Expert Guide

FOR INTEGRATORS AND SOLUTION PROVIDERS

SECURITY in a Work-from-Anywhere World

Inside

The hybrid workforce is shaping up to be a widely adopted model for businesses of all sizes. Two challenges for channel pros are protecting workers accessing the corporate network from anywhere, and keeping organizations' cloud-based applications, servers, and storage repositories safe from attackers.

This Expert Guide includes tips on building a work-from home security stack, a look at the IoT security minefield (and opportunity), some best practices for cloud security, and a first-hand account of how one channel pro is expanding the circle of safety for her business, customers, and employees.

POWERED BY ChannelPro
WWW.CHANNELPRONETWORK.COM

IoT playbook
WWW.IOTPLAYBOOK.COM

ILLUSTRATION: FEODORA CHIOSEA / ISTOCK

BUILDING THE ULTIMATE WORK-FROM-HOME SECURITY STACK

BY RICH FREEMAN

While there's no one perfect recipe for protecting remote employees, channel pros have learned a lot in the last year about what works best.

OUT OF SIGHT, out of mind, the saying goes. Thanks to COVID-19, however, most channel pros are positively obsessed with what they *can't* see these days.

That's because their clients are still mostly working remotely, beyond the reach of the email gateways, content filtering systems, firewalls, and other technologies that protect them at the office. "Once users are out of that environment and they're using their devices at home, we no longer have any visibility or control," says Stanley Kaytovich, director of operations at QWERTY Concepts, an MSP in Piscataway, N.J.

Cybercriminals, moreover, are well aware of that fact. Indeed, malware attacks generally jumped 358% in 2020 and ransomware attempts specifically rose 435%, according to endpoint and mobile security vendor Deep Instinct, due in part to the rise of work-from-home (WFH) computing.

Confronted without warning last spring by the coronavirus pandemic, IT providers improvised remote work arrangements for their customers in a hurry. They've been refining the security measures they put in place in those same hectic days ever since. Along the way, they've learned a lot about what makes WFH security unique and how best to construct a layered work-from-home security strategy.

Continual Headaches

Inadequate visibility and control are just part of what makes securing home-based employees so difficult. Their ever-changing, unpredictable hours as they juggle childcare with work make the pattern analysis many security solutions rely on to distinguish normal from suspicious user behavior difficult as well.

Worse yet, many SMBs have been relying on Microsoft's Remote Desktop Protocol to connect homebound employees with office resources despite RDP's well-known vulnerabilities. In fact, security software maker Kaspersky observed a 242% leap in brute force attacks against RDP in 2020. "Honeypot" servers set up by researchers at security vendor Sophos last year, meanwhile, received a median average 467,000 RDP login attempts each over a 30-day period. That's about 600 an hour, or one every six seconds.

Unauthorized apps have been a continual headache too, according to Lawrence Cruciana, president of Corporate Information Technologies, a provider of security and managed IT services headquartered in Charlotte, N.C. For example, he notes, users have been holding meetings on conferencing solutions other than approved systems like Teams and Zoom. "We started seeing that kind of blossom in software audits," he says. "There were some we'd never even heard of."

The worst problem of all, though, is also the most familiar to channel pros: users doing business on home PCs with consumer rather than business-grade security software onboard, or perhaps none at all. Making matters thornier, remote workers often switch back and forth between corporate and personal devices at will—and without notifying their employer.

> "In many cases, when employees are using their own systems you might not know about it until after credentials have been compromised [and] information has been breached."
>
> **KEVIN BEAVER** Founder and Principal Consultant, Principle Logic

"In many cases, when employees are using their own systems you might not know about it until after credentials have been compromised [and] information has been breached," notes Kevin Beaver, founder and principal consultant of Principle Logic, a security consultancy based in Acworth, Ga.

To address issues like those, channel pros must embrace a combination of tools and techniques built around four fundamental objectives.

1 PROTECT THE DATA

NANCY SABINO

Ultimately, everything in your work-from-home security stack is about protecting data, because data is the most valuable and coveted asset your customers have. Keeping data safe begins with encrypting it, according to Nancy Sabino, CEO of SabinoCompTech, a security and support services provider in Katy, Texas.

