Tech Data

SECURITY SENTINEL

// SECURITY NEWS YOU CAN USE

SPRING / SUMMER 2020

TABLE OF CONTENTS

WELCOME TO THE SPRING/SUMMER EDITION OF *SECURITY SENTINEL*, OUR PARTNER NEWSLETTER, TO KEEP YOU UPDATED ON THE LATEST SOLUTIONS WE PROVIDE THE CHANNEL.

I trust there are many of you who are settled into working from home, or at least have your new routine defined. I recently participated in an online panel discussion about best practices when working from home, and there are so many great ideas. The most important is regular communication with your teams. Whether you use Skype, Slack or Zoom, make sure you turn on the video camera and see your team. It can create that motivation we all need to tackle the day. Our team has been experimenting with fun games during our meetings like "crazy hat day," "guilty-pleasure comfort food day" and "t-shirt you should have thrown away 10 years ago day." Whatever you do, do it often and make it real. Ask how people are doing and let them talk to you about their challenges if they need to. It'll relieve pressure and keep everyone focused on the task at hand.

One of the most common questions I've been asked recently is where I think the security market is going over the coming quarters. There's still much uncertainty about the exact timeline of progression, but we do know that security will remain an important part of the strategy for most customers. In the short term, sales of firewall licenses, endpoint security solutions, VPN clients and email security will continue to rise as companies are stabilizing a new work-from-home employee base.

I've also seen an increase in ransomware and malware attacks as bad actors assume that IT staff are distracted with other tasks. This increase creates an outstanding opportunity for the channel to respond with a continued focus on security solutions for customers. Assessments offer a fantastic entry point to identify areas of opportunity in a network, and penetration testing is a great way to provide your customer with some assurance that they are prepared ... or not. Email security will also remain important, as almost 90% of threats start with a user clicking an email hyperlink that they shouldn't. Let's stay focused and take advantage of the opportunity to support those customers who desperately need our help.

With so many people working from home who suddenly have more free time, it also creates an opportunity for training and enablement of both the channel as well as your customers. For partners, check out our new Digital Security Practice Builder website. It has over 30 hours of content to help you build or enhance your security practice. We also offer RangeForce, which is a self-service, on-demand cybersecurity technical training program featuring over 160 interactive modules made to hone cyber skills. Reach out to securityservices@techdata.com to learn about these offerings and more.

In closing, I believe security managed services will continue to see growth this year as customers will be challenged in managing their own security and look to outsource that function. The Tech Data RECON MSP Catalog is embedded in the Tech Data SPI Tool. It provides a list of all the security vendors offered by Tech Data, which have programs designed for MSSPs, including subscription pricing and white-labeled solutions. Stay tuned this year as our team releases new MSSP focused content and virtual events.

The opportunity to assist your customers with securing their employees and networks is tremendous, so reach out to your Tech Data representatives for more information about how we can help you create bundled security solutions that will make a difference. Until next time...

Alex Ryals
Vice President, Security Solutions, Americas, Tech Data

EXPERT INSIGHT IS KING:
EXPLORING THE TECH DATA CYBER RANGE WITH cSTOR

The Tech Data Cyber Range offers both physical and virtual events for partners and end-users who are looking to expand their knowledge and capabilities in cybersecurity. With Tech Data's valued reseller partner, cStor, take a look into all that the range offers.

The challenge of staying in the know when it comes to cybersecurity is a constant process. With threats constantly evolving, many end-users struggle to find the best security solutions for their business.

This obstacle is one of the primary challenges cStor faces daily.

"Understanding what's out in the marketplace, who's good and who's not good, who's going to be here next year and who's not is definitely a challenge for our customers since they don't have the time to do that research." Said Andrew Roberts, Chief Cybersecurity Strategist at cStor. "So usually, we spend that time doing the research for them."

Founded in 2002, cStor has succeeded in its mission to create solutions for clients when other companies could not. Specializing in cybersecurity, data centers and digital transformation for businesses of all sizes, they're continually looking for new and innovative ways to solve customers' problems.

However, that doesn't just mean they only look for the latest and greatest technology – rather, they look to their people to gain the skillsets and knowledge to guide partners to the right solution for their business.

"If we know where they [customers] are and where they're going, we can help guide them to a solution." Andrew said, "that also lets us guide their product selection so that something they buy today will still be useful three years down the road...If we have people who understand their long-term cybersecurity strategy, we can get them the right solution."

As cStor moved forward with their goals to increase mindshare and provide the best technology for their clients, they discovered the Tech Data Cyber Range.

The Tech Data Cyber Range is an immersive, hands-on learning environment designed to simulate real-world cybersecurity situations. These simulations can be used to prevent, detect or respond to known or simulated cyber threats. With Tech Data's cybersecurity experts providing guidance and insight, partners and end-users alike can solve for some of the most complex challenges facing the cybersecurity space.

But the one thing that drew cStor to Tech Data's Cyber Range, in particular, was the people that run it.

"I've been involved in cybersecurity for many years, and a lot of the people running the range I already know and have a lot of respect for," Andrew said on his favorite part of the range, "It really is about the people too, because technology is technology. Anyone can throw a few racks into a space, put some servers in there and run a few products to test out, it's the people that make it what it is and whether it's successful or not."

Vice President of Security Solutions at Tech Data, Alex Ryals, couldn't agree more. When talking about the Cyber Range, he said that expert insights were one thing he wanted to emphasize in the range itself. "I've seen lots of businesses and institutions put together cyber ranges in the past. However, they have not been successful because they didn't get the right people who actually understand what's going on or how to convey that information to others."

Since finding the range, cStor has utilized its resources and engineering expertise to showcase solutions to customers. From walkthroughs of new technology to case study reviews, cStor sees the range as a hands-on way to interact with partners, regardless of where they're located. "It's an environment where you can easily build relationships, whether it's cStor and Tech Data or our clients and us or a combination of all three," Andrew added.

As of now, cStor is planning for the potential of expanding to virtual events with the range, bringing together their team with Tech Data's engineering experts to create digital content and interact with partners. Andrew said regardless of if they can show up physically or not, "The Cyber Range can be used to bring people together, talk about their problems and not just hear about how they can solve it, but see it happen as well. And again, it all goes back to people and relationships, which is something we want to continually build with our clients."

Want to start building your cybersecurity relationships with Tech Data's expert team at the Cyber Range?

Check out our website at cyberrange.techdata.com to get started today!

Practice Makes Perfect:
The Importance of Stress Testing in Ransomware

VERITAS

*By: **Simon Jelley, Vice President, Product Management, Veritas Technologies LLC***

When it comes to ransomware, prevention is no longer enough. You need to have a data backup plan, and that plan has to be measurable and repeatable to keep pace with today's fast-moving attackers.

