Demian Jennings

Professor DeAndre Favors

ACC Cybersecurity Block 2

06 August 2022

Research Project

Altamaha Tech Incorporated has recently contracted a third party to a security firm to review and audit our current cyber security posture. As a result of that audit there were several areas of concern that we as a company need to address. This paper will address the concerns of the security audit that was conducted.

Assessment Techniques

The investigators recommended a risk register to monitor, track and calculate risks. We will implement a risk register to assess ongoing risks and threats. The risk register will identify context, identify risks, analyze risk, estimate risk importance, determine and execute the risk response, and identify and respond to changes over time. This document will be used to track and communicate risk information throughout the enterprise. The purpose of our risk register is to :

1. Aggregate risks from adversary threats and system failures that result in adverse impacts.
2. Normalize information across organizational units to provide senior leaders with the information needed to measure cybersecurity risks that would affect enterprise objectives.

3. Prioritize operational risk response activities by combining risk information with enterprise mission and budgetary guidance to implement appropriate responses.

Notional Cybersecurity Risk Register											
ID	**Priority**	**Risk Description**	**Risk Category**	**Current Assessment**			**Risk Response Type**	**Risk Response Cost**	**Rick Response Description**	**Risk Owner**	**Status**
				Likelihood	**Impact**	**Exposure Rating**					

Table 1 - Notional Cybersecurity Risk Register [Stine,15]

ID (Risk Identifier)	A sequential numeric identifier for referring to a risk in the risk register
Priority	ordinal value (e.g., 1, 2, 3) or in reference to a given scale (e.g., high, moderate, low)

Risk Description	A brief explanation of the cybersecurity risk scenario (potentially) impacting the organization and enterprise. Risk descriptions are often written in a cause and effect format, such as “if X occurs, then Y happens”
Risk Category	An organizing construct that enables multiple risk register entries to be consolidated (e.g., using SP 800-53 Control Families: Access Control (AC), Audit and Accountability [AU] as illustrated in Figure 7). Consistent risk categorization is helpful for comparing risk registers during the risk aggregation step of ERM
Current Assessment – Likelihood	An estimation of the probability, before any risk response, that this scenario will occur. On the first iteration of the risk cycle, this may also be considered the initial assessment
Current Assessment – Impact	Analysis of the potential benefits or consequences that might result from this scenario if no additional response is provided. On the first iteration of the risk cycle, this may also be considered the initial assessment
Current Assessment – Exposure Rating	A calculation of the probability of risk exposure based on the likelihood estimate and the determined benefits or consequences of the risk. Throughout this report, the combination of impact and likelihood is referred to as exposure. Other common frameworks use different terms for this combination, such as level of risk (e.g., ISO 31000, NIST SP 800-30 Rev. 1). On the first

	iteration of the risk cycle, this may also be considered the initial assessment
Risk Response Type	The risk response (sometimes referred to as the risk treatment) for handling the identified risk. Values for risk response types are listed in Table 3 and Table 5 of this document
Risk Response cost	The estimated cost of applying the risk response
Risk Response Description	A brief description of the risk response. For example, “Implement software management application XYZ to ensure that software platforms and applications are inventoried,” or “Develop and implement a process to ensure the timely receipt of threat intelligence from [name of specific information sharing forums and sources]
Risk Owner	The designated party responsible and accountable for ensuring that the risk is maintained in accordance with enterprise requirements. The Risk Owner may work with a designated Risk Manager who is responsible for managing and monitoring the selected risk response
Status	A field for tracking the current condition of the risk and any next activities

Table 2 - Notional Cybersecurity Risk Register guide [Stine,16]

Physical Threats and Vulnerabilities

Altamaha Tech is located in the Grixdale Farms neighborhood of Detroit Michigan. According to the site areavibes.com [areavibes,1]. Total crime in the area is 233% higher than the national average. Violent crime is 512% higher than the national average, and property crime 178% higher than the national average.

Altamaha Tech is a textile manufacturer. There is an inherent threat from flammable textiles. We must address the risk of fire . Our Fire Protection system will include smoke and flame detectors located in all vulnerable areas. The fire suppression system will have fire extinguishers located around the facility as well as a fire sprinkler system for all manufacturing and storage facilities. Due to the risk of crime we must also implement property and safety precautions. The entire premises will be fenced off as well as a security gate to enter the property which will require an employee badge to enter or an escort on to the property. The front entrance will have Bollards installed at the front entrance of the building leading to the main entrance where the reception will be manned with security personnel. There will be an electronic door installed leading from the security desk to the working area. The guards will screen all employees and visitors at the main gate and entrance, documenting all names about visitors, conducting patrols on the premises. A visitor log will be maintained recording entry and exit information. CCTV will be installed in all areas of the premises. Electronic locks will be installed in sensitive areas which will require badge access. Warning signs of restricted areas will be posted. The current alarm system will be improved to include window breakage detectors as well as sensors to indicate if opened. The plant will be divided into security zones based on location and function. CCTV will include Day and Night CCTV cameras and Dome CCTV cameras for indoor activity.