"Whether it's a laptop or a desktop, if it's going home with a user then it needs to be encrypted, because someone could break into their house and steal that device," she says. Encrypting data also allows companies to avoid the financial fallout and reputation damage that inevitably follow publicly disclosing a breach, something most data privacy regulations require businesses to do.

BitLocker, a drive encryption feature provided free with Windows 10 Pro and Windows 10 Enterprise licenses, is an obvious place to start, but protects only data "at rest" on an individual device. A wide variety of business-oriented encryption solutions keep data free from snooping "in transit" between devices as well.

2 PROTECT THE ENDPOINT

LAWRENCE CRUCIANA

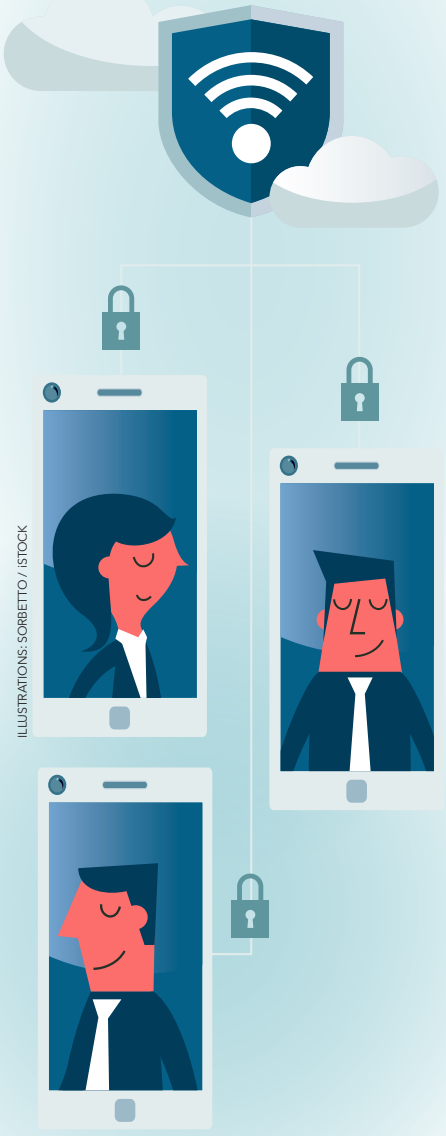
It probably goes without saying that every desktop, laptop, or other device used for work at home should have an enterprise-caliber endpoint security system on it and at least a local firewall enabled. Cruciana recommends making DNS filtering software mandatory too, and further advises choosing a product that users can't easily shut off or bypass. "It's not that we want to be the internet police, but we want to make sure that we're not introducing additional risk," he says.

Software for managing endpoints, like an RMM solution, is critical as well, Cruciana adds. "At a minimum, we're doing daily software and configuration audits of the device, [and] limiting and restricting the use of administrative access on those endpoints so that users aren't able to go and install software and make changes."

Sabino, for her part, leans on mobile device management software to ensure that she can lock or wipe work-from-home hardware if it's lost or stolen, or if its owner changes jobs. Though Sabino uses Intune, Microsoft's single-tenant MDM offering, alternatives with the multitenant management capabilities MSPs require are available from vendors like VMware and SolarWinds MSP.

Cruciana, meanwhile, employed an increasingly popular shortcut last year to secure devices for some of his clients with especially strict regulatory requirements: a virtual desktop solution. Products like Windows Virtual Desktop centralize potentially vulnerable resources in a heavily fortified Microsoft data center. "In the right client set, that obviated the need for a lot of the stuff on the endpoint," Cruciana notes.

3 PROTECT THE NETWORK



ILLUSTRATIONS: SORBETTO / ISTOCK

Perhaps the most unnerving moments in securing WFH clients are when you know someone is connected to their network, but you're not sure who. That makes identity and access management software, or at least a good password management system, especially important with remote users.

"We find a lot of people are writing down their passwords on Post-it notes," says Kaytovich. Too many of them have been using short, obvious passwords too, so QWERTY now pushes users to adopt more effective replacements. "They don't like typing in long and complex passwords, but ultimately the longer and the more complicated the password, the harder it is to breach," Kaytovich notes.

Multifactor authentication software can further help channel pros prevent imposters from slipping into customer networks. According to Microsoft, in fact, organizations protected by MFA are 99.9% less likely to be compromised. Kaytovich is a believer in the technology as well but, like many channel pros, struggles to convince clients that the extra safety makes the hassle worthwhile.