Ransomware is now big business. With estimated annual revenues of $1 billion, it's become a parasitic sub-economy, whose continued rise seems inexorable. However, getting attacked is not a price worth paying. The average attack costs businesses over $150,000 and does long-term damage to reputation and customer confidence. What's more, paying the ransom is no guarantee you'll get your data back – 20% of paying victims never reclaim their stolen data.

Data is your strongest asset, but it can also be your biggest weakness. It helps you anticipate change and cater to your customers, but it's also becoming more complex, varied and difficult to protect. To stop it falling into the wrong hands, you must have a strong security configuration and backup strategy in place. Now more than ever, you also need to put it through its paces.

Despite the heightened threat of ransomware attacks, organizations often still neglect to put their backup strategies into practice. Many data officers and managers think that 'it could never happen to me,' but ransomware attacks are very common. Across Europe, the Middle East and North America, more than a third of finance and insurance companies have been victims. A ransomware attack isn't a question of if, but when.

Complacency only puts your data in danger. If an attack is inevitable, then you shouldn't be caught unprepared. Backup plans are complex and multi-layered, spanning across multiple data and cloud environments. It's hard to predict how your backup plan will interact with all these systems until you put it into action.

It's important to stress that you can't just focus on the resilience of your primary data. The secondary data you create through backups and copies also needs to be properly defended and tested. Review how your backups are saved and then put them through the same process as your primary data. What's more, a number of backup solutions are building ransomware resiliency capabilities into how secondary is stored and accessed – take advantage of these.

When it comes to ransomware, prevention is no longer enough. You need to have a data backup plan, and that plan must be measurable and repeatable to keep pace with today's fast-moving attackers. You can't say you've truly recovered from a ransomware attack if it has done damage to your business through downtime and data loss. A tried and tested approach will not only boost response and resilience, it will deliver confidence to customers and stakeholders.

FOR ADDITIONAL INFORMATION, CONTACT THE TECH DATA VERITAS TEAM AT VERITAS@TECHDATA.COM OR CALL 800-237-8931, EXT. 5540408.

DISCOVER TECH DATA'S DIGITAL SECURITY PRACTICE BUILDER WITH BLACKHAWK DATA'S MARYANN PAGANO

By: Chris DesRosiers, Director, Security Solutions, Sales, Tech Data

With more and more businesses investing heavily in security products and solutions, and with cybercrime only increasing, the time to power a sustainable security practice is now. For technology solution providers, it can be time-consuming and costly to figure out how to build a security business that offers customers the best value and stands out from the rest.

Knowing this, Tech Data took on the challenge to remove the guesswork and help channel partners capture this opportunity through our Digital Security Practice Builder. Tech Data's Digital Security Practice Builder is an on-demand program that helps partners rapidly build a profitable security practice and empowers them to choose their path toward greater security growth. Through a simple assessment, the program offers partners a foundational way to quickly increase their knowledge and expertise around security as well as gain proficiency in one or more vendor technologies. It also provides a comprehensive outline of all the key components that are needed to help our partners and their customers build a new technology practice or expand their existing one.

With the recent launch of the program, we had the opportunity to connect with BlackHawk Data's Maryann Pagano, CEO and Director of Sales Operations, to find out firsthand the advantages of Tech Data's Digital Security Practice Builder.

DesRosiers: Thanks for joining us, Maryann! To start, what was your security practice like before you started the Tech Data Digital Security Practice Builder program?

Pagano: *I think we struggled to understand where to start, beyond just a firewall. I didn't realize how many vendors were out there and the diverse portfolio of security offerings available. I have a much better idea now and can see where our practice was lacking direction.*

DesRosiers: I'm happy to hear the program was able to provide you and your team more direction! Going into the program's process itself, how was the registration process to enter the program? Was the overview video by Alex Ryals helpful before you entered the program?

Pagano: *It was very easy! I liked the introduction from Alex because that was where I got a good understanding of building a security focus. Before that, honestly, I was clueless.*

DesRosiers: As you became comfortable navigating the platform, what did you gravitate towards first?

Pagano: *I reviewed the strategy portion first. Next, I moved to marketing and then services. Now, I am working through the enablement section.*

DesRosiers: Interesting path! What was the part of the program that offered the most insights for you as it relates to your role?

Pagano: *I think the understanding of the different areas of security so far. As we go deeper into the program, I think, marketing strategy will be a great help. Also, getting a better understanding of which vendors to go to market with was extremely helpful.*

DesRosiers: Where are the areas of the program that you thought were missing?

Pagano: *I can't tell yet. I think it has a lot. I can't wait to start to get people involved in the program from an engineering side to learn and get to pick their focus. I also want our sales teams to learn how to sell security through the program and how to ask the right questions.*

DesRosiers: What might you like to see on the site going forward?

Pagano: *I will come back to this one is a few weeks. So far, nothing.*

DesRosiers: How would you rate the program on a 1-10 scale, 10 being the best?

Pagano: *So far, for me, the program is a 10! I think it really sheds light on what you need to know to help give you overall direction.*

Are you ready to elevate your security practice? Visit practicebuilder.techdata.com/security to learn more and start your assessment today!

EVOLVING ENDPOINT SOLUTIONS AT TECH DATA

As we face a rapidly changing landscape in the technology industry, the conversation of workplace transformation remains a familiar concept to our endpoint organization. It has been the bedrock of our go-to-market strategy as we've helped our customers provide required mobile devices and next-generation collaboration solutions.

We understand that your customers need security solutions, and that alone can create incredible growth and earning opportunities for you. In addition to your network, cloud, mobile and IoT security opportunities, our endpoint product experts are ready to enhance and enable your security practice.

With more than 150,000 products with expert services and solutions supporting software, PC systems, mobile devices, displays and other customer electronics, we're ensuring that our customers are equipped to respond to changing demands in the market, including the increasing need for security solutions. As we work to adapt our strategies to fit the ever-changing needs of the technology channel, we're also adjusting the ways we disperse messaging to meet customer needs.

In fact, Tech Data's Endpoint organization brought many top vendor messages to market through the Virtual Endpoint Symposium. It featured the latest information from vital channel brands and kept partners connected with information to help them adapt to new marketing conditions.

You can view the recordings of our Virtual Endpoint Symposium at techdata.com/endpointsymposium.

Cyberinc

Eliminate attacks before the breach through Zero Trust Browser Isolation

"Remote browser isolation provides one of the strongest proactive security measures to prevent threats from reaching desktop devices, significantly reducing the attack surface. Cyberinc's offerings can help our partners looking to provide stronger defenses against the ever-evolving threat landscape and enable them to simplify and scale their security."

Alex Ryals,
President, Security Solutions, North America, Tech Data.

Great Margins	*Channel First Commitment*
Opportunity registration program with additional new customer bonus.	Complete support throughout the sales cycle.

