Tech Data | Security Solutions

WORK-FROM-HOME SECURITY PLAYBOOK

HOW TO USE THIS PLAYBOOK

Whether you're new to security solutions or you've already been selling security, this playbook offers a way to both learn about work-from-home security solutions and services and find new ways to enhance your practice. Plus, there are tips and tools to share with your team and clients.

It's impossible to cover everything here. But Tech Data has many resources to help you solve your customers' issues – from subject matter experts to training and education tools to digital resources. If you can't find what you need, ask us.

Thank you for your partnership. Here's to a more secure future for you and your customers!

The Tech Data Cybersecurity Team

TABLE OF CONTENTS

DO YOUR RESEARCH

BUSINESS TRANSFORMATION IN THE NEXT 2-5 YEARS

Have you been wondering what our world will look like in the next two-to-five years? Here are five insights from Alex Ryals, Vice President of Security Solutions, Americas at Tech Data.

I was thinking the other day about how our world will be different as a result of the evolving workforce. I asked friends, family members and business acquaintances, and started compiling a list. I'm up to 20 things that I think will change or be different, and wanted to share these first five insights around business transformation.

WORK FROM HOME

I don't think it's been a surprise that work-from-home has been an interesting experience for everyone. Employers have learned that employees can be trusted to work from home and be productive and efficient, as well as balance their work/home life. There are some interesting side effects that'll come from our work-from-home experience. Some studies say anywhere between 25-50% of people won't return to an office to work. Imagine the savings of those who can reduce the size of their office environment, while still providing a meeting place for people who need to work in an office space. Imagine having employees who can really work from anywhere, as long as they have internet connectivity. This opens up a whole new set of employees you can recruit!

SALES PROCESS

The second area I think that's going to change is the sales motion. Now I love getting in front of a customer and helping craft a solution that can make it better for them. But the truth is, the sales cycle—especially in the IT industry—can be anywhere from three to nine months, and not every meeting has to be face to face. If we've learned anything, it's that Zoom can not only be effective, it can be a lot of fun. I use a lot of cool, fun backgrounds to liven things up with my own team, as well as customers. In fact, I would argue that seeing people's kids and pets in the background creates a sense of intimacy with your customer you probably never had before, especially when we used to show up in business suits putting on our best face. While the face-to-face sales process will be absolutely important, it'll shift over the next few years to more remote meetings.

CONT: BUSINESS TRANSFORMATION IN THE NEXT 2-5 YEARS

INVESTMENT IN DIGITAL TRANSFORMATION

I'm very passionate about digital transformation and could talk for hours about it. But a couple of areas will be different moving forward.

- ***E-Commerce –***
  E-commerce will ramp up like never before. There's still a large segment, especially SMBs, that haven't yet moved their products to an online experience. We're going to see more of a movement to that area with new e-commerce technologies that make it simpler and better to go to market.

- ***Supply Chain –***
  The supply chain will also experience a major digital revolution as we need to secure it differently. I'm thinking of a matrixed environment where I can source products and technologies from many sources, so I'm not dependent on one country or industry that might not be able to sustain a major disruptive event in the future.

- ***Robots and Automation –***
  We're also going to see robot automation digitally transform. McDonald's has talked for years about putting more kiosks in their restaurants so you don't have to interact with a human just to buy a Big Mac. We're also going to see retail moving to more of an Apple-like kiosk or self-serve experience where the whole buying process is largely digital. Not every industry is there yet, but I think over the next few years we're going to see large investments in doing just that.

- ***5G –***
  Another favorite digital transformation topic for me is 5G technology. Many countries are ahead of the United States in this area, but we're coming on strong. 5G tech will allow higher data throughput and higher bandwidth, so more information can be pushed over cellular at a faster speed than ever before. Imagine watching video on your phone over a cellular connection instead of having to have Wi-Fi to stream video. Imagine the small store owner or law firm that no longer has to pay for a slow DSL connection at great cost. 5G cellular technology can pull an internet signal from a cell tower down the street and provide many different types of online services or in-store services that haven't been provided before. It'll be fun to see how the e-commerce and in-store experiences change based on 5G technology.

CYBERSECURITY

The fourth area of business transformation is also near and dear to my heart: cybersecurity. Hacking has increased almost 400% since March 2020. Imagine all the social engineering emails a hacker could send – receive a government check, get N95 masks, go back to work. These are just a handful of scenarios the bad guys are using right now to convince people to click links they shouldn't click, and download and install malware to their endpoint device to infect them and possibly their employers.

This brings me to another security topic. Employers have sent employees to work from home, but employees aren't necessarily secure in their home environment. How long has it been since they've upgraded the firmware on their modem? Are they using WPA2 personal encryption instead of WEP? Do they even know the difference? Securing their wireless network, securing home IoT devices so they won't infect the company-provided laptop—and, therefore, infecting the company—are things we haven't thought about in the past. So, I anticipate new technologies rolling out for home users to protect themselves and the devices used to connect to company networks.