"For the last three months, we've been trying to roll out MFA for [Microsoft] 365 to all of our clients, and we're getting a lot of resistance," he says. "People don't want to enter codes. They don't want to use their mobile device." The only answer, he and others say, is to tell customers that like it or not, MFA is an obligatory fact of life these days, whether you're accessing your personal checking account online or a corporate file share.

RDP, by contrast, is increasingly avoidable, and most channel pros have phased it out in favor of VPN services. Where that isn't possible, secure RDP services from providers like PC Matic and TruGrid enable end users to employ the Microsoft protocol more safely.

Kaytovich, meanwhile, explicitly bars WFH users on personal hardware from utilizing RDP or VPN. "If this was a business-owned device, it would inherit the permissions and the security policies from the business network. If it's a home device, unfortunately, there's no way for us, without managing it, to be able to enforce that," he says. In such cases, therefore, Kaytovich lets employees open SSL-protected connections to the network via the remote access software included with the RMM platform his company uses, which also requires MFA.

Sabino further mitigates the risks that come from linking personal LANs to corporate ones by separating business traffic on home networks from everything else—especially if the user in question has teenaged children. "I have a teenager at home myself," she says. "They're getting smarter and they're starting to learn how to get past certain security [measures]." Most consumer routers have built-in segmentation functionality these days, Sabino adds.

READER ROI

WORK-FROM-HOME devices and networks are vulnerable to attack and difficult to monitor, manage, and secure.

TO OVERCOME THAT CHALLENGE, channel pros must employ a layered combination of tools and techniques to secure data, endpoints, networks, and network connections.

CLEARLY WRITTEN and firmly enforced policies are an essential part of WFH security strategies, along with ongoing security awareness training.

IT PROVIDERS should protect their own remote workers with the same technologies and best practices they use with customers.

4 PROTECT THE USERS

Strictly speaking, the goal in this part of a work-from-home security strategy isn't protecting users from attackers so much as protecting businesses from their users. That begins with setting clear rules of the remote work road, and enforcing them rigorously.

"Your documented security policies are worthless unless you have something to back them up," Beaver observes.

Written policies concerning personal hardware are particularly critical, according to Sabino, who insists that her customers give remote workers two options: Use a company-owned machine or let us secure your machine as if your employer owned it. "If you want to use your personal device, then the same controls have to be applied to it as if it were a company device," she says, adding that home-based employees must also consent to have their personal device wiped should they take a job elsewhere.

Like many channel pros, Cruciana puts end users through continuous security awareness training as well. "We've seen a four-digit rise in the volume of highly targeted, very, very convincing phishing emails toward our clients," he says. Teaching them how to recognize fake messages is at least as effective a defense as the latest email security solution.

"They have to be kind of both our first and last line of defense against what these threat actors want to accomplish," says Cruciana of users.

But then again, when has that *not* been the case? Work-from-home computing has complicated security in many ways, but it hasn't changed the field completely. "The same requirements that we had back in the old normal [are] still the case today in the new normal," Cruciana says. "We just have some new hurdles and obstacles."

EATING YOUR OWN SECURITY DOG FOOD

DESK JOCKEYS EVERYWHERE have been working from home since the arrival of COVID-19 last year. That very much includes channel pros, most of whom have been providing help desk services and performing remote maintenance from a collection of living rooms and kitchen tables instead of cubicles at the office. Protecting those technicians from attackers who were already targeting MSPs before the pandemic has been as big a priority for many channel pros as safeguarding customers.

Nancy Sabino, of SabinoCompTech, has employed a simple principle to guide that process: Embrace every security tool and policy she recommends to customers within her own business. "If we're asking our clients to do something, we ourselves have to test it and implement it within our own environment," she says.

Stanley Kaytovich, of QWERTY Concepts, has taken a similar approach, enforcing multifactor authentication among his technicians and deploying an automated security awareness training solution that tests users for susceptibility to phishing attempts. The system quickly fooled someone who thought he knew better, in fact—Kaytovich himself.

"I kind of just wasn't thinking, and I failed this test," he says. So far, none of his techs have made the same mistake.

