Hikes R Us

Cybersecurity Program

Sylena Beccles

Brandon Morgan

Michael Varrella

Table of Contents

Figures and Tables

1.0 Introduction:

Hikes R Us located in Glassboro, New Jersey provides high-quality outdoor gear tailored for activities popular in the area, such as hiking, kayaking, and birdwatching. Offering both products for purchase and rental. Along with selling equipment, they provide local expert-led guided tours for all activities and interactive workshops to sharpen your outdoor skills. To support their store and website they staff around 10 employees and bring in about $200,000 of annual profits.
Key operations include:

1. Supply & Sell – Supply locals with products for sale/rent for all their outdoor activity needs.
2. Workshops - Host workshops on outdoor skills like navigation, wilderness first aid, and sustainable outdoor practices.
3. Tours - Expert-led guided tours are provided locally for the surrounding New Jersey and Pennsylvania areas.

2.0 Program Foundations

2.1 Objectives & Goals:

Hikes R Us Cybersecurity Objectives

1) Protect the privacy of customers’ and employee's data.
2) Minimize disruption of business operations
3) Maintain the integrity and availability of the system

4) Protect critical assets.

Hikes R Us Cybersecurity Goals

1. Develop a weekly schedule for performing system patches, updates, and backups to provide the newest and most up-to-date security and maintain system readiness and availability.
2. Enhance the security awareness around the company and for all employees involved. Annual training is required, and 85% correctness must be achieved before completion.
3. Create an incident response plan for data recovery, system operations, and business continuation. This plan must be built around the protection of the CIA and have the ability to be implemented immediately.

2.2 Previous Findings:

In the recent audits of Hikes R Us, many vulnerabilities and areas of threat have been identified. Mostly to insider threats, data interception, and unauthorized access to employee accounts and data. Due to the lack of account deletion when it comes to terminated employees Hikes R Us is very susceptible to insider threats. Especially since all accounts have the same access level of administrator. This allows anyone with account information to do a lot of damage to business operations and data. Additionally, it has been identified that no encryption is being used. Meaning that all data is in plain text and is readable by anyone. It is also notable that there is no schedule for updates and patches which is shown by all their software and hardware being very out of date. This itself leaves the business network incredibly vulnerable to whatever those updates and patches were made to fix.

Hikes R Us is striving to make its Business continuity plan as efficient and important as possible. Focusing on data loss, phone/internet failures, and supply/inventory outages they developed a strategic plan to keep their business up and running during what would be some of their hardest times. New policies are being implemented along with intensive testing and routine maintenance to allow for smooth processes. Additionally, they are building relationships with fellow businesses to help support each other in times of need. Most of all the employees are being provided with training on how to react and move forward in these times.

2.3 Budgetary Considerations:

Hikes R Us plans to use 5% of its annual profits to upgrade its cybersecurity throughout the business. Annually they bring in $200,000, and $10,000 of it will be used. This will be used to buy new equipment, upgrade/maintain devices, and perform assessments. With such a low annual budget, there should be consideration taken annually to decide what is needed and highest priority.

1. Needs (subscriptions, new equipment for compliance, fixing what is broken)
2. Maintenance (Firmware/software, performance monitoring, settings updates)
3. Assessment (vulnerability scans)

Expenses:

1) Astra's Vulnerability Scan Assessment - $1,999[1]
2) Cybersecurity Insurance - $1700[2]
3) Google Drive Cloud Solution - $100[3]
4) GTT DLP (Data Loss Protection) Software - $1200 - $10/month per user[4]
5) 1Password Encryption Protection Software – $358.80 - $2.99/month per user[5]
6) Norton Antivirus Software - $180 for 10 devices[6]
7) Break-in Alarm - $3,200 for equipment installation and monitoring subscription monthly[7]
8) 4 Onforu Motion Sensor Lights - $240[8]

[1] Astra Vulnerability Scan Assessment

2 Cybersecurity Insurance

3 Google Drive Cloud Solution

4 Data Loss Protection Software

5 Encryption Software

6 Norton Antivirus Software

[7] Break in Alarm

[8] Onforu Motion Sensor Lights

3.0 Program Framework & Compliance

3.1 Overview:

The leadership of Hikes R Us being the business owner will meet quarterly with IT support to discuss the topic of cybersecurity and how to build a better framework along with keeping up with compliance. Throughout this time ongoing vulnerabilities and threats will be assessed along with strategizing about what should be implemented. These implementations are:

1. Adding, editing, and removing policies.
2. Creating new and improved procedures tailored to the employees.
3. Upgrading or updating hardware to the newest product if feasible or just by keeping up with the updates and patches.
4. New mitigation tactics that keep up with trends and threats in the cyber world.

With the suggestions from IT support Hikes R Us business owners must ensure the company's compliance with state and federal regulations. In doing so the business owner will also keep in mind the protection and security of the company's assets and data of its customers. These implementations by the business owner will be approved with the thought of business continuity in mind. Keeping all business operations running normally is a high priority hence why these quarterly meetings are of most importance.

3.2 Compliance & Standards:

Hikes R Us regulation adherence:

1. Hikes R Us must comply with the Payment Card Industry Data Security Standard (PCI-DSS). This involves managing customers' debit and credit card information when they make purchases at the business. Any company accepting card payments must follow this standard. Hikes R Us is committed to providing a secure network with vulnerability management, monitoring, assessments, and scanning to protect sensitive data from unauthorized users.[9]

2. To ensure the security and protection of customer data and the business itself Hikes R Us implements New Jersey best practices for cybersecurity.