DIGITAL HEALTHCARE

The fifth area I wanted to talk about is the adoption of digital healthcare solutions. We have a lot of feedback around ways to make healthcare workers' jobs easier and better using digital transformation – such as digitizing patient healthcare records and digitizing technology used in hospitals that make it faster to communicate information, even nationwide, to a hospital network. These are basic ideas that can be improved upon, and I think companies will step up to make these solutions over the next few years and evolve our healthcare system in America.

SECURITY TRENDS ON THE WAY BACK TO WORK

Where's the security market going over the next month? The next quarter? The next year? The truth is, there's still considerable uncertainty. What we do know is that security will remain an important part of the strategy for most customers.

CONSIDER THESE SHORTER-TERM OPPORTUNITIES:

- ***Remote Work –***
  As organizations stabilize their remote workforces and, in some cases, make them permanent, sales of firewall licenses, endpoint security solutions, VPN clients and email security will continue to increase.

- ***Ransomware And Malware –***
  Bad actors seek to exploit your customers' overwhelmed IT teams, ramping up ransomware and malware attacks. Assessments and penetration testing offer both an entry point to identify areas of opportunity in your customers' networks, and a great way to provide assurance they're prepared. Or not.

- ***Email Security –***
  Email security will also remain important, as almost 90% of threats start with a user clicking an email hyperlink – yet another way to support your customers.

In terms of longer-term opportunities and with so many people working from home, consider these:

- ***Education –***
  Consider further training and enablement to up your skills and prepare your customers. Stay tuned as we release new MSSP-focused content and virtual events.

- ***Managed Services –***
  Security managed services will continue to grow this year as customers support remote workforces, return to work or some combination of those two models. In addition to supporting the business, IT teams will be challenged to manage their security and will look to outsource that function.

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'll make a difference.

PHISHING: A SIGN OF THE TIMES

Phishers seize upon any opportunity to prey on people, and the current climate provides plenty of opportunities for attacks.

Industry experts say that phishing attacks are becoming even more sophisticated and timely, as bad actors stoke fears over current events and exploit uncertainty over the upcoming elections.

As managed security services providers (MSSPs), you have your hands full, not only monitoring and applying countermeasures, but staying on top of the latest schemes.

PHISHING EXAMPLES: HOOKING CUSTOMERS WITH TIMELY BAIT

- Soliciting donations for fake healthcare research initiatives
- Spoofing official Centers for Disease Control and Prevention updates to spread ransomware
- Sending emails from a domain nearly identical to a well-known hospital, indicating that the recipient may have been exposed to a virus and asking them to schedule a virus test by completing an attachment
- Registering more than 4,000 lookalike domain names with "Zoom" in the name – a harbinger of attacks to come
- Sending a map showing how a virus is spreading, pressuring recipients to download more details to see if their region is affected
- Using greater personalization, prompting recipients to click on a link that automatically downloads malware capable of logging the individual's keystrokes
- Mimicking a familiar site, so when recipients click on a normal-looking URL, they're prompted to reset their passwords – and essentially hand over their credentials

WHAT CAN MSSPS DO?

Besides continuously educating customers on threats, MSSPs can add significant value in helping to combat phishing attacks. Here are some examples:

- ***Multifactor Authentication (MFA) –***
  A key phishing countermeasure—especially if a user's credentials have been compromised by a phishing attack—MFA nullifies more than 90% of attacks and should be implemented across all companies.
- ***Test Phishing –***
  Send test phishing emails to corporate staff, which then provide metrics to security leadership about the efficacy of their anti-phishing training programs.
- ***Endpoint Detection and Response –***
  After malicious actors successfully infiltrate an organization, they stay under the radar in the system, moving laterally and using scanning tools until they have enough control to exfiltrate information and send ransomware. This makes it critical to detect an intrusion at the very beginning.
- ***Breach Detection and Response –***
  These tools use orchestration and automatic remediation, enabling you to block potentially malicious code before it has the ability to spread to customers.
- ***Security Integration –***
  Many out-of-the-box and cloud-based security systems, though easy to deploy, often don't meet all of your customers' requirements, particularly if they're now supporting a remote workforce. In addition, having too many vendors doing too many things make it difficult to holistically manage a security strategy. The goal is to have a single dashboard with all the features needed to simplify security management.

SHORING UP (WORK FROM) HOME NETWORKS

Last fall, Tech Data Security Consultant John Komer, made a stunning prediction. Over the next 24 months, he claimed, employees working remotely would increase by 40%, accelerating the need for businesses—and employees themselves—to shore up wireless home networks to keep corporate networks safe.

Virtually overnight, mass numbers of employees were sent home, instantly elevating the need to secure home wireless networks – and immediately creating a demand for customers to help their end users secure their networks.

