# Expert Guide

FOR INTEGRATORS AND SOLUTION PROVIDERS

# CYBERSECURITY: Protect and Prepare

## Inside

There's no "finish line" with cybersecurity, just another twist, turn, or leg in the race to prepare your customers for new cyberattacks, protect them from current known threats, and put a plan in place if there is a security incident.

This Expert Guide offers some helpful advice on incident response management, how to expand your security offerings by partnering with security providers, and what you should know about zero trust. It also provides some tips for protecting customers against phishing attacks and deep fakes, and highlights some common mistakes to avoid in your own practice.




POWERED BY ChannelPro
WWW.CHANNELPRONETWORK.COM

IoT playbook
WWW.IOTPLAYBOOK.COM

# 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.

JAYSON FERRON

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.

### 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

MICHAEL COCANOWER

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.

## 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."

BRIAN WEISS

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.

### 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."

# PARTNERING WITH SECURITY PARTNERS

## Outsourcing security provides MSPs access to valuable expertise and technology, but it is still a shared responsibility.

By Colleen Frye

*This article is based on a panel discussion at* ChannelPro*'s August 2021 Cybersecurity Online Summit.*

**WHEN IT COMES** to cybersecurity, it's increasingly difficult for an MSP to go it alone. Partnering with a managed security provider is a viable way to shore up protection for customers without investing in expensive solutions or personnel.

"We're past the question of, should we be doing this?" says Joshua Liberman, president and founder of Net Sciences, an MSP in Albuquerque, N.M. "You need to be doing this for sure, unless you have confidence that you can build out a SOC, and that is a bigger challenge than ever."

According to Robert Boles, founder and president of BLOKWORX, a managed security service provider (MSSP) in Larkspur, Calif., the rationale for MSPs outsourcing security is similar to why SMBs outsource IT. MSPs can "leverage a partner who has those standard operating procedures and all of that expertise already in house, as well as not having to make the significant financial investment in operating and maintaining tools like SIEM and SOAR and a 24/7 security operations center." That allows MSPs to focus on what they do best, he notes.

For successful relationships, MSPs need to choose their cybersecurity partners wisely, however, and then follow best practices for working with them.

### What to Outsource?

To determine what to outsource, Boles says to identify gaps in your expertise and then find solutions to fill those gaps.

Liberman says he made some "practical choices," recognizing that he didn't have the resources to run a 24/7 NOC or SOC. Net Sciences uses one partner to manage log reading and response services through the firewalls. "They alert, they do auto blocking. Once they detect a real persistent threat of some sort, any kind of APT, we get reports, but they actually interact and do this in near real time, 24/7."

## READER ROI

- **FOR MANY MSPs,** partnering with a security service provider offers access to expertise, standard operating procedures, and technology that would not be feasible otherwise.
- **IDENTIFY GAPS** in your expertise and seek security partners that are aligned with your core values and capable of supporting your stack.
- **VET PARTNERS** thoroughly, trust their onboarding process, and establish lines of responsibility and good communication.

He uses a different MSSP for endpoint log reading and response services. "We really wouldn't be able to identify the true issues or respond quickly enough. They can also do things like lockdown traffic flow from that endpoint to their SOC, so they can remediate it at the endpoint or just keep it off the network entirely."

MSPs also must decide whether to partner with a single provider or take a best-of-breed approach like Liberman. "The downside to that is that's two different vendors, not one, two different consoles, two different things to manage," he acknowledges.

Boles cautions against partnering with multiple SOC providers because no one provider will have complete visibility.

Liberman doesn't disagree, but argues that some overlap in security tools and services not only safeguards against missing a critical event but also provides a safety net should a security partner get acquired.

### Choosing a Security Partner

When selecting a security partner, don't choose solely on lowest cost, but look first and foremost for a provider that is compatible with your culture and core values, advises Boles. "If your core values are such that defending the client is your highest priority, your process and your selection is going to be a little bit different than someone who's just looking for the lowest cost so they can have maximum profitability."