[9] PCI-DSS Certification

This is done by:[10]

1. Conducting regular risk assessments
2. Implementing a written security policy
3. Training employees
4. Installing anti-virus software
5. Encrypting sensitive information
6. Regularly backing up data
7. Implementing access controls
8. Monitoring network activity
9. Creating an incident response plan
10. Staying informed about potential threats

4.0 Risk Management & Physical Security

4.1 Risk Management Strategies:

Risk is a possible threat that could cause harm or loss. Many strategies could be put into place to mitigate or eliminate risk. These strategies all pertain to different business areas but contribute to protecting all company assets. Strategies that Hikes R Us have adopted are:

1. Conduct routine cybersecurity risk assessments.
2. Implement firewalls, anti-virus software, and access controls.
3. Implement physical security measures.
4. Build an incident response plan.
5. Create a schedule for updating and patching network devices.
6. Transferring risk by purchasing cybersecurity insurance.

4.2 Physical Security Measures:

Physical security is not just needed for employee safety but also for all business assets. These security measures add a defense in depth layer to protect all the company/customer data. Without physical security, businesses become very vulnerable to many cyberattacks. Listed is what Hikes R Us already has in place along with what is planned to be implemented.

[10] Cybersecurity Best Practices

1. **Physical Barriers:**
    a) Floor-to-ceiling around the infrastructure room
2. **Access Control Systems:**
    a) Badge Access – Implemented within every entrance/exit to the building along with the infrastructure room.
3. **Surveillance and Monitoring:**
    a) 5 pre-installed surveillance cameras - Three surround the outside allowing for full coverage. Two cameras are placed inside with one being inside the computing infrastructure room and the other in the front of the house watching who comes in and out of the store along with what is being purchased.
4. **Intrusion Detection System:**
    a) Break-in Alarm – This will be installed and monitored through a subscription with the provider.
5. **Lighting:**
    a) 4 Motion Sensor Lights – For the surrounding perimeter of the building to act as a deterrent.

5.0 Cybersecurity Leadership & Workforce Development

5.1 Leadership Overview:

Given the value of cybersecurity to Hikes R Us and the limited size of the company, cybersecurity efforts are an integral part of job responsibilities for employees of the company. The Chief Executive Officer (CEO) is responsible for the oversight of cybersecurity efforts, and the implications they have on the business as a whole. This includes the effects of policies on everyday work responsibilities, how Hikes R Us' security posture compares to the industry and if enough is being done to protect the business, and being the one to coordinate a response to stakeholders (and the media if necessary) in the event of a security incident. The IT Manager / Lead Database Admin is responsible for coordinating cybersecurity projects and overseeing the company's database systems. The company's cybersecurity analyst is responsible for conducting routine cybersecurity posture assessments, which include vulnerability scans, monitoring threat feeds, monitoring logs, and reporting findings to the IT Manager. Hikes R Us' Web Developer is responsible for operating the company's website, which includes fixing security vulnerabilities,

conducting thorough change testing, and coordinating with the cybersecurity analyst to keep the company's public-facing domain safe.

5.2 Roles & Security:

Hikes R Us consists of the following employment hierarchy:

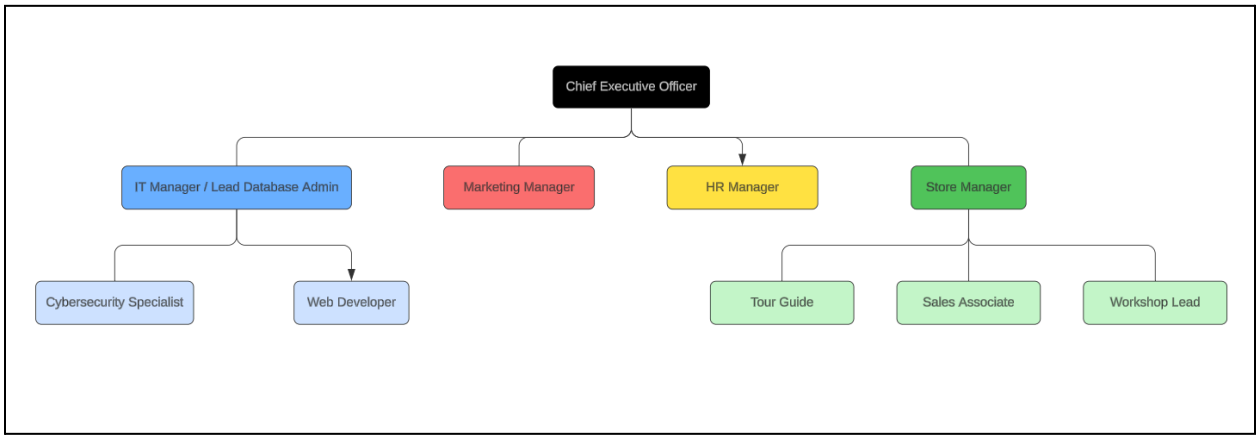

Figure 1 - Hikes R Us Employee Hierarchy

Below is a table detailing the background checks that every Hikes R U employee is subject to upon time of hire. All employees are required to sign a non-disclosure agreement out of respect for the company's trade secrets. Employees have been grouped into specific training groups, with each group consisting of tailored training to their job roles.

