Expert Guide

FOR INTEGRATORS AND SOLUTION PROVIDERS

CYBER-SECURITY

Trends and Tips

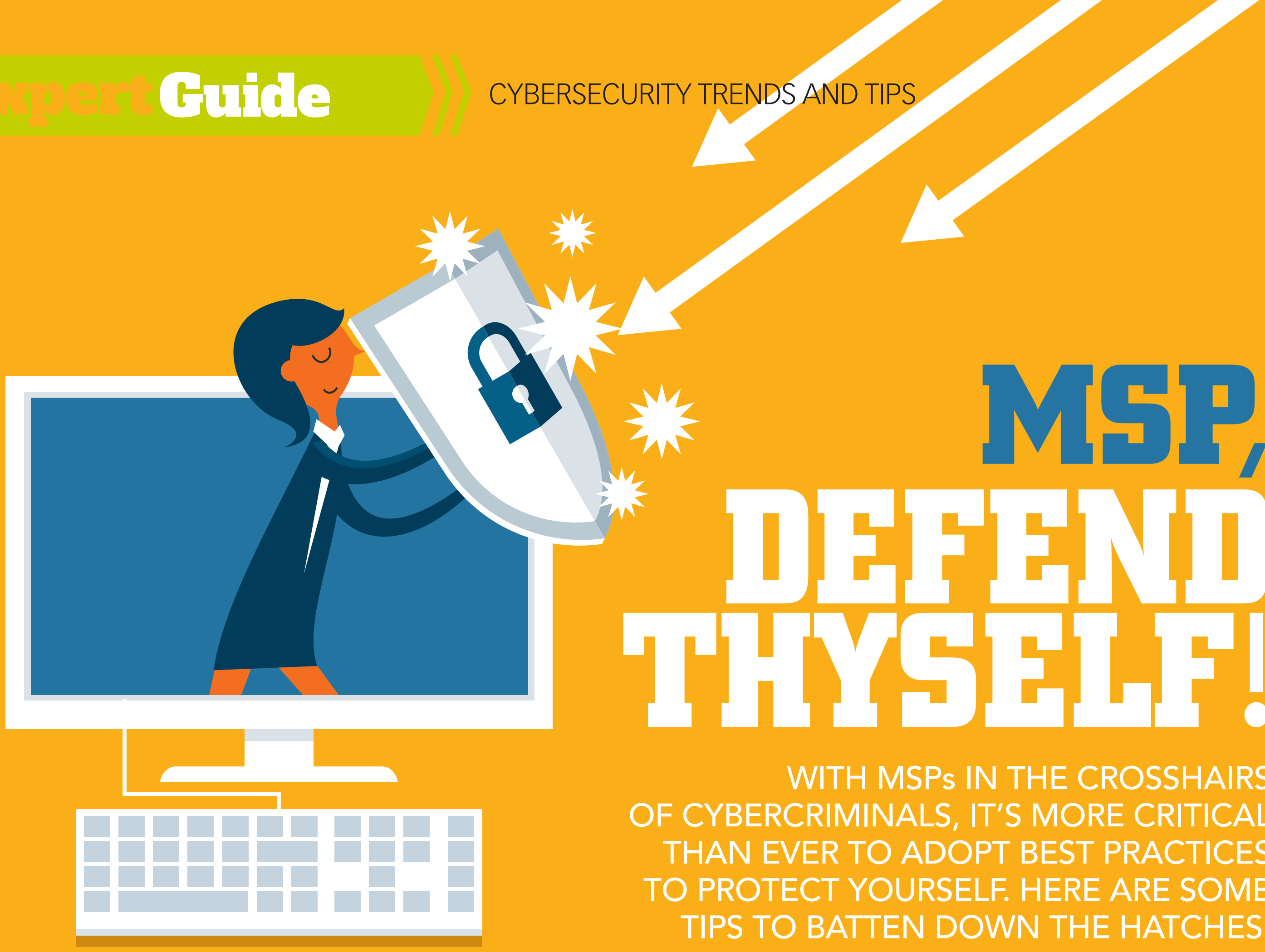
Inside

Trends in security are always in flux, but some that are top of mind for IT solution providers today include providing protection at the edge, for work-from-home environments, and for their own businesses.

This Expert Guide offers some best practices for defending against attacks on managed service providers' systems, shoring up risk management strategies to avoid lawsuits, protecting edge computing devices, and keeping remote workers safe.

POWERED BY ChannelPro
WWW.CHANNELPRONETWORK.COM

IoT playbook
WWW.IOTPLAYBOOK.COM

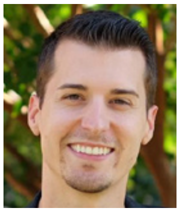


MSP, DEFEND THYSELF!

WITH MSPs IN THE CROSSHAIRS OF CYBERCRIMINALS, IT'S MORE CRITICAL THAN EVER TO ADOPT BEST PRACTICES TO PROTECT YOURSELF. HERE ARE SOME TIPS TO BATTEN DOWN THE HATCHES.

