EBOOK

8 Cyberthreats to Watch Out For

A Guide from the Managed Services Experts at TPx

EXECUTIVE SUMMARY

Technology is constantly innovating and evolving. As new technology emerges, so do the corresponding cyberthreats and cybersecurity responses. This “threat landscape” encompasses all recognized and potential threats affecting a sector, a group, a designated time, a particular technology and so forth – and it changes almost daily.

For these reasons, it’s challenging for businesses of any size to be vigilant to all identified or predicted threats – much less research, vet, deploy and manage the appropriate protections and countermeasures. This eBook outlines eight cyberthreats on the rise or that are lesser known.

Key Takeaways

Cyberthreats are complex and evolving.

Cyberattacks are increasing year over year.

Stakeholder education is key to detecting, avoiding and mitigating cyberthreats, but it can be challenging to maintain constant vigilance in a response-react environment.

Working with a cybersecurity provider can give businesses instant access to expertise and quicker response times without adding overhead.

Table of Contents

Cyberthreat 1: Funds Transfer Fraud

Funds Transfer Fraud (FTF) isn't a new way to attack, but it is evolving. FTF used to be focused on downloading emails to steal credentials and extort a payment.

Now, it's about tricking a victim into wiring funds. The process is the same. Threat actors (TAs) use social engineering techniques like phishing. They intend to gain access to a business' email system to cause a business email compromise. Once a TA has access to a corporate mailbox, the TA often manipulates a user's contacts and inbox, looking for payment instructions. This attack usually happens without triggering any security alerts.

Prevalence

According to Coalition's [2022 Cyber Claims Report](), there's been a noticeable uptick in claims and attacks related to FTF. For example, the frequency of FTF attacks significantly increased, rising 54% in the second half of 2021. This is especially true for small and mid-sized businesses.

Potential Business Impact

Coalition concluded that from 2020 to 2021, losses from FTF increased 69% overall, and among enterprises with revenue under $25 million, the frequency went up 21%. Initial losses from FTF among small and mid-sized businesses jumped 102% to more than $309,000 in the second half of 2021.

Real-World Example

In October of 2022, a manufacturing company received an invoice from a staffing firm. The accounts payable department transferred a $207,000 payment, believing nothing was out of the norm. Eventually the staffing firm checked in on their late payment status and the fraudulent payment was discovered. In this specific instance, either the manufacturing company or the staffing firm could have been out the $207,000 without remediation from a knowledgeable security services provider.

What Can You Do?

- Turn on multi-factor authentication (MFA) for email and other critical systems.
- Treat all new payment instructions or changes as suspicious. Verify the request by phone using the last known number of the person making the request. Never use the contact information in the email, as this information is often fraudulent.
- Install a verification procedure with a defined, two-party transfer approval process and required reviews for payment change details. For example, verify the transaction with another executive, either verbally or in writing.
- Have a cybersecurity education program that teaches employees how to recognize and report potential attacks.

Cyberthreat 2: Deep Fakes

Deep fakes use artificial intelligence (AI) technology to create convincing – but misleading – audio, video or still images. In the workplace, a threat actor (TA) will use a deep fake to trick employees into making unauthorized payments or disclosing sensitive information. The attacks may be in real-time, such as telephone calls or virtual meetings. They may also be asynchronous, such as chat, email, voicemail or social media. Deep fake technology can be so realistic that imposters can successfully impersonate high-ranking executives, as profiled by the Wall Street Journal.

In this publicized case from 2019, a corporate employee believed an emergency wire transfer request came directly from the company's CEO, as the voice-spoofing technology was so accurate. Deep fake attacks are thorough, often deploying compromised email accounts to set up meetings, send additional requests or follow up with further requests.

Prevalence

Since its earliest days, email has been an easy way for a TA to phish for targets. With the rise of the remote and virtual workplace, it's more common to use video and voice channels – and phishing has followed along. As technology evolves, deep fake campaigns will be more common – and more successful. With deep fakes, AI is the cause and the prevention. AI technology, such as machine learning (ML), can analyze suspicious communications and help detect deep fakes.