Employee Title	Background Checks	Employee Training Group
Chief Executive Officer (CEO)	Criminal History Check, Drug Test, References, Internet Usage Checks, Verified Employment, Verified Education, Watchlists Check, Legal Affairs Check, Credit Check	Manager
IT Manager/Lead Database Admin	Criminal History Check, Drug Test, References, Internet Usage Checks, Verified Employment, Verified Education, Legal Affairs Check, Credit Check	Manager
Cybersecurity Specialist		IT
Web Developer		IT
Store Manager	Criminal History Check, Drug Test, References, Internet Usage Checks, Verified Employment, Legal Affairs Check, Credit Check	Manager
Workshop Lead		General
Tour Guide		General
Sales Associate		General
HR Manager	Criminal History Check, Drug Test, References, Internet Usage Checks, Verified Employment, Verified Education, Legal Affairs Check, Credit Check	Manager
Marketing Manager		Manager

Table 1 - Employee Background Checks

All employees are provided with standard rights and permissions and are then distributed additional permissions dependent on the employee's job role. Providing this access to employees allows them the ability to perform standard job responsibilities, such as submitting timesheets, submitting vacation time, and accessing the company's network. This ensures that employees can perform their necessary duties, while also limiting access based on the principle of least privilege.

The CEO and IT Manager/Lead Database Admin are provided with admin accounts in addition to their standard account. The reasoning for this is to allow these personnel the ability to perform uncommon tasks in the network that can't be typically accessed via their standard accounts. These tasks consist of having direct read and write access to the company's database, direct access to other company systems (e.g. timesheet system), and emergency system

maintenance. Providing two accounts to these personnel allows them the ability to make system changes when necessary as well as perform incident response steps in the event of a security incident. These two personnel are the most trusted cybersecurity employees in the company.

5.3 Training Plan:

In any system environment, regardless of company, cybersecurity training is crucial to be distributed to employees regardless of role. As the cybersecurity landscape continues to evolve, employees must be prepared for new complex threats. As part of the company's evolution of cybersecurity, this training plan will be distributed to all employees, with specialized training provided to employees based on their roles.

Standardized for all employees, they must complete annual security awareness training to continue being employed by Hikes R Us. This training will be distributed through platforms like KnowBe4[11], Huntress[12], and the government agency CISA[13] (Cybersecurity and Infrastructure Security Agency). These platforms deliver exceptional training materials online to employees to prepare them for evolving cybersecurity threats and techniques used to attack systems. In addition, employees will be expected to review Hikes R Us' cybersecurity policies during onboarding as part of the company's hiring process. The HR Manager will be responsible for ensuring the completion of this training, as well as notifying employees if it is incomplete.

For ongoing training, employees will be contacted by the HR Manager for any additional training that needs to be completed by Hikes R Us employees. This training will be provided by the IT Manager as well as the Cybersecurity Analyst on an as-needed basis. Employees completing this training will be provided the opportunity to report any feedback they have, such as what training they felt was not very useful, or training they'd like to see more of. The HR Manager is responsible for reading this feedback and reporting it back to the IT personnel in charge of overseeing the training, with the intention of tailoring the training to their employees. The IT personnel will be responsible for monitoring metrics surrounding the training and making connections based on whether the training was effective at keeping the employees safe or not.

Following the plan below will provide Hikes R Us employees with effective training:

[11] KnowBe4
[12] Huntress
[13] CISA

1. General Training Plan
    a. Training Topics:
        i. Common phishing techniques as well as trends found within the emails/texts/phone calls.
        ii. The effects of effective online security practices such as being mindful of how user data is collected/stored as well as identifying malicious websites.
        iii. Effective password management practices include password complexity, password length, password randomness, and the importance of password managers.
        iv. Effective office security etiquette such as clearing desks of sensitive information when absent and locking workstations when absent.
    b. Frequency of Training
        i. Annual training based on time of hire.
        ii. Quarterly refresher training sessions.
2. IT Training Plan
    a. Training Topics:
        i. Present-day phishing techniques including trends and tools used to deliver phishing attacks.
        ii. Modern threats and malware and how to prevent organizations from being affected by these.
        iii. Incident response training including how to prepare a plan and adapt plans to modern threats.
        iv. Tools used to perform incident response and monitor security events.
    b. Frequency:
        i. Quarterly training sessions.
3. Manager Training Plan
    a. Training Topics:
        i. How to continue running a business in the event of a security incident.
        ii. Leadership training including how to orchestrate business operations based on the department in the event of a security incident.
        iii. Modern cybersecurity threats and their impact on business operations.

iv. How to manage cybersecurity risks within an organization.

b. Frequency:

i. Quarterly training sessions and updates on legal compliance.

6.0 Policy, Technology, and Asset Management

6.1 Policy Development:

At Hikes R Us, it is crucial that effective policies are written and enforced within the system environment. Below is a list of policies that Hikes R Us must implement to improve its security posture, and a sample policy can be found in Appendix A:

- **Access Control Policy** - Defines the access that employees will have, including both the network and physical access to rooms within the company.
- **Acceptable Use Policy** - Defines the level of acceptable use for company resources. This includes what is allowed to be searched on the company network and how company resources should be utilized.
- **Badge Policy** - Defines the requirement of having a badge to access the building and company resources, such as the printer. This includes the penalty for misplacing/misusing badges.
- **Business Continuity Policy** - Defines the process of what to do in the event of a security incident/event that imposes additional challenges for business operations.
- **Change Management Policy** - Defines the process for implementing changes into the system environment.
- **Clean Desk Policy** - Defines that employees should have a “clean desk” free of any sensitive documents/information when absent from their desk.
- **Cybersecurity Policy** - Defines the overall management of the company’s cybersecurity program, including its goal and the responsibilities the employees have to contribute.
- **Data Classification Policy** - Defines how data used by the business is classified and handled according to its classification.

