Hajoca Corporation Documentation

Larry Baucum and Timothee Andre

Bowie State university

CTEC 345

Dr. Latson

Company profile

Hajoca Corporation is a wholesaler that serves the United States with HVAC, pool supplies, industrial PVF, and plumbing products (Our brands, 2022). Hajoca has over 400 locally managed locations under 50 trade names (Our brands, 2022). Hajoca’s locally managed locations are spread throughout the United States. Hajoca was founded in 1858 and started as a key stop grinding store for plumbers in Philadelphia (About Us, 2023). Hajoca works with over 500 suppliers to deliver over 100,000 products to local businesses, entrepreneurs, residential, and industrial customers (Services, 2023). According to Dun & Bradstreet Hajoca is headquartered at 2001 Joshua Rd Lafayette Hill, PA.

Hajoca has a main headquarters and product warehouse. The different groups that Hajoca has are executives, sales, operations, marketing, finance, human resources, information technology, customer service, product management, quality assurance, and legal. Hajoca will use hub and spoke WAN and star LAN topologies for their network. Hajoca will use the NIST framework and fall under the Payment Card Industry Data Security Standard and Federal Trade Commission regulations. Hajoca has many assets that require protection including customer and employee information, supplier and subsidiary business information, sales history, networking equipment, logical network, products, product support tools, and physical locations.

Headquarters

A building with a blue awning

Description automatically generated

Product Warehouse



Appropriate authentication credentials

Hajoca will require users to create complex passwords that are made up of a mix of 12 alphanumeric and special characters, an uppercase letter, a lowercase letter, a number, will be case sensitive, cannot contain the username, first name, or last name, no repeating of the same 4 characters, and a special character. Passwords will also be checked against lists of known compromised passwords. Per the requirements of the payment card industry (PCI) we will change our passwords every 90 days. This will allow our users to only need four passwords per year to hopefully reduce the number of passwords necessary to be remembered per year and increase the complexity of the user-generated passwords. Passwords may not be reused for two years. According to NIST, we will use SHA-2 to protect our password digest as it is a known quantity in cybersecurity. SHA-2 has been proven to be an effective cybersecurity tool that is used by the government. This industry standard hashing algorithm should provide CIA for our secrets held within our password digest.

In addition to passwords, we will use multifactor authentication to allow more flexible authentication options. These options will be an authenticator app through the Hajoca Supply Zone app and security key tokens that will allow authentication. Security keys will be used as part of the primary way to authenticate users and will work in tandem with passwords. They will be required to access company resources that when logged in with an authenticated username and password will be prompted to connect their security key via USB or Bluetooth. Security keys and smart cards will be required to access executive areas and server rooms to ensure that access to top-secret and mission-critical resources have an extra layer of security.

Account management procedures

Accounts will be assigned using the principle of least privilege to ensure that users only have access to the resources that are necessary to them. Active directory will be used to facilitate single sign-on across all Hajoca resources, permission control across all accounts, and access control for on-premises users and off-premises users. Single sign-on will be key due to Hajoca’s many subsidiaries and suppliers that reside across the United States. We will use security assertion markup language for federation within active directory. Guest, shared, and generic account types will be disabled to lessen the attack surface. Group policy will be implemented to ensure that accounts are properly grouped according to their department. Account placement and privileges will be continually reviewed to ensure that as the organization changes and grows accounts remain in their proper place. Doing this will ensure that the ability for a threat actor to move laterally remains limited. Any account creation, termination, and modification will need to be validated by an administrator. All account events will be documented and reviewed to ensure no malicious activity was conducted and to search for vulnerabilities. Account deactivation will be triggered by employee termination, transfer, or lack of necessity. Accounts will have protection against various password attacks through account lockouts. Accounts will be placed into lockout after 3 unsuccessful login attempts. The duration of the lockout will increase if another lockout is triggered consecutively. After two lockouts the account can only be unlocked by an administrator. Accounts will also have an auto logoff timer tied to inactivity to lessen the ability for data compromise. that will Account events will undergo regular monitoring to detect anomalous account behavior. Our configurations will be continually audited to ensure that our security has the least amount of vulnerabilities and attack vectors.

