A Comprehensive Guide to

Ransomware

FROM THE MANAGED SERVICES EXPERTS AT TPX

Executive Summary

In recent years, businesses of all sizes have become increasingly under threat from financially devastating cyberthreats like ransomware.

This comprehensive guide looks at ransomware's common attack vectors and how businesses can protect themselves from this pervasive malware.

Key Takeaways

- Ransomware is the most common form of cyberattack.
- Ransomware attacks are increasing year over year.
- Paying a ransom doesn't mean organizations will successfully recover their data.
- Breached organizations risk double extortion (or more) from a single successful ransomware attack.
- Cyber insurance payouts aren't a comprehensive cyber incident response plan.

Table of Contents

PART 1

What is Ransomware?

Ransomware is a type of malware in which the data on a target device is locked via encryption and a ransom payment is demanded before the data is decrypted and access is returned to the victim. Ransomware remains the most common cyberthreat to small and medium businesses (SMBs), with **60 percent of MSPs reporting that their SMB clients have been hit as of third quarter of 2020**, Datto reveals.

How Does Ransomware Work?

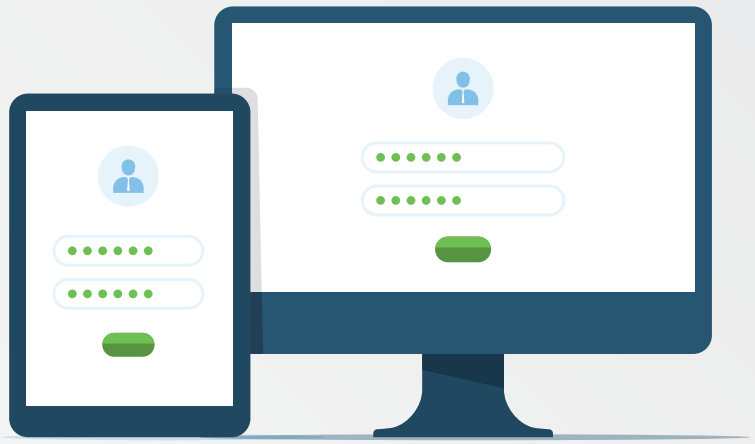
Ransomware must gain access to a target system to execute. Once access is achieved, ransomware will lock access to affected files through asymmetric encryption. Then, cybercriminals will demand a ransom from the victim (individual or company) in exchange for the means to unencrypt the files, which typically is a decryption key.

What Are Triggers of Ransomware?

Ransomware will enter a target system through multiple pathways that organizations need to be on the lookout for, including:

- **Phishing** — Phishing is a data breach through social engineering. It's the bad guys fooling your employees into admitting them into your network or otherwise helping them commit cybercrimes against your business. Typically, the hacker disguises its email, phone, or other means of communication to appear as if it's coming from a legitimate source. Your staff is tricked into divulging critical information such as passwords or other sensitive data. Phishing might result in identity theft or financial theft through fake invoices or payroll diversion fraud, among other crimes.
- **Drive-by Downloading** — Drive-by download attacks occur when malicious programs install on your computer or mobile devices without your consent as an unintentional download. A drive-by download can take advantage of an application, operating system (OS) or web browser that contains security flaws due to failures to update. Unlike a majority of other types of cyber attacks, a drive-by doesn't rely on the user to do anything to activate the attack. Once on your system, a drive-by download will hijack your device to build a botnet, infect other machines, extract information, destroy data or disable your device.
- **Social & Instant Messaging** — Social and instant-messaging threats work the same way email ones do; malware is launched when the recipient clicks on an executable file attachment or on a hyperlink that links through to a malicious website.
- **Poor Patch Management** — Technology and software providers can accidentally release "bad patches" that can cause system downtime or problems with other applications or your systems. New software updates and patches also can be incompatible with elements or integrations with your tech stack, leading to security vulnerabilities and gaps in your network or even in critical systems like firewalls.

- **Unmonitored Environments** — A successful ransomware attack must go through several steps, such as initial access, lateral movement and defense evasion. Each of these phases can be monitored, detected and stopped with the right tools in place. Without these tools, an organization is unlikely to detect a ransomware attack until it's too late.
- **Weak Passwords & No Identity Access Management (IAM)** — If a malicious actor can guess a user's passwords easily or trick the user into giving them their password (potentially through a phishing email), they will gain a foothold in your organization's network. So, if you don't have a process for identity access management, you'll be more vulnerable to ransomware.
- **Remote Desktop Protocol (RDP) Compromise** — Remote Desktop Protocol or RDP is a proprietary Microsoft protocol that allows users to connect to a system remotely over a network connection. RDP compromise is a cyberattack whereby a hacker uses RDP to remotely connect to a system to deploy and execute a ransomware program.



