Expert Guide

FOR INTEGRATORS AND SOLUTION PROVIDERS

CYBER-SECURITY

Defensive Playbook

Inside

Security is a team sport, often requiring a variety of players and solutions to help protect organizations from cybercriminals. It also requires staying on top of the latest attack types and techniques. And when a breach does occur, having a plan in place to mitigate the damage is critical.

This Expert Guide offers some advice on partnering with security service providers to expand the skills and resources needed to keep customers safe, a look at rising threats like "smishing" and deepfakes, and practicial tips for incident response management.

POWERED BY ChannelPro

WWW.CHANNELPRONETWORK.COM

IoT playbook

WWW.IOTPLAYBOOK.COM

Knowing which security functions to outsource—and which not to—is an increasingly important skill for channel pros.

YOU AND WHAT ARMY?

★ ★ ★ By Rich Freeman ★ ★ ★

SECURITY, THE SAYING GOES, is a team sport. Most channel pros with a winning team get at least some of the skills and resources they need to keep customers safe from beyond their own staff.

"MSPs tend to think that they can do everything, and that's not really the truth," says George Monroy, CEO of San Antonio-based Monroy IT Services.

Especially these days, adds Michael Goldstein, president and CEO of LAN Infotech, an MSP and solution provider in Fort Lauderdale, Fla. "I need a fleet of people with all the new vulnerabilities that are out there," he says, not to mention enormously expensive tools. Partnering with outsiders makes far better financial sense and results in better protection for end users.

More and more of Goldstein's peers have reached the same conclusion. Given the ever-expanding range of threats SMBs face these days, they agree, the question isn't whether to outsource a portion of their security services. It's which ones to outsource, and how best to do it.

The round-the-clock monitoring and analysis provided by a security operations center (SOC) with state-of-the-art SIEM software is usually a good starting point. "Most companies are not going to be able to do that," Monroy observes. "It's a huge investment."

RORY SANCHEZ

Setting up a facility and equipping it with software, moreover, are just part of that investment. Hiring experienced security specialists is a steep yet indispensable expense too.

"There's a lot of intricacies to the business," observes Rory Sanchez, CEO of True Digital Security, which provides outsourced security services to corporate IT departments and channel pros from offices in Florida, New York, and Oklahoma. "A lot of MSPs don't have the in-house expertise to really get into the weeds on security issues, so who do they escalate that to when they really get into a jam?"

On a more day-to-day basis, he adds, third-party SOC providers can help IT generalists spot risks they might otherwise miss, separate real issues from false positives, formulate incident response plans, and assist with post-breach threat hunting. "A lot of MSPs are not really equipped to make sure that the bad guys are out," Sanchez says.

Fresh Set of Eyes

Leaning on outsiders with deep knowledge of HIPAA, GDPR, and other complex regulations is a wise choice for most channel pros as well. "It's a highly specialized area," observes Monroy, who recently partnered with an outside firm to help a newly signed client comply with the Cybersecurity Maturity Model Certification (CMMC), a federally mandated set of security standards for companies that design, produce, and maintain weapon systems.

Sanchez advises IT providers to bring in third parties for audits and penetration tests too, noting that almost everyone benefits from having a fresh set of eyes double-check their work. “We’re all about outside validation,” he says.

Of course, offloading everything you do in security could leave customers wondering what they’re paying you for, so setting limits on outsourcing is important. Monroy, for instance, performs hands-on, relationship-enhancing tasks like policy setting and strategic consulting himself. Goldstein generally draws the line at endpoint protection and other basics performed behind the firewall.

“Anything inside the network, I want to handle ourselves,” he says. “Anything coming into the network, I would probably want to outsource.”

Working Well Together

Given the potential consequences of a security lapse (91% of SMBs would consider switching IT providers to get better cybersecurity services, according to a research study commissioned last year by managed services vendor ConnectWise), choosing the right outside security partner is critical.

“You have to interview them almost like they’re going to be your employee, because really they’re going to be an extension of your business,” says Monroy, who grills prospective outsourcers about their SLAs in areas like response time and service hours.

“Are they available 24/7?” he asks. See if they provide access to live security analysts or rely solely on artificial intelligence, he adds. Goldstein, for his part, confirms that security partners won’t contact his clients without permission and don’t sell direct.

Once you’ve found a partner you like, clarify your division of labor with them to ensure important tasks don’t fall through the cracks. “You want some clearly drawn lines on what are [they] responsible for and what are we responsible for,” Sanchez says.