Access control management and controls

Hajoca will use role-based access control to ensure that the principle of least privilege is kept consistent. Our administrators who manage access control will be separated into auditors and function controllers. We will implement firewalls to protect our databases that contain sales, customer, and employee information. These firewalls will contain inbound and outbound rules that will help to control the flow of traffic within our network. Inbound rules will check source and destination IP addresses to ensure that the information is coming from an authenticated user. Outbound rules will be set that will block traffic that comes from unauthorized protocols and IP addresses. Firewalls will reference lists of known malicious entities that will be contained in an ever-updating blacklist. There will also be a required system notification that will be triggered at every login screen providing information on acceptable use of organization resources and failed login penalties.

Using a class A IP address range we will be prepared for future growth and events that may require many IP addresses to be assigned when most or all employees are working on-premises and many suppliers and subsidiaries are connecting simultaneously. We will likely never worry about running out of IP addresses, but there will be more than enough space for any future needs. The subnet for the headquarters is 28.185.0.1. The subnet will be split into vLANs for our different groups which are executives, marketing, finance, sales, human resources, legal, quality assurance, product management, customer service, and information technology. Each group will receive proper privileges based on what they need to access. There is also a subnet for the product warehouse 28.185.32.1 that follows the same grouping and naming structure as the headquarters. IP address management will be handled by our IPAM and DHCP servers. IPAM will ensure that our DHCP scopes are appropriately corresponding to their respective groups. IPAM will allow our administrators to centrally manage IP addresses so that we can track and audit our IP address usage and allocation. DHCP and IPAM will also be used to reserve and exclude IP addresses to ensure that only authorized IP addresses are being used making anomalous activity easier to detect. Only administrators will be able to access and manage our IPAM, DHCP, and DNS configurations.

Our network and endpoint devices will have many layers that protect them. Starting with the policy that must be followed by employees. Our employee policies will be the beginning of our layers. We will implement strict rules that disallow phones to be used for work, work-relevant documents or files may not be left unattended, devices must be logged off, no attempts to recreationally web browse on organization devices, no tampering with company devices whether it is using software or hardware, and more. We will monitor employee activity and provide constant security awareness training especially as policies are changed. All endpoint devices that connect to company resources must have antivirus/antimalware. Our chosen hashing SHA-2 must be used for all sensitive data. Our intrusion detection system and intrusion prevention system allow us to detect vulnerabilities and attacks to mitigate the impact of malicious events. Our IDS and IPS will fall under the management of our SOAR and SIEM products. Allowing us to have better supervision of security events happening in our system. We will be able to set up dashboards that will allow us to see anomalous behavior and alert notifications that will allow us to respond to incidents promptly.

We will use VPN servers working together to handle load balancing and redundancy to ensure that we can handle the large number of connections from subsidiaries and suppliers. We will protect file transmission with FTPS. There will be filtering for data types and approval will be required for unusually sized file transfers. Similarly, we will use SMTPS for email protection. There will be filters set up to block known spam email attempts that will be updated through employee reporting and online security resources to limit known threats. Our connections with subsidiaries and suppliers will be handled using a VPN to encrypt confidential data transfer. Our radius server will be configured to handle authentication, authorization, and accounting for all VPN connections.

Our applications and operating systems will be regularly updated to guard against vulnerabilities. We will whitelist preapproved applications to ensure that rogue or malicious applications cannot be installed onto our endpoints. This will be accompanied by monitoring and reporting of malicious software installation attempts to uncover hidden threats and vulnerabilities. We will continue to harden our systems by disabling unnecessary protocols, services, and features as recommended by vulnerability scanning and continued auditing. Our filesystems will also employ encryption using features like BitLocker that will enable our files to remain secure in the event of an incident. Below is a simple diagram of the way our system will connect with our sites and suppliers.

Internet

Firewall

Inter site

Edge Router

Supply

Core switch

Warehouse

Hq

Sub

Plans for Physical Security:

Access control: having access cards, locks, other systems that restrict access to servers, inventory, and sensitive information to the business.

Fences, surveillance cameras, intrusion detection systems that monitor the unauthorized people or threats.

Making sure networking equipment is secure such as servers, routers and other endpoints being locked away for protection against unauthorized people, or damage.

Have security awareness training to employees on best practices and procedures.

Vulnerability assessment strategy:

To assess vulnerabilities, Hajoca will conduct penetration testing to uncover vulnerabilities and then exploit them, just as a threat actor would. They will also be doing vulnerability scans in order to continuously identify vulnerabilities and monitor cybersecurity progress.

Organizational Security

A) Explain the components of a business continuity plan, such as contingency planning, incident response, emergency response, backup, and recovery efforts.

