Seven-point cybersecurity assessment

Are you secure? Is your data at risk? Do your employees understand their responsibilities to uphold confidentiality?

✓ *Users.* ✓ *Network.* ✓ *Access.* ✓ *Vendors.* ✓ *Incident response.*
✓ *Emerging technology.* ✓ *Common threats.*

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

Are you working aggressively to protect your information systems and data, yet you're still unsure of the effectiveness of your security controls?

These seven areas can shed light on how well you're protecting the confidentiality, availability, and integrity of your information and IT assets, as well as compliance with various security and privacy regulations.

1 Users

To perform their day-to-day functions, users are provided with access to your systems and data. These users can present a high risk to your organization, mostly from negligent practices such as weak passwords, indiscriminate downloading, phishing attacks, etc. It's important you properly on-board, train, and hold your users accountable for their actions on information systems. This includes a regular review of your on-boarding and termination processes and user awareness training.

2 Network

Your network is an interconnected group of systems that communicate and operate together on a technology infrastructure, including software, hardware, services, and other resources. Your network should be hardened through proper configuration and separation from public networks. It should also be periodically tested and continuously monitored to help detect and defend against potential cyber incidents.

3 Access

Access refers to your user’s permissions and how they are restricted based on roles and responsibilities. Permissions should be annually reviewed and access levels granted, revoked, or changed per duties.

4 Vendors

Third-party service providers that support your organization could potentially have access to confidential information or networked systems. Your organization should have vendor oversight to ensure services are performed securely and any data shared with vendors is duly protected. This includes a process for vetting vendors based on the risk of their responsibilities, and reviewing vendor contracts for cybersecurity control requirements, breach notification language, and confidentiality clauses.

5 Incident response

Your organization should have a tested process and plan in place to respond to a cybersecurity incident. Without a formal plan, your organization’s stakeholders, employees, IT systems, and reputation can be negatively impacted. Your incident response team should include representatives from all major departments and internal or external legal counsel.

6 Emerging technology

The technology landscape is constantly changing as organizations become increasingly more advanced and connected through various devices. Your organization should plan for the security risks these new technologies bring. This includes reviewing mobility, remote connections, cloud computing, and other connectivity points.

7 Common threats

Cybersecurity attacks are constantly evolving and the impacts are becoming more severe. Common threats include phishing, malware, ransomware, denial of service, and data theft. You should proactively evaluate your organization’s safeguards to ensure you have protection from these common threats.

Cybersecurity process

Controls over people, process, & technology

Cybersecurity includes the application of administrative, technical, and physical controls in an effort to protect against threats to the confidentiality, use, and integration of technology throughout organizations. Today, those threats affect more than just IT, they affect the entire organization. With that in mind, an organization-wide security strategy is essential for the successful protection of confidential data throughout the organization.

People
Process
Technology

We can help

Our seven-point cybersecurity assessment can help you focus on developing solutions for the areas that present the most risk to your organization.

Contact us

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

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

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

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

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

Stay in the know:
plantemoran.com/subscribe