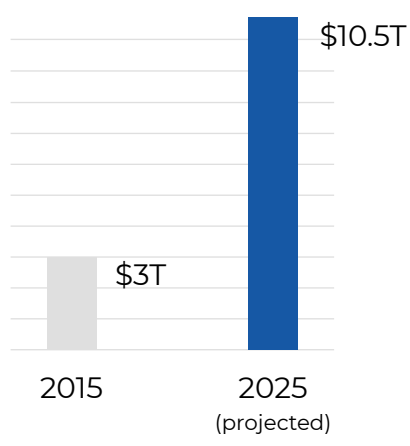
Nationwide®

Staying Resilient Against the Latest Cyberthreats

Amid evolving threat vectors, rising attacker sophistication and advancing technology solutions, the current cybersecurity landscape has presented challenges for businesses of all sizes and sectors. In fact, the cost of cybercrime is projected to reach **$10.5 trillion by the end of 2025**, more than tripling from $3 trillion in 2015 and making businesses increasingly vulnerable to related losses.[1] With this in mind, it's clear that your business can't afford to ignore cyber risk management.

By upholding a strong cybersecurity posture, you can minimize your company's digital exposures and safeguard your operations against potential losses.



Cost of cybercrime

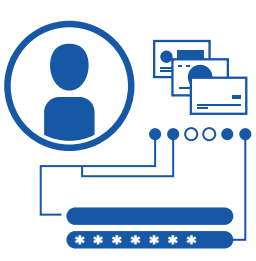
Read on for an overview of **common threat vectors** and **best practices** for navigating this ever-changing cybersecurity environment.

Common Threat Vectors

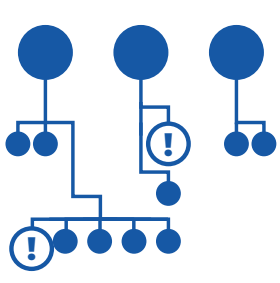
In the realm of cybersecurity, a threat vector refers to any avenue or method a cybercriminal can leverage to infiltrate a target's network, system or device. In other words, threat vectors serve as pathways for cybercriminals to conduct their attacks. Here are some common threat vectors:[2]

Social engineering and phishing scams—Social engineering entails cybercriminals utilizing deceptive communication and other manipulation tactics to lure targets into sharing sensitive information or providing unauthorized access to their systems. One of the most prevalent social engineering methods is phishing. A phishing scam consists of a cybercriminal sending deceitful messages—via email, text message or phone call—to trick their target into supplying confidential data or downloading malicious software.

Malware and ransomware attacks—A malware attack involves a cybercriminal launching harmful code or a malicious program with the intent of damaging or shutting down their target's network. One example of malware is ransomware, which cybercriminals use to demand payment in exchange for the restoration of the target's network (as well as any data stored on it).



Identity-based attacks—An identity-based attack pertains to a cybercriminal stealing their target's personal login credentials and using this information to impersonate them across their network. A cybercriminal may leverage an identity-based attack to remain undetected in their target's network while conducting fraudulent fund transfers or accessing sensitive data.



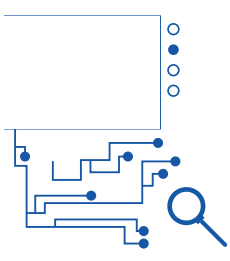
Insider threats—Although many cyber incidents stem from external attackers, some could arise from insider threats—namely, current or past employees. These employees may exploit their employers by using their access to confidential systems or information to steal data or help cybercriminals deploy attacks.

Distributed denial-of-service (DDoS) attacks—During a DDoS attack, cybercriminals aim to disrupt or fully halt a target's online service or system by overwhelming it with a flood of fake traffic. This is achieved by sending a surge of requests that exceed the capacity of the service or system, forcing it to shut down. These attacks usually utilize large groups of internet-connected devices (also called botnets) to send an excess of requests.

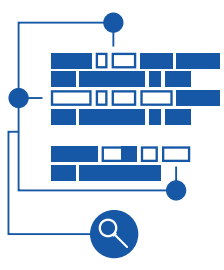
Key Controls to Better Your Cybersecurity Posture

It is important to implement control measures to protect your business against various threat vectors and uphold a solid cybersecurity posture. Consider the following cybersecurity control measures.

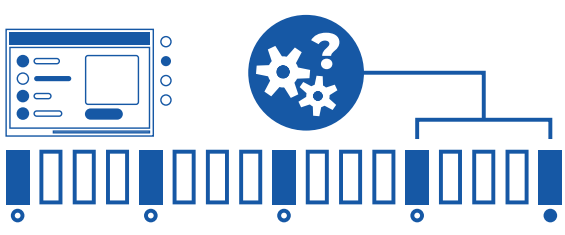
Multifactor authentication (MFA)—MFA encompasses a layered approach to safeguarding networks and systems in which users are required to provide a combination of two or more credentials (e.g., a password and a security question) to confirm their identity before gaining access. This extra login hurdle can help prevent cybercriminals from easily unlocking and infiltrating accounts.



Endpoint detection and response (EDR)—EDR solutions can provide continuous monitoring capabilities and enhanced overall visibility into network and system activity, allowing for improved threat identification and remediation amid cyber incidents. Key features of EDR solutions include data search and investigation triage; contextualized threat hunting; and malicious activity detection, validation and containment.



Patch management—Workplace technology is most effective and secure when it receives regular software updates (also called patches). The best way to stay on track with these updates is through patch management. This is the process of applying patches across systems and networks, which can, in turn, fix bugs, reduce digital vulnerabilities and improve performance. Patch management can be carried out by senior leadership, IT experts or automated tools.



End-of-life (EOL) software management—When software reaches the end of its life, manufacturers discontinue technical support and upgrades for this technology. As a result, EOL software generally contains additional vulnerabilities that can be exploited in cyberattacks. To avoid these exposures, it's imperative to implement life cycle management plans that outline protocols for introducing new technology, phasing out unsupported software and planning for replacements when necessary.

Employee education and awareness—Employees are widely considered the first line of defense against cyberattacks. After all, cybercriminals often target employees in phishing scams and malware incidents. Compounding concerns, the vast majority (95%) of cyberattacks stem from human error.[3] That's why routine employee training is essential. This training should educate employees on the latest cyberthreats and how to properly mitigate and respond to them.

It's evident that today's dynamic digital landscape requires a **proactive cybersecurity posture** and **innovative risk management controls**. For more information on Nationwide's cybersecurity solutions and insurance offerings, click here.

1 https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/
2 https://www.fortinet.com/resources/cyberglossary/attack-vector
3 https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf

Nationwide®