{ Are you protected? }

Overview of Cybersecurity Services

plante moran

Why Plante Moran

is built on thousands of success stories.

CLIENT FOCUS
The confidence that the client's needs are put ahead of the firm's by a professional team that cares as much about the client's business as the client does.

DEEP INDUSTRY EXPERTISE
Deep audit, tax, and consulting expertise from professionals who specialize in the client's industry, so that the client receives the benefit of timely industry trends and metrics, on-target solutions to help meet the client's business and personal goals, and tax-saving strategies.

NO SURPRISES
The security of knowing there will be no unwanted surprises because of upfront planning, regular communications, and our inclusion of a standards team member on the engagement team.

HIGH VALUE ON RELATIONSHIPS
A service delivery promise that guarantees the client feels listened to, informed, and valued by a firm that is known for its caring culture.

INTEGRATED SERVICES
A comprehensive approach brings together audit, tax, and consulting, creating efficiencies and strong solutions in one integrated delivery system.
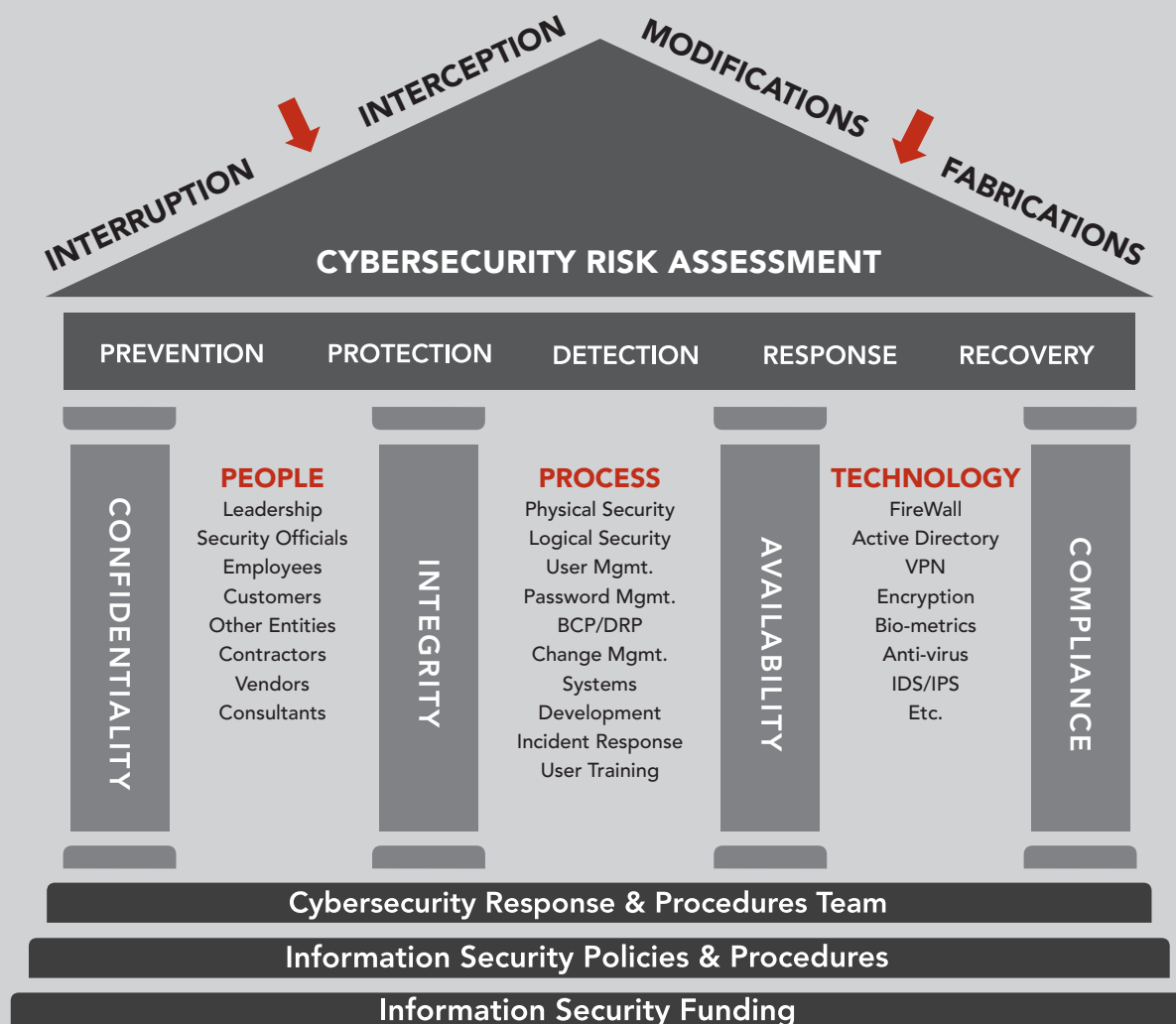
{ Table of contents. }

