INFORMATION SECURITY REVIEW

Company Private & Confidential

January 1, 2020

XYZ company

EGP Secure

SANDBOX TECHNOLOGIES

INFORMATION SECURITY REVIEW

TABLE OF CONTENTS

1. DOCUMENTATION ____ 2
2. GENERAL NETWORK ____ 6
3. USER & USER WORKSTATIONS ____ 19
4. MOBILE DEVICES ____ 23
5. WEB, CLOUD & OFF-SITE PROVIDERS ____ 25
6. TELEPHONY ____ 27
7. BACKUP & DISASTER RECOVERY ____ 28
8. INSURANCE & RISK MANAGMENT ____ 30
9. PHYSICAL SECURITY ____ 31
10. AUDITING / VERIFICATION ____ 32
11. INFORMATION SECURITY POLICIES FOR USERS ____ 35
12. USER & WORKSTATION MAINTENANCE ____ 36

STATUS SUMMARY REPORT ____ 38

Appendix A: Dark Web Search - xyzcompany.com ____ 44

Appendix B: Content Filtering Categories - FortiGate ____ 45

Appendix C: Geo-IP Filtering Regions - FortiGate ____ 46

1. DOCUMENTATION

1.1. Maintain diagrammatical representation of network architecture, equipment elevations, and formal inventory

Diagrams provide a high-level overview of the environment and illustrate the relationships between various network components. Clear and accurate representations promote better management and facilitate the efficient diagnosis of network issues.

Support of XYZ Company's network environment is currently facilitated via the SolarWinds RMM console which aggregates live network data; however, the organization's network is not currently diagrammed or formally documented.

It is recommended that detailed network diagrams, equipment elevations and other formal documentation be created and maintained to supplement the SolarWinds RMM data and facilitate the recommended visibility.

1.2. Create formal IT Policies

IT policies are formal written documents governing the authorized use of company IT systems and tools, such as email, computer workstations, telephony and server resources. These policies cover topics such as user conduct, acceptable use of systems, actions requiring written authorization from management, and secure data handling. IT policies should clearly articulate the conduct that is consistent with management's vision for the security and stability of the technology environment. IT policies are often incorporated into an organization's human resources manual.

XYZ Company currently has IT policies in place. The auditor did not conduct a review of said policies, however on the basis that such were created through the join efforts of internal XYZ COMPANY staff and its compliance consultants, they are presumed to represent the wishes of the firm's management and compliance decision makers. A secondary review of XYZ Company's existing IT policies can be conducted upon request.

1.3. Create formal IT security standards

Given their role in administering systems, IT personnel often possess unrestricted access credentials. This inherent necessity creates a point of weakness that is particularly common in smaller enterprises. Engaging highly qualified individuals, conducting background checks and performing periodic audits, can reduce exposure. However, one of the most effective controls a company can implement is an IT Strategy and departmental standards.

Guidelines and controls set internal standards and bolster an organization's security. These guidelines include data sanitization practices, software approval requirements, administrative rights assignment, directory structure and equipment disposal.

IT Security Standards should not be confused with IT policies. IT security standards pertain to the internal operation of the IT Department itself, whereas IT policies are generally applicable to all users within an organization.

XYZ Company currently has no formal standards in place. As such, it is recommended that the firm adopt formal IT Security Standards.

It is recommended that documentation be created and maintained as described. To the extent possible, Active Directory rights should be structured based on roles rather than individuals, which will help to streamline the process of managing occasional turnover.

1.14. Create formal procedures for Change Management

Change management is beneficial for ensuring that proposed changes to the environment or workflow processes do not create new vulnerabilities, conflict with existing configurations, or cause unintended consequences on business operations.

There is currently no formal documentation for change management within XYZ Company.

The implementation of change management procedures is a typical business best practice. The level of attention warranted is of course to some degree commensurate with an organization's size. In the case of XYZ Company, the limited number of individuals employed inherently mitigates some aspects of exposure. For example, it would be less likely to experience problems encouraging the active use and adoption of a new software solution if the solution was selected by the same and sole individual that would be using it. Nonetheless, it is recommended that some manner of formal framework and procedures be created and followed whenever a reasonable need is identified.