Contact the Tech Data Cyberinc team at
cyberincUS@techdata.com / 1-800-237-8931 x5540509

www.cyberinc.com

EMPLOYEE SPOTLIGHT:
JULIE WAGONER, MARKETING COMMUNICATIONS SPECIALIST II

Q: What is your job title and briefly describe what you do at Tech Data.

Wagoner: *As a marketing communications specialist for our security department, I own the execution of key marketing campaigns and digitally led demand generation activities across the full funnel. I manage the security content strategy, overseeing content creation for a variety of our online channels including paid media, blogs, e-mail blasts, our website and social media posts. I'm also in charge of distributing the content to the appropriate media channels and measuring the success of our content marketing activities.*

Q: How does what you do provide value for the company, our customers and/or vendors?

Wagoner: *I'm responsible for increasing brand awareness and demand generation through our marketing content. Our content positions helps our brand to become top of mind and educates our partners on the latest security trends and offerings that are available to help them meet their customers' security demands.*

CONTINUE >

Give remote workers the protection they need

Carbonite® endpoint solutions are easy to deploy and manage from anywhere

Carbonite® Endpoint 360

Centrally managed endpoint protection for the entire workforce

- Remote deployment
- Admin- or user-restore
- Remote wipe & poison pill

Carbonite® Backup for Office 365

Cloud backup for Microsoft Office 365 applications

- Simple, central management
- Site-level or granular recovery
- Audit reporting & role-based access

Now's the time to protect the data that fuels the remote workforce!

For more information or to purchase, reach out to your Tech Data Team at 800-237-8931 Ext. 5540414.

CARBONITE
an opentext company

EMPLOYEE SPOTLIGHT: JULIE WAGONER, MARKETING COMMUNICATIONS SPECIALIST II

Q: What do you enjoy most about working at Tech Data?

Wagoner: *Working with great people. We have an amazing team of professionals who are experts and extremely passionate about what they do. This is an exciting industry to be a part of since cybersecurity is constantly changing. I love seeing our team adapt to these changes to find innovative solutions to help our partners keep their customers secure. It's an honor to help the team market game-changing opportunities like our Cyber Range and Digital Security Practice Builder.*

I also enjoy the opportunity to be part of a hard-working, creative marketing team, led by Kate Sneider. Last year, this new team quickly had to prepare to a comprehensive marketing plan to launch the Cyber Range as well as our inaugural Tech Data Security Enforce event. These projects were in addition to our monthly marketing efforts. It was a lot of work, involving many after hours, but both events were very extremely successful. I'm thankful to have had a marketing leader like Kate who provided her past experiences and direction to us to execute the launch of both events.

Q: What's a fun/interesting fact about you that not many people know?

Wagoner: *Most of my colleagues know that I've spent a lot of years working in social media. But I actually started obtaining my digital skills back in 1998. I worked with friends on creating a blog and in 2003, I conceptualized and produced a weekly online entertainment zine which featured album reviews, concert reviews, interviews with performers and industry related articles. I worked closely with publicists and promoters to obtain promotional materials, photo passes and interviews with the talent. This experience gave me the desire to pursue a career that would allow me to utilize my communication skills to positively contribute to a company's business objectives.*

Another fun fact – and this fact will totally confirm me as a millennial, but I've had my social content retweeted by Steven Tyler of Aerosmith, Lil Jon, Shania Twain and Ozzy Osbourne. I've also created content that received over a million views in less than 24 hours.

Valuable Resources to Build a
Secure Remote Workforce

We are in the middle of a seismic shift in how people work. As Time Magazine said it back in February, this will be the "World's Largest Work From Home Experiment." The number will dwarf the 3.2% of remote workers that normally comprise remote workers.

With your clients shifting to remote workers, it's your job as their technology solution provider (TSP) to help them build a secure remote workforce. It takes a group effort to secure a remote workforce—from security measures, tools, end-user training, and more.

Want to learn more?
Visit ConnectWise.com/OnePlatform-TD to see how ConnectWise can help you securely optimize your Remote Workforce.

ConnectWise®

Contact Tech Data to learn more about ConnectWise Solutions
1-800-237-8931 x87663 | ConnectWiseTD@TechData.com

VENDOR SPOTLIGHT: DISCOVER THE ISLA PLATFORM WITH CYBERINC'S TRACY HICKOX

By: Tracy Holtz, Director, Vendor Management, Tech Data

As we kick off our new fiscal year and expand our portfolio to bring on new vendors, I'm excited to host a new vendor spotlight and introduce you to one of our newest partners, Cyberinc!

Cyberinc is a pioneer in isolation-based cybersecurity solutions. Tracy Hickox, Vice President of North American Channel Sales and I had the opportunity to sit down and discuss their partnership with Tech Data, the current market conditions, and the benefits Cyberinc can provide to our security partners.

Holtz: We're excited about our partnership with Cyberinc and launching with our security partners. First, can you provide a brief overview of Cyberinc?

Hickox: *Cyberinc was formed in 2016 with a specific focus on the remote browser isolation space. Cyberinc helps you experience a safer internet by proactively stopping web, email, and document-based threats and effectively eliminating a wide variety of attacks delivered via these vectors – ransomware, phishing, malvertising, rootkits, and more. Cyberinc's Isla Isolation Platform is grounded on the principle of Zero Trust Security. The platform uses cutting-edge isolation technology to neutralize threats and prevent them before they have a chance to act, simplifying the security strategy and delivering immediate protection.*

Holtz: That's an interesting value-add Cyberinc brings to the table! With that in mind, what most excites you about the partnership with Tech Data?

Hickox: *We're very excited about your security practice builder program. Tech Data's broad reach into the partner community and your focus on educating and enabling your partners is critical to helping Cyberinc build our channel in the security space.*

Holtz: We're happy to have you joining our practice builder program as well! Speaking of practice builders and improving security postures - as cybercriminals continue to get smarter and more targeted in today's threat landscape, how does Cyberinc help protect against phishing, ransomware and malicious URLs?

Hickox: *Cyberinc's Isla isolation platform operates on the premise that with the outside world can represent a risk to the business and therefore isolates (or remotely renders) all access. All URLs – malicious or otherwise – are fetched, executed and rendered remotely, in a disposable remote browser, providing a clean visual stream to the endpoint to ensure a malware or exploit cannot impact an end-user.*

Isla protects against ransomware threats by disrupting the delivery of the initial exploit that can lead to a ransomware attack on the endpoint, thereby thwarting any encryption of data or lateral movement. Crucially, the Isla approach also doesn't necessitate any response and recovery from ransomware, thereby improving user productivity and unburdening security teams.

Plus, phishing attacks can be prevented again by isolating the execution of URLs, scripts and attachments from end-user devices, impeding the delivery of malicious content. Isla simplifies deployment and user experience while seamlessly integrating with the existing email infrastructures.

Isla even supports a native browsing experience, enabling end-users to continue using standard browsers, on all major platforms, including Windows, OSX and Linux.

