The 2025 State of Cybersecurity

FROM THE MANAGED SERVICES EXPERTS AT TPX

Executive Summary

The cybercrime ecosystem is evolving, with cyberattacks becoming more sophisticated, frequent and effective. In response, businesses must educate themselves on the latest cybersecurity trends and consistently update their cybersecurity strategies to combat new cyberthreats.

Cybercriminals are constantly finding new ways to penetrate business networks, steal sensitive information and damage systems, crippling business operations. Businesses must stay a step ahead. With that in mind, let's explore top cybersecurity predictions for 2025.

Key Takeaways

- Artificial intelligence will help fuel and defend against cyberattacks.
- Ransomware continues to be a popular and profitable cyberattack method.
- Businesses and government agencies are combating sophisticated cybercrime.
- Every employee has a responsibility to maintain healthy cybersecurity habits.
- Privacy laws and compliance are becoming concerns for businesses and policymakers.
- Zero-trust cybersecurity frameworks offer reprieve from evolving cyberthreats.

Table of Contents

TREND 1:

Artificial Intelligence (AI) Will Cause & Prevent Cyberattacks

Artificial Intelligence is a Powerful and Valuable Tool — for Businesses and Cybercriminals Alike

Artificial Intelligence isn't new, but dramatic advancements in the last year are expected to continue unabated. Leaps in AI capabilities are beneficial for companies seeking improvements in employee productivity, workflow efficiency and cybersecurity. Unfortunately, AI also is a powerful weapon in the hands of cybercriminals. Businesses must be vigilant in understanding AI's role in cyberattacks and how it can be used to defend against them.

What is AI's role in cyberattacks?

Machine Learning

Cybercriminals use machine learning to optimize phishing scams and false identities to be more convincing and effective in fooling employees. AI-powered phishing emails have a higher success rate than human-made emails.

Deep Fakes

With recent advancements in AI, deep fake technology has become more convincing and easier for cybercriminals to access. In some cases, deep fakes can simulate images, video and text to near-perfect accuracy, making communications almost indistinguishable from reality.

Human Error

Employees unknowingly put themselves and their companies at risk by sharing proprietary or personal information with AI-powered services like ChatGPT. All data shared with third parties must be deliberate and carefully secured, no matter how widely used or trusted they are.

What is AI's role in cyberdefense?

Machine Learning

Cybersecurity tools leverage machine learning to detect deviations in network traffic patterns and send real-time alerts to address and resolve breaches immediately. Additionally, machine learning helps cybersecurity agencies develop databases of cybercriminal information and behavior.

Hidden Threats

AI has the ability to comb through enormous amounts of data and detect hidden threats or suspicious activity based on configurable criteria. Many business networks are already infected by cybercriminals stealing data for a long period of time. AI can help identify and mitigate these breaches.

Cybersecurity Tools

AI is instrumental in powering and enhancing proven cybersecurity tools like antivirus, antimalware, anti-fraud, Intrusion Prevention Systems (IPS), data loss prevention, threat detection, Identity and Access Management (IAM) and risk and compliance management.

TREND 2:

Ransomware Attacks Are Still on the Rise & Remain the Most Common Threat

While the toolkit of cybercriminals has expanded substantially, ransomware continues to be the most common method of attack.

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 most often enters target systems through phishing, drive-by downloading, social media communications, instant messaging, poor patch management, unmonitored environments and weak passwords.

What are the most common types of ransomware?

Crypto

Crypto ransomware is a variant of ransomware that allows cyberattackers to encrypt files stored on target devices to extort money by decrypting the files. The encrypted files are typically deleted if the ransom isn't paid by the deadline.

Locker

Locker ransomware blocks basic computer functions. For example, someone may be denied access to their desktop, mouse and/or keyboard. Victims can then interact with a window containing the ransom demand to make the payment, but cannot interact with anything else.

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. Scareware attacks aim to scare victims with false threats and manipulate them into buying and downloading malware or other malicious code.

Leakware

Leakware is a type of ransomware attack where the cyberattacker threatens to leak sensitive information to the public. Leakware creates an urgency to pay the ransom quickly since knowledge of the attack can’t be controlled by 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 so they can extract ransom not only for decrypting the data but also for threatening to release sensitive information.

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.

What are the impacts of ransomware in numbers?

$353,000

is the Average Cost of a Ransomware Claim for SMBs in 2024

Coalition report finds severity of ransomware attacks increased 68% in first half of 2024.

$265B

in Ransomware Damages by 2031

The damages from ransomware attacks are expected to increase to hundreds of billions of dollars within a decade.

