Sample Pty Ltd

Cyber Security Assessment for Board/C Suite focused on handling Sensitive Data and in line with DISP , ITAR and ACSC ISM

GuardWare ASSESSOR

Briefing Intent

- This sample is indicative of the report which you'll receive at the end of an assessment.
- This redacted report is from assessments done on a number of Defence Suppliers.
- The report provides clarity around the type of user behaviour, data movement and cyber risks that you can expect to be covered during the assessment.

Assessment Scope

The scope of GuardWare Assessment is to assess Client's current security processes and controls (ISMS) based on the following criteria:

1. **Ability to securely handle commercially sensitive data in line with Information Security Manual (ISM) recommendations.**
2. **Ability to securely handle Defence related data in line with the requirements of Entry Level DISP.**
3. **Ability to securely handle ITAR related data.**

Note: Physical security of office environment and equipment is out of scope for this project.

Assessment Summary

Monitoring Parameters:

- Only Client owned devices were covered.
- The following types of data were monitored:
  - Sensitive data covering ITAR and Defence labelled information
  - Generic Documents
  - General files of any type including source code, images, zip etc
- Monitoring USE CASES included those recommended under ACSC ISM, ITAR and for secure handling for Defence Related Data under DISP.

Monitoring done from 26th Nov to 13th Dec 2022	158 users monitored on 146 devices
16 High risk actions detected which require urgent attention	4 Medium risk actions detected
2 suspicious activities detected – Need urgent action	No controls in place to ensure secure handling of Sensitive data
No incident detection capability present in the event of a loss or theft of data	Non-Compliance with 2 of ES8 control. App Control and Restrict Admin privileges
Non-Compliance with Secure Defence data handling procedures as per DISP and ISM	Non-Compliance with ITAR regulation.

Risk Summary

Use Cases	Technical Control Implemented/Partial/Not Implemented/Failed Control	Risk Level (No Risk, Low, Medium, High)
Data transfer using external storage media		
High use of unencrypted USBs. 44 users detected using unencrypted USBs to transfer data.	**Technical control not implemented**	**High**
High transfer rate. 8 users transferred over 1000 files.	**Technical control not implemented**	**High**
Outside of normal business hours. High rate of transfers detected outside of normal working hours.	**Technical control not implemented**	**High**
Transfer of Potential Sensitive Data. • Top 8 users detected transferring 1000s of design related files. • Several users transferred files containing potential sensitive data	**Technical control not implemented**	**High**
Visibility of transfers. Visibility of sensitive data transferred using external media	**Technical control not implemented**	**High**
Suspicious User Activities		
Suspicious User Activity – User1 - **Use of personal emails to send corporate data** 1. User detected using his personal email to send highly sensitive ITAR marked data to unauthorized 3rd parties. 2. Non-Compliance under ITAR.	**Technical control not implemented**	**High**
Suspicious User Activity – User2 – **Data copied by user about to leave the organisation.** 1. User copied 1000s of design files also printed his CV during the same time. 2. There is evidence he has visited job sites (Indeed) and applied for Defence related engineering jobs around the same time when he copied the files. 3. The files have been copied on unencrypted USBs which most likely are personal. 4. He is also seen accessing and uploading files to personal Google Drive. 5. He belongs to the Defence User Group.	**Technical control not implemented**	**High**

Use Cases	Technical Control Implemented/Partial/Not Implemented/Failed Control	Risk Level (No Risk, Low, Medium, High)
Corporate Email Analysis		
Corporate emails forwarded to own personal emails. Email detected being forwarded to user own personal email.	**Technical control not implemented**	**Medium**
Visibility of email forwards. Visibility of what files have been forwarded by users to personal and free emails to ensure they are accounted for.	**Technical control not implemented**	**High**
Use of Personal Emails		
Use of Personal emails detected. Personal emails have been used to send data.	**Technical control not implemented**	**High**
Visibility of Personal Email Use. Visibility is required to ensure company data is not being sent out via personal emails.	**Technical control not implemented**	**High**
Use of Non Organisational Unauthorised Applications		
Technical Control Circumvented. The users seem to have found a way to install non-organisational applications. **Non-Compliance of 2 of the ES8 Controls.** 1. Restrict administrative privileges 2. Application control	**Failed Technical Control**	**High**
Visibility of Application Use. Visibility of what applications are being used by users.	**Technical control not implemented**	**High**
Data transfer using Non-Corporate Data sharing APPs and Websites		
Risky Transfer Application Use. 6 users detected using Dropbox or Google Drive to transfer files. Transfers include potentially sensitive data.	**Failed Technical Control**	**High**
Risky website Use.19 users detected using Facebook and potentially transferring data.	**Technical control not implemented**	**High**
Visibility of transfers. Visibility of sensitive data transferred using APPs and encrypted websites.	**Technical control not implemented**	**High**

Use Cases	Technical Control Implemented/Partial/Not Implemented/Failed Control	Risk Level (No Risk, Low, Medium, High)
Printing of Sensitive Data		
Printing of potential sensitive data. Printing of sensitive data was observed.	**Technical control not implemented**	**Medium**
Printing use personal Printers. As users are allowed to work from home there is risk of files being printed using home printers.	**Technical control not implemented**	**Medium**
Visibility of Printing. Visibility of what files have been printed either via organisational or personal printers to ensure they are accounted for.	**Technical control not implemented**	**Medium**
Access of information		
Authorised Access of sensitive Information. Ensuring authorised users can access files	**Implemented**	**No Risk**
Access Visibility. Visibility of who is accessing what files	**Implemented**	**No Risk**

Trusted Insider Program monitoring suggestion as per ISM and DISP

Trusted insider program

As a trusted insider's system access and knowledge of business processes often makes them harder to detect, establishing and maintaining a trusted insider program can assist an organisation to detect and respond to trusted insider threats before they occur, or limit damage if they do occur. In doing so, an organisation will likely obtain the most benefit by logging and analysing the following user activities:

1. excessive copying or modification of files
2. unauthorised or excessive use of removable media
3. connecting devices capable of data storage to systems
4. unusual system usage outside of normal business hours
5. excessive data access or printing compared to their peers
6. data transfers to unauthorised cloud services or webmail
7. use of unauthorised Virtual Private Networks, file transfer applications or anonymity networks.

Control: ISM-1625; Revision: 1; Updated: Dec-22; Applicability: All; Essential Eight: N/A
A trusted insider program is developed, implemented and maintained.

Control: ISM-1626; Revision: 0; Updated: Nov-20; Applicability: All; Essential Eight: N/A
Legal advice is sought regarding the development and implementation of a trusted insider program.

Reference: ACSC Information Security Manual.