Holtz: Sounds like a great solution – but where would you recommend Solution Providers/MSPs begin to look for opportunities within their clients? Which verticals or markets do you see driving the most demand for Web Isolation?

Hickox: *We believe remote browser isolation gives solution partners the opportunity to introduce their customers to a truly innovative security program to customers across a wide spectrum of industries. Large and small businesses can benefit alike from the simplicity of security, improve the efficacy of security teams, and productivity of end-users.*

Gartner estimates that over 80% of malware is delivered through the internet browser - a risk virtually every customer faces. This risk keeps growing every year as more applications and customers move to the cloud. In addition to these increasing risks, more customers are faced with the need to support people working remotely, whether at home or other locations.

Isla is offered two ways: either as a software, deployable in virtual or private cloud implementations, or as a completely scalable, turn-key cloud security service. It can also be delivered as a hardware appliance to customers who prefer a hardware-based deployment. Isla doesn't require endpoint agents or complicated installation or configuration.

Holtz: Moving into the benefits outside of the solutions Cyberinc can provide, what are some of the benefits of Cyberinc's partner program for Solution Providers/MSPs? What margin can a partner expect to make selling Isla?

Hickox: *Cyberinc's channel partner program ensures great partner margins through comprehensive deal registration, including a new customer bonus. Cyberinc Isla provides additional value to MSPs by reducing the number of security events they need to address, allowing them to focus resources more efficiently. The Control Center is fully multi-tenant and supports remote administration, policy management and reporting.*

Holtz: This is all great information, Tracy! I have one more question: who should our solutions providers call if they need a demo or POC setup on Cyberinc's Isla platform?

Hickox: *Cyberinc is ready to support partners with in-depth product training and sales support for customer opportunities. Please reach out to Sam Lucas, our dedicated sales specialist at Tech Data:*

Sam can be reached at cyberinc@techdata.com, or you can call him at 727-539-7429, ext. 5584244.

We continue to expand our portfolio regularly, bringing to market new technologies. Just this month, Tech Data also launched RangeForce. RangeForce offers 130+ continuous hands-on real-world simulation cybersecurity training, which can be leveraged to expand your clients or your internal security skills. You can learn more by contacting our security team at securityservices@techdata.com.

EMPLOYEE SPOTLIGHT: CHRISTINE MCGETTIGAN, VENDOR DEVELOPMENT MANAGER II

Q: What is your job title and briefly describe what you do at Tech Data

McGettigan: *My role is in enterprise sales and security solutions, which equates to everything services related under Tech Data's security umbrella – assessments: pen tests, vulnerability, compliance, product installations, configurations, upgrades plus our SIEM solutions. Geographically, I help cover areas east of the Mississippi.*

Q: How does what you do provide value for the company, our customers and/or vendors?

McGettigan: *My job is to provide services to our partners that don't have them already. We have a lot of partners who sell product, but don't have any consulting arm to help with installs – that's where I come in.*

We have a large team of subcontractors in place with Tech Data, giving me quick and easy access to consultants for just about any security product out there. I also talk to a lot of partners who want to offer pen tests and vulnerability assessments to their installed bases but have no desire to build that as part of their own business. Instead, they'll use Tech Data for that and our amazing pen testers that we have on staff.

CONTINUE >

WE'RE CHANGING THE RULES OF SECURITY

CYBERSECURITY HAS BECOME OVERLY COMPLEX.
WE WANT TO MAKE IT SIMPLE.

IBM®

THREAT MANAGEMENT

COMPLIANCE & PRIVACY

STRATEGY AND RISK

DIGITAL TRUST

OPEN INTEGRATION

HYBRID, MULTICLOUD ARCHITECTURE

AUTOMATION & ORCHESTRATION

SAAS/MSSP OPTIONS

CONTACT IBMSECURITYSOLUTIONS@TECHDATA.COM FOR MORE INFORMATION AND TO SCHEDULE YOUR VIRTUAL IBM SECURITY DEMO

EMPLOYEE SPOTLIGHT: CHRISTINE MCGETTIGAN, VENDOR DEVELOPMENT MANAGER II

Q: What do you enjoy most about working at Tech Data?

McGettigan: *I really love working with so many different partners and getting to meet so many different people. Even though I am 100% remote and don't get to meet my partners in person, I have the privilege of getting to know some great people online. I get to talk to people all over the US, and I like hearing about my partners' professional plans as well as their personal backgrounds.*

I also love working with this Security team. I'm very proud to be part of such a great group of folks and feel like I learn something new every day. I'm surrounded by smart people with some ground-breaking ideas, and you can't help but be proud to be part of something like that.

Q: What's a fun/interesting fact about you that not many people know?

McGettigan: *I don't have a hobby or talent, but living in New Hampshire allows for some great travel: We live surrounded by some of the most beautiful states with the Atlantic Ocean as part of the background.*

When my boyfriend and I began dating five years ago, we started doing a one-night-away trip every other month. Over the years we've been on some amazing getaways: We've seen the sunrise from the summit of Mt. Washington in New Hampshire; we've visited the 9/11 Memorial and Museum and Statue of Liberty in New York City; saw reindeer and traversed Cadillac Mountain in Maine; visited mansions, walked the Cliff walk and attended the WaterFire event in Rhode Island; scoped out some forts in Massachusetts; rode bikes around Lake Champlain in Burlington, Vermont; boated on Lake George; took in the beach and pier in Atlantic City; and spent time on Cape Cod, Martha's Vineyard and Plum Island. New England is truly an amazing place to see, and we never have a shortage of places to go!

Eyes wide open.
Phishing attacks shut.

Train employees to thwart and report phishing attacks with Barracuda PhishLine.

For more information, contact Sean Connoly:
barracuda@techdata.com
1 (727) 539-7429 ext: 5583859

Barracuda®
Your journey, secured.

Copyright 2020 Barracuda Networks, Inc. All rights reserved. All logos are trademarks or registered trademarks of their respective holders.

IS IT TIME FOR MSPS TO TRANSFORM?

By: Tracy Holtz, Director, Vendor Management, Tech Data

As you set business plans and strategies for the new year, an important element of your strategy is knowing when the right time is to transform engaging in new technologies and services.

I recently had the opportunity to sit down with Erick Simpson, co-founder of one of the first "pure play" MSPs in the industry, to discuss MSP transformation and why current market conditions are ideal right now to start making the switch.

Holtz: Hello, Erick! For starters, do you feel it's still a good time in the current market for a Solution Provider or MSP to become a trusted advisor and incorporate security solutions? Why?