While margin is important and price is always a factor, he says, "the value of your partnership is when the poop hits the fan, and the more aligned your core values are, the more aligned everybody's going to be in responding to what the event is."

Also, be sure the security provider supports and monitors what's in your stack. "If I have WatchGuard, I probably want to partner with a SOC who will monitor WatchGuard," Boles says, as an example.

Liberman recommends building a decision tree. The first question is, best of breed or single-source vendor? "If you're going to do the latter, your decisions are far less complicated, and you're really narrowed down in the SMB world to a few of them. If you're going to do the former and weave together your own solutions, you need to find a way to visualize this."

Then thoroughly vet potential partners, Liberman advises. That includes asking peers as well as meeting in person with the provider. "You're choosing a partner here to do the single most important thing to do. … That's always a personal experience for me. I don't do it on the phone, or even by Zoom. I meet these folks, which is clearly harder than it used to be."

Determining a partner's financial stability is the most difficult part, he adds. "Are they really stable? A true SOC, SIEM, SOAR is a very serious investment. And the question is, will they continue to deliver on their promises? Will they grow as I'll have to do and still deliver the services and the support and the responsiveness that you need?"

### Best Practices for Working with a Security Partner

When working with a security partner, Boles says, both the MSP and MSSP must maintain objectivity and minimize emotion. "When emotions get involved in cyber, that's somewhat of a vulnerability because we're not really thinking clearly on factual data … and that introduces risk."

> "The value of your partnership is when the poop hits the fan, and the more aligned your core values are, the more aligned everybody's going to be in responding to what the event is."

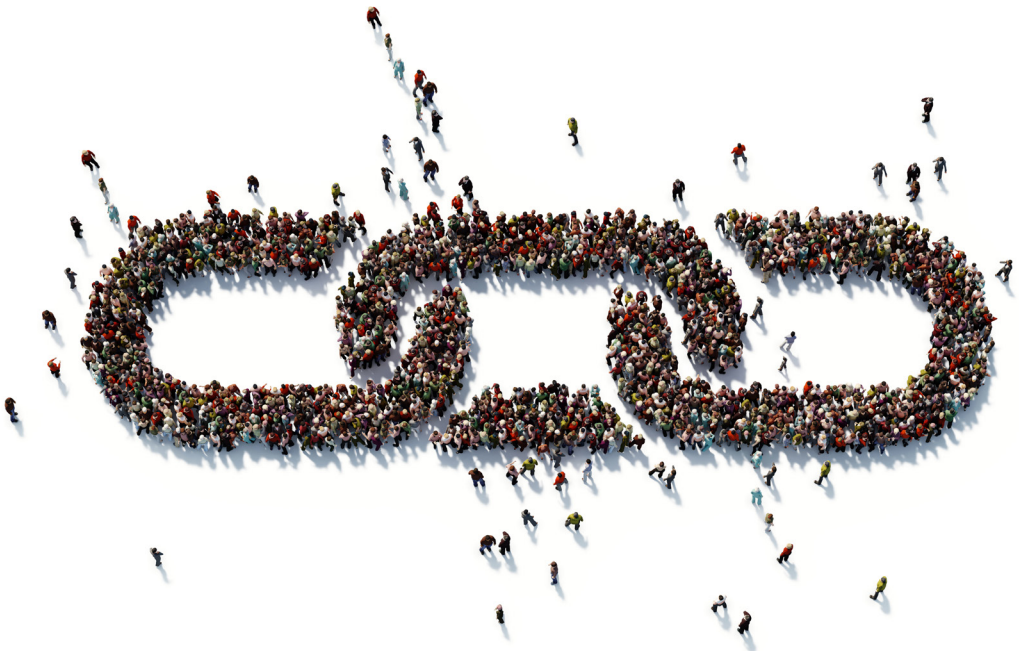
ROBERT BOLES
Founder and President, BLOKWORX

Another best practice is to trust and complete the onboarding process, he says. "When we onboard partners, it's very thorough," he explains. "We go through a process of script auditing and script control, where we actually create white- and blacklists for scripts. And I can't count how frequently partners just don't complete the process." Following the plan to the end, or as Boles puts it, "participating in your own rescue," is the best way to protect your customers and yourself, he says.

