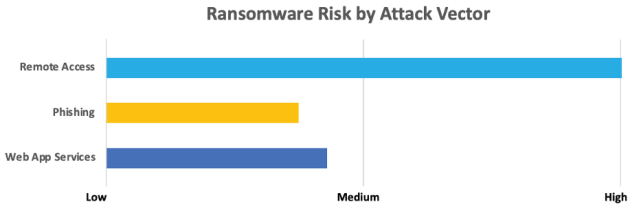
Ransomware Readiness Evaluation

Ransomware has become the number one cybersecurity risk in the world. According to the U.S. Department of Justice, there have been an average of 4,000 ransomware attacks every day since 2016. Cybercriminals have turned malware and hacking into a robust, money-driven industry complete with commercial-grade exploit kits widely available to those who seek them. A haphazard approach to online security will not suffice. New cyberthreats emerge every minute and businesses need to protect themselves against costly security incidents.

Ransomware is especially dangerous for small and medium businesses, many of whom do not have the resources in place to fend off these attacks. With a Ransomware Evaluation, you can quickly understand your exposure to ransomware attacks — and how to protect your business. By partnering with TPx's cybersecurity experts, your business can quickly gain rich insights into where you have the most exposure as well as mitigation techniques to deploy against ransomware.



A cybersecurity expert from TPx will walk you through a series of questions that will evaluate your ability to defend against and respond to a ransomware attack. By focusing on the three primary ransomware attack vectors — phishing, remote access, and web applications — we are able to quickly identify weaknesses and provide you with actionable information.

This complementary 30-minute ransomware evaluation will help you learn:

- Whether your business is properly protected against malicious web content
- If your network visibility is sufficient
- If your staff knows how to avoid security risks in email and other attack vectors
- If your backup strategy will allow your organization to recover quickly from an attack and minimize downtime

The resulting report will present an evaluation of current readiness, along with customized recommendations on what aspects of your security footprint can be improved to help you withstand ransomware attacks.