Simpson: *It's now more essential than ever for providers to enhance their value as trusted, strategic advisors to their customers by focusing on enhancing their security posture. Guarding against cybersecurity threats and breaches as well as protecting corporate, customer and employee data is the number one concern of business owners today. Failing to rise to meet this challenge is simply unacceptable by anyone's measure. This statement may sound harsh, but I believe that any solution provider or MSP that's not already incorporating security services and solutions in their portfolio for their customers or are planning to do so in the near future, is doing themselves and their customers a disservice. Developing cybersecurity expertise is the single biggest opportunity I've seen in my 30-year career in this industry, and those that don't prioritize building this competency and capability now will regret it later.*

Holtz: That's a strong stance. Jumping off of that, from your perspective, what differentiates a managed service provider (MSP) from a managed security service provider (MSSP)?

Simpson: *This is a great question, and one that I've seen create confusion in both providers and their customers. I believe it ultimately comes down to focus, expectation and outcome.*

On one hand, a provider that has been delivering Managed IT Services as an MSP for many years probably feels that their focus is more about maintaining business continuity for their customers' users, business systems, services, devices and infrastructure. Because part of that business continuity philosophy happens to include patching, updating and protection from viruses and malware, they may have felt they were doing a good job of providing an acceptable basic level of security – and several years ago, some may have agreed. So, the expectation they have established with their customers is more than likely a sense of security and peace of mind that comes with a monitored, patched and updated technology infrastructure and end-user technical support, along with reports of how many tickets were closed on their behalf, backups completed, systems patched, and viruses mitigated.

In this scenario, it should be no surprise when a client believes they are also receiving "MSSP"-type services are amazed when their MSP now wants them to invest in additional security services to protect them from today's threats.

This brings us to an MSSP's additional value. An MSSP is typically focused solely on protecting systems and data from the threat of cyberattacks or breaches, as well as achieving and maintaining security regulatory compliance for specific businesses. This includes meeting minimum security compliance standards, monitoring for and mitigating security vulnerabilities, rapidly responding to security incidents, and potentially making security awareness training available to end-users.

Because of the focus of the MSSP, they typically don't bear the direct responsibility for maintaining the proper operation of the customer's hardware, system or services or manage end-user support requests as an MSP does, save when it impacts the security of the organization. This distinction allows for the co-existence of MSPs, or IT Providers in general, and MSSPs in serving the needs of shared customers.

Holtz: Absolutely! Co-existence provides an opportunity for all partners to support the evolving needs of their clients and offer unique value. What do you feel are the most important elements of a security offering that a partner should be offering as an MSP or MSSP?

Simpson: *A comprehensive portfolio to offer customers must address internal as well as external vulnerabilities and include security strategies to harden hardware, software, operating system, services and end-user security postures.*

An example cybersecurity solution stack would typically include multiple services like data and systems backup and disaster recovery, security event monitoring and incident identification and management, security software hotfixes, patching and updating, email anti-phishing, anti-malware and anti-spam solutions, DNS protection, dark web monitoring, firewall and core endpoint security monitoring and management, web filtering, password management, privileged access control, end-user security awareness training, mobile device management, Cyber liability insurance, security assessments, PHI/PII data scanning and encryption, multi-factor authentication and security regulatory compliance services. Some MSSPs may also offer these and other services through a security operations center (SOC).

Holtz: Wow, that's a lot to cover! It also leads me to my next question: At what point in an MSSP business should they build their own SOC vs. outsourcing?

Simpson: *As with any critical business decision, several factors need to be weighed when deciding to build vs. outsource. These include the organization's readiness in areas such as technical competency, scalability, efficiency, cost, profitability, and most importantly – risk.*

Many MSSPs decide to outsource SOC responsibilities to a third party because of their lack of maturity or readiness in these and other areas, finding it an equitable trade-off in exchange for the investment required to do so.

My personal rule of thumb is simple: a provider should generally only dezel they can do so better than anyone else. If delivering SOC services (or any other services, for that matter) does not meet this criteria, they should seriously consider outsourcing them until they improve their capabilities to do so in the future.

Holtz: That makes sense. Let's switch the topic to cyberattacks: Why do you feel the cybercriminals continue to target MSSPs with ransomware? What are your recommendations for partners to protect themselves from being a target?

Simpson: *These cybercriminals are evolving to become much more strategic over time, including intensive online research and employing social engineering tactics on their targets.*

Think about this: if it takes the same amount of effort to breach a single organization as it does to breach an MSSP that can become a conduit to potentially thousands of organizations, which approach pays the highest possible ROI for that effort? The answer is clear. To protect themselves from these cybercriminals, MSSPs should very simply be practicing what they preach – by implementing and consuming all of the security services they are delivering to their customers.

These should also always include investing in end-user security awareness training for their staff and adding cyber-liability insurance policies and riders to their existing business coverage.

Finally, they should ensure that the platforms they use to monitor, manage and maintain their services for their customers are highly secure, monitored, patched and updated regularly. They should also implement independent, complex passwords and two-factor authentication tools to manage all internal and external systems and service authentication activities.

Holtz: These are great tips! We're also excited to have you join our upcoming MSP Evolve virtual workshop. What are the three areas of value that a partner will take away from these working sessions?

Simpson: *We'll be covering three things. First, we'll discuss the operational considerations and strategies required to build a successful, high-performing cybersecurity practice. Second, we'll cover the services and vendors to partner with and include in your cybersecurity product portfolio as well as how to build, tier and price them for maximum margin. Finally, we'll discuss how to prospect for, qualify, present to and close cybersecurity business with new and existing customers.*

Holtz: Thank you for your time today, Erick! Before we end this discussion, I have one more question: We feel the workshops offer MSPs a business development curriculum to stimulate accelerated growth and sales velocity from participating partner firms. What are your thoughts on Tech Data's position in the market and our new value offerings such as Digital Security Practice Builder and the SPI Tool?

Simpson: *Tech Data has done an excellent job at enabling its partners to compete, win and grow their businesses utilizing advanced online tools and platforms like its Digital Practice Builder for training and enablement. Or its SPI Tool to help partners quickly and easily architect custom solutions with the right vendors, services and solutions to meet their clients' unique business needs.*

Holtz: Thanks again for the opportunity to sit down and discuss MSPs with you, Erick! We look forward to our upcoming July MSP workshop and partnering to provide our MSP community an opportunity to accelerate their growth.

Erick Simpson, co-founder of one of the first "pure play" MSPs in the industry, and creator of the MSP Mastered® Methodology for Managed Services business performance improvement and the Vendor Channel Maturity Level Index™ that identifies IT channel program maturation for strategic growth, is a strategic technology business growth specialist. He is one of the most prolific, recognized, and sought-after business improvement and transformation experts, authors, consultants and speakers in the industry.

With over 30-years of experience as an enterprise CIO, MSP and strategic consultant, Simpson is a business process improvement expert with hundreds of successful ITSP, MSP, security, and cloud improvement engagements, and has worked with numerous clients on the buy, sell, and integration sides of the M&A process. A highly sought-after IT, cloud, security, and managed services thought leader and speaker, Simpson has authored over 40 business improvement best practice guides and four bestselling books.