MSPs can't be hands off once they bring in a security partner either, because defending the client is a shared responsibility, Boles says. For instance, if the MSSP is protecting 200 machines, but then the MSP retires one, onboards another, and fails to either install the agent or inform the MSSP, "We're not going to know because in our dashboard, we're still going to see 200 machines. We're just going to see one that's inactive."

That's why it's critical to define partner responsibilities, Boles says, and establish good communication. "I can't underscore how important it is to communicate and to adhere to, 'Hey, we're all in the boat together, from a security perspective.' The bad guys only have to win once. They only have to find one gap."

Ultimately, though, the buck stops with the MSP, Liberman stresses. "You hold the burden. … Everybody you use to do that job is your problem. You're holding the contract with your customer. And even outside of that, ethically speaking, morally speaking, it's your commitment."

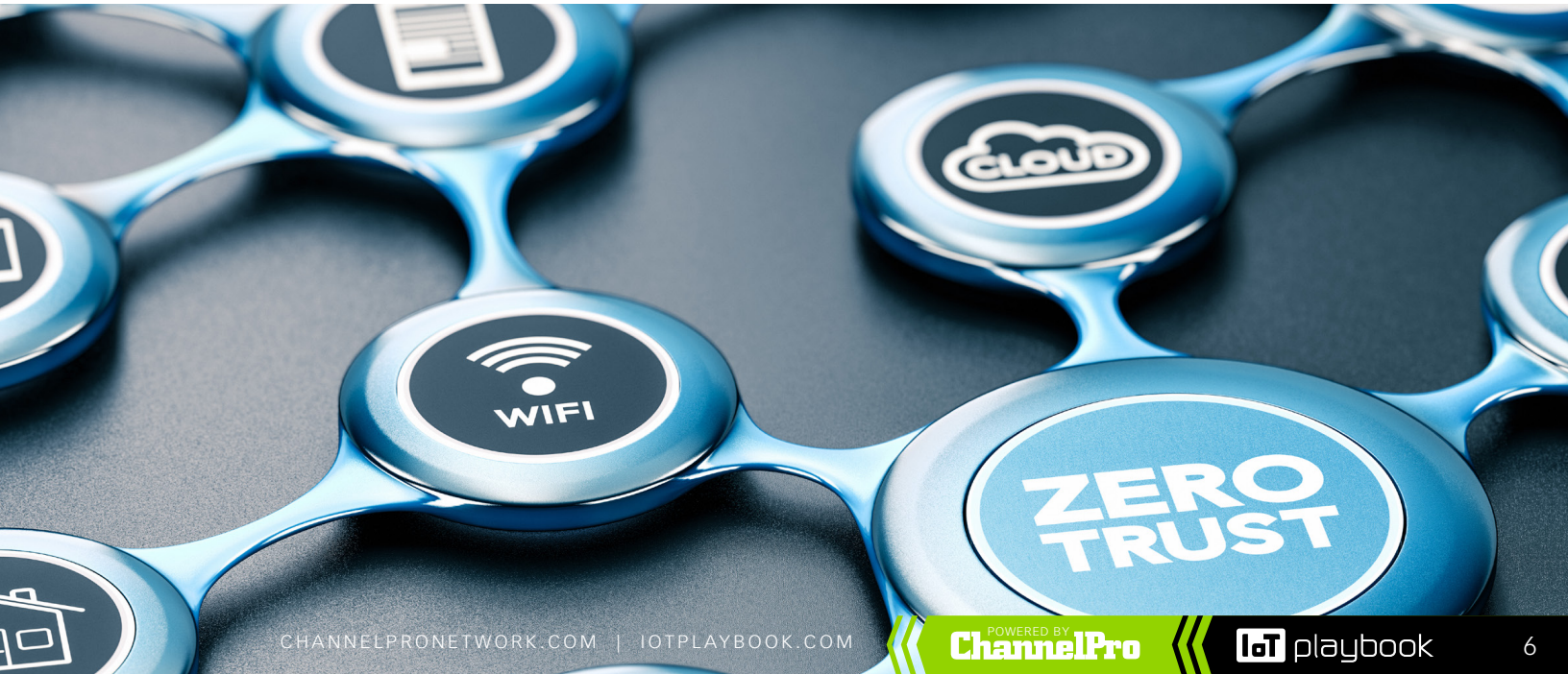


# THREE QUESTIONS, THREE ANSWERS ABOUT ZERO-TRUST SECURITY

## NOT SURE WHAT IT IS OR HOW TO DO IT? LEARN WHAT EXPERTS HAVE TO SAY. BY RICH FREEMAN

**TRUST** has always been a dangerous commodity in IT. In the era of cloud computing and work from anywhere, in which attacks grow continually more sophisticated and defensible perimeters no longer exist, it's a luxury that neither channel pros nor their customers can afford. Businesses today need a new approach to protecting information and assets that many experts call "zero-trust security."

At a recent SMB Forum event, *ChannelPro* asked three experienced providers of cybersecurity services to explain exactly what that term means and how to put it into practice with end users. Here are their thoughts on three fundamental questions about a critical concept.



# 1 WHAT IS ZERO-TRUST SECURITY?

More than a specific technology, or even a set of them, zero-trust security is a mindset in which no person, process, application, or endpoint—inside or outside the network—is considered implicitly trustworthy, and every attempt to access any resource must prove that it comes from a legitimate source with appropriate privileges.

"I think about it in terms of authentication," says Michael O'Hara, principal consultant at MEDSEC Privacy Consulting, a healthcare industry cybersecurity service provider. "What you're really looking at is who's trying to access the data, who or what has the ability and the rights to access the data, and how is that being monitored so that at any given time a person trying to access a workload, whether it's in the cloud or on-prem, is authenticated and validated."