Building a strong working relationship is equally vital. “You have to make sure that there’s good communication there,” Monroy says.

That communication should be with specific individuals you can count on to take your calls when it counts, Goldstein adds. “I don’t want to be at the mercy of support for something simple,” he says. “I need to be able to get to someone.”

Goldstein also recommends speaking regularly with contacts on an outsourcer’s sales team to keep informed about services and capabilities on the roadmap. “We want to know what’s coming up the pike,” he says.

Getting to know an outsourcer takes time, Monroy notes, so avoid switching companies any more than necessary. “MSPs like to jump around from vendor to vendor often because they think something’s better somewhere else,” he says. “You need to just find one and stick with them.”

Or maybe a few, but sharing security duties with someone other than yourself is increasingly a must.

“I’m seeing MSPs all over the place, trying to piecemeal something together,” Monroy says of security. “An MSP should really look to outsource it or partner with somebody from day one.”

READER ROI

OFFLOADING SELECTED SECURITY TASKS to third parties is a cost-effective alternative to expensive in-house tools and talent.

SOC SERVICES, compliance support, and penetration testing are all good candidates for outsourcing.

POLICY SETTING, strategic consulting, and other relationship-enhancing functions are typically poor candidates.

CULTIVATING CLEAR LINES of responsibility and strong lines of communication are essential to working successfully with a security outsourcer.

TO WHITE LABEL OR NOT TO WHITE LABEL?

CHANNEL PROS often white label outsourced services to ensure that credit for great work flows to them rather than their vendors. When it comes to outsourced security, however, honesty is often the best policy. For one thing, experts say, you don’t want to take all the blame for bad work. For another, pretending you do everything yourself rarely fools clients.

“It always seems like you’re hiding something,” says George Monroy of Monroy IT Services, which doesn’t white label its security offerings. “I’m going to tell them why we’re working with a particular partner … why it benefits them, and why it benefits us.”

Same goes for Michael Goldstein, of LAN Infotech. “I want my customers to know that we’re going to best-of-breed products,” he says.

GEORGE MONROY

Phishing + SMS = Smishing

NOT CONTENT to rely on email, cybercriminals are increasingly embedding phishing lures in text messages in a technique dubbed “smishing.” Smishing is particularly effective because people tend to click on text links frequently and impulsively, and unlike the misspellings and Nigerian princes that populate phishing emails, the brevity of texts mitigates those red flags.

Typically a smishing message conveys a sense of urgency, such as “Your account has been compromised,” or “Your password has changed,” explains Joseph Neumann, cyber executive adviser at Coalfire, a cybersecurity firm in Westminster, Colo. “The attacker attempts to get you to click on an embedded link to visit the site, and possibly download malicious content or enter credentials,” he says.

Scammers may also effectively spoof messages from well-known companies and direct recipients to legitimate-looking sites, turning smishing into social engineering on steroids.

It’s on the rise too, according to Lawrence Cruciana, president of Corporate Information Technologies, a provider of cybersecurity services to SMBs in Charlotte, N.C. Anecdotally, Neumann agrees. “I currently receive two to three of these types of text a week, offering mortgage refinancing or account resets,” he says.

Attackers don’t just target individual users. According to the 2021 *State of the Phish* report from security company Proofpoint, 81% of U.S. organizations faced smishing attacks last year. “More commonly, smishing is part of a blended attack that is actually targeted into smaller organizations because they are easier prey,” Neumann says.

> “Smishing is often part of a blended attack that is actually targeted into smaller organizations because they are easier prey.”
>
> **JOSEPH NEUMANN**
> Cyber Executive Advisor, Coalfire

Lack of awareness is a top reason smishing is successful, Cruciana says. While many MSPs have done a good job with educating their clients about phishing, little attention has been paid to smishing. Thus, education will go a long way toward mitigating risks.

“Users should protect themselves by simply deleting and ignoring these messages,” says Neumann. “Never click on a link provided!” Other best practices include logging out of websites, closing browsers when not in use, keeping operating systems updated, and upgrading phones to the latest version possible.

Cruciana also recommends that companies clearly outline the conditions under which employees can use mobile devices to access corporate data and deploy mobile endpoint management software. “As a practice, we deploy a unified endpoint management product for our clients,” he says. “We require the use of encryption, strong pass phrases, and apps that are supported and updated.”