- **Data Retention Policy** - Defines how long data is retained by the company, and how it is handled in accordance with state and federal legislation (e.g. California Consumer Privacy Act).
- **Data Storage Policy** - Defines how data is stored within the company's systems including the encryption that is used, as well as how it is accessed.
- **Disaster Recovery Policy** - Defines how the business is going to recover from the event of a disaster, including the general process to be followed regardless of disaster type.
- **Email Policy** - Defines how company emails should be used and how often emails should be reviewed based on job responsibilities.
- **Incident Response Policy** - Defines how the company will respond to security incidents, including those directly involved as well as the process.
- **Mobile Device Management Policy** - Defines how any mobile devices distributed by the company will be managed and how they should be used by recipients.
- **Network Policy** - Defines acceptable use of the company's network as well as the security controls implemented.
- **Password Policy** - Defines the company's password requirements, including how often passwords will need to be changed by the employee.
- **Patch Management Policy** - Defines how the company should conduct patches to its systems in the environment, including the roles responsible for and how to perform patching.
- **Physical Security Policy** - Defines the physical security implemented by the company to protect critical assets such as servers and workstations.
- **Removable Media Policy** - Defines the acceptable use of removable media and how it should be used. It will be explicitly stated that removable media slots (e.g. USB ports) will be disabled by default, and a request must be made to have them enabled.
- **Social Media Policy** - Defines the acceptable use of how employees use social media, including the types of posts that can be made and what information can be shared.

6.2 Technology & Tools:

In order for Hikes R Us' security posture to evolve, the company must implement the necessary and effective tools/technology for meeting the company's security posture goals. Below is a list detailing the tools/technology that must be implemented:

- **GTT DLP (Data Loss Protection) Software** - Any data that is detected leaving the company's systems via the company's network will be blocked from leaving, and an alert will be sent to the corresponding personnel. This will protect the company's data from any unidentified attacks, as well as irresponsible misuse of company resources by the employees.
- **1Password Encryption Protection Software** - Employee passwords will be encrypted and managed within the 1Password system platform. Managing platforms from a central location will allow employees to have easier control over their passwords and implement an additional security control.
- **Norton Antivirus Software** - Implementing antivirus software onto employee workstations and other devices provides additional protection against computer viruses, not originally flagged by the employee. This adds extra protection to company data and prohibits access to unauthorized individuals.

6.3 Data Classification:

It is crucial that Hikes R Us implements accurate and easily identifiable classifications for the data they are utilizing and collecting. This is important, as incident response plans and security control implementations rely on company data being accurately identified. For instance, confidential data must be encrypted, whereas public data is fine to be stored in plaintext. Hikes R Us utilizes four different data classifications: Confidential, Restricted, Private, and Public.

Confidential data is the most important data that Hikes R Us houses. Losing this data could pose immense damage to the company, including financial, reputational, and legal damage. All confidential data is stored with the strongest encryption and is accessible through an isolated section of the network. Admin accounts are the only accounts with the ability to access this data. Below are examples of this data:

1. Customer data. This includes any personally identifiable information (PII) (e.g. name, address, email, etc.), as well as payment card information. It is crucial that this data is fully protected, as there is compliance with the law at stake.
2. Trade secrets. Serving as a pillar of Hikes R Us, it is crucial that this data is protected, including trail routes, workshop content, and profitable business moves.

3. Employee data. Similarly to customer data, it is equally as important to protect the employees of Hike R Us' data. This also includes passwords to accounts and usernames.

Restricted data is the second most important data owned by Hikes R Us. This data applies more to the physical store. This data is employed with strong encryption; however, is not on an isolated section of the network. Below are examples of this data:

1. Store inventory. All of the goods that Hikes R Us sells to its customers are safely stored within the company's inventory management system. Allowing this data into the hands of unauthorized viewers could expose trade secrets and valuable market data for vendors.
2. Door passcodes. These passcodes are saved to allow the employees access to the building to open and close for the day. Doors that have passcodes as well are the doors to the server room on-premises.
3. Floor plan. This data must be safely stored because it contains the locations of crucial assets on-premises, such as servers, power supplies, generators, and other sensitive location data.
4. Incident response and business continuity plans. Keeping this data encrypted is vital, as attackers cannot gain access to this data, otherwise they know what to expect Hikes R Us to do in the event these occur.

Private data is data that is not directly accessible to the public and is only accessible by internal employees. This data is not as vital as confidential and restricted data; however, it is still important for business operations and must be safely stored. This data is published to the company's intranet, which is only accessible via employee accounts connected to the company's network. Below are examples of this data:

1. Sales events calendar. Protecting this data is vital to the success of retail sales as if this information is leaked to customers, sales will take a hit.
2. Asset inventory. It is necessary to keep this data private from customers and other malicious attackers, as having access to this data could allow attacks to be orchestrated.

3. Training materials. Preventing attackers from knowing what training materials are distributed is crucial, as it could allow attackers to gain an advantage, as they know to use methods that employees aren't being trained on.
4. Policies and procedures. These can consist of both security and non-security-related policies and procedures.
5. Company events. Any events that consist of employees being absent from the location give attackers a chance to break into the physical location, as no one is there to witness it.

As for public data, if it is not listed above, it is classified as public data. While this data may not be directly advertised to the public, it does not pose a risk to the company if it gets into the hands of the public. This includes materials such as product documentation and outdoor materials.