Logical(Technical) Threats and Vulnerabilities

In addition to Physical threats we must also protect against logical threats. We must have controls in place restricting access to devices in order to protect the integrity of sensitive data. The components of technical security controls include:

- System access controls. System access controls are used for the restriction of access to data according to sensitivity of data, clearance level of users, user rights, and permissions. Access to data will be based on a need to know basis.
- Network access controls. Network access controls offer various access control mechanisms for network devices like routers and switches.
- Authentication and authorization. Authentication and authorization ensure that only users with appropriate privileges can access the system or network resources.
- Encryption and Protocols. Encryption and protocols protect the information passing through the network and preserve the privacy and reliability of the data.
- Network Security Devices. Network security devices such as firewall and IDS are used to filter and detect malicious traffic, thus protecting the organization from threats.
- Auditing. Auditing refers to the tracking and examining of the activities of network devices in a network. This mechanism helps in identifying weaknesses in the network.

Acceptable Use Policy(AUP)

Our Acceptable Use Policy and Password policy is dictated below. Users must not visit gambling sites, sites containing pornographic material, torrent sites.

Password Policy-

- 8 – 14 characters
- Contain uppercase and lowercase letters, numerical digits, and special characters (@,%,$,&, _ , or ;)
- Passwords must be unique and cannot be reused. Maximum password age: 90 days
- Avoid using personal information and use of company name in the password is prohibited

Password Best Practice-

- Do not share your computer user account details.
- Do not keep a common password for all accounts.
- Do not share passwords.
- Never write the password anywhere.
- Employees should not communicate their password through email, phone, or instant messages to anyone.
- Do not leave the machine unattended. Always log off or lock the system when leaving the desk.

Mobile Device management

- Disable interfaces such as Bluetooth, infrared, and Wi-Fi when not in use
- Set Bluetooth-enabled devices to non-discoverable mode

- Avoid connecting to unknown Wi-Fi networks and using public Wi-Fi hotspots
- Connect the mobile devices to encrypted Wi-Fi networks only
- Configure web accounts to use secure connections
- Isolate a group of users using different SSIDs and segment the traffic for these groups to different VLANS
- Apply different firewall rules and filters to different combinations of user groups or devices
- Configure web accounts to use secure connections

Personally Identifiable Information Policy

Altamaha Tech Inc. develops, manufacture, sell and service wearable medical

devices. The medical devices collect sensitive data about the patients that utilize

the devices. In order to comply with GPDR and PCI-DSS specifications, we will be implementing and drafting new policy documentation. A full disclosure document that states exactly what medical data is being recorded and the purpose that it is used for, will be part of our terms and conditions. So for example, if we are monitoring the heart rate, we will only have the data that is associated with collecting the heart rate information and nothing else like say blood sugar.

The data will be collected for the specified time frame by the user and be discarded within 30 days after collected unless specified differently by the user. User data will be verified by the user and the user will have the option of which data to keep persistent. Data will not be shared with any 3rd party. This policy will be audited every 60 days to ensure compliance. Stored data will be encrypted at rest

PCI-DSS

The network will have its own payments and processing segment and will be on its own dmz behind a firewall in accordance with PCI-DSS requirement no. 1.3.1. All network transmission with sensitive payment information will be executed with encrypted data and stored at rest in an encrypted database. Payment processing will be handled by Stripe. All payment details retrieved and sent from our payment portal to stripe will also be encrypted. The network itself will have nightly backups and the anti-virus software is set to automatically download and install the anti-virus software in accordance with our Vulnerability Management Program. Access to customer payment data will be restricted to the payments and processing department manager and those whose specific job function needs that data. Every member of the payments and processing team will be assigned a Unique ID that each employee will have his ID associated with all of their transactions. The server room where cardholder data is stored will be secured with electronic locks accessible with badge entry and special permissions limited only to designated personnel. Our server entry log is maintained by the group manager, containing all names and id's of authorized personnel.

Continuous Security Monitoring

Network traffic signature is defined as a signature set of characters that define network activity, including IP addresses, Transmission Control Protocol (TCP) flags,and port numbers.Before Network traffic can be analyzed, we must first establish a normal traffic signature.

Normal Traffic Signature should contain [EC-Council, 1094]:

- To establish a three-way handshake, TCP uses SYN, SYN ACK, and ACK bits in every session.
- The ACK bit should be set in every packet, except for the initial packet, in which the SYN bit is set.
- FIN ACK and ACK are used in terminating a connection. PSH FIN and ACK may also be used initially in the same process.
- RST and RST ACK are used to quickly end an on-going connection.
- During a conversation (after a handshake and before termination), packets only contain an ACK bit by default. Occasionally, they may also have a PSH or URG bit set.