2. GENERAL NETWORK

2.1. Implement one or more business class firewall appliances to restrict direct outside access.

Firewalls are the first line of defense for a network environment, as well as a central hub for VPN services to secure communication and limit exposure. Business class firewalls feature advanced security and advanced routing controls. They allow for more security Inspection   at higher speeds, they are typically much more secure, and generally support faster throughput, superior uptime, and better reliability.

XYZ Company has currently implemented one FortiNet 400E at its office. The firmware version as of January 1, 2020 is 6.5.2.2-44n. The support agreement expires on December 31, 2020.

There are currently no additional recommendations.

2.2. A minimum of two WAN connections should be implemented to increase Internet stability.

A WAN (Wide Area Network) connection is the link connecting a perimeter firewall to public internet resources and is the connection over which all public communication takes place. Having only one WAN connection creates a single point of failure, a failure of which causes interruption to any WAN dependent services, such as email, hosted VOIP services, cloud providers and general Internet connectivity.

A dual WAN configuration allows the firewall to fail over to a secondary WAN connection in the event of an ISP (Internet Service Provider) failure, mitigating downtime and loss of service.

There is currently only a single WAN connection setup. It is recommended that XYZ Company obtain a secondary WAN connection to provide failover in the event of an outage on the primary line.

3. USER & USER WORKSTATIONS

3.1. Implement drive encryption for laptops & user workstations.

In the event of loss or theft, unencrypted computer data (files, cached emails, saved passwords, etc.) can be susceptible to unauthorized access. Password security on unencrypted devices can be circumvented easily by removing and attaching the device’s hard drive to another computer. With minimal effort, even deleted files can often be accessed, provided they have not been overwritten by other data.

Whole disk encryption is designed to prevent anyone except the password holder from accessing data.

Currently, no formal group policy exists requiring that disk encryption be installed on XYZ Company’s desktops or laptops. Whole disk encryption is recommended for all workstations and laptops that access company resources or contain company data. While workstation encryption can be enabled on an individual basis using the built-in encryption capability of Windows 10, policy-based deployment is recommended for proper control and visibility. Optimally, a third party solution with the ability to centrally manage keys and facilitate encryption using software other than the built-in BitLocker encryption is recommended.

3.2. Automate deployment of patches & fixes

Software vendors regularly release updates intended to fix security vulnerabilities and system instabilities. Keeping operating systems and software up to date helps to mitigate exploitation of security flaws. Downtime due to known software bugs is also reduced, along with the attendant support costs.

There is currently no system for the automated deployment of patches and software updates in place for network devices, and there is no automated comprehensive workstation patching solution.

It is recommended that a provision for the deployment of patches and software updates be implemented to help ensure that devices and software remain up-to-date.

3.3. Disallow local administrative rights on user workstations.

Granting local administrative rights to user workstations creates a serious security weakness. Often, full administrative rights to a local machine are required for viruses, trojans and rootkits to take full effect. While infection is sometimes still possible without local administrative rights, the restriction of privileges for normal domain users can reduce the likelihood of infection.

It is also possible for domain users with administrative access to make unauthorized changes to their workstations (creating shares, installing unauthorized software) or, in some cases, to bypass security policies entirely. This in turn can affect system stability by nullifying security configurations and creating security flaws that can be used as attack vectors inside the network environment.

Most users within XYZ Company are currently permitted local administrative access to their workstations.

It is recommended that each user’s applications and workflow be reviewed to determine if local administrative rights are required for day-to-day operations. If users do not require local administrative rights for business operations, it is recommended that such rights be removed.

4. MOBILE DEVICES

4.1. Mobile Device Manager for remote wipe/disabling/management of mobile devices

In the event of a mobile device loss, unmanaged devices are at risk of being compromised, which can lead to the exposure of sensitive data. An MDM (Mobile Device Management) system facilitates managing devices in a controlled manner. Most MDM solutions offer the following functionality:

- Remote lock.
- Remote wipe.
- Mandatory PIN/Password enforcement.
- Data encryption.
- Device encryption.
- Software policies/restrictions, and
- GPS tracking.

