Cyber Hygiene Report Template

# Introduction

In this assessment the tool should be used to generate an Hygiene score to relay to management and key stakeholders.

# Purpose

This project’s objective is to increase cybersecurity ecosystem resiliency by helping organisations to overcome the resource-intensive and often thankless nature of security hygiene. The project aims to increase awareness of the importance of security hygiene issues, recommend specific prioritised actions to overcome common obstacles, and establish a natural path for organisations to continue on to achieve a comprehensive security hygiene program based on existing standards, guidance, and publications.

The driver behind security hygiene is that there are a relatively small number of root causes for many data breaches, malware infections, and other security incidents. Implementing a few relatively simple practices can address those root causes to prevent many incidents from occurring and to lower the potential impact of incidents that still occur. In other words, security hygiene practices make it harder for attackers to succeed and reduce the damage they can cause.

Even though there is widespread recognition that patching can be incredibly effective at mitigating security risk, patching is often resource-intensive, and the act of patching itself can reduce system and service availability. Attempts to reduce resource utilisation and expedite patch distribution, such as not testing patches before production deployment, can inadvertently break system functionality and disrupt operations, in some cases causing a significant negative impact to the organisation. On the other hand, delays in patch deployment create a larger window of opportunity for attackers

Patching is a particularly important component of cyber hygiene, but existing tools are insufficient for many environments and situations. For example, many organisations lack tools to help them measure and assess the effectiveness and timeliness of their patching efforts. Many organisations also struggle to prioritise patching efforts, test patches before deployment, and adhere to policies for how quickly patches need to be applied in different situations.

Each organisation must balance security with mission impact and business objectives, and figure out their risk tolerance for each. Recent cybersecurity attacks have highlighted the dangers of having equipment that has not been patched. Even with recent events and the historical attacks that have been successfully carried out due to unpatched systems, patching remains a problem.

# Scope

The assessment reviews physical equipment, software, configurations, hardware, people and process compliance for the company.

The objective of this project is to demonstrate a proposed approach for improving enterprise patching practices for general IT systems. In this project, commercial and open source tools will be used to aid with the most challenging aspects of patching, including system characterisation and prioritisation, patch testing, and patch implementation tracking and verification. These tools will be accompanied by actionable, prescriptive guidance on establishing policies and processes for the entire patching life cycle, to include defining roles and responsibilities for all affected personnel, and establishing a playbook with rapid mitigation actions for destructive malware outbreaks that organisations can execute tactically in the first 30 days, and recommendations that can be implemented strategically beyond 30 days. The scope of this building block is general IT systems. There are additional challenges with patching for legacy IT systems and virtual systems, as well as industrial control systems (ICS), Internet of Things (IoT) devices, and other technologies stemming from operational technology (OT). Future work could add some or all of these system types to the building block. All aspects of security hygiene other than those related to patching are out of the scope of this project.

# Security Hygiene Checklist

# Introduction

Risk assessment tools can greatly assist an agency in determining the gaps in its information security program and provide guidance and direction for improvement. The way it is done is by using a very simple “Yes or No” questionnaire to determine a large amount of information for consistency throughout the results given by the employee's.

# How to Interpret your results

The way the data is interpreted is once the questorners are all correlated together they will put them through the computer to add up the amounts of the yes and no's to see how the employees answered the questions with an overall mark. It is one by adding up all the questions of the questions, example being ten and if the score is below or five they need to improve their cyber hygiene to have adequate protection. If the score is above five and below 7, they might need to think of something in the near future but not that urgent. If there is a score above eight, that is deemed considered adequate.

# Hygiene Checklist

**Equipment and Operation**

|  |  |  |  |
| --- | --- | --- | --- |
| **Questions** | **Yes** | **No** | **ISO 27002-2015 Section NIST** |
| 1. Are there controls against malware with appropriate user awareness? |  |  | Section 12.2.1 |
| 1. Is there a backup policy in place to regulate information backup and routine software & system image tests? |  |  | Section 12.3.1 |
| 1. Are events such as user activities, exceptions, faults and information security events being logged and reviewed? |  |  | Ssction 12.4.1 |
| 1. Are there procedures to control the installation of software on operational systems? |  |  | Section 12.5.1 |
| 1. Are information about technical vulnerabilities of information systems being obtained in a timely fashion? |  |  | Section 12.6.1 |
| 1. Are development, testing, and operational environments separated to minimise unauthorised access risk? |  |  | Section 12.1.4 |
| 1. Are operational procedure documents available to all users? |  |  | Section 12.1.1 |
| 1. Are logging facilities and log information protected against tampering and unauthorised access? |  |  | Section 12.4.2 |
| 1. Are there rules in place to govern the installation of software? |  |  | Section 12.6.2 |
| 1. Are system admin & operator activities logged and regularly reviewed? |  |  | Section 12.4.3 |
| **Score:** |  |  | **Total:** |