BY COLLEEN FRYE

YOU DON'T *achieve* security, says Kyle Hanslovan, "you have to constantly earn it." Continually reassessing and verifying your security posture is critical, stresses the CEO of Huntress Labs, a provider of managed threat detection and response services. However, he says, "We're not seeing MSPs do that. And we're definitely not seeing that happen in the clients' networks."



KYLE HANSLOVAN

With cybercrooks increasingly targeting MSPs for attack, it's more critical than ever to adopt best practices to defend yourself, and by extension, your clients.

Jayson Ferron, chief technologist at Interactive Security Training, agrees that a lot of MSPs are not following good security hygiene. "I hate saying this, but it's the truth," he sighs. "We know that from the forensics, but the MSP is not telling the customer, 'Hey, it's my fault.' But it really *is* your fault because you didn't follow good behavior internally."

Even more troubling, some MSPs are not being transparent when there is a breach, either in their own networks or their clients', says Jason Coffer, principal of the Coffer Group, a San Francisco-based IT and cybersecurity solutions provider. "They know about something, but they hope no one will notice. In this industry, people always eventually notice."

The Threat

The October 2019 research report *Under Attack: The State of MSP Cybersecurity in 2019*, commissioned by Continuum (acquired by ConnectWise that same month) and conducted by Vanson Bourne, found that 74% of MSPs had suffered a cyberattack in the previous 12 months, with 83% reporting that their SMB customers had suffered one as well. In addition, two-thirds of MSPs surveyed said they were worried that they wouldn't be able to defend their customers during a cyberattack.

In a reader survey *ChannelPro* conducted in June 2020, 46% of respondents said they had experienced a cyberattack on either themselves or their customers.

Why MSPs are now the targets of cybercriminals should be obvious, says Ferron, noting that a decent MSP has anywhere between 20 and 100-plus customers. "If I can get into the software that the MSP is using, I can affect 20 to 100 different companies from one attack."

SMB customers have become more attuned to the issue too, says Hanslovan, who adds that was not typically the case just a year ago. Now, he says, people are telling him "I'm leaving because my MSP was compromised,"

ILLUSTRATIONS: SORBETTO / ISTOCK

or "I have heard the MSPs can get you compromised," or "I'm considering not using an MSP and doing it in-house."

Coffer, whose firm and its customers have not experienced a security incident, has clients in the financial services sector that are subject to industry regulations, and they read the headlines. "Because our companies are regulated by the SEC, they need to do a certain amount of cybersecurity themselves, and they look to us to help them with that. But at the same time … we need to fill out due diligence questionnaires to make sure our cybersecurity standards are up to the standards they need to be, because we're their vendor and they worry about that."

Lack of Skilled Security Staff

For MSPs, part of the problem is a lack of skilled security staff and resources. According to the *ChannelPro* reader survey, 24% of respondents say they do not have enough of and/or the right skilled staff to proactively protect their own company as well as their customers. The Continuum/Vanson Bourne report had a similar finding, with more than 1 in 5 MSPs saying their organization does not have the right technical skills, certifications, and knowledge, while 40% of MSPs struggle to obtain and retain the skills necessary to deliver and sell security services.

"They don't have enough security people on board, but the problem is much bigger than MSPs," Hanslovan says, "because there is so [little] security talent [and] you have inflation of security salaries. So the reality is MSPs just can't afford truly great security talent."

That said, Hanslovan and others say MSPs *can and should* improve their security posture by adhering to the following best practices:

DETERMINE YOUR BASELINE

MSPs need to know what they've got on their network and how it's configured, Ferron says. Auvik, IT Glue, RapidFire Tools, and others make solutions that can assist with this process. Smaller MSPs, Ferron notes, can access a free network scanning tool like Nmap. "It'll show you all the computers it sees. It'll tell you what ports and services are running on those machines. If you don't know what's running on your network right now, how are you going to know when it changed? And guess what, Mr. MSP, you should be doing exactly the same thing for your customers."

ADOPT A SECURITY FRAMEWORK

Ali Zadeh, CISSP, CISM, CISA, who leads the cybersecurity practice at the Coffer Group, recommends following a security framework like the customized version of the NIST Cybersecurity Framework that his firm uses. "I personally believe that if you're not using a security framework, you don't have a security program," he says. "You have to start with the framework, customize it, and then based on that you build your policies."

IMPLEMENT LAYERED SECURITY

Layered security is the mantra for most MSPs these days. For Coffer that includes anti-virus, DNS filtering, multifactor authentication, mobile device management, encryption, complex and unique passwords, single sign-on, dark web monitoring, auditing, logging, and more. Coffer Group has partnered with third-party specialists for its security operations center (SOC) and 24/7 monitoring as well.

