**Secure Sheds Risk Analysis**

**Executive Summary**

Thank you for inviting me to assess and analyse your organization’s cyber security. In my first report we identified your most likely cyber threats and how to mitigate against them from a physical, procedural and technical perspective.

This report can be used in parallel, but with the aim to give each vulnerability a risk score based on the probability they could occur combined with the severity of the occurrence which will convey the overall risk to your organization. I counted 15 key vulnerabilities within your organization and listed them in the risk register below, ranked by severity in descending order. Whilst I strongly advise you to mitigate all these risks, the order will enable you to prioritise your most vulnerable situations, start with the biggest threats and work your way down until you are confident that you have all the necessary measures in place to make you a very challenging target for any experienced adversary’s.

I have also included a RACI chart which will help you to clarify employee roles and responsibilities in keeping your systems up to date to the latest threats. The chart is designed to ensure clear communication and smooth workflows across all parts of your teams.

There is also a 10-slide presentation which I will present and distribute to your employees which covers the most important cyber principles they should adhere to. Your employees can either be your biggest vulnerability, or your biggest asset in staying one step ahead of cyber threats. If you ensure that their roles include cyber awareness practises then they will now doubt enable you to stay secure.

Whilst it is sadly impossible to ever be 100% secure against potential cyber threats, if you follow my guidelines and put all the necessary security measures in place, then to a hacker you will no longer be considered an easy target and thus with a much greater chance of staying secure, you can look forward to peace of mind, safe in the knowledge that you are doing your best by any standards to keep your business, customers and suppliers secure and can look forward to a long and successful business.

**ABC (Always Be Cybersecure)**

**Risk Register**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ID | Date raised | Risk Description | Probability | Severity | Overall Risk | Mitigating Action |
| 1 | 03/11/21 | I could visit any dubious websites on any of your computers. | Frequent 4 | Catastrophic 4 | High 16 | Preventative measures need to be put in place to control and limit access to harmful websites. |
| 2 | 03/11/21 | No employee cyber awareness training. | Frequent 4 | Catastrophic 4 | High 16 | All employees/management to undergo in depth annual cyber & GDPR awareness training where each employee can only resume their normal duties upon successful completion of the exam |
| 3 | 03/11/21 | I was able to install software without any access issues. | Frequent 4 | Catastrophic 4 | High 16 | Decide on access privileges and how to prevent employees from installing harmful software |
| 4 | 03/11/21 | You have Remote Desktop open to the internet. | Frequent 4 | Catastrophic 4 | High 16 | Limit users who can log-in, use 2 Factor Authentication and ensure to disconnect or timeout after inactivity at the end of each session. |
| 5 | 03/11/21 | Staff are using the simplest passwords for hackers to exploit e.g. ‘guest’. Simple passwords can be cracked within minutes by experienced hackers who then have full access to the computer system. | Probable 3 | Catastrophic 4 | High 12 | Use strong passwords (mixed case, minimum 14 characters, including at least 1 special character) for all systems with each important program e.g. email, payroll, payment systems, requiring a different login and password per user. |
| 6 | 03/11/21 | Your employees are connecting their laptops and mobile devices to public wi-fi connections when they are travelling which leaves them wide open to attacks. | Probable 3 | Catastrophic 4 | High 12 | If they have to use public networks Employees should use a VPN when connecting that will encrypt their data and offer online privacy. |
| 7 | 03/11/21 | A server that isn’t backed | Probable 3 | Catastrophic 4 | High 12 | Backup your data: creating copies of data held within your systems & saving it to another device or to cloud storage.  Regular backups (preferably automatic) so that your backups are always up to date with your business operations. Have one backup that is not connected to your network, ideally in a separate secure location. |
| 8 | 03/11/21 | With the exception of finance and personnel folders I could copy and read any Customer, Sales/Marketing, Production, Research/development and Supply Chain Management files on your server. | Probable 3 | Critical 3 | Serious 9 | Control who is permitted access to business systems and folders based on their position and responsibilities within the company. |
| 9 | 03/11/21 | A consumer wireless router and switch. | Probable 3 | Critical 3 | Serious 9 | Upgrade from consumer grade to business routers. Business routers favour security, scalability, traffic management, Robust VPN support & remote access.  Business/Managed switches manage, configure and monitor your network better, giving you greater control over how data travels and who can access that data. |
| 10 | 03/11/21 | Daisy chain network: if a hacker gains access to one of your computer systems, they can then ‘piggyback’ onto other systems causing further damage. Daisy chain networks are also very slow and if there’s a problem with once device, it can cause the whole network to go down. | Probable 3 | Critical 3 | Serious 9 | Use a hierarchical network which has the following benefits:  Helps to design, install and maintain a high performance scalable, trustworthy, cost-effective hierarchical network.  Better management and troubleshooting to isolate network issues.  Better filters to cleanse traffic data |
| 11 | 03/11/21 | Your offsite hosted website for taking orders, keeping customer details and linking to an online payment service, written and currently maintained by a local software developer who you don’t seem to know much about. Could he have a conflict of interests? | Remote 2 | Catastrophic 4 | Serious 8 | A total revamp of your current website, online payment systems and all databases using a reputable software developer who is not local unless you recruit them full time and specialises in the design and maintenance of websites for medium size businesses. |
| 12 | 03/11/21 | Easy access to gain entry though the loading bay to the main office and MD’s office. | Remote 2 | Catastrophic 4 | Serious 8 | Barbed wire tall fences and locked gates on external perimeters.  To gain entrance to the building, warehouse staff should have separate access to office staff with strict security monitoring measures for employees to move between departments e.g. key cards & security monitoring 24/7/365.  To gain entry to the main office, you should first have to bypass a reception or security check which only allows authorised personal to pass through with CCTV and logging of each entry. |
| 13 | 03/11/21 | Server, printer and router in the MD’s office vulnerable to unauthorized access to print data obtained by hacking into the server or router. | Remote 2 | Critical 3 | Serious 6 | Servers, routers, switches, firewalls should be locked away and protected in layered security, making it impossible for intruders to gain physical access.  Servers should be held within the deepest layer and protected not only from unauthorised access, but also from the elements e.g. humidity, temperature, fire, water as well as motion/door sensors & CCTV. |
| 14 | 03/11/21 | Unattended PC’s left unlocked in the general office, giving anyone access to hack or steal data. | Remote 2 | Critical 3 | Serious 6 | Make it company policy for employees to lock their computers when left unattended. Update the settings on every pc to automatically lock after a short period of inactivity. |
| 15 | 03/11/21 | No USB security to control the access of devices to your USB ports | Occasional 2 | Critical 3 | High 6 | Make it company policy that personal or unknown USB devices including personal mobile phones cannot be plugged into company USB drives.  Use passwords and encryption on your USB drive to protect your data.  Disable autorun |

**Patch Management RACI chart**

**RACI: Responsible, Accountable, Consulted, Informed**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **System Administrator** | **Management** | **Non-management employees** | **Application owners** |
| Perform regular update scans and inform administrator when completed | AR | A |  | I |
| Evaluate the risk of applying the patch update | CR | A |  | I |
| For critical (zero-day attacks) identify the required resources and mitigation strategies if unable to patch immediately. | RC | A | I | I |
| Provide resources or authorise/reject mitigated level of risk | AC | RA |  | I |

**Risk Analysis Conclusion:**

I Found 15 critical vulnerabilities within your organization. Each vulnerability has a maximum threat score of 16 which equates to a total overall score of 240. Your level of risk from serious threats total score is a high 161 out of 240 with an average score of 10.73 / 16. You have at least a 67% of being breached and falling victim to a serious cyber threat.