**Physical Security**

|  |  |  |  |
| --- | --- | --- | --- |
| **Questions** | **Yes** | **No** | **ISO 27002-2015 Section NIST** |
| 1. Do you have policies and procedures for authorization of physical access to electronic information? |  |  | Section 11.1.1 |
| 1. Do you have policies and procedures specify methods used to control physical access to you secure areas like door locks, access control systems and security officers? |  |  | Section 11.1.1 |
| 1. Is access to your computing area controlled? |  |  | Section 11.1.2 |
| 1. Is their surveillance within and outside the property for protection? |  |  | Section 11.1.2 |
| 1. Secure offices, rooms and facilities? |  |  | Section 11.1.3 |
| 1. Is their physical protection against malicious attacks or accidents? |  |  | Section 11.1.4 |
| 1. Are their locations to store equipment securely? |  |  | Section 11.2.1 |
| 1. Are there supporting utilities in case of power failures and other disruptions? |  |  | Section 11.2.2 |
| 1. Is their cabling security on the interior and exterior of the building? |  |  | Section 11.2.3 |
| 1. Are the current software being used up to date and licensed? |  |  | Section 11.2.7 |
| **Score:** |  |  | **Total:** |

**Wireless Network**

|  |  |  |  |
| --- | --- | --- | --- |
| **Questions** | **Yes** | **No** | **ISO 27002-2015 Section NIST** |
| 1. Are users provided with the correct authorization on the network? |  |  | Section 9.1.2 |
| 1. Ensuring authorized user access to correct systems |  |  | Section 9.2 |
| 1. Are workers bringing the correct user IDs into work? |  |  | Section 9.2.1 |
| 1. Once an employee leaves, is their user account deleted? |  |  | Section 9.2.2 |
| 1. Do users have privilege access rights? |  |  | Section 9.2.2 |
| 1. Is the wireless network available from the car park? |  |  | Section 9.2.2 |
| 1. Does the boss review the user account on a regular basis? |  |  | Section 9.3 |
| 1. Is there a use of secret authentication in the office |  |  | Section 9.3.1 |
| 1. Are the employers able to prevent unauthorized access to systems? |  |  | Section 9.4 |
| 1. Is there a secure log on procedures for the company's computers? |  |  | Section 9.4.2 |
| **Score:** |  |  | **Total:** |

**Electronic Security Concerns**

|  |  |  |  |
| --- | --- | --- | --- |
| **Questions** | **Yes** | **No** | **ISO 27002-2015 Section NIST** |
| 1. Do passwords have an 8 character minimum? |  |  | ISO/IEC 27002 9.1.1 - 9.2.3 |
| 1. Are passwords changed every 3 months? |  |  | ISO/IEC 27002 9.1.1 - 9.2.3 |
| 1. Are passwords kept confidential between employees? |  |  | ISO/IEC 27002 9.1.1 - 9.2.3 |
| 1. Is Two factor authentication enabled? |  |  | ISO/IEC 27002 9.1.1 - 9.2.3 |
| 1. Do users only have necessary permissions? |  |  | ISO/IEC 27002 9.1.1 - 9.2.3 |
| 1. Are access controls enforced? |  |  | ISO/IEC 27002 9.1.1 - 9.2.3 |
| 1. Are uncessessory privileges removed regularly? |  |  | ISO/IEC 27002 9.1.1 - 9.2.3 |
| 1. Is plain ftp disabled? |  |  | ISO/IEC 27002 9.1.1 - 9.2.3 |
| 1. Is hardware/software security updates applied regularly? |  |  | ISO/IEC 27002 9.1.1 - 9.2.3 |
| 1. Are unusual login/authentication attempts logged? |  |  | ISO/IEC 27002 9.1.1 - 9.2.3 |
| **Score:** |  |  | **Total:** |

**Data Backup Procedure**

|  |  |  |  |
| --- | --- | --- | --- |
| **Questions** | **Yes** | **No** | **ISO 27002-2015 Section NIST** |
| 1. Are backups stored in a remote location? |  |  | Backups ISO/IEC 27002 A.12.3.1 |
| 1. Are the backups stored in a secure & safe location from theft and environmental damage? |  |  | Backups ISO/IEC 27002 A.12.3.1 |
| 1. Are the backups disposed of so that data cannot be read or recovered? |  |  | Backups ISO/IEC 27002 A.12.3.1 |
| 1. Are the backups protected with a password? |  |  | Backups ISO/IEC 27002 A.12.3.1 |
| 1. Is backup media and equipment being regularly tested? |  |  | Backups ISO/IEC 27002 A.12.3.1 |
| 1. Are the backups done regularly in a son, father, grandfather rotation? |  |  | Backups ISO/IEC 27002 A.12.3.1 |
| 1. Has the integrity of the backups been verified? |  |  | Backups ISO/IEC 27002 A.12.3.1 |
| 1. Are backups containing confidential information being encrypted? |  |  | Backups ISO/IEC 27002 A.12.3.1 |
| 1. Is customer data being backed up? |  |  | Backups ISO/IEC 27002 A.12.3.1 |
| 1. Are operating system backups being done? |  |  | Backups ISO/IEC 27002 A.12.3.1 |
| **Score:** |  |  | **Total:** |