CHANGE YOUR DNS

Ferron recommends changing your DNS to a managed DNS server, such as OpenDNS from Cisco or others. "That way, if your machine wants to go somewhere that OpenDNS or any of these managed DNS providers [know is a bad location] it will block it."

Furthermore, Ferron says, have your firewall only allow DNS traffic from the DNS server, "which means that if a machine gets infected and it wants to query DNS and bypass the company, the firewall says 'no, no, no, you can't do that.'"

REMOVE THE LOW-HANGING FRUIT

While Hanslovan says humans are the weakest link security-wise, "there's still low-hanging fruit like misconfigured services and unpatched things. … Misconfigurations is a big one; that was one that Verizon actually called out." Indeed, Verizon's *2020 Data Breach Investigations Report* found misconfigurations were up nearly 5% from the last study.

Coffer stresses the importance of patch management, which goes beyond patching a product and assuming it's doing its job. "Making sure things don't fall through the cracks is really important," he says. "So first you build on a good RMM tool that can patch those things properly and automate the process."

He recommends using a Splunk-type tool to aggregate information from multiple sources as well. "The RMM provides a lot of information, but there's other information that goes beyond what the RMM provides."

Hanslovan says "self-investment" is one of the most important steps an MSP can take, starting by learning how to use all the built-in security in their RMM such as group policies and configuration management. "They're not hardening their environments and they're not using group policies. They're also not minimizing their attack surface. … If they did know how to use what they were already paying for, they could provide better encompassing security."

UTILIZE A SECURE DOCUMENTATION/PASSWORD MANAGEMENT SYSTEM

"One of the biggest problems that MSPs have is all the shared accounts," says Zadeh. In addition to minimizing those, he recommends storing credentials, customer data, project information, IP network information, and more in a documentation system, or what he calls a "secure vault." This type of database allows you to enable multifactor authentication, change passwords, and have an audit trail, he says. Examples include SolarWinds Passportal, IT Glue, and others.

DON'T SACRIFICE SECURITY FOR SHINY THINGS OR EASE OF USE

Built-in security factors high in vendor selection for the Coffer Group. "If they said we don't do multifactor, we would just say forget about it, we're not even working with you," explains Coffer, who adds that he recently passed on a promising new company's product because it wasn't SOC 2 certified. "It's a high hurdle that they have to get over because that's ultimately our liability too if their product doesn't work in a safe and secure manner."

Zadeh adds that MSPs need to resist the temptation to sacrifice security "to gain access to a tool that can make things much, much easier for you."

WEIGH THE BENEFITS OF A SOC 2 AUDIT

Becoming SOC 2 compliant can be time consuming and expensive, so Hanslovan recommends weighing its applicability to your business. "It will make you better, but you should figure out what is most important, like Maslow's hierarchy of needs." For instance, do your customers require SOC 2? Do they see the value in it? Will it allow you to increase your revenue and the service you deliver? Get SOC 2 certification only if you answer yes to such questions, Hanslovan stresses.

HAVE AN INCIDENT RESPONSE PLAN

Create an incident response plan *before* you have an incident, advises Zadeh.

Adds Coffer, "We want to have [a plan] in place so we know what our obligations are internally, who we need to notify internally to get things forward, and if and when there's a need, who do we notify, and under what circumstances, [at] the client, as well as understanding the severity of something, so we know how quickly we need to respond, what information we need to gather."

If there is an incident, speed of response is important, he says, so having a plan ready "is really valuable."

IMPLEMENT SECURITY AWARENESS TRAINING

Security awareness is a challenge for almost all MSPs, Zadeh says, so he recommends training employees with "a program just like we do for our clients. It's really important internally that everyone knows to look for the warning signs" in emails and phone calls. Keeping employees up to date on the latest scams and best practices should be ongoing too, he adds.

GET CYBER INSURANCE

Cyber insurance isn't optional anymore if you're an MSP, stresses Hanslovan.

The Continuum/Vanson Bourne research found that 43% of MSPs claim that their organization would be held solely accountable if one of their customers experienced a cyberattack. Additionally, 83% said that their customers would take legal action against them in the event of a cyberattack.

ChannelPro's reader survey found that more than 43% of respondents have cyber insurance, but nearly 17% worry that it isn't enough.