THE THREAT: INADEQUATELY SECURED HOME NETWORKS

Hackers have increasingly targeted home networks over the last couple of years, employing similar threat vectors previously used on corporate networks. In the Target breach, for example, hackers used Target's HVAC systems and smart buildings to gain access to their corporate network and compromise their POS systems. In all, the cardholder data of 70 million customers was stolen.

Hackers have even used a beverage machine as a pivot point within a corporation's network to gain broader access and steal data.

Home networks have similar components. Computers connect within the home using a local area network (LAN), which also wirelessly connects TVs, refrigerators, security systems, video doorbells, gaming systems and other IoT devices to the internet. Hackers can use any of these and other internet-connected devices to deliver malware to the home network, then pivot to compromise the work computer and corporate network.

WHAT CAN MSSPS DO?

As work-from-home scenarios become the norm, help customers deploy anti-virus solutions, like firewalls, with monitoring to secure their environments through their devices – including home computers, home Wi-Fi and smart home IoT systems.

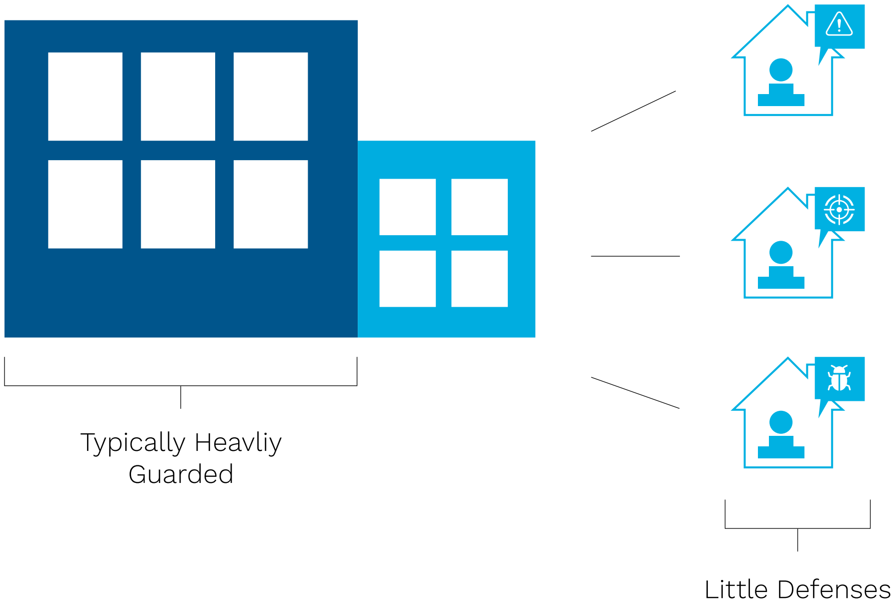
Using MFA, and deploying endpoint detection and response with firewalls provides full visibility into employees' endpoint devices and confirms they're adhering to corporate security policies. These security solutions have been in place for corporate mobile phone users for several years now.

The shift to work-from-home employees will continue to grow and, as it does, we need to continually look for unique solutions to address this problem.

HOW WORK-FROM-HOME EMPLOYEES PUT YOUR CUSTOMERS' DATA AT RISK

The corporate network is typically heavily guarded. All of the tools are in place and monitored to ensure unauthorized users don't get in. While at work, security policies are typically adhered to, and most companies have defenses and safeguards in place to enforce policies and protect data.

But employees' home networks are a different story. They typically lack the stringency of corporate policies and practices. There's more often than not a single internet connection used by everyone in the home. Equipment tends to be plug-and-play to make sure that users can use it. And unlike rules for work, home network rules are more relaxed.



LACK OF SECURITY HYGIENE

HOME NETWORK

- Weak security encryption
- Lack of firewall
- Outdated router firmware

IOT DEVICES

- Outdated firmware
- Shares the same network as work devices
- Weak or reused passwords

LAX SECURITY PRACTICES

WORK DEVICE

- Allowed access by others
- Download unapproved apps
- Connect unapproved removeable storage devices

PERSONAL DEVICE

- Autosaved passwords
- Weak or reused passwords
- No password manager

CONSIDERATIONS FOR WORK-FROM HOME SECURITY

Malicious actors want to exploit the work-from-home workforce. Help customers lower their risk of cyberattacks by reviewing their policies, technologies and training.

POLICIES

- Are security policies updated to support the remote workforce?
- Does the current security policy include how remote employees should handle bring your own device (BYOD)?
- Does the business continuity plan include how to continue supporting the remote workforce?

TECHNOLOGY

- Is there endpoint protection on all devices remotely connecting to the corporate network?
- Are remote workstations backed up and enabled with encryption?
- Is proactive monitoring set up to identify suspicious or unauthorized activities?

TRAINING

- Are employees up to date on the latest cybersecurity and privacy awareness training?
- Do employees know how or when to report suspicious or malicious activity?
- Are phishing attack simulations actively being deployed?