Cybersecurity Program

A critical component for companies competing in today's market is to leverage information technology systems to maximize production efficiency while effectively controlling and securing their informational assets. The technology landscape is rapidly changing with the introduction of cloud computing, mobile technology, open source development, software-as-a-solution, social media, etc. As a result, companies need to evolve their security and control frameworks to meet the changing landscape.

To assist our clients in defining appropriate security practices or assessing existing control structures, Plante Moran has developed a range of cybersecurity services to assist our clients' obligations to protect the confidentiality, availability, and integrity of their information and IT assets, as well as compliance with various security and privacy regulations.

Our services take into account various regulatory requirements, including the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), the Payment Card Industry Data Security Standard (PCI DSS), and Sarbanes-Oxley (SOX 404), and map out a service delivery approach that reduces the overlap between these regulatory requirements and the various cybersecurity needs of our clients. It is also derived from the National Institute of Standards and Technology (NIST) cybersecurity framework, Control Objectives for Information and Related Technology (COBIT), and International Organization for Standardization (ISO 27001 series) of cybersecurity control standards. These security control standards are a guideline for organizations that have a desire to focus on information and cybersecurity.

CYBERSECURITY RISK ASSESSMENT

INTERRUPTION · INTERCEPTION · MODIFICATIONS · FABRICATIONS

| PREVENTION | PROTECTION | DETECTION | RESPONSE | RECOVERY |

CONFIDENTIALITY

PEOPLE
Leadership
Security Officials
Employees
Customers
Other Entities
Contractors
Vendors
Consultants

INTEGRITY

PROCESS
Physical Security
Logical Security
User Mgmt.
Password Mgmt.
BCP/DRP
Change Mgmt.
Systems
Development
Incident Response
User Training

AVAILABILITY

TECHNOLOGY
FireWall
Active Directory
VPN
Encryption
Bio-metrics
Anti-virus
IDS/IPS
Etc.

COMPLIANCE

Cybersecurity Response & Procedures Team

Information Security Policies & Procedures

Information Security Funding

Organizations value and view cybersecurity, risk, and control differently. Some of these differences are related to risk and threat profiles impacting an organization based on factors such as industry, location, product/services, etc. Some differences are related to management's view of or commitment to security and some are based on organizational experience with prior security incidents.

By focusing on three major considerations for effective cybersecurity implementations — people, process, and technology — our methodology is flexible enough to assist our clients, regardless of management's understanding, interpretation of risk, or existing corporate culture.

Cybersecurity Process

Controls over people, process, & technology.