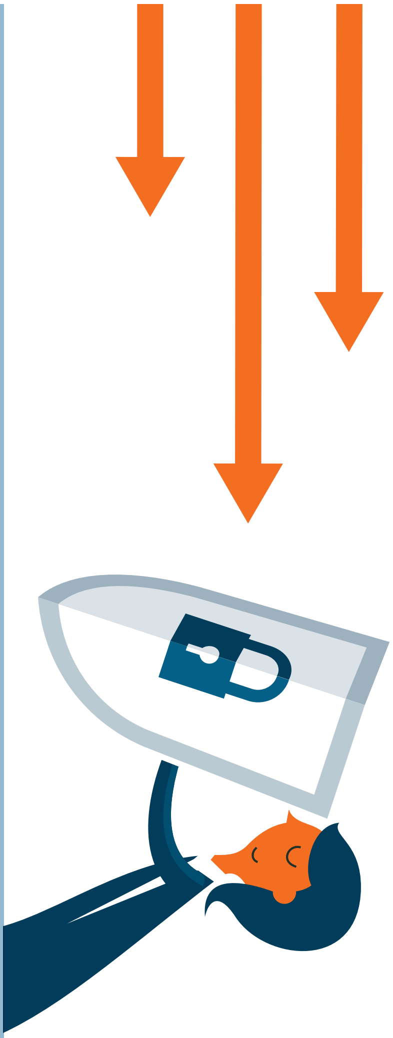
Indeed, Hanslovan says insurers are scrutinizing claims more. "They're starting to pay out much different. [In] 2019, insurance was paying out claims like there was no tomorrow." Now, he says, cyber-insurance companies are doing more forensics on incidents to determine if the MSP was negligent or at fault. "They're actually calling their own incident responders in to represent the insurance [company] to help figure out who is negligent."

For Coffer, his company has cyber-security insurance because it is "an expectation." However, he says, while that provides peace of mind to customers and protects them after the fact, his top priority is prevention. "Our focus is really to secure our systems and to make sure our employees understand what to watch out for and to follow proper procedures."

STAY INFORMED

With attack vectors and techniques constantly changing, Ferron recommends that every MSP join InfraGard, a partnership between the FBI and the private sector, that shares information on cyberattacks.

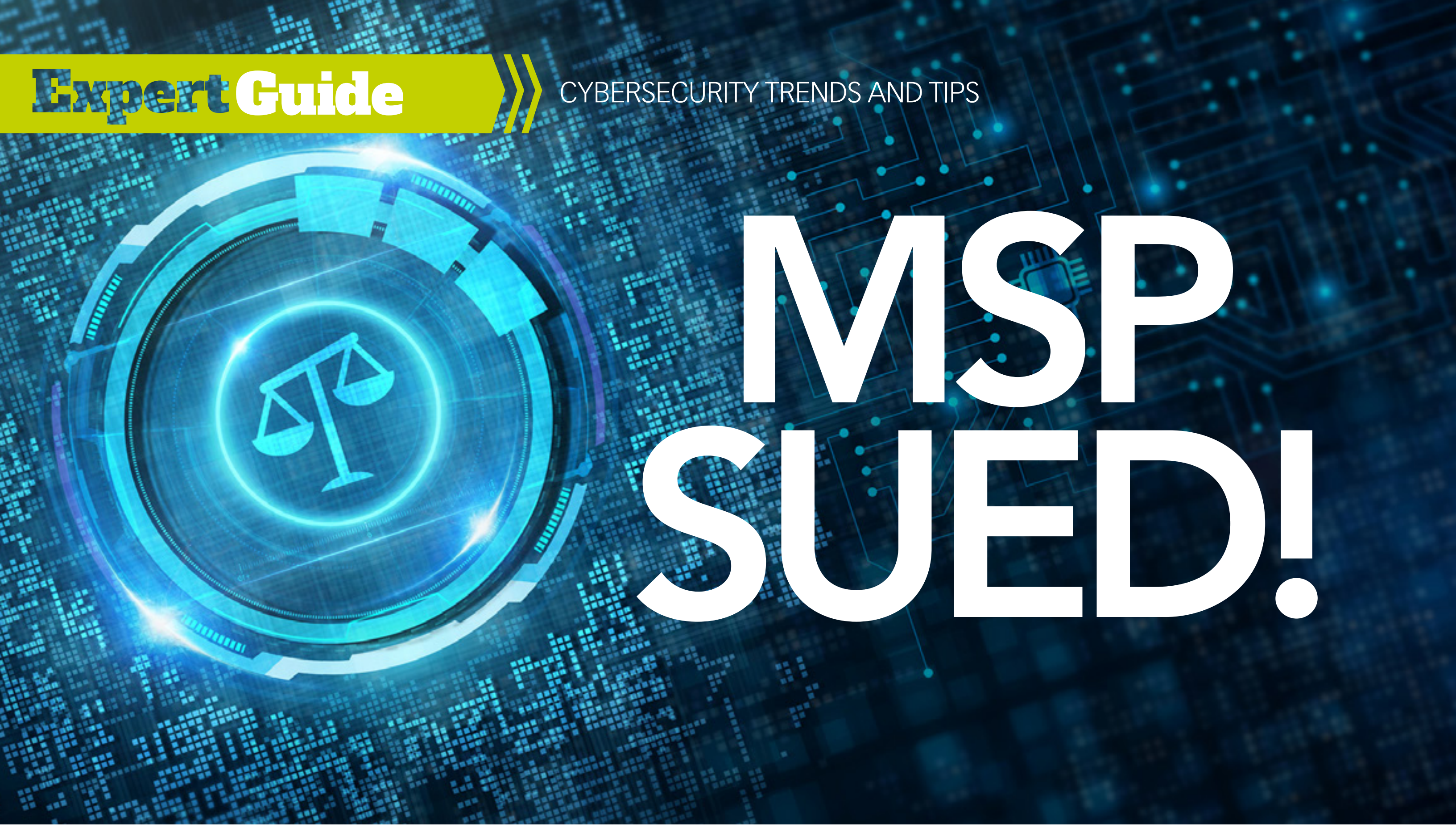
Another resource is the MSP information sharing and analysis center (MSP-ISAC) formed by Datto, Huntress, ConnectWise, and Kaseya last summer, and since joined by numerous other vendors who exchange threat information through a Slack channel. The TSP-ISAO, created by ConnectWise last year and now run by CompTIA, is an option as well.