Suspicious Traffic Signature will have one or more of the following [EC-Council, 1094]:

- If both SYN and FIN bits are set, the TCP packet is illegal.
- SYN FIN PSH, SYN FIN RST, and SIN FIN PSH RST are all variants of SIN FIN. An attacker sets these additional bits to avoid detection.

- A packet having only a FIN flag is illegal as FIN can be used in network mapping, port scanning, and other stealth activities.
- Some packets have all six flags unset; these are known as NULL flags and are illegal.
- The source or destination port is zero. If the ACK flag is set, then the acknowledgement number should not be zero.
- If a packet has only the SYN bit, which is set at the beginning to establish a connection, and any other data is present, then it is an illegal packet.
- If the destination address is a broadcast address (ending with 0 or 255), it is an illegal packet.
- Every TCP packet has two bits reserved for future use. If either or both are set, then the packet is illegal.
- All conversations originating inside the demilitarized zone (DMZ) are trusted traffic items.
- Any traffic violating the network policies is malicious traffic, e.g., the existence of File Transfer Protocol (FTP) traffic when this type is restricted indicates a potential issue.
- Any Dynamic Host Configuration Protocol (DHCP) traffic from unknown DHCP servers indicates a rogue DHCP server.
- Mail traffic originating in the network but not sent to a mail server is suspect.
- Any DNS traffic not sent to the DNS server is suspect. Any outgoing traffic with internal addresses not matching the organization’s address space may be malicious.

Network monitoring will be done with Wireshark. The Setup procedure is as follows -

1. setup all special privileges required to start a live capture
2. set the correct interface to capture packet data. In most cases it will be eth(ethernet)
3. Set the location in the network to monitor
4. Start capturing data.

Monitor traffic for volume, malicious activity, policy violation attempts and applications using unnecessary/restricted services.

Continuous Education

Altamaha Tech Inc. develop, manufacture, sell and service wearable medical. When an employee is hired, security training will be given on an online portal that must be completed in the first week of employment and renewed yearly, also on the online portal. Quarterly sessions will also be given which attendance is mandatory. Topics covered are:

- Expertise to defend themselves and an organization against threats;
- Follow security policies and procedures for working with information technology;
- Know whom to contact if they discover a security threat;
- Should be able to identify the nature of data based on data classification;

- Protect the physical and informational assets of an organization when the employees come into contact with them—for example, contacting with information;

- Know how to handle critical information such as review of employee non disclosure agreements;
- Know the proper methods for protecting critical information on systems with password policy and the use of two-factor authentication;
- Know the consequences of failing to secure information, which may result in employment loss;

Physical security training-

- Minimize breaches
- Identify the elements that are more prone to attack
- Assess the risks handling sensitive data
- Ensure physical security at the workplace

The training or awareness program should

- Provide methods to reduce attacks;
- Examine all devices and the chances of a data attack;

- Teach the risks of carrying sensitive information;
- Teach the importance of having security personnel;
- Inform employees about whom should report to about suspicious activities;
- Teach what to do when employees leave systems and workplaces unattended; and
- Teach the disposal procedures for disposing critical paper documents and storage media.

Employee Awareness and Training: Social Engineering

Areas of risk, Attack Techniques, Train employee/Help Desk on

phone, Impersonation,Not providing any confidential information, if this

has occurred

- Dumpsters, Dumpster Diving, Not throwing sensitive documents in the trash
- Shredding document before putting into the trash
- Erasing magnetic data before putting into the trash
- email,Phishing, malicious attachment,Differentiating between legitimate email and a targeted phishing email.Not downloading malicious attachment

Some of the social engineering techniques the employees should be aware of include:

- Physical social engineering (tail-gai ng, piggy-backing);
- Changing passwords (attacker poses as an authority and asks to change the username and password);
- Name-drop (using the higher authority's name to gain access to something);
- Relaxing conversation (trying to build up a rapport with the employee); and
- New hire (attacker poses as a new employee to take a tour around the office).

Continuous operations

A model for development and implementation of a cyber security operations centre(SOC) encompasses human, process, and technology factors. This model was developed based on a review of previous studies and the results of the descriptive analysis, correlation, and regression tests[Majid, 1].

CONCLUSION

The actions covered in the response are just the initial steps that should be taken to address our Cybersecurity concerns. As we discover more about our organization and our cybersecurity readiness we will respond to new threats that we have uncovered.

Works Cited

"Grixdale, Detroit, MI Crime",areavibes, 07 Aug, 2022,www.areavibes.com/detroit-mi/grixdale/crime/

Stine, Kevin.et al. "*NISTIR 8286, Integrating Cybersecurity Enterprise Risk Management(ERM)"*, Oct 2020,U.S. Department of Commerce

EC-Council, *Network Defense Essentials ,* EC-Council*, Albuquerque, NM*, 2021.

Majid, Maziana Abd, "Model for successful development and implementation of Cyber Security Operations Centre(SOC), *PLoS*, e0260157, 2021, 16(11),www.ncbi.nlm.nih.gov/pmc/articles/PMC8604312/