

Sample Pty Ltd

Cyber Security Assessment focused on secure handling of PII and Sensitive Company Data and ensuring Compliance.

Audience: Board/C Suite/Senior Management



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 Organisations.
- 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 customer's current security processes and controls (ISMS) based on the following criteria:

- 1. Ability to securely handle sensitive data namely PII information in line with the requirements of Australian Privacy Principals and NDB Scheme.**
- 2. Ability to securely handle commercially sensitive data in line with ISO/IEC 27001, ACSC Essential 8 and ACSC Information Security Manual (ISM) recommendations.**
- 3. Assess current state of IT Security Governance in line with cyber security controls and the ability to handle a data breach.**

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

Executive Summary

Company faces considerable risk of a Data Breach.

Assessment showcased risky handling of PII data.

The assessment has shown that the company lacks data monitoring controls and faces the risk of losing sensitive IP either due to human error or malicious intent.

During the assessment 2 suspicious activities regarding company IP were also detected which need urgent action.

Company lacks full implementation of ACSC ES8 controls. Two of the controls being detected as failing.

The company doesn't have any IT Security Governance processes in place. This further increases the risk of data loss and breach.

Company is advised to take immediate actions to rectify the current state of cyber security. A list of recommendations based on their priority is provided at the end of this document.

Monitoring done from 26th
Nov to 13th Dec 2022

158 users monitored on 146
devices

ISMS Evaluation Criteria	Implementation level	Risk Level (High, Medium, Low)
Ability to securely handle sensitive data namely PII information in line with the requirements of Australian Privacy Principals and NDB Scheme.	20%	High
Ability to securely handle commercially sensitive data in line with ISO/IEC 27001, ACSC Essential 8 and ACSC Information Security Manual (ISM) recommendations.	20%	High
Assess current state of IT Security Governance in line with cyber security controls and the ability to handle a privacy breach.	20%	High

16 High risk actions detected
which require urgent attention

4 Medium risk actions
detected

2 suspicious activities
detected – Need urgent
action

Non-Compliance to ES8 and
when handling PII data

Risk Summary

IT Governance Summary

No	IT Governance Aspect	Implemented/Partial/ Not Implemented	Risk Level (No Risk, Low, Medium, High)
1	Information security policies	Not Implemented	High
2	Organisation of information security	Partial	Medium
3	Ensuring responsible use of information assets	Partial	High
4	Control Access of data (Access control)	Partial	medium
5	Ensuring data is secure when stored. (Data at rest)	Partial	Low
6	Monitoring Movement of Data (Data Egress Monitoring)	Not Implemented	High
7	Supply chain security	Not Implemented	High
7	Information security incident management	Partial	High

Data Handling Risk Summary

Monitoring Parameters:

- Only customer owned devices were covered.
- The following types of data were monitored:
 - Sensitive PII data covering TFN, Credit Card, Mobile numbers, Account numbers, Medicare Numbers, Name and Address.
 - Generic Company IP Documents
 - General files of any type including source code, images, zip etc
- Monitoring USE CASES included those recommended under ACSC ISM around Insider Threats and Secure handling of PII Data

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

Use Cases	Technical Control Implemented/Partial/Not Implemented/Failed Control	Risk Level (No Risk, Low, Medium, High)
PII and Sensitive Company IP transferred 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 User detected using his personal email to send highly sensitive Intellectual Property marked data to unauthorized 3rd parties.	Technical control not implemented	High
Suspicious User Activity – User2 – Data copied by user about to leave the organisation. - User copied 1000s of design files also printed his CV during the same time. - There is evidence he has visited job sites (Indeed) and applied for related engineering jobs around the same time when he copied the files. - The files have been copied on unencrypted USBs which most likely are personal. - He is also seen accessing and uploading files to personal Google Drive. - He belongs to the Engineering 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 – PII Data forwarded by staff to personal emails.		
Customer data forwarded to personal emails by staff. 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
PII data transfers using Cloud Applications and non-organizational 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 PII 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 ACSC ISM