There is currently no Mobile Device Manager implemented at XYZ Company. The only potential controls are the default controls for email provided by Microsoft Exchange via Intermedia.

It is recommended that an MDM system be deployed. Additionally, although the company could consider the use of a legal authorization between XYZ Company and its employees (often referred to as a “BYOD” or “Bring Your Own Device” policy) it is recommended that the organization disallow the use of any devices that are not owned and controlled by XYZ Company.

4.2. Restrict the ability to access the organization’s email systems from mobile devices without prior authorization of both management and I.T.

By default, ActiveSync (the mechanism used for communication with mobile devices) permits anyone with a valid username and password to connect a mobile device to the associated mail host. Hackers often exploit this vulnerability to circumvent multi-factor authentication protections, because said protections do not apply to mobile devices.

In Microsoft Exchange/Office365 environments, it is a recommended practice to enable a feature known as “ActiveSync Quarantine”, which requires an authorized administrator to electronically approve new mobile devices before they are permitted to connect.

Currently, ActiveSync Quarantine is not enabled for XYZ Company’s email system. Further, due to Intermedia’s proprietary implementation of hosted Microsoft Exchange, it is not possible to enable ActiveSync Quarantining while utilizing Intermedia for email services.

It is strongly recommended that the risk posed be weighed against the cost of migrating to a service that does support this. If it is determined that the need for ActiveSync Quarantining outweighs the associated cost of transferring service, it is recommended that XYZ Company migrate their email services to Microsoft’s Office 365 platform.

5. WEB, CLOUD & OFF-SITE PROVIDERS

5.1. Develop and implement security standards for the consistent secure deployment of XYZ Company's Web properties.

Websites are sometimes overlooked as a critical security vulnerability. Whether an organization's Web presence(s) link to sensitive data like credit cards and personal information, or merely serve as an online brochure, there are a myriad of ways that a breach can cause damage to an organization. As such, it is important to secure websites and other public facing systems aggressively.

There are currently no formal security standards for XYZ Company's Web properties.

It is recommended that IT work with management to create formal security policies. The current web property www.xyzcompany.com should be reviewed for compliance and corrective action taken as needed.

5.2. Employ the use of TLS/SSL Certificates for XYZ Company's Website properties.

An SSL (Secure Sockets Layer) certificate is a two-part key pair used to encrypt communication, including traffic to and from a publicly accessible website. TLS (Transport Layer Security) is the next generation of SSL and differs from SSL by the protocol used to establish a secure connection. SSL and TLS utilize the same certificates; however, the protocols are different, and availability is dependent on the environment hosting the Web property. A minimum of TLS 1.1 should be enabled on web properties when using secure certificates.

Currently, TLS is supported by the www.xyzcompany.com property, however a secure connection is not required, and the certificate itself is not trusted when used for XYZ Company's specific domain name.

It is recommended that an SSL certificate be obtained from a respected third party (Verisign, Thawte, DigiCert) and that the certificate be installed on the Web property. It is also recommended that a secure connection be required, and that attempts to make any insecure connection(s) redirect the client to a TLS session.

5.3. Web host security

Web host security is a key consideration. While organizations engaged in e-commerce or other revenue generating activity generally attend to this requirement, those with only basic publicity sites often overlook its importance.

The host currently responsible for the Web property www.xyzcompany.com is unknown to the auditors.

It is recommended that the Web host's security practices, technologies and audit reports (if any) be requested and evaluated to confirm they adequately meet the needs of XYZ Company.

5.4. Check integrity of website code

Older Web technologies and sites that have not been kept current can often be exploited with relative ease. When a website is compromised, hackers can potentially insert malicious code, copy the site and

6. TELEPHONY

6.1. Implement LSP (Locally Survivable Processor) for telephony solution to provide automatic failover/redundancy in the event of an equipment outage.

An LSP (Locally Survivable Processor) is a local redundant telephony appliance that can act as a call processor in the event of a failure impacting the primary unit.