Potential Business Impact

Deep fakes are a slippery slope. If audio and video can be fabricated, so can other ways to determine the veracity of a request, including security logs, network administration and so forth. With human error still the main source of a security compromise, there is a high likelihood that a stakeholder will innocently play into a deep fake. Or, even worse, be the subject of or the victim of a deep fake.

Real-World Example

In March of 2019, the CEO of a UK-based energy firm believed he was on the phone with his boss, the chief executive of the energy firm's German-based parent company, when he followed verbal orders to immediately transfer $243,000 to the bank account of a supplier. In reality, the voice belonged to a fraudster using AI voice technology to spoof the chief executive of the parent company.

What Can You Do?

- Have a cybersecurity education program that focuses on deep fake phishing tactics and how to spot suspicious cues, such as unnatural facial movements in a video or choppy, pieced-together audio.
- Challenge the request! Take time before responding to any requests for sensitive information. For example, pause and think about whether this person would typically make that request.
- Implement a verification policy for any requests for financial or other sensitive information. For example, enforce verification in multiple channels for both real-time and asynchronous requests.

Cyberthreat 3: Multichannel Threats

Email remains the top threat vector, but businesses can't ignore other channels. The rise of hybrid and remote work means more employees use personal devices to access business applications. It also means they rely increasingly on productivity platforms – such as SMS/text, Microsoft Teams, Webex, unified communications and collaboration platforms and more – to stay connected. Although these channels are popular, they may not be monitored and protected to the same degree as email. This provides ample opportunities to trick users into revealing sensitive information.

These "multichannel" threats often start as a typical invitation from a co-worker's compromised messaging account. This spear-phishing tactic would contain a malicious link to log in to the "meeting." Once in this meeting, the victim would enter their personal credentials for that app – and then it's off to the races for the TA, who now can deliver attacks from a legitimate service.

Prevalence

According to Coalition's 2022 Cyber Claims Report, claims and attacks show a noticeable uptick. For example, the frequency of FTF attacks significantly increased, rising 54% in the second half of 2021. This is especially true for small and mid-sized businesses.

Potential Business Impact

How we work and where we work has changed. Cybercriminals have seized this new frontier and have shifted their approach accordingly. Most multichannel attacks can skirt most detect tools, as the attacks originate from shared and typically trusted services. Growth in multichannel threats is only expected to grow.

Real-World Example

Attackers targeted a U.S. network technology company named Ubiquiti Networks and managed to steal $46.7 million using spear phishing. Attackers impersonated executives and convinced the finance department to transfer money to an offshore bank account.

What Can You Do?

- Assess existing cybersecurity measures to determine if your organization is vulnerable. Is the workforce using personal or unprotected mobile devices? Are employees protected when using URLs?
- Ensure cybersecurity plans include education, processes and tools. Create awareness about multichannel phishing tactics. Enable alerts and a process for reporting suspicious requests.
- Deploy security tools that can detect and block threats across Internet and mobile services, not only email.

Cyberthreat 4: Supply Chain Attacks

Supply chains take various forms. There's the physical supply chain, with raw materials and manufactured goods. There's also the digital or network supply chain. A digital supply chain attack, also called a partner network or third-party attack, occurs when a trusted partner's service is already compromised when the victim grants it access – and then passes on that vulnerability to other users and customers. Often, the end user doesn't know these vulnerabilities as they are so well disguised and buried deep within the original platform.

Prevalence

Supply chain attacks are on the rise and are expected to continue threatening businesses of all sizes. In 2021, supply chain attacks on open-source software grew 650%. As most of these threats are established during production or distribution, they can be more challenging to detect and prevent by the end user. Headline-makers, such as Log4Shell vulnerability and the massive SolarWinds attack, are sophisticated and coordinated threats with global repercussions.

Potential Business Impact

In early 2020, hackers compromised Texas-based SolarWinds' systems and added malicious code directly into the company's software system. This system, called Orion, was used by more than 33,000 companies to manage IT resources. SolarWinds regularly distributes software updates to patch vulnerabilities or add new features like most providers. After the hack, SolarWinds sent out updates containing malicious code, creating a backdoor to every customer's systems using Orion.