What Are Types of Ransomware?

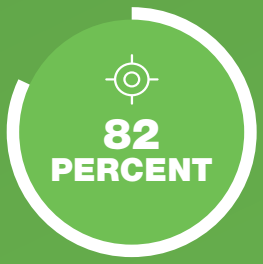
- **Crypto** — Crypto ransomware is a variant of ransomware that allows the attacker to encrypt the files stored on the target device to extort money to unencrypt the files. The encrypted files are typically deleted if the ransom isn't paid by the deadline.
- **Locker** — This type of ransomware blocks basic computer functions. For example, you may be denied access to the desktop while the mouse and keyboard are partially disabled. This allows you to continue to interact with the window containing the ransom demand to make the payment. Apart from that, the computer is inoperable.

- **Scareware**— A scareware attack is often launched through pop-ups on a user's screen, warning them that their computer or files have been infected and then offering a solution. This attack aims to scare users with the perception of a threat to manipulate them into buying and downloading unwanted malware designed to steal the user's data from the target device.
- **Leakware** —Leakware is a type of ransomware attack wherein the organization or individual affected must pay the ransom, not only to recover encrypted data but also to prevent the thief from leaking data to the public. This tactic creates an urgency to pay the ransom since the knowledge of the attack won't be contained within the affected organization.
- **Double Extortion** — A double extortion ransomware attack occurs when threat actors exfiltrate a victim's sensitive data in addition to encrypting it. This gives the criminal leverage to collect multiple ransom payments since they can repeatedly threaten to release sensitive data if additional ransoms aren't paid.
- **Ransomware as a Service (RaaS)** — Ransomware as a service (RaaS) is a subscription-based model that enables affiliates to use ransomware technology to execute ransomware attacks. Affiliates earn a percentage of each successful ransom payment.

PART 2

Why Worry About Ransomware?

Now, you might be thinking, “What’s the big deal? My team is smart, and we won’t fall victim to phishing emails or instant messages. Why should I be concerned?” Well, even businesses with intelligent teams get hit with ransomware since the volume of attacks is increasing at alarming rates, escalating in sophistication and coming from more organized sources.



SMBs Are a Primary Ransomware Attack Target

Your business is not too small to be a target. In fact, **82 percent of attacks that took place in 2021** impacted organizations with less than a thousand employees.

Increase in Ransomware Attacks

Ransomware attacks are becoming more and more common.

The FBI **received** 3,729 complaints from ransomware victims in 2021 with estimated losses at more than $49.2 million.

The FBI's Internet Crime Complaint Center **reported 2,084 ransomware complaints** from January to July 31, 2021. This represents a 62 percent year-over-year increase.

Escalation in Ransomware Attack Sophistication

From crypto and lockers to scareware and leakware to double extortion and RaaS, ransomware attack vectors have grown in complexity.

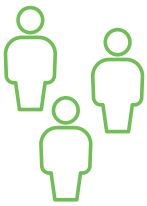
Microsoft's 2020 Digital Defense Report data from October 2019 to July 2020 shows that hackers have rapidly improved the sophistication of cyberattacks.

Evolution in Types of Ransomware Attackers

It's no longer the stereotypical lone hacker in a basement who's going after your business. Full-fledged crime syndicates and organizations funded, backed and even run by nation-states employ full-time hackers, quite literally with salaries and benefits like any corporate office job, to infect your systems.

Lone Hackers

Crime Syndicates



Nation-States

Costs of Ransomware

The impact of a ransomware attack can be immense. The average cost to recover from one recent ransomware attack in 2021 was $1.4 million.

During the first half of 2022, the **average cost of a claim for a small business owner increased to $139,000**, which is 58 percent higher than levels during the first half of 2021.

It took businesses on average one month to recover. Ninety percent of firms said the attack impacted their ability to operate, and 86 percent of private sector victims said they lost business and/or revenue because of the attack, according to the **State of Ransomware 2022 global survey**.

