Brenner Financial Services: Risk assessment

Current assets

Assets managed by the IT Department include:

* Hardware:
* Servers: Responsible for hosting and managing various applications, databases, and services.
* Desktops and Laptops: End-user computing devices used by employees for their daily work.
* Networking Equipment: Routers, switches, firewalls, and other devices that enable communication within the organization's network.
* Software:
* Operating Systems: Management and maintenance of server and end-user operating systems.
* Productivity Software: Applications such as office suites, email clients, and collaboration tools.
* Financial Software: Specialized software for managing financial transactions, accounting, and related functions.
* Security Software: Antivirus programs, intrusion detection/prevention systems, and other security-related tools.
* Custom Applications: Any proprietary or customized software developed or utilized for specific business needs.
* Data and Databases:
* Database Servers: Management of database systems storing critical financial and customer data.
* Data Storage Systems: Storage solutions for structured and unstructured data.
* Data Backups: Systems and processes for regular backup and recovery of essential data.
* Network Infrastructure:
* Networking Components: Routers, switches, firewalls, and other devices that form the organization's network backbone.
* Wireless Access Points: Infrastructure supporting wireless connectivity within the organization.
* Cybersecurity Tools:
* Firewalls: Hardware or software-based systems protecting the organization's network from unauthorized access.
* Intrusion Detection/Prevention Systems (IDS/IPS): Monitoring and response systems for detecting and preventing security threats.
* Antivirus and Anti-malware Solutions: Tools to protect against malicious software.
* Communication Systems:
* Email Servers: Infrastructure supporting email communication.
* Unified Communication Systems: Tools for integrated communication, including voice, video, and messaging.
* End-User Devices:
* Mobile Devices: Management of smartphones and tablets used by employees.
* Printers and Scanners: Peripheral devices used for document management.
* Cloud Services:
* Cloud Infrastructure: Management of resources hosted on cloud platforms.
* Software as a Service (SaaS): Utilization and management of cloud-based software applications.
* IT Service Management (ITSM) Tools:
* Ticketing Systems: Platforms for tracking and resolving IT-related issues.
* Asset Management Systems: Tools for tracking and managing IT assets throughout their lifecycle.
* Physical Security Systems:
* Access Control Systems: Systems regulating physical access to data centers and other critical IT infrastructure.
* Surveillance Systems: Monitoring systems for physical security.
* Documentation and Policies:
* IT Policies and Procedures: Documentation outlining the rules and guidelines for IT-related activities.
* System Documentation: Information detailing configurations, processes, and procedures for IT systems.

Risk description

Threats such as malware, ransomware, phishing attacks, and advanced persistent threats that can compromise the security of IT systems and data is something that Brenner Financial Services is dealing with. With the new implementation of malware practice, the risk should lower.

Control best practices

Mobile Device Management (MDM):

Enforce Mobile Security Policies: Implement MDM solutions to enforce security policies on mobile devices, including encryption, remote wipe capabilities, and application controls.

Secure Development Practices:

Code Reviews: Conduct regular code reviews to identify and address security vulnerabilities in applications.

Secure Coding Training: Provide developers with training on secure coding practices.

Risk score

On a scale of 1 to 10, the risk score is 6, which is fairly high. This is due to a lack of controls and adherence to necessary compliance regulations and standards.

Additional comments

Cybersecurity is an ongoing process, and a holistic approach that combines technology, processes, and people is essential for effectively mitigating risks and securing the digital assets of Brenner Financial Services. Regular reviews, updates, and a proactive mindset are key elements of a successful cybersecurity strategy.