SolarWinds may be the poster child for a large-scale supply chain attack, but with more solutions being developed and distributed, it's not hard to see how any business could be potentially compromised.

Real-World Example

In 2023, a supply chain attack exploited an SQL injection vulnerability in MOVEit's software, a managed file transfer platform. The attack affected over 130 organizations worldwide, including British Airways, the BBC, Zellis and the Minnesota Department of Education. The extortion attacks from hackers will result in losses of over $75,000,000 in total.

What Can You Do?

- Start as you mean to finish. For developers, this means implementing more security controls by checking open-source providers and their security measures. Vet the security measures all partners take.
- Think differently about security. Take steps to ensure all steps of development and testing are secure.
- Monitor system performance after doing an update. If there's anything unusual or suspicious, flag it and report it immediately.

Cyberthreat 5: API Attacks

An application programming interface (API) allows two or more systems to talk to each other – think of it as a messenger between one platform and another. It's a way to get one app to agree to "listen" and respond to another.

APIs are used more than ever before by developers and by businesses. For example, think of a mobile app or a website accessing information from a financial account. Or a weather app that is pulling data from a weather service. APIs are used in countless ways because they make programming easy. APIs are widely used across all industries and are increasingly vulnerable to attack. For example, in a business logic attack, a threat actor (TA) uses APIs in unintended ways to find vulnerabilities in data storage and retrieval processes.

Prevalence

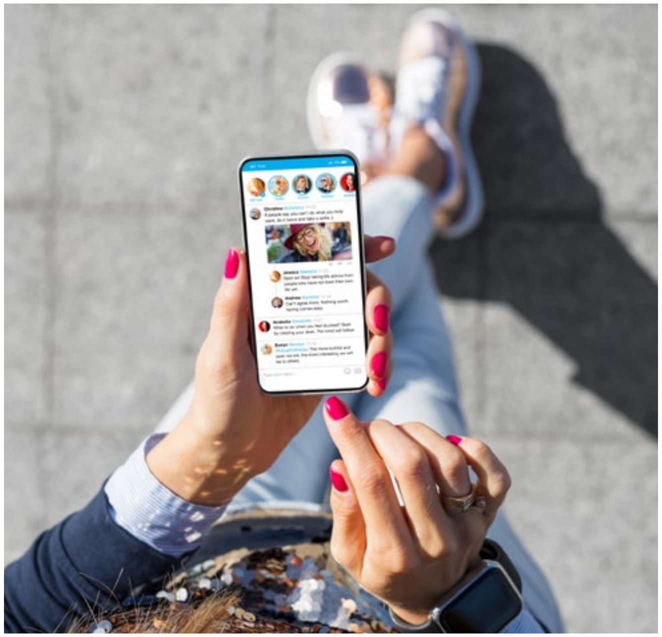
According to Gartner, 2022 was the year of the API attack, noting: "… API attacks will become the most-frequent attack vector, causing data breaches for enterprise web applications." It tracks: as businesses move more of their infrastructure and platforms to the cloud, more APIs are used to help manage and connect that data. It follows that cybercriminals will use them, too.

Potential Business Impact

APIs are the building blocks of most applications, and their numbers are nearly incalculable. The use of APIs is growing as they enable critical business functions, enhance user experience, and facilitate digital transformation. This accessibility and sheer numbers make APIs a preferred attack vector – and that attack surface is growing. APIs are not software, so traditional security solutions may not detect vulnerabilities.

Real-World Example

In July of 2022, the social media platform Twitter reported an API breach that occurred from late 2021 into 2022 and exposed the PII of 5.4 million user accounts. The vulnerability was with an API that allowed users to find other users, and mistakenly revealed PII.



What Can You Do?

- Recognize that APIs are challenging to protect. The Open Web Application Security Project, or OWASP, recommends focusing on strategies and solutions to recognize and mitigate the unique vulnerabilities of APIs.
- Assign API security leads. These can be across multiple departments, such as security and DevOps, or concentrated entirely in development.
- Consider a security platform explicitly designed for APIs that collect, store and analyze Big Data.