People

Process

Technology
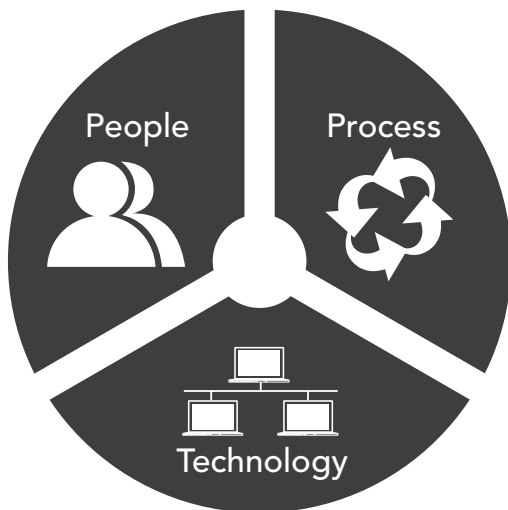
Cybersecurity includes the application of administrative, technical, and physical controls in an effort to protect against threats to the confidentiality, integrity, and availability of company information. Because of the pervasive use and integration of technology throughout organizations today, those threats affect more than just IT, they affect the whole business. With that in mind, an organization-wide security strategy, including cybersecurity awareness and active involvement by internal audit, is essential for the successful implementation of an organization-wide cybersecurity framework.

Our services consider the integration of people, process, and technology as essential when providing our clients with comprehensive cybersecurity solutions.
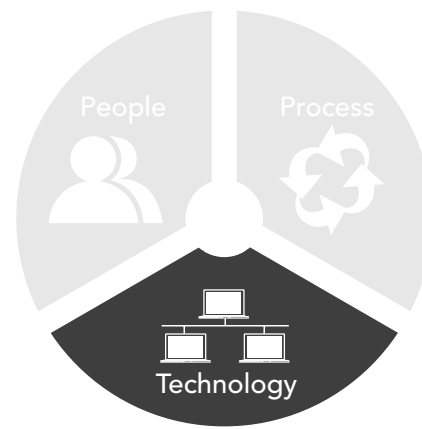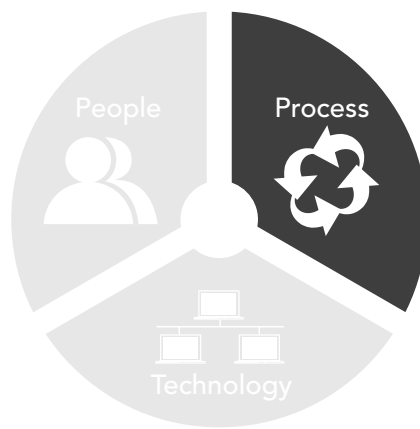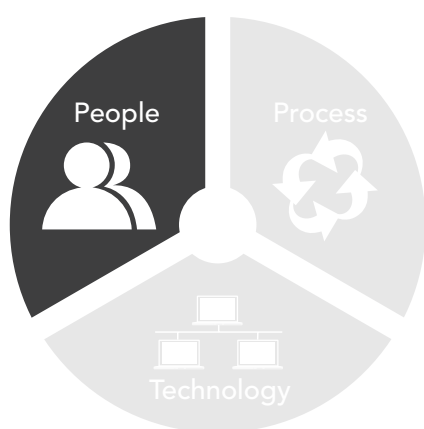
The **"people"** component of cybersecurity includes end users, members of IT who monitor and administer security for the organization, the organization's management team that has overall responsibility for cybersecurity, and third parties who have access (in different forms) to organizational data. The end users include employees, contractors, or consultants who access internal information systems and customers who access online information systems. In simple terms, "people" includes anyone who accesses organizational information systems or data. The "people" effectively execute the processes (i.e., security awareness, proper usage of systems, clean work area, etc.).

The **"process"** component involves the overall cybersecurity governance model and the processes developed to manage various aspects of security (i.e., physical and logical security, user access management, password management, BCP/DRP, change management, systems development, incident response, and user awareness training). Importance is placed on the effectiveness of the process as designed and not just the documentation of the process. As security evolves, so too should the "process" for managing risk.

The **"technology"** component includes security software and hardware that are deployed to manage cybersecurity. The "technology" component of security is constantly evolving as new technologies are implemented and security software and hardware become available, such as encryption, bio-metrics, mobile security, etc. The "technology," if properly implemented, enhances the effectiveness of both the "people" and the "process" which guide their security activities.