Mapping to Trusted Insider USE CASEs as per ACSC ISM

Recommended Use Cases Under ISM	Detected/Not Detected/Not Tested
excessive copying or modification of files	Detected
unauthorised or excessive use of removable media	Detected
connecting devices capable of data storage to systems	Detected
unusual system usage outside of normal business hours	Detected
excessive data access or printing compared to their peers	Detected
data transfers to unauthorised cloud services or webmail	Detected
use of unauthorised Virtual Private Networks, file transfer applications or anonymity networks.	Detected

Mapping to Entry Level DISP requirements

Entry Level DISP Requirements	Current Status in Client	Compliant/Non-Compliant
Meeting top 4 requirements of the ACSC Essential 8: • Application control; • Patch applications; • Restrict administrative privileges; • Patch operating systems	Potential use of non-organisational applications has been observed. If these were explicitly not allowed by Admin the company will fail the following ACSC ES8 Controls. 1. Restrict administrative privileges. 2. Application control.	Non-Compliant
Handling Official and Official Sensitive information as per DSPF and ISM. The requirements place a **Need to** requirement when accessing, transferring and printing sensitive information. Further transfer of Official information should be done using encrypted channels.	The company lacks visibility of users accessing, transferring and printing data and has no technical means to verify the **Need** of any of the actions. Further use of unencrypted external storage devices has been observed.	Non-Compliant
Insider Threat Program. Under this requirement users are required to handle sensitive information appropriately.	The company lacks visibility of users accessing, transferring and printing data and has no way to verify if the correct steps are being taken by the staff members on an ongoing basis	Non-Compliant
Incident Detection and Response. Under this requirement clear visibility of risky incidents involving sensitive data is required. Only when you know that data has been put at risk can you try and address it through appropriate responses.	The company lacks visibility of users accessing, transferring and printing data. This can place company's data at risk without their knowledge.	Non-Compliant

Storage Media Analysis

Covers all types of media including phone sync.

The Dangers of USB Drives

USB drives, sometimes known as thumb drives, or Memory Sticks, are small, readily available, inexpensive, and portable, so they are popular for storing and transporting files from one computer to another.

However, these same characteristics make them appealing to attackers.

Attackers can use USB drives to infect computers with malware that automatically runs when the USB drive is inserted into a computer. The malware remains on the USB, infecting every computer it is inserted into.

Attackers may also use their USB drives to steal information directly from a computer, If physical access to the computer is possible.

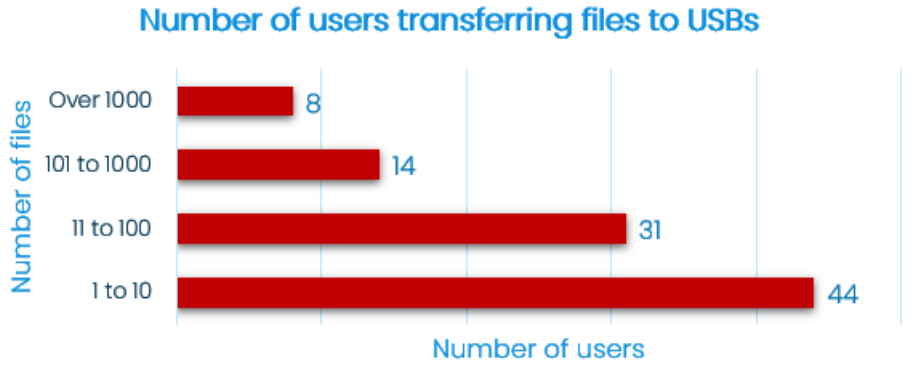
The most obvious security risk for USB drives, though, is that they are easily lost or stolen. If the information on the drive is not encrypted, anyone who has the USB drive can access the data on it.

How can you protect your data?

- **Do not plug an unknown USB drive into your computer.** If you find a USB drive, give it to the appropriate authorities (a location's security personnel, your organization's information technology [IT] department, etc.). Do not plug it into your computer to view the contents or to try to identify the owner.
- **Take advantage of security features.** Use passwords and encryption on your USB drive to protect your data, and make sure that you have the information backed up in case your drive is lost.
- **Keep personal and business USB drives separate.** Do not use personal USB drives on computers owned by your organization, and do not plug USB drives containing corporate information into your personal computer.
- **Disable Autorun.** The Autorun feature causes removable media such as CDs, DVDs, and USB drives to open automatically when they are inserted into a drive. By disabling Autorun, you can prevent malicious code on an infected USB drive from opening automatically.
- **Use and maintain security software and keep all software up to date.** Use a firewall, antivirus software, and anti-spyware software to make your computer less vulnerable to attacks. Ensure you keep the virus definitions current! Also, keep the software on your computer up to date by applying any necessary patches

Data transfer using USBs

Data transfer using external storage media		
High use of unencrypted USBs. 44 users detected using unencrypted USBs to transfer data.	**Technical control not implemented**	**High**
High transfer rate. 8 users transferred over 1000 files.	**Technical control not implemented**	**High**
Outside of normal business hours. High rate of transfers detected outside of normal working hours.	**Technical control not implemented**	**High**



The use of USBs may be for legitimate reasons but there are significant risks involved.

Risk. Loss of phone or USBs is a common source of data breach and should be monitored and accounted for.

Risk. Potential Insider risk. Non-compliant with Trusted Insider Program monitoring requirements as per the ISM.

Risk. Non-compliance risk to DISP/DSPF. Under these regulations there should be a valid NEED for transferring Defence related information and there should be appropriate visibility to ensure Insider Threat Management and Incident Response in case of loss.

Risk. Use of unencrypted USBs can easily lead to Data loss

User Name	User Group	Total Events
xxxxx	Customer Group	26256
xxxxx	Customer Group	5221
xxxxx	Customer Group	4212
xxxxx	Customer Group	3362
xxxxx	Customer Group	2326
xxxxx	Customer Group	2125
xxxxx	Customer Group	1782
xxxxx	Customer Group	1506
xxxxx	Customer Group	9
xxxxx	Customer Group	5
xxxxx	Customer Group	4
xxxxx	Customer Group	3
xxxxx	Customer Group	2
xxxxx	Customer Group	2

Hour	Working Day	Non-Working Day
0:00 - 1:00	0	0
1:00 - 2:00	0	0
2:00 - 3:00	0	0
3:00 - 4:00	0	0
4:00 - 5:00	0	0
5:00 - 6:00	0	0
6:00 - 7:00	0	0
7:00 - 8:00	0	0
8:00 - 9:00	562	0
9:00 - 10:00	41	320
10:00 - 11:00	10	8798
11:00 - 12:00	2	331
12:00 - 13:00	2221	4444
13:00 - 14:00	14	2144
14:00 - 15:00	5312	0
15:00 - 16:00	18620	0
16:00 - 17:00	421	0
17:00 - 18:00	2904	0
18:00 - 19:00	7563	0
19:00 - 20:00	33111	0
20:00 - 21:00	7	0
21:00 - 22:00	5	0
22:00 - 23:00	2	0
23:00 - 24:00	2	0