Work-from-Home IoT Security

The need to clear the IoT device security minefield on home office networks is a challenge and an opportunity for channel pros. **By James E. Gaskin**

WHEN WORKERS were sent home at the start of the coronavirus lockdown, few companies had a plan to provide secure remote tools. Fewer still had a way to examine and secure home networks littered with Internet of Things devices like video doorbells, smart assistants, bathroom scales, and more that could ride the company VPN back to HQ. Now that work from home may continue indefinitely, managed service providers need to start including IoT under their security umbrella.

How many home-based workers have some type of IoT on their network? "I'd say *all of them*," suggests Cary Wagner, technical operations director and CEO of Pacific North-West I.T. Services in Coeur d'Alene, Idaho.

A big challenge is that there's no strict standard of security across all the different IoT manufacturers, explains John Hammond, senior security researcher at security services firm Huntress Labs. Every Google Nest Mini or Amazon Alexa is an attack vector, and that doesn't include items you might overlook, such as a garage door opener you can control with your phone.

"Since you can't control IoT devices with a mouse and keyboard, some sort of remote access to manage and configure the devices is needed," Hammond says, adding that those admin portals are well known to hackers.

Another challenge is getting businesses to shore up their workers' home networks. "We have 150 clients, and I can count on one hand the number who asked us to configure an employee's home network," says Al Alper, CEO of Absolute Logic, a managed service provider in Wilton, Conn. "For the three or four who asked, we changed default usernames and passwords on home routers, set up a guest Wi-Fi network for all the IoT devices, and added endpoint security software everywhere possible." This approach is more affordable for home use than a firewall with unified threat management (UTM), which is more appropriate for the corporate network.

> "We have 150 clients, and I can count on one hand the number who asked us to configure an employee's home network."

AL ALPER
CEO, Absolute Logic

Alper says it's possible to reset usernames and passwords on existing home networks remotely, so MSPs don't always have to send a technician to the home. He likes to add a Sophos RED (Remote Ethernet Device) to the firewall at the company's headquarters to provide UTM to the home network. He's also seen a marked increase in remote desktops over Windows Virtual Desktop on Azure.

MSPs should convey to their customers that securing a home network doesn't require a "rip and replace," Alper adds.

Wagner's first security fix for home IoT is "to get a firewall, and configure it to deny all, and only open up what you need."

Hammond suggests MSPs have a policy to check and install new firmware, patches, and hotfixes to all the IoT devices possible. "Of course, the 'security basics' never die, so check for hardcoded or default credentials set on the remote access modules of IoT devices."

MMR Opportunity

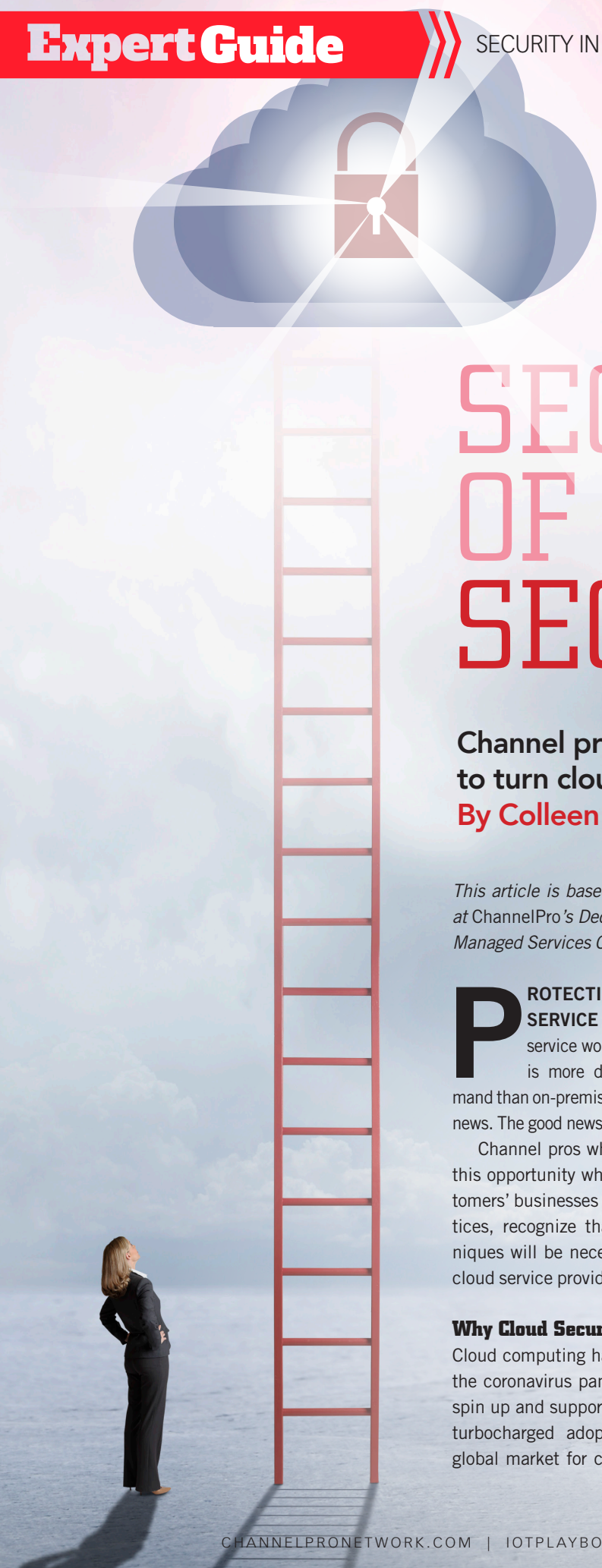
MSPs and integrators can turn home network security into MRR in many cases. Alper, for instance, bundles any new equipment customers need with setup services and bills for ongoing management per home user monthly. "If they need to upsize the HQ firewall, you're in the black from the jump," he adds.

