Expert Guide

FOR INTEGRATORS AND SOLUTION PROVIDERS

CYBERSECURITY: Actionable Advice from the Front Lines

Inside

For IT solution providers, there's never a cease-fire when it comes to cybersecurity. In addition to constant vigilance, staying on top of trends is critical.

This Expert Guide includes some tips on avoiding phishing attacks, a look at why new approaches to cybersecurity are required, what to know about cyber insurance market changes, and how to implement zero trust for IoT. In addition, a channel pro in the trenches shares how to get clients on board with security best practices.

POWERED BY ChannelPro

WWW.CHANNELPRONETWORK.COM

IoT playbook

WWW.IOTPLAYBOOK.COM

Sharp Tips to Dull Spear Phishing Attacks

With spear phishing looming larger on the threat landscape, channel pros must take steps to help SMBs with protective measures. **By Geoffrey Oldmixon**

IMAGINE A SCENARIO in which a midlevel executive has been emailing her real estate agent about a transaction for weeks. In the final days of negotiation, the executive's administrative assistant is expecting to deliver a down payment check, but at the last minute receives an email from his boss: "Change of plans; we're not cutting a check," she writes. "Instead, please wire the funds here"—and the email includes a link with directions for entering account details.

If the assistant does as his boss instructs, he will have fallen victim in this case to "spear phishing." Although it's not a new phenomenon, spear phishing is becoming an increasingly common type of attack.

Unlike broad phishing attacks that spam large recipient pools, spear phishing employs impersonation and targets specific individuals. "[The attackers] leverage authority and scarcity to get people to click," sums up Diana Kelley, CTO of SecurityCurve, based in Rye, N.H. "They do a really good job of enticing us to click and respond."

That's because the "bad guys" are doing homework so they can tailor their attack to a specific person or organization, "tricking end users to hand over credentials to their email account or take some kind of action," explains Chris Hamm, CTO of Premier One, a managed service provider based in Topeka, Kan.

Many initial spear phishing attacks begin with urgent notifications seemingly from trusted services, like Microsoft 365 or a routine file-sharing or document-signing platform. "With any of these cases," Hamm says, "once the attacker can get a valid username and password, they're going to login directly." The attacker may then read dozens of emails and devise a finely tuned spear phishing plot.

> "If you get an email from Dave in Accounting, but there's a tag across the top, you know it didn't come from inside the company."

CHRIS HAMM
CTO, Premier One

The types of attacks Hamm describes are becoming "far greater than SMBs' ability to detect and respond," says Ori Arbel, CTO of Israel-based Cyrebro, a cloud-based security operations center-as-a-service provider. As a result, he adds, the SMB market lags behind in addressing the threat.

Moreover, Arbel says the average MSP is "not as equipped to defend clients from spear phishing as they need to be." For instance, he says, "Two-factor authentication is not widely adopted or enforced, and 'don't click' policies are not communicated enough."

Two-factor authentication is the biggest protective measure MSPs can take, according to Hamm. "The Office 365 account absolutely has to have multifactor authentication," he stresses, adding that "you really need it for any online account—all your banking and financial accounts, and even Amazon and Facebook."

Kelley agrees and cites other "really low-hanging fruit" for MSPs to implement—namely, the DMARC email authentication protocol (so outsiders can't spoof your address) and mail exchange (MX) records in the Sender Policy Framework (SPF) of a Domain Name System (to define the exact IP addresses permitted to send email). "This is good mail hygiene," she says.

Hamm offers another set of frontline solutions: external email tagging and AI-driven email scanning.

"Most systems include a pretty simple tag that says it's coming from outside the organization," Hamm notes. "So, if you get an email from Dave in Accounting, but there's a tag across the top, you know it didn't come from inside the company."

As for email scanning, Hamm says these AI systems are "scanning for characteristics of emails compared to other emails in the inbox or in the company as a whole to identify [suspicious] things." Barracuda Sentinel is one example, and it integrates with Microsoft 365.

Still, nothing is as effective as user awareness. "Training employees on a regular basis on how to recognize common tactics and properly protect their stations is vital," Arbel stresses.

Kelley says what's needed is a change in the culture of response. "There used to be a lot of dismissive comments [from channel pros] that the problem existed between the chair and keyboard. I'm happy to see that changing. We've got a real opportunity to engage in deeper learning that can be fun and gamified. People shouldn't be made to feel embarrassed if they get fooled by a really good phish."