**Online Access and Purchase**

|  |  |  |  |
| --- | --- | --- | --- |
| **Questions** | **Yes** | **No** | **ISO 27002-2015 Section NIST** |
| 1. Online portals (customer-facing & internal) are able to be accessed timely and with decent responsiveness. |  |  | Capacity Management ISO/IEC 27002 A.12.1.3 |
| 1. Network content should be kept private, secured and accessible to relevant individuals |  |  | Network Controls ISO/IEC 27002 A.13.1.1 |
| 1. Disclaimer issued for individuals using the Chameleon online processes (intranet or otherwise) |  |  | Security Of Network Services ISO/EAC 27002 A.13.1.2 |
| 1. Customer-facing network activities should be kept adjacent/distant from intranet/company network activity |  |  | Segregation In Networks ISO/EAC 27002 A.13.1.3 |
| 1. Customer transactions/interaction with the network are to be secured with SSL & certificate. |  |  | Information Transfer Policies and Procedures ISO/EAC 27002 A.13.2.1 |
| 1. Customer/s are prompted with information pertaining to how their information is handled or otherwise utilised |  |  | Agreements On Information Transfer ISO/EAC 27002 A.13.2.2 |
| **Score:** |  |  | **Total:** |

|  |  |
| --- | --- |
| **Calculated Hygiene Ranking** | **Percentage:** |
| **Overall Cyber Hygiene Score:** |  |
| **Equipment and Operation** |  |
| **Physical Security** |  |
| **Wireless Network** |  |
| **Electronic Security Concerns** |  |
| **Data Backup Procedure** |  |
| **Online Access and Purchasing** |  |

# Mitigation Strategy

**Priority: Low / Medium / High**

**Suggest action mitigation within: … weeks / months**

# Electronic Security Concerns

Remediation

* Security assets (cameras, video recording devices etc.) should only be accessed by staff or kept from public sight. Store floor assets should be locked and be tamper-proof without specific tools or professional servicing.

Priority:

Suggest action mitigation within:

* If connected to wireless infrastructure ensure that security assets are either hard-wired OR have encrypted signal access to prevent MitM or similar.

Priority:

Suggest action mitigation within:

* Ensure that assets are up-to-date and that hardware and software are regularly maintained/updated as necessary.

Priority:

Suggest action mitigation within:

* Restrict access to electronic security assets to specific staffing tiers (least access policy). (Priority **…** / Suggest action mitigation within **…**)

Priority:

Suggest action mitigation within:

* Ensure a backup power supply (redundancy) is active to prevent a power short allowing security bypass.

Priority:

Suggest action mitigation within:

* Password requirement policies in-place. 8 character minimum, requires capital letter, passwords changed regularly.

Priority:

Suggest action mitigation within:

# Physical Security

Remediation

* Guards in store should be made aware of restrictions regarding physically manipulating suspected criminals (i.e. policy should be made to incorporate police actions and step-by-step theft procedures that preferably do not involve physical intervention.

Priority:

Suggest action mitigation within:

* Locks should be of adequate standard and resistant to low-tier B&E methods. Biometric locks, whilst extreme, should be used for higher level security (i.e. server rooms or surveillance rooms).

Priority:

Suggest action mitigation within:

* Desks (such as POS and secretarial/reception) should be aligned in such a way that they look out over the store floor but do not allow customers to peek (‘shoulder surf’) staff using terminals or documentation. Ideally should be behind locked, short half-doors that only staff can access but do not create a hostile environment of full enclosure.

Priority:

Suggest action mitigation within:

* Security tags (dependent on cost) should be attached to more expensive items depending on cost, and associated with a door-mounted alarm system.

Priority:

Suggest action mitigation within:

* Signs indicating surveillance should be mounted in-store (NOTE: may also be used if no actual surveillance is taking place to act as a deterrent.)

Priority:

Suggest action mitigation within:

* Doors and gates should be shatter/break resistant. As brute-force is likely the most common forcible access type, ensuring that materials are suitable to safety standards and policy (store, organisation and shopping centre as implied).