Movement of Sensitive Data using USBs

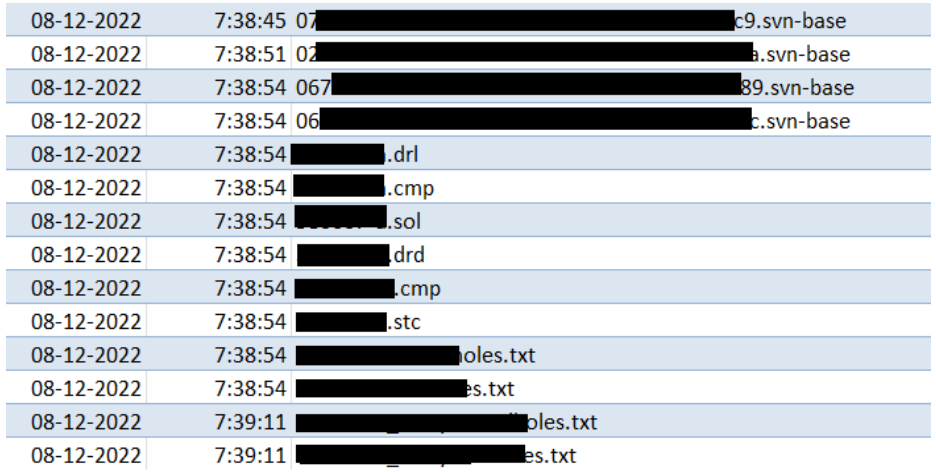
Data transfer using external storage media		
Transfer of Potential Sensitive Data. • Top 8 users detected transferring 1000s of design related files. • Several users transferred files containing potential sensitive data	**Technical control not implemented**	**High**
Visibility of transfers. Visibility of sensitive data transferred using external media	**Technical control not implemented**	**High**

Risk. Without the ability to monitor what is transferred, the company will not even know if data is lost or stolen and will not be able to perform Incident management.

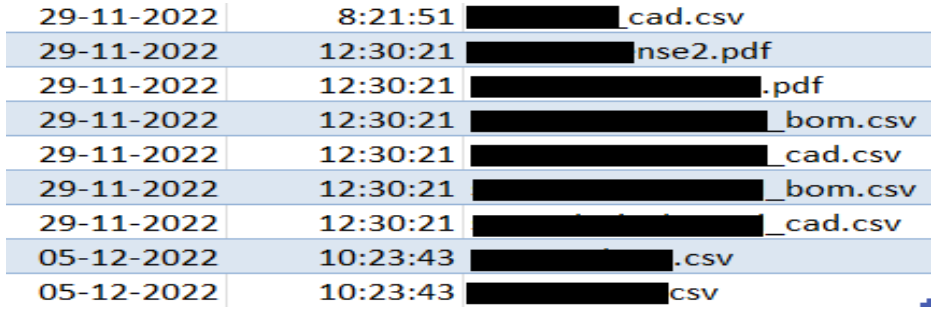
Risk. Potential Insider risk. Non-compliant with Trusted Insider Program monitoring requirements as per the ISM.

Risk. Non-compliance risk to DISP/DSPF. Under these regulations there should be a valid NEED for transferring Defence related information and there should be appropriate visibility to ensure Insider Threat Management and Incident Response in case of loss.

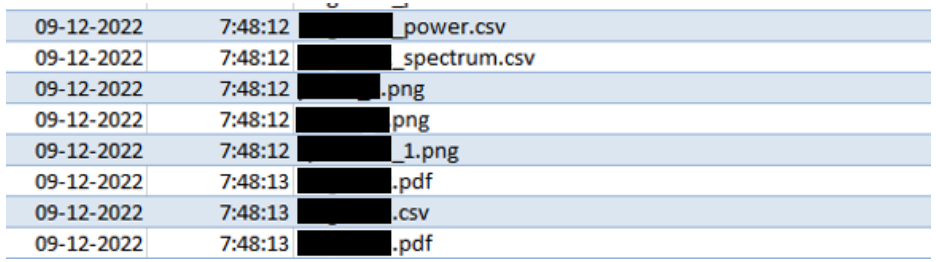
Risk. Use of unencrypted USBs can easily lead to Data loss



User 1



User 2



User 3

Suspicious User Activity

Insider Threats

An insider threat can be either unintentional or intentional.

Malicious insiders can be employees, former employees, contractors or business associates who have legitimate access to your systems and data, but use that access to destroy data, steal data or sabotage your systems. It does not include well-meaning staff who accidentally put your cyber security at risk or spill data.

•**Unintentional Threat**

- Negligence – An insider of this type exposes an organization to a threat through carelessness. Negligent insiders are generally familiar with security and/or IT policies but choose to ignore them, creating risk for the organization. Examples include allowing someone to "piggyback" through a secure entrance point, misplacing or losing a portable storage device containing sensitive information, and ignoring messages to install new updates and security patches.
- Accidental – An insider of this type mistakenly causes an unintended risk to an organization. Organizations can successfully work to minimize accidents, but they will occur; they cannot be completely prevented, but those that occur can be mitigated. Examples include mistyping an email address and accidentally sending a sensitive business document to a competitor, unknowingly or inadvertently clicking on a hyperlink, opening an attachment that contains a virus within a phishing email, or improperly disposing of sensitive documents.

•**Intentional Threats** - Intentional threats are actions taken to harm an organization for personal benefit or to act on a personal grievance. The intentional insider is often synonymously referenced as a "malicious insider." The motivation is personal gain or harming the organization. For example, many insiders are motivated to "get even" due to unmet expectations related to a lack of recognition (e.g., promotion, bonuses, desirable travel) or even termination. Their actions include leaking sensitive information, harassing associates, sabotaging equipment, or perpetrating violence. Others have stolen proprietary data or intellectual property in the false hope of advancing their careers.