TECH DATA CYBER RANGE: REMOTE CYBER TRAINING EXERCISES

Now might be an excellent time to hone your cybersecurity skills in advance of a career change or business opportunity, skill up new employees, or re-train laid-off employees in anticipation of a return to work. Or just exercise your security brain.

The Tech Data Cyber Range, led by elite security experts, is now open to customers and end users who want to participate from the comfort of home.

Tech Data is committed to growing new cybersecurity talent and significantly improving the skills of existing cybersecurity professionals through the following remote training opportunities:

- ***Capture the Flag (CTF) Events –***
  CTF games offer a series of challenges, based on real-world incidents and vulnerabilities, that require you to exercise different skillsets. In addition to being fun, they're highly educational and professionally rewarding. They give novices a chance to experience how cybersecurity is actually done and better prepare mid-level players to defend their own systems from different types of attacks.

- ***Incident Response Experiences –***
  Hands-on Incident Response experiences enable you to unleash multiple cyberattacks into your customer's live environment. More than a tabletop exercise, this build-your-own-adventure experience uses our sophisticated threat intelligence platform to help your customer rehearse a plan of action. Every aspect of their cybersecurity plumbing is tested. At the end of the day, they'll see where their gaps are and be better prepared for an attack – with no impact to their environment.

- ***Defense in Depth (DiD) Training –***
  DiD is a method in cybersecurity where organizations have multiple layers of security controls in place, to protect data and information from cyberattacks. If one of the security controls fail, then another layer within the controls will hopefully protect data and information, thwarting the attack. Participants who complete this training will come away with a better understanding of how adversaries bypass traditional defense strategies, and develop a well-defined framework for protecting their business infrastructure from adversaries.

- ***Zero Trust Training –***
  Zero Trust is a security concept centered on the belief that organizations shouldn't automatically trust anything inside or outside its perimeters. Organizations must verify anything and everything trying to connect to its networks and systems before granting access. Participants who complete this training will be able to evaluate and plan for implementing or converting to a Zero Trust framework

- ***Remote and Self-Service Training Courses –***
  Students can learn practical cybersecurity skills through instructor-led remote or self-service training. Students can also participate in immersive, instructor-led Cyberattack Missions, featuring a specific type of cyberattack, that puts their detection, investigation or remediation skills to the test. Or we can tailor course content to specific objectives.

Of course, Tech Data continues to offer you cyberthreat briefings with the latest threat intelligence – all delivered virtually.

Visit the Tech Data Cyber Range website for more information about our training opportunities.

GROW SECURITY REVENUE WITH DIGITAL SECURITY PRACTICE BUILDER

With cyberattacks increasing some 400% since the beginning of 2020, and more and more organizations investing in security solutions, the time to power up a sustainable security practice is now.

Whether you're new to security or have an established practice, consider acquiring or deepening your skills and proficiency on emerging threats, security best practices, new and proven solutions, and more.

The Digital Practice Builder from Tech Data allows you to quickly and cost-effectively train employees, as well as build a culture that aids in retention, while delivering greater value to your customers. We make it easy to dive right in.

- ***Security Assessment –***
  How strong is your security capability today? Are you a Starter? A Transformer? An Accelerator? Our Security Practice Assessment helps you identify where you fall on the maturity scale in your security business, and areas for improvement.

- ***Security Training –***
  After you complete the Security Practice Assessment, you can access curated security training courses that accelerate your growth and improvement. If the content is too basic and you don't want a refresher, move on the next module. Where you go and how fast you want to ramp up is entirely up to you.

- ***Business Builder –***
  As you complete training courses, you'll gain key insights into how to leverage security best practices in your business. You'll better understand:

  Strategy Development –
  Maximize revenue by determining the right area of security for your business.

  Training and Enablement –
  Learn how to ensure your team has the tools of the trade and knows how to sell security solutions.

  Marketing Plan –
  Your business is only as good as the next customer.
  Learn what you can do to get the get the word out about your business.

  Services –
  What type of professional and managed services will be the most profitable for your company? We'll help you nail it down.

  Sales Execution –
  Finally, understand how to recruit, hire and retain talented security leaders.

Visit the Tech Data Digital Security Practice Builder website to get started.

IDENTIFY DECISION MAKERS & QUALIFY PROSPECTS

QUALIFYING QUESTIONS TO UNCOVER SECURITY OPPORTUNITIES

You can identify opportunities for your security practice by asking smart questions and intelligently identifying what security topics to discuss with your clients. When uncovering opportunities, ask:

- “What’s your biggest concern about security?”
- “What would happen if that happened?”

Because almost everyone has a difficult time keeping up with security issues, what you learn from this question will give you insights into where to probe further in your customers’ organizations.

QUALIFYING QUESTIONS

Identity and Access Management

- How do you control access and audit activities around your critical data?
- What would happen if critical customer data got in the hands of the wrong people?
- How will you keep this from happening?
- What are your plans to protect sensitive data safe when accessed via mobile devices?
- What levels of access control are you required by law to maintain?
- What’s the potential legal exposure if your organization inadvertently permits access to someone unauthorized?