39%

of SMBs

Lost Customer Data to Cyberattack in 2023

According to a 2023 survey of SMB security software buyers, well over a third have lost customer data due to cyberattack.

What are the costs of ransomware?

- Data Theft
- Ransom Payment
- Lost Productivity
- Complete Data Loss
- Downtime
- Paying & Losing Data Anyway
- Reputational Harm
- Data Recovery & Restoration Costs

TREND 3:

The Cybercrime Atlas Will Increase Global Cybersecurity

The Cybercrime Atlas is an international initiative founded by the World Economic Forum (WEF), in partnership with Banco Santander, Fortinet, Microsoft and PayPal, to create a database of all activities of the cybercrime industry.

The database is used by law enforcement worldwide to combat the increasing organization and sophistication of the cybercriminal ecosystem.

Who is a part of the cybercriminal ecosystem?

- Individual Coders and Programmers
- Cybercrime Businesses
- Organized Crime Syndicates
- Distributors and Vendors of Malicious Tools
- Disgruntled Employees and Bad Actors
- Nation-States

What data about cybercriminals is being collected by the Cybercrime Atlas?

- Names
- Addresses
- Bank Account Information
- Ties to Associate Cybercriminals
- Social Media Accounts
- Digital Footprints
- Bulletproof Hosting (BPH) Services
- Anything and Everything

The Cybercrime Atlas is one of many important steps to ensuring international safety in the digital world. The cybercrime empire is getting bigger and craftier every day — businesses and governments across the world have a vital role to play in protecting the global community.

TREND 4:

Board of Directors & Company Leadership Will Gain Cybersecurity Expertise to Make Educated Decisions

Today's boards of directors and company leadership must educate themselves on cybersecurity trends and best practices.

Company leaders are vested in protecting business operations from attack and disruption, and board members have fiduciary oversight. Both parties can also be held personally liable for inaction that leads to a cyber breach.

What cybersecurity challenges does leadership need to understand?

Cybersecurity is a Living Practice

The threatscape is evolving, revealing new vulnerabilities and ways for cybercriminals to attack businesses and their networks. Cybersecurity strategies must constantly respond and adapt to these evolving cyberthreats.

Cybercrime is Organized & Highly Profitable

Cybercrime has become a profitable industry, with hackers, businesses and criminal entities collaborating to identify vulnerabilities and penetrate business networks. As the industry grows, cyberattacks will continue to increase in frequency, sophistication and effectiveness.

Every Industry & Vertical Needs Cybersecurity

In the recent past, only highly-regulated industries, like finance and healthcare, prioritized cybersecurity. Now, organizations of any scale and in every sector are vulnerable to attack, including manufacturing, retail, energy, infrastructure and education.

The Way & Where We Work Have Changed

Remote and hybrid work strategies are now commonplace, dramatically increasing cyber vulnerabilities with networks and workers spanning multiple platforms and locations. The more digitized work processes become, the more avenues for cyberattack become available.

As work situations change and cybercrime gains traction, company leadership and the board of directors must be aware of dangers and understand the importance of continual investment in cybersecurity to make educated decisions concerning cybersecurity strategy.

TREND 5:

Cybersecurity Skills Gap Will Widen With Specialist Turnover

The disparity in knowledge between cybersecurity specialists and other IT staff is already substantial, and will widen as specialists leave the space.

By 2025, nearly half of cybersecurity leaders are expected to change jobs this year, and 25 percent will shift to completely new roles due to stress and overwork. Businesses can mitigate this trend by fostering a culture that supports cybersecurity professionals, or they can get help from a Managed Services Provider (MSP).

MSPs deliver and manage IT solutions and services for businesses. Managed Security Services Providers (MSSPs) are the experts at deploying, integrating, customizing, monitoring and troubleshooting cybersecurity solutions. MSPs aren't subject to the same employee turnover as other businesses because they're specifically built to support and accommodate cybersecurity teams. They have ample internal resources and expertise to help their staff and clients achieve their cybersecurity goals.

How can MSPs support cybersecurity goals for different roles?

IT Teams

Most IT teams are overworked and have too many responsibilities to realistically handle themselves. MSPs can take the load off so IT teams can focus on other critical projects. Additionally, MSPs can often outperform IT teams because they have dedicated resources and regular training that ensure agents are prepared for any cyberincident.

Company Leadership

Company leaders and board directors always seek areas to reduce risk and save money. MSPs can do both by delivering modern, up-to-date cybersecurity solutions at an affordable cost. Additionally, MSPs support productivity and growth by enabling leadership to focus on strategic business initiatives.

