surveyed by Enterprise Strategy Group (ESG) report widening visibility gaps in their cloud infrastructure, while 75 percent found the same problem across end-user and IoT devices. Do you know what software is running on all those assets? You can't really proceed to the next two steps until you have this one covered.

Secure your endpoints

Is your endpoint security focused on preventing attacks or detecting and responding to them? Most endpoint security providers will tell you they do both, so dig into your solutions to determine if they're better at one or the other. And remember: MDR and XDR might sound good—they certainly enjoy a lot of hype—but they won't prevent an attack. The more you spend on prevention, the lower your total costs will be.

Secure your environment—*continuously*

What's your current process for keeping software up to date? Who's responsible for installing updates? For vulnerability scans? For remediating problems once discovered? With an average of 50 common vulnerabilities and exposures (CVEs) discovered every day and software updates and releases happening regularly, it's impossible for once-a-quarter (or once-a-year) scans to reflect accurately the threats and vulnerabilities in each environment. Even once a day won't get it done, because you'll miss an average of 49 others every 24 hours.

Compliance is not a security strategy

Mastering the basics boosts resilience across the board, so any organization that thinks meeting compliance standards gets them off the hook for embracing security basics should think again.

Security often gets bumped in favor of the capabilities customers want, particularly in high-growth sectors like technology and in compliance-driven industries like financial services and

© Pipeline Publishing, L.L.C. All Rights Reserved.

Not for reproduction or distribution. © Pipeline Publishing, L.L.C. All Rights Reserved.

healthcare. But when companies get into the habit of thinking compliance provides security, they lose their cyber resilience. From basic IT hygiene (such as patching vulnerabilities or comprehensive asset management) to user education(including better email protections or password habits), we know from the post mortem of every successful breach that human error almost always plays a role, and compliance standards can't eliminate people. In other words, compliance alone won't protect against attack.

Market aggregators like managed security services providers (MSSPs) or value-added resellers (VARs) aren't a strategy either. They may help sift through the deluge of security products, implement solutions, or assess existing cyber investments, but they can be costly relative to results, and all too often the heavy lifting falls on the buyer.

Never forget that, pre- or post-breach, all of the solutions we buy must be managed and maintained continuously. Defined resources—whether in-house or outsourced—need to be explicitly responsible for making sure that happens.

The path to cyber resilience

Successful security programs build on the basics using the three pillars of people, process, and technology. Organizations that look no further than technology will find they've invested in only one-third of a complete solution; without adding skilled resources and proven security protocols, even the best technology will leave them vulnerable to attack.

Unfortunately, the cost and complexity associated with cyber risk makes it hard for organizations to make the three pillars work in concert, but the newly emerging cybersecurity-as-a-service (CSaaS) trend marries them seamlessly—and affordably. CSaaS takes the guesswork, high costs, and high levels of difficulty out of the equation by using a holistic approach, proven technologies, and successful, repeatable best practices designed to scale.

Traditional providers mark up the technologies they sell and charge additional fees to install new software or remediate in the event of a breach, obscuring the total cost of any given solution. CSaaS bundles comprehensive offerings into all-in-one monthly subscriptions based on the buyer's needs, so pricing is consistent and predictable month over month, even should an incident occur.

Importantly, CSaaS makes formerly expensive solutions accessible and affordable for even the smallest organization, which traditional product companies cannot do. The subscription model allows CSaaS providers to deliver the same robust security enjoyed by large enterprises at price points friendly to startups and SMBs so they too can effectively combat rising threats. The ICARM method (for installation, configuration, assessment, remediation, and maintenance) enables them to realize quantifiable returns on their cyber investments. Figure 1 shows how it works, with the steps of the ICARM methodology explained.

© Pipeline Publishing, L.L.C. All Rights Reserved.

Not for reproduction or distribution. © Pipeline Publishing, L.L.C. All Rights Reserved.