Cyberthreat 6: Insider Threats

Insider threats are caused by anyone with authorized access to a system, which has the potential to harm that system through their actions. Unlike the usual cyberthreats, insider threats require defending the system from someone on the inside. This is often an employee but can also be a third-party vendor with authorized access.

There are three major sources of insider threats:

Unintentional Negligence
Not all insider threats are deliberate or malicious, as they're caused by human error, so it's often harder to detect harmful insider activities.

Malicious Action for Personal Gain
Insiders have a unique perspective regarding knowing weaknesses in an organization's cybersecurity or where sensitive data is stored. This provides opportunity and often greed or ill will is the opportunity.

Stolen User Credentials
Attackers can use stolen credentials to gain access to sensitive information. This can be the result of poor cybersecurity practices as much as it can be from a deliberate hack.

Prevalence

According to Kroll, insider threats peaked at their highest quarterly level in Q3 2022, accounting for nearly 35% of all unauthorized threat incidents. The recent “Great Resignation” led to a spike in employees leaving one job for another. This shift created an opportunity for disgruntled employees to steal data, corrupt files or leave general chaos in their wake. Or for others who simply want to move over contacts or proprietary information to help them kickstart a new job.

Potential Business Impact

According to Ponemon Institute’s 2022 Cost of Insider Threats report, incidents have risen 44% over the past two years, with costs per incident up more than a third to $15.38 million. Insider threats can have far-reaching consequences – even if the event is caused by accident or no corporate harm intended. If a data breach results, financial and reputational harm can follow. Penalties for failing to protect the organization and meet cybersecurity requirements are expected. Customers – and other internal stakeholders – can quickly lose trust.

Real-World Example

In January 2021, four lawyers of the Elliott Greenleaf law firm stole the organization’s files and deleted its emails, including correspondence, pleadings, firm records and the client database. Insiders stole sensitive files for personal gain to help Armstrong Teasdale and his competing law firm launch a new office in Delaware. As a result, Elliott Greenleaf lost the ability to compete effectively in Delaware and their office in Wilmington was put out of business.

What Can You Do?

- Foster a “threat aware” culture – cybersecurity is the responsibility of an entire organization, not one person or team.
- Use a multi-vector approach of detecting, identifying, assessing and managing to protect your organization.
- Remember that there is no one-size-fits-all approach to threat assessment. Develop a threat assessment process to compile and analyze information based on behaviors, not profiles.
- Focus on helping, not harming. Keep the approach holistic and respectful.

Cyberthreat 7: Encrypted Malware

Malware runs malicious code and is often spread by phishing. Encrypted malware takes it to the next level. Encrypted malware incorporates encryption technology, allowing it to “hide” in plain sight. The ransomware package it may contain is also encrypted – creating a multi-layered threat that’s harder to detect – even when using robust security tools and protocols.

🟩 Prevalence

Encryption is used to protect data from being compromised. Conversely, threat actors (TAs) also use encryption technology to protect their malware, which is on the rise. In 2020, Sophos reported that nearly half (46%) of all malware was hidden within an encrypted package. This is thanks to Transport Layer Security (TLS) – one of the most significant contributions to Internet privacy and security of the past decade – being deployed by TAs.

Potential Business Impact

Most organizations do not have the resources to monitor and detect these encrypted packets and may be allowing massive amounts of malware to enter their networks. As encrypted malware infiltrates by stealth, it poses a tremendous threat to data. Whether that data is compromised, stolen or destroyed due to the attack doesn’t matter – the entire business can falter.

Real-World Example

Sportswear brand Puma lost control of around half of its employees’ personal information in February 2022, after ransomware actors hit the company’s cloud provider, Kronos Private Cloud (KPC), leading to the theft of data from 6,632 of Puma’s employees.

What Can You Do?

- Ensure prevention and detection systems are up-to-date and optimized
- Use secure sockets layer (SSL) inspection to identify and stop encrypted threats
- Have a scheduled and redundant backup system
- Emphasize the importance of verifying websites before providing credentials
- Use virtual private network (VPN) technology to connect to the Internet
- Use password management applications

Cyberthreat 8: Fileless Malware

Fileless malware uses a computer system's legitimate software and programs to execute an attack. Much like an autoimmune disease in a body, fileless malware takes advantage of inherent vulnerabilities in installed software and targets them. It can be challenging to detect due to the focus many endpoint security solutions place on scanning files rather than processes. This attack doesn't leave a trail because it doesn't rely on files.

