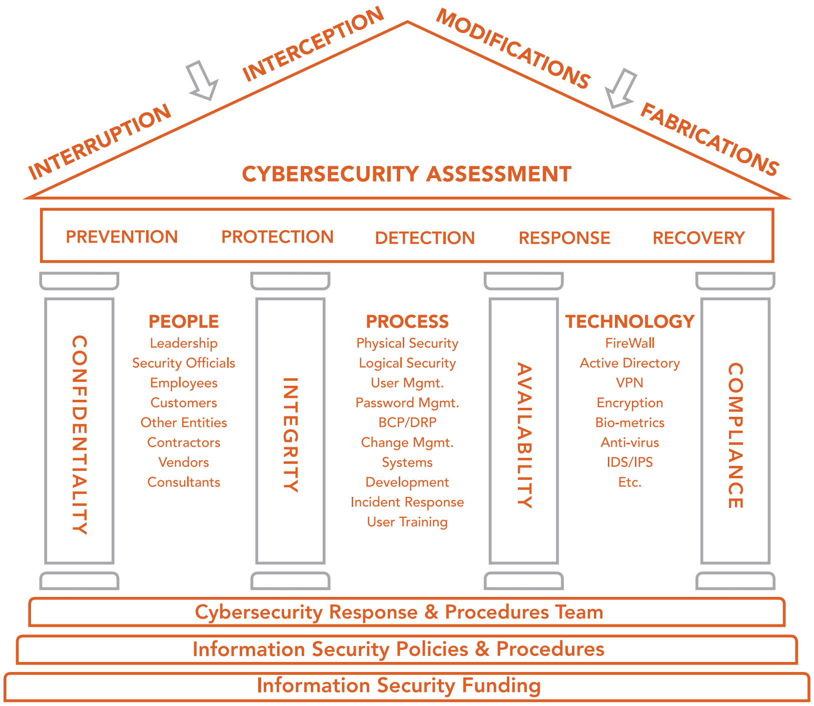
plante moran | Audit. Tax. Consulting.
Wealth Management.

Cybersecurity for Government

Fortify your IT and data security defenses with people, process, and technology

Technology touches nearly every aspect of government today, and cybersecurity threats affect every employee and government entity, and their affiliates. As cybersecurity threats continue to evolve, government agencies are prime targets due to valuable citizen data related to identity, finance, health, etc.

Our house of security methodology addresses everything from risk assessments, prevention, and recovery, to the full development of response procedures, security policies, and identifying information security funding. To keep hackers from exploiting all-too common vulnerabilities, it takes a strong and coordinated defense that includes three major controls: people, process, and technology. Additionally, mandatory compliance to various frameworks such as HIPAA, CJIS, IRS1075, make it critical to establish robust cybersecurity layers around the data.



People

End users are your first line of defense in protecting citizen data. With the best intentions to provide fast, friendly service, employees often click on links or attachments in phishing emails in an effort to fulfill seemingly legitimate requests. This action enables hackers — unbeknownst to you — to install malicious software, request credentials such as passwords and security questions and answers, and initiate wire transfers.

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 incident response, too, needs to evolve to address the increased downtime from new threats like ransomware.

Technology

While IT supports and facilitates your operations, it also must secure citizen and private data entrusted to your organization. Strong controls are critical, whether you manage your IT in-house or outsource. Government agencies must ensure, not assume, vendor processes and controls align with the latest security protocols for your organization and stakeholders' expectations balanced with citizen confidentiality requirements.

How we help

Our team provides government agencies with a complete range of risk assessment, risk mitigation, technical safeguards, and compliance services.

We take a personalized approach, interviewing your staff to fully understand your technology. An organization-wide approach to assess cybersecurity can help to understand the necessary controls and develop actions plans for any identified gaps. We offer strategic and tactical services to address your cybersecurity needs. These include the following:

SEVEN-POINT ASSESSMENT: HEALTHCHECK

Our seven-point cybersecurity assessment focuses on major security concerns and effective controls throughout your organization to determine your IT security posture and identify vulnerable areas.

PENETRATION TESTING: ATTACK & PEN

Using the most current threat intelligence, we'll help you identify specific target areas and launch controlled attacks from common footholds to identify gaps and weaknesses.

HIPAA/HITECH/CJIS/IRS1075 REVIEWS

Achieving compliance and maintaining HIPAA/HITECH, CJIS, and IRS1075 requirements can be challenging and time-consuming. We offer a streamlined approach to meet and sustain compliance requirements for administrative, physical, and technical safeguards, as well as strong practices for business associate agreements and breach notifications.

CYBERSECURITY STRATEGY AND GOVERNANCE

Addressing security guidelines and maintaining a strong security environment for employees to follow is challenging. We'll help you establish an effective information security program including governance, and relevant policy and procedures to sustain data confidentiality, integrity, and availability. Security programs are built using industry standard frameworks such as NIST800, ISO27000, and more.

Rajiv Das
rajiv.das@plantemoran.com ✉
517-898-2033 ☎

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

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