Application and Data Security

- How do you control access and audit activities around your critical data?
- What would happen if critical customer data got in the hands of the wrong people?
- How will you keep this from happening?
- What are your plans to protect sensitive data safe when accessed via mobile devices?
- What levels of access control are you required by law to maintain?
- What’s the potential legal exposure if your organization inadvertently permits access to someone unauthorized?

Security Compliance and Vulnerability Assessment and Management

- What mandates are you required maintain?
- What levels of access control are you required by law to maintain?
- How do you stay up to date on these mandate requirements?
- How do you ensure you’re in compliance?
- What’s your financial and legal exposure if you’re out of compliance?
- What policies do you have in place to manage an out-of-compliance situation?
- How do you control access and audit activities around your critical data?
- What would happen if critical customer data got the hands of the wrong people?
- How will you keep this from happening?
- What are your plans to protect sensitive data when accessed via mobile devices?

CONT: QUALIFYING QUESTIONS TO UNCOVER SECURITY OPPORTUNITIES

SMB Security

- If your data system was disabled, either from an intentional attack or an accident, how confident are you that you could quickly restore critical business systems before there was substantial impact?
- What records are you required to maintain by law?
- What would happen if critical customer data got the hands of the wrong people?
- How are you ensuring these records are secure?
- What's the potential legal exposure if your organization cannot fulfill contractual obligations?
- What would happen if your company's financial records were destroyed? What would that cost?
- What are your plans to keep this from happening?
- What are your plans to protect sensitive data when accessed via mobile devices?
- Do you have a formal security policy?
- What incidents have you planned for?
- When was the plan last reviewed?
- When was the last time your employees and management had training on data security?
- If we did a quick survey of your team, how many security weaknesses or breaches do you think we'd find?

Secure Content and Threat Assessment

- If your data system was disabled, either from an intentional attack or an accident, how confident are you that you could quickly restore critical business systems before there was substantial impact?
- What would happen if critical customer data got the hands of the wrong people?
- How will you keep this from happening?
- What are your plans to protect sensitive data safe when accessed via mobile devices?

IDENTIFYING DECISION-MAKERS

If it's a customer you already have a relationship with, you likely already have access to the decision-making team. If it's a new customer, identify who's impacted when there's a breach or ask who's responsible for the areas below.

Identity and Access Management –
Look for a title such as chief information officer (CIO), security officer, legal officer, IT administrator, compliance officer or similar title. Ask who's responsible for data access security.

Application and Data Security –
Look for a title such as security officer, legal officer, IT administrator, compliance officer or similar title. It could also be the chief financial officer (CFO).

Security Compliance and Vulnerability Assessment and Management –
Look for a title such as chief operating officer (COO), security officer, legal officer, compliance officer or similar title. Ask who's responsible for ensuring compliance with all applicable regulations and mandates.

Small- and Medium-Size Business (SMB) Security –
You probably already have access to the SMB decision-maker because of your customer relationships. If not, ask who's responsible for data security.

Secure Content and Threat Management –
Look for a title such as CIO, security officer, legal officer, IT administrator, compliance officer or similar title. Ask who's responsible for data security.

OFFER SOLUTIONS & SERVICES

SOLUTIONS

Cyberthreats are constantly evolving, so you need a portfolio that provides the latest cybersecurity technologies to help you keep your customers safe.

Identity and Access Management (IAM) –
Management combines three elements: Authentication (who you are), authorization (what you can do), and accounting (what you have done). Authentication requires users to prove who they claim to be. MFA requires two steps to prove their identification. Authorization allows or disallows users to access resources, services, and data based on their roles. Accounting measures usage for billing purposes, and also monitors and tracks unauthorized access attempts.

Application and Data Security –
For most companies, their greatest asset—after customer loyalty—is their data. Electronic intellectual property is more than 70% of the market value of a typical U.S. company, according to PriceWaterhouseCoopers. It's about protecting the customer's data with appliances, software or managed services.

Security Compliance and Vulnerability Assessment and Management –
Make sure your customers comply with mandates for protecting and preserving corporate assets, and minimize their exposure to security risks.

SMB Security –
SMBs are under attack and they're a desirable target because:

- They're big enough to be worth stealing from
- They're small enough to not have sophisticated security or data protection
- They don't often have the resources to pursue legal action
- It only takes a single intrusion to compromise everything
- The owner often thinks they're immune to attack and doesn't need to go beyond basic security measures, like antivirus

Secure Content and Threat Management –
The bad guys want to crack the company vaults and help themselves to valuable business data and salable customer information. Secure content and threat management is about deploying advanced technologies—intrusion protection systems (IPS), firewalls, and DLP— to protect your customers' data from network-based attacks.