While smishing may be a new twist on an old scam, defending against it requires the same general ingredients: a good portion of commonsense accompanied by a dose of security tools.—*Megan Santosus*

Brace Your Customers for Deepfakes

WHEN QUEEN ELIZABETH performed a TikTok dance during her Christmas 2020 video address, people saw the joke but not the warning. The last *Stars Wars* movie featured actors dead for two decades. Can you trust your senses anymore?

Deepfake, a mashup of deep learning (artificial intelligence and machine learning) and fake, manipulates one person's image or voice for deceptive purposes. Faked voices are a bigger problem today than videos, because the technology is easier and more available. "In Germany [in 2019], criminals impersonated a person's voice to scam $250,000," says Joseph Steinberg, a cybersecurity adviser in New York. "Imagine how fake advice from Elon Musk could affect the stock market."

He warns 2021 is the beginning of deepfake attacks, and they'll be dramatically better in five years.

Joe Palmer, president of iProov in North America, a biometric authentication company in London, agrees. "We see 2021 as the year of the deepfake," he says. "It's hard to do well, but if a gang does the work, they can scale their crimes. An example is filing false unemployment claims for hundreds of people, routing the checks to themselves."

Similar deepfake attacks are being used on other government accounts. There are only a small number of people able to pull these crimes off, but Palmer believes they'll soon appear for rent like access to botnets. Social engineering attacks using deepfake voices and images are also being used for breaches like installing malware.

The remote workforce is a target too. "Deepfakes are much more dangerous when people are remote," adds Steinberg. "In an office, you can see each other."

One tool for protecting against deepfakes is facial verification, which now has protections against the easiest deceptions. "You can no longer just hold up a picture of a face, which did work early on," says Palmer. Techniques such as looking for eyes to blink could be spoofed with an iPad simulating a blink, he adds, but the industry has closed that gap.

Now facial recognition technology can measure how light reflects on the face to make authentication more reliable. And costs for these solutions are dropping into the SMB range, especially when existing webcams and smartphone cameras are used.

For high-dollar transactions in particular, Palmer says users feel more comfortable with processes that include advanced tools like facial authentication. "The best two authentication sources are your face and a verified device." If you can trust the face.

Steinberg says authentication technology will always lag behind criminal efforts, however, so he advises training users and putting processes in place to verify transactions that can be spoofed. For example, if you get a voicemail from your boss demanding an immediate payment to a supplier, verify it.—*James E. Gaskin*

INCIDENT RESPONSE MANAGEMENT

In the heat of a cyberattack, successful mitigation depends on good incident response planning and execution. By Colleen Frye

This article is based on a panel discussion at ChannelPro's *Cybersecurity Online Summit held earlier in the year.*

A DECISIVE PLAN, fast response, and clear communication are all critical components when a cyberattack occurs. Here, seasoned channel pros provide advice on four incident response scenarios.

PHOTO: FLORIANA / ISTOCK

YOUR CUSTOMER JUST GOT HIT BY RANSOMWARE. WHAT'S THE FIRST THING YOU DO?

1. ACTIVATE YOUR INCIDENT RESPONSE PLAN

Assemble your incident response team and implement the plan, which includes determining the type of breach and where the exposure is, advises Corey Kirkendoll, president and CEO of 5K Technical Services, in Plano, Texas. That may include bringing in your legal team and your insurance agency for guidance, particularly if you have a customer that deals with medical or financial records and must follow compliance regulations.

A step-by-step plan is critical, agrees Jayson Ferron, CISO/CEO of Interactive Security Training. "You should have it on the wall [showing], I'm going to do this first, this second, this third, this fourth." It's also important for proving due diligence, says Brian Weiss, CEO of iTech Solutions, in San Luis Obispo, Calif.

JAYSON FERRON

2. COMMUNICATE, COMMUNICATE, COMMUNICATE

Immediately inform the client that they've been hit with ransomware and that you may need to cut off users from company resources to mitigate the threat, says Weiss.

Urge your client to involve their own insurance company right away if they have compliance regulations they need to adhere to, he adds. "If they're going to be responsible for funding for damages, they're going to want to make sure you're following what they want you to do. Otherwise, they might come back and say, 'Hey, you didn't perform due diligence. Therefore, we aren't covering this set of damages.'"

3. ISOLATE THE THREAT VECTOR

As soon as you know what the threat vector is, remove it from the network and begin mitigation efforts, Kirkendoll advises. After you understand the depth of the exposure, he adds, start collecting evidence logs. At the same time, locate backups and make sure they're offline in case the attacker is still active in the network, says Michael Cocanower, CEO of Phoenix-based itSynergy.