Mike Jack, senior manager of product marketing at telcom company Spirent Communications, suggests channel pros can offer services that help companies enforce at-home IT device strategies. "Work with IT organizations to put better rule sets in place to segment remote users from corporate assets," he explains.

Training and education can be part of the solution as well, says Wagner. "You can't treat them like your worst enemy but their best friend if you want to get them to change. Human beings are our own worst enemy."

Finally, Alper points out that "users in the office don't think about network security, and it's more of the same when they go home." Therefore, having a plan in place that includes WFH security instructions, hands-on and remote configuration and monitoring services, IoT security practices, and affordable equipment upgrades where needed can keep users just as obliviously safe at home as they are at work.

JAMES E. GASKIN *is a* ChannelPro *contributing editor and former reseller in the Dallas area.*



SECRETS OF CLOUD SECURITY

Channel pros can follow these tips and best practices to turn cloud security from headache to opportunity.

By Colleen Frye

This article is based on a panel discussion at ChannelPro*'s December 2020 Cloud and Managed Services Online Summit.*

PROTECTING SOFTWARE-AS-A-SERVICE and infrastructure-as-a-service workloads in multiple clouds is more difficult and more in demand than on-premises security. That's the bad news. The good news is it's more lucrative too.

Channel pros who want to capitalize on this opportunity while protecting their customers' businesses need to adopt best practices, recognize that new tools and techniques will be necessary, and choose their cloud service providers (CSPs) wisely.

Why Cloud Security Is Hard

Cloud computing has been on the rise, but the coronavirus pandemic and the need to spin up and support remote workforces has turbocharged adoption. IDC expects the global market for cloud services, software, and hardware to exceed $1 trillion annually by 2024, with a compound annual growth rate of 15.7%. Unless properly protected, all those cloud-based applications, servers, and storage repositories will continue to be a massive target for attackers.

It's imperative, then, that managed service providers embrace and excel at cloud security. There are several challenges, however. For one, the potential threats MSPs face in a cloud environment aren't necessarily the ones that they're used to dealing with in an on-premises environment, so different skills, techniques, and tools are required.

The tools channel pros are accustomed to implementing "are designed to work in environments that we control," says Michael Cocanower, CEO of itSynergy, a Phoenix-based MSP. The challenge now is securing customers in an environment the MSP *doesn't* control, he explains.

MSPs need to adjust in two ways, Cocanower says. First is examining whether

PHOTO: DNY59 / ISTOCK

their current tools support integration with cloud platforms. "A lot of the tool vendors … have started to enable new functionality in their tools that allows you to hook into the cloud environments and plug those into your existing management infrastructure."