Contingency plans are tactical solutions addressing a core business resource or process, such as how to handle the loss of a specific vendor. It involves finding potential risks in a business and making a strategy to mitigate them. This includes scenarios like natural disasters, cyber-attacks, or equipment failures.

Incident response is a set of written instructions for reacting to a security incident. There are six steps to be taken when an action occurs.

Preparation: Equipping IT staff, management, and users to handle potential incidents when they arise.

- Identification: Determining whether an event is a security incident.

- Containment: Limiting the damage of the incident and isolating those systems that are impacted to prevent further damage.

- Eradication: finding the cause of the incident and temporarily removing any systems that may be causing damage.

- Recovery: After ensuring no threat remains, permitting affected systems to return to normal operation.

- Lessons Learned: Completing incident documentation, performing detailed analysis to increase security and improve future response efforts.

Emergency responses are the immediate actions taken to preserve lives and safeguard property and assets, such as an evacuation plan.

Backup and recovery efforts are measures taken to protect the businesses data, systems, or assets from loss or damage. Examples of this are regular data backups, offsite storage, and redundant systems.

B) Describe a disaster recovery plan that ensures minimal downtime and quick recovery.

A disaster recovery plan is the recovery and resumption of critical technology assets in the event of a disaster. It is a written document that details the process for restoring IT resources following an event that causes significant disruption in service. To minimize downtime and have a quick recovery, Hajoca would need to create a restoration order that works for the business. They would need to prioritize restoring the network before other applications that rely on the network are restored. Critical systems must be restored before other systems.

Security Policies

Hajoca will have account management policies, that are restrictions to user accounts. This is who is authorized to access resources, and when, how, and where they can do it. Example: credential policies for making passwords.

There would be an asset management policy; that provides the guidelines and practices that govern decisions about how assets should be acquired, maintained, and disposed of.

Respond

Hajoca’s plan in the event of a system failure is to move all essential personnel to the product warehouse that doubles as a hot site until full system restoration is possible. The leads of the IT department and lead supervisor will receive the contingency plan so they can act swiftly when the headquarters essentially personnel moves to the warehouse for temporary operations. As best as we possibly can we will try to keep downtime minimal using redundant servers and backups. The biggest objective in recovering from a system failure or disruption will be to ensure that sensitive data and business operations can be swiftly restored. We will try to maintain a three nines level of availability to ensure that connections we can connect with customers and uphold a reputation of reliability. Our plan will be constantly audited and reapproved by the top administration to create the best chance to maintain business continuity. All incidents will be logged to prevent future incidents. We will run disaster activities with all employees so that all personnel are well trained in the event of a disaster. Not only will employees be well trained in the event of a disaster, but they will also be trained to look for and report signs of an impending disaster. Employees can then report these signs of a disaster to potentially avoid the issue or respond faster and minimize the impact it could have.

Identify

Hajoca will take inventory of all network devices, endpoints, and accompanying hardware. Hajoca will also take account of their serial numbers, location, configurations, and attached devices such as peripherals. Our inventory will be regularly reviewed to ensure that errors and discrepancies are addressed. Our inventory practices will also be audited to ensure our accounting maintains its integrity. Any changes to the inventory will be logged and monitored to ensure that malicious activity is not present and the inventory complete.

Hajoca’s transaction data, employee and customer personally identifiable information data, and supplier data are top secret. Secret data is the location of our network equipment, servers, product research, and product warehouse inventory. Our endpoint locations and marketing research are confidential. Our criteria for defining what is critical to our organization is the impact on business operation, impact on reputation, and impact on CIA of sensitive data. We will analyze every asset in our organization to create a critical analysis of mission-critical assets and how they should be accessed. We will use this analysis to define and redefine as necessary what assets are critical.

Hajoca will perform risk assessments to find ways to best protect our reputation, business relationships, products, subsidiaries, customer data, and employee data. We will have a team do quarterly risk assessments that will include management, security, operations, and IT employees. The scope of our risk assessment will envelop the headquarters, product warehouse, and different regional subsidiaries to get different perspectives of where risk can arise. Our risk assessment will allow us to determine what risks threaten our organization and if they should be mitigated, avoided, accepted, or handled by a third party. Every facet of the risk assessment will be monitored and logged. Our risk assessment process will be audited after each assessment to continually improve our risk assessments. Our risk mitigation plans will rely heavily on risk assessment data. We will assign customer data as a medium risk that we must mitigate through authentication by sales associates. Employees will be a high risk that we accept as they are needed for business operations. Supplier relationships are high risk due to the access that they will have when connecting with our network.