Learn more at www.ericksimpson.com.

Fortinet's Secure SD-WAN includes best-of-breed next-generation firewall (NGFW) security

Fortinet delivers a security-driven networking WAN edge transformation in a unified offering

To learn more,
Visit the Fortinet SD-WAN HUB at
https://partnerportal.fortinet.com.

Contact the Tech Data Fortinet team at
Uspmfortinet@techdata.com
or
1-800-237-8931 x 5545031

FORTINET®

www.fortinet.com

EMPLOYEE SPOTLIGHT: TIM AYER, SENIOR MANAGER, SECURITY SOLUTIONS

Q: What is your job title and briefly describe what you do at Tech Data.

Ayer: *My primary role as a Senior Manager within Tech Data's Security Solutions organization is to lead our network security-focused vendor teams in support of our customers. In some respects, I run a community within a greater community. My team works closely with our strategic security vendors to provide the specialized sales assistance, technical support, marketing content, and business programs that enable our customers to deliver secure solutions quickly, confidently, and profitably. I consider myself fortunate to work with a team of dedicated professionals motivated in serving our partnerships, especially in such a critical area as cybersecurity.*

Q: How does what you do provide value for the company, our customers and/or vendors?

Ayer: *My primary objective is to make it easy for our customers to do business with Tech Data through an experience that earns their business. Within the company, my focus is to put the best people in a position, with the right resources and training, to provide a superior experience. My role requires that I balance the objectives of three constituents, enable customers to win with their end customer, partner with our vendors to bring their products to market and grow their footprint and serve the team that I lead so they can be successful.*

CONTINUE >

Boost your security revenue with Microsoft 365

$720 average revenue

Secure your customers

Sell Microsoft 365 Business

- Licensing sale
- Base security feature deployment
- Supplement on-prem AD with AAD
- Reduce operational cost

+$310 average revenue

Drive assessment

Add high-value, easy-to-sell services based on deployment of Microsoft 365.

- Cloud security assessment
- Hybrid security assessment (CSAT)
- Implement compliance features
- End-user security readiness

+$340 average revenue

Monetize with services

Grow the lifetime value of the customer relationship with services that set you apart.

- Monitoring and alerting
- IAM policy management
- Device policy management
- Threat remediation (P2P)
- Compliance as a service (P2P)

Three-year **average revenue** per SMB seat from Microsoft 365 Business

Source: The Microsoft 365 Partner Opportunity, A Forrester Total Economic Impact™ Study Commissioned By Microsoft, July 2019

Microsoft

Contact your Tech Data Microsoft Cloud Team
Call 800-237-8931 ext. 5545006
or email Microsoft@techdata.com

Learn More at: Bit.ly/TDSecurity

EMPLOYEE SPOTLIGHT: TIM AYER, SENIOR MANAGER, SECURITY SOLUTIONS

Q: What do you enjoy most about working at Tech Data?

Ayer: *Having worked in the IT Channel for over 20 years, I enjoy the innovation that drives our industry, the partnerships that connect us and the integrity in how Tech Data operates.*

Tech Data is a very resilient company with talented people that doesn't stray from its core principles of connecting our IT vendors and our Channel customers. As an example of bringing our vendors and customers together, I am excited about the recent opening of Tech Data's Cyber Range, a forum for expanding education, knowledge and awareness around the skills needed to face the shortage of cyber-skilled professionals. Additionally, we have recently broadened our successful Security Practice Builder Program with a digital curriculum to elevate our customers' security practices. The program is definitely worth checking out.

Q: What's a fun/interesting fact about you that not many people know?

Ayer: *As a hobby, I have been tracing our family genealogy with my kids. My fourth cousin, four times removed, is Abraham Lincoln, according to one of the genealogy apps. I suppose we're all connected, but I do enjoy learning about history and spending time with my family in that pursuit.*

MICRO FOCUS®

Expanded and Extended Product Trials for Select Products Supporting the Remote Workforce

- Multi-Factor Authentication with NetIQ Advanced Authentication
- Encypt and Secure eMail with Voltage SecureMail
- Application Performance Testing with LoadRunner

Micro Focus Tech Data team microfocus@techdata.com or call 1-800-237-8931 ext. 5678326

ENABLE YOUR CUSTOMERS TO IMPROVE THEIR SECURITY READINESS

By: Ruben Cabrera, Senior Manager, Security Services, Tech Data

The cybersecurity threat landscape continues to become more complex, and it's your job to ensure that your customers are protecting their businesses from becoming another casualty. Tech Data offers two very effective services that your customers need to protect themselves from cyber threats.

Penetration Testing Service: This service, delivered by Tech Data-employed ethical hackers, puts customers' cyber defenses to the test by allowing them to be hacked.

Our ethical hackers, also known as pen testers, are trained to think like threat actors and use the same tactics that threat actors use to navigate their way through even the toughest barriers to gain access to a customer's network. They work to gather, review, and analyze exposed customer information that can be used and leveraged to penetrate the customer network. No level of automated scanning and automated testing can simulate the advanced tactics used by our pen testers.

The most considerable value of this service is the detailed reports presented to our partners and their customer at the completion of this service – it details precisely how our pen testers exposed the network and what actions they took. This is extremely valuable because our reports articulate the customer's risk and exposure to threat actors.

Threats are evolving, EDR is no longer enough.
In fact, the latest threats have been engineered to hide from your standard detection and response security.

Good news: We're staying one step ahead.
Trend Micro™ XDR gives your organization the ability to detect and respond to threats across email, endpoints, servers, cloud workloads, and networks.

Beautiful news: Trend Micro XDR is available now!

AI & Expert Security Analytics

Beyond the Endpoint

Complete Visibility

When you can correlate alerts and information from multiple vectors to effectively secure your organization
That's a beautiful thing.
Trend Micro XDR
Learn more at **trendmicro.com/XDR**

TREND MICRO™

For more information contact our dedicated Trend Micro Team at (800) 237-8931 ext. 5585122 or trendmicro@techdata.com

RECON ISAO: As cyber threats quickly change, most businesses find it impossible to keep up with every new potential threat. To address this challenge, many companies choose to join cybersecurity communities.

By presidential order, information sharing and analysis organizations (ISAOs) were created in 2015. These organizations allow companies, local governments, and security professionals to form communities that collaborate, share intelligence, and deliver training and conferences to take place under the veil of mutual non-disclosure agreements. This allows the participants to freely share timely, analyzed and highly relevant data amongst each other.

Tech Data's RECON™ ISAO solution draws from a vast community of members and leverages vetted analysis delivered through experts with years of experience. It also provides access to a private portal with educational references and technical resources.

If you're interested in learning more about either of these services, feel free to reach out to your security sales rep or email us at securityservices@techdata.com.

Advance.
Discover.
Explore.

Keep your focus on your business.
Choose exceptional protection
that couldn't be easier to manage.