MICHAEL COCANOWER

Second, he says, MSPs need to get up to speed on the security tools that cloud providers like Amazon and Microsoft offer and learn how to "tweak those … so that they're optimally configured to secure our customers' environments."

Another challenge is getting buy-in from customers on a shared security model. "A lot of folks believe that if they put their application, their work process, [their] data up in the almighty cloud, that someone else is going to take care of the security," says Michael O'Hara, owner and principal consultant of Sparta, N.J.-based MEDSEC Privacy Consulting. He calls that belief "the threat of misunderstanding."

In actuality, cloud security is a shared responsibility, stresses Angela Davis Dogan, founder and CEO of Davis Dogan Advisory Services, a risk management consultancy in the Greenville, S.C., area. "There's certain security measures that need to take place on the client side. There's certain security measures that the client needs to make sure are in place on the cloud side. And then the cloud side needs to execute and make sure that those security measures are in place and that they're proactively ensuring security exists in their environment."

MSPs, therefore, must understand the cloud provider's security model and what they may need to implement to protect their clients. O'Hara suggests asking cloud providers for their "matrix of responsibilities" document, which should outline what the CSP and the tenant client are responsible for.

Best Practices to Get Cloud Security Right

MSPs should have their own well-documented security policies and procedures in place, of course, and convey those to cloud providers so that expectations are clear. "That's where that matrix [of responsibilities] comes in, because you want to make sure that your outsourced cloud provider is living up to, if you will, the same security standards that you require internally," Davis Dogan advises.

Along with the CSP, customers too must adhere to a security baseline that includes policies for access control, firewall rules, backup methodologies, and so on. O'Hara says this can be an opportunity for MSPs. "You can help your customer write those policies and procedures so that they have that baseline security," he says, adding that once those policies are in place they should be audited. "Security is not a set-it-and-forget-it proposition."

Enforcement of customer adherence to policies should be in every MSP's contract, according to Davis Dogan. "The contract gives you the backing to be able to have the enforcement practices, to ensure that your security policies and standards that you've set forth are being adhered to," she says.

ANGELA DAVIS DOGAN

Cocanower adds that adherence is particularly important if the MSP's customer is in a regulated industry such as financial services or healthcare. "If you're a federally regulated entity, that's one of the first things that an inspector is going to look at is when the … Office of Compliance Inspections and Examinations [renamed by the SEC in December to the Division of Examinations] comes in to audit a financial adviser. Yes, they're going to ask for copies of all your policies, but when we see letters of corrections or deficiencies from these inspections, one of the biggest sources that they say [is], 'Yeah, your policies are beautiful. You're not following them. So it doesn't matter. It doesn't count.'"

MSPs may need to adjust contracts in further ways if they're providing cloud security, Cocanower notes. With an all-you-can eat model for a fixed monthly fee, for instance, he believes MSPs "dramatically underestimate" the amount of risk they're taking on. "And I truly question whether they are pricing those agreements appropriately to compensate them."

Choosing Cloud Vendors

If implementing, enforcing, and staying up to date with cloud security sounds daunting, Davis Dogan recommends adopting a framework such as the NIST Cybersecurity Framework, ISO 27001 and 27002, or the Cloud Security Alliance Cloud Controls Matrix (CCM). Following a framework can also help in choosing secure cloud vendors, she says. CCM, for instance, includes the Consensus Assessments Initiative Questionnaire (CAIQ). "CAIQ gives you the questions that you should ask."

This line of questioning is particularly important when evaluating smaller cloud providers, Cocanower notes. While it's probably safe to assume that big public providers like Microsoft, Amazon, and IBM "have their ducks in a row … you really need to dig in if it's somebody you haven't heard of before, or if it's a small line-of-business application vendor who's just moved to the cloud in order to stay relevant," he says.

Remember that the cloud is really just "a server farm somewhere that somebody is running," O'Hara adds, and how sophisticated that server farm is and what safeguards are in place will vary.

The bottom line is security is never simple, O'Hara says, but if MSPs "start with the foundational policies and procedures and contracts, and make sure that you're constantly challenging your conceptions of security, you're off to a great start."

READER ROI

PROTECTING CUSTOMERS' WORKLOADS in the cloud is difficult, but can be lucrative for MSPs that adopt best practices and new tools and techniques.