That, in turn, is fundamentally an exercise in defining, setting, and enforcing sound policies, according to Bruce McCully, chief security officer at Nashville, Tenn.-based Galactic Networks, a managed security services provider. "What we're doing with our partners and other MSPs to help them protect themselves is really help them get to a point where they're managing these different policies and basically monitoring them for changes and abuse, rather than just throwing on more and more agents and hoping that the next anti-virus is going to protect them," he says.

O'Hara stresses the particular importance of policies that give people everything they need to do their job—but nothing more—by assigning access rights on a "least privilege necessary" basis. The same logic should apply to applications, hardware, and everything else, he adds.

"When we think about traditional least privilege, it's for users," O'Hara notes. "We don't really think about that when we're talking about our workloads or our network equipment or our servers."

# 2 WHAT ARE SOME CORE ELEMENTS OF A ZERO-TRUST SECURITY ARCHITECTURE?

There are several technologies commonly found in well-designed zero-trust environments, including identity and access management systems and whitelisting software. One that pretty much every zero-trust architecture should include, however, is disk encryption, which is available to most end users at no added cost via the BitLocker feature of Windows 10 Pro.

"It's a low-cost, high-yield solution that's going to really help secure you," O'Hara observes.

It can also frighten channel pros who worry about lost decryption keys and inaccessible data, observes Paco Lebron, CEO of Prodigy-Teks, an MSP in Chicago. "It's either that or more work for you ... if someone has stolen data, or a laptop's stolen, and you're trying to figure out how to track it down," he notes. "You'd rather have that peace of mind in that case."

McCully calls multifactor authentication another no-brainer for zero-trust environments. Indeed, according to Microsoft, organizations protected by MFA are 99.9% less likely to be compromised by cyberattacks.

Microsegmenting the network can be highly effective as well, McCully adds, citing an MSP that hosts its RMM and PSA applications locally as an example. "Instead of just having a subnet where they're up there sitting, and all of your workstations are sitting on the same wire and all of this other stuff, you create a vLAN for your workstations, a vLAN for your RMM, and a vLAN for your PSA, and you only let through the things that should be moving through the LAN inside of your firewall."