Kaspersky
Endpoint Security
Cloud

Learn More

kaspersky BRING ON THE FUTURE

For more information please contact
PSCKaspersky@techdata.com
or call 1-800-237-8931 ext. 5545037.

SOCIAL SELLING: THE KEYS TO THE PROSPECT KINGDOM

By: Heather Murray, Vice President, Security, Tech Data

Social selling is the process of developing sales relationships on social networks (such as LinkedIn, Twitter, etc.), and it's becoming more relevant in an increasingly remote work world. A recent study shows 91% of top salespeople state, "social selling is a key tool for achieving my goals." Additionally, 62%* of technology buyers state they would rather interact on social media instead of via a phone call or email. Clearly, this is the time to be an expert at social selling!*

Joining me today are Janet Schijns and Dr. Ashlyn Szilva, of JS Group. They're both leaders in the social selling industry and experts on this topic.

Murray: Hello Janet and Ashlyn! To start our conversation on social selling, what is it and how does it differ from standard business marketing on social media?

Schijns: *At the most basic level, social selling is simply sales done via a social media platform, with the sole objective being the generation of revenue. On the other hand, social media marketing is any social media activity that does not have revenue generation as its primary goal. You could say social selling drives prospects to revenue, while social media marketing drives awareness and engagement.*

Murray: Interesting! Knowing that, how do you measure success in social selling?

Szilva: *The great news about social selling is that it offers sales managers true quantitative measurements. One of the most popular metrics is the LinkedIn Social Selling Index, and with good reason. A salesperson with a score above 70% regularly achieves 45% more sales than peers with a lower score. Other areas you can measure easily are inbound connections, network growth, content engagement, prospect referrals, and lead activity. Frankly, there is nowhere to hide – if you aren't doing the work, it will show up in the metrics.*

**JS Group March 2019 Survey, State of Social Selling*

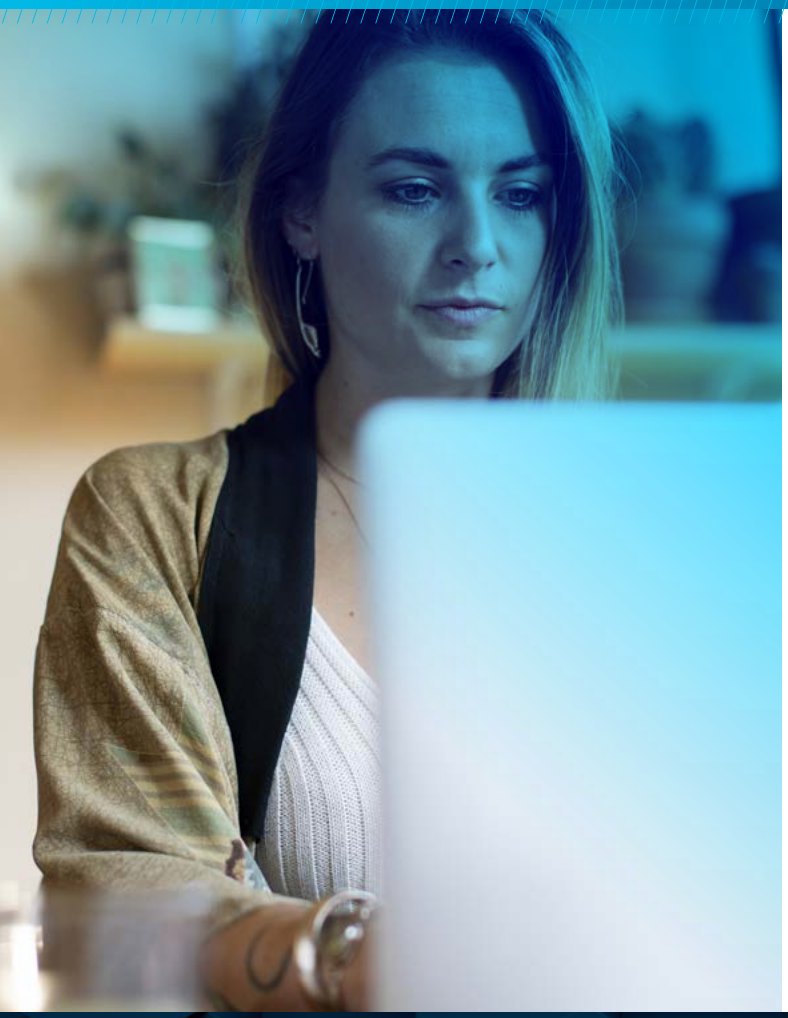
Murray: Whose responsibility is it to drive a social selling culture?

Schijns: *The culture starts at the top; this isn't a strategy that allows an owner or sales manager to set it and forget it. Every executive in the firm must evolve their approach and be engaged and engaging on social media platforms to demonstrate the right behaviors to the rest of the organization.*

Murray: That makes sense. Going off of that, if a partner converts their sales team to a social selling methodology, what results should they expect?

Szilva: *When we work with partners to convert their sales teams, we see a few basic benchmarks fundamentally evolve as a result of the social selling program. The first is prospect management: the funnel becomes much more dynamic and moves, on average, 19% more quickly through the buying journey. Secondly, we see a more robust funnel with a 33% increase in sales qualified leads in just 90 days! Finally, we see a lower marketing expense as the sales and marketing teams are working together to generate highly qualified leads at a much lower cost per lead.*

secureappsware
Connect and protect your apps and data everywhere.
TechData
vmware
Ready to see how VMware Security Solutions can strengthen and simplify your security stack?
Contact **vmware@techdata.com** to learn more!
vmware
Carbon Black Protection™
RUN NSX®



Murray: That's a lot of returns, but how do sellers get started? What competencies does a salesperson need to become an expert seller?

Schijns: *To be an expert social seller, you need to refine your brand persona, determine your value to clients, share valuable content, engage with high-quality connections, and move those connections through the sales funnel to a proposal. This is a journey that starts with understanding why social selling matters and the basics of daily social selling activities applied to your solution sales. JS Group conducts Security Social Selling workshops that are available exclusively through Tech Data. We also have a social selling persona builder and content tools available on Tech Data's Digital Security Practice Builder that help ease the journey for sellers.*

Murray: Great, it sounds like partners can get started fast then! My final question is: who might we want to follow to see more social selling in action?

Szilva: *I would follow Erick Simpson, Janet Schijns, Evan Kirstel, and you, Heather Murray, to see more about how to position yourself and provide value to customers – after all, that's what really matters in any sales engagement: value.*

SONICWALL™

Embrace Secure BYOD With SonicWall SMA

SonicWall Secure Mobile Access (SMA) is a unified secure access gateway that enables organizations to provide anytime, anywhere and any device access to any application.

SONICWALL SMA CAN PROVIDE:

- A granular access control policy engine
- Context-aware device authorization
- Application-level VPN and advanced authentication with single sign-on

This technology enables organizations to move to the cloud with ease, embrace BYOD and secure mobility in a hybrid IT environment.