The use of a Locally Survivable Processor is a common recommendation for organizations that cannot afford to sustain any significant downtime in the event of an internal telephone system failure. XYZ Company's current Avaya telephone solution does not feature an LSP

Based on the current understanding of the organization's operational needs and priorities, it is the auditor's view that the value of an LSP to XYZ Company may not justify the expense. While such is a decision for XYZ Company's senior management and not the auditor, if that should be the case, it is nonetheless recommended that at a minimum, the organization should maintain a suitable equipment warranty and maintenance agreement at all times.

6.2. Implement redundant voice connectivity for continuity in the event of a telephone carrier outage.

There are numerous means of connectivity employed to provide dial tone to internal telephone systems. SIP trunks are an Internet-based voice product employed to provide dial tone to an organization's internal telephone equipment. Copper PRI (Primary Rate Interface) is typically a T-1 line with 23 voice channels and a single data/control channel. A single PRI can facilitate up to 23 simultaneous calls and has guaranteed QoS (Quality of Service). Copper PRI lines are very common and traditionally quite reliable; however, they are largely being replaced by SIP trunks and Fiber PRI connections

Fiber PRI connections are similar to copper PRI circuits; however, they are typically delivered via an organization's Internet service provider. As a contingency against a carrier service outage, organizations that cannot afford downtime often employ the use of redundant connections through disparate carriers. There is currently no redundant voice connection that can be leveraged in the event of a telephony carrier outage.

Based on the company's headcount and operations, it is the auditor's opinion that the cost of a redundant voice solution is unlikely to justify the significant additional expense. Because this determination should only be made by XYZ Company's senior management, is recommended that the firm review the relative pros and cons of adding a redundant voice connection. Should the company choose to do so, further information and assistance can be provided upon request.

7. BACKUP & DISASTER RECOVERY

7.1. Implement local incremental file backup solution w/on and off-premises virtualization capability

Regular backups are a cornerstone of network integrity, as they are the primary means of preventing data loss, as well as maintaining historical records of data. Disasters, such as floods, fires, theft, etc., can destroy locally stored backup data, so it is critical to maintain a secure, offsite repository for Disaster Recovery purposes.

Currently, backup and disaster recovery is provided by a Datto Siris 3 BDR device.

As the Datto provides both cloud based and local file, bare metal and emergency virtualization protections, there are currently no further recommendations.

7.2. Implement redundant backup of the organization’s Cloud-based email environment

Cloud-based email hosts typically offer their own retention policies to protect organizations against loss of data in the event of corruption or deletion – intentional or willful. Retention policies typically vary based on the host, and the retention options selected. Redundant backups of hosted email solutions are generally implemented for one or more of the following reasons:

1) The provider’s backup retention policies do not meet the organization’s requirements in terms of frequency or duration.
2) The provider offers suitable protection; however, the premium for the desired level of protection is more costly than a third-party solution.
3) The organization wishes to have a redundant means of backing up the system that is managed by an entirely separate party, and
4) The organization opts to maintain a minimal retention policy for data in the Cloud, with longer-term retention facilitated by a device in the possession of the organization, and under its direct control.

XYZ Company does not currently leverage a redundant backup of the cloud based email system.

Notwithstanding existing compliance measures in place with Intermedia.net, it is additionally recommended that a third-party system such as Code Two or SkyKick be implemented for redundancy,

7.3. Implement a Disaster Recovery plan

A written DR (Disaster Recovery) plan outlines the steps, order of action and team member responsibilities in the event of a disaster. A properly implemented DR plan facilitates a rapid and more seamless response in the event of a loss or failure, with the objective of minimizing both data and productivity loss due to downtime.

XYZ Company currently has a disaster recovery plan in place. The auditor has not reviewed the plan, however on the basis that the plan meets the firm’s operational and compliance requirements, there are no recommendations at this time.

8. INSURANCE & RISK MANAGMENT

8.1. Cyber-insurance coverage

Various forms of Cyber-insurance policies exist to protect organizations and individual users against certain exposure stemming from IT-related incidents. Examples of first party coverage include losses from data destruction, extortion, theft, hacking, and denial of service attacks. Types of liability coverage can include indemnification for third party losses due to errors and omissions, defamation and failure to safeguard data. Other coverage benefits can include coverage for breach-related investigative expenses, security audits, mandatory notifications/compliance, criminal rewards, and public relations initiatives. Coverage options can vary significantly.