ENSURE YOUR CUSTOMERS' REMOTE WORKFORCES ARE SECURE

With the current health crisis continuing to alter our definition of a company's network, it is time for every business to proactively assess their security risks, specifically targeting their remote workforce. Tech Data offers a Remote Home Secure Program, which will assess the cyber risk of a company's remote employees through the following process:

1. Review: Tech Data will review the company's security policies, technologies and security practices as it pertains to securing their remote workforce.

2. Interview: Remote employees are interviewed to determine the current configuration of their home networks and gauge the understanding, implementation and adherence to company security policies. Tech Data's cybersecurity experts conducting these interviews will locate key security risk areas in a non-invasive way and deliver high-level recommendations to address all identified vulnerabilities.

3. Report: Results are then compiled and delivered as a detailed report that includes an executive summary, identification of major security gaps and how to address the risks found.

4. Recommend: The report also includes a recommended Unified Threat Management solution that protects your customer's remote home office executives. This robust solution, offered as a monthly subscription, provides extra protection against malware and secures sensitive information business executives engage in regularly.

For more information about Tech Data's Remote Home Secure program, contact us at ***securityservices@techdata.com.***

UNCOVER ADDITIONAL REVENUE OPPORTUNITIES THROUGH SERVICES

Security threats are changing constantly, and addressing them can be both costly and complex for companies. Leading with services can help you uncover and address your customers' challenges more quickly and efficiently.

ASSESSMENT SERVICES

Assessment Services evaluate the technical security of a customer's network in the form of vulnerability assessments, penetration testing or security profile assessments. The outcome of these services identifies security weaknesses and exploitable vulnerabilities with objective results and clear recommendations. This not only provides Tech Data's customers with a roadmap to recommend and deliver appropriate security products, but also services that best fit the customer's needs.

- ***Security Profile Assessment*:**
  This complimentary assessment only takes 90 minutes to perform and can reveal ample information on your customer's security practices. It starts with running your customer's system through an evaluation to gather information about their security controls. We'll help you reveal potential flaws in their infrastructure and compile a report for you to give to customers that contains a security scoring, summary of events and customized action plan to improve their security posture. With a 50% closure rate, this assessment alone can create a robust pipeline for you to access while helping your customers.

- ***Vulnerability Assessments*:**
  Vulnerability Assessments are security services that provide a comprehensive view of technical vulnerabilities and common misconfigurations attackers can exploit within a customer's systems. Plus, it's combined with financial data for a full-risk analysis and can provide customers with methods to allocate limited resources efficiently.

- ***Penetration Testing*:**
  If you need a realistic look at your customer's cybersecurity defense posture, try our penetration testing services. With penetration testing, Tech Data can help you demonstrate necessary conditions and methods used to exploit vulnerabilities. Penetration testing also reveals pathways that lead to sensitive data disclosure and proves which exploitable vulnerabilities should be prioritized for remediation.

- ***Additional Assessments*:**
  Outside of our own in-house portfolio, Tech Data also partners with various third-party service providers to provide additional assessment capabilities, including security risk assessments, physical security assessments, physical penetration testing, cloud (POV) and GDPR assessments.

COMPLIANCE SERVICES

Tech Data can help you in delivering compliance readiness services on behalf of partners. We offer governance, as well as risk and compliance services across many of the industry-wide regulatory companies such as HIPAA, HITRUST, PCI-DSS, NIST 800-171, ISO 270001, NERC-CIP, SOC 1&2, GDPR and many others. Our services provide peace of mind and serve as a compliance advocate from understanding the driving needs: whether that means working with designated third-party auditors or helping certify additional staff as needed during the process.

IMPLEMENTATION SERVICES

Tech Data offers implementation services, including new installations, integrations, patch services, configurations, as well as staff augmentations across many of the security products.

Ensure your customers have a comprehensive security trategy for their business. Contact us for help today at ***securityservices@techdata.com.***

CLOSE THE DEAL

OUTLINING THE COMPELLING VALUE OF THE SECURITY SOLUTION

When you choose a security vendor—with help from your Tech Data Sales rep—you'll frequently have access to tools that'll help develop strong value propositions to share with your customers. Couple this with the research you've done by asking qualifying questions, and you'll be able to present a compelling reason for your customers to take action now.

You can calculate what a data breach costs for your customers with the ***Ponemon Institute and IBM Data Breach Risk Calculator.*** You can also get current comparisons with others in the industry to benchmark data risk costs from this resource.

MANAGING OBJECTIONS

You'll probably encounter objections when speaking with your customers about security solutions. Here are the most common ones and some suggestions on how to manage them:

"Our systems are already secure."
Great! But what happens when there's an issue? How quickly can you protect your systems and data? Let me take a look at your systems to look for gaps. If we find anything, it'll save you the cost and embarrassment of an attack. If we don't, you can say you're just being cautious and exercising reasonable care.

"We're in compliance."
I'm sure you are! There are all of these new mandates and sometimes it's a challenge to keep up with them. Do you have a third party that audits your plans? I'm happy to look at your systems and see if there are any gaps. If we find anything, it'll save you the cost and embarrassment of non-compliance. If we don't, you can say you're just being cautious and getting a second opinion.