6.4 Asset & Data Management:

Hikes R Us has documented its assets in the table below:

Asset	Hardware Category	Serial Number
Router (1)	Network	RN001
Switch (1)	Network	SN001
Firewall (1)	Network	FN001
Printer (2)	Office	PO001 - PO002
Docking Station (8)	Office	DSO001 - DSO008
Monitor (8)	Office	MO001 - MO008
Surveillance Camera (10)	Security	SCS001 - SCS010
Break-In Alarm (5)	Security	BAS001 - BAS005
Badge Reader (5)	Security	BR001 - BR005
Door Codepad (5)	Security	DCS001 - DCS005
Uninterruptible Power Supply (2)	Security	UPSS001 - UPSS002

Asset	Hardware Category	Serial Number
Motion Sensor Light (4)	Security	MSLS001 - MSLS004
Development Server (1)	Server	DS001
Production Server (1)	Server	PS001
Walkie Talkie (4)	Telecommunication	WTT001 - WTT004
Phone (8)	Telecommunication	PT001 - PT008
Desktop (2)	Workstation	DWS001 - DWS002
Laptop (10)	Workstation	LWS001 - LWS010

Table 2 - Asset Inventory

Hikes R Us has documented its software licenses below:

Software License	Software Category
GTT DLP (10)	Security
1Password (1)	Security
Norton Antivirus (10)	Security
Break-In Alarm Subscription (1)	Security
CRM (1)	Productivity
Google Drive (10)	Productivity
Adobe Acrobat[14] (1)	Productivity
Adobe Suite (1)	Productivity
Google Cloud Subscription (3)	Productivity
Power BI[15]	Productivity
Microsoft Office 365 Subscription (5)	Productivity

Table 3 - Software Inventory

[14] Adobe Acrobat
[15] Power BI

7.0 System Security & Maintenance

7.1 Configuration & Patch Management:

Configuring[16] and patching[17] devices properly is integral to the cybersecurity posture of an organization, as it ensures systems are up to date and can be reverted in the event that something goes wrong unexpectedly. This is crucial for system hardening, as it provides the organization a sense of security that their devices are up to date and properly configured for updates.

Below is a procedure for how to conduct configuration management in Hikes R Us' system environment:

1. Declare a configuration that should be established as a baseline. This means that all systems being added to the environment should have a standardized baseline configuration. For example, devices should be configured with automatic updates and antivirus software enabled.
2. Ensure configurations are accurate by deploying a configuration management tool such as Puppet[18]. When a new system is added to the environment, the tool will analyze the system's configuration and compare it to the baseline configuration established. It will provide the user with a report if the device is properly configured or not. These tools can perform these functions on an automated schedule for any changes that might be made to the baseline configuration.
3. As threats continue to evolve, configurations should be updated as needed based on threat intelligence feeds. For example, this may consist of malicious traffic being flooded to the company's servers. To defend against this attack, all firewalls should be configured to block this malicious ingress[19] traffic.
4. In the event a device's configuration needs to be changed, it should be done so according to a formal change control process[20] that is abided by the IT personnel within the company. Adhering to this process ensures that the system is updated properly, and can be rolled back if necessary. Change control processes typically utilize a test environment before being put into production, depending on the change (e.g. code).

[16] Configuration Management
[17] Patch Management
[18] Puppet
[19] Ingress Traffic
[20] Change Control Process

Below is a procedure for how to conduct patch management in Hikes R Us' system environment:

1. Working within the test environment, any patches applied to a system or application should be done so within this environment. This ensures that any patch applied only affects the test environment, and it can be deduced that the patch is not safe to be applied to the system/application. Deeming it not safe could mean it poses a security risk to the organization or has an impact on the availability of the system/application.
2. All systems/applications will be updated within the test environment first, making it a good practice to enable automatic updates on the systems/applications. This can be completed by navigating to the operating system's security settings and enabling automatic updates.
3. Patches should be completed in accordance to a priority hierarchy established by the company, with reference to industry standards. Below is a chart of how Hikes R Us should prioritize patches. Defining this allows the company the ability to prioritize how soon patches need to be applied, ensuring a more secure environment:

Patch Priority[21]	Risk	Installation Timeframe
High	Critical to potential	Within 72 hours
Medium	Slight	Within 2 weeks
Low	Minimal	Within 1 month

Table 4 - Patch Prioritization

4. A short audit should be conducted on a monthly basis to ensure that system/application patches are being applied correctly and automatically. A tool such as ManageEngine Patch Manager Plus[22] will do this on an automated schedule and will provide the user with a report detailing its findings.

[21] Professor Tarabah Cybersecurity Program - 7.2
[22] ManageEngine Patch Manager Plus

5. In the event there are any patches that need to be applied the same day (zero-day vulnerabilities[23]), then an emergency procedure should be available to the responsible IT personnel.

7.2 Network & Website Security:

In Hikes R Us' system environment, the network is the most critical asset internally, while the website is the most critical externally. The website drives sales, while the network allows employees the ability to communicate amongst one another, as well as interact with systems. It is essential that these aspects of the system environment are secured, upholding the CIA triad[24].

