Stimulus
TECHNOLOGIES

Stimulus CyberSCORE Questions

Infrastructure

1. We maintain an inventory of all workstations, servers and network equipment and we have implemented a sustainable hardware refresh cycle.
   Recommendation: *Purchase date, serial and warranty tracked on all equipment and hardware is replaced when it reaches end-of-life*
2. We utilize an incident ticketing system, we provide our management team with regular response and resolution time reports and the results of those reports are meeting the organization's expectations.
   Recommendation: *Online ticketing service desk where all incidents are logged and reported on*
3. Our wireless network prevents guests from accessing our internal network and employees have unique usernames and passwords assigned for wireless access.
   Recommendation: *Separate employee and guest wireless networks and RADIUS auth with Active Directory or Azure AD*
4. Our office locations utilize redundant internet service provider connections, and our firewall or router automatically swaps connections in the event of an outage.
   Recommendation: *Primary copper/fiber and backup cable (COAX) connection and firewall with automatic ISP failover*
5. Our servers and network equipment are protected with uninterruptible power supply units that are replaced every 3 years, are in a physically secure location, and has separate HVAC systems.
   Recommendation: *APC UPS with managed ethernet for power monitoring automatic server shutdown feature.*

Cybersecurity

1. I am confident that we have the proper cybersecurity software deployed to protect personal and corporate data from attacks such as phishing and ransomware, including any remote devices that are used to access critical infrastructure and data.
   Recommendation: *Advanced EDR with 24/7/365 Security Operations and Real-Time Remediation*
2. We engage with all organization employees and properly train them to identify ransomware, phishing and social engineering attacks coming from email, text message and web sites.
   Recommendation: *End-user training software with at least bi-weekly phish testing and real-time micro learning*
3. All organization IT systems and devices that contain PII or sensitive company information are encrypted to protect against loss or left.
   Recommendation: *Bitlocker AES 256 encryption managed by Azure Active Directory*
4. We use single sign on and two-factor authentication across all critical line of business applications such as Office 365, our ERP system and remote access.
   Recommendation: *Email, outside access to ERP and VPN, RDP, VDI all use DUO or Microsoft MFA*
5. The level of cybersecurity insurance carried by our business is adequate to protect our organization and our clients from financial loss.
   Recommendation: *Standalone policy with 1m per occurrence and 2m of aggregate coverage*

Compliance

1. We apply regular server and workstation security patches and updates across our technology infrastructure.
   Recommendation: *Weekly Windows and Mac OS updates are applied using an automated patching system*
2. We have a properly segmented corporate network (meaning workstations, servers, phones and guests are kept in separate logical networks).
   Recommendation: *VLAN segmentation and proper access control is in place to prevent unauthorized access between networks*
3. We perform a regular network vulnerability scan and have archived all historical scan data for reporting and compliance purposes.
   Recommendation: *Ongoing Rapidfire Tools Cyberhawk network scans with a minimum of quarterly Network Detective scans.*
4. We have a written information security policy (WISP) that has been agreed to by all employees.
   Recommendation: *Centrally documented WISP that includes User Termination, Incident Response, Sanction, Network Security, Access Control, Computer Use, Equipment Disposal, BYOD and Facility Security policies.*
5. We are meeting all state and federal compliance requirements such as HIPAA, PCI DSS, FINRA and all federal and state PII Rules and we are confident we would pass an audit.
   Recommendation: *Depending upon specific vertical. Nearly every NJ business will have some level of NY SHIELD compliance requirements.*

Backup & Disaster Recovery

1. We proactively monitor our server and cloud infrastructure for failures and performance issues so that business affecting problems can be prevented.
   Recommendation: *Service and network monitoring with real-time alerting and paging – responsible parties respond and remediate*
2. We regularly review our backup strategy, and we adhere to a documented process for backup frequency, retention and location.
   Recommendation: *Centrally documented backup and RPO (recovery point objective) document agreed to by all relevant parties*
3. We perform regular backup recovery testing, and we have a clear time objective for restoring critical systems and data.
   Recommendation: *At least quarterly recovery testing performed and logged of file, server and environment*
4. Our management team understands and has agreed to the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for backup and disaster recovery and both are monitored and tested regularly.
   Recommendation: *Cost of user, department, location and company downtime calculated, documented and known so it can be utilized when making IT related decisions*
5. We have a well-defined disaster response team with clearly defined roles, responsibilities and communication protocols.
   Recommendation: *1 or more persons with specific roles and processes in place to manage and/or perform data recovery and end-user access restoration*

Business Strategy

1. The organization's management team views technology as an investment, not a cost and they agree to implement best practices when recommended by the IT team.
   Recommendation: *Technology is seen as a functional area of the business and ownership/leadership understands the importance of investing in proper technology*
2. We perform a regular technical alignment assessment to identify areas of our technology infrastructure that do not meet best practices.
   Recommendation: *Utilizing a set of best practices and standards, a GAP analysis is performed quarterly or bi-annually.*
3. We meet regularly as a team to assess risk, discuss strategy and perform IT budget planning for our organization.
   Recommendation: *Ownership/Leadership meets with IT personnel quarterly or bi-annually to discuss GAPs and identify areas in need of improvement. These are logged into a proper organization budget.*
4. We have a clear process for making IT related decisions in our organization, a project plan is agreed upon before implementation and communication within our organization is clear and consistent.
   Recommendation: *IT projects are reviewed and understood by management. All IT projects are performed only when a proper project plan is created, approved and followed by IT personnel.*
5. We consistently bring advances in technology to the attention of our management team, which increase employee productivity and gives us an edge over our competitors.
   Recommendation: *IT personnel are aware of new technology advancements that could help the business increase productivity and profitability. These ideas are discussed at regular strategy meetings.*

Cloud

1. We utilize a secure cloud-based email solution like Microsoft 365.
   Recommendation: *Office 365 or Google Workspace email*
2. Our cloud services are configured according to service provider recommended best practices.
   Recommendation: *Follow Continuous Networks Office 365 Cloud best practices (or applicable vendor)*
3. Our cloud-based email and file services are configured with data loss prevention policies and alerting to prevent data breaches.
   Recommendation: *Microsoft 365 DLP policies for Email and OneDrive/Sharepoint – Alerts are sent to responsible parties*
4. All users are provided with training on applicable cloud services and are required to understand and agree to a written company Cloud Usage and Security Policy.
   Recommendation: *Windows Virtual Desktop*
5. We utilize a 24/7 SOC that monitors and alerts on our network, cloud services and critical data systems.
   Recommendation: *Perch or other real-time Intrusion Detection System with 24/7/365 Security Operations*