"We don't have the money."
I get that. What have you budgeted for a data breach? What are you doing to ensure that conduct and protect your critical assets? Let's take a look to see what it would cost if someone accessed information they weren't supposed to and what it would be worth to prevent that from happening.

"We're going to look at that in the future."
Great idea! How do you plan to protect access to your data between now and then? Let me at least put together an interim plan to keep you protected until you can put together a full solution.

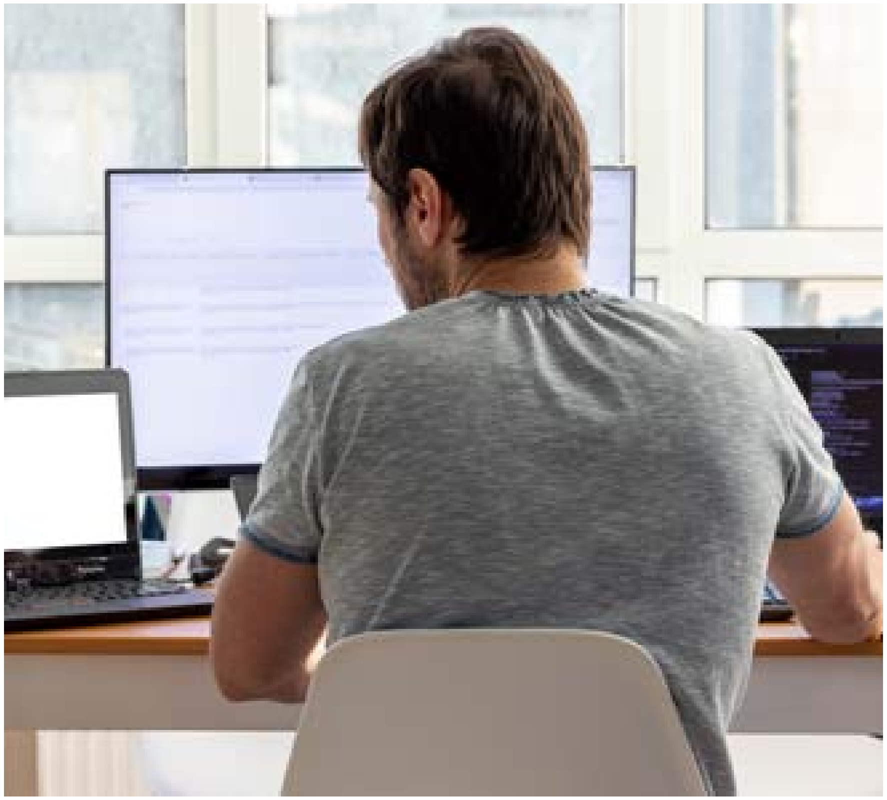
CLOSING THE DEAL

Security solutions offer cost reductions due to efficiency (performance improvements) and insurance (loss mitigation). Using the solution's total cost of ownership (TCO) or return on investment (ROI) calculator, determine the value of the proposed security solution and the monthly savings.
For example, if you're calculating TCO, divide the solution value by 36 (three-year estimate) or 60 (five-year estimate). Use the resulting monthly savings to show the value of making a decision now rather than later.

For example, if the security solution you're recommending saves them $30,000 a month, every month they delay the decision means they write an unnecessary check for $30,000.

Also, align with their internal deadlines. If the chief executive officer (CEO) has promised that a security solution will be implemented in the next six months, use this information to your advantage. Any time you can link your proposal to meeting internal deadlines, you'll speed the deal.

Some security projects require more executive involvement than others. Consider working with the executive team to identify execution plans and externally driven deadlines.



