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

Cybersecurity

Are you protected?

Contents

Introduction 1

Our methodology 2

Services 4

Tailored approach 6

Our value proposition 12

CYBERSECURITY

Introduction.

Cybersecurity is like a rollercoaster ride for many organizations today.

At times, they're upside down, in the dark, or not feeling secure. Even though there are controls in place, they're still nervous. By focusing on three major considerations for effective cybersecurity implementations — people, process, and technology — our services are designed to help clients manage the rollercoaster ride of cybersecurity risks, and to implement and maintain effective controls during the ups and downs of the cybersecurity rollercoaster.

Our cybersecurity practice at a glance

20+
years of experience providing cybersecurity consulting services

50+
staff dedicated to providing solutions to your unique security needs

1 of only 32
nationally approved HITRUST assessors also providing PCI and ISO services

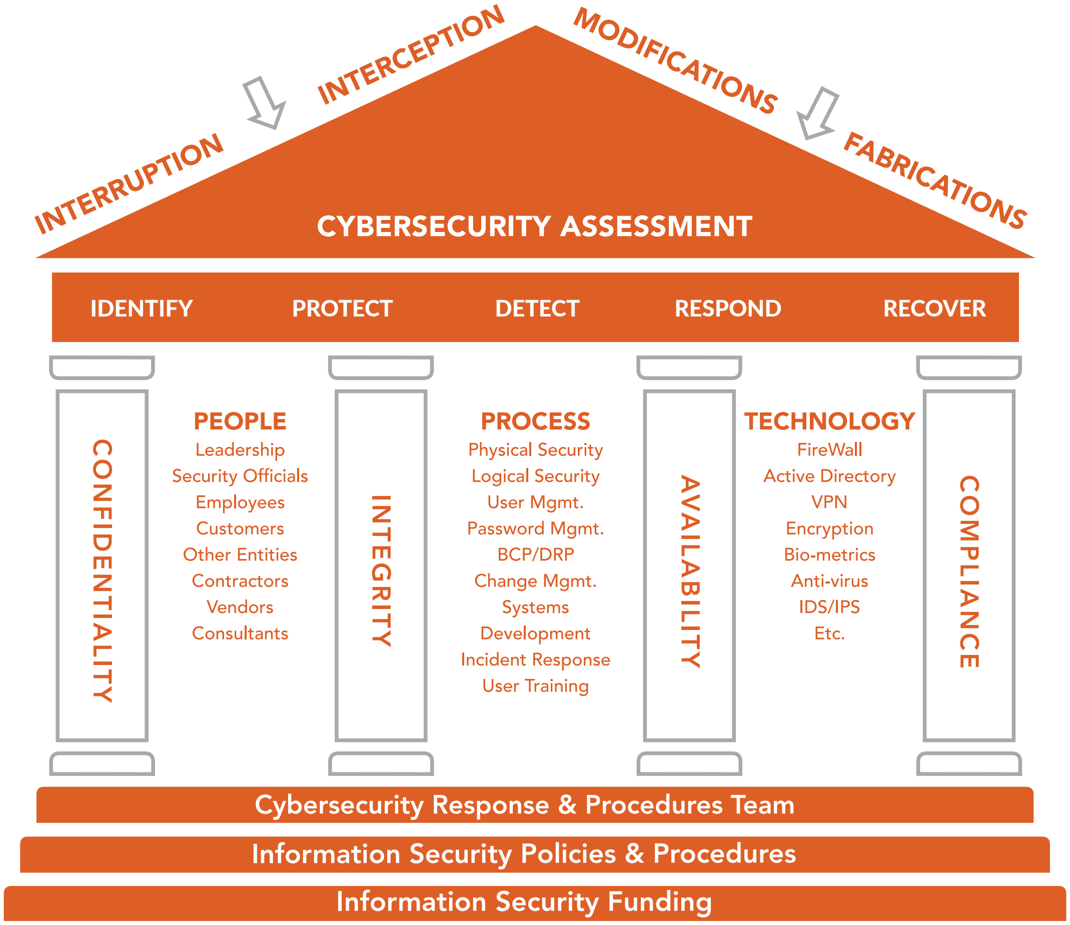
Our team's certifications

CISA	Certified Information Systems Auditor
CISSP	Certified Information Systems Security Professional
QSA	Qualified Security Assessor
CPA	Certified Public Accountant
CEH	Certified Ethical Hacker
CCNA	Cisco Certified Network Associate
CFE	Certified Fraud Examiner
CRISC	Certified in Risk and Information Systems Control
CISM	Certified Information Security Manager
CCSK	Certificate of Cloud Security Knowledge

CYBERSECURITY

Our methodology.

Over the years, we've developed our house of security methodology that addresses everything from risk assessment, prevention, and recovery, to the full development of response procedures, security policies, and identifying information security funding.