By focusing on people, process, and technology, our approach provides clients with a greater understanding of how cybersecurity threats might affect their organizations and a clear view of the design and effectiveness of the technical, administrative, and physical controls implemented to protect against these threats.

Cybersecurity Services

to meet today's cybersecurity needs.

When your goal is to provide a secure, well-controlled IT environment, Plante Moran can assist with:

SECURITY GOVERNANCE
- NIST Cybersecurity Standards
- ISO 27001 Security Standards
- COSO/COBIT Standards
- SANs Top 20 Security Controls
- Security Awareness
- Cyberincident Response Planning
- BCP/DRP

SECURITY RISK ASSESSMENTS
- Data & Application Mapping
- Vendor Management
- Threat Analysis
- Controls Mapping
- Maturity Models
- Risk-based IT Audit Planning
- Cybersecurity Program

SOC EXAMINATIONS
- Readiness Assessment
- SOC 1/SSAE 16
- SOC 2/Trust Services Principles
- SOC 3/Trust Services Principles

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

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

SECURITY COMPLIANCE
- Sarbanes-Oxley
- PCI DSS
- Financial Services Regulations (FFIEC, BSA, NACHA, etc.)
- Privacy Regulations (HIPAA/HITECH, GLBA, FERPA, FISMA, etc.)

Cybersecurity Approach

Based on this custom methodology and approach, Plante Moran has developed a number of services to help our clients:

- Understand their 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 remediation implementation and project management
- Build training and reporting programs to enhance both user and executive management's understanding of control activities and the effectiveness of their implementations

Our services are customized for the unique technical, administrative, and physical control environments implemented for our clients.

Plante Moran utilizes a phased approach for assisting organizations in successfully improving their current cybersecurity capabilities. This approach provides for a structured and focused effort throughout the project. Plante Moran also understands the importance of discussing all findings and recommendations with the key owner prior to escalating to others and writing in the report.

PHASE

1 START UP & PREP
- Planning
- Kickoff

2 DISCOVERY
- Review existing documentation
- Interview key personnel

3 TESTING
- Manual
- Automated

4 KNOWLEDGE & SHARING
- Detailed discussion of findings
- Demonstration of security tools

5 MANAGEMENT OF MEETINGS
- Discussion of results and recommendations

6 REPORTING
- Draft report
- Management response
- Final report

Our Leadership Team

RAJ PATEL, CISM, CISA, CRISC, FCCA | PARTNER

raj.patel@plantemoran.com | 248.223.3428

Raj has over 20 years of experience and is the partner-in-charge of Plante Moran's cybersecurity practice. Known for his practical approach to managing cybersecurity risks, Raj understands the challenges inherent in information technology and assists clients in managing risks pertaining to confidentiality, availability, and the integrity of information assets. He also helps organizations comply with the various cybersecurity and privacy regulations.

Most recently, Raj has focused on advising clients on various security and privacy compliance requirements and security mechanisms and processes for emerging technologies such as cloud computing, social media, mobile applications, and collaboration tools like Microsoft SharePoint. He is frequently quoted in national and regional periodicals as an expert on technology and cybersecurity topics. Raj was awarded the "40 under 40" award in 2009 and "American Dreamers" award in 2007 by Crain's Detroit Business in recognition of his professional accomplishments.

JOSEPH OLEKSAK, CISSP, CRISC, QSA | PARTNER

joe.oleksak@plantemoran.com | 847.628.8860

Joe has over 17 years of cybersecurity, controls, and IT audit experience in a number of industries. Joe's experience includes: IT strategic planning, IT risk assessments, SAS70/SSAE16/SOC, global/local network security projects, business continuity and disaster recovery management, IT audit, and web application security. In addition, Joe has extensive experience in working with various cybersecurity control frameworks (e.g., NIST 800, ISO 27001/27002, COBIT, HIPAA, FERPA). Joe is a Certified Information Systems Security Professional (CISSP) and a PCI Qualified Security Assessor. He is also Certified in Risk & Information Systems Control. Joe has presented on security related topics in various white papers, newsletters, and magazines and at various conferences.