Securing the company's internal network is comprised of the following, in no specific order (this can be referred to as a checklist):

- Any host-based security agents should be installed on the servers themselves. Including this software on the server upholds the defense-in-depth principle and ensures that if an attacker is able to reach the company's servers, there is another security control standing in the way of gaining access to the information on the server.
- Firewalls should be deployed onto the network. Firewalls should be deployed to the network and specifically between the servers and the rest of the network/Internet. These firewalls should have rules for both ingress and egress traffic, as it is crucial that any data coming in that is not wanted is blocked, and that any crucial data is not being unintentionally sent out. Other firewall features such as built in Intrusion Prevention System[25] (IPS) and malware protection should be enabled in addition to the firewall rules.
- Data loss prevention tools should be installed onto any systems interacting with data on the network. For any system that is working with internal data, a data loss prevention tool should be installed onto it. The data loss prevention tool will identify any data based on tags (Hikes R Us data classification policy) that is leaving the network to be stopped from leaving the network, while also triggering an alert to the appropriate IT personnel.

[23] Zero Day Vulnerability
[24] CIA Triad
[25] IPS

- Virtual local area networks[26] (VLANs) will be deployed to the network, isolating specific sections of the network. Based on Hikes R Us data classification policy, confidential data is required to be placed into an isolated section of the network. Implementing this will require that the appropriate IT personnel enter the configuration terminal on the switch, and create a VLAN on the network switch itself. This consists of connecting ports.
- Annual vulnerability and penetration testing. Vulnerability testing should be performed on a monthly annual basis, while thorough penetration testing should be conducted on a yearly basis. Performing these assessments will identify any weaknesses in the company's security posture, and will provide reports on how to address these weaknesses.
- Implementation of multi-factor authentication. Multi-factor authentication[27] (MFA) should be implemented as a standardized way of accessing the Internet. Employees will be required to follow MFA prompts when accessing the network, regardless of internally or remotely.
- Data encryption. Any data that is sent across the network as well as to the Internet should be encrypted. This means that proper network protocols such as HTTPS[28] (port 443), SFTP[29] (port 22) and SSH[30] (port 22) should be used to secure data. SFTP and SSH utilize the same port, as SFTP defaults to using SSH to secure its data transfers. Employing this provides an additional security control to the network, ensuring that in the event of an unaware attack, data cannot be viewed. E2EE (End to End Encryption[31]) will be employed onto the network.
- Set up a SIEM tool. A SIEM (Security Information and Event Management[32]) tool allows the user the ability to monitor system logs on the network, and identify any anomalies within the network traffic. Most SIEM tools allow the user the ability to set up alerts for any suspicious behavior within the environment that can be reported to the appropriate IT personnel. SIEM tools should be installed on both the servers, and any endpoints within the system environment.

---

[26] VLAN
[27] MFA
[28] HTTPS
[29] SFTP
[30] SSH
[31] E2EE
[32] SIEM

Securing the company's website is comprised of the following, in no specific order (this can be referred to as a checklist):

- Secure the source where the website is hosted. As previously mentioned in securing the network, the company's website is hosted within their own production server. This server has the ability to log and monitor traffic, control traffic coming in and leaving and perform automatic updates. This ensures that the website is hosted in a secure environment where there is control over how secure it is.
- Strong passwords and MFA. In accordance with the company's relevant policies and network security, MFA and strong passwords are required for any access to the website and its server. Enforcing these policies ensures that the website is not easy to access, and requires additional authentication beyond just connecting to the network.
- SSL/TLS certificate. A proper SSL/TLS certificate should be obtained for the company's domain, as it will allow for continuous customer traffic and improve sales. A certificate can be obtained through a Certificate Authority[33] (CA) such as GoDaddy[34], and a Certificate Signing Request[35] (CSR) should be made on the production server. Once the certificate is received and assigned, the server should be configured with the certificate, allowing for traffic to be verified between the customer and the company.
- Proper vulnerability scanning. Similarly to the network security of the company, vulnerability scanning should be conducted on a monthly basis. This consists of using tools like OpenVAS[36] as well as fuzzing[37] tools like FuzzDB[38] to test against unexpected user actions as well as SQL injection attacks[39].
- Have DDOS mitigation techniques. Distributed denial of service[40] (DDOS) mitigation techniques should be implemented into the system environment, such as using load

[33] CA
[34] GoDaddy
[35] CSR
[36] OpenVAS
[37] Fuzzing
[38] FuzzDB
[39] SQL Injection Attack
[40] DDOS

balancers and having backup servers hosted within the cloud. This is implemented in the event a DDOS attack occurs. This ensures the availability of the website is still intact.

- Implement a backup schedule for the website's database. Incremental backups should be performed on a weekly basis on the website's primary database, which houses customer data, inventory, and payment card information. In the unexpected event something happens, such as a natural disaster or DDOS attack, implementing backups allows the system to be brought back to a normal state in a short amount of time. Backups should ideally be in the cloud, and a backup procedure should be included within the business continuity and disaster recovery policies and procedures.

8.0 Program Monitoring & Future Outlook

As Hikes R Us grows, it is essential to continuously monitor and evaluate the cybersecurity program to ensure it evolves with the company's changing needs and the increasing reliance on digital and in-store operations. This section defines how often the program should be reviewed, the key metrics for measuring its success, and the process for reporting updates to relevant stakeholders.

8.1 Monitoring & Evaluation:

The cybersecurity program will be regularly assessed to protect the store and website, which are critical for day-to-day operations and customer transactions.

8.1.1 Key Performance Indicators (KPIs):

1. **Secure Transaction Handling**

   KPI: Percentage of secure transactions processed through the online store and in-store POS systems (ex. encrypted payment methods, secure payment gateways).

   Target: 100% of all customer transactions are processed securely, ensuring protection against fraud and data breaches.