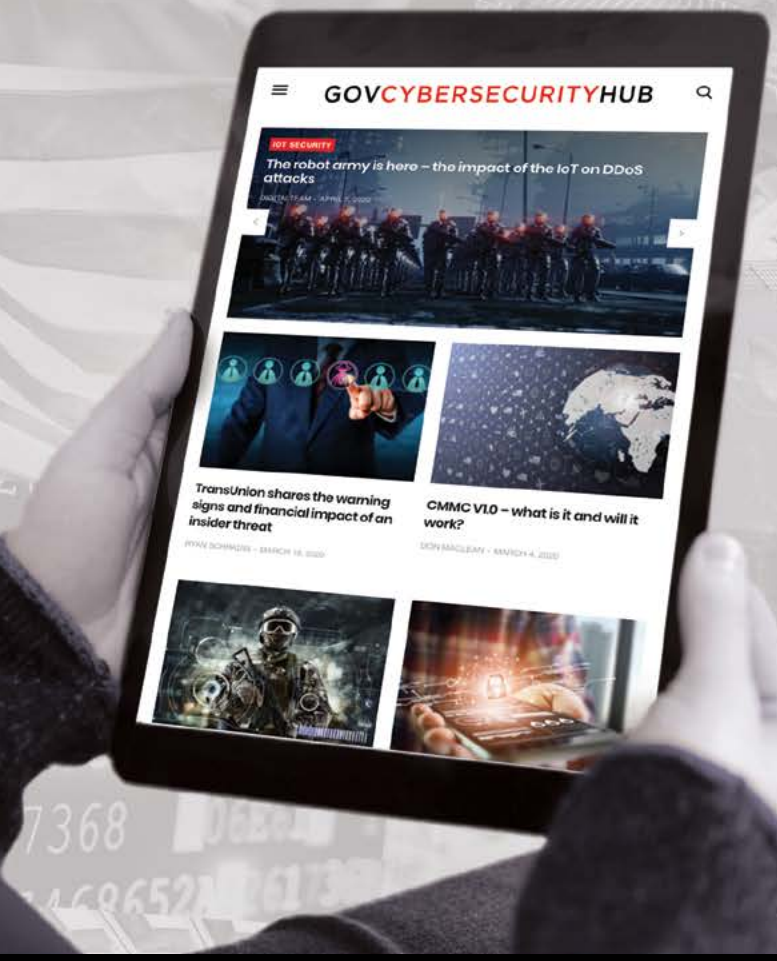
Contact your Tech Data sales rep for the latest promotion at sonicwall@techdata.com.

DLT
A TECH DATA COMPANY

TARGETED READERSHIP

TURNKEY AGENCY-BASED MARKETING

QUALIFIED LEAD GENERATION



The threat environment has changed. Public Sector decision makers charged with protecting our nation's interests need to stay informed in order to stay protected — and they need tomorrow's solutions to meet today's cybersecurity challenges. GovCybersecurityHub brings together news, analysis, and featured content that addresses the real challenges faced by government cybersecurity experts, end-users, and policy makers. Position your solution to the high value target customers by meeting them where they are — in the digital channel.

Find out how:
govcyberhub.com/advertise

GOVCYBERSECURITYHUB

EMPLOYEE SPOTLIGHT: CJ PUHALA, STRATEGIC ENTERPRISE CONSULTANT, SECURITY

Q: What is your job title and briefly describe what you do at Tech Data.

Puhala: *In my role as a Security Solutions Sales Consultant, I work with my client executives to support our Eastern Region value-added reseller (VAR) channel. I consult, evangelize and establish/develop their Security sales offerings, including managed and professional services (offered both organically and as outsourced where applicable, including virtual CSO) as they align with our robust portfolio.*

My role also includes customizing security solutions sales training, go-to-market alignment with technical resources, marketing programs and collateral, practice building, assistance with coordinating vendor relationships and any additional assistance required. My main objective is to position our partners for success in their respective industry verticals in both the public and private sectors.

Q: How does your position provide value for the company, our customers and/or vendors?

Puhala: *I help our partners determine the market potential for their security practice, develop a differentiated security solution portfolio, execute training programs for their sales and technical teams and build marketing plans to promote their practice.*

CONTINUE >

IT'S TIME
FOR A NEW GENERATION OF SECURITY.

Yesterday's protection is no match for today's threats. Hackers have evolved. **Has your cyber security?**

Check Point 5th generation cyber security: protecting businesses everywhere.

Contact our dedicated Tech Data Check Point Team to for more information:
Phone: 800-237-8931 ext. 5545036 | Email: checkpoint@techdata.com

WELCOME TO THE FUTURE OF CYBER SECURITY

Check Point® SOFTWARE TECHNOLOGIES LTD

© 1994-2019 Check Point Software Technologies Ltd. All rights reserved.

EMPLOYEE SPOTLIGHT: CJ PUHALA, STRATEGIC ENTERPRISE CONSULTANT, SECURITY

Q: What do you enjoy most about working at Tech Data?

Puhala: *The satisfaction that comes with the realization that I've helped to ensure our partners' success, in terms of building or expanding their security practice, so they're positioned as their clients' strategic consultative advisor, thereby enabling them to create and maintain deep, lasting relationships.*

Additionally, I have the privilege to work with a top-notch team of highly skilled professionals whom I can call on in a moment's notice. We all share the common goal of ensuring that our partners demonstrate the highest level of expertise in terms of securing their clients most critical assets daily!

Q: What's a fun/interesting fact about you that not many people know?

Puhala: *Prior to entering the IT arena, I was a traveling, professional musician. I studied percussion and played drums with a touring band for many years, signing a record deal with MCA records. I also love teaching and taught percussion before "hitting the road."*

Upon leaving the "road," I went back to school and earned a Computer Science degree, which enabled me to achieve success in my "new" career here. I still play music to relieve stress too! My hobbies include working out and reading, both for business and pleasure. I also love scuba diving, but in all honesty, I need to get back to it (time permitting)! I also enjoy movies - any genre, if the acting is good!

Concerned With Where Your Data Goes?

Gain visibility and control to protect data everywhere

- Visibility
- Control
- Compliance
- Data Protection
- Threat Prevention
- Cloud-Native

MVISION Unified Cloud Edge protects data from device to cloud and prevents cloud-native threats that are invisible to the corporate network. This creates a secure environment for the adoption of cloud services, enabling cloud access from any device and allowing ultimate workforce productivity.

For more information contact the Tech Data McAfee team at mcafee@techdata.com 1-727-539- 7429 ext. 5545034.

McAfee™

McAfee and the McAfee logo are trademarks or registered trademarks of McAfee, LLC or its subsidiaries in the US and other countries. Copyright © 2020 McAfee, LLC