Based on this custom methodology and approach, we've developed a number of services to help you:

UNDERSTAND YOUR RISK EXPOSURE TO CYBERSECURITY EVENTS.

IDENTIFY CONTROLS IMPLEMENTED TO MITIGATE THIS EXPOSURE.

ASSESS THE CONTROL DESIGN AND EFFECTIVENESS TO IDENTIFY GAPS OR RESIDUAL RISK.

FACILITATE IMPLEMENTATION OF TAILORED CYBERSECURITY FRAMEWORK AND CONTROL ENHANCEMENTS RECOMMENDATIONS.

BUILD TRAINING AND REPORTING PROGRAMS TO ENHANCE BOTH USER AND EXECUTIVE MANAGEMENT'S UNDERSTANDING OF CONTROL ACTIVITIES AND THE EFFECTIVENESS OF THEIR IMPLEMENTATIONS.

Services

An in-depth look at our capabilities

CYBERSECURITY

Capabilities.

Cyber governance

- NIST Cybersecurity Standards
- COSO/COBIT Standards
- SANs Top 20 Security Controls
- Security awareness
- Cyber incident response planning
- BCP/DRP
- 7-point cyber assessment

IT audits

- General controls review (access, physical, operational controls)
- Application controls assessment (SAP, Oracle, PeopleSoft, QAD, Plex, Epicor)
- User access reviews
- ERP security & controls
- Pre/Post-implementation controls review

Security compliance

- Sarbanes-Oxley (SOX)
- PCI DSS
- HITRUST
- ISO27001 Security Standards
- Financial services regulations (FFIEC, BSA, NACHA, etc.)
- Privacy regulations (HIPAA/HITECH, GLBA, FERPA, GDPR, etc.)

Cyber risk assessments

- Data & application mapping
- Vendor management
- Threat analysis
- Controls mapping
- Maturity models
- Risk-based IT audit planning
- Cybersecurity program

Attack & pen

- External penetration testing
- Infrastructure security assessment
- Vulnerability assessment services
- Social engineering tests
- Web application security
- Database security
- Wireless security
- Virtualization security
- Cloud computing security
- Mobile device security

SOC Examinations

- Readiness assessment
- SOC 1
- SOC 2
- SOC 3
- SOC for cybersecurity
- Privacy reviews

Tailored approach

How can we help you?

CYBER RISK & GOVERNANCE

Do you understand the risks to your business?

Cybersecurity is evolving with multiple attack vectors, making it difficult for organizations to manage the risks effectively. Organizations are also confused as to what standard or framework to use — i.e. NIST Cybersecurity, COSO/COBIT, CIS Critical Security Controls, ISO 270001, etc. Complicating matters further are the various security and privacy regulations.

How we help

We will identify a risk assessment methodology that addresses the risks to your organization. Our team will further help integrate the applicable governance models, including NIST and ISO 27001.

We can help you develop a risk governance framework and a cybersecurity roadmap that is manageable and sustainable for your organization and culture.

Our services include:

- Cyber risk assessment
- NIST cybersecurity assessment
- SANS CIS Critical
- Security Controls
- Cyber incident response planning
- Business continuity/disaster recovery planning
- Security awareness training

We can help you develop a risk governance framework and a cybersecurity roadmap that is manageable and sustainable for your organization and culture.

ATTACK & PEN

Are you vulnerable to a cybersecurity attack?

No business is beyond the reach of hackers regardless of size, industry, or location. Every day, we hear about new cybersecurity hacking incidents. These attacks can originate from external hackers or, at times, even your own employees.

As technology evolves, new vulnerabilities are identified and security gaps keep widening. Most organizations become a target because of what they don't do, or simply what they don't know.

How we help

Using current threat intelligence, our cybersecurity specialists will work with you to identify specific targets and launch controlled attacks from common footholds including network perimeter, remote access, unauthenticated and authenticated internal network access, enterprise applications, and physical access.

Our attack and pen reviews are performed using our threat emulation methodology, which is based on various penetration testing standards. This methodology utilizes multiple threat scenarios to simulate a real hacking incident. These threats range from external, non-knowledgeable "drive-by" attacks to targeted insiders.

Our attack and pen reviews are performed using our threat emulation methodology, which is based on various penetration testing standards.

Our services include:

- Penetration testing (external & internal)
- Vulnerability analysis (external & internal)
- Social engineering (phishing, phone calls, impersonation, etc.)
- Web application testing
- Internal network security assessment
- Wireless security assessment

IT AUDITS

Do your controls address confidentiality, integrity, availability, and compliance requirements?

Many organizations rely solely on their IT department to manage controls over network infrastructure and business applications. Others rely heavily on technology to secure data. Granting access can be complex and confusing to many organizations, and frequently results in unauthorized access. Additionally, organizations have the challenge of complying with various customer and legal requirements.