THE ATTACK WASN'T JUST RANSOMWARE, THEY GOT INTO THE CLIENT'S DATABASE TOO. WHAT DO YOU DO?

1. VERIFY BACKUPS

Once you've done so and know how far back the hack goes, you can perform a full or partial recovery, Kirkendoll says.

2. IDENTIFY THE ACCESS METHOD

Whether it's through the cloud or on premises, identify how the attack came in, Weiss advises. Was it via an API connection or through a user account? "Shutting down the database could be a quick and easy way to cut off access." He adds that you may want to implement conditional access to block a particular IP or country.

3. DETERMINE THE TYPE AND VALUE OF EXFILTRATED DATA

If there is potential exposure of personally identifiable information (PII), for instance, your customer may be subject to data privacy requirements, says Cocanower. Every state has different disclosure requirements and different reporting time frames, he adds. Bringing in the legal team from your customer's cybersecurity provider can help you understand the obligations.

MICHAEL COCANOWER

THIS TIME *YOU* ARE THE VICTIM, YOUR RMM HAS BEEN BREACHED. WHAT ARE YOUR FIRST THREE STEPS?

1. SECURE YOUR RMM

Shut down your RMM, inform clients immediately, and begin remediation, Weiss says. This can involve disabling accounts, resetting passwords, and setting up conditional access, among other things. Bring in your RMM vendor too, Weiss adds. “There may be things they know about that you don’t.”

If it’s a cloud-based RMM, he continues, “you’re immediately looking for scheduled or quick jobs that [attackers] might have kicked off across your devices that maybe haven’t run yet … even if you cut off their access, they could have left something behind [and] it’s still doing damage.”

Know the emergency contacts for a cloud-based RMM provider, Ferron stresses, and be sure they spell out how they’ll notify you if another MSP in that shared environment had a breach.

In addition, stop all automated scripts, Kirkendoll says, and make sure you have a way to access client devices outside of the RMM, so you can continue to manage those devices remotely if your RMM system isn’t available.

BRIAN WEISS

2. BRING IN THE EXPERTS

Tap your insurance company as quickly as possible for access to legal, PR, and other resources, Cocanower says. And if you have clients with regulatory concerns, contact their insurance companies as well, Weiss adds.

If you’ll be performing a forensic analysis later, disconnect the server from the network but leave it running, Ferron advises. “When the forensic team comes in, they can grab the memory that’s running in the server,” he explains.

3. COMMUNICATE FACTS

Once you’ve collected logs and fully understand what happened, communicate that to clients, Kirkendoll says.

Cocanower agrees. “What you don’t want to do is create a bunch of confusion in the beginning where you’re putting out all kinds of information and then having to go back and correct some of that later.”

WHAT ARE THE BEST WAYS TO PREPARE YOUR CUSTOMERS AND YOUR EMPLOYEES FOR AN INCIDENT *BEFORE* ONE OCCURS?

1. TRAIN, TRAIN, TRAIN

5K Technical Services offers security awareness training both in-person and online, and conducts mock tabletop exercises on incident response. “[Clients] get a chance to understand what we do in the event that something happens,” Kirkendoll says. “It also helps us continue to get better and helps make them aware of what is really important—what’s valuable when it comes to recovery—because that’s key for us as well.”

COREY KIRKENDOLL

2. FOCUS ON BUSINESS CONTINUITY

Weiss says it’s important for clients to understand that an incident can happen so they recognize the importance of investing in business continuity technology and drafting their own incident response plan. “There are things that they’re going to be responsible for doing on their end in order for you to be successful.”

3. USE THE POWER OF STORYTELLING

Talking with customers about the dangers of cyberattacks doesn’t always resonate, Cocanower says. Telling them a story about a real cyberattack, the sequence of events, what that customer had to go through, and what the implications were “makes it very real” and a more powerful message.

POST-MORTEM

While a security incident is unfortunate, it’s also a tremendous time for learning, Cocanower says. “If you aren’t disciplined about sitting down with your team after the flames have died down and really going through in a calm and methodical fashion, and determining what lessons can be learned, and then changing your processes based on those lessons, you’ve really wasted an opportunity.”

Cocanower says MSPs also need to be disciplined in following the same advice given to clients. “All those things you put in place for your customers, like the risk assessments and the incident response plans, you need to be doing those for yourself as well.” If you’ve done that, he says, you’re ready when an incident occurs: “Pull your incident response plan off the shelf, turn to page one, and start following the directions.”