XYZ Company currently has cyber-insurance coverage through Berkshire Hathaway.

It is recommended that coverage be maintained at all time, and that policy provisions be reviewed periodically to ensure suitability as needs change.

9. PHYSICAL SECURITY

9.1. I.T. room access control

The ability to gain physical access to I.T. equipment should be highly controlled and tracked. Unauthorized physical access to hardware exposes an organization to numerous attack vectors, including data theft, malware implantation, network traffic sniffing, etc. Physical access to network and other I.T. equipment should be tightly controlled and logged at all times by an access control system. IT equipment within should be maintained inside one or more locked data cabinets.

Physical access to the IT room is currently controlled via a pin and tumbler lock. The individuals who currently have a key are Mike Smith, Carly Clark, and the office of the building.

It is recommended that an access control system be implemented for the purpose of tracking ingress and egress to this room.

9.2. Surveillance cameras and card access control

Surveillance cameras and card access control are key to maintaining an organization's physical security. Suitable coverage of the organization's space, and ample retention of recorded video content is can be essential when investigating an internal cybersecurity or other event. Similarly, the organization's access control system should be well managed, and include ample storage for the retention of historical card activity.

There are currently no surveillance cameras in the suite.

It is recommended that a surveillance camera system be implemented to record activity at all suite entrance(s). The implementation of a surveillance camera system monitoring the IT equipment area is also highly recommended. (Note: Implementation of surveillance systems should always be undertaken by a qualified professional in keeping with applicable laws and privacy rights.)

9.3. Visitor access logging/control

Electronic sign-in systems and visitor identification badges enhance an organization's physical security, and act as an added deterrent to individuals seeking easy targets for equipment theft and other crimes.

Such measures are particularly beneficial in high-traffic environments, and in areas where sensitive data is housed. The use of visitor badges raises employee awareness, and aids in identifying individuals that may be on the premises without authorization.

There is currently no visitor access logging in place. Although the above measures are always recommended, given the relatively low visitor traffic experienced and the type of guests visiting the suite, the use of badges could potentially be excessive.

10.AUDITING / VERIFICATION

10.1. Scheduled test of surveillance camera functionality

As with all security systems and devices, surveillance cameras should be tested regularly to insure proper function and availability in the case of a cybersecurity or other event. Without testing or monitoring, it is possible for camera NVR or DVR devices to become suspended and cease recording without an organization's knowledge.

At this time, there are no surveillance cameras to be tested.

10.2. Adopt outside penetration testing schedule (Third party)

Penetration testing is the practice of conducting simulated attacks on an environment as a means of identifying vulnerabilities.

There is currently no outside penetration testing being conducted for XYZ Company.

Periodic penetration testing is highly recommended to aid in identifying vulnerabilities. Such information can then often be used to bolster security in those areas.

10.3. Review of firewall port configuration

A periodic review of firewall port configurations helps to identify and eliminate unnecessary attack vectors. As technology needs change, inbound and/or outbound ports may occasionally need to be opened or closed to meet communication requirements. Reviewing ports is a particularly useful practice in environments with multiple administrators.

Currently firewall port configuration is reviewed on an as-needed basis.

It is recommended that a periodic review of port configurations be implemented and conducted for XYZ Company's firewall. It is recommended that a list be maintained of all users authorized to make port configuration changes, and that logs of all changes be retained for audit purposes.

10.4. Review firewall firmware revision

New firewall firmware is released as bugs and/or security flaws are resolved. Firmware updates are critical to maintaining the best available protections against newly discovered exploits, and system stability impediments.

Currently firewall firmware is updated on an as-needed basis by the firm's IT vendor.

It is recommended that a periodic review be conducted of the firewall firmware revisions, and that such be performed via NOC (Network Operation Center) personnel, or as part and parcel of a SAAS (Security as a Service) subscription. The aforementioned services can be provided at a flat rate by the firm's current provider and scheduled to occur outside of business hours.