A New World

The security threat landscape has changed a lot since many MSPs got into the business, and it continues to demand more from them as they work to protect themselves and their clients, says Ferron. "If you think about the history of MSPs, they were break-fix … Now we're asking the MSPs to learn new technologies on security, and then they've got to convince their customer to buy this new offering, to help them secure their environment. That also means that they have to have people inside their building who understand security, who understand alerts, who understand incident response."

There's no sugar coating the challenge, Hanslovan says. "The reality is it's just such a big problem that I would like to see more investment in people, more investment in the basics."



MSP SUED!

PHOTO: PUTILICH / iSTOCK

ARE YOU READY?

HERE ARE 10 RISK MANAGEMENT STRATEGIES TO SAVE YOUR REPUTATION, YOUR MIND, AND YOUR RETIREMENT.

BY MIKE SEMEL

WARREN BUFFETT SAID, "It takes 20 years to build a reputation and five minutes to ruin it. If you think about that, you'll do things differently." Translation: As an MSP, you need to protect yourself from yourself, because you could lose everything if you are sued.

This January, MSP Involta was sued by Boardman Molded Products, after the Ohio manufacturing company fell for a fake invoice phishing scam and lost $1.7 million. The lawsuit said that the MSP should have warned the customer about phishing and mishandled the work ticket after the client reported the incident. It also stated that the MSP "was in charge of maintaining a secure environment and was to set security rules accordingly."

The lawsuit includes specific allegations that Involta failed to conduct promised quarterly business reviews and to ensure anti-virus software was installed on all of the client's systems. An audit showed systems missing anti-virus protection.

The lawsuit was not just about what was promised in the MSP's legal agreement, which contained a lot of fine print. It quotes the MSP's marketing claims to show potential jurors what the customer was promised. According to the lawsuit, Involta sold Boardman on the fact it would be their "one-stop shop for all IT needs." The suit refers to Involta's website terms and conditions, which said that Involta claimed "there would be no need for any other service providers for any purpose ... Let your staff focus on innovation and business-oriented tasks ..."

If that sounds familiar, follow these steps to protect your business:

1. ALWAYS USE A CONTRACT

Never provide *any* service without a signed, written contract, and always have your contract created by an attorney familiar with the MSP industry, your business, and the laws of your state. Your contract should protect your company, state the scope and scale of your work, include any responsibilities shared with the client, and limit your risks.

2. LIMIT YOUR EXPOSURE

Clearly state what is and isn't included in your managed service fees and what services you are offering (don't overpromise). Include what is *not* your responsibility or covered under the cost of your services, and what might prevent you from delivering the services, like the COVID-19 pandemic.

If you cause a data breach, take responsibility for it, but don't get dragged into a client's mess.

You should also state that cybersecurity and regulatory compliance are shared responsibilities, and that your client is responsible for their users and ensuring their own compliance. You may be able to help them with that for an additional fee.

3. LIMIT YOUR LIABILITY

Limit your liability for managed services to just one to two months of fees paid by your client. Make sure you aren't responsible for consequential damages that result from your failure. That means that if the client loses $1.7 million in a fake email scam, you are not responsible for their loss. It also means that if your client gets hit with ransomware, and misses a bid deadline, for instance, you aren't responsible for the resulting business losses or penalties.

4. ALIGN YOUR MARKETING AND SALES WITH YOUR CONTRACT

This is a BIG deal. You can't assume that the fine print in your contract will protect you from the claims you make on your website; what you, your sales reps, and your technical folks tell prospects and clients; and what you put in your proposals. Remove any language that promises things like: "We will take care of your IT so you don't have to worry about it."

5. AUDIT YOUR SERVICE DELIVERY

Imagine receiving a lawsuit and reading in a legal document that your company had not installed anti-virus protection on all the client's computers, and that you had never done a QBR, as promised in your marketing and contracts. How mad would you be at your team and at yourself?

Perform internal audits twice a year for each of your clients and have hard discussions with your team if the reports show gaps, such as missing security patches—and then address those gaps immediately.

6. DON'T INVESTIGATE INCIDENTS (WHICH DOESN'T MEAN YOU SHOULDN'T RESPOND)

I'm not suggesting that you not respond to an incident, but it isn't your role to *investigate* it.

