Sheds and Things Risk Analysis Report

Introduction

As discussed, here is the risk report requested as a follow up to the initial assessment.
Before discussing any suggestions or implementations, I am going to state assumptions made about the organisation, state the scope of the assessment and explain the methodology used in the risk analysis process.
Should any assumptions be incorrect or if you would like further information about the frameworks used please get in touch.

Assumptions

Sheds and Things consists of the following departments:
- Sales
- Management: General and HR
- Manufacturing
- Purchasing and Finance
- Delivery and Site Installation

Following the initial assessment an IT department has been created.

The offsite hosted website is hosted on a company owned server.
The local software developer is to be considered an employee for the purposes of being informed of risk and working practices relating to the organisation.

Scope

This document **does** cover:
- Information assets (on and offsite) [e.g. Laptops, data in transit]
- The physical security of the building and IT assets [e.g. Ensuring the building is locked at night]

This document **does not** cover:
- The manufacturing process [e.g. Risk of injury due to tools]
- The delivery and installation process [e.g. Lifting and handling of heavy objects]
- Vehicles [e.g. Maintenance of the business's cars/vans]

Risk Methodology

This report uses the modern approach to risk, identifying possible occurrences before any loss occurs and focusing on the threats and vulnerabilities that face assets.
It also uses a 4x4 matrix with the following terminology. With an organisation's overall risk level also able to be represented on the matrix.

Impact Likelihood	Critical [4]	Severe [3]	Moderate [2]	Marginal [1]
Frequent [4]	High [16]	High [12]	Medium [8]	Medium [4]
Probable [3]	High [12]	High [9]	Medium [6]	Low [3]
Unlikely [2]	Medium [8]	Medium [6]	Medium [4]	Low [2]
Rare [1]	Medium [4]	Low [3]	Low [2]	Low [1]

Risk Assessment

Risk Register

Asset	Risk Description	Risk Owner	Impact	Likelihood	Risk	Mitigation Strategy	Post Mitigation Impact	Post Mitigation Likelihood	Mitigation Complete
Company Network	The system could be compromised by a user falling victim to a phishing attack. Worst cases here are loss of access to the system or a data breach	Management	4 - Extended downtime and time spent restoring the system Fines as a result of a data breach	4 - Phishing scams and ransomware are increasly common	16	Educate employees in phishing techniques.	4	2	8
Company data	Lack of formal backup policies and procedures.	IT/Management	4 – Loss of data means that data will no longer be available. Recovering from data loss can be a long process without accessible backups	4 – It is almost certain that some kind of incident that requires a back up will occur.	16	Have a stronger password policy, requiring 14 characters, numbers, upper case letters and special characters.	1	4	4
Company devices	All devices need to be regularly updated. As an organisation grows it is easy to lose track of devices.	IT	4 – Poor patch management leaves an organisation vulnerable to lots of attacks that can shut down the system or allow unauthorised access to data	4 – Unpatched devices are one of the biggest security threats to an organisation.	16	- The department can keep track of devices by using asset management software. - This along with strong patch management ensures that all devices are kept secure	4	2	8

Company Network	There is a risk users could browse on websites with poor security practices and fall victim to a malware attack or another attack of opportunity. Worst cases here are loss of access to the system or a data breach	IT	4 - Extended downtime and time spent restoring the system Fines as a result of a data breach	3	12	Install an application proxy at the edge of the network	4	1	4
Desktops/ Servers	Weak password policy, permitting 5 letter passwords with no special character, numbers or upper case letters.	Management	4 - Compromise of system. Data exfiltration or risk of ransomware attack.	3 - Opportunist password attacks are a regular threat.	12	Have a stronger password policy, requiring 14 characters, numbers, upper case letters and special characters.	4	1	4
Desktops/ Servers	Open ports on a device increase its attack surface allowing an attacker to connect via insecure services	IT	4 - Compromise of system by attackers.	3 - Websites like Shodan make it easy for hackers to find open ports to attack.	12	If RDP is not necessary then disable it and ensure the port is closed. If essential, set up a terminal server or set up a company VPN and ensure RDP is only accessible from within the VPN.	4	1	4
Company Network	All users are able to install software.	IT	4 – An easy way for malware to get onto the network.	3 – Deliberate attacks are possible. Accidental issues due to poor user awareness	12	Implement secure configuration settings and only allow administrators to install software.	4	1	4

				quite likely					
Portable devices/company data	Devices containing data can be stolen in attacks of opportunity.	Sales/Deliver & Installations	3 – Theft of devices containing confidential data such as emails. If an employee is logged in to various services the thieves will have access to those	4 – Laptops and phones are easy to steal	12	- Full disk encryption can limit the damage caused when theft occurs. - Remote wipe means that stolen devices won't hav any valuable data on.	1	4	4
Company network	Devices connecting to the company wifi might be compromised and transmit their malware across it	IT	4 – Once an attacker finds a vulnerability lateral movement across the network is easy.	3 – With no way to assess the state of devices all it takes is one rogue devices to shut the network down	12	Implementing network access control ensures that connecting devices meet the minimum security requirements. - Create a separate BYOD network to limit the impact of compromise should it occur	2	1	2
Website	Poor web development practices can lead to massive vulnerabilities. For a detailed look at these consult the OWASP site.	Web Developer	4 – Defacement of a website can impact a company's reputation. A data breach can have financial implications.	3 – Vulnerable websites are often the target of opportunistic hackers. SQL injection is very easy to do when inputs are unsanitised	12	- Ensure third parties are up to date with secure development practices and are familiar with the OWASP top 10. - Be willing to change contractors if the site is not up to standard	4	1	4
Files on the network	A permanently logged in account,	IT	3 – Critical data could be lost or	3 – Users usually use current session	9	Set the computer to log out after a moderate	3	1	3