GEOFFREY OLDMIXON *is a Massachusetts-based freelance writer and editor.*

Modern Cybersecurity Requires New Approaches

NEW RESEARCH from CompTIA finds U.S. employees believe the state of cybersecurity is declining, with 70% satisfied with their company's approach, a drop from 82% in 2020. Indeed, just 3 in 10 respondents say they are "completely satisfied" with their organization's approach to cybersecurity, according to the *2021 State of Cybersecurity* report.

Currently, the most common cybersecurity practices are: monitoring for cybersecurity incidents (49%), workforce assessment/education and threat intelligence (both at 41%), incident detection and response (39%), and business continuity (37%).

Because cybersecurity is such a complex, multifaceted problem, the research concludes that new approaches are required. No surprise that the top trigger for change is the shift to a remote workforce, according to 43% of respondents. Hurdles to change, however, include belief that current security is "good enough" (45%), prioritization of other technology initiatives (39%), lack of budget dedicated to security (38%), and low understanding of new security threats (37%).

On the bright side, respondents do expect overall spending on cybersecurity in 2021 to increase 12% over 2020, with the highest increase (41%) being directed at cloud security.

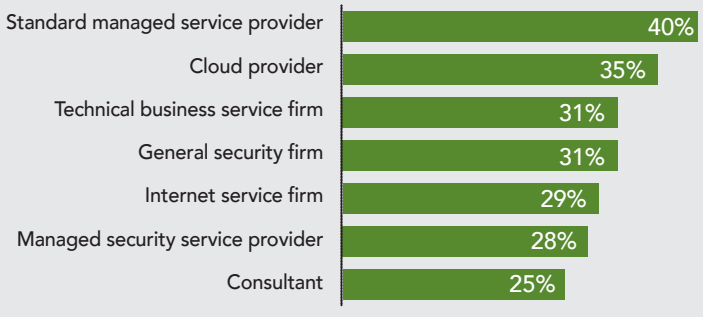
The top issue driving that spend is the number of hackers, according to 49% of respondents. Other key drivers are: variety of attacks, privacy concerns, scale of attacks, and reliance on data.

Changes to cybersecurity approaches vary by company size. For instance, midsize and small businesses favor a focus on education (45% and 36%, respectively) and process change (37% and 39%), while large companies prioritize incident response (46%), followed by education and new metrics.

Respondents plan to improve their cybersecurity skills by training current employees, hiring new ones, expanding current partnering, exploring new partners, and certifying current employees.

Here's what channel pros should note: When evaluating third-party cybersecurity firms, respondents say they are looking for excellence in core offerings, specific knowledge in a focused area, broad knowledge across multiple domains, ability to perform cost/benefit analysis, and access to threat intelligence.—*Colleen Frye*

Types of Third-Party Firms Involved with Cybersecurity



SOURCE: COMPTIA, *2021 STATE OF CYBERSECURITY*

Cyber Insurance Market in Flux

THANKS TO rapidly growing cybercrime, SMBs (along with the rest of the business world) are finding cyber insurance coverage for losses resulting from malware, ransomware, phishing, and other types of attacks more necessary than ever before—and increasingly harder to get.

In fact, according to Forrester, demand for cyber insurance currently outstrips supply, and losses due to cybercrime are at an all-time high. "Fitch Ratings [a credit rating company] estimates that 2020 US cyber direct loss ratios were at 73 percent, the highest recorded level in six years, highlighting the extent of increased cyber damages and claims," states Forrester's 2021 report, *The Cyber Insurance Roller Coaster: As Demand Speeds Up, Some Insurers Disembark*.

The result? Forrester finds "a hardening market where premiums for standalone cyber policies are expected to increase by 30 percent in 2021—if they can be bought—and insurers tightening up their underwriting standards and exclusions."

"It's a mess out there," says Joseph Brunsman, president of The Brunsman Advisory Group, an Annapolis, Md.-based professional liability and cyber insurance broker, whose client base includes MSPs, and co-author of *Damage Control: Cyber Insurance and Compliance*.

Companies selling cyber insurance are "losing serious money," he notes. At the same time, he says, "We are seeing entire classes of businesses where it's becoming near impossible to even get a quote."

New and/or renewal quotes from major cyber insurers are now often accompanied by strict conditions too.

"We are seeing mature, established players demanding that companies implement specific controls, along the lines of, 'You have to have cloud-based backups of critical data—and if you don't, we are going to limit you to a $25,000 ransomware sublimit,' which is way below what most companies need," Brunsman reports.