Hacking and ransomware are crimes. They often result in criminal investigations and lawsuits, and you may be sued because of your responsibility to manage the client's network. Never touch any evidence because it may be used against you.

So what *should* you do?

- Contain the incident by disconnecting devices, shutting down services, etc.
- Tell your client to get their attorney involved, right from the beginning.

Advise your client to follow the U.S. Department of Justice's recommendations in its "Best Practices for Victim Response and Reporting of Cyber Incidents."

Note that your client's cyber insurance will determine what lawyers and forensic experts will be hired and paid. You may end up doing a lot of work for free if you aren't a preapproved forensics company authorized by your client's insurance company.

Also, make sure that none of your employees talk to a client after a reported breach, scam, or ransomware attack until you have been informed and have talked with your attorney about your risks and how you should proceed.

7. BE COMPLIANT WITH REGULATIONS

Laws require you to comply with regulations based on the services you provide and the clients you service. Advertising your compliance or placing a seal on your website is not a substitute for thoroughly following the applicable regulations.

Implementing the NIST Cybersecurity Framework (NIST CSF) in your own business, and aligning your managed services to the NIST CSF, will help you sell more services, deliver a high level of security, and stand up to the scrutiny of an audit, breach investigation, or lawsuit.

8. BE CONSISTENT

Consistency is required in cybersecurity and compliance. Schedule and repeat regular audits. Spot-check your service delivery. Train your employees and hold them all to high standards.

9. TAKE FULL OWNERSHIP (YOU *ARE* THE OWNER)

Get hands-on. Check the work of even your best employees. Validate that things like anti-virus are consistently managed, that you are delivering on your QBRs, and that you have documentation to prove everything.

10. HAVE GREAT INSURANCE, BUT DON'T ASSUME IT WILL COVER YOU

You may think Errors & Omissions (E&O) insurance will protect you. Don't be so sure.

My company has a good E&O insurance policy underwritten through Lloyds of London. I worked hard with my agent to make sure it had the coverages I need to pay legal fees if I am sued and to cover any settlements if we screw up and must settle a claim.

It's a great policy, but the following exclusion means that it will not pay if we don't do what is expected of us or we fail to deliver things we promised:

> ***The coverage under this Policy will not apply to any Loss arising out of:***
>
> ***Deceptive Business Practices****, Antitrust & Consumer Protection—****any actual or alleged false, deceptive or unfair trade practices****, antitrust violation, restraint of trade, unfair competition, violation of consumer protection law,* ***false, deceptive or misleading advertising****, inaccurate cost estimates or* ***failure of goods or services to conform with any represented quality or performance****.*

This means you can't insure yourself out of claiming that you will deliver services and then not doing it consistently or at the quality level you promised. You must deliver every day, which is why I religiously follow these 10 steps in my business.

MIKE SEMEL *is a former MSP and founder of Semel Consulting, which provides advisory services to MSPs and end users for compliance, cybersecurity, and business continuity planning.*

SECURING THE EDGE

Edge computing solutions are highly powerful and highly vulnerable. Here's how to protect them. By Rich Freeman

THERE'S GOLD out there at the edge of the network.

From factories and power plants to smart buildings and beyond, businesses are increasingly using data from sensors, cameras, and other Internet of Things devices to drive real-time action in ways that increase efficiency and create new revenue streams.

Along the way, however, they're adding hundreds and sometimes thousands of tempting targets to already vulnerable networks. Indeed, protecting edge computing hardware takes all the security challenges channel pros already know and compounds them with a bunch of new ones.

"They're lower-cost devices, there's a lot more of them, and they're at remote locations," says Ivan O'Connor, head of IoT at ActionPoint, a multinational software development and managed IT services provider based in Limerick, Ireland. "Those three factors alone make edge device security a tough nut to crack."

And there's more to edge security than just devices. The cloud solutions those devices connect to and the networks they employ to communicate with the cloud are potential attack surfaces as well. O'Connor and others with edge experience agree, however, that any IT provider familiar with the basic rules of edge security can successfully offer it.

"As long as you commit to those principles, there are very good platforms out there to do it with now," O'Connor says. "There isn't any rocket science involved here."

Inventory and Assess

The volume and widely dispersed location of edge solutions aren't the only reasons they're difficult to protect. Security is often an afterthought among manufacturers of edge hardware, and few edge devices can accommodate endpoint security software. Managing edge devices, moreover, isn't as easy as managing a laptop or smartphone.

"They mostly don't have a user interface," observes Ben Frame, vice president of product at ClearObject, an IoT solution provider based in Fishers, Ind.

BEN FRAME

To make matters worse, edge deployments in industries like manufacturing and transportation are often overseen by operational technology (OT) professionals who aren't as well versed in security as their IT counterparts. "They may understand physical security, but cybersecurity is something that is often new to them or is not well understood," observes Barry Dellecese, senior director at Stratus Technologies, an edge computing integrator headquartered in Maynard, Mass.