TIMOTHY BOWLING, CPA | PARTNER

tim.bowling@plantemoran.com | 312.980.2927

Tim has over 15 years of experience performing financial auditing, management consulting, and internal controls attestation projects for clients in financial services and technologies industries. Because Tim manages SOC engagements and financial audit engagements, he regularly consults clients on best practices in designing risk assessments that meet requirements of users of SOC audit reports. Tim's experience includes starting an internal audit division at a publicly traded lighting manufacturer to guide it through its audits of internal control. Working in a corporation gave him a clear understanding of the operations and accounting challenges companies face. He is a member of the Information Systems Audit & Control Association (ISACA), American Institute of Certified Public Accountants (AICPA), and the Illinois CPA Society.

SARAH PAVELEK, CRISC | PRINCIPAL

sarah.pavelek@plantemoran.com | 847.628.8884

Sarah has over 14 years of cybersecurity, control, and IT audit experience in a number of industries, including technology, service, insurance, financial institutions, and health care. Sarah's experience includes: SOC/SAS 70 examinations, IT risk assessments, IT audits, application security controls reviews, internet banking compliance reviews, security & privacy assessments (GLBA, HIPAA/HITECH), and Sarbanes-Oxley 404 IT compliance reviews. In addition she has performed business process mapping documentation and evaluation, and has assisted clients in management information system selection projects. Sarah is Certified in Risk and Information Systems Control (CRISC) and is a member of the Information Systems Audit & Control Association (ISACA). She has presented on security-related topics in various white papers, newsletters, and webinars and at conferences.

F. ALEX BROWN, CPA | SENIOR MANAGER

furney.brown@plantemoran.com | 248.223.3396

Alex has over 16 years of information technology audit, technology regulatory control compliance, and system integration project experience. Alex has extensive experience with assessing and testing IT controls in support of technology audits and cybersecurity regulatory compliance engagements (e.g., HIPAA/HITECH cybersecurity assessments and Sarbanes-Oxley cybersecurity compliance control testing). In addition, Alex has extensive experience in working with various cybersecurity control frameworks (e.g., NIST 800, ISO 27001/27002, COBIT, HIPAA, FERPA). Alex has extensive industry experience including health care, manufacturing, and financial services. Alex's experience includes planning and performing engagements to evaluate and assess IT risk, evaluate the effectiveness of control measures implemented, identify IT control deficiencies, and develop remediation recommendations. Alex is a Certified Public Accountant and is a member of the American Institute of Certified Public Accountants (AICPA).

SCOTT PETREE, CPA, CISA, CFE, QSA | SENIOR MANAGER

scott.petree@plantemoran.com | 248.223.3898

Scott has over 14 years of experience in information technology consulting services including information systems audit, forensic technology, and enterprise risk mitigation for financial institutions, heath care, automotive, manufacturing, and government industries. Scott's experience includes: SAS 70/SOC reviews, IT risk assessments, IT audits, cybersecurity assessments, SOX 404 IT controls documentation and testing, computer forensics, FCPA compliance, and enterprise risk management. Scott is a member of the AICPA, MACPA, ISACA-Detroit chapter, and ACFE. Scott's certifications include Certified Public Accountant, Certified Information Systems Auditor, and Certified Fraud Examiner. Scott has presented on security related topics for webinars and conferences and published articles in newsletters.

Plante Moran in Brief

BY THE NUMBERS
- Founded: 1924
- Rank: 13th largest in the U.S.
- Team: 2,200+
- Locations: 23 offices in Illinois, Michigan, Ohio, China, India, and Mexico