Priority:

Suggest action mitigation within:

* Glass frontage and viewing surfaces should be shatter-resistant whilst not restricting customer vision.

Priority:

Suggest action mitigation within:

# Wireless Network

Remediation

* Wireless encryption should be civilian standard (WPA2 minimum).

Priority:

Suggest action mitigation within:

* Wireless broadcast distance should be reduced to minimum of store/office distance and no further. Additionally the WAP may be made invisible for extra security.

Priority:

Suggest action mitigation within:

* Optional: wirelessly connected assets may be limited to MAC addresses.

Priority:

Suggest action mitigation within:

* Ensure that signal is reliable and clear; may be advised to include a 4/5G sim card into the router to prevent drop-outs causing ceased EFTPOS etc.

Priority:

Suggest action mitigation within:

# Data Backup Procedure

Remediation

* Where possible keep both a hard-copy of security vision and data AND an electronic (i.e. hard drive) resource.

Priority:

Suggest action mitigation within:

* For hard copy of data, ensure that data rotation (son, father, grandfather) occurs on a cyclic basis. More vital for central server/mainframe but individual shops may also engage in this practice depending on security breaches, goods loss etc.

Priority:

Suggest action mitigation within:

* Practice least-access for staff access to secured data.

Priority:

Suggest action mitigation within:

* Keep data and backup data in secured, reinforced locations to prevent degaussing, damage to data etc.

Priority:

Suggest action mitigation within:

* Establish and follow backup procedures. The procedures should address the frequency and type of backups, storage of backup media, testing of backup and restore functions, and retention. Recommend installing commercial backup software on both servers and a DAT or DVD-RW drive in one server to be used for backing up both servers. In addition to the scheduled backup, a full backup of each server should be completed prior to upgrading the operating system or installing patches. Storage facilities for the backup media should be fireproof and have controlled access. This recommendation can be accomplished by using a small fireproof safe for local storage. There are a number of options for off-site backup media storage, including specialized secure storage companies that will pick-up and deliver the media and rent a secure storage.

Priority:

Suggest action mitigation within:

* Frequency: Perform backups on a regular basis as identified in the security policy. Full backups can be time-consuming, therefore perform monthly or weekly backups with frequent partial backups of changed files.

Priority:

Suggest action mitigation within:

* Storage: Always validate backups to ensure the integrity of the data and validate the file restoration procedures.

Priority:

Suggest action mitigation within:

* Security: Backups should be transported to an approved offsite storage location on a daily, weekly, or monthly rotation, as required by the security policy.

Priority:

Suggest action mitigation within:

* Validation: Backups should be protected using strong passwords. The password is required to restore the data.

Priority:

Suggest action mitigation within:

* Disposing of backup data: All backup data must be disposed of appropriately to ensure that: The drive no longer contains sensitive data and that the drive's current or past contents cannot be read or recovered.

Priority:

Suggest action mitigation within:

* Storing Backups**:** Must be saved with a short description which contains the following: Backup date, resource name and the type of backup method (Full or Incremental).

Priority:

Suggest action mitigation within:

Online Access and Purchase

Remediation

* Ensure that the website is maintained on a regular basis (preferably by a dedicated web administrator) and up-to-date with internet standards, plug-ins and associated software.

Priority:

Suggest action mitigation within:

* Test for web vulnerabilities on a regular basis.

Priority:

Suggest action mitigation within:

* Stipulate customer data handling policies; expiration of data (for deletion), in case of breaches, notification policies etc.

Priority:

Suggest action mitigation within:

* Subject the webpage/company entry points to random security tests (NOTE: if commercially viable) periodically. Any detected vulnerabilities should be dealt with ASAP and on a professional basis.

Priority:

Suggest action mitigation within:

* Ensure staff credentials are rotated (preferably annually) and that staff understand and practice good cyber hygiene as stipulated by official company policy/s.

Priority:

Suggest action mitigation within:

* In the event of breaches caused by lax staff implement punitive measures in line with company policy.

Priority:

Suggest action mitigation within:

* Keep webpage status in line with professional enterprise-tier tools.

Priority:

Suggest action mitigation within:

# Equipment and Operations:

# Remediation

* The wireless security WPA should be upgraded to Wi-Fi Protected Access 2, WPA2 for wireless networks to provide stronger data protection and network access control.

Priority:

Suggest action mitigation within:

* Ensuring that all electrical devices are up-to-date and making sure all computers have Windows 10 installed.

Priority:

Suggest action mitigation within:

* Separate the databases to different servers to ensure higher security of each database and prevent all files to be compromised when one is breached.

Priority:

Suggest action mitigation within:

* Disable paypass contactless payment facility on EFTPOS machines.

Priority:

Suggest action mitigation within: