A Special Edition Of MSP Success

MSP CYBERSECURITY MAGAZINE

As Phishing Evolves, So Does The Need For Prevention Strategies

With Manoj Srivastava

Page 20

Brian + Lisa Johnson

The Battle Of Cybersecurity: What You Need To Know About Shielding Your Organization Against Cybercrime

Page 14

Special Issue: Cybersecurity Champions - Curated Experts Edition for MSPs

MSPSuccess.com

MSP CYBERSECURITY

PUBLISHER Tulip Media Group
EDITOR Robin Robins
GRAPHIC DESIGN Jessica Embree
COORDINATORS Jeanne Romage
Allison Foelber
Jen Kershaw
Erika MacLeod

CONTRIBUTORS Lisa & Brian Johnson
Datto
Danny Jenkins
Konrad Martin
Paul Tracey
Blackpoint Cyber
Dean Lause
Manoj Srivastava
Matt Katzer
Mike Moran
Gary Tonniges Jr.

PHOTOGRAPHY All images sourced from Tulip Media Group or iStock.com unless otherwise identified.

MSPSUCCESS.COM
INFO@MSPSUCCESS.COM

CONTENTS

Kaseya + datto

Kaseya+Datto is all set to burn some rubber across the world over the next few months with its Connect Local events, bringing together the industry's greatest minds to help you speed past business and technology hurdles with ease. Covering everything from cybersecurity to IT best practices, Kaseya has assembled the IT dream team to present their insights and opinions on current market trends and how you can capitalize on every single opportunity in 2023. Join us at the closest Connect Local and gear up for a series of great events.

At a Connect Local event, you can expect to:

- Participate in thoughtful sessions on Cybersecurity, M&A, Sales & Marketing and other hot topics.
- Pitstop at a venue in your own town! A Connect Local is coming to 80 cities worldwide.
- Rev up your networking engine because each venue will be teeming with potential opportunities.
- Learn from both peers and guest speakers who possess exceptional subject matter expertise.
- Receive exciting giveaways!

Register and save your

FREE SEAT TODAY!

How To Prepare For The Security Threats Of Tomorrow

Make no mistake about it: cybercrime is becoming more complex and more frequent, and SMBs are looking outside their organizations for help dealing with evolving threats. This is a gigantic opportunity for MSPs as long as they understand two things: the current state and emerging trends of the cybersecurity landscape, and what tools they can use to combat it. To start, let's take a look at the cybersecurity landscape, and analyze the threats, trends, and opportunities.

PROTECTING SMBS FROM RANSOMWARE ATTACKS

Cybercriminals are increasingly targeting SMBs. Studies show that 43% of all cyberattacks were against small businesses. This is problematic because roughly 60% of SMBs go out of business in the six months following an attack. Because so many SMBs don't have the resources to support an internal IT and data security operation, many look to MSPs to prove the level of protection they need.

The most common threat is ransomware, which was reported by 70% of MSPs in Datto's most recent *Global State of the Channel Ransomware Report*. So, how do MSPs combat ransomware threats? They have to be proficient in three areas.

Prevention — Obviously, succeeding in this phase is what every MSP hopes to do: eliminate the threat of an attack in the first place. Although there is no airtight approach to do this, there are measures MSPs can take to help keep their SMB clients from becoming ransomware victims. This includes the use of detection or antivirus tools or enabling automated patch management to fix potential vulnerabilities as soon as they are discovered.

Detection — Despite the MSP's best efforts, ransomware can still get through the protection layer. That's why there should be measures in place to identify when ransomware is present rather than assuming an attack will never be successful. The earlier it is detected, the earlier actions can take place to eliminate it.

Response — When ransomware is detected, responding to the attack and eliminating it must be done with the utmost efficiency. MSPs must be prepared to act by taking the following steps:

- **Scan networks for confirmation of an unfolding attack.**
- **Identify the infected computers and isolate them from the rest of the network.**
- **Secure all backup data or backup systems immediately.**

MSPs that are able to optimize ransomware prevention, while also detecting and quickly responding to attacks that are successful, can have a tremendous impact on their clients and the industry as a whole. Ransomware attacks were estimated to cost roughly $20 billion in 2021, and the MSPs that are able to save their clients from suffering those financial damages can help prevent them from succumbing to closures. MSPs' efforts in this area will go a long way toward strengthening their reputation as a security service provider and can leverage that to win more business.

Now that we have a better understanding of the threat of ransomware, what MSPs need to do to combat it, and what they can gain from successfully doing so, let's take a look at how MSPs can help prevent, detect, and eliminate ransomware.

FINDING THE RIGHT TOOLS TO COMBAT RANSOMWARE

SMBs entrust MSPs with access to critical systems and data. The payoff is that they feel protected because the MSP will be able to act swiftly and effectively when a threat arises. MSPs need to reward that trust by arming themselves with tools that will facilitate quick and decisive action.

For example, remote monitoring and management (RMM) tools provide MSPs with access to their clients' endpoints so they can keep them secure, patched, and operational. Datto RMM does this on an incredible scale in a secure, cloud-based environment. With automated patching, MSPs can leverage Datto RMM to proactively fix any vulnerabilities before they are attacked, helping optimize all ransomware prevention efforts.

But, again, the idea is to always be prepared in case ransomware attacks are successful. Datto RMM also takes the next step on ransomware defense by including native ransomware detection, which monitors for crypto-ransomware and attempts to kill the virus to help reduce the impact of an attack. Users get alerts at the first detection of crypto-ransomware and automatically isolate impacted devices.

The ability to detect ransomware immediately enables the MSP to execute an action plan sooner rather than later. As ransomware infects systems, it can cause extensive damage, which as we have established, may prove too costly for many SMBs to overcome. Ransomware detection is a surefire way to maintain damage control, keep clients operating, and continue revenue streams for MSPs.

Of course, no ransomware response plan is complete without systems in place to protect the most vital company resource—its data. Backing up data regularly can mitigate the risk of downtime when a ransomware attack is successful, but the system must be secure and reliable. Datto SIRIS is designed to protect physical, virtual, and cloud infrastructures and data. With Datto SIRIS, data is well protected and easily accessible so it can be recovered rapidly when needed. SIRIS also detects ransomware within backups, saving time when locating the last clean system restore point.

LEVERAGING SECURITY SERVICES TO GROW YOUR BUSINESS

In Datto's *Global State of the MSP Report*, MSPs shared what challenges they will be focused on this year. Unsurprisingly, most focused on security on some level, whether that be securing endpoints, protecting data, or understanding just how to be better against the threat of ransomware. They also told us that they are focused on sales and marketing, particularly as it relates to tools that will help them hit their growth goals in coming years. As we have previously mentioned, all SMBs share a growing concern over security, and it is a business opportunity for MSPs. Those who understand the state of the security landscape and are able to quickly adapt as that landscape changes will end up winning in the end. But to be effective in doing that, MSPs must arm themselves with the tools that allow them to be agile so they can continuously meet their clients' ever-changing needs.

Security threats will never go away—they can only be kept at bay. With the right partner, MSPs can do this effectively, protect their clients, and discover new levels of success.

Visit Datto.com to learn more. ■

How ThreatLocker Is Using "Zero Trust" To Change The Cybersecurity Game

MSPs today are losing the battle. The size of the endpoint security market is about $9 billion a year. In 2021, cybercrime and ransomware cost the world $6 trillion. In essence, it's like cybercrime is the GDP of Japan and all measures of cybersecurity combined is the GDP of Somalia or Burundi.

When you have an entire industry that is outmatched while ransomware attacks are up 800% and cybercriminals continue utilizing cryptocurrency that's virtually undetectable, how do you flip the script and take back control of cybersecurity?

According to Danny Jenkins, CEO and cofounder of ThreatLocker, it starts with "zero trust," a network security model based on a strict identity verification process.

Danny says, "In simple terms, zero trust means 'least privilege.' Don't give access where access isn't required. Zero trust applies to different levels. At the application and file levels, you are only giving access to those who need access. At the network level, you're thinking about what ports are open."

DISPELLING THE MYTHS OF ZERO TRUST

MSPs and end-users who are hesitant to adopt a zero-trust model of cybersecurity often have a false perception of what it entails. They may think that the C-level executive who has always accessed an application will now be shut out entirely. That's not the case. If someone in the organization routinely accesses an application or file, it makes perfect sense for them to still be able to access it.

"When you roll out a cybersecurity solution like ThreatLocker, it learns what's in your environment," says Danny. "It will learn which applications and files are accessed and by whom. Then the MSP can either allow or deny access based on the findings." Some also believe that the zero-trust philosophy is brand new and a far more aggressive approach to cybersecurity. That's not entirely true.

Danny says, "Zero trust is simply a framework. A target. Everyone already has some level of zero trust in their business. Do they have administration permissions? Do they have a firewall that blocks inbound traffic? Those are levels of zero trust."

> **"WHILE A ZERO-TRUST APPROACH IS ABOUT DENYING ACCESS TO THOSE WHO DON'T NEED ACCESS, THE CASTLE-AND-MOAT APPROACH TOWARD SECURITY IS FAR MORE LENIENT."**

Certainly, the maturity of zero trust is a lot further along than it was just two or three years ago, but cyberthreats are also a lot more frequent and aggressive today.

"Back then," Danny says, "MSPs took a stance of allowing by default instead of denying by default. They focused on only blocking the bad stuff. Then, once a year, they would do a full restore for ransomware. That's now changed. A good portion of MSPs have now implemented zero trust. In fact, ThreatLocker has thousands of partners who have implemented zero trust for all of their customers where it's needed most—at the application and endpoint levels."

ZERO TRUST VS. CASTLE-AND-MOAT SECURITY

While a zero-trust approach is about denying access to those who don't need access, the castle-and-moat approach toward security is far more lenient. It assumes all applications and files inside the network (the castle) are safe while everything outside the firewall (the moat) is not safe. Both are fallacies.

Danny says, "Castle-and-moat security is focused on keeping out external factors. Well, that's essentially the whole world. So, when anyone on your team downloads an email, a program, or a game, you're talking about the whole world."

He continued, "Also, think back to the Dark Ages when there were real castles and moats. Well, the knights didn't leave their castle without full armor. Today, people are inside the perimeter, go outside their network to work from home or at Starbucks, then come back in. That's where incredible risk occurs."

THE GAME HAS CHANGED

Think about where we were just 10 years ago. Cybersecurity was more focused on curbing spam, ridding your computer of adware, and avoiding nuisance viruses that sent risqué pictures. That was the definition of "bad" back then. Today, a cyberattack could cripple a business and cost their life's savings.

Because the threat of cyberattacks has changed, cybersecurity has to change to keep up with those threats. Much of cybersecurity today revolves around monitoring and detection. With that approach, you are essentially deciphering between the good and the bad. The goal obviously is to get alerts or even shut down all possible threats.

Danny says, "I try to avoid the word detection. ThreatLocker isn't really about detection. It's more blocking what is not allowed. Rather than trying to determine if it's good or bad, it doesn't matter. None of it is allowed in. We're less about alerts and more about what's required in your environment, then blocking everything else."

THE REAL QUESTION: DOES ZERO TRUST WORK?

While you can certainly question if adopting a zero-trust environment is the right approach to cybersecurity, it's hard to question the results.

"Cybercriminals prefer to attack on weekends," says Danny, "especially holiday weekends. On the Fourth of July weekend, we had 46 MSPs get an attempted hit to all of their devices. Ransomware was attempted to be pushed out to their clients. Thanks to ThreatLocker, all but one of those 46 MSPs had everything blocked. The only reason the one attack went through was because that MSP was still in a learning mode. One week later, and they would have been fine."

As for where the trend of zero-trust security is headed:

- This year, 80% of new digital business applications opened up to ecosystem partners will be accessed through zero-trust network access.
- By 2023, 60% of enterprises will have phased out of their remote-access VPNs in favor of zero-trust network access.

THE FUTURE OF CYBERCRIME AND OUR RESPONSE

Does the cybercrime industry show any signs of slowing down? Not according to Danny.

"We're going to see a lot more cybercrime," he says, "and it will continue to get more sophisticated. All these hackers do every single day is search for every vulnerability imaginable. So, we're going to see more vulnerabilities and more attacks at the entry points. It's going to lead to more ransomware, more costs, and more businesses being hurt. That's why our team at ThreatLocker invests so much time in our cybersecurity solutions. To keep MSPs and their clients safe."

Visit ThreatLocker.com to learn more. ■

8 Ego-Driven Myths That Make Your Customers Vulnerable To Cybercrime

BY KONRAD MARTIN, CEO OF TECH ADVISORS

HUMBLE LEADERSHIP IS A POWERFUL WEAPON

The moment an executive or business owner decides to hire an MSP, they declare a commitment to the organization and employees to protect networks and data from cybercriminals. What they need to understand is this is not a responsibility handoff but, instead, the beginning of their involvement.

Winning the battle against cybercrime requires all hands on deck. Hackers are oblivious to job titles and prey on fragile egos, and while this is a touchy topic to broach with clients, MSPs are negligent if we omit any potential roadblocks to safety. An awkward conversation with leadership early on beats explaining later that had they followed the rules expected of everyone else, they could have prevented a devastating hack. We advocate to involve everyone in the organization in the training process from the start—and to smash the hierarchy.

8 EGO-DRIVEN MYTHS THAT MAKE SMBS VULNERABLE TO CYBERCRIME

As MSPs, we are all technology experts, but we cannot forget that computers and software are only as effective as their human operators. It may not strike the nerdy skills that drew you to this work, but attention to behavior management will keep your business sustainable.

Here are eight common falsehoods we have seen SMB leaders espouse that can pose cybersecurity risks. We also suggest ways your MSP can respond to promote the kind of humble leadership that can make or break the company's security.

1. Our Revenue Is Too Small To Appeal To Hackers, So We Don't Need Any Security Measures.

You'll encounter this person when scrambling to salvage their company after getting hit.

It makes no difference to cybercriminals if a company reports $4 billion or $40,000 in annual revenue. Both a sandwich shop that only sells pastrami on rye and a big-box department store hold personal identifiable information (PII) on the network. PII is a hacker's capital.

Think of apple picking. If you go to an orchard, do you climb to the top of the tree? Not if your goal is to fill the basket quickly. You grab the low-hanging fruit. Cybercriminals do the same thing. They have the ability to climb the tree—as evidenced by the Colonial Pipeline and Bank of America takedowns—but more often, they'll pick easier targets.

When a huge corporation gets hacked, they can finance the recovery. Joe's Car Wash, with its 15 employees, can't afford it. If the cost doesn't take them down, the bad publicity alone will drive clients to competitors.

2. We Created A Written Information Security Plan (WISP) A Couple Of Years Ago. We're Fine.

If that WISP is not current, it's not in compliance. It needs to outline up-to-date protocols for employees to ensure they keep PII away from thieves.

Leadership should understand what the WISP entails and why it affects cyber insurance qualifications. Then, continually educate everyone about their role in protecting the company.

(Yes, CEOs, that includes you.)

And for those organizations that review the WISP whenever the mood strikes? Guess what. Cybercriminals don't just punch in every couple of years. They work every single day, courting you until you click on a nefarious link in an email—which is how 87% of hacks occur. While you sit back, thinking you're fine, they're developing more sophisticated ways to access your system, building a fast-growing cybercrime industry.

3. I'm Too Smart To Click On Something Like That. Only Fools Fall For Phishing Scams.

Intelligence is irrelevant. It's about awareness and attention at a given moment.

If a leader feels superior to their staff and arrogantly skips simulated phishing training, they can miss key lessons and be more susceptible to falling for the scam. This can also happen to anyone who feels stressed out or preoccupied; those people don't look closely at details in an email.

Remember, hackers are pros at tricking people, and some of the brightest people have gotten hit. And in this ever-changing industry, even information technology professionals like MSPs can't possibly know everything about cybersecurity. The bottom line is that all employees need regular training. If a higher-up's ego needs coddling, remind them they have a powerful responsibility to protect others, and employees are counting on them.

4. People Who Click On Phish Bait Should Feel Ashamed.

This might be the most harmful lie of all. As mentioned above, anyone can click on a bad link. Model humble leadership; show clients how to cultivate a safe environment where shame and blame are not tolerated—and be the first to admit culpability.

Never ask, "Who clicked on it?" It doesn't matter. Someone was fooled. It might have even been you.

Education tools like simulated phishing demonstrate what a mistake might look like. Note that managing partners tend to sit out of these trainings, but 90% of the time, the hacker targets the manager. Simulations allow people to learn how to identify when an email doesn't look right, and spotting the signs is most effective with practice.

Keep in mind these programs are like catch-and-release fishing. If you get caught with real phishing, you're not going to live.

5. We're An IT Company, So We Can Handle This On Our Own, Thanks.

Nope. If you work in cybersecurity, you can still get hit. We're an IT company, and it has happened to us.

You are not shrewder than the cybercriminals. Your commitment to defense will never reach theirs to harming you. Don't underestimate them.

Seriously, we're good. We don't need simulated phishing. I assure you, there's no question you need simulated phishing! Tech Advisors does it here, too.

6. My Reputation Will Be At Stake If I Tell Anyone I've Clicked On A Bad Link.

If you click on something that doesn't seem legit, the worst thing you can do is keep it to yourself. If your company gets hacked, tell your MSP—ASAP!

Some of the worst zipped-lip offenders are managing partners. Help them understand that an ego can be the flame that burns down the company. Make sure your clients feel comfortable calling you and appreciate the urgency.

Once they learn how to recognize suspicious emails, they should get in the habit of letting you know when they receive one. Cost should not be a deterrent since this time is likely already included in most MSP packages.

7. I Wouldn't Dare Question The Person In Charge.

If employees fear speaking up to bosses more than making a huge bank transfer outside of normal protocol, there's a bigger cultural problem to address. Encourage your clients to be approachable and regularly communicate with their team. Building relationships can break barriers to safety. An employee should never feel embarrassed to contact their supervisor.

8. I Don't Need To Worry About Employee Social Media Habits.

Unless you've slept through the entire pandemic thus far, you'll know this is not true. The surge of people working outside of the office's protective firewall has caused cybercrime to go through the roof since early 2020.

The blurring of work and personal activities online has made it more evident that people share too much information on social media. Cybercriminals scoop up personal data, which become clues to crack passwords. When accessing the company's network from home, every action can affect the organization.

Remind clients that the networks they originally configured to occasionally accommodate a handful of work-from-home (WFH) employees were not designed for use by everyone all the time. This capacity overload makes WFH security even more precarious.

You'll hear all kinds of excuses from companies that resist putting proper security systems and programs in place. We at Tech Advisors cannot emphasize enough the importance of showing up for yourselves and your staff with transparency and humility. Hold yourself accountable, support your own growth, and encourage clients to take on a team-oriented mind-set in the fight against a hacker's tricks.

Cybercriminals know that the easiest way into any organization, no matter how secure, is through its employees—human beings who can be tricked and manipulated. Lead by example, commit to continued learning, and stay suspicious!

For more information on Tech Advisors, visit Tech-adv.com. ■

Let's Get SOCIAL

Like And Follow Us On Social Media For Even More **Exclusive Content** And Videos.

MSP SUCCESS

Scan Me!

datto
A Kaseya COMPANY

Effortless & Effective Endpoint Detection and Response for MSPs

With Datto Endpoint Detection and Response (EDR) you can detect and respond to advanced threats. Datto EDR is an easy to use cloud based EDR solution that's designed to meet your needs as an MSP.

GET A DEMO TODAY

Why Your Customers Need To Adopt A HIPAA MIND-SET

Paul Tracey's Mission To Make HIPAA The Standard Across All Industries

WITH PAUL TRACEY, FOUNDER AND CEO OF INNOVATIVE TECHNOLOGIES

Every morning, when Paul Tracey, founder and CEO of Innovative Technologies, wakes up, he's greeted with a new list of cybersecurity threats.

The morning we spoke, one of Tracey's clients had an employee who downloaded a document at their home, uploaded it to their Google Drive, then downloaded it again when they got to work. Loaded with malware, the document put the client's company in danger. Fortunately, because of the procedures Tracey had in place, his team discovered the document immediately and ended that threat within 35 seconds from when it started. But for many companies that don't have a cybersecurity plan in place, this wouldn't have ended so well.

Tracey realized early in his IT career that companies were grossly undereducated about and unprepared for cyberthreats. Therefore, for over a decade, Tracey has been on a mission to educate SMB owners whose livelihoods are at risk by what they don't know about IT and cybersecurity threats. The author of *Delete the Hackers Playbook* and co-author of *Cyberstorm* (released in 2022), he started his own company after witnessing a large hospital pay hefty fines when their lax security caused a major breach. Realizing that "cybersecurity inequity is highly problematic," Tracey dedicated himself to fighting cybercrime for the business owners who are the most vulnerable. Today, he helps businesses establish a company culture that supports safe, secure, and efficient IT.

The framework Tracey uses to protect client data is based on the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule. "While HIPAA was designed to protect the privacy of patient records, it is actually an excellent framework for any organization's security plan," Tracey explains. "It not only addresses technical measures needed to control the physical environment but also emphasizes the administrative processes necessary to secure data."

Tracey's idea to use HIPAA as a standard for all clients is even more relevant now that states have passed laws that mirror many of the core principles of HIPAA. But even if your state hasn't passed laws yet, Tracey urges compliance, saying companies can't afford to wait. "It is crucial for organizations to implement tight safety protocols long before they are legally required to do so," Tracey says. "We're finding serious issues such as malwares that hijack your browser and do things in the background without being found. By the time a company calls for help, often their entire office is already filled with malware. You can't afford to wait the 3–5 years it takes from proposal to enforcement—always follow stricter safety policies than the law dictates."

WHY HIPAA STANDARDS MATTER

Every single day, 2,300 small businesses are breached. According to the FBI, 95% of all successful cyberattacks during 2020 came through email phishing scams or links. Tracey believes that if more companies followed the HIPAA standards, this number would be greatly reduced. "Small companies end up going out of business and quietly just disappear," he says. "The larger companies are still susceptible, but they don't get hit as often because they are investing in educating their employees. Small businesses aren't having that conversation, and that's a real problem. Hackers are having success with small businesses because of the lack of security tools and security training these businesses have."

The new work-from-home environment has only made the situation worse. "If security measures were loosely followed before the pandemic, consider how problematic it became as masses of people were deployed to work from home using computers that weren't set up with proper security, firewalls, or other protocols," Tracey says. "Sadly, we've already seen a substantial uptick identified in digital threats targeting platforms that remote workers use. HIPAA standards could have prevented that."

HOW TO GET A COMPANY TO ADOPT A SECURITY MIND-SET

Tracey recommends the following actions to help transform a company's security:

1. Execute Training: "The workforce is significantly undereducated about technology," Tracey says. "And keeping up with the number of new threats popping up every day is tremendously difficult. That's why we focus on employee education. It must be met with the same kind of commitment and persistence as doing the security work."

2. Gamify Security: "We gamify the security practice," Tracey says. "We send videos with security tips and phish and spear-phish all users by sending out a phishing email from us. If a user clicks on that link, it immediately sends them to training. We've found this on-the-spot training to be extremely effective at changing the behavior."

3. Change the Culture: "The culture can completely change and be unrecognizable when you shift the employee computer behaviors and mind-set," Tracey says. "Frequently, I notice how people refer to their company computer and data as the 'agency's computer or data.' Once we change employees to think in a possessive manner regarding the technology, they are more careful with it."

4. Outsource an IT Firm: "Organizations simply do not have enough hours per year to do HIPAA training and implementation correctly," Tracey says. "We realized we could provide a package that freed up clients' time. Companies only need to allocate 15–20 hours per year to HIPAA compliance. We do the rest."

5. Educate Companies on the Benefits of Compliance and the Consequences of Noncompliance: Providers often don't realize that the fines for violations may be less severe if they have taken proper measures to comply. "If a provider has properly trained an employee and received the policy attestation for the issue in question, the fine and/or associated legal actions can be greatly mitigated," Tracey explains. "However, if the violation is deemed negligent because training and policy were not in place, the fines can be 10 times higher. But a breach doesn't have to qualify as a HIPAA violation to be catastrophic. It may result in data loss, costly downtime, and further ramifications if the data gets sold, which can happen even when the ransom is paid."

6. Implement Rules and Procedures Following the HIPAA Standard: Most companies don't know what data they hold or where it's located in their systems. They also have misconceptions about which data is protected. "Regularly, companies, especially smaller businesses, do not have procedures in place for even simple things such as what to do when you download a file and copy it or move it," Tracey says. "A client may tell us they store all their medical data in an electronic health records (EHR) program, then invite us to perform an audit. It's not unusual to find 6–8 months' worth of information that never got deleted or $2 million worth of medical information saved in download folders and other unencrypted locations—all outside the EHR."

> **"While HIPAA was designed to protect the privacy of patient records, it is actually an excellent framework for any organization's security plan."**

With so many companies unaware of how much time it takes to make sure a company is safe and how overworked most internal IT departments are, there needs to be more conversations around the risks and what companies can do to protect themselves. "The conversation about cybersecurity inside of organizations is long overdue," Tracey says. "While there's a long list of things to be afraid of, fortunately, there are reasonable solutions for all those bad, scary things. HIPAA is truly the gold standard and should be applied across all industries. An effective entry point is education. And an understanding of what threats you're dealing with at this moment in time will help you make a plan to deal with those in order of the highest priority. Regardless, immediately start getting employees cybersecurity training, even if it's minimal. Mandate and verify they do it. It's time to take cybersecurity seriously because there's no time to drag your feet."

For more information on Innovative Technologies, please visit UpstateTechSupport.com. ■

The Battle Of Cybersecurity: What You Need To Know About Shielding Your Organization Against Cybercrime

WITH BRIAN & LISA JOHNSON, PRESIDENT & VICE PRESIDENT, AVC TECHNOLOGY

In today's digital age, cybersecurity is no longer something that can be pushed to the bottom of your IT list; rather, it's a major risk exposure that all organizations need to be actively addressing. And what you may not realize is that some easy things can be done to identify and mitigate cybersecurity risks. So, let's dive into what you need to know about shielding your organization from cybercrime, including simple, actionable steps to better protect yourself today.

CYBERSECURITY INSURANCE

For starters, we recommend cybersecurity insurance for all organizations, no matter your size or maturity level. But it's not enough to just get a cybersecurity insurance policy. You need to ensure that you'll actually be protected in the case of a breach. As part of the underwriting process, there will be several security protocols and measures you'll be required to attest to, and this is where we see some organizations fall into this trap of thinking they're covered when, in reality, they're not.

There are two common pitfalls. One, an organization will buy cyber insurance and then blindly attest to these measures, even if they're not properly implemented, making their insurance void. Or two, cyber insurance companies don't clearly identify the requirements, and then you're not even aware that you're operating outside of compliance. Therefore, the first thing we recommend is understanding these requirements and taking the proper measures to ensure you'd be covered in the case of an incident.

UNDERSTAND YOUR VULNERABILITY

Beyond having proper cybersecurity insurance for your organization, you must understand where your vulnerabilities are and immediately take steps to remedy them and increase your security. That's why the first thing we do when speaking with prospective clients is go in and test everything security-wise—and customers are often shocked with the results. For example, it's common for us to be able to pull hundreds (yes, hundreds!) of passwords off a computer and map them to dark web breaches just by having users click a single link. Now imagine if that was a real phishing email sent from a cybercriminal.

Something else that people often don't think about (until it's too late) are the old pieces of software that sit in the corner of your computer somewhere. If nobody is looking at these things, it can become ground zero for a major hacking event that starts a chain reaction throughout the organization just because of one piece of old software (or even a new piece of software that hasn't been patched properly) that a cybercriminal was able to attack. As we like to say at AVC Technology, don't be the low-hanging fruit for these hackers. Take steps to bolster your security before a breach occurs.

USER TRAINING

Another way you can proactively address your cybersecurity protocols is by having solid user training. We're all human, and sometimes we go too fast and click on something we shouldn't—it happens. However, by putting your employees through user training, you can increase their awareness, which has been shown to significantly decrease your chances of becoming a victim of cybercrime. And there are many different kinds of attacks to be aware of and prepared for, including ransomware, malware, supply chain attacks, and phishing, to name a few.

In addition to consistent user training, we always recommend having multiple layers of security for added protection. This could be as simple as having basic antivirus software installed, going one step further and having endpoint security in place on the computers, or, for clients that require more advanced security, there are zero-trust tools that will prevent anything from running that hasn't been approved prior. Ultimately, no matter what level of security you decide on for your organization, it's crucial that your employees not only understand what to look for but they know what procedures to follow if there is a cyber breach.

MONITORING AND MANAGEMENT

There's a big misconception that once you put some cybersecurity protocols in place, you can basically "set and forget it." This is simply not true. In order to ensure that your organization is protected to the fullest extent possible, you (or your IT partner) need to constantly monitor and manage your cybersecurity protocols to limit your risk. Not only that but you'll want to work with a company that spends time vetting the products and understands how to install, manage, and support these new tools.

For example, when cloud services became the new thing in IT, many organizations switched over and got a false sense of security, thinking that the cloud would do everything for them. However, if you don't have someone who knows how to manage these services, you could actually be at an increased risk of things like password compromises or data loss. And if you experience a critical breach, that could be the end of your organization, especially if you're a small to medium-sized operation. So, instead of gambling with the previous protocols you've put in place, it's always best to be doing ongoing assessments, audits, and vulnerability management on a recurring basis.

FINAL THOUGHTS

Although cybersecurity may seem overwhelming on the surface, we hope these actionable steps will help you become more comfortable with and aware of what you should be doing to keep your organization safe. Start by understanding your cyber insurance policy and ensuring compliance, knowing where your vulnerabilities are and working to resolve them, training your users properly so that they can be the first line of defense, and monitoring and managing your cybersecurity solutions to make sure they continue to protect your organization. By doing these simple things, you can be proactive in the cybersecurity battle and keep yourself shielded from cybercrime in this ever-evolving digital age.

Still looking for further support? Our team at AVC Technology is on hand to help you implement robust cybersecurity protocols, operate within compliance, and bolster your overall security for your organization. ■

Brian & Lisa Johnson

President & Vice President

AVC Technology

AUGMENTING DATA LOGGING With True MDR With blackpoint

ADVANCED ATTACKS ON THE RISE

When the pandemic made its impact around the globe in early 2020, it simultaneously ushered in an exponential surge in cybersecurity attacks. In the scramble to mass-migrate businesses to virtual work environments, many companies did not have the time or resources to implement strong cybersecurity policies and processes. This climate has allowed cyberattacks to boom in nearly all industry verticals, impacting critical infrastructure, utilities, transport, food supplies, health care, education, and the US economy at federal, state, and municipal levels.

Advanced cyberattacks are now considered a risk to national security following the sweeping uptick in cyberattacks.

Once targeting small companies or individuals, threat actors are now making headlines by growing their attack radius to include major infrastructure companies and even leading security firms. What's more is that threat actors are quickly evolving their tactics and targets when it comes to deploying their assaults.

INCREASED FOCUS ON DATA LOGGING

To combat these cyberattacks, more and more MSPs are turning to security logs to understand developing security incidents, achieve compliance, conduct post-incident investigation, and ensure the day-to-day health of their IT environment. Regular security logging is often instrumental when it comes to knowing the ins and outs of your network security and operations.

WHAT ARE SECURITY LOGS USED FOR?

Security logging is a process that collects a full record of events occurring within an MSP's networks and systems. Security logs contain log entries—data related to each of those specific events. The log entries are then regularly audited and used for the following:

- Identifying indications of unauthorized activities attempted or performed on a system, application, or device
- Satisfying security compliance framework requirements
- Establishing normal operational baselines and trends and building organizational standards, policies, and/or controls
- Providing evidence during investigations, audits, and forensic analysis

CHALLENGES OF IMPLEMENTING SECURITY LOG MANAGEMENT

Often, MSPs looking to bolster their logging capabilities turn to tools such as SIEM (security information and event management) and LMS (log management systems). No doubt, these types of tools can aggregate incredible amounts of data from multiple sources in an infrastructure to provide visibility. However, with so many MSP products available on the market, which ones truly enhance your security stack?

Traditional logging tools collect raw data in a centralized platform and apply behavioral logic to trigger notifications on incidents or security events. In a combination of data collection, rules, notifications, and data consolidation and correlation, they work to provide real-time visibility across an organization through event log management. After consolidating the data across all sources of network security information, they then correlate the events gathered based on pre-established rules and profiles, and finally notify on security events.

While these tools are designed to dig through copious amounts of logs and identify anomalous behavior or opportunities vulnerable to threat actors, they are slow to derive immediate context, especially in the event of a security breach where response times are critical. When building a trusted end-to-end security offering, it is vital to understand how logging tools work, their benefits, and their limitations so you can make an informed decision on how to better secure your IT environment.

Cannot Provide Real-Time Response

During a security event, cutting down on response times is crucial to safeguarding sensitive data. To do so, MSPs need a proactive and agile approach to real-time response. While many logging platforms are good for defending against known threats within fixed parameters, their rule-based approach may not translate well to advanced threat response. Since they are built to alert on potential threats after locating evidence within aggregated data logs, their reactive models can lack the context needed to provide actionable data right away. If you are unable to pinpoint anomalies in real time, you will not be able to make timely decisions on how to tackle critical events. Real-time logging is a start to collecting valuable information and ensuring visibility across an IT environment, but the true value is in real-time data interpretation allowing for immediate action.

Requires Expert Configuration And Manual Upkeep

Logging tools need to be configured specifically to meet an MSP's business needs and its unique threat landscape. Many logging tools require management from a dedicated team to parse logs and reports, update rules, respond to alerts, and keep the software updated. Much of this work is manual, which can be a significant hit to efficiency levels. And consider this: The configuration will need to be reviewed often to ensure that the platform augments data analysis rather than hindering it. If it is not regularly calibrated to monitor evolving types of networks, it cannot keep up with logging dynamically changing data.

Managing Data Collection, Analysis, And Search

The effectiveness of logging tools is based on both the quality and amount of data they logs. It is easy to overload your systems with huge volumes of data sources, creating noise and alert fatigue. If a team is busy responding to an unfiltered stream of alerts, they may miss the ones that are critical in identifying bad actors. The team would also need to perform manual parsing, filtering, and consistent re-evaluation for validity. Furthermore, many logging tools operate under the use case scenarios that you implement. There is simply no way to categorize incoming data into a simple binary of "malicious" or "safe."

In the long term, the key takeaway is to understand that traditional logging platforms and tools are designed to log thousands of events daily. As you store these ongoing logs, it can be overwhelming to keep data organized enough to ensure efficient search capability. The more information that you must interpret, the more inefficient it is to derive real meaning from the data.

HOW TO ENHANCE LOGGING WITH MDR

Combining both data logging and advanced tradecraft detection technologies means that you can monitor your account activity and behavior in real time—a critical factor in staying ahead of threat actors. A 24/7, active threat hunting-and-response service provided by experienced analysts can detect reconnaissance activities at their earliest stages. With logging, monitoring, detection, and response executed in tandem, managed detection response (MDR) analysts have unparalleled visibility into hacker tradecraft, lateral spread, and remote privileged activity.