	allowing users access to confidential information.		altered. Either maliciously or accidentally Confidentiality of data is also compromised	rather than logging in with their own account		amount [5 minutes?] of inactivityi. Educate users in good security practices and encourage them to log off when leaving a device.			
Physical IT infrastructure	The router and server are accessible to anyone. It is possible to plug devices into them	IT	4 – Long term compromise of business critical infrastructure.	2 – Requires considerable planning. Given the location of the site, opportunist attacks on physical infrastructure are unlikely.	8	Store the server and router in a lockable cabinet keep them out of harms way.	4	1	4
Company data	Connecting to the company network over public wifi whilst off-site can mean that unencrypted data is being broadcast in public and vulnerable to eavesdroppers.	Sales/Delivery & Installations	4 – Depending on the nature of the attack, data confidentiality can be compromised. MITM attacks can impact the integrity and non repudiation of data	2 – Attacks like this require a lot of effort to set up and given the itinerant nature of the connections made it is unlikely for	8	Use a VPN alongside a wifi connection when working remotely to protect traffic from eavesdroppers	4	1	4
Confidential data stored on the network	The server is badly configured allowing users to access the majority of files on it	IT	4 - Compromising the confidentiality, integrity and availability of data.	2 – It's unlikely an attack will happen but this setup makes accidents possible	8	- Use Active Directory and Group Policy Settings for centralised control over users and devices, providing a more organised way of managing the	2	1	2

						network. Alternatively controlling file permissions using ACLs - Have backups of the data			
Files on the company network	Unauthorised use of USB files to transfer data	IT	4 – Theft of data. Potential fines for violating GDPR	2 – More likely to happen accidentally.	8	- Configure user accounts to deny access to USB ports by default. - Group Policy settings will limit user access to files	2	1	2
Physical Items/Devices on site	Leaving the dock door open and unattended can make it easy for unauthorised people to access the premises. Unchallenged they can steal equipment or access IT systems	Delivery & Site Installation	3 – Intentional misuse of company equipment can cause disrupt the work day.	2 – Unlikely due to how out of the way the warehouse is located	6	-Close secondary entrances when not in use. -Limit customer access to sales area -Employees should approach anyone unfamiliar outside of the sales area.	3	1	3
Card payment details	Theft of customer payment information	IT	4 – Reputational damage	1 – Low risk as payment system is outsourced to a third-party	4	None required	4	1	4
Physical IT devices [Printer, server, router]	Placing devices in accessible places can leave them open to damage	IT	2 – Damage to router can make services unavailable	2	4	Store server and router in a lockable cabinet[1] keep them out of harms way. Wall mount if space is an issue.	2	1	2

1 https://www.cablemonkey.co.uk/371-data-server-cabinets

Overall Organisation Risk Level

Using the risk matrix we can see that the organisation's risk level is currently high. Implementing the suggested mitigation strategies will bring the risk level down to a more manageable medium

Impact / Likelihood	Critical [4]	Severe [3]	Moderate [2]	Marginal [1]
Frequent [4]	High [16]	High [12]	Medium [8]	Medium [4]
Probable [3]	High [12]	High [9]	Medium [6]	Low [3]
Unlikely [2]	Medium [8]	Medium [6]	Medium [4]	Low [2]
Rare [1]	Medium [4]	Low [3]	Low [2]	Low [1]

Current risk level

Post-mitigation risk level

Patch Management

A key part of risk mitigation is patch management, a process that is more involved than scheduling updates every Tuesday. The following RACI chart looks at the roles each department plays in the different patch management processes.

RACI Chart

	IT	Management	Sales	Manufacturing	Purchasing and finance	Delivery/ Installations	Web Developer
Patch Implementation schedule/prioritisation	R – Suggest the schedule	A –Will be ansewring questions if the schedule disrupts the work week.	I – Will be notified of service down time due to patching.	I	I	I	C – Third parties need to be included in the patching process
Inventory Management	RA – This falls under the remit of IT	C – Are the ones spending money					
Reviewing Security Patch/Update Releases	RA - This falls under the remit of IT	I – Management need to be aware of security risks but can't overwrite the decisions of IT					I – Needs to be aware of security risks
Testing Patch Compatibility	RA - This falls under the remit of IT						C – Need to discuss patch impact on the web interactions.

Choose a vulnerability management solution	R – Decides on the solution	A – Signs off on the solution					I – Is made aware of what they are working with
Website Updates	A – Interfaces between the developer and the organisation	C – Is involved in the decision making process but lacks the knowledge of the IT dept.					R – Maintains the website
Internal communication of patching process	A – Provides information for HR to distribute	R – All internal communications go through HR	I - Will be notified of service down time due to patching.	I	I	I	C – Informs IT of necessary website updates.
Hardware patching	RA – A key IT duty	C – Regular device users need to inform IT when their devices are free	C		C		
Firmware Updates	RA – Another key IT duty	C – Consulted on ideal period for downtime					