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

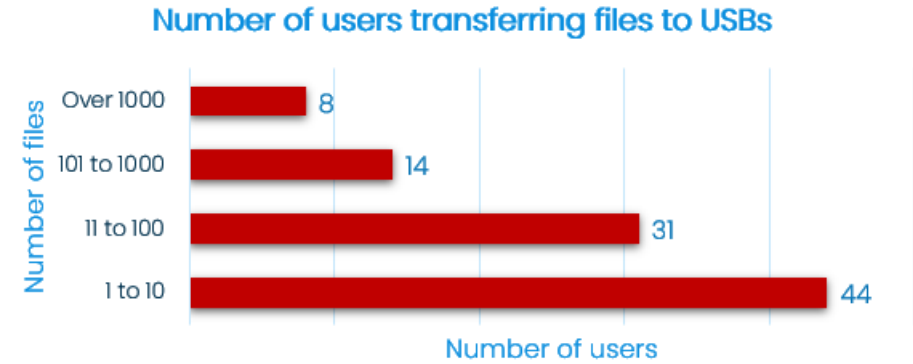
Recommended Use Cases Under ISM	Detected/Not Detected/Not Tested
excessive copying or modification of files	Detected
unauthorised or excessive use of removable media	Detected
connecting devices capable of data storage to systems	Detected
unusual system usage outside of normal business hours	Detected
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

Storage Media Analysis

Covers all types of media including phone sync.

PII and Sensitive Company Data transfer using external storage media

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. Compromise of sensitive corporate information. There should be a valid NEED for transferring sensitive corporate 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
xxxxxx	Customer Group	26256
xxxxxx	Customer Group	5221
xxxxxx	Customer Group	4212
xxxxxx	Customer Group	3362
xxxxxx	Customer Group	2326
xxxxxx	Customer Group	2125
xxxxxx	Customer Group	1782
xxxxxx	Customer Group	1506
xxxxxx	Customer Group	9
xxxxxx	Customer Group	5
xxxxxx	Customer Group	4
xxxxxx	Customer Group	3
xxxxxx	Customer Group	2
xxxxxx	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 PII and IP 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. Compromise of sensitive corporate information. There should be a valid NEED for transferring sensitive corporate 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

08-12-2022	7:38:45	07 [REDACTED] c9.svn-base
08-12-2022	7:38:51	02 [REDACTED] a.svn-base
08-12-2022	7:38:54	067 [REDACTED] 89.svn-base
08-12-2022	7:38:54	06 [REDACTED] c.svn-base
08-12-2022	7:38:54	[REDACTED] .drl
08-12-2022	7:38:54	[REDACTED] .cmp
08-12-2022	7:38:54	[REDACTED] .sol
08-12-2022	7:38:54	[REDACTED] .drl
08-12-2022	7:38:54	[REDACTED] .cmp
08-12-2022	7:38:54	[REDACTED] .stc
08-12-2022	7:38:54	[REDACTED] .oles.txt
08-12-2022	7:38:54	[REDACTED] .s.txt
08-12-2022	7:39:11	[REDACTED] .oles.txt
08-12-2022	7:39:11	[REDACTED] .es.txt

User 1

29-11-2022	8:21:51	[REDACTED] .cad.csv
29-11-2022	12:30:21	[REDACTED] nse2.pdf
29-11-2022	12:30:21	[REDACTED] .pdf
29-11-2022	12:30:21	[REDACTED] .bom.csv
29-11-2022	12:30:21	[REDACTED] .cad.csv
29-11-2022	12:30:21	[REDACTED] .bom.csv
29-11-2022	12:30:21	[REDACTED] .cad.csv
05-12-2022	10:23:43	[REDACTED] .csv
05-12-2022	10:23:43	[REDACTED] .csv

User 2

09-12-2022	7:48:12	[REDACTED] power.csv
09-12-2022	7:48:12	[REDACTED] spectrum.csv
09-12-2022	7:48:12	[REDACTED] .png
09-12-2022	7:48:12	[REDACTED] .png
09-12-2022	7:48:12	[REDACTED] _1.png
09-12-2022	7:48:13	[REDACTED] .pdf
09-12-2022	7:48:13	[REDACTED] .csv
09-12-2022	7:48:13	[REDACTED] .pdf

User 3

Suspicious User Activity

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 corporate data to unauthorized 3 rd parties.	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 is consistently reported as one of the keyways data is lost or stolen in organisations and needs to be monitored.