2. **Customer Data Protection**

   KPI: Number of data breaches involving customer information, including personally identifiable information (PII) and payment data.

   Target: Maintain a 0% breach rate for customer data due to inadequate system configurations, or failure to follow proper data handling practices.

3. **Patch Management of Systems**

   KPI: The time taken to implement patches for critical vulnerabilities in the store's POS system and website.

   Target: 100% of security patches installed within 48 hours of release to maintain up-to-date protection across all systems.
4. **Employee Cybersecurity Training**

   KPI: Employees complete mandatory cybersecurity training.

   Target: 100% of employees are trained within three months of being hired, with annual training materials released to keep everyone up-to-date with emerging cybersecurity threats.
5. **Incident Detection & Response Time**

   KPI: Average time from detecting an incident until it is resolved.

   Target: Critical incidents should be resolved within 48 hours, and other incidents within 72 hours.

8.1.2 Review Schedule of the Cybersecurity Program:

1. The cybersecurity program should be reviewed quarterly by the management team to assess the effectiveness of existing security measures, review the progress of KPIs, and identify any areas for improvement.
2. An annual security audit will be conducted to ensure compliance with industry standards and state regulations.
3. The program will be reassessed whenever there are significant operational changes such as adding new services (ex. new rental service) or updating technology. This ensures that cybersecurity measures remain aligned with business operations.

8.1.3 Continuous Improvement Methodology:

Hikes R Us will use the PDCA (Plan-Do-Check-Act) cycle to maintain and enhance its cybersecurity program. This approach uses a systematic process for addressing security challenges and adapting to changes in the organization.

1. **Plan:** Identify areas of improvement based on quarterly reviews, employee feedback, and audit results. Areas of focus may include updating security policies, addressing gaps in training, or adapting to new cybersecurity threats.

2. **Do:** Implement solutions to address identified vulnerabilities. This can include revising training materials, upgrading technology, or enhancing incident response protocols.
3. **Check:** Assess the impact of implemented changes by reviewing relevant KPIs, analyzing feedback, and evaluating incident reports to ensure improvement meets the organization's goals.
4. **Act:** Adjust strategies and revise processes based on the “Check” phase. Document lessons learned and utilize them in future planning.

8.1.4 Reporting:

Hikes R Us is committed to maintaining clear and transparent communication with all stakeholders regarding cybersecurity updates and the role they play in protecting company data and day-to-day operations.

1. **Management Team**
    a) The cybersecurity program’s progress, including KPI performance and recommendations for improvement, will be reported quarterly during management meetings.
    b) Significant incidents or breaches will be reported to the management team within 24 hours of detection.
2. **Employees**
    a) Employees will receive a quarterly email update summarizing cybersecurity initiatives including reminders of best practices.
    b) Individuals responsible for the impacted areas should be notified within 24 hours of any incident.
3. **Customers**
    a) If a data breach occurs and customer information is compromised, affected customers will be notified as soon as possible to comply with applicable laws.
    b) Updates on significant cybersecurity program improvements will be shared through the company website and email newsletters to create customer trust.

8.2 Conclusion:

The cybersecurity goals and KPIs developed for Hikes R Us are designed to safeguard critical assets, minimize operational disruptions, and have strong security awareness across the company.

By addressing these areas through clear objectives and measurable outcomes, Hikes R Us will be prepared to tackle emerging threats while ensuring business continuity.

1. **Secure Transactions:** Ensuring 100% secure processing of customer transactions protects sensitive payment information and reduces the risk of fraud and data breaches.
2. **Data Protection:** Maintaining a 0% breach rate reflects Hikes R Us's commitment to protecting customer and employee data.
3. **Enhanced Patch Management:** Implementing patches within 48 hours of release ensures that systems remain secure and ready to support business operations.
4. **Employee Awareness:** Requiring all employees to complete cybersecurity training enhances their ability to identify potential threats, and reduces human error as a security vulnerability.
5. **Rapid Incident Response:** Mitigating critical incidents within 48 hours minimizes potential damage and downtime, demonstrating the company's ability to address security incidents effectively.

9.0 Revision History Table

Version	Authors	Date	Changes
v 0.1.0	Brandon Morgan Sylena Beccles Michael Varrella	11/25/2024	First Draft
v 1.0.0	Brandon Morgan Sylena Beccles Michael Varrella	12/02/2024	Presented documents to the CEO Sally, and made recommended changes
v 2.0.0	Brandon Morgan Sylena Beccles Michael Varrella	12/10/24	Updated KPIs and program monitoring section
v 3.0.0	Brandon Morgan Sylena Beccles Michael Varrella	12/14/2024	Version approved by CEO Sally

Table 5 - Revision History Table

9.1 Change Control Process:

The change control process ensures that any modifications to this plan are thoroughly evaluated, approved, and implemented. The process includes the following steps:

1. **Proposal Submission:**
   Any employee proposing a change must complete a change request form and submit it to IT Support for initial review
2. **Initial Review & Assessment:**
   IT Support will evaluate the change's technical aspects, including its potential impact on the cybersecurity posture and business operations.
3. **Business & Compliance Assessment:**
   If the changes are reasonable, they will be escalated to the Business Owner, to decide if they align with the company's objectives. The Business Owner will consult external advisors if legal or compliance concerns arise.
4. **Approval Process:**
   Approval requires:
   a) IT Support (technical aspect)
   b) Business Owner (business aspect)
   c) Additional stakeholders (ex. Marketing Specialist, Inventory & Sales Manager) if the change affects customer-facing platforms or operations.
5. **Scheduling & Implementation:**
   IT Support will schedule the changes, ensuring minimal disruption to operations. Implementation will have a testing phase to ensure that the change does not introduce new vulnerabilities.
6. **External Stakeholder Communication:**
   If the change impacts external stakeholders, the Marketing Specialist will communicate it to them.
7. **Documentation and Archiving:**

IT Support will update the documentation, archive previous versions, and ensure the revision table reflects the new version.