This situation is driving a fast-growing emphasis on adoption of cybersecurity controls, he notes, which in turn presents opportunities for channel pros.

"For a lot of business owners, cybersecurity is a massive, overwhelming topic that they know nothing about," Brunsman says. MSPs can help these businesses implement the cybersecurity controls required for a cyber insurance policy, he says, most of which are recommended best practices anyway.

MSPs need to take steps to protect themselves as well, according to Brunsman.

"The more businesses we see getting hit [by cyberattacks], the more likely it is that MSPs will eventually have clients that wind up bringing lawsuits or claims against them," he explains.

To help head this off, Brunsman says, "I tell all of my MSP clients to consider contractually requiring all of their clients to carry cyber insurance themselves."—*Martin Sinderman*

Zero-Trust IoT

To keep corporate networks secure, implement a least-privilege, zero-trust approach with devices, not just users. **By Martin Sinderman**

INCREASINGLY CONSIDERED a sound strategy for network security in general, zero trust (ZT) is arguably even more critical when it comes to IoT solutions. With 41.6 billion connected IoT devices expected by 2025, according to IDC, the stakes are high.

"Any computing device, including IoT devices, implemented within a digital ecosystem can become a pathway to every other component attached to the network if strong security controls are not implemented," says Rebecca Herold, CEO of Privacy and Security Brainiacs, an information security, privacy, technology, and compliance services provider, and part of a NIST team developing an IoT cybersecurity framework.

Currently, most network security is based on one-time validation/authorization of an entity (typically a user) logging into an entry point along the network perimeter, which Sean Tufts, IoT/OT practice director at cybersecurity solutions integrator Optiv Security, likens to a "moat" surrounding a walled-in castle. In this "ultimate trust" scenario, he explains, "once someone 'vaults the moat' with one central login and makes it over the walls into the castle, they have access to everything within that network environment."

With ZT security, in contrast, access to network components (i.e., the "rooms" in the castle) must go through additional layers of authorization and approval.

"ZT security is implemented throughout the full scope of the digital ecosystem, within which the ZT architecture has been implemented, to validate component connections, communications, and relationships on an ongoing basis, through established and enforced access policies and workflows," explains Herold. "The goals of ZT are to prevent unauthorized access to data, objects, and services, as well as to use access control that is as granular as possible to enforce 'least privileges' needed by any given component to perform requested actions," she notes.

> "Any computing device, including IoT devices, implemented within a digital ecosystem can become a pathway to every other component attached to the network if strong security controls are not implemented."

REBECCA HEROLD
CEO, Privacy and Security Brainiacs

ZT focuses not only on data access, but also on securing access to all other types of network components—including IoT devices, according to Herold.

Given the ubiquity and diverse applications of IoT devices, not securing them specifically can have significant consequences. Herold cites a well-publicized incident in 2017 in which a Las Vegas casino was hacked through an internet-connected thermostat in an aquarium. "The cybercriminals used it as a pathway to access the casino's computer systems and databases, where they exfiltrated 10 gigabytes of sensitive and confidential data that went to a device located in Finland," she notes.

Had the casino implemented a ZT architecture, it would have ensured, on an ongoing basis, "that not only would specific authorized components alone be able to access the aquarium capabilities, but [also] that the IoT aquarium could only access a limited set of specific components on the casino's network," she explains.

Implementation Notes

Traditional network security has historically been seen as product/technology-led, as in, "here is a technology to solve a problem," says Tufts. In contrast, ZT entails a more comprehensive look at an organization's network and operations, he notes, including analysis of the "criticality level" of specific functions and letting that be a determinant of the level of security necessary.

"An organization that wants to implement ZT architecture needs to determine the scope of applicability for the use of ZT, and then spend all the time necessary to do thorough planning up front, before implementation," says Herold, adding that "the more time spent planning, the less time will be spent fixing the areas overlooked when the ZT architecture was implemented."

Meanwhile, there are a number of zero-trust network access (ZTNA) solutions utilizing artificial intelligence and machine learning that channel pros can implement for both IoT and the rest of their digital ecosystems. Examples include BlackBerry's BlackBerry Gateway; Inferati's Zero Trust AI; Vectra's Cognito platform; Accenture XDR; and General Dynamics IT's (GDIT) Cyber Stack.