•**Other Threats**

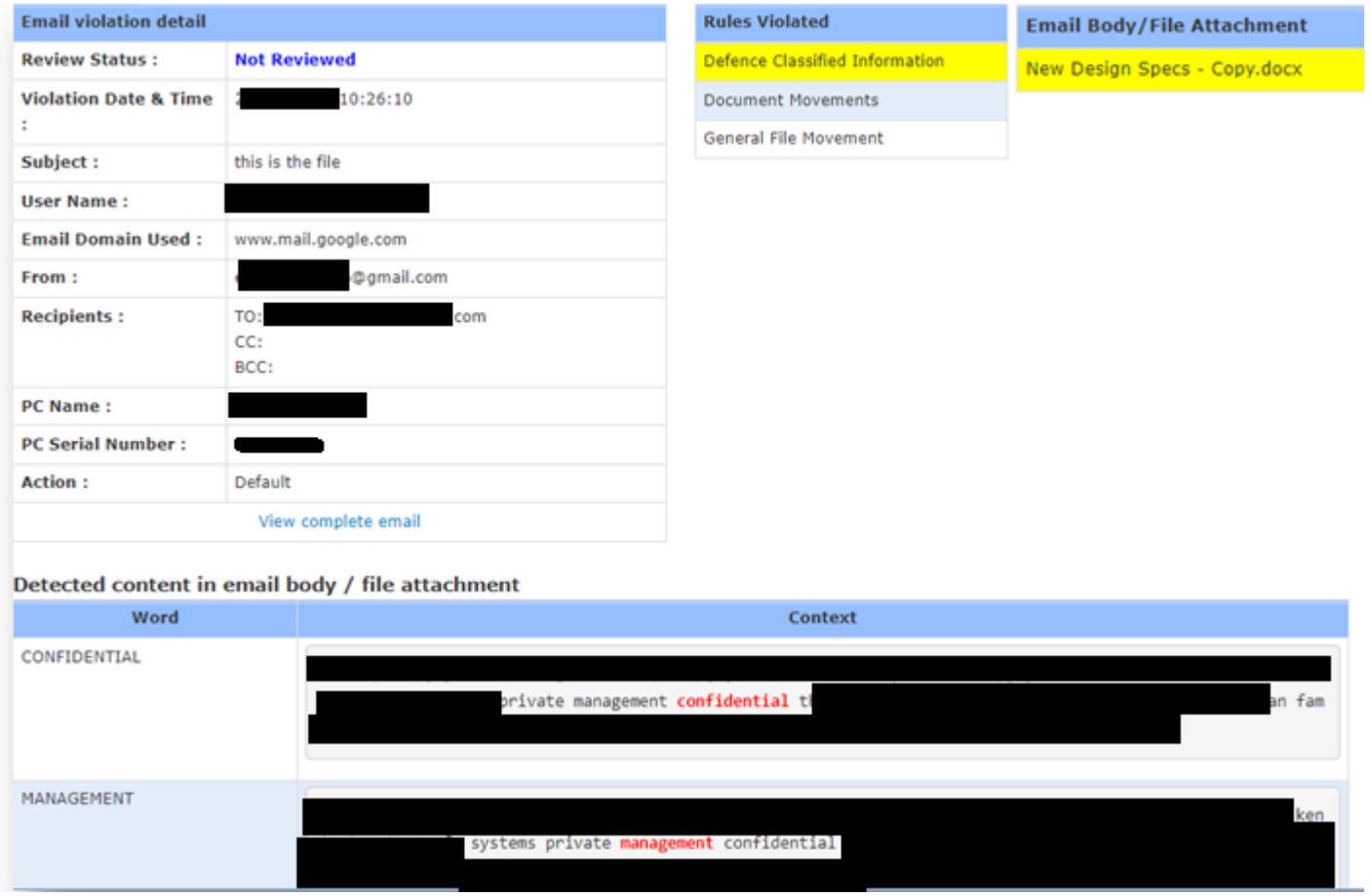
- **Collusive Threats** – A subset of malicious insider threats is collusive threats, where one or more insiders collaborate with an external threat actor to compromise an organization. These incidents frequently involve cybercriminals recruiting an insider or several insiders to enable fraud, intellectual property theft, espionage, or a combination of the three.
- **Third-Party Threats** – Additionally, third-party threats are typically contractors or vendors who are not formal members of an organization, but who have been granted some level of access to facilities, systems, networks, or people to complete their work. These threats may be direct or indirect threats.
  - Direct threats are individuals who act in a way that compromises the targeted organization.
  - Indirect threats are generally flaws in systems that expose resources to unintentional or malicious threat actors.

Suspicious User Activity – User1 - Suspicious User Activity – User1 - **Use of personal emails to send corporate data**

Suspicious User Activity		
Potential Insider Risk. 1. User detected using his personal email to send highly sensitive ITAR marked data to unauthorized 3rd parties. 2. Non-Compliance under ITAR.	**Technical control not implemented**	**High**

Use of personal emails is a common occurrence in organisations but needs to be monitored as can lead data leak.

Risk: Use of personal emails to exfiltrate data out consistently reported as one of the key ways data is lost or stolen in organisations and needs to be monitored.



Email violation detail	
Review Status :	Not Reviewed
Violation Date & Time :	[redacted]10:26:10
Subject :	this is the file
User Name :	[redacted]
Email Domain Used :	www.mail.google.com
From :	[redacted]@gmail.com
Recipients :	TO:[redacted]com CC: BCC:
PC Name :	[redacted]
PC Serial Number :	[redacted]
Action :	Default

View complete email

Rules Violated
Defence Classified Information
Document Movements
General File Movement

Email Body/File Attachment
New Design Specs - Copy.docx

Detected content in email body / file attachment

Word	Context
CONFIDENTIAL	[redacted] private management confidential t[redacted]an fam
MANAGEMENT	[redacted]ken systems private management confidential

Suspicious User Activity – User2 – Data copied by user about to leave the organisation.

Suspicious User Activity		
Potential Insider Risk. 1. User copied 1000s of design files also printed his CV during the same time. 2. There is evidence he has visited job sites (Indeed) and applied for Defence related engineering jobs around the same time when he copied the files. 3. The files have been copied on unencrypted USBs which most likely are personal. 4. He is also seen accessing and uploading files to personal Google Drive. 5. He belongs to the Defence User Group.	**Technical control not implemented**	**High**

Risk. Rapid and frequent transfer of large amounts of company data, the fact that the user is reviewing his CV and is applying for jobs are all tell-tale signs of a potential insider threat in progress.

Risk. The user has personal Dropbox installed meaning he has circumvented company policy.

Print Event List for XXXXX using printer Canon-X53Series

User Name	User Group Name	PC Name	File Name	Event Date	Event Time	File Path
XXXXX	Client Group	LAP2u82	my cv 2022.docx	02-12-2022	13:40:55	c:\users\XXXX\Downloads\my cv 2022.doc

Data copied to 2 distinct unencrypted USBs. Early Morning and on Weekend.

Serial Number	Insertion Date/Time	Removeal Date/Time	Number Files
531455422	2022-12-18 22:20:16	2022-12-18 00:00:00	9685
531455422	2022-12-18 09:47:04	2022-12-18 10:20:16	6622
931222212	2022-12-25 08:31:19	2022-12-25 09:47:04	15633
931222212	2022-12-25 19:35:33	2022-12-25 20:31:19	8952

Suspicious User Activity- User 1

Applying for Job on Seek the next day.

Date/Time	Duration	Full URL
2022/12/03 17:00:00	0:05:36	au.indeed.com/[redacted]edabda9de58bfe0f2ff
2022/12/03 17:30:00	0:18:41	au.indeed.com/[redacted]
2022/12/03 17:00:00	0:01:40	au.indeed.com/job/[redacted]c
2022/12/03 17:00:00	0:01:30	au.indeed.com/job/[redacted]2
2022/12/03 17:00:00	0:01:09	au.indeed.com/job/[redacted]ff
2022/12/03 17:00:00	0:01:10	au.indeed.com/job/[redacted]f
2022/12/03 17:00:00	0:00:50	au.indeed.com/job/[redacted]f
2022/12/03 17:00:00	0:00:44	au.indeed.com/companies/[redacted]
2022/12/03 17:00:00	0:00:41	au.indeed.com/companies/[redacted]
2022/12/03 17:00:00	0:00:36	au.indeed.com/companies/[redacted]
2022/12/03 17:00:00	0:00:29	au.indeed.com/job/[redacted]0
2022/12/03 17:00:00	0:00:26	au.indeed.com/job/[redacted]f6
2022/12/03 17:00:00	0:00:25	au.indeed.com/job/[redacted]
2022/12/03 17:00:00	0:00:23	au.indeed.com/job/[redacted]
2022/12/03 17:30:00	0:00:23	au.indeed.com/job/[redacted]
2022/12/03 17:00:00	0:00:16	au.indeed.com/job/[redacted]
2022/12/03 17:00:00	0:00:13	au.indeed.com/job/[redacted]77
2022/12/03 17:00:00	0:00:11	au.indeed.com/job/[redacted]b5
2022/12/03 17:00:00	0:00:11	au.indeed.com/job/[redacted]
2022/12/03 17:30:00	0:00:11	au.indeed.com/job/[redacted]
2022/12/03 17:00:00	0:00:06	au.indeed.com/job/[redacted]f
2022/12/09 17:30:00	0:00:06	au.indeed.com/job/[redacted]2
2022/12/03 17:00:00	0:00:04	au.indeed.com/job/[redacted]
2022/12/03 17:30:00	0:00:04	au.indeed.com/job/[redacted]6
2022/12/03 17:00:00	0:00:03	au.indeed.com/job/[redacted]

Email Analysis

Covers both Corporate and Personal Email transactions.

