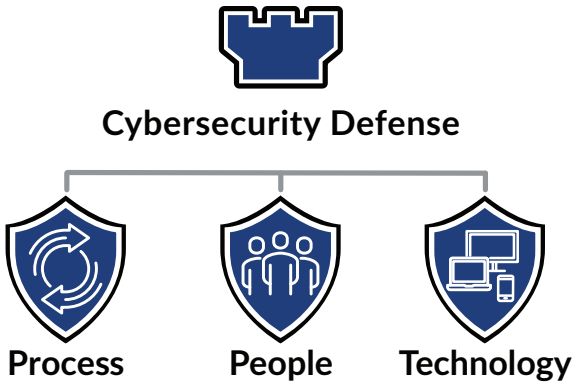
plante moran | Audit. Tax. Consulting. Wealth Management.

Fortify Your Cyber Defenses

In today's increasingly connected world, your customers, prospects, and even future staff expect your organization to have a fortified digital presence. As your technologies continue to grow and expand, so does your exposure to cyberthreats. It's no longer enough to simply protect your data and systems, you also need to build a resilient cyber program for unforeseen cyberattacks.

Establishing a comprehensive, organization-wide cybersecurity program centered around defense needs to be a top priority for your business. Cybersecurity threats don't just come from sophisticated hackers — people with very little technical knowledge and know-how have the capability to threaten your organization. To ensure your business is protected from cyberthreats, it's crucial to build a flexible cybersecurity program that considers control baselines and standards, threat detection and response activities, and clearly defined responsibilities across the organization.



Our team of cybersecurity experts has established a cyber defense methodology based on decades of experience providing cybersecurity and technology audit services for clients. Our overall cybersecurity framework uses a risk-based approach to map controls covering the confidentiality, integrity, and availability of systems and data, while complying with customer expectations and the numerous security and privacy regulations imposed upon organizations today. By focusing on three major considerations for effective cybersecurity implementations — **process, people, and technology** — our services are designed to help organizations implement and maintain an effective cybersecurity resilience program. We assist our clients with forward-looking strategies to protect against unknown future threats, rather than threats of the past. Fortifying your cyber defenses is a rigorous, ongoing effort; our approach will help you structure, simplify, and standardize the process.

Process

As threats constantly evolve, your processes to detect and resolve new threats must evolve as well. Patches to operating systems and third-party applications, for example, must be rigorously maintained to protect against the latest vulnerabilities. Your recovery planning process, too, needs to evolve to adequately address increased new threats, such as ransomware.

People

End-users are your first line of defense from attacks. With the best intentions to provide fast service, employees may fall for phishing emails. This enables hackers — unbeknownst to you — to install malicious software, request credentials such as passwords and security questions and answers, and initiate wire transfers.

Technology

While IT supports and facilitates your operations, it also must secure sensitive data and information. Strong controls are critical, whether you outsource or manage your IT organization in-house. You must ensure, not assume, vendor processes and controls align with the latest security protocols and your organization's and stakeholders' expectations.

plante moran | Audit. Tax. Consulting. Wealth Management.

A future-focused approach is essential

Many organizations use past incidents — rather than future threats and scenarios — to build their cybersecurity program. Our team of over 100 dedicated cybersecurity consultants are future-focused and stay at the forefront of industry trends and regulations to help you build a cyber defense strategy that can manage and mitigate the next big threat.

Our cybersecurity capabilities include:

CYBER ASSESSMENT

- IT audits
- Risk assessments
- ERP security & controls
- Cloud security
- User access reviews
- Privacy compliance
  - HIPAA, GLBA, GDPR, CCPA
- General controls review
  - Access, physical, operational controls
- Application controls assessment
  - SAP, Oracle, PeopleSoft, QAD, Plex, Epicor

CYBER ADVISORY

- Seven-point cybersecurity assessment
- Cyber strategy
- Frameworks
- NIST, CIS Top 20
- Cyber PMO
- Risk analysis
- Business continuity plans (BCPs), disaster recovery plans (DRPs)
- Cyber incident response planning
- CyberKPi & dashboards

CYBER ASSURANCE

- Readiness assessments
  - SOC 1, SOC 2, SOC 3
  - SOC for cybersecurity
  - SOC for supply chain
- PCI DSS certification
- HITRUST certification
- ISO27001 Security Standards certification

CYBER SOLUTIONS

- Solution selection & integration
- Custom dashboards
- GRC tools
- Identity management
- Mobile/device management
- Threat intelligence
- End-point security
- IDS/IPS
- SIEM tools

CYBER LAB

- Physical lab environment
- Network security assessments
- Vulnerability scans
- Web/mobile security
- Malware testing
- Red/blue team exercises

CYBER FORENSICS

- Comprehensive six-step incident management process
- Prepare summary report and detailed findings report

CS.SS23.051322

Furney Brown
furney.brown@plantemoran.com
248-223-3396

plantemoran.com/cybersecurity