11. INFORMATION SECURITY POLICIES FOR USERS

11.1. Information Security Policies

Inclusion of policies addressing the following topics is recommended, subject to prior review and approval by qualified legal counsel.

Recommended topics for inclusion in XYZ Company's Information Security Policies are:

- Protection of confidential information
- Protection of passwords issued
- Physical security of equipment assigned (laptops, smart phones, etc.)
- Access / Responsibilities & Limitations
- Restrictions, prohibiting technical changes & modifications
- Non-company equipment use prohibited
- Responsibility to attend company sponsored employee/contractor security training and awareness.
- External media/device control
- International travel policies / safety / VPN & mobile device use
- Virus awareness & avoidance
- Proper use of electronic information systems
- No unlawful or unauthorized purposes
- No unauthorized removal/copying/deletion/dissemination of information
- Branding & use of company logo & imagery
- Company confidentiality policies & guidelines
- Blogging/Social media use policies & restrictions
- Compliance with copyright law
- Restrictions governing torrents & questionable websites
- Inappropriate communications, harassment & discrimination
- Company rights
- All information transiting company's systems property of company
- Define company systems (include third party hosts, smart phones, other connected devices as applicable.)
- Company right to monitor/view/record, no employee or contractor right to privacy
- Post-termination employee/contractor conduct
- Return or destruction of information
- Duty to assist/provide passwords
- Mandatory Employee Security Training and Awareness Initiatives

11.2. Mandatory Employee Security Training and Awareness Initiatives

Many network security failures are the direct result of phishing and other social engineering methods that target users. Such dangers cannot be eliminated with technical measures alone. Recent data from the ITRC (Identity Theft Resource Center) cite phishing, ransomware/malware, and skimming as the primary vectors of attack in 63% of overall breaches reported.

XYZ Company currently has mandatory annual security awareness training through its provider. Supplemental training is provided via a subscription to the KnowBe4 service.

12. USER & WORKSTATION MAINTENANCE

12.1. Remove inactive user accounts from network resources and company services.

Legacy accounts relating to former users, unused services, and inactive vendors pose a security risk. Ex-employees and former vendors may be in possession of access credentials, and unused credentials may predate stricter security measures, leaving them with weak or non-expiring passwords that could be breached by malicious parties.

Currently, any user accounts for former users, services, and vendors that are no longer required (ex. for a terminated employee) are set to inactive and the password is changed.

At the time of Inspection, there were six Active Directory accounts that had not logged in within the past 90 days:

- Jim Maloney
- Rick Socha
- Tamara Savinsky
- Horace Helmsworth
- Sue Pham

Is recommended that these accounts be reviewed and removed if they are determined to no longer be required for ongoing use, archival or discovery purposes.

12.2. Remove inactive workstations from Active Directory.

When a workstation is no longer used, its domain account should be removed to simplify management and administration. Such helps to prevent Active Directory from becoming cluttered, increasing the time required to locate and relocate items for the purposes of security, Windows GP's, etc.

At the time of Inspection , there were two workstations that had not logged into the Active Directory network within the last 90 days:

- SUEPHAM16
- SCAN1

It is recommended that XYZ Company's compliance team and IT personnel devise and implement a formal a policy for removing inactive users from Active Directory

12.3. Remove domain administrator rights from any users that do not require them.

Users who are members of domain administrative groups (Domain Admins, Enterprise Admins, Built-In Administrators, etc.) have full administrative permissions as relate to domain-attached resources on the network. Such should be understood to include the possibility of accessing any data stored on those resources.

Given that they grant largely unfettered access, domain administrative rights should be assigned very carefully and sparingly, with serious consideration being given to the risks posed by the assignment of rights. At the time of Inspection, no users were granted administrative rights on the Active Directory domain. There are no additional recommendations at this time.