Email violation detail		Rules Violated	Email Body/File Attachment
Review Status :	Not Reviewed		
Violation Date & Time :	[REDACTED] 10:26:10	Document Movements	New Design Specs - Copy.docx
Subject :	this is the file	General File Movement	
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			
Detected content in email body / file attachment			
Word	Context		
CONFIDENTIAL	[REDACTED] [REDACTED] private management confidential [REDACTED] an fam		
MANAGEMENT	[REDACTED] ken [REDACTED] systems private management confidential [REDACTED]		

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 industry 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 Engineering 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		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	Removal 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 Jobs on Indeed.com 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]
2022/12/03 17:00:00	0:01:30	au.indeed.com/job/[redacted]
2022/12/03 17:00:00	0:01:09	au.indeed.com/job/[redacted]f
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]6
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]
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.

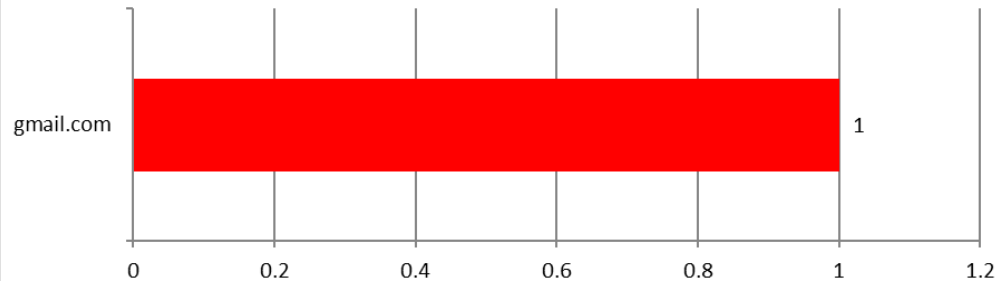
Customer data forwarded to personal emails

Corporate Email Analysis		
Customer data forwarded to personal emails by staff. 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

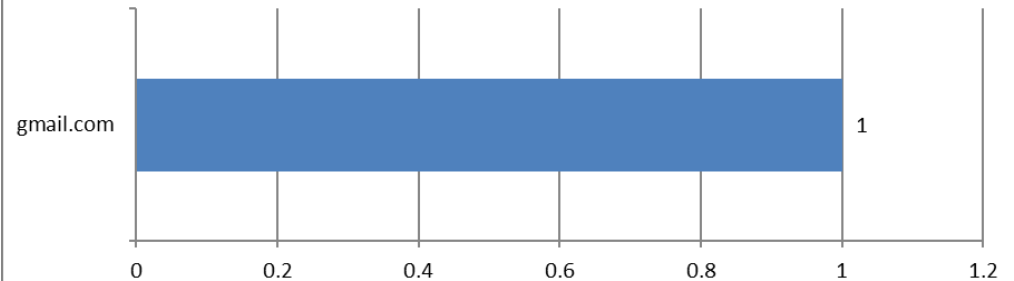
Forwarding emails to personal and other free emails is a common cause of leakage and non-compliance

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.

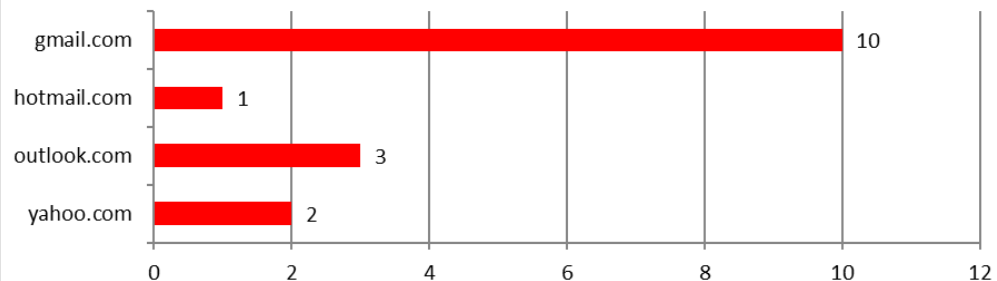
Users With Emails To Own Free Email Address