While traditional logging tools such as SIEM and LMS are not effective for real-time threat detection and response, they are an excellent means of discovering raw data and meeting compliance expectations. Their strength lies in housing the substantial amounts of data needed to aid in investigative efforts and audits. Also, they are valuable in helping organizations build monitoring controls and improving threat profiles based on logged evidence of suspicious behavior.

To create a more robust security solution and ensure full threat visibility, place the power of log aggregation with an MDR platform. MDRs are designed to provide real-time response across your IT environment, proactively threat hunt for evidence of advanced malware, and identify key indicators of compromise. Experienced analysts can sift through complex security logs, collecting the threat intelligence needed to actively search networks, then detect and detain threats that evade antivirus or anti-malware solutions. Implementing an MDR solution allows the data to be quickly parsed for patterns and correlations that may not have otherwise been recognized.

In the hands of an experienced MDR team, real-time comprehension, threat hunting, and response can enhance the value of security logs and telemetry collected from your network processes, devices, and systems. Maximize the power of log collection by pairing it with active threat hunting and immediate response provided by an MDR. MDR analysts can leverage the raw data logs to help MSPs stay ahead of cyberthreats. Rather than overwhelm your teams and systems with complex data logging platforms, extensive data logs, and alerts, an MDR team would be able to pinpoint indicators of threat in the data quickly so you can fight back against threats within minutes and hours, not days and weeks. ■

Making BYOD Safe

How Dean Lause Is Mitigating The Massive Cybersecurity Risk All Businesses Face With His Bring Your Own Device (BYOD) Plan

WITH DEAN LAUSE, CTO/COO OF ARGENTUM IT

In early 2020, Dean Lause, Chief Technical Officer of Argentum IT, received a frantic call from the head of a prominent law office.

The staff at the law firm had become accustomed to working remotely, and business was booming. The partners were enjoying the advantages of the work-from-home environment—productivity was up, costs were down, and employees were feeling a greater sense of work-life balance. It only took a few seconds for that to change. Across town, one of the firm's attorneys was running to an appointment while quickly sending a few emails. Suddenly, he froze and had an uneasy feeling. Did that last email go to its intended recipient? He checked his sent items and felt his knees buckle. Sure enough, the message, which contained the firm's entire customer list, had just been delivered to its biggest competitor. The fallout was tremendous.

Not only did the head of IT find himself looking for a new position, but the law firm also found itself in the precarious position of needing to reestablish trust with its clients after proprietary information had been disclosed so carelessly.

It's disasters like this that play out in companies every day that have Lause on a mission to get companies to implement what he refers to as the Bring Your Own Device (BYOD) plan. "Part of what I do is help companies implement BYOD strategies that work," Lause explains. "With the proper security controls and precautions in place, you can protect organizations and prevent sensitive data leakage, potential lawsuits, and even sabotage."

Lause, who adopted a work-from-home lifestyle 25 years ago, says that even before the COVID-19 crisis, companies were adapting to the BYOD environment because of the numerous advantages, which include reduced expenses, improved productivity, and greater employee satisfaction. "Businesses that take advantage of BYOD practices can save at a minimum $350 a year per employee," Lause says. "Using portable devices for work purposes saves employees about an hour per workday as well as improves productivity by up to 33%."

While there are advantages, BYOD also poses a significant risk to a company's network, files, phone systems, emails, and contacts as well as a host of sensitive information, including human resources reports, health information, legal documents, trade secrets, and even marketing lists. "You can no longer be penny-wise and pound-foolish when it comes to cybersecurity and devising BYOD policies," Lause says. "If companies are going to allow individuals to use their own device to access company data, they must have some way to contain the information that is private or proprietary to their organization

and have control over what happens. As an example, an individual cellphone connected to internal wireless networks could have malware on it. That individual can inadvertently download it and infect a company's network. This is just one of the many reasons for having the policies in place ahead of time."

When Lause devises BYOD policies, he begins by leading clients through a discovery process, which includes determining their needs, figuring out what they are trying to protect, defining their framework for security, and assigning protocol. "It's vital for companies to consider why they want BYOD in place and to examine their needs and concerns," Lause says. "This is the most important item to decide upfront. For example, is it to improve workplace productivity or is it to make a network more mobile? Whatever the reason, a BYOD policy should be designed to optimize goals and be based on a strategy."

THE 4 ESSENTIAL ELEMENTS OF A BYOD PLAN

Once clients go through the discovery process, it's time to map out a detailed plan, which includes consideration of four essential elements: security, privacy, updates, and education.

"The mobile device policy is a place to outline the safeguards a company has in place and what they reserve the right to do with them to protect the good of the company," Lause says.

"This includes things such as protecting mobile devices with passwords, requiring applications to be approved before being installed, and policies for lost devices or how you'll remove data when an employee exits, among others."

When instituting these guidelines, there are some areas that you'll walk a fine line when addressing, such as privacy and updates. "If you choose not to include things like mandating system updates in the BYOD policy, you at least want to make a provision that the employee will be liable if data is stolen as a result of their device not being kept current," Lause advises.

He also stresses that everyone be educated on the policies and restrictions in the BYOD policy. "If employees don't understand, don't have the ability to ask questions, or don't know which questions to ask, the policies put in place are going to fail," Lause says.

Lause has a comprehensive cybersecurity process for his clients that includes weekly microtraining and a dashboard that consistently updates their security score, which is much like your credit score, but for the entire organization. Companies that are compliant are not only more protected from hackers but they are also likely to get a break on their cybersecurity insurance rates. "If companies can prove they're doing the training and keeping their BYOD policy up to standards, then they get significantly reduced rates on their premiums," Lause says.

> **"IF YOU'VE TAKEN REASONABLE CARE TO ENSURE THAT YOUR CLIENT'S TECHNOLOGY AND BYOD POLICY IS CURRENT, THE CHANCES OF THEIR GETTING HACKED ARE GREATLY MINIMIZED."**

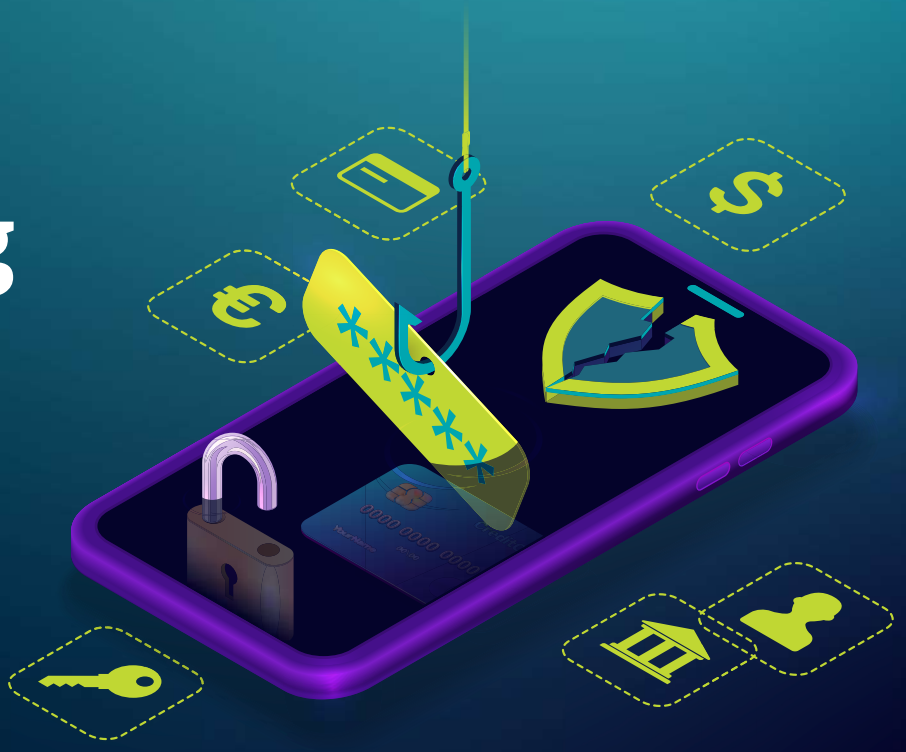
As the number of small businesses getting breached continues to go up, Lause advises MSPs and managed security service providers (MSSPs) to offer BYOD policies and urge their clients to put one in place immediately.

"It's no longer an option as to whether or not you should put a BYOD plan in place," Lause says. "Hackers love to target small businesses because too often, small businesses don't invest in current technology, don't enforce making sure machines are patched and up-to-date, and don't have policies in place. The stiff fines, data privacy rules—which can require additional costs, such as providing credit-monitoring services to all your customers if you get breached—and the recovery costs can put people out of business. But this can all be mitigated in a cost-effective solution if companies work with a knowledgeable MSSP. And when you compare the cost of recovering from a security breach to the cost of maintaining a high-level secure environment, there is no comparison. The cost is minimal for investing in current technology versus lost business reputation, fines, and recovery, which most small businesses find difficult to do and is why 60% of them are out of business within six months or less after a breach."