Tackling problems like those, he continues, should begin with a security audit aimed at inventorying edge assets and assessing their exposure. "You'll look at where your

PHOTO: ONURDONGEL ISTOCK

threats are or where your potential vulnerabilities are, both physical and digital, and then begin thinking about what is going to be your plan to either accept those risks or put in place remediation plans so you can reduce the risk," says Dellecese, adding that OT should participate in that process.

Gateways and Encryption

Those remediation plans should encompass edge devices, cloud solutions, and the networks that link them. Start with the hardware by performing basics like changing default administrator passwords set by the hardware maker. If a device has built-in security features like a secure bootloader, which verifies the authenticity of firmware before running it, make sure they're enabled.

ActionPoint then takes an extra step. "We typically push a Windows 10 IoT gateway in there as the gatekeeper for the sensors," O'Connor says. To make that unit as tamper-proof as possible, he continues, technicians enable its Trusted Platform Module feature, lock down any unnecessary ports, and ensure that only outbound connections to the cloud are permitted.

If possible, counsels Prakash Sangam, founder and principal of IT advisory firm Tantra Analyst, employ LTE or 5G networks rather than Wi-Fi to connect edge devices to the cloud. Mobile carriers typically encrypt data and authenticate users effectively, he notes. "If you're using Wi-Fi then there are a lot of ways it could be hacked."

Don't rely solely on mobile providers for encryption, though. Secure edge solutions use it all the way from the sensors to the cloud. "Encryption is a big deal," Frame says. "We want to encrypt data in transit and we want to encrypt data at rest."

Cloud platforms like AWS IoT Core, from Amazon Web Services, Google Cloud IoT Core, and Microsoft Azure IoT Central all offer encryption for data at rest, along with a host of other essential security features, such as over-the-air patch management for edge hardware.

"It's not a question of if, but *when* those devices will need to be updated," Frame notes. "We want to make sure that that process is robust." All three leading IoT platforms are also relatively easy to learn, he adds, and include APIs you can use to integrate them with your other management systems.

ActionPoint, once again, goes a little further than many of its peers by segregating customer data in dedicated cloud instances. "That's not something that every IoT solution provider does," O'Connor says. "Some solution providers kind of provide a SaaS model where all data goes into one tenancy, and then there's authenticated access to that data." Storing each client's data separately, however, provides an extra bit of safety that clients worried about cloud security find reassuring.

Training and Policies

Even the best tools can't safeguard edge solutions alone, however. "A lot of it's about the people and process before you get to technology," Dellecese observes. Getting the people piece of the formula right is mostly about giving users security awareness training on a regular basis. The process part entails setting policies in areas like access management that limit permissions to people who truly need them, and carefully controlling access by outside third parties.

Those are principles familiar to most channel pros already, however, and there's no shortage of relevant and effective edge security technologies out there. "There really is no reason for any systems integrator or solution provider to not be able to build a highly secure system," O'Connor says.

He continues, "Yes, it may take a little bit longer time and it may cost the customer a little bit more in terms of the upfront build and the ongoing service costs, but all of those modules are there and they're pretty accessible."

READER ROI

THE IoT HARDWARE, broadband connections, and cloud platforms that form edge computing solutions introduce a host of vulnerabilities for hackers to exploit.

AN EFFECTIVE EDGE SECURITY STRATEGY starts with a thorough asset inventory and risk assessment process.

ENCRYPTING DATA in transit and at rest is also essential.

LEADING CLOUD VENDORS like Microsoft, Amazon Web Services, and Google all offer solutions that make managing edge solutions significantly easier.

SECURITY AWARENESS TRAINING and smart policy-setting must factor into edge security strategies as well.

MAKING WORK-FROM-HOME SECURITY WORK

Six months after COVID-19 turned office dwellers into instant telecommuters, best practices for protecting remote workers are coming into focus. By Rich Freeman

JOSHUA LIBERMAN still remembers the first work-from-home (WFH) PC he helped set up for a client. It belonged to the CEO of a $15 million business who had owned it for 14 years, shared it with other family members, and used it on a Wi-Fi network without even WPA in place. The device had anti-virus software, but the license had expired roughly seven years earlier.

For Liberman, who is president of Albuquerque, N.M.-based solution provider and MSP Net Sciences, that was just the beginning of a wider, now familiar challenge.

“We had this kind of perfect storm where we had to provide access to genuinely terrible machines on miserable networks and insecure connections,” recalls Liberman of those frantic early days after COVID-19’s arrival. “Security was an afterthought. We had to connect people first and there was just no chance that we were going to get the time, much less presence in the home, to do the things we needed to do to truly secure these connections.”

Hard as it is to believe, however, half a year has passed since coronavirus-inspired lockdowns first turned millions of office dwellers into instant telecommuters. Channel pros like Liberman have used those months to learn valuable lessons about keeping remote workers safe.