SHARE TIPS & TOOLS

WORK-FROM-HOME SECURITY BEST PRACTICES

- ***Increase Security Awareness Training –*** Emphasize user education and training, not overly restrictive measures.
- ***Lock Your Doors –*** Make physical security as important as data security by keeping devices safely behind locked doors.
- ***Block the Sight Lines –*** Keep those in public places from prying by blocking their view of your screen.
- ***Create a Comfortable Workspace –*** Seek out comfortable seating and reduce eye strain with good lighting.
- ***Always Secure Your Hardware When Traveling -*** Keep devices with you at all times, even when it might be easier to stow them in the trunk or entrust them to someone else.
- ***Configure Wi-Fi Encryption –*** Configure your network connection correctly by ensuring it requires a password for anyone connecting to it.
- ***Avoid Using Public Wi-Fi Connections –*** Avoid public Wi-Fi and use a personal hotspot from a dedicated device or your phone.
- ***Avoid Using Random USB Drives –*** Avoid using USB drives if you don't know where they came from or where they've been.
- ***Use a USB Data Blocker When Charging Company Devices at Public Charging Stations –*** Protect devices with a USB data blocker to prevent data exchange and guard against malware from unknown USB ports.
- ***Change Your Default Router Login and Password –*** Change the login and password required to enter the router settings from the default (usually "admin").
- ***Screensaver and Password Lockout Policy –*** Lock your screen whenever you leave your device to keep prying eyes away and innocent parties from accidentally pressing "send."
- ***Use Company Provided Means of Communication –*** Use the company-provided email, messaging, and other communications systems, and keep from using tools that IT doesn't support.
- ***Update Programs and Operating Systems –*** Regularly update and patch software and automate updates for remote employees.
- ***Use an Endpoint Security Solution –*** Remotely deploy endpoint protection and centrally configure, manage, and monitor all endpoints (include a strong anti-exploit component to shield unpatched programs and legacy systems).
- ***Encrypt Local Data and Remote Communications –*** Encrypt hard drives to protect any data stored locally, as well as data attached to an email, and set devices to have all stored data encrypted in case of theft.
- ***Keep Work Data on Company Systems –*** Avoid using personal devices for work and downloading or synching files or emails to a personal device.
- ***Establish a Physical Device Separation Between Work and Personal Hardware (computers, tablets, phones, etc.) –*** Avoid using personal devices for work, even if it's tempting to do so.
- ***Use Good Password Hygiene –*** Require employees to use strong passwords and ask that they password-protect their phones, in case of device theft or loss, or to make them harder to hack.
- ***Track Your Work Progress –*** Stay transparent by being available during normal business hours and reporting on tasks you're working on.
- ***Stay Vigilant –*** Carefully read and respond to messages to ensure they're legitimate, and confirm suspicious requests and senders by calling the sender.

TIPS FOR LEADING WORK-FROM-HOME TEAMS

Many of you have settled into working from home, or at least have your new routine defined. Here are some tips for leading remote teams:

- ***Regularly Communicate With Your Teams –***
  Have daily one-on-ones. Whether you use Webex, Skype or Zoom, make sure you turn on the video camera and see your team. It can create that motivation needed to tackle the day.

- ***Put the Focus on Outcomes, Not Activities or Hours –***
  With teams spread out across locations, it's not possible to manage every aspect of their work. Stick to outcomes and measure their performance accordingly.

- ***Add a Little Fun –***
  Experiment with fun games during 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 –***
  Let them talk about their challenges, if they need to. It'll relieve stress and keep everyone focused on the tasks at hand.

- ***Be Flexible –***
  Some team members are new to remote work and thrust into home-schooling kids, juggling work demands and trying to find a work/life balance. A little flexibility goes a long way.

- ***Hold Virtual Events –***
  Getting together over lunch can be a great way to ease the stress of isolation that some team members may be experiencing. Gathering over lunch, enjoying happy hour and celebrating birthdays should all be encouraged. You can even surprise employees by arranging to have lunch delivered to them!

Cybersecurity will continue to be in high demand, so we're here to be your trusted advisor and help your customers avoid business disruption by providing the best and latest security technology and expertise.

For more information on how Tech Data can help your customers return to work and strengthen their remote workforce, please contact us at:

securityservices@techdata.com
or visit techdata.com/security

TECH DATA RESOURCES

- *SPI Tool*
- *Digital Security Practice Builder*
- *Cyber Range*

INDUSTRY RESOURCES

- ***National Vulnerability Database nvd.nist.gov –***
  The U.S. government repository of standards-based vulnerability management data.
- ***The SANS (SysAdmin, Audit, Network, Security) Institute www.sans.org/security-resources/ –***
  Resources for computer security training, network research and resources.
- ***Hoax Reference Site http://snopes.com –***
  Resources to verify if an email warning or story is a hoax.
- ***The Security-Specific Search Engine SearchSecurity.com –***
  Offers a variety of newsletters or webcasts dedicated to security, including security-specific daily news, thousands of links and interaction with leading industry experts.
- ***Security and Privacy Research Center www.cio.com –***
  Resources to keep a network and site secure—from creating and implementing a security policy to dealing with rogue programmers.
- ***Computerworld Knowledge Center https://www.computerworld.com/category/security/ –***
  Includes the latest headlines, upcoming events, links to vendors, security statistics and reviews, and online discussions.
- ***Electronic Privacy Information Center www.epic.org –***
  This public interest research center covers the gamut of online privacy issues.
- ***The CERT Coordination Center www.cert.org –***
  A major reporting center for Internet and network security vulnerabilities at Carnegie Mellon University.
- ***Information Systems Security Association www.issa.org –***
  A nonprofit association for information security professionals that promotes secure information systems management practices.
- ***Center for Internet Security www.cisecurity.org –***
  CIS members identify security threats of greatest concern and develop practical methods to reduce the threats. Provides methods and tools to improve, measure, monitor and compare the security status of your Internet-connected systems and appliances.
- ***NIST's Computer Security Resource Center csrc.nist.gov –***
  Resources from the National Institute of Standards and Technology's Computer Security Division, including resources and standards for government IT deployments.