General Staff

Everyone has a role in maintaining good cybersecurity practices, including every member of the staff. MSPs are experts at aligning employees with IT teams and educating them on healthy cybersecurity habits. They can deliver training, resources and expertise as needed to ensure employees are adequately prepared for cyberattacks.

Specialist turnover is a significant concern in cybersecurity. All it takes is one breach to cripple an organization, so ensuring complete, effective cybersecurity is paramount. MSPs can help organizations develop cyber resilience – with prevention, detection and recovery strategies for business continuity.

TREND 6:

Data Privacy Standards Will Become a Competitive Advantage for Companies

Modern privacy regulations now cover the majority of consumer data. Businesses that adopt comprehensive data privacy programs and policies in response will surge ahead of competition.

What are the benefits of a data privacy program for businesses?

- ✔ Enhanced Data Security
- ✔ Differentiation from Competition
- ✔ Partner and Client Trust
- ✔ Broader Data Use
- ✔ Improved, Up-to-date Data
- ✔ Compliance with Cybersecurity Regulations

At a minimum, businesses will need to conform to the General Data Protection Regulation (GDPR), the data privacy and security law pushed by the EU that details hundreds of new requirements for businesses across the globe. The GDPR is extensive, and cybersecurity teams must review its requirements in detail, but here are the highlights:

Lawfulness, Fairness & Transparency
Processing must be lawful, fair and transparent to data subjects.

Purpose Limitation
Data processing must be for legitimate purposes specified explicitly to data subjects when collected.

Data Minimization
Data should only be collected and processed as necessary for specified purposes.

Accuracy
Personal data must be accurate and up-to-date.

Storage Limitation
Personally identifying data can only be stored for as long as necessary to fulfill specified purposes.

Integrity & Confidentiality
Processing must be conducted while ensuring appropriate security, integrity and confidentiality.

Accountability
Data controllers are responsible for demonstrating compliance with all specified GDPR data principles.

Comprehensive data privacy programs are critical but can be challenging to develop and implement. MSPs can support cybersecurity teams in developing data privacy programs by delivering expert advice and hands-on management to ensure security and compliance.

TREND 7:

Employee Vigilance & Engagement Will Become More Vital in Securing Organizations

Chief Information Security Officers (CISOs) can't secure an entire business' operations alone. The responsibility of securing a business falls to every individual employee that makes up an organization — from the C-Suite to the IT team to leadership and workers. In fact, most successful attacks today result from human error among the rank and file.

What primary forms of cyberattack target employees?

Phishing

Phishing is a data breach conducted through social engineering. Typically, the hacker disguises its email, phone or other means of communication to appear as if it's coming from a legitimate source. Employees are then tricked into divulging critical information such as passwords or other sensitive data.

Ransomware

Ransomware is a type of malware where cybercriminals hijack victims' systems and data and keep them encrypted until victims pay their ransom. If victims fail to pay, the data is damaged, destroyed, stolen or leaked. Ransomware remains the most common cyberthreat to SMBs.

Domain Spoofing

Domain spoofing is a form of phishing wherein an attacker impersonates a known business or person with a fake website or email domain. These false domain names appear legitimate with nearly identical URLs, so the sites appear correct at a glance. A spoof website or email can mimic a legitimate enterprise or business's logos, navigation menu layouts, and visual design, ultimately tricking people into revealing sensitive information.

Drive-by Downloading

Drive-by download attacks install malicious programs on computers or mobile devices without consent as a hidden, unintentional download. A drive-by download can hijack applications, operating systems (OS) or web browsers that are outdated and contain security flaws. Unlike most other types of cyberattacks, a drive-by doesn't need user input to activate.

How can security awareness training reduce the risk of human error?

Security awareness training is crucial in educating staff so that every member of an organization is in alignment with best cybersecurity practices and policies. High-quality security awareness training programs typically include:

Automated Reporting

Weekly reports are provided to managers and administrators to help companies track progress toward meeting their cybersecurity goals.

Scheduled Training Courses

Each month, team members should be automatically enrolled in self-paced online classes that adhere to National Institute of Standards and Technology (NIST) curriculum guidelines.

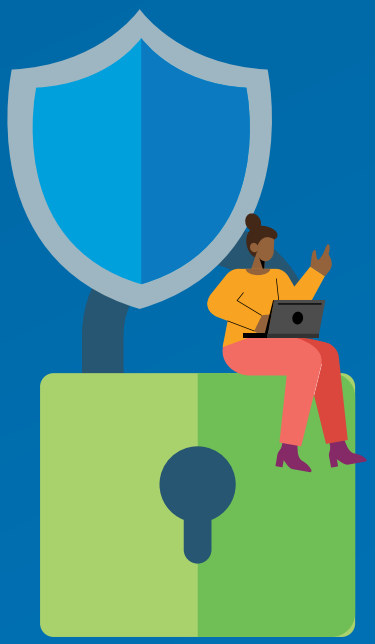
Phishing Simulations

Enrolled learners should receive phishing simulation emails each month. Email templates and randomized delivery times are more effective at testing employees.