In the end, it's important to remind your clients that your BYOD plan is not a "set it and forget it" policy. Review it with them regularly and stay current with the new dangers popping up every single day. "If you're not talking to your clients about security and their BYOD policy on a quarterly basis to review their exposures and new threats, your clients are likely behind the times and vulnerable to much larger risks," Lause says. "The most successful BYOD policies are adaptable and fluctuate with our times and technological capabilities. Remind your clients that it is never a bad idea to consult you, and that regardless, they should always exercise due diligence and use common sense. If you've taken reasonable care to ensure that your client's technology and BYOD policy is current, the chances of their getting hacked are greatly minimized."

For more information on Argentum IT, visit ArgentumIT.com. ■

As Phishing Evolves, So Does The Need For Prevention Strategies



BY MANOJ SRIVASTAVA, GENERAL MANAGER, ID AGENT/GRAPHUS

Phishing is, and will continue to be, the cybercriminal's favorite mode of attack. The reason is because it's very simple to dupe even the smartest person with a cunning email designed to wreak havoc on an organization. Approximately 97% of employees across multiple industries cannot recognize a sophisticated phishing email. It creates tremendous risk for companies and adds pressure on MSPs to keep them safe. Unfortunately, phishing is here to stay, and the bad guys are only getting better at it.

TYPES OF ATTACKS ON THE HORIZON

MSPs should be mindful that phishing attacks will continue to evolve in 2023. They will need to budget accordingly and anticipate spending more funds on preventive measures than they did last year so they can protect their customers' infrastructure as well as their own. Here's what to look out for.

Attacks will get more creative. Spoof emails will become more difficult to differentiate from authentic ones. Email users may see clever subject lines with messages such as "changes to your health benefits" or "unusual login detected." Other popular modes of attack could revolve around declined memberships, fake calls-to-action about subscriptions, and billing and payments alerts.

Cybercriminals are also getting savvier with their use of deceptive links. Unsuspecting users may be misled to click on links that then send them to malicious websites. And that's not it. Methods using artificial intelligence (AI), such as cloning someone's voice to get them to reveal sensitive information, will become more commonplace.

Clients in certain sectors may require more support. The top five sectors in which employees interact with phishing messages are consulting, apparel and accessories, education, technology, and conglomerates/multinationals. There are opportunities here for MSPs when it comes to offering security awareness training as well as the implementation of anti-phishing tools.

KEEPING CLIENTS SAFE

Phishing prevention requires a comprehensive strategy that incorporates AI, email security, and cybersecurity awareness training. The first line of defense is to invest in AI-based prevention tools that monitor and analyze email communications for behaviors such as the devices' external senders and employees, whom they message, what time of the day do they communicate, and where they communicate from. This information is used to generate profiles of trusted email senders, then compares incoming emails to these profiles to authenticate the sender and detect and prevent phishing attacks. AI-based monitoring software can even detect false login pages and recognize altered signatures via scanned images. Malicious emails are automatically quarantined so the end user never interacts with harmful messages.

> **"APPROXIMATELY 97% OF EMPLOYEES ACROSS MULTIPLE INDUSTRIES CANNOT RECOGNIZE A SOPHISTICATED PHISHING EMAIL."**

Email security is another essential tool to combat cybercriminals. Solutions that offer warning banners and flag suspicious emails allow users to quarantine or mark the message safe with one click. Compromised passwords can open the door to cyberattacks. An identity and access management (IAM) tool can combine single sign-on (SSO), multifactor authentication (MFA), and password management into one integrated solution. Another option is passwordless authentication, which reduces security risks associated with passwords. It works by authenticating a user's identity using biometrics, such as fingerprints and one-time passwords that require users to input a code that is provided to them via email, SMS, or an authenticator app.

Finally, an organization is only as strong as its people. Security awareness training is no longer a "nice-to-have." It is a necessity, and one that can be offered by MSPs as a service. By increasing security awareness, an organization can reduce its chance of having a cybersecurity incident by up to 70%. Security awareness training should be offered when onboarding employees. After that, phishing campaigns should be carried out monthly, since research shows that trained employees start losing what they learned at 4–6 months after each session.

CHANGING MIND-SETS IS PART OF THE STRATEGY

It's hard to argue against cybersecurity training, given the threat landscape, but it can be burdensome. For this reason, many organizations and their employees may not prioritize it, or they'll skip it altogether. The opportunity for MSPs to offer this training is ripe, with the easy sell that a cyberattack can result in lost revenues, damage reputations, compromise data, cause operational disruptions, and even lead to lawsuits.

To engage employees in company training so they don't see it as a chore or task, it needs to be simple. Training should be delivered in easy-to-communicate content, such as videos. The ideal time frame is 15–30 minutes to ensure maximum retention of what was learned. When it comes to compliance topics, there may be a lot of ground to cover. Rather than making trainings longer, they should be broken up into two or more segments. Whatever the subject matter, training should always be focused on one main idea and provide sample scenarios where participants are asked questions to test their knowledge of best practices.

Another thing to keep in mind is that there are many types of cybersecurity training that target various aspects of security. Topics such as clean desk policy, strong password practices, and how to avoid phishing scams would fall under training for protecting passwords, while data privacy would cover privacy risks and secure connections. Other useful training topics range from physical security to cybersecurity threats such as ransomware, account takeover, and business email compromise, among others. With many employees still in remote or hybrid work scenarios, mobile security training is equally critical, teaching employees how to secure their mobile devices and educating them about Wi-Fi security, device management, and backups as it pertains to mobile.

Phishing is not going anywhere, and attacks are only getting more sophisticated. There is tremendous opportunity for MSPs to help their clients with their cybersecurity strategies and solutions. It's more important than ever to be aware and stay on top of the latest threats to best advise and protect clients as well as your own business. ■

PHISHING AT A GLANCE

- **1 in 3 employees are likely to click the links in phishing emails.**
- **1 in 8 employees are likely to share information requested in a phishing email.**
- **60% of employees opened emails they weren't fully confident were safe.**
- **45% click emails they consider to be suspicious "just in case it's important."**
- **45% of employees never report suspicious messages to IT for review.**
- **41% of employees failed to notice a phishing message because they were tired.**
- **47% of workers cited distraction as the main factor in their failure to spot phishing attempts.**

Manoj Srivastava is the general manager of security for Kaseya's ID Agent and Graphus companies. He is the cofounder and former CEO of Graphus before it was acquired by Kaseya.

Learn more about how to prevent phishing attacks by visiting Graphus.ai or IDAgent.com.

What's The Secret To Bringing The Best Value To Your Clients?

WITH MATT KATZER, CEO OF KAMIND IT

Compliance will become mandatory for all businesses in 18–24 months, and Matt Katzer, CEO of KAMIND IT, introduces a new strategy that helps organizations grow their business and add value to clients amidst increasing security regulations.

In 2017, the United States Department of Defense (DoD) introduced a new security standard called NIST 800-171. It deals with the handling of CUI (controlled unclassified information) that applies to all contractors and subcontractors of the DoD. A few years later, in 2020, the DoD released the Cybersecurity Maturity Model Certification (CMMC) to enforce the new standard.

Any contractors who don't meet these standards by 2025, the DoD says, must forfeit their contracts. Matt Katzer knew that the CMMC was going to be a game-changer, so he decided to do something different. He realigned his business strategy in a way that would bring even more value to his clients.

"I knew CMMC would affect a portion of my clients at KAMIND IT, about 10%," says Matt. "However, instead of limiting CMMC to those clients, we chose to deploy a new strategy. We applied the CMMC security model to all our clients and treated security management and compliance as a continuous process." The result was added value for KAMIND's clients in terms of increased responsiveness, better education, holistic protection, and lower costs.

THERE ARE MORE DEMANDS FOR CYBERSECURITY STANDARDS THAN EVER BEFORE

When Matt worked at Intel Corporation, he was known for discerning new trends. "I'm able to look at data points and say, 'If we need to be here, we must do X, or we need to head in this direction,'" says Matt. "In terms of cybersecurity, there have been a few key factors that show which way the industry is trending. CMMC was one inflection point. Another inflection point occurred when the Biden administration announced an executive order."

In May 2021, Biden announced Executive Order 14028, "Improving the Nation's Cybersecurity," which seeks to, among other things, implement stronger security standards in the federal government. Matt points out that the federal government isn't the only institution pushing for strong regulations. Cybersecurity insurance companies are asking questions like "Have you deployed multifactor authentication?" and "Have you deployed security standards?" before they issue policies. Some are even demanding official accreditation. At the state level, governments are trying to decide what standards to implement. All eyes are on states like New York, which released a set of new cybersecurity regulations under 23 NYCRR 500 and is putting ubiquitous standards in place.

"There are many companies, including our clients, that are saying that if you want to do business with us, you're going to have to be at this level of maturity," says Matt. "We recognize that compliance is going to be required, and we better be ready."