Risks arise with our connections which are remote access VPN, cat cabling through the headquarters and the warehouse, and access points. We will secure our connections with multifactor authentication, strong password requirements, account lockouts, restrict access from known risks using next generation hardware firewalls at the network edge, and use software firewalls at on-prem endpoints, and regular software updates. We will protect our cabling using plenum-rated cables, allowing enough space to reduce heat, and use flame retardant cable accessories. Our access points will be protected using our physical security measures such as locks requiring tokens, on network equipment and doors to network equipment, access point range will be adjusted to not bleed outside of authorized areas, restricting access based on IP address, and requiring multifactor authentication upon requesting network access. Our monitoring software will also detect anomalous and malicious activity. We will log every event and audit our practices with all connections both physical and software to learn and improve our security strategies.

Hajoca is privately owned so our security controls and risk assessments will be authorized by the owners, suppliers, and subsidiaries to ensure that our risk assessment plan is aligned with every appropriate party's security expectation. This includes our Chief Information Security Officer, Security analysts, security engineers, and security operations center analyst for our cyber security personnel. Our stakeholders are our owners, suppliers, customers, subsidiaries, and employees. Our first step will be to create a detailed document that contains tables that identify asset vulnerabilities. We will outline our expected response time and the potential footprint of the vulnerability being exploited. Those assets will be products, sensitive customer and employee data, supplier information, sales history, financial records, Hajoca app data, and subsidiary sensitive information. Our cybersecurity team will use public and private threat intelligence data from local, state, and national sources to try to stay ahead of vulnerabilities. We will also constantly scan for internal threats like rogue employees, poor configuration, and poor practices by employees. We will monitor and scan for external threats such as threat actors. We will monitor anomalous behavior in resource utilization, employee endpoint habits, configuration modification, and alerts from our security software. We will next create a list of shared resources such as customer and supplier sensitive information, application access, VPN access to the headquarters network, internet access, and product warehouse access that a subsidiary may require regarding a sale. Shared resources will have an impact score assigned to them that denotes how impactful the compromise of a shared resource would be and the response time to the compromise to mitigate the impact. Using the previously described tables to identify threats

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | 1. Negligible | 2. Minor | 3. Moderate | 4. Major | 5. Catastophic |
| 5 | Team member out sick | Employee miscommunication | Network Congestion | Competitor opens |  |
| 4 | Temporary power outage | Data entry errors | Someone tailgates into warehouse | Client info stolen in breach | Server room overheating |
| 3 | Minor software bugs and glitches | Equipment malfunctions | Successful phishing attack, limited breach | Insider threat from team member | Lawsuit against company |
| 2 |  | Losses due to theft | Accidental file deleting | Loss of staff | Major natural disaster |
| 1 |  |  | DNS poisoning attack | Extended power outage | Internet loss for entire company |

will allow us to assign risk scores to be represented in a threat matrix. Our risk response list will

be updated quarterly with local, state, and national threat intelligence data and cyber security advisors to ensure the safety of Hajoca assets. Our risk assessment will undergo auditing from our cyber security specialist and third-party cyber security specialist during planned training activities.

We will also perform quarterly security awareness training for all employees and send weekly emails to all employees containing safe practices, social engineering threats, and emerging cybersecurity threats. The information will be sent daily to all cybersecurity professionals through threat intelligence feeds. We will regularly update software after checking for potential vulnerabilities in patches.

Detect

DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed AC-4, CA-3, CM-2, SI-4

By using endpoint software firewalls, next generation firewalls at the network edge, segmentation, and a DMZ for external connections we can control how data flows through our network. Hajoca will vulnerability scan every section of the network daily. We will also perform yearly pen testing using third party testing services to get a different perspective on our security infrastructure. Using RBAC and active directory we will standardize our configurations across our network. Our CISO will authorize and audit our configurations monthly. For monitoring, we will use SIEM to monitor, log, alert, and respond to anomalous and malicious activity. Accompanying that will be endpoint antimalware/virus software on every device that connects to our network. Security analysts will aggregate and analyze logs created from monitoring software. Using rate limiting and traffic filtering we can mitigate denial-of-service attacks. Our accounts will be analyzed by user behavior analytics reviewed by security analysts. We will restrict users from installing unauthorized software onto our machines and require employees to review and accept software usage rights. We will monitor physical access to sensitive areas with CCTV and use security tokens to limit access to authorized personnel only. All physical security devices will be inventoried regularly. The inventory will be audited regularly for accuracy and completeness. Our personnel will all be screened with background checks and reference checks.