To get up to speed on zero trust, Herold recommends NIST's Zero Trust Architecture report. "[The report] provides significant research and insights about ZT architecture that clients of MSPs will find helpful," she notes, "and also will demonstrate to them that their MSPs are providing guidance based upon some of the most rigorous cybersecurity guidance available."

MARTIN SINDERMAN *is a freelance writer in Savannah, Ga.*

Peer to Peer

ERIC WEAST

PRESIDENT AND PRINCIPAL
ECW NETWORK & IT SOLUTIONS

FOUNDED 2004

LOCATION Deerfield Beach, Fla.

NUMBER OF EMPLOYEES 25

WEBSITE ecwcomputers.com

COMPANY FOCUS We are cloud first, security first

PROFESSIONAL MEMBERSHIPS CompTIA ISAO, Dark Cubed Advisory Council

FAVORITE PART OF MY JOB Orchestrating solutions to integrate

LEAST FAVORITE PART Printers

WHAT PEOPLE WOULD BE SURPRISED TO KNOW ABOUT ME
I love to cook.

CUSTOMER LITMUS TEST

ECW Network & IT Solutions put a stake in the cybersecurity ground, is now planting one with cloud, and wants only customers who will take that journey.

BY ERIC WEAST ○ PHOTOGRAPH BY STEVE BOXALL

AS ECW NETWORK & IT SOLUTIONS has matured over nearly two decades, being choosey about our customers has been key to scalability and growth. Saying "no" is how we are getting our business and our customers to a security-first, cloud-first model that protects against cyberthreats, prepares for future trends, and drives mutual success.

We want customers who, first and foremost, are willing to go to the next iteration of technology. We also want customers we can grow with. If they're not investing in security or cloud, they might not be around in five years. Finally, we want customers who trust that we know what they need. Think about a builder whose client hands him a bunch of toothpicks and marshmallows and demands he build a house. The answer, of course, would be "no."

Our ideal customer understands the necessity of cybersecurity and understands that technology changes. Those are the people we can approach with new ideas. Anyone who thinks they only need to replace the server every seven years, or still won't upgrade that legacy piece of software to get them onto the latest version of Windows, is not a good fit.

ECW first culled customers we couldn't grow with when we moved from break-fix to managed services in 2014. We transitioned those who didn't understand or want the benefits of monitoring and management to other providers.

The next phase of selectivity started about four years ago: Enforcing a security baseline. It's a much easier conversation than it used to be because everyone seems to be living the headlines to some degree. We get calls from business owners all the time telling us their friend at the golf course got hacked or they heard of a breach at a neighboring business, so it's become an extremely real thing to them. Only a handful ended up leaving us because they didn't want to comply.

Being intentional about the customers we choose to work with isn't easy. It doesn't happen overnight, and there is some risk, of course.

The Next Phase

We are now moving to a cloud-first approach as well for net-new customers. A lot of businesses are still not fully in the cloud, and we know that Gartner and others say that something like 95% of workloads are going to be cloud-based by 2025. Our job is to get our customers there.

Going forward, our strategy is to take the Microsoft-centric plunge and move on-premises workloads to Azure to take advantage of things in the stack like VDI, automation, and authentication mechanisms.

Cloud will be our new customer litmus test because we know we can better maintain and secure systems that are cloud based. It's easy to do the math. With the ability to automate, we'll be able to serve more cloud customers than we could on-premises customers. Our goal with cloud is not to make more money with cloud subscriptions, but rather to grow revenue with stability and scalability.

So, the first thing we talk to prospects about now is their vision for the future. If they are not committed to getting their infrastructure entirely into the cloud over time, we are not interested in working with them at this stage in time.

With existing customers, we'll follow a similar path as we did with moving them to our security stack. We won't fire those who aren't 100% cloud, but we are encouraging them to move as many legacy and on-premises systems to the cloud as possible. This is a conversation that's just beginning, and the pandemic has certainly made it real as businesses recognize the long-term need to support a remote or hybrid workforce.

When we get to the latter part of 2023, however, we will start culling those who are reluctant to invest in their future and by 2025 focus only on customers who want to grow—and who ECW can grow with.

STEPS RECOMMENDED BY ECW FOR CREATING A SECURITY-FIRST CUSTOMER BASE:

- Carefully craft your pitch about the importance of adopting your security stack and understand that you may get fired.
- Don't approach 100% of your customers all at once.
- Transition customers to your security stack on a rolling basis.
- Expect a multiyear effort to get all customers onboard.
- Don't accept net-new customers who will not comply.