For many businesses, prior to 2017, cybersecurity was an afterthought. However, in 18–24 months, Matt points out, businesses will need to prove they are meeting some minimum standard. "Now we are in the stage where people are demanding proof that you're doing what you said you're doing," says Matt. "It's no longer acceptable to attest to something . . . you now have to prove it." If businesses can't provide evidence and data to prove they're meeting compliance

standards, they'll lose out on insurance policies and client loyalty, and they'll struggle to compete in the marketplace.

CYBERSECURITY IS FOUNDATIONAL TO BUSINESS STRATEGY

KAMIND's philosophy is that cybersecurity is a fundamental component of your business strategy. KAMIND provides its clients the capabilities to implement cybersecurity as a foundation that continually improves and builds on itself. It's a new strategy and has led to KAMIND rethinking how it adapts Microsoft's strategy and licensing, and how organizations deploy compliance and security management on top of it.

Matt knows this strategy is effective because he wrote the book on *Office 365, Securing Office 365: Masterminding MDM And Compliance in the Cloud*, which has sold more than 280,000 copies. KAMIND is committed to spreading the message that organizations can no longer afford to think of cybersecurity as an afterthought. "Unless you put cybersecurity at the core of your strategy, you're going to struggle through the CMMC process. Not to mention, without a secure foundation, all functions are at risk, including cost, schedule, and performance, which are only effective in a secure environment," cautions Matt.

That's why Matt helps clients with a new approach: to view security management and compliance as a continuous process by utilizing CMMC so organizations can adapt and evolve successfully and add value to their customers.

AN IMPROVED APPROACH: SECURITY MANAGEMENT AND COMPLIANCE AS A CONTINUOUS PROCESS

CMMC was designed to offer a cost-effective solution for organizations to deploy a layered security strategy at all levels of the business. It builds on existing regulations and verifies by combining cybersecurity best practices from across the industry. It maps the process from basic to advanced cyber-hygiene and reduces the risk of specific cyberthreats. It's a blueprint for managing security and compliance over time—a continuous process innovation.

Of the 30,000-plus Microsoft Partners in the United States, there are only 276 that are managed Microsoft Partners, and only 54 of those can sell the DoD GCC–High and Azure Enterprise Agreement (EA) licenses. KAMIND IT is one of them.

Because the CMMC process and subsequent accreditation are often intimidating, Matt created a four-step process to help organizations prepare. They have also developed a simple DIY kit for CMMC Level 1 attestation.

KAMIND is a provider of cloud services in five different areas, including Academic, Corporate, Charity, Government Community Cloud, and GCC High (Azure Government) environments.

KAMIND IT security standards are designed around CMMC (Levels 1 and 3), NIST 800-171, and compliance standards so they can help clients build a baseline infrastructure. "If we don't start addressing cybersecurity and taking it a lot more seriously—every one of us—it's going to hurt a lot more than just your company," says Matt. "It potentially could hurt the entire nation."

THE RESULT IS BETTER VALUE FOR YOUR CLIENTS

When a business is designed around a continuous process, it is constantly evolving and has better responsiveness to clients and improved product deliverability. "Microsoft is already DoD compliant, and so, by going through CMMC and using Microsoft, you're already picking up all those layers of compliance," says Matt. "There's no need to bring in another tool because that could put your organization at a security risk, and you'd have to retrain your team on this new tool."

Think of an MSP business or an IT organization, for example. "Everyone wants to figure out how to leverage the technology so they can offer better service," explains Matt. "Continuous process, consistency, standardization, a common set of world-class tools—those things drive the business forward."

Once an organization gets a skill set built into their team, it can add more value by building onto those skills instead of teaching new ones. With that kind of education philosophy, businesses can provide unique offerings and, in turn, become price-competitive in the marketplace.

CREATING VALUE

Whether at General Motors, Intel, or KAMIND IT, Matt has seen the benefits of the continuous process innovation model. KAMIND's growth has been 25%–30% year over year because they've created a strategy of continuous improvement. It's evident that in another year or two, businesses need to have clear, documented, and verifiable plans in place, and KAMIND's goal is to help clients get to that next level of growth and bring more value to their team and clients.

"It's about the value you bring to your business and the value you bring to your team, because now you have a homogeneous strategy," says Matt. "Your team knows how to execute. Your team knows what the guardrails are. Your team can provide a better product to your customers and their clients and your clients' shareholders."

For more information about KAMIND IT, Inc. and Microsoft security, visit KAMIND.com. ■

9 Critical Questions Your Customers Need To Answer To Survive

BY MIKE MORAN, PRESIDENT OF AFFILIATED RESOURCE GROUP

As more and more cyberattacks hit the headlines, business owners today are waking to the realization that they must have a robust cybersecurity solution. Unfortunately, far too many organizations are just barely scraping the surface of what cybersecurity truly requires today.

What's typically missing is a comprehensive security plan and cybersecurity checklist that everyone in the organization can follow. Just like a cyberattack, ignoring these important cybersecurity policies and procedures can bring a business to a screeching halt.

Mike Moran, president of Affiliated Resource Group, has been serving Central Ohio manufacturers, distributors, professional services firms, and health care practices for over 20 years. For nearly a decade, Mike has also been sounding the alarm for his clients to follow a well-defined cybersecurity and compliance plan.

Which Businesses Put Themselves At Risk By Not Following A Security Plan?

Mike says, "Any organization that captures, uses, stores, manages, or transmits protected data must have a cybersecurity plan in place. Some industries, such as the financial industry, health care industry, and Department of Defense contractors—and subcontractors—require data protection plans. But ultimately, any executive concerned about their reputation and bottom line should have a comprehensive cybersecurity plan." The state of Ohio even passed a Cybersecurity

Safe Harbor Law that provides a defense against civil litigation when a company has created and actively implemented a cybersecurity plan."

Cyberattacks wreak havoc on bottom-line dollars. Sixty percent of the time, cybercriminals target small businesses. Then, on average, it can take three workdays or longer to recover. Think about how much revenue loss and productivity loss—and how many potential lost customers/clients—you could incur in those three days.

5 Steps Toward A More Proactive And Secure Environment

When disaster strikes at home, you know what to do. But most executives have no clue what to do when a hacker locks down all their data and demands tens of thousands of dollars in cryptocurrency.

Mike says, "Affiliated Resource Group has modeled our checklist and cybersecurity solutions based on the government-recommended best practices approach [the NIST Cybersecurity Framework], and we have presented this five-step security model to all our clients and prospects over the past five-plus years. And once they start adopting these measures, they start to gain control of their IT environments."

STEP 1: IDENTIFY

Before you can protect your network and data, you must better understand what you are protecting.

✓ What exactly are you trying to protect? Make a thorough list of your technology assets.

✓ What are your expectations in getting your systems back up and running and preventing a data breach?

✓ Determine your current level of risk with a comprehensive risk assessment.

"With our once-a-year risk assessment," says Mike, "we help our customers with their assets and software. Next, we sit down with the leadership team and put their priorities on paper to maximize IT efficiencies and security."

STEP 2: PROTECT

This is where most companies focus their IT efforts, but it can't be the only area of focus. In this vital step, you should be able to answer the following questions:

✓ How do you log in to your systems and who can log in?

✓ Do you have a password policy and procedure? More importantly, is everyone in your organization following it?

✓ Do you have current policies and procedures regarding adding antivirus software and patches?

✓ How does your backup work and what does it cover?

"In a recent survey," Mike says, "one-third of companies admitted their backups were not good enough if they ever had to recover from an incident. They risk losing considerable data and productivity."

✓ Are you simply protecting your end points with antivirus software?

✓ Do you have a user-awareness training program?

Simply sending out a phishing email test once a quarter is not sufficient. You should implement an ongoing awareness program that trains every team member.

STEP 3: DETECT

People often assume burglar alarms prevent robberies. However, it's more of a detection tool because an alarm sounds and people are notified of a potential incident. In cybersecurity, the proactive stage of detection is crucial to significantly reducing exposure and preventing data theft.

✓ Can you detect when your network is potentially compromised?

✓ How soon after this compromise do you get an alert?

"Many ransomware attacks start with the hacker breaking into the system months before they lock your data and request a large payment," Mike says.

STEP 4: RESPOND

You come into the office, find your system is down, and can't access any files. Fear consumes you as you stare at a daunting message saying you won't get your customer records until you pay $25,000—or more. What do you do? Mike says, "The steps you take next could very well determine if you get your data back, how much you pay, if anything, and just how long your employees are sitting idle and unproductive."

✓ How do you mitigate the threat and isolate it to a single computer?

"Most people simply turn off the compromised computer," Mike says. "That's not necessarily what you do. Rather, you keep it on and disconnect it from the network. Also, instead of scrubbing the machine, it's important to do forensics on it to prevent further damage."

✓ Have you documented your response plan?

✓ Whom do you need to call—your cyber liability insurance or the authorities?

✓ What is the message you want your staff to convey to customers, clients, vendors, etc.?

STEP 5: RECOVER

"This is why I love my job and our team," says Mike. "In the rare case where a client endures a cyberattack, I get to call and tell them that our managed backup-solution process worked—we successfully remediated the exposure and recovered all their files. At that moment, I can feel all their worries melt away."