Prevalence

Fileless malware first gained traction as a mainstream threat in 2017. The very nature of fileless malware makes it successful. In a fileless attack, a user clicks on a link or an attachment in a phishing email. This allows a threat actor (TA) to access the system using trusted applications or the operating system itself. Headline-making fileless attacks include the Democratic National Committee and Equifax. The Equifax attack alone exposed the personal information of 143 million people.

Potential Business Impact

Fileless malware is used to access data across an entire network and is designed to spread from one device to another. The business implications can be enormous. Equifax, for example, agreed to a global settlement with the Federal Trade Commission (FTC), the Consumer Financial Protection Bureau, and all U.S. states and territories for upwards of $425 million.

Real-World Example

The Democratic National Committee (DNC) was breached by a fileless malware attack in 2015, by two Russian computer hacking groups. The malware program resulted in successful spying on communications including all DNC email and chats and stealing of DNC opposition research.

What Can You Do?

- Update all software and applications. This simple (and often overlooked) move is the best way to patch and enhance security.
- Use cloud-based solutions to ensure automatic updates
- Deploy an integrated approach that looks at the entire threat lifecycle
- Recognize that there are different fileless threats and different tactics to block them. As the TAs become more sophisticated, so have the ways to thwart them.
- Educate all stakeholders on proper Internet and application hygiene and proper protocol to verify if a request is legitimate

Part 2: Why Use a Managed Services Provider?

Ultimately, companies have a handful of options to address their cybersecurity needs – they can take it on themselves, work with a qualified managed services provider (MSP) or ignore the threats altogether and pray they don't fall victim to an attack.

Why Should Your Business Work with a Managed Services Provider?

Organizations like yours work with an MSP for their cybersecurity needs instead of handling it in-house for these key reasons:

Lack of Expertise

The breadth and depth of knowledge demanded by IT teams today is vast and spans not only cybersecurity expertise but data storage, data integrity insight, software development, information technology infrastructure library (ITIL) knowledge, database design and management, network services, cloud computing, data analysis, troubleshooting and more. Security is a unique and complex discipline in itself.

Lack of Time

Due to the interconnected nature of integrated applications, devices and other technologies, IT departments are stretched thin putting out fires. Many teams don't have the time to effectively handle complex cybersecurity measures, including vigilance and awareness of the changing threat landscape.

Lack of Talent

The IT skills gap is a well-known challenge for businesses, especially SMBs, that cannot typically pay for hard-to-source expertise. This skills gap is prominent in the hyper-specialized realm of cybersecurity protection.

What are the Benefits of Working with a Managed Services Provider?

Working with a managed services provider gives businesses the following benefits:

Instant Access to Expertise

Working with a managed service provider (MSP) delivers instant access to teams of trained personnel who are experts in protecting your business from cybercrime.

Reduced Overhead

You won't need to hire, retain or train cybersecurity specialists in-house since the MSP takes care of that expense.

Affordable, Predictable & Scalable Plans

Working with a managed services provider can be significantly less expensive than developing and deploying sophisticated cybersecurity resources internally. MSP solutions are scalable and offer predictable pricing, giving you control over your IT budget.

The Ability to Focus on Your Business

Cybersecurity is a complicated undertaking and an entire business unto itself. You can focus on managing and growing your core business by working with a managed service provider.

Part 3: What Should You Look for in an MSP?

When seeking the right MSP to partner with, you must find one you can rely on to help you through your company's growth phases. That means top-tier expertise, financial stability, the size and reach to scale with your company as it grows, flexibility, reliability and 24/7/365 support.

Key attributes to look for when selecting an MSP to manage your cybersecurity include:

Portfolio Breadth
An all-in-one provider with a fully managed IT suite of networking, security and communications solutions will give your business a cohesive solution and even pass on cost savings in the form of comprehensive service bundles.

Pricing Models
Generally speaking, larger MSPs can give you the ability to pay off capital expenses like firewalls and network builds over time, which can help you get the best solution for the job while making your IT and finance teams happy.

Service Levels

The MSP should offer 24/7/365 fully managed services and provide the flexibility to co-manage the solution or operate on an on-demand basis. As your business scales, your MSP should adapt to meet your requirements.

Certifications

Certifications present an instant test for credibility. An MSP certified by dozens of technology vendors and compliance auditors will keep your solutions up-to-date and in line with industry standards.

Geographic Availability

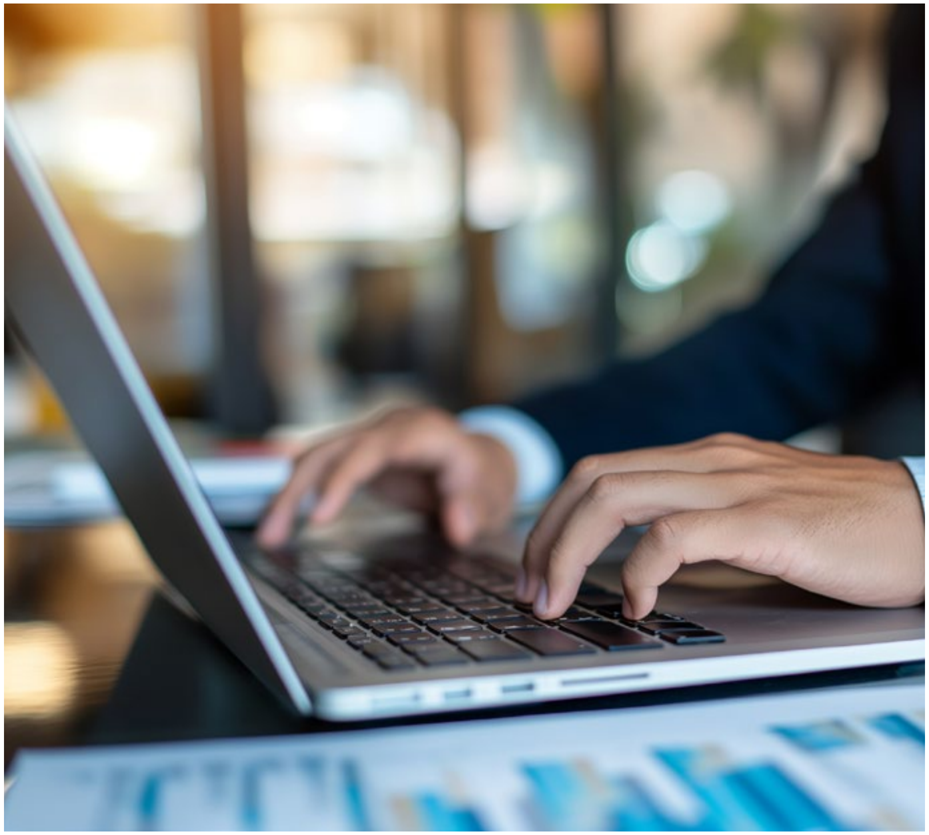
An MSP with nationwide coverage can grow with your business as you expand into new regional markets and meet the IT needs of multiple locations.

Technical Expertise

Your MSP should have specialists on staff who can handle installation, ongoing management and troubleshooting for every solution set you're using, including ransomware protection services.

Size for Scale & Influence

Small MSPs lack the resources to deliver a fully managed IT solution that spans a broad spectrum of services. Further, the relationship power of large MSPs pays off in ways that smaller MSPs can't match, with priority given to technological collaboration and product advancement between underlying providers. Smaller and regional MSPs don't have that same clout.



Technical Infrastructure

Your MSP should have the infrastructure necessary to manage the solutions they provide. These include capital investments like Security Operations Centers (SOCs) for managed security vendors, remote desktop access for instantaneous support and testing labs for testing firmware and software updates in staging environments before applying them to your live setup.

Part 4: Why Choose TPx for Cybersecurity Protection?

You have enough challenges in your business life. You don't also need to worry about data breaches and the potentially catastrophic impact of cyberthreats on customer relations, business operations, workflow and your bottom line. At TPx, we have the products, services, experience and certifications to keep your network safe and running smoothly.

TPX
Explore our Managed IT Services
Bringing the Best of IT Together
Business Internet
Networking
Cybersecurity
Cloud Communications

Why Choose TPx?

- ✓ We solve the biggest IT issues – cybersecurity, connectivity and collaboration – under one umbrella.
- ✓ Our buying power enables us to customize your solutions for maximum effectiveness within your budget.
- ✓ We have 120+ certifications across 60+ competencies, like CompTIA, Cisco, Fortinet, Microsoft, SMC and more.
- ✓ We have the IT solutions, staff and experience you need for effective results within your budget.
- ✓ We provide enterprise-class and 24/7 support for ongoing, proactive support tailored to your business.
- ✓ We mix and match solutions and deliver a variety of service levels customized to meet your needs, including managed and co-managed options.
- ✓ We modernize your IT, connectivity and communications while minimizing your risk from cyber threats.
- ✓ With thousands of customers nationwide, we're big enough to get the job done and small enough to be agile.

Essential “Must-Haves”

Backup and Disaster Recovery (BDR)

We help organizations quickly recover from system downtime and data loss caused by cyberattacks, human error, system failures and natural disasters. Using advanced hybrid local/cloud technology and skills management resources, TPx delivers a turnkey BDR solution that will meet your recovery objectives. All backups are scanned for ransomware and when a ransomware footprint is detected, you can roll back your systems as if it never happened.

Next-Generation Firewall (NGFW)

The firewall protects your network from internet-based threats. Next-generation firewalls block today’s advanced threats while providing secure access, visibility and control to help your business be more productive. TPx ensures UTM features such as web filtering, antivirus, application control, intrusion prevention and VPNs are properly configured, monitored and maintained.

Endpoint Management and Security

TPx helps keep your servers and workstations healthy, secure and performing optimally. Our endpoint security service leverages remote monitoring and management (RMM), patch management and security. Together with expert support personnel and security analysts, we provide an “always-on,” best-in-class, 24/7/365 service.

Managed Detection and Response (MDR)

Discover, prevent and recover from cyberthreats faster. TPx’s MDR helps you identify more threats, reduce attack dwell time, and proactively mitigate attacks. We offer managed detection and response for both firewalls and endpoints.

Strategic “Must-Haves”

Security Advisory Services
TPx advisory services provide comprehensive security consulting that can help improve your security posture and protect your business. Our services comprise a cybersecurity gap assessment, network vulnerability and penetration scanning, network security assessment, wireless security assessment and ransomware readiness assessment.

Penetration Scan
TPx experts show how exploiting a vulnerability could result in a significant impact on your environment.

Vulnerability Scan
TPx evaluates devices connected to the network to identify vulnerabilities present due to open ports, missing patches, etc.

Network Security Assessment
TPx evaluates your organization’s network security posture and profile.

Wireless Security Assessment
TPx evaluates your organization’s wireless infrastructure and configuration, security posture and functional capabilities.

User Security

Inbox Detection & Response (IDR)

TPx's Managed IDR service allows users to easily report suspicious emails with an Outlook plug-in to quickly determine if the emails are safe or malicious.

Security Awareness Training (SAT)

Users are your first line of defense. The more they know, the less prone they are to becoming victims of phishing scams or other security incidents. Our service includes monthly phishing simulations and Security Awareness Training courses with automated reporting to track your results.

DNS Protection

We protect systems and users from malicious websites using leading DNS protection software. Windows devices are protected both on the corporate network and while traveling. Network-based DNS protection covers BYOD, guest wireless, and non-Windows devices to deliver comprehensive DNS security and reduce your risk of attack.

Need Help With Cybersecurity?

CONTACT US

ABOUT TPX

TPx is a nationwide managed service provider helping organizations navigate the growing IT complexity. Founded in 1998, TPx offers comprehensive managed IT services including internet, networks, cybersecurity, and cloud communications. With a focus on service, TPx is dedicated to the success of its customers by making IT easy with solutions that address today's evolving technology challenges. For more information, visit www.tpx.com.

For more information

in X f You Tube tpx.com