Appendices

Appendix A – Clean Desk Policy[41]

Purpose

The purpose of the policy is to maintain a secure, organized, and professional work environment by ensuring that sensitive information, whether physical or digital, is protected from unauthorized access.

Scope

This policy applies to all employees, including full-time, and part-time.

Policy Guidelines

1. Workstation Organization
    a. At the end of each workday or shift, all workstations shall be cleared of papers, files, and other materials that contain sensitive information or confidential information.
    b. Documents should be stored in locked drawers, cabinets, or other secure locations.
2. Digital Devices
    a. All computers and digital devices shall be logged out of when not in use, especially when unattended.
3. Printed Documents
    a. Confidential and sensitive documents should not be left on desks, printers, or other shared spaces.
4. Personal Items
    a. Employees should ensure that personal items do not clutter workspaces or interfere with essential equipment.
5. Common Areas
    a. Shared spaces such as break rooms, conference rooms, and workstations must remain tidy and free of confidential information.

[41] Policy Template

6. Employee Responsibility
    a. All employees are responsible for ensuring that they are compliant with this policy and must report any violations or concerns to management.
7. Policy Enforcement
    a. Periodic checks will be conducted to ensure compliance with the Clean Desk Policy.
    b. Violations of this policy may result in disciplinary action, depending on the severity.

Training & Awareness

Employees will be briefed on the Clean Desk Policy during their onboarding process and receive annual reminders to reinforce its importance.

Appendix B – Encryption Standard for Hikes R Us

1. **Purpose**

   This standard outlines the minimum encryption requirements to protect sensitive data at Hikes R Us. Encryption protects information from unauthorized access during storage and transit, ensuring confidentiality and integrity.

2. **Scope**

   This standard applies to all sensitive data including:

   a) Customer information
   b) Employee records
   c) Financial data
   d) Confidential business information

3. **Encryption Requirements**

   3.1 Data at Rest[42]

   Sensitive data stored on any system must be encrypted to protect it from unauthorized access. The following encryption requirements apply:

   a) Use Advanced Encryption Standard (AES) with a minimum key length of 256 bits.
   b) Laptops and other portable devices containing sensitive data must be encrypted with full-disk encryption.
   c) Sensitive data stored in cloud environments must be encrypted using AES-256.

   3.2 Data in Transit[43]

   Sensitive data transmitted over any network must be encrypted to prevent interception. The following encryption requirements apply:

   a) Use Transport Layer Security (TLS) version 1.3 for all network communications.
   b) All data transmitted must use secure protocols such as HTTPS or SFTP to ensure data is protected in transit.

   3.3 Backup Data

   Backup data must comply with the same encryption requirements as data at rest, regardless of storage location.

[42] Data at Rest
[43] Data in Transit

4. **Key Management**[44]

   To ensure secure encryption practices, the following key management practices are required:

   a) Utilize a secure key management system (KMS).
   b) Generate keys using industry-approved algorithms.
   c) Rotate encryption keys at least annually or if compromise is suspected.
   d) Securely destroy expired or unused keys.

5. **Review & Updates**

   This standard will be reviewed annually or in response to:

   a) Significant operational or technological changes
   b) Updates to relevant regulations or industry standards
   c) New vulnerabilities in encryption methods

[44] Key Management Overview

Appendix C – Authorization Levels SOP

The Standard Operating Procedure is put into place to standardize processes that comply with the newest industry regulations. This is to ensure efficiency, consistency, and the quality of the operations. In this SOP authorization levels will be defined along with step-by-step instructions on how to conduct routine tasks within this organization. [45][46]

High Access:

This is for the cyber personnel working on the system and is tasked to protect the data. Has full access to all the cloud and network infrastructure. This is to be able to troubleshoot and configure whenever needed. Have read, write, transfer, and deletion privileges. Employees of lower levels must contact this privilege level for any authorization request changes.

Medium Access:

This is for the employees tasked with adding or making changes to data due to the organization's request. Has limited privileges to only be able to read and write to stored data. Must contact high-access personnel to transfer or delete stored data.

Basic Access:

This is a customer service role for when organizations request data for data confirmation. It is limited to only look up and view organizational/personal data from the storage system. This is for support of the organization in need of information. For any modifications, additions, transfers, or deletions higher access personnel must be contacted.

[45] https://workflowautomation.net/blog/standard-operating-procedure-sop

[46] https://limblecmms.com/blog/standard-operating-procedure-sop/

New Account Setup:

1. Locate the start button and in the search bar type:
    - Active Directory Users and Computers
2. In Active Directory navigate to the Users folder.
3. Right-click on the Users folder and select:
    - New
    - User
4. The New Object – User pane will display. Enter:
    - “First name”
    - “Last name”
    - “Initials”
    - “Full name”
    - “User Login Name”
5. Select Next
6. Enter the chosen password
7. Renter chosen password
8. Deselect “User must change password at next login” checkbox
9. Select Next
10. This completes the addition of a new user.

Note: At this point, you can right-click the user in the Users folder and go into properties to add or make changes to the profile.