THESE INCLUDE getting buy-in from customers on a shared security model, establishing policies and procedures, and requiring adherence to baseline security guidelines.

VET CLOUD PROVIDERS on their "matrix of responsibilities," get up to speed on their security tools, and establish clear expectations for all parties.

PEERTOPEER

EXPANDING THE CIRCLE OF SAFETY

CDN Technologies has a three-pronged approach to safety: protecting clients, employees, and the MSP business.

By Barb Paluszkiewicz / Photography by Fotografia Boutique

LAST YEAR, we all learned a lot about the importance of contact tracing to help reduce the spread of COVID-19. CDN Technologies is applying a similar concept to protect our clients against the spread of ransomware and other cyberattacks. It's all part of our 2021 theme of safety—for our clients, our company, and our employees.

As MSPs, we do everything possible to keep our clients' data safe. They trust that we'll proactively protect them against cyberattacks through our services, which include penetration testing, security awareness training, tabletop incident response exercises, webinars, and workshops. But our clients don't transact business in a bubble. They interact with their customers and vendors and take advantage of APIs to automate processes. These touchpoints leave openings for cybercriminals. That's why CDN Technologies is expanding the circle of safety for our clients by offering some of our security services to our clients' customers and vendors—for free. With pen testing, for instance, we help them discover the *how*, not who. We show them the holes and how a hacker could get in, and ask them to consider if they have the right tools in place to defend themselves and prevent a future incident. In addition, our incident response tabletop exercises focus on the *who*, not how. Our team helps with who will be responsible for what actions if an incident occurs, because it's everybody's responsibility.

What has resonated: We're all in this together. Our clients have been very receptive to inviting their customers and vendors to participate in our free offerings. We can see in our CRM that they are sharing and forwarding the free version of our security awareness training on YouTube to help secure and protect their circle of safety.

The byproduct of this effort is twofold. First and most important, we are making our clients safer because we're making their supply chain safer. Second, it allows CDN Technologies to expand our marketing and become more widely known as a trusted authority and resource.

Keeping Ourselves Safe

At the same time, we work to keep the company safe by staying apprised of industry threats and developments. We pen test internally, continually work on our SOPs, and maintain detailed records. We also require a strong security posture from vendors. For example, our security questionnaire asks them to specify where they store our data, if they have an incident response plan, if they are NIST compliant, and more.

CDN Technologies prioritizes employee safety, both physically and mentally. MSPs are deemed essential workers in Canada so we have kept our office open. Although our employees can choose to work from home, most want to be in the office, so we have completely revamped our space to ensure social distancing and to keep traffic in communal areas light. When technicians need to go onsite, everyone follows all COVID protocols.

On the mental health side, our longstanding practice of having all employees go through professional development training from the Disney Institute has not only enabled us to deliver superior service, but has given our staff the emotional skills to navigate the unique challenges and stresses we are all facing. Disney training teaches how to be "givers" when it comes to the emotional needs of clients, how to stay calm, and how to keep things moving forward in a positive direction.

These invaluable skills are another tool for keeping clients amenable to security protocols. While users are waiting to be authenticated, for example, our technicians know how to engage them in a conversation about the weather or cat filters on Zoom. This interaction lessens the pain of taking that extra security step while deepening relationships at the same time.

While we can't put our clients, our employees, or our business in a bubble, we *can* expand the circle of safety for all.

BARB PALUSZKIEWICZ

CEO, CDN TECHNOLOGIES

FOUNDED 1989

LOCATION Toronto

NUMBER OF EMPLOYEES 18

WEBSITE cdntechnologies.com

COMPANY FOCUS We offer technology products and services to improve and secure Canadian businesses while helping solve our industry's greatest challenge, the technical skills shortage.

PROFESSIONAL MEMBERSHIPS CompTIA, Positive Strategies, Tech Tribe

RECOMMENDED BOOK *Hyper Sales Growth*, Jack Daly (ForbesBooks, 2014)

FAVORITE PART OF MY JOB Speaking engagements

LEAST FAVORITE PART Ransomware and business email compromises

WHAT PEOPLE WOULD BE SURPRISED TO KNOW ABOUT ME
I have two degrees, one in chemistry and one in physics. So that means I'm a rocket scientist!