How we help

By focusing on people, process, and technology, our services provide clients with a greater understanding of threats and controls.

Our IT audits focus on general controls, with the potential for additional phases to include application and user access reviews. By assessing the information security posture of your organization, we're able to recommend areas for improvement, as well as provide you comfort in having an independent source review the maturity of the existing control environment.

Our services include:

- General controls review (access, physical, operational)
- Application controls assessment (access, change management, backups)
- User access reviews
- Business process controls & security
- Pre/post-implementation controls review

Our IT audits focus on general controls, with the potential for additional phases to include application and user access reviews.

SOC EXAMINATIONS

How do you provide assurance regarding your internal control environment?

AICPA
SOC
EXAMINATIONS

Recent cybersecurity incidents and regulations are forcing businesses that outsource work to demand more controls information and assurance from their service providers.

Without a current service auditor's report, you may have to entertain multiple audit requests from customers and their respective auditors. This can place a strain on your resources. A service auditor's report ensures that all user organizations and their auditors have access to the same information to satisfy auditor requirements.

How we help

Our team will deliver a comprehensive, timely, independent service auditor's report regarding your control design and operating effectiveness.

We'll identify which SOC report best fits your needs based on the services you provide. From there, we'll perform readiness assessments to identify control weaknesses and develop recommendations for remediation prior to undergoing the formal SOC assessment.

We'll identify which SOC report best fits your needs based on the services you provide.

Our services include:

- Readiness assessment
- SOC 1 (Type I, Type II)
- SOC 2 (Type I, Type II)
- SOC 2+ additional subject matter
- SOC 3
- SOC for cybersecurity
- Privacy reviews

SECURITY COMPLIANCE

Are you in compliance with privacy and security regulations?

Organizations are faced with a number of privacy and security regulations. You may face compliance with various state and federal regulations. If you're an SEC-registered company, you face additional Sarbanes-Oxley (SOX) 404 regulations. If you accept credit card payments, you're also required to meet PCI-DSS compliance. In the event of a cybersecurity incident where there is a loss of private information, organizations can face fines, legal fees, and, perhaps most detrimental, reputational damages.

How we help

We understand the regulations you face and will help map your control environment against each applicable requirement. We'll provide a concise overview with dashboards of your compliance status.

Additionally, our firm is a Qualified Security Assessor (QSA) company and can certify your organization's compliance with PCI data security standards. We're also a CSF assessor for HITRUST and can certify your organization's readiness and compliance with the HITRUST common security framework.

Our services include:

- PCI DSS
- HITRUST
- ISO 27001 review
- Sarbanes-Oxley Act (Section 404)
- Japanese SOX (J-SOX)
- Privacy regulations (HIPAA/HITECH, GLBA, FERPA, GDPR, etc.)
- Financial services regulations (FFIEC, BSA, NACHA, etc.)

> We understand the regulations you face and will help map your control environment against each applicable requirement.

Custom solutions

to achieve your unique goals

CYBERSECURITY

Value proposition.

Deep industry expertise

Our cybersecurity professionals are organized by industry, resulting in a team that knows the inherent risks you face and can provide deep subject-matter expertise.

We'll help you meet your business goals and objectives by discussing current trends and metrics, regulatory requirements, and on-target solutions.

Client focus

We have an award-winning culture based on one simple premise: We care. The result? Seamless service from talented staff who love what they do.

- 96% of our clients would recommend Plante Moran to others.
- 20 consecutive years named to Fortune magazine's list of "100 Best Companies to Work For" in America.

Efficient approach

Our colleague partnering model, with at least two partners on your engagement team, allows us to provide you with more diverse, expert, and well-rounded thinking to solve increasingly difficult day-to-day challenges and complex issues.

Our unique "one-firm" firm philosophy and structure mean clients receive the collective power of the firm, regardless of location or geography.

We ensure no unwanted surprises with upfront planning, regular communications, and our inclusion of a standards team member on every engagement team.

Flexible, proactive solutions

Our comprehensive approach will provide you with tailored solutions based on a strong understanding of your organization, strategies, and unique risks.

Our forward-thinking perspective will keep you abreast of upcoming developments.

Our professionals know that no two companies are alike; thus, we provide customized solutions that are flexible to your specific needs.

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

Please contact us with any questions.

Raj Patel
Partner
248-223-3428
raj.patel@plantemoran.com

Sarah Pavelek
Partner
248-223-3891
sarah.pavelek@plantemoran.com

Joe Oleksak
Partner
847-628-8860
joe.oleksak@plantemoran.com

Angela Appleby
Partner
303-846-3332
angela.appleby@plantemoran.com

Tim Bowling
Partner
312-980-2927
tim.bowling@plantemoran.com

Stay in the know: plantemoran.com/subscribe

plantemoran.com