DISTINCTIONS
- FORTUNE's list of the "100 Best Companies to Work For" for 17 consecutive years (highest-ranked accounting firm in 2008, 2009, 2011, 2012, 2013, 2014, and 2015)
- "2012 Employer of the Year" award by International Accounting Bulletin
- Number 16 on Crain's "Best Places to Work in Chicago" (2013)
- Number 7 on Crain's Chicago Business Best Places for Women to Work (2012)
- Sloan Award for Excellence in Workplace Flexibility (2008 and 2009)
- Among the lowest staff turnover rates in our industry
- One of the "Best Accounting Firms for Women," American Society of Women Accountants and the American Women's Society of Certified Public Accountants, or AWSCPA
- One of "West Michigan's 101 Best and Brightest Companies to Work For" (2009 for four consecutive years)
- On Human Resource Executive (HRE) magazine's exclusive list of "18 Great Companies for Millennials" (2008)
- Listed among Crain's Detroit Business's first list of "Most Admired Companies" (2009)
- Number 7 on WorkplaceDynamics' list of "America's Top Workplaces"

UNIQUE CULTURE AND CLIENT SERVICE APPROACH
- Resources, experience, and deep technical expertise of a larger firm
- Responsive, personal attention of a smaller firm
- Deeply ingrained culture of trust and respect for our clients, co-workers, work, families, and each other
- Commitment to exceeding client expectations
- Among the lowest staff turnover rates in our industry
- Reputation for reasonable fees

Our Services

span every inch of the office and every corner of the globe.

A FULL SPECTRUM OF CAPABILITIES

Whether you need a single, specific function or comprehensive service on a worldwide scale, Plante Moran has the knowledge, experience, and resources to meet your goals.

FINANCIAL
- Audit, review, & compilation
- Benefit plan audits
- Federal tax
- State & local tax
- International tax
- IFRS conversion & reporting
- Forecasts & projections
- Internal audit
- Interim financial services
- Bankruptcy advisory
- Financial restructuring & turnaround
- Valuation & investigative services

HUMAN CAPITAL
- Personnel assessment
- Leadership development
- Organizational strategy
- Training & coaching
- 401(k) & retirement plan consulting
- Incentive & deferred compensation
- Vendor selection & management

OPERATIONS & PROCESS
- Operational restructuring
- Facility analysis & rationalization
- Plant layout & flow
- Supply chain management
- Program & launch management
- Lean inventory management
- Process improvement
- Supplier risk assessment
- Transportation & logistics cost reduction
- Balanced scorecard

STRATEGY & GLOBAL
- Strategic planning
- Global assessment
- Low-cost country sourcing
- Supplier development
- Engineering consulting
- Expatriate contracts
- Financial structuring

TECHNOLOGY
- ERP system implementation
- Technology assessment
- Technology selection
- Contract negotiations
- Cybersecurity

TRANSACTIONS
- Acquisitions & divestitures (buy & sell side)
- Capital raising
- Due diligence (financial, strategic, & operational)
- Corporate real estate (lease, buy, build, monetize, & sale/leaseback)

WEALTH MANAGEMENT
- Institutional investment
- Insurance services
- Investment advisory
- Individual tax
- Trust

Client Feedback

Pursuing Excellence

"For some of our staff, however, having 97 out of 100 clients say they would be willing to recommend us to their colleagues isn't good enough.

It's that kind of spirit that makes us different from other professional service firms. A laser focus on client service is central to our culture."

Gordon Krater
Managing Partner

FINDINGS FROM PLANTE MORAN'S 2014 INDEPENDENT CLIENT SATISFACTION SURVEY (NOTE: INDEX IS 0-100, BUT NOT A PERCENTAGE)

PLANTE MORAN

89

AMAZON

86

NORDSTROM

86

COSTCO

84

APPLE

84
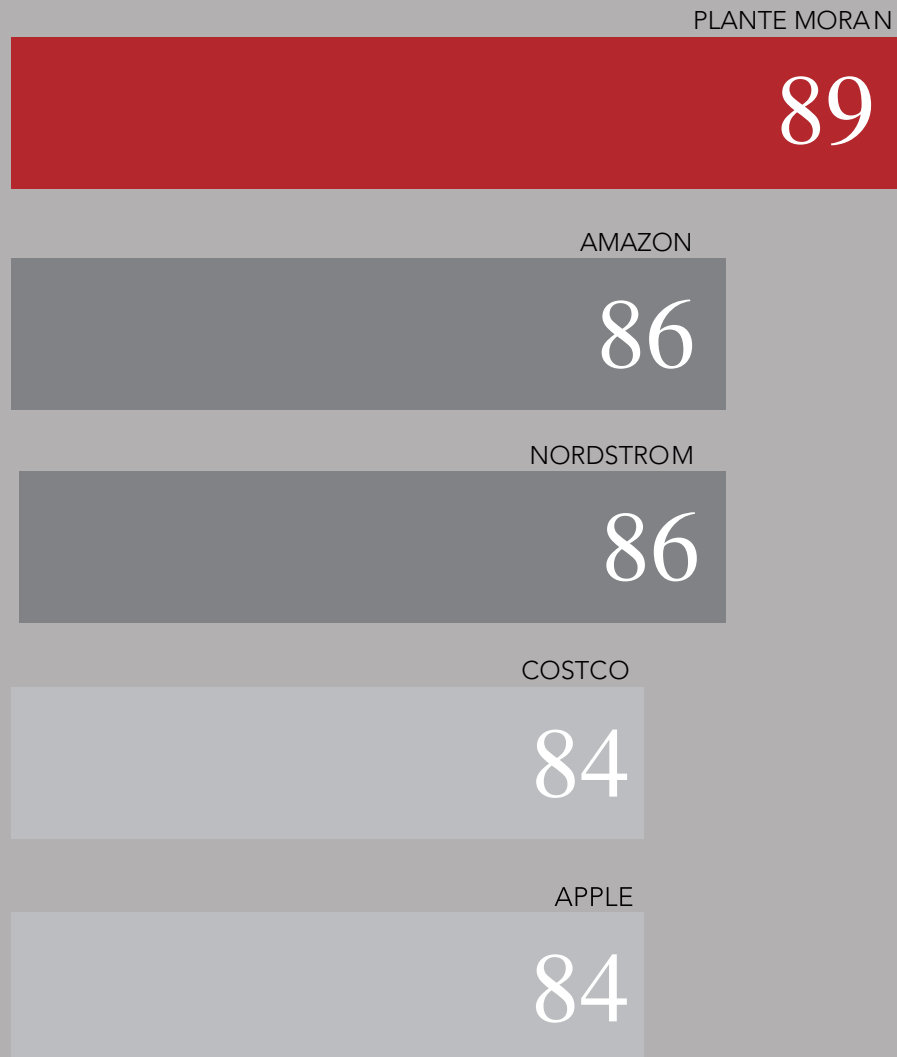
2014 Index

SOURCE: PLANTE MORAN'S RATING IS FROM OUR 2014 CLIENT SATISFACTION SURVEY CONDUCTED BY CFI GROUP USING THE AMERICAN CUSTOMER SATISFACTION INDEX (ACSI) – OTHER COMPANIES' SCORES PROVIDED BY THE ACSI.
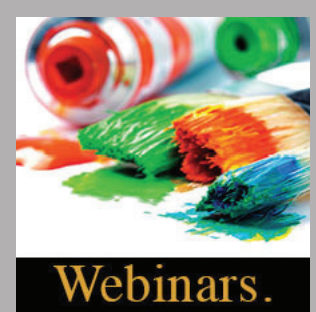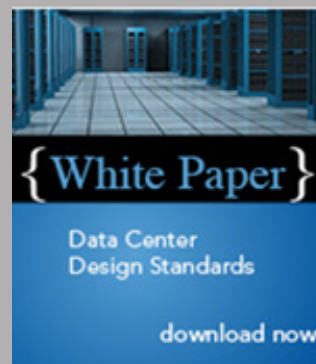
Thought Leadership

Knowledge to keep clients ahead of the curve.

WEBINARS, PUBLICATIONS, AND ONLINE CONTENT

Plante Moran invests in an ongoing commitment to research and thought leadership to ensure that the firm's professionals and our clients understand the forces driving leading trends and impacting profitability.

We deliver this thought leadership via webinars and podcasts and through online and printed publications.