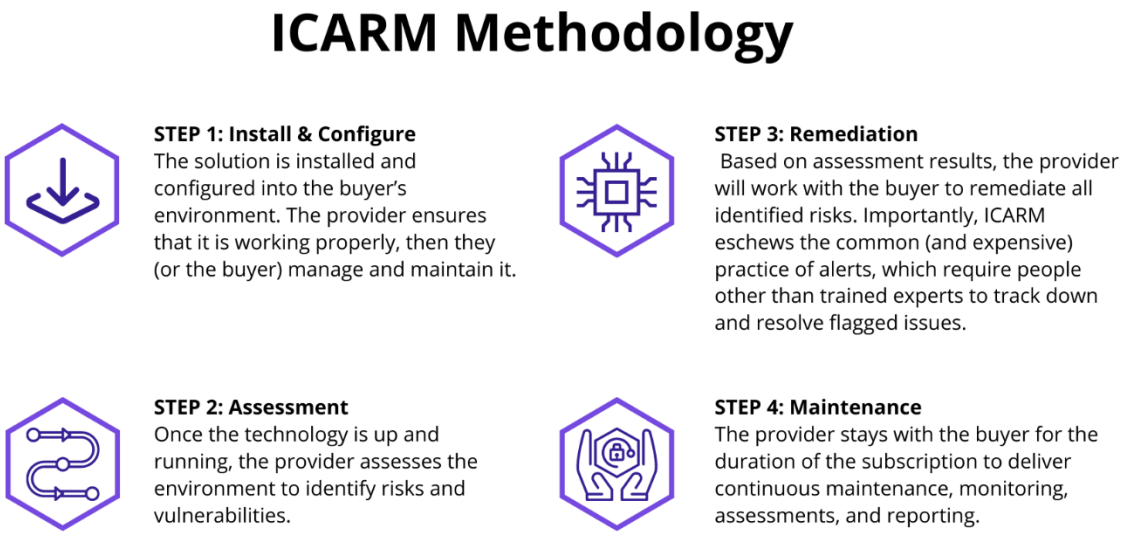

Figure 1: ICARM Methodology
click to enlarge

ICARM simplifies complex security engagements by effectively certifying and continuously remediating the buyer's environment. Universal guidelines like the CIS top 18 make the process flexible and repeatable, designed to support organizations as they change and grow so they can seamlessly remediate new risks around the clock.

Cyber insurance for protection and peace of mind

For some organizations, however, even CSaaS and ICARM are not enough to quell the anxiety of possible ransomware attacks that could jeopardize the entire business. They seek protection beyond their day-to-day operations to defray breach-related costs should an incident occur—because even if a company practices good cyber hygiene, its supply chain vendors might not.

Without proper security health checks and a certified environment, insurance can be prohibitively expensive, especially for startups and SMBs. But for organizations willing to embrace the cybersecurity basics, implement sound controls, and certify their security environments, cyber insurance can be a cost-effective way to get peace of mind—and some financial assurance to manage service-disruption costs related to ransomware threats, business email compromise (BEC), compliance penalties, audit failures, regulatory fines, legal liability claims, business interruption expenses, and more.

© Pipeline Publishing, L.L.C. All Rights Reserved.

Not for reproduction or distribution. © Pipeline Publishing, L.L.C. All Rights Reserved.

Some security products already come with warranties, but buyers seeking financial assurance are then limited both in their choice of product and their range of coverage. If a company chooses to seek cyber insurance on its own, they must do their own due diligence and navigate complex, lengthy underwriting processes. In either case, there's a good chance they will end up with big bills that aren't covered in the event of a cyberattack.

Combining cyber insurance with CSaaS is an important innovation for cybersecurity generally and one of the fastest-growing trends in CSaaS specifically. Not only does the CSaaS provider validate that the insurance offered is the best available, they also complete the application for the buyer and certify the buyer's environment, which streamlines underwriting while securing the best rates and lowest premiums for buyers. Additionally, the alignment of security and insurance means that, in the event of a claim, forensic data is more quickly and securely communicated between parties, so claims are paid faster.

The best cyber insurance offerings today are technology agnostic, include conventional cyber insurance coverage, ***and*** provide financial assurance to CSaaS subscribers in the aftermath of an incident. Some providers are going even further, offering service guarantees with broader protection than product-specific warranties. Subscribers enjoy this automatic protection for no additional charge, serving as a kind of "deductible" that may further lower premiums on a full cyber insurance policy.

Think of it this way. A small cookie shop suffers a DDoS attack that prevents online orders from being placed. Every hour that passes costs the shop in terms of lost revenue. With a CSaaS subscription, the service guarantee may be the shop's first line of defense, covering the initial costs related to operational downtime, legal fees, or compliance fines. If the costs to remediate and recover exceed the protection in their subscription, or if additional coverage (to handle reputational damage, for example) is required, their cyber insurance kicks in. The same is true in a ransomware attack: once the maximum reimbursement provided by the CSaaS subscription is reached, including ransom payments, the buyer's cyber insurance takes care of everything else. Both the service guarantee and the access to affordable, comprehensive cyber insurance are inherent benefits of the CSaaS model.

CSaaS is all in one, all at once. With CSaaS, insurance, like compliance, becomes a by-product of a sound security strategy.

For many decades, the marriage of people, process, and technology has been a proven best practice, but somehow this union has passed cybersecurity by. Now, organizations can save money, boost business velocity, and increase cyber resilience by choosing cybersecurity as a service coupled with cyber insurance to achieve advanced protection from today's threats and peace of mind that confidential data is safe from hackers.

Best of all? They'll find they can actually afford it.

© Pipeline Publishing, L.L.C. All Rights Reserved.

Not for reproduction or distribution. © Pipeline Publishing, L.L.C. All Rights Reserved.