Cybersecurity Gap Assessment

TPx is a leader in cybersecurity for small and medium businesses and public-sector organizations. Our depth of expertise enables us to offer standards-based security consulting services developed from our experiences in solving strategic and operational challenges for customers.

TPx consultants are subject matter experts in their field and thought leaders in security. All of our offerings are based on best practices derived from Information Security Standards (CISSP Domains, NIST, ISO 27000 series, etc.) and our extensive experience deploying, architecting, operating, and securing environments nationwide.

Any successful security strategy must be disciplined, thorough, and quantifiable. With an ever-expanding network perimeter, a continuously evolving threat landscape, users demanding access to a myriad of services (both internal and external), and increased scrutiny on risk, privacy, and compliance, a structured approach to organizational security is more important than ever.

TPX's Cybersecurity Gap Assessment enables customers to evaluate their security posture in a methodical way, comparing it against industry standards and best practices, to generate a prioritized list of actions to lower organization risk while maximizing the impact of their limited security budgets.

Get answers to these questions…

- Do I use the best information security practices to protect my business and control my risks?
- Are my systems and data vulnerable to ransomware and other security threats?
- Am I protected against unauthorized access?
- If I do suffer a data breach, am I prepared to recover as quickly, safely, and cost-effectively as possible?
- What most important weaknesses should I fix first?
- What are the efforts needed to improve my current level of protection?

Our Cybersecurity Gap Assessment is founded on common industry standards such as NIST 800-171 as well as current best practices.

Overview

TPx's Cybersecurity Gap Assessment is founded on industry standards such as NIST 800-171 and current best practices. The assessment is divided into two main components:

- **Security Strategy** TPx will assess the security policies, standards and procedures as well as the security management processes, and roles and responsibilities related to your information security.
- **Operational Security** TPx will assess the technical security measures implemented within your network infrastructure.

Your information security posture is assessed based on a set of categorizations (e.g. access controls and network protections). The categorizations covered during the gap assessment focus on areas of cybersecurity that have the highest likelihood of incidents and breaches for your organization.

Gap Assessment Activities

The main objective of the gap assessment is to assess the security maturity of your organization and prioritize security risks for your leadership team. The areas of focus can range from information security governance to cybersecurity infrastructure and capabilities.

Information Security Organization Accountability Information security accountability and compliance, including strategic roles and responsibilities and information security policy

Human Resource Security Management Human resource security management, including information security in hiring, awareness, education and training, and change and termination

Identity and Access Management User access management and password policies

Information Security Incident Management Information security incident management preparation, identification and assessment, response and continuity, and testing

Change Management Change management including planning, building, testing, and implementation

Network Segmentation, Isolation and Protection Network security architecture including segmentation, isolation, firewalls, and threat management

Security Services Core security services including onboarding/offboarding, account and access management, and backup services

Server and Workstations Security Endpoint security including access controls, technical vulnerability management and protections

Email Service Security Email security including architecture, access controls, technical vulnerability management and protections

Reporting

Upon completion, TPx will provide two reports: an Executive Summary and a detailed Best Practices report. They speak to two different levels of resources: the leadership and the security practitioner. A detailed recommendations report will be provided and validated with your personnel in order to present the results and observations related to your security posture. In addition, you will receive recommendations for your top three priorities based on your business, your sensitive data, your exposure landscape, and the CIS top twenty controls.

43% of attacks are aimed at small and medium-sized businesses, but only 14% are prepared to defend themselves.

Accenture 2019 Cost of Cybercrime report