ILLUSTRATION: ANILYANIK / ISTOCK

Tremendous Risk

Good thing too, because WFH employees are not only using personal PCs on unprotected networks, they’re doing so with kids underfoot, a recession underway, and the path toward an end to the pandemic still far from clear—all of which makes them ripe targets for hackers.

“You have users who are in various states of certainty and uncertainty, and the bad guys know this,” says Rob Boles, president of BLOKWORX, a managed security service provider with offices in Arbuckle and Larkspur, Calif. That’s one reason ransomware attacks were up 109% year over year in the U.S. during the first half of 2020, according to SonicWall.

Simply waiting out that cybercrime wave isn’t an option either, because the WFH phenomenon is here to stay. Indeed, businesses globally expect 25% of their staff to work remotely even after COVID-19 is behind us, according to a July study by network and application performance management vendor Riverbed.

Safeguarding remote workers now and into the future, experts say, begins with the basics, like deploying endpoint security and DNS filtering systems on home-based endpoints, and patching those devices. Multifactor authentication software is a must too, according to Rory Sanchez, CEO of True Digital Security, a security solution provider with locations in Florida, New York, and Oklahoma.

"Almost every phishing attack that we've seen could have been prevented with multifactor authentication," he says.

If your customers use Microsoft's remote desktop protocol (RDP) technology to connect with office PCs, turn your attention there next. Too many channel pros desperate to get clients online earlier in the year used unsecured RDP connections. "I literally as an operator cannot count the times in the last six months that we've been called to remediate or help clean up an environment because of ransomware due to RDP open to the internet," Boles says. "The risk is tremendous."

A good, solid VPN solution will help mitigate that risk, but proxied RDP services, like the one from TruGrid that Liberman uses, are an option too. Such systems redirect RDP traffic to cloud-hosted servers that inspect and clean it before sending it to its destination. They also share reporting data.

"We can get alerts about multiple failed connections. We can get alerts about what I call 'geofence hopping,' or basically connections that are coming from IPs or regions that they shouldn't be," Liberman explains.

Scott Beck, CEO of Riverview, New Brunswick-based MSP BeckTek, took a different approach, using the remote access software included with his RMM solution rather than RDP to connect personal endpoints to the office, and then blocking all file transfers from the local machine. "So basically, we turned a home PC into a TV with a keyboard and a mouse," Beck says. "That's how we got them into the network securely without having to worry too much about their actual device."

Sanchez has an even simpler suggestion: Replace your customer's physical desktops with cloud-based ones. Solutions like Windows Virtual Desktop and Amazon WorkSpaces, he notes, make RDP and technologies like it unnecessary.

> "Almost every phishing attack that we've seen could have been prevented with multifactor authentication."

RORY SANCHEZ
CEO, True Digital Security

Stacking More Gains

When stay-at-home orders first went into effect six months ago, getting clients online fast was job No. 1. With that initial scramble now long since over, however, helping users work safely from home should be the new priority.

According to Boles, establishing a clearly articulated policy for secure WFH computing is a great place to start that process. "If there's no security policy, everything else doesn't matter," he says, adding that deploying next-generation firewalls with sandboxing functionality and zero-day protection is a wise next step. BLOKWORX uses such products to perform health checks on remote hardware attempting to join the network.

"Before the device can even connect, we're querying for patch status and that the security software is intact, basically that the profile and machine is what we want it to be," says Boles, who also advises channel pros to segment home networks that support smart thermostats and door locks in addition to WFH devices.

Sanchez recommends carefully rechecking the permissions assigned to work-from-home gear and other security settings. "Lots of things were deployed quickly," he notes, and giving devices excess rights can be tempting when time is short. Putting rigorous change management processes in place, Sanchez continues, can help stop configuration errors from endangering customers in the future.

Longer-term plans should include layering in data security software, data loss prevention solutions, dark web monitoring, and security awareness training systems. "Each one by itself might not be huge, but stacking those types of things is where you make your gains," Boles says.

You might be surprised at how willing even your most tight-fisted customers are to pay for those gains, too. Beck is one of many channel pros who've been pleasantly surprised at how open-minded businesses are lately about investing in better security.

"If you haven't had that conversation around security because you were worried that your client might not want to spend on it or might go away, this is the time to start having that talk," Beck says. "Do it now before it's too late, because bad things are going to continue to happen."

READER ROI

IN THE SIX MONTHS since coronavirus lockdown orders went into effect, channel pros have learned valuable lessons about secure work-from-home computing.

ENSURING THAT BASICS like endpoint protection, DNS filtering, and multifactor authentication are in place is an essential first step.

REMOTE ACCESS SYSTEMS and proxied RDP solutions are effective ways to help remote workers use Microsoft's Remote Desktop Protocol safely.

SETTING CLEAR POLICIES, implementing change management, and layering in additional solutions should be core elements of a longer-term WFH security plan.