STATUS SUMMARY REPORT

Status	Topic	Section Number	Page Number
	DOCUMENTATION	**1**	**2**
🟥	Maintain diagrammatical representation of network architecture, equipment elevations, and formal inventory	1.1	2
🟩	Create formal IT Policies	1.2	2
🟥	Create formal IT security standards	1.3	2
🟥	Create formal employee onboarding & termination procedures	1.4	3
🟥	Overseas travel, Nation-specific travel policies (smart phone & VPN, encryption recommendations, legal restrictions)	1.5	3
🟥	Replacing End of Life equipment	1.6	3
🟥	IT Budget/Forecasts	1.7	3
🟥	Purchase asset tags and implement tracking system. (Dual category I.T./Fixed Asset, depreciation, coordinate with finance.)	1.8	4
🟩	Create incident response plan for responding to and managing cybersecurity events, and to mitigate negative effects and restore operations.	1.9	4
🟥	Create Technology Vendor Questionnaire, implement review process, maintain records for outside vendors	1.10	5
🟥	Request and maintain copies of third party security audit/compliance results from outside software vendors, hosts, etc. (Backup services, Web hosts, etc.)	1.11	5
🟥	Establish system for classifying sensitive data & security requirements	1.12	5
🟥	Maintain user documentation including a list of any authorized non-standard configurations (power users, third party services, etc.)	1.13	5
🟥	Create formal procedures for Change Management	1.14	6

	GENERAL NETWORK	2	6
🟩	Implement one or more business class firewall appliances to restrict direct outside access.	2.1	6
🟥	A minimum of two WAN connections should be implemented to increase Internet stability.	2.2	6
🟥	Implement HA (High-Availability) for optimal firewall device uptime. (Requires purchase of second firewall, usually at a slightly lower cost than the primary firewall.)	2.3	7
🟩	Gateway Antivirus	2.4	7
🟩	IPS (Intrusion Prevention Service) / Stateful packet Inspection of traffic traversing gateway.	2.5	7
🟥	Web content filtering (Firewall Level)	2.6	8
🟥	SSL Traffic Inspection	2.7	9
🟥	Require password complexity & minimum length.	2.8	9
🟥	Enforce mandatory password change requirement.	2.9	10
🟥	Enforce discrete passwords for network devices and cloud services	2.10	10
🟥	Enforce unique credentials for administrative users	2.11	10
🟩	Limit the number of concurrent inbound connections and activate DDOS protection	2.12	11
🟥	Enable Geo-IP Filtering.	2.13	11
🟥	Close all non-essential firewall ports, protocols and other services.	2.14	11
🟩	Spam/Malware Pre-filtering	2.15	12
🟩	Perimeter firewall protection to segment wireless from corporate LAN.	2.16	12
🟥	Implementation of Multifactor authentication for domain and other systems.	2.17	12
🟩	Servers and confidential information (to the extent possible) to be maintained in an internal zone, behind a DMZ.	2.18	13

🟥	Discuss direct access restrictions & necessary accommodations for essential vendors/services. Document any compromises and disseminate to management for explanation & authorization.	2.19	13
🟩	Minimum WPA2 encryption for all wireless	2.20	14
🟥	Implement an enterprise-class, controller-based wireless network.	2.21	14
🟥	Separate, segmented wireless networks with discrete SSID's for guest, employee BYOD and IoTS use purposes.	2.22	14
🟥	Implement segmentation of corporate network & procedures specifically geared toward the protection of financial data.	2.23	14
🟥	Limit server roles (i.e., single role per server, file, DC, etc.)	2.24	15
🟥	Consider email keyword scanning for content, limitation of legal exposure (keywords).	2.25	15
🟥	Consider Web use monitoring (security, productivity)	2.26	15
🟥	Scheduled/automated LAN traffic analysis.	2.27	16
🟥	Allow remote administrative access only via encrypted connections. (SSH, VPN, TLS, SSL)	2.28	16
🟥	Segmentation of VM's	2.29	16
🟩	Antivirus/anti-malware for servers.	2.30	17
🟥	Review the use of Skype & IM clients, and the associated risks.	2.31	17
🟥	Implement DNS filtering solution	2.32	17
🟥	Implement battery backup/power continuity system	2.33	17
🟥	Fire suppression for network equipment	2.34	18
	USER & USER WORKSTATIONS	**3**	**19**
🟥	Implement drive encryption for laptops & user workstations.	3.1	19
🟥	Automate deployment of patches & fixes (Windows updates alone do not meet requirement)	3.2	19
🟥	Disallow local administrative rights on user workstations.	3.3	19