And the attacks show no signs of letting up. **Sixty-six percent of surveyed organizations were hit with ransomware last year**, up from 37 percent in 2020.

Ransomware can cost your business in many ways aside from the ransom payment itself, including:

- **Damage or Theft of Data**
- **Ransom Payment**
- **Paying + Losing Data Anyway**
- **Lost Productivity**
- **Downtime**
- **Data Recovery + Restoration Costs**
- **Reputational Harm**

Ransomware in Real-World Scenarios

Ransomware doesn't discriminate.
All industries and verticals are vulnerable to attack.

Education

Broward County Public School in Fort Lauderdale, Fla., fell victim to ransomware when **hackers demanded a ransom of $40 million**. An offer of $500,000 wasn't large enough for the hackers, who had reduced the ransom to $10 million, so they posted 25,971 of the school's files online.

Government

Costa Rica **declared a national emergency in response to a cyberattack** in April 2022. The ransomware attack impacted government services and private sector companies engaged in import and export. Ransomware group Conti took responsibility for the attack and demanded the government pay a ransom of $20 million.

Oil & Gas

A **ransomware attack was made against Colonial Pipeline in May 2021**, starting in the billing system. To prevent spreading, the company ceased control system operations. This in turn caused closure of a pipeline that moves 45 percent of fuel on the U.S. East Coast. $4.4 million was paid to the cybercriminals to regain access.

Manufacturing

Nvidia, the world's largest semiconductor chip company, was **compromised by a ransomware attack in February 2022**. The ransomware group, Lapsus$, took responsibility for the attack and claimed they had access to 1TB of exfiltrated Nvidia data they would leak online and demanded $1 million and a percentage of an unspecified fee from Nvidia.

Aviation

Indian airline **SpiceJet dealt with an attempted ransomware attack in 2022**, leaving hundreds of passengers stranded in several locations in the country for multiple hours.

Retail

British-based discount stationery and books retailer **The Works was targeted by ransomware in April 2022,** forcing it to shut down five stores.

PART 3

How Can You Protect Against Ransomware?

Now. that you're appropriately warned about the dangers of ransomware, you need to know how to protect your business from ransomware attacks and how to respond when an attack is successful.

The experts at TPx have identified four typical response options worth most organizations' consideration. More than one response option can be used and include:

- Response Option 1: To Pay or Not to Pay
- Response Option 2: Report Ransomware
- Response Option 3: Collect Cyber Insurance
- Response Option 4: Secure + Safeguard

Let's dive into the details of reach response option.

What are Responses to Ransomware Attacks?

Response Option 1: To Pay or Not to Pay

The choice every ransomware victim must face is whether to acquiesce to the hackers' demands and pay the ransom or not pay them. While paying a ransomware attack is an option, it's one that governments have taken a unified stand against. Some have issued laws, such as the 2020 ruling by the U.S. Department of Treasury's Office of Foreign Assets Control (OFAC) and Financial Crimes Enforcement Network (FinCEN), that make most cases of **paying ransoms illegal**. If you're considering paying up, here are some factors to keep in mind:

Law enforcement advises against ransomware payouts. The Federal Bureau of Investigation (FBI) and the Department of Homeland Security (DHS) officially recommend that organizations avoid paying ransoms.

Payment doesn't guarantee all your data will be restored. On average, **only 65 percent of the data is recovered** and only eight percent of organizations manage to recover all of their data. Encrypted files could be unrecoverable, with decrypters provided by your ransomware attackers crashing or failing, resulting in your company needing to try to build a new decryption tool. Even if you don't encounter any glitches, recovering the data can still take several weeks, depending on the volume of encrypted data. Plus, hackers may retain copies of your data, leaving you vulnerable to double extortion.

11% of organizations said they paid ransoms of $1 million or more, up from 4 percent in 2020.

Ransom payments are becoming increasingly higher. In 2021, **11 percent of organizations said they paid ransoms of $1 million or more**, up from 4 percent in 2020, while the percentage of organizations paying less than $10,000 dropped to 21 percent from 34 percent in 2020.

More victims are paying out the ransom. According to the State of Ransomware 2022 global survey, in 2021, 46 percent of organizations with data encrypted in a ransomware attack paid the ransom. Twenty-six percent of organizations that were able to restore encrypted data using backups in 2021 also paid the ransom.