Security Operations Analysts will monitor security alerts and investigate potential threats. The incident response team will respond to and mitigate the security incidents. The network security engineers will design and maintain security controls for Hajocas network. Security trainers will be used to provide best practices to employees and how to identify security incidents. To meet with standards that align with Hajocas organizational policies, there will be a compliance review, regular audits to check compliance, and training and awareness to employees. Collaborating with legal teams will also ensure that regulations are being met within Hajoca. Hajoca will test detection processes to ensure effectiveness. Penetration testing to simulate various threats and identify weakness in a network. Red team exercises that will simulate attacks and try to find vulnerabilities. Lastly, Hajoca will have incident response drills in order to improve on how to detect security incidents.

Hajoca will have established communication channels meant for reporting on threats that have been detected. Microsoft teams will be used to communicate during such events. Stakeholders such as senior management, legal teams, and IT personnel that need to know about security events will be notified. Escalation paths will be established, to where incidents can be responded to based on severity. To stay ahead of growing technology, and evolving cyber threats, Hajoca will have to continuously improve detection processes. Have to regularly analyze data to find patterns and trends in cyber incidents, have continuous monitoring or network traffic, system logs, and use IDS, IPS, and SIEMs. Hajoca will continuously look at new technologies and stay informed on evolving technologies. Investing in new training and education for personnel will also improve detection processes.

Recover

After going through cybersecurity incidents, Hajoca will have a recovery plan in place that involves post-incident analysis, and recovery strategies in case of similar events happening again. Logs, incident reports, and interviews with people involved will be reviewed to learn from these incidents. The recovery plans will identify what went well, what can be improved, and recommendations for future references. The recovery plan will be continuously updated to make sure Hajoca is able to recover more efficiently from cybersecurity incidents.

Protect

To focus on protecting account access, Hajoca will have systems ensuring only authorized users can access to accounts and systems. Multi-factor authentication will be used to add security when verifying user accounts from clients, and employees. The principle of least privilege will be used so that users only have the required permissions for their roles. Hajoca will have systems in place that will ensure the physical security of assets, data, and other systems. Physical barriers such as gates, fences, security guards, and surveillance systems will be used to protect Hajocas assets. A badge and other measures will be required to enter buildings to verify authorized personnel. Hajoca will have to encrypt sensitive data stored in servers, and databases which will ensure that if unauthorized access happens, the data is unreadable without decryption keys. They will use TLS protocols to encrypt the data between inventory software and databases. Endpoint data loss prevention will be used on warehouse systems for the security of data.

Roles in the company will be defined, and access permissions will be assigned to each role based on their tasks. Access control lists will be implemented within Hajocas systems, databases, and physical areas. To prevent conflicts of interest and misuse of privilege, separation of duties among staff will be used. The network will be divided into zones based on security requirements, and sensitive data to control access and have the ability to contain security attacks. Using network segmentation on Hajocas network will protect against unauthorized access and other malicious activities.

**References**

*About Us*. Hajoca. (2023, January 20). https://www.hajoca.com/about-us/

*Our brands*. Hajoca. (2022, November 21). https://www.hajoca.com/about-us/our-brands/#:~:text=Founded%20in%201858%2C%20Hajoca%20currently,a%20best%20in%20class%20experience.

Services. Hajoca. (2023b, October 18). <https://www.hajoca.com/our-customers/>

dun & bradstreet. (n.d.). Hajoca Corporation. <https://www.dnb.com/business-directory/company-profiles.hajoca_corporation.84b39c052fe0de124f88a1d7c44258f2.html>

<https://csrc.nist.gov/projects/hash-functions/nist-policy-on-hash-functions#:~:text=SHA%2D3%20(i.e.%2C%20SHA3,that%20employ%20secure%20hash%20algorithms>.

<https://www.auditboard.com/blog/nist-password-guidelines/>

<https://www-s.nist.gov/NCNR-IMS/passwordTips.jsp>

<https://csf.tools/reference/nist-sp-800-53/r5/ac/>