TREND 8:

Zero-Trust Cybersecurity Frameworks Will Become More Commonplace

With the increasing accessibility and efficacy of cyberattacks, more companies are implementing zero-trust cybersecurity frameworks. Traditional network security models rely on implicit trust that assumes all uses are inherently trustworthy.



As we all now know, this is not the case. Users can have malicious intent, be negligent or even be infected without knowing it. On top of evolving cyberthreats, shortcomings in the implicit trust model have led businesses to adopt zero-trust cybersecurity frameworks that assume users aren't safe unless proven otherwise. Any traffic, regardless of their location, that enters or leaves a zero-trust network is never trusted until strict identity verification criteria are met. The zero-trust model operates on the principle of "never trust, always verify" to guarantee protection of organizations' networks.

What does zero-trust adoption enable businesses to do?

- Protect Sensitive Data & Critical Systems
- Connect Users to Apps & Services as Needed
- Automatically Quarantine Suspicious Users
- Immediately Respond & Remediate Potential Breaches
- Access Complete Visibility into Network Traffic
- Use Microsegmentation to Silo Compromised Networks

What should businesses consider before adopting zero-trust policies?

Zero-Trust is an Ongoing Process

Since most IT tools and solutions rely on implicit trust models, zero-trust adoption cannot happen immediately. It requires careful thought and strategy combined with follow-through to ensure all gaps in security are covered.

Zero-Trust Doesn't Play Well with Legacy Tech

Zero-trust frameworks and tools don't accommodate legacy tech well, and may require extensive troubleshooting to function properly. Businesses that are overly dependent on legacy tech may need to consider upgrading their equipment before adopting zero-trust frameworks.

Zero-Trust isn't Straightforward

Like many digital transformation strategies, zero-trust isn't a product or tool, but an ongoing strategy that doesn't have clearly defined rights and wrongs or obvious milestones.

Zero-Trust isn't Always Smooth

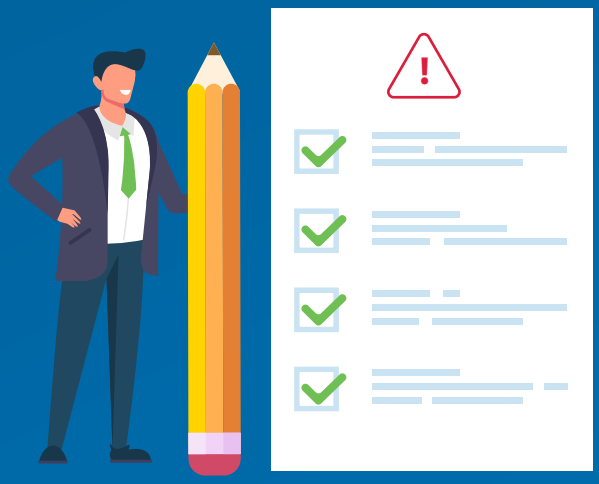
Transitions to zero-trust frameworks require substantial upfront time and resource investment to execute correctly, which will undoubtedly slow regular business processes temporarily. Even after the transition, the extra layers of security can become burdensome and clunky, though effective.

Zero-Trust can be Overkill

There are many ways to secure business operations against cyberattacks, with varying levels of resource investment and effectiveness. While zero-trust frameworks are effective, they may not be necessary for businesses with low digital presence or insufficient resources to implement them fully.

TREND 9:

Risk Management is the Main Driver of Cybersecurity Policies in 2025



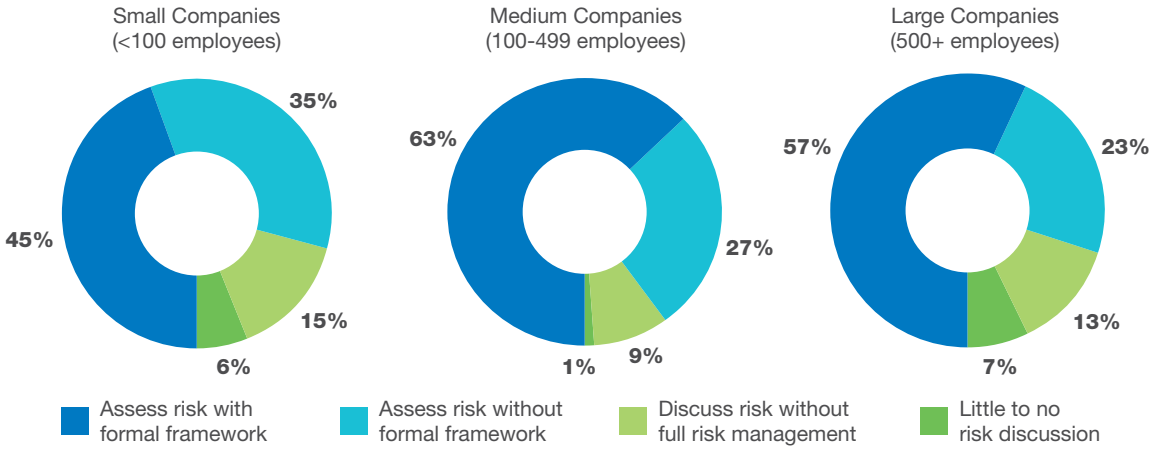
Risk management is becoming the primary method for solving the connection between cybersecurity strategy and business operations. When cybersecurity professionals implement adequate risk management strategies, the link between cybersecurity spending and desired outcomes gets stronger.

Risk management from a cybersecurity standpoint is the process of identifying, assessing and mitigating cyber risks to protect an organization's data and IT infrastructure.

An effective risk management strategy:

- Identifies, analyzes and mitigates all possible cyber risks, not just the common or well-known ones
- Develops proactive strategies to anticipate cyberthreats
- Reduces the impact of potential cyberthreats and company vulnerabilities
- Assigns probabilities to cyber incidents
- Determines potential costs of data breaches
- Proposes effective incident response plans
- Continually assesses the efficacy of cybersecurity strategies

How are businesses of different sizes approaching risk management?



2024 State of Cybersecurity Report, CompTIA

Business leaders and company stakeholders desire, and in many cases need, hard data that tells them the exact impacts of their decisions. While there's no magic method to get 100 percent certainty on business decisions' efficacy and cybersafety, high-quality risk-management strategies can help point leadership in the right direction.

How Can Businesses Benefit from Hiring a Managed Service Provider to Support Security?

Managed services require talent, bandwidth and expertise to monitor and troubleshoot 24/7. Outsourcing services to a managed services provider (MSP) for cybersecurity brings additional value by delivering key benefits, which include:

Instant access to expertise

With MSPs, you get immediate access to teams of trained personnel that are experts in deploying, managing and troubleshooting the security solutions that protect your business from cybercrime.

Reduced overhead costs

MSPs save you time and money by providing valuable resources, including educational materials, training, software and skilled specialists that you would otherwise have to procure and handle internally.

Affordable, predictable & scalable plans

Outsourcing your cybersecurity can be significantly less expensive than developing and deploying cybersecurity technology and talent internally. Moreover, MSP solutions are instantly scalable and offer predictable pricing, giving you control over your IT spending.

More focus on your own business

Cybersecurity is a complex undertaking and an entire business unto itself. You can focus on managing and growing your core business by outsourcing it.

Why Choose TPx?

You have enough business challenges. Partnering with TPx provides the support it needs so you can focus on core business goals. At TPx, we have the products, services, experience and certifications to keep your network and applications running smoothly and safely.

Our mission is being the easiest MSP to do business with	We solve the biggest IT issues – cybersecurity, connectivity, and collaboration – under one umbrella	We have 120+ certifications across 60+ competencies, like CompTIA, Cisco, Fortinet, Microsoft, SMC and more
We offer HIPAA, PCI-DSS, and SOC 2 Compliant solutions	We provide enterprise-class, 24/7 support	We offer different service levels and highly customizable solutions
We have a national footprint, with multi-site, multi-carrier, partner coverage	With thousands of customers nationwide, we're big enough to get the job done and small enough to be agile	We have various dedicated teams to ensure service excellence
We continuously invest in automation, self-service innovation, and back-office transformation	We are committed to providing the most densely monitored service delivery platform in the industry	We understand and embrace the criticality of our customers' performance analytics

TPx is Your One-Stop Shop for Managed Security Services

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.

Security Awareness Training

Users are your last 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.

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 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.

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.

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.

Managed Inbox Detection and Response (IDR)

Help users make better email security decisions with Managed IDR. This powerful user security solution provides professional evaluation and handling of suspicious emails reported by users — right from the inbox. Put your employees in the driver's seat and make them be part of your business security.

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.

Backup and Disaster Recovery

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.

Ransomware Detection

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

Interested in securing your business against growing cyberthreats?

CONTACT US TODAY