Implementing secure access service edge (SASE) solutions, which fuse security functionality with network connectivity and then deliver it via the cloud, extends the same logic to every device that connects to corporate resources, McCully notes. "Basically, you're moving the segmentation to the endpoint itself."

## READER ROI

- **ZERO-TRUST SECURITY** is an essential strategy for protecting businesses in the age of cloud computing and work from anywhere.
- **AT ITS HEART**, zero trust is a mindset in which no person, process, application, or endpoint is considered implicitly trustworthy.
- **ENCRYPTION, MFA**, and microsegmentation are all core elements of a good zero-trust architecture.
- **PENETRATION TESTS** are useful for convincing customers to invest in zero-trust technologies.

# 3 HOW DO YOU GET END USERS TO ACCEPT THE COST AND INCONVENIENCE OF ZERO-TRUST SECURITY?

As most channel pros know only too well, persuading clients that the safety conferred by MFA justifies the hassle isn't easy. Convincing them to invest money in a zero-trust architecture is usually just as hard, Lebron notes.

"A lot of them are in that space of, 'Let me throw up an anti-virus and I'll be okay,'" he says. Walking customers through the risks you're concerned about and how each one of the technologies you're proposing plays an indispensable role in mitigating those risks is the key to overcoming that false confidence.

"It's really up to us as the managed service provider to provide good talking points that are not going to go over their head and that are specific to their business," Lebron says.

McCully has had success with a related tactic: making the danger of inaction tangible by running a penetration test of the customer's environment. "It's just really, really effective as an MSP to show them what the attackers will get into if somebody on their team clicks a malicious link or something," he says.

Have a better technique? Use it. The important thing is having zero tolerance for anything more than zero trust.

# 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.*

# MSP Security No-No's

**BRUCE McCULLY** has been in the security trenches as a former MSP and now as founder and chief security officer of third-party security auditor Galactic Advisors. From his "both sides of the fence" perspective, he identifies three key mistakes with backup as the prime way MSPs are making themselves and their customers vulnerable.

First is **shared accounts**. Galactic recently helped an MSP recover data for a new customer that was hit with ransomware. The customer's previous MSP used a backup tool that required a local copy that was backed up to the cloud, which McCully says is "pretty standard," but made a mistake by backing up to a Windows Server with a shared account. "It was actually domain joined," McCully notes, "so the attackers, once they got to the domain, they just used that machine to then destroy the cloud backup."

Second is **putting RMM software on the backup device**. "Think about that for a second. If you have an event where your RMM becomes the attack vector ... now they've dropped ransomware on the backups and on the original data set at the same time. So we have a complete loss and we're not able to recover," McCully notes.

Third is **allowing users to login to their backup device** from a computer that's being backed up. "You're running the risk that the attacker has gathered your credentials and is now able to get to that backup," McCully says.

The remedy, he adds, is to implement the following best practices:

1. Build a special, micro-segmented "red" network just for your backups. There should be no shared accounts or shared passwords on that domain.
2. Only use backup tools that require multifactor authentication.
3. Designate responsibility for backup to one technician.

"When I was running my MSP, we had somebody that was responsible for backups. They were the only one logging into the backup, so the only one with the keys to the kingdom."

In addition to backup mistakes, according to McCully, many MSPs fail to implement least privilege and zero trust. For instance, he says, the average MSP gives their engineers global admin rights, including full domain and RMM access.

Solo MSPs should create two admin accounts that are separate from what they use for email and other daily tasks, McCully recommends. One admin account should use SMS-based MFA from a cellphone; this is what he calls your "break glass" account that you typically will never use. Your working admin account, which you only log into through a private browser, should use app-based MFA.

Larger MSPs should restrict global admin rights to just a few trusted individuals, who follow the same steps as above, McCully advises.—*Colleen Frye*

# 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*