Ransomware Readiness Assessment

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 cannot keep up. 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 to fend off these attacks. By partnering with TPx's cybersecurity experts, your business can quickly gain rich insights into where you have the most exposure in your business and how you can mitigate yourself against ransomware attacks. Our Ransomware Readiness Assessment can help you identify your organization's weaknesses, and ultimately help save your business money and reputation by giving you a stronger security posture.

Prepare and Respond

- Are my network entry points effectively secured?
- Are my systems properly patched against vulnerabilities?
- Do I have the visibility I need into who is on my network?
- Does my organization's staff know how to avoid security risks in email and other attack vectors?
- Does my backup strategy allow me to recover quickly and minimize downtime?
- Is my incident response plan detailed enough to enable my team to respond effectively in the event of an attack?

Quickly understand your exposure to ransomware attacks — and how to protect yourself. All in a matter of days.

Overview

TPx's Ransomware Readiness Assessment (RRA) is founded on industry standards developed by the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA). This assessment focuses on the aspects of cybersecurity that have the highest value in defending your organization against ransomware attacks. As a subset of TPx's full-blown Security Program Gap Assessment, the RRA provides a cost-effective way for small and medium businesses to understand the risk of ransomware to their organization. It also provides an actionable roadmap that enables these organizations to quickly address their areas of highest exposure, to reduce their ransomware risk.

TPx will assess the security policies and practices surrounding the most common attack vectors that cybercriminals use in ransomware attacks: social engineering, email-based attacks, compromised credentials, and external-facing software vulnerabilities. Through the use of both administrative and technical controls, organizations can reduce their attack surface and encourage cybercriminals to move on to easier targets.

Defense is only part of the story, however. Risk can be reduced, but it can never be eliminated completely. To practice truly effective security, you must be well-prepared to act in the event of a breach. Time is critical during an attack, and it is imperative that your procedures & systems are thoroughly defined and tested. TPx will provide expert advice on the aspects of your incident response plan, your data backup and storage policies, and your ability to recover to a working state with a minimum of downtime and operational impact.

Readiness Assessment Activities

The assessment will focus on the following areas:

- Network Perimeter Monitoring
- Application Integrity and Allowlists
- Web Browser Management and DNS Filtering
- Phishing Prevention and Awareness
- Asset Management
- Risk Management
- Patch and Update Management
- User and Access Management
- Data Backups
- Incident Response
- Manual or Independent Operations

Through document review, interviews, and policy analysis, TPx will conduct a baseline review of your organization's exposure to ransomware and its effect on your business in the event of a successful attack.

Upon completion of the assessment, TPx will provide two reports: an Executive Summary and a prioritized list of specific actions you can take to reduce your exposure to ransomware attacks. In less than a week, you and your team will have the information you need to tighten your security and reduce the risks you face due to the most widespread method of cyberattacks today.

There were 65,000 successful ransomware attacks in 2020 — one every 8 minutes

Recorded Future