Personal Email Accounts

Forwarding organisation emails to personal email accounts is a security threat, and one of the major ways that data leaks outside of organizational control. If those emails carry sensitive content, or have organisation files attached, there is potential risk of data leakage as unauthorized persons may access these emails.

Good Things Leaking Out

The first problem with allowing personal email from within the corporate network is that it represents a path through which trade secrets and other intellectual property can leave the organization with no record or audit trail concerning the correspondence. Many companies have adopted an HR policy that explicitly allows the employer to monitor employee email traffic. But if the organization does not monitor or block the use of personal email accounts, the email monitoring policy is effectively nullified.

Bad Things Sneaking In

A second problem is that personal email may be an avenue through which non-business-related content may enter the corporate network. Although most personal email providers take appropriate actions to screen malware from their systems, such controls may be less stringent than those required for corporate networks. Even if malware is blocked by the personal email provider, personal email accounts may be an avenue through which music files, jokes, chain letters, spam, and other distractions may enter the workplace.

Losing Control of Business Records

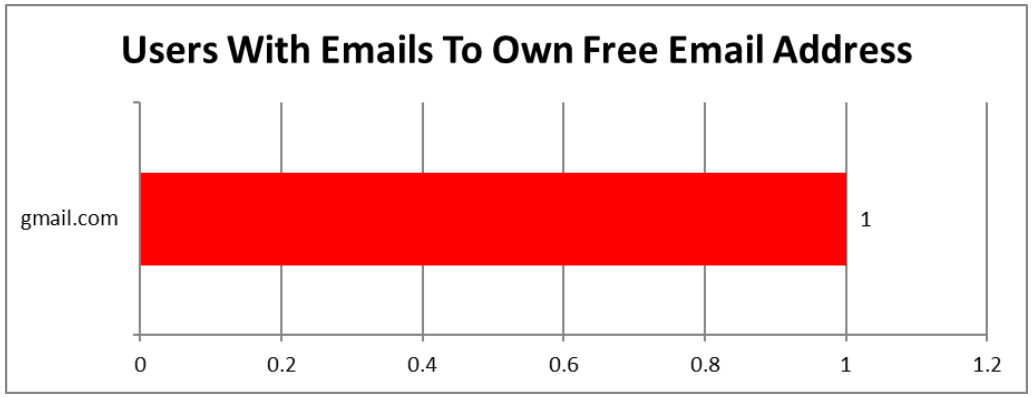
A third problem with the use of personal email from within the corporate network stems from the fact that employees will sometimes use such accounts to send both personal email and business email. Regardless of its origin, emails sent from behind the corporate network firewall can be considered the responsibility of the company. Thus, an email sent from a personal email account in this manner can be subject to a subpoena. However, personal email is seldom tracked and is even less likely to become part of the company's official records. Should a legal issue arise, the inability of the company to produce all emails sent or received on the matter at hand can have severe legal implications.

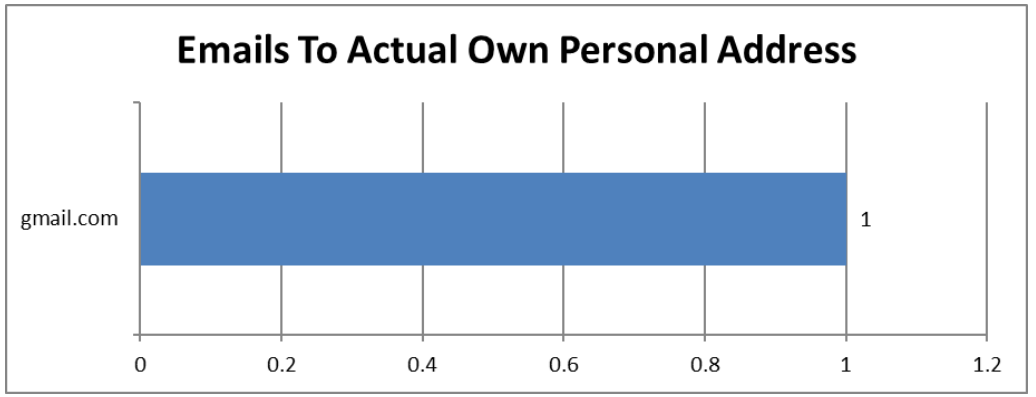
Forwarding emails to personal emails

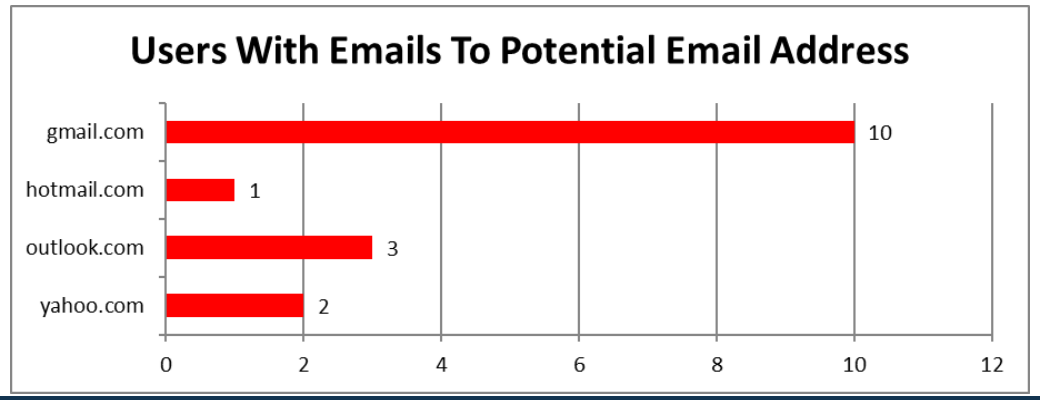
Corporate Email Analysis		
Corporate emails forwarded to own personal emails. Email detected being forwarded to user own personal email.	**Technical control not implemented**	**Medium**
Visibility of email forwards. Visibility of what files have been forwarded by users to personal and free emails to ensure they are accounted for.	**Technical control not implemented**	**High**

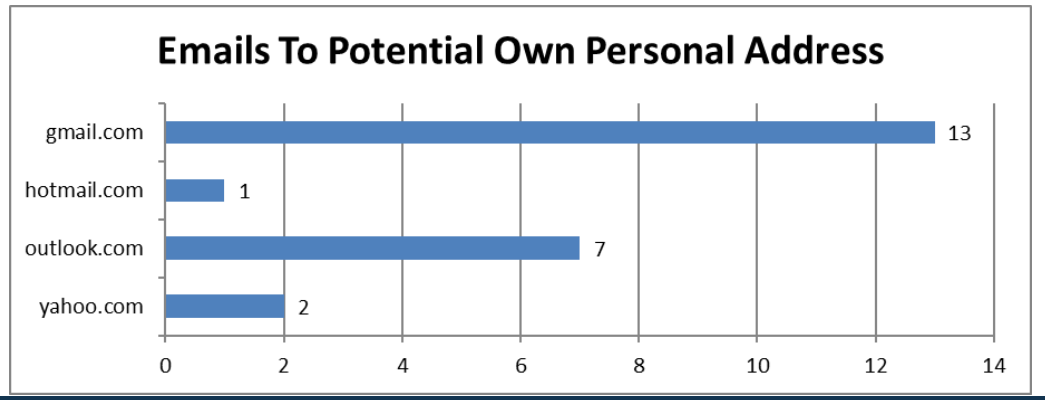
Forwarding emails to personal and other free emails is a common cause of leakage and non-compliance

Risk: Forwarding corporate information to personal emails leads to information creep. The action needs to be checked in the event sensitive information is forwarded to free emails.







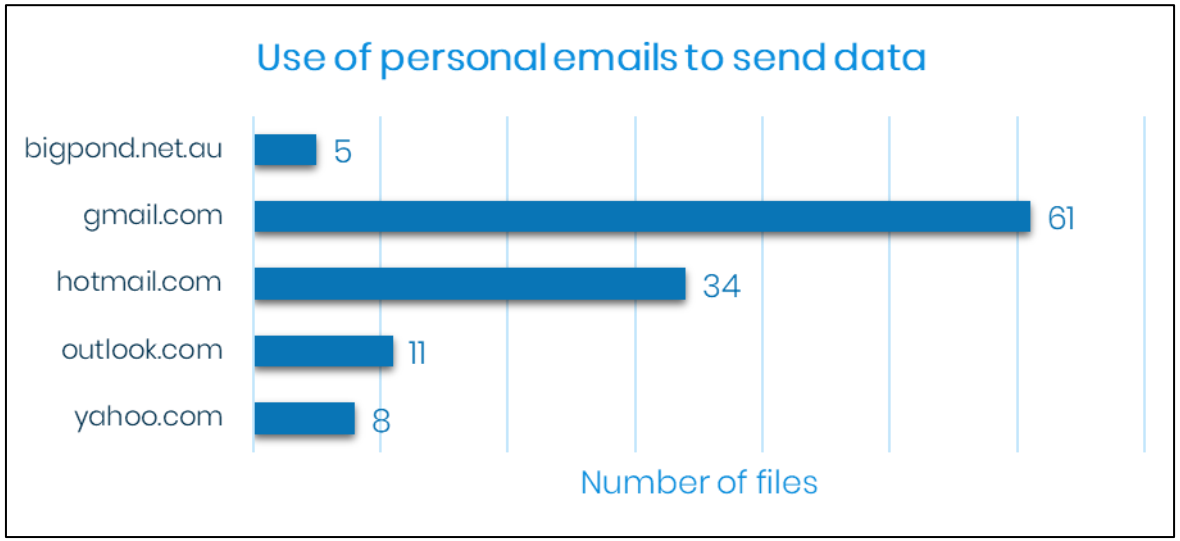


Use of personal emails to send data

Use of Personal Emails		
Use of Personal emails to send corporate data detected. Personal emails have been used to send corporate data.	**Technical control not implemented**	**High**
Visibility of Personal Email Use. Visibility is required to ensure company data is not being sent out via personal emails.	**Technical control not implemented**	**High**

Use of personal emails is a common occurrence in organisations but needs to be monitored as can lead to data leaks.

Risk: Use of personal emails to exfiltrate data out consistently reported as one of the key ways data is lost or stolen in organisations and needs to be monitored.



Use of Non Organisational Unauthorised Applications

Non-Compliance of 2 of the ES8 Controls.

1. Restrict administrative privileges
2. Application control

Application Control

Application control is a security approach designed to protect against malicious code (also known as malware) executing on systems.

When implemented robustly, it ensures only approved applications (e.g., executables, software libraries, scripts, installers, compiled HTML, HTML applications, control panel applets and drivers) can be executed. While application control is primarily designed to prevent the execution and spread of malicious code, it can also prevent the installation or use of unapproved applications.

- Extract from "Implementing Application Control, ACSC Essential Eight"

Many business professionals experienced a heightened level of empowerment with application choices during the pandemic. Organizations often told an emerging remote workforce to "do whatever it takes to maintain productivity", a radical departure from the traditional principle of using corporate approved applications only.
During the first months of 2020 GuardWare clients detected a 50% jump in data movement, with the vast majority employing non-company channels, as overloaded company VPNs faltered under the unexpected demand.
Whilst organizations survived the unplanned imposition of 'Work-From-Home', the strategies employed to achieve this saw breathtaking amounts of sensitive data find its way onto cloud services and personal email clients…technical data breaches in every instance!
Cloud services like Dropbox, IDrive and Google Drive are comprised of vast collections of data warehouses, spread across the world, that make access to your data possible from any device with an account.
However, there are some serious issues with these services.

- Data stored on these services is now on hardware the organisation responsible for the data has no ownership or control over. Technically a Data Breach!
- Data can be stored anywhere in the world where the cloud service has a data warehouse, the user will not know, a serious ITAR breach.
- Archival backups are stored for much longer than the Cloud providers "Fine-Print" admits, for obvious legal reasons. So, data that has been considered "Deleted" may live on in data archives that the user cannot be assured are deleted.
- Cloud email lives forever, so long as you do not exceed your account data limit. Personal emails are also outside of organisational control…another example of a "Data Breach"!

Installation and Use of Non-organisational applications

Data transfer using non-corporate applications		
Technical Control Circumvented. The users seem to have found a way to install non-organisational applications. **Non-Compliance of 2 of the ES8 Controls.** 1. Restrict administrative privileges 2. Application control	**Failed Technical Control**	**High**
Visibility of Application Use. Visibility of what applications are being used by users.	**Technical control not implemented**	**High**

Software Name	Vendor	Number of PCs with Software Present	Number of PCs with Software Usage	Total Usage Duration
MESSENGER.EXE	Facebook Inc.	5	3	1:15:00
TELEGRAM.EXE	Telegram	5	2	0:41:40
WHATSAPP.EXE	WhatsApp	6	2	0:17:30
FILEZILLA.EXE	FileZilla Project	1	1	0:08:41
DROPBOX.EXE	Dropbox, Inc.	8		
OPERA.EXE	Opera Software	2		

The use of personal applications without proper authorization and vetting may be for legitimate reasons, but there are significant risks involved.

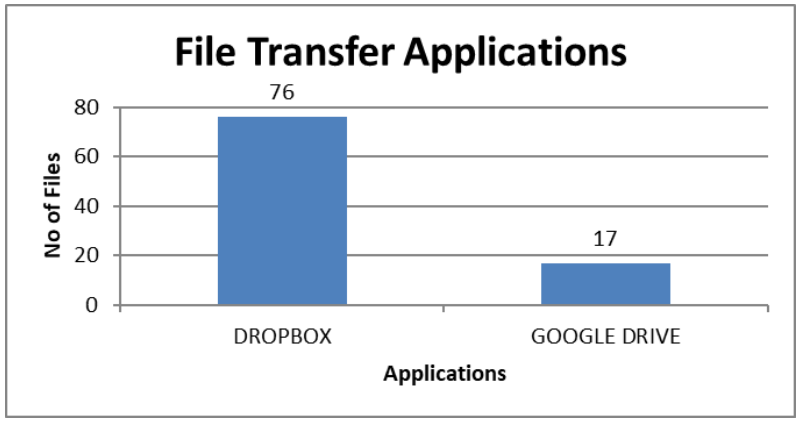
Risk. Standard users should not have admin rights to install applications. It can result in malware infection and highlights that the current controls are failing to implement 2 of the ES8 Controls.

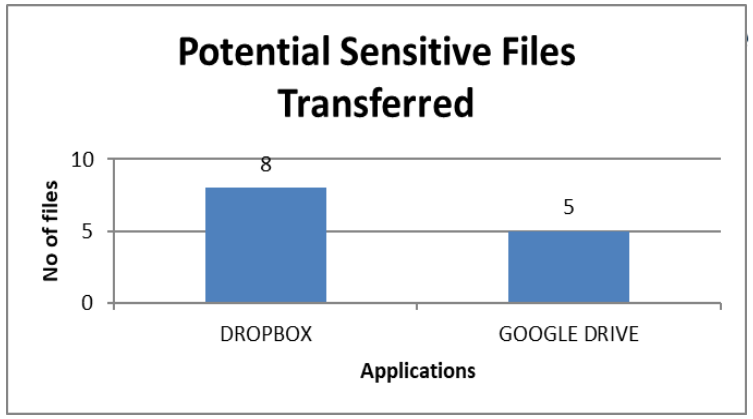
1. Restrict administrative privileges
2. Application control.

Data transfer using Non Corporate Data sharing APPs and Websites

Data transfer using Non-Org applications

Data transfer using non-corporate applications		
Risky Transfer Application Use. 6 users detected using Dropbox or Google Drive to transfer files. Transfers include potential sensitive data.	**Failed Technical Control**	**High**
Visibility of transfers. Visibility of sensitive data transferred using external media	**Technical control not implemented**	**High**





User Name	User Group	Total Events
xxxxxx	Client Group	34443
xxxxxx	Client Group	1722
xxxxxx	Client Group	1428
xxxxxx	Client Group	17

The use of personal cloud services and applications may be for legitimate reasons, but there are significant risks involved.

Risk. Unauthorized access by former staff members. Information stored in personal cloud account remains with its user after he leaves a company and therefore can result in a breach as per NDB Scheme.

Risk. Applications like Dropbox, OneDrive, and Google Drive sync files to any device where a user is logged into these applications. This may include their personal devices or, even worse, those of a different company, which could result in the loss of sensitive information.

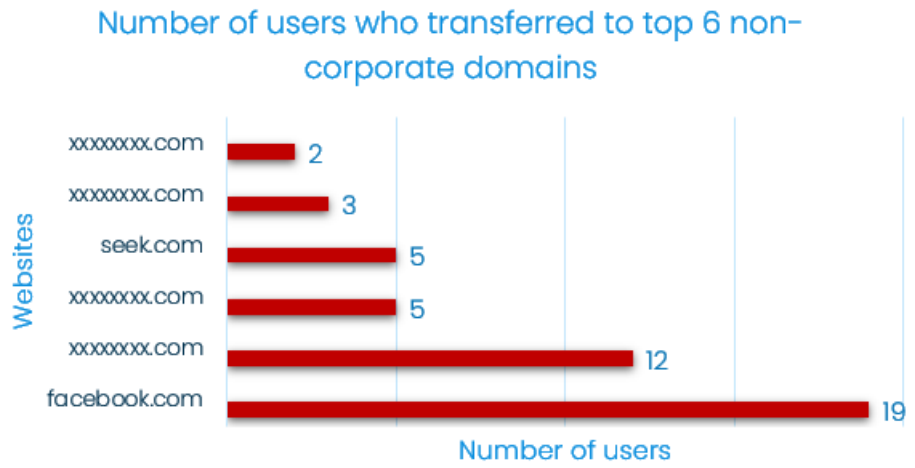
29-11-2022	14:03:28	DROPBOX	1231212.docx
29-11-2022	14:03:28	DROPBOX	1-product comparison-latest- jun 2018 copy.xlsx
29-11-2022	14:03:28	DROPBOX	1-product comparison-latest- jun 2018.xlsx
29-11-2022	14:03:29	DROPBOX	1231212_00.docx
29-11-2022	14:03:29	DROPBOX	1231212_00_11.docx
29-11-2022	14:03:29	DROPBOX	amex2222_3.xls
29-11-2022	14:03:29	DROPBOX	az-100.docx
29-11-2022	14:03:30	DROPBOX	capture.png
29-11-2022	14:03:30	DROPBOX	claim - copy.xls
29-11-2022	14:03:43	DROPBOX	client4.4.0.10 - lc-temora.msi
29-11-2022	14:03:56	DROPBOX	contract form.doc
29-11-2022	14:03:56	DROPBOX	creditcard.docx
29-11-2022	14:03:57	DROPBOX	customer info.xlsx
29-11-2022	14:03:57	DROPBOX	customer_info.docx
29-11-2022	14:03:58	DROPBOX	customer_offer letter.docx

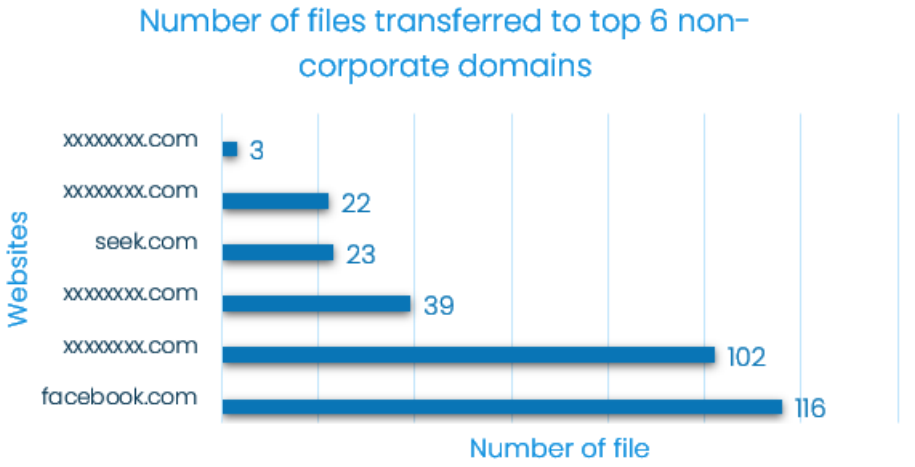
Data transfer using Non-organisational websites

Data transfer using non-corporate applications		
Risky website Use.19 users detected using Facebook and potentially transferring data.	**Technical control not implemented**	**High**
Visibility of transfers. Visibility of sensitive data transferred using APPs and encrypted websites.	**Technical control not implemented**	**High**

Transferring of files to non-corporate websites may be for legitimate reasons, but there are significant risks involved.

Risk. Can result in a breach if sensitive or PII data is uploaded to non-corporate websites either accidentally or due to malicious intent.

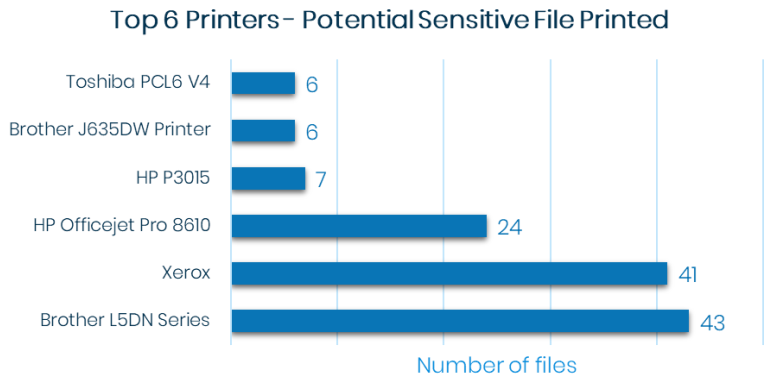




Printing Analysis

Printing of Potential Sensitive Information

Printing of Sensitive Data		
Printing of potential sensitive data. Printing of sensitive data was observed.	**Technical control not implemented**	**Medium**
Printing use personal Printers. As users are allowed to work from home there is risk of files being printed using home printers.	**Technical control not implemented**	**Medium**
Visibility of Printing. Visibility of what files have been printed either via organisational or personal printers to ensure they are accounted for.	**Technical control not implemented**	**Medium**



Printer Name	Total Events
\\rbcmon02\[redacted]-Office	25
\\RBCPRN01\[redacted]-Office	22
\\rbcprn01\[redacted]Office	19
\\RBCPRN01\[redacted]-Office	12
D-Accounts	6
Microsoft Print to PDF	5
\\rbcmon02\[redacted]-Office2	5
\\rbcprn01\[redacted]-Office	5
Microsoft Print to PDF	4
\\rbcprn01\[redacted]-Manager Office	3
Canon TS3300 series	3
OneNote for Windows 10	2
Adobe PDF	2
\\RBCPRN01\[redacted]-Office	2
I Block Lv2 Toshiba	2
[redacted]-Admin	2
HP8A771D (HP Officejet Pro 6830)	2
\\rbcprn01\[redacted]-Office	1
Adobe PDF	1
HPBBF063 (HP OfficeJet Pro 8710)	1
\\RBCPRN01\[redacted]-Office	1
[redacted]	1
HP000756 (HP Officejet 6600)	1
Brother HL-1110 series	1
Adobe PDF	1
Brother MFC-L3750CDW series Printer	1
\\RBCPRN01\[redacted]-Office	1
\\rbcprn01\[redacted]-Office	1
Canon MG6200 series Printer XPS	1

The use of these printers may be for legitimate reasons but can result in a breach.

Risk. According to ACSC Loss of printed information is a common occurrence leading to a data breach. As such printing of material needs to be monitored and controlled. Users should be made responsible for the security of printed materials. All printing events need to be monitored.

Access of files

Access of files

Access of information		
Authorised Access of sensitive Information. Ensuring authorised users can access files	**Implemented**	**No Risk**
Access Visibility. Visibility of who is accessing what files	**Implemented**	**No Risk**

The company has visibility and means to validate if authorised users are accessing sensitive data.

DLP File Access Incidents by Rule Name

Rule Name	mber of	Number of Files
Defence Classified Information	79	1086
Document Access	146	19567

File Name	User Name	Date	Time	File Path
mp-23 project brief.doc	[redacted]	29/11/2022	12:42:56	c:\users\User\document\Client Profile\mp-23 project brief.doc
ac_id_74 - signed.docx		29/11/2022	15:21:49	c:\users\User\document\Client Profile\ac_id_74 - signed.docx
security snippets nov 2022.pdf		29/11/2022	9:36:52	c:\users\User\document\Client Profile\\security snippets nov 2022.pdf
agreementreconciliation.pdf		29/11/2022	11:55:43	c:\users\User\document\Client Profile\agreementreconciliation.pdf
202208_client.xlsx		29/11/2022	10:13:53	c:\users\User\document\Client Profile\202208_client.xlsx
performance report.pdf		29/11/2022	11:21:31	c:\users\User\downloads\performance report.pdf
performance report (1).pdf		29/11/2022	11:21:39	c:\users\User\downloads\performance report (1).pdf
protect 1st work package costing.xlsx		6/12/2022	13:29:50	c:\users\admin\desktop\demos\project f20\protect 1st work package costing.xlsx

RECOMMENDATIONS TO REDUCE RISKS

1. Users need to be educated and informed regarding their risky actions. There is a need to conduct user training on the identified risks. Moving forward, department heads can be passed reports about risky actions of their staff to ensure compliance on an ongoing basis. This also ensures better security as movement of information is reviewed by users who understand its sensitivity and use.

2. Use of network shared drives should be encouraged as a means for sharing files internally, and use of USB storage should be minimised. In case movement of information is required using USBs, DLP and encryption software should be used to provide visibility and protection of files.

3. Sensitive information should be encrypted when being sent to trusted 3rd parties or copied to removable USB storage or cloud applications. This ensures that, even in the case of loss or theft, sensitive information is not compromised, and fines or reputational loss can be avoided.

4. Disk or file-based encryption should be considered to protect data stored locally on devices. Microsoft's Bitlocker is a good option.

5. Access of sensitive files in cloud drives should be restricted to company devices and users only. There are multiple ways to implement this. Some examples include implementing CASB or file-based encryption.

6. Use of personal cloud drives and uploads to websites should be closely monitored. Access to them should be given only on a strong need basis.

7. Moving sensitive information via emails is unavoidable. Where required, it should always be zipped and password protected. A better approach is to maintain the files encrypted so that only authorised users can have access to the data in case of a breach.

8. Forwarding and sending sensitive corporate information to personal and 3rd party free accounts should be monitored. Business dealing using free email user accounts can make investigation tough in case of any litigation.

9. Use of non-corporate networks and printers should be monitored. Preventing users from using non-corporate network can greatly impact productivity, so a better approach would be to use specialised security software to monitor devices when connecting from home or using personal printers.

10. Users should be encouraged and reminded to seek advice from IT departments before installing and using non-corporate applications. Specialised asset management software can provide the visibility of use if they do not comply and can block the applications from running.

GuardWare offers several products designed to keep your data safe and can help implement the recommendations in this report.

Contact Information

Level 13, 465 Victoria Avenue,
Chatswood, Sydney 2067, Australia.

Email: sales@guardware.com

Phone: +61 2 9994 8061