Response Option 2: Report Ransomware

Remember, ransomware is a federal crime, with penalties under the federal Computer Fraud and Abuse Act (CFAA) that will result in fines and imprisonment for up to 10 years for first-time offenders and up to 20 years for second-time offenders. As such, ransomware should be **reported to the FBI** and treated by your organization with the same seriousness and haste as a physical break-in at your place of business.

> "If You're Hit by Ransomware, Don't Forget to Call Us."
>
> — FBI

Reporting the ransomware attack to authorities may have tangible results; federal investigators recovered $500,000 in ransom payments after a Kansan medical provider called the FBI about the incident, says U.S. Deputy Attorney General Lisa Monaco.

Response Option 3: Collect Cyber Insurance

Cyber insurance is good for many organizations since it can help them recover from worst-case scenarios. However, receiving a cyber insurance payout shouldn't be the crux of your organization's incident response plan. Cyber insurance does nothing to actually prevent an attack from occurring.

Moreover, securing quality cyber insurance coverage today requires that your organization implement tangible cybersecurity measures. **Ninety-seven percent of respondents to the State of Ransomware 2022 global survey** indicated they made changes to their cyber defenses to better position themselves for insurance coverage, which brings us to our next response option; securing and safeguarding your business.

Response Option 4: Secure + Safeguard

Securing your business against ransomware attacks through safeguards is critical to your incident response plan. You can often prevent the attacks from occurring, mitigate data exposure, avoid serious consideration of paying ransom demands and render a successful attack fruitless for hackers.

What Are Safeguards Against Ransomware Attacks?

Effective safeguards against ransomware attacks include:

Updating & Patching Software

According to Ponemon Institute, four out of 10 data breaches occur because a patch was available but not applied. No doubt your IT department understands how critical updating and patching software across your companywide user base is, but there are only so many hours in the day. Automated patch management is vital to an attack prevention strategy and should be part of your safeguards against ransomware.

Backing Up Data with a Backup & Disaster Recovery (BDR) Solution

Backing up your data is the practice of copying or duplicating your system data so that after a data loss event (like a ransomware attack) occurs, your business can retrieve the lost data. While this is effective at mitigating the effect of a ransomware attack, hackers may leave successfully installed malware dormant for long periods so that data backups also are infected when your company is targeted with a ransomware attack. As a result, you may have no data backup rescue and your company might be forced to capitulate to the ransom demands. Instead, source a backup and disaster recovery (BDR) service that can launch a virtual copy of your files in minutes as a temporary solution that keeps your business running while your server is rebuilt.

Requiring Security Awareness Training

Research suggests that 90 percent of successful breaches are caused by human error. With the right security awareness training program, you can prevent the loss of personal identifying information (PII), intellectual property (IP), money or your company's brand reputation. Phishing is one of the top attack methods used by cybercriminals, and the right security awareness training program can reduce phishing email click rates by 75 percent.

Preparing with Ransomware Tabletop Exercises

A ransomware tabletop exercise is a verbally-simulated attack scenario that is run through between security teams and stakeholders to test an organization's readiness to deliver on a ransomware attack response plan and recovery. The exercise helps key stakeholders and response teams understand the procedure in case of an actual breach and identifies gaps in the organization's cyber incident response plan.

Deploying Security Solutions

Effective security solutions to help your business both prevent and respond to ransomware attacks include:

- **Next-generation Firewalls** — A firewall creates a barrier around your network and monitors traffic in and out of that network based on security rules. A firewall alone can't protect your network, but it's one excellent weapon. That's especially true if your system is protected by next-generation firewall (NGFW) technology, which does everything a traditional firewall does but boosts protection through heuristics (i.e., analysis using rules, estimates and educated guesses for prediction) or artificial intelligence (AI). Next-generation protection also delivers unified threat management (UTM), which includes:
  - Antivirus software
  - Intrusion Detection System & Intrusion Prevention System (IDS/IPS)
  - Deep Packet Inspection (DPI) of Secure Sockets Layer (SSL) traffic
  - Safelisting/blocklisting software

- **Password Management** —Hackers buy and sell lists of the most common passwords and patiently try them through automated program scripts on their intrusion targets. Most businesses know how easy it is to guess short and obvious passwords. Effective passwords are longer, alphanumeric, include at least one special character, and must be changed regularly. But even these passwords can't present an operation problem since users must remember them.

  Password managers enable users to know only one master password translated into a unique encrypted password for each place a password is used. Most password managers use military-grade AES-256 encryption and keep the encrypted passwords in a virtually impenetrable vault. No cybersecurity tool is perfect, but a password manager is as close as you'll get when keeping employee and customer passwords out of the wrong hands.

- **Multi-Factor Authentication (MFA)** — MFA is the access process by which two or more means of authentication must be provided to gain access. The most common method asks users to respond to security questions with previously provided answers, such as mother's maiden name, first car, favorite pet, etc. This approach isn't foolproof since many of those answers might be found within the user's social media content.

  More recent and trustworthy secondary verification methods include codes sent to external devices, such as users' cellphones or wearable devices like Bluetooth-enabled bracelets. The idea here is that, while a data thief might have stolen a password, the hacker probably (though it's a possibility) isn't also in possession of secondary codes or users' phones or other devices receiving it. MFA methods are also being developed to use biometric verification, such as user fingerprints or eye scans.

- **DNS Protection** — Domain Name System (DNS) Protection provides an additional layer of protection between employees and the Internet by blocklisting dangerous sites and filtering out unwanted content. A secure DNS solution can be deployed to protect both in-office and at-home networks and typically provides:
  - Content filtering
  - Malware and phishing blocking
  - Botnet protection
  - Advertisement blocking
  - Typo correction to prevent entry to malicious domains
  - Improved lookup speeds

- **Endpoint Detection & Response (EDR) & Managed Detection & Response (MDR)** —The technology monitors traffic, detects problems and remediates the issue through both a tool and a human-managed security operations center (SOC) at firewall and endpoint locations.

EDR

EDR is perfect for enterprises with existing IT teams. It enables:

- Next-gen antivirus
- Improved systems reliability and performance
- Reduced downtime
- Increased employee productivity

MDR

MDR is ideal for organizations without an IT team. It has all the benefits of EDR plus:

- Advanced threat hunting
- Proactive threat mitigation
- Identifies more threats than antivirus
- Reduced dwell time
- Fully-managed 24/7/365 monitoring

PART 4

Why Outsource Ransomware Protection?

Ultimately, companies have a handful of options to address their ransomware protection needs. They can take it on themselves, outsource it to a qualified managed services provider (MSP) or choose to ignore the threat altogether and pray they don't fall victim to an attack.

Why Should Your Business Outsource Ransomware Protection?

Organizations outsource protection from ransomware instead of handling it in-house for these key reasons:

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 handle complex cybersecurity measures, like ransomware protection, effectively.

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 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 widened in the hyper-specialized realm of cybersecurity and ransomware protection.

What Are the Benefits of Outsourcing Ransomware Protection?

Outsourcing ransomware protection to a managed services provider (MSP) provides your business with:

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 outsourcing.

Reduced Overhead

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

Affordable, Predictable & Scalable Plans

Outsourcing your ransomware protection 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.

Instant Access to Expertise

Outsourcing to an MSP delivers instant access to teams of trained personnel that are experts in protecting your business from cybercrime.

PART 5

What Should You Look for in an MSP?

When seeking the right MSP, find one you can rely on to help you through all of your company's growth phases. That means looking for 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 ransomware protection 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, such as the TPx Connect & Protect bundle.

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 that 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 6

Why Choose TPx for Ransomware 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 ransomware 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.

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, AWS, 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 18,000 clients in 49,000+ locations, we're big enough to get the job done and small enough to be agile.

TPx Is Your One-Stop Shop for Managed Security Services

Ransomware Detection

All backups are scanned for ransomware and when a ransomware footprint is detected, you can roll back your systems and make it as if it never happened.

Next-Generation Firewall (NGFW)

The firewall is the first line of defense in protecting your business 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.

Endpoint Management & 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.

Security Awareness Training

Users are your last line of defense. The more they know, the less prone they are to be 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.

Unified Threat Management (UTM)

TPx ensures UTM features such as web filtering, antivirus, application control, intrusion prevention and VPNs are properly configured, monitored and maintained.

Managed Detection & 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.

Email Security

Protecting your email communications is an important part of any security strategy. Whether it's protecting against email-based cyberattacks like phishing or ensuring that sensitive information doesn't fall into the wrong hands, we can help you navigate the email security challenge

Backup & 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.

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.

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.

Ready to Take Charge of Your Ransomware Protection?

CONTACT US TODAY