🟥	Require password complexity	3.4	20
🟩	Disable USB ports	3.5	20
🟩	Antivirus/Anti-Spyware on all workstations, automated deployment of virus definition updates.	3.6	20
🟩	Supported operating systems only	3.7	21
🟥	Set screen savers to lock automatically after a period of inactivity. (Suggest maximum unattended time of 15-30 minutes)	3.8	21
🟥	Prohibit remote access methods that are not approved and formally documented.	3.9	21
🟥	Adopt formal hardening standards for all workstations	3.10	21
🟩	Do not permit users to attach to third party storage services (ex. iCloud, Dropbox, Hightail, etc.) without the express authorization of IT.	3.11	22
	MOBILE DEVICES	**4**	**23**
🟥	Mobile Device Manager for remote wipe/disabling/management of mobile devices	4.1	23
🟥	Restrict the ability to access the organization's email systems from mobile devices without prior authorization of both management and I.T.	4.2	23
🟥	Destruction or indelible marking of mobile devices used in nations considered 'hostile', prohibit use of said devices outside of such nations.	4.3	24
🟥	Implement an encrypted calling platform for use abroad.	4.4	24
🟥	Device encryption & secure instant messaging	4.5	24
	WEB, CLOUD & OFF-SITE PROVIDERS	**5**	**25**
🟥	Develop and implement security standards for the consistent secure deployment of XYZ Company's Web properties.	5.1	25
🟥	Employ the use of TLS/SSL Certificates for XYZ Company's Website properties.	5.2	25
🟥	Web host security	5.3	25

🟥	Check integrity of website code	5.4	25
🟥	SPF and DKIM implementation	5.5	26
	TELEPHONY	**6**	**27**
🟥	Implement LSP (Locally Survivable Processor) for telephony solution to provide automatic failover/redundancy in the event of an equipment outage.	6.1	27
🟥	Implement redundant voice connectivity for continuity in the event of a telephone carrier outage.	6.2	27
	BACKUP & DISASTER RECOVERY	**7**	**28**
🟩	Implement local incremental file backup solution w/on and off-premises virtualization capability	7.1	28
🟥	Implement redundant backup of the organization's Cloud-based email environment	7.2	28
🟩	Implement a Disaster Recovery plan	7.3	28
🟩	Residential backup	7.4	29
	INSURANCE & RISK MANAGMENT	**8**	**30**
🟩	Cyber-insurance coverage	8.1	30
	PHYSICAL SECURITY	**9**	**31**
🟥	I.T. room access control	9.1	31
🟥	Surveillance cameras and card access control	9.2	31
🟥	Visitor access logging/control	9.3	31
	AUDITING / VERIFICATION	**10**	**32**
⬜	Scheduled test of surveillance camera functionality	10.1	32
🟥	Adopt outside penetration testing schedule (Third party)	10.2	32
🟥	Review of firewall port configuration	10.3	32
🟥	Review firewall firmware revision	10.4	32

🟩	Review firewall logs to identify potential attacks	10.5	33
🟥	Miscellaneous third-party service and other auditing/analysis	10.6	33
🟥	Regular backup functionality verification	10.7	33
🟩	Review of passwords; verify removal of default vendor passwords.	10.8	33
🟥	Application review, confirm only authorized software installed.	10.9	34
🟩	Audit Requirements Checks - MPAA, Sarbanes Oxley (SOX), FINRA, SEC, HIPAA, etc.	10.10	34
	INFORMATION SECURITY POLICIES FOR USERS	**11**	**35**
⬜	Information Security Policies	11.1	35
🟩	Mandatory Employee Security Training and Awareness Initiatives	11.2	35
	USER & WORKSTATION MAINTENANCE	**12**	**36**
🟥	Remove inactive user accounts from network resources and company services.	12.1	36
🟥	Remove inactive workstations from Active Directory.	12.2	36
🟩	Remove domain administrator rights from any users that do not require them.	12.3	36
🟥	Check company emails against third-party breach disclosures.	12.4	37