But if you want a happy ending to your own story, it's crucial that you have a plan in place to successfully restore and return your affected systems and devices back to normal. Here are questions to consider during the recovery step:

✓ Can the system be restored from a trusted backup?

✓ How soon can systems be returned to production?

✓ How do you ensure similar attacks will not reoccur?

For over 27 years, Mike Moran and his team have been affiliated with their clients to help them accomplish their goals. He says, "We have customers who have counted on us for 12, 15, and even 18 years. We do everything we can to improve their protection and improve their efficiency. We are affiliated with them, and they are affiliated with us. Hence, our name—Affiliated Resource Group."

For more information on Affiliated Resource Group, visit AResGrp.com. ■

9 QUESTIONS EVERY ORGANIZATION NEEDS TO ANSWER TODAY

You should never abdicate the critical pieces of your business. That includes information technology. While your internal IT team or third-party IT provider should handle your cybersecurity technical environment, you should also have a clear picture of your cybersecurity policies and procedures. After all, a cyberattack will negatively affect your business, your finances, and your productivity.

At the very least, you should know the answers to these nine crucial questions:

1) What do we want to protect?

2) What are we required to protect?

Mike Moran says, "Your state, your industry, and the type of data you collect determine if you must protect that data or risk fines and lawsuits."

3) How are our applications prioritized, and which of them are most important?

4) What are the relevant threats to our organization?

"While everyone thinks of external threats like ransomware and viruses, you must also consider internal threats," says Mike. "As an example, your customer list is an attractive asset to employees who are considering leaving the organization."

5) How comfortable are we as an organization with our ability to actively respond?

6) Who is responsible for our programs?

Mike says, "Simply saying, 'My internal IT team or our third-party IT provider is responsible' is the wrong answer. Everybody in your organization, especially the leadership, is responsible."

7) Do we have a response plan in place in case we get hit?

8) When was the last time we reviewed and updated our systems or had a risk assessment?

9) Can we do this ourselves?

Is Reliable IT At The Top Of Your Customers' Risk Management? It Should Be!

BY GARY TONNIGES JR., CPA & CEO OF TRIQUEST TECHNOLOGIES

In the past, cybersecurity and tech have stayed in the IT department. Today, CFOs must lead the conversation about cybersecurity business risks or jeopardize the business altogether.

Four times a year on average, business executives—including but not limited to CFOs, CEOs, and department heads—sit down around a rectangular table facing a whiteboard or projector screen. At the top of the whiteboard, written in red marker, reads "Key Business Risks." They have a detailed report in front of them with worst-case-scenario line items like compliance failure, building risks like fire, and human risks like injury. Then somewhere down on that list is "cybersecurity." On that item, the conversation is brief. It's not the executive's problem; after all, that's why they have an IT team. "Let's make sure data is protected and our systems are secure," they say, and everyone at the table agrees. They assign their IT tech to the task and check the box. Done and dusted, right? Not quite.

WELCOME TO THE DIGITAL REVOLUTION

Before the digital age, it was routine for businesses to leave tech conversations within the IT department—outside of larger dialogues around operations. IT was tucked away in a back office, taking care of abstruse coding and software installations, and the business plugged along.

Today, we're in the mid-digital age, the dual-sided coin of digital transformation where, on the one side, nearly every business uses some level of technology—like apps, scanners, or mobile devices—to connect processes and execute business strategy across the entire enterprise.

The other side of the coin is more problematic: though businesses use digital tools prolifically, they don't fully grasp the risk that ineffective technology practices pose to their business. Keeping discussions about technology isolated in the IT department is the root of the problem. What happens when their business tech suddenly stops working? Is confidential information or customer loyalty at stake?

What separates a business that thrives from a business that flounders—or closes entirely—is whether they are having conversations at the executive level about how reliable IT impacts business strategy and business risk. It's a conversation that CFOs need to initiate. If they don't, they leave vulnerabilities on the table ripe for exploitation. Money isn't the only thing it will cost them. Odds are it will cost them the entire business. Data from the National Cybersecurity Alliance reports that 60% of SMBs that suffer a cyberattack go out of business within six months.[1]

TECHNOLOGY-ENABLED PROCESSES

What gets businesses thinking in the right way is to see the big picture and lay out their most essential processes: the steps, tools, and people they use to get their product or service from the factory floor to their customers. How many of these processes require technology to complete? Imagine what would happen if, during those processes, technology stopped working. Here's an example: A manufacturer ships products across the nation. To get products to customers, employees use computers and scanners that document and track packages as they are loaded on a truck. Then tracking software gets hit with ransomware, and the company is locked out. Business productivity decreases, employees are less efficient or can't work at all, and valuable customer loyalty is lost because their package never shows up. All that comes down to

losing dollars—a lot of them. Similar scenarios can be applied to all businesses. The processes businesses use to accomplish tasks and meet goals are what I call "technology-enabled processes."

Historically, we didn't have to worry about them because they didn't exist. In the mid-digital age, nearly every process, start to finish, involves some level of technology. The architect draws their plans for a wall on AutoCAD and sends it to the contractor. The general contractor receives it on an iPad, and they send it to the foreman in the field. The foreman has a wireless setup on-site, and they use the iPad to show the drywall contractor how to do the work. If the iPad stops working or can't open the AutoCAD file, work halts until the tech is back up and running. This costs time, and we all know that time costs money.

Businesses must understand that for them to make a profit, protect employees, satisfy customers—and consequently grow—they need reliable IT. They need processes that work every time, updated software, backup plans, and regular assessments. Efficient IT processes must be a priority at the executive round table.

IT IS THE HOW, BUSINESSES ARE THE WHY

The tendency is to think that IT is recondite—CFOs don't think through IT strategy because they "have people for that." We need to shift that mind-set. Here's a distinction that helps business executives understand: IT teams are the how; the whole picture of the business—from customer needs to employee safety—is the why. This gets problematic because tech teams assume that CFOs understand how much they rely on IT. CFOs assume IT people will come to them and say, "If you don't replace this tech next year, you'll have a big problem." However, IT teams aren't always privy to the innards of business processes outside their department. Because of this misunderstanding about where IT should live, there's a malinvestment of resources to cybersecurity, putting businesses at much greater risk.

What reliable, responsive IT means to each business is as unique as a thumbprint. The general contractor needs wireless mobile devices that work in the field every time. A theater needs scanners that never miss a ticket barcode and get guests through the door and seated for a show in minutes. A manufacturer needs scanners and label printers to send packages out on time.

Processes are unique, but what's consistent is the fact that while technology can't create strategy, it can help implement it, and that's why tech decisions must move into the boardroom to be evaluated alongside other key business risks. Tech is the how, but business strategy is the why.

"IF ONLY WE KNEW"

Oftentimes at TriQuest Technologies, we get new customers who come to us after an attack and say, "If I had understood how important cybersecurity was, of course I would have spent more money to protect the business." So, what we try to do is underline the connection between IT solutions and what is likely to happen in a business—i.e., business risk—because that's effective cybersecurity. When executive teams discuss key business risks, they think about what's most likely to happen, what the cost or damage will be if it does, and how to go about reducing the likelihood of that occurring. Cybersecurity issues are very likely to happen; that's the reality.

It's most likely that through an email system, someone is going to compromise employee credentials and use them to implant viruses or impersonate employees and reroute customer payments to themselves, for example. The ultimate expression of what a business values is where they spend their money. If they thought of cybersecurity like protecting against a fire hazard—where purchasing software that blocks malicious emails is like buying an automatic fire-suppression system—they'd be putting value in the right place: protecting against the right risks with reliable solutions. As businesses strategize around how to reduce risk, funding effective cybersecurity practices must be a priority.

HOW TO ALIGN BUSINESS EXPECTATIONS AND REALITY

At TriQuest, we help business leaders understand the status of their technology processes by interviewing every department head. We ask what's going well, what can be improved, and how technology impacts their short-term and long-term goals. We ask leadership the following question: If technology stopped, what's the most damaging thing that would happen to your department? Expectations and reality must match.

Then we create a glide path—a three-year budget that includes a business's most critical data or processes and a pulse of IT performance. At the end of every year, we re-evaluate and create an adjusted three-year plan, and so on. This way, we're accounting for new growth, updated processes, and renewed goals. With a reliable IT plan in place, businesses benefit from interdepartmental cooperation, consistent decision making, and standardized processes.

It's a digital revolution. Data abounds, everything is connected, and files live in the cloud. Businesses that consider effective cybersecurity practices along with other key business risks can lessen the impact on profit, downtime, and efficiency as well as negative effects on employees and customers. Businesses that have unreliable IT are held back when they try to push the gas pedal. Next quarter, have a conversation with your clients. Help them reduce the risk to their business and customers by demanding reliable IT and keeping up in the digital age.

For more information on TriQuest Technologies, please visit TriQuestTech.com. ■

1. See www.sec.gov/news/statement/cybersecurity-challenges-for-small-midsize-businesses.html.