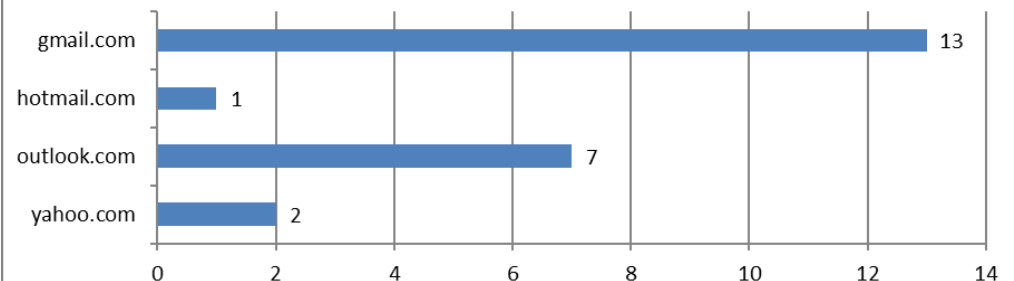
Emails To Actual Own Personal Address



Users With Emails To Potential Email Address



Emails To Potential Own Personal Address

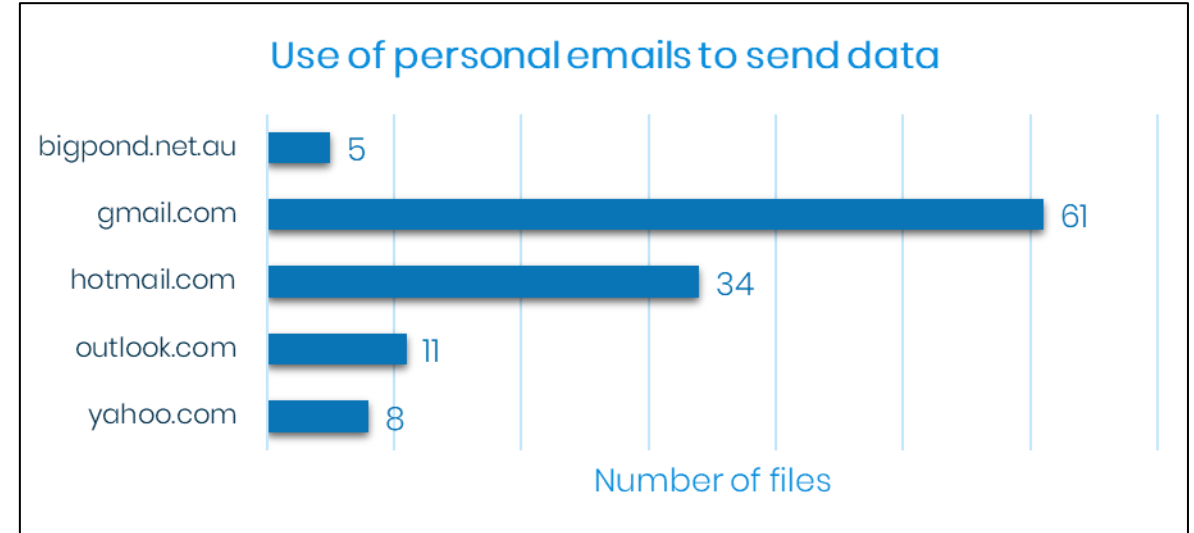


Use of personal emails to send data

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 is 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

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

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.

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		

Data transfer using Non-Corporate Data sharing Apps and Websites

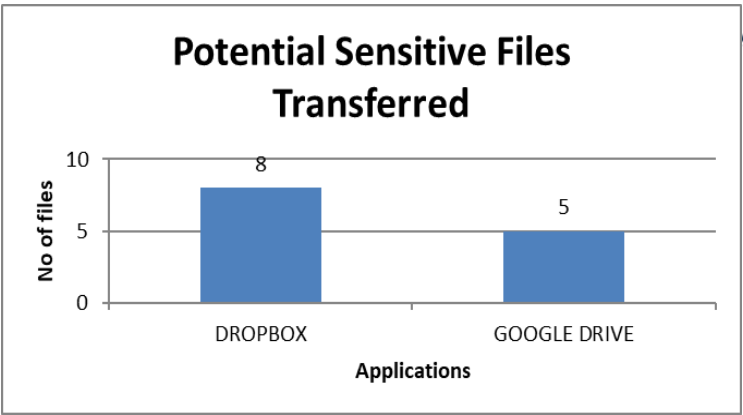
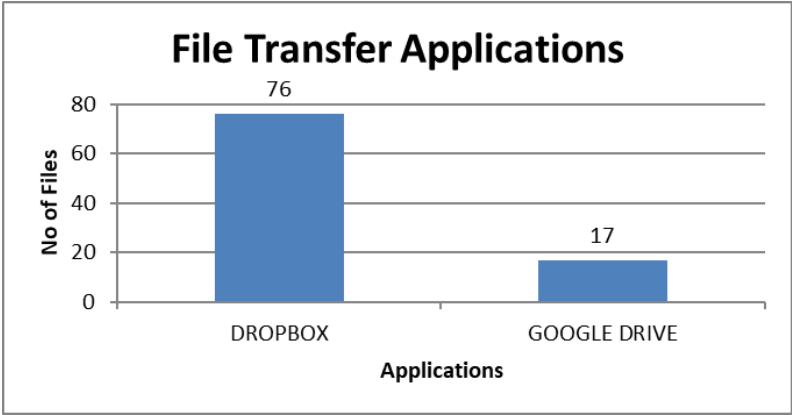
PII data transfers using Cloud Applications

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

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.



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

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

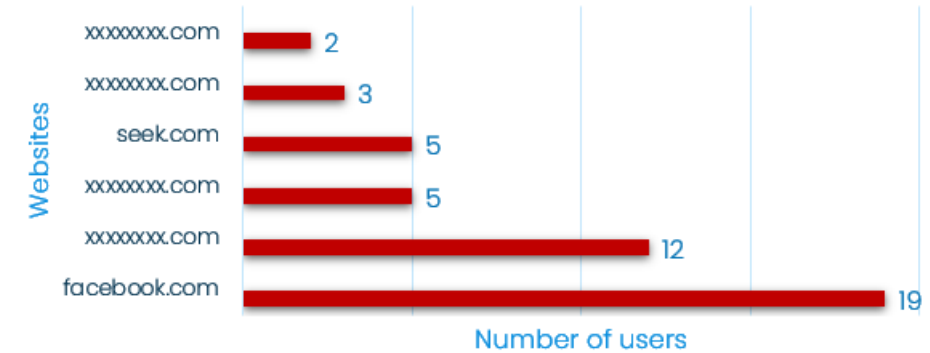
Data transfer using Non-organisational websites

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

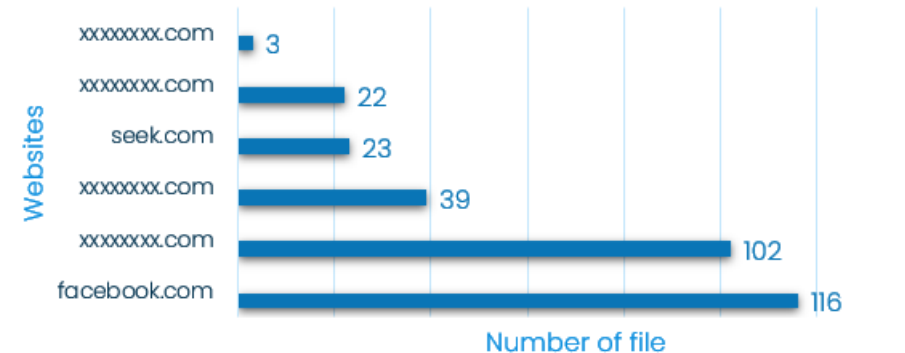
Transferring of files to non-corporate websites may be for legitimate reasons, but there are significant risks involved.

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

Number of users who transferred to top 6 non-corporate domains



Number of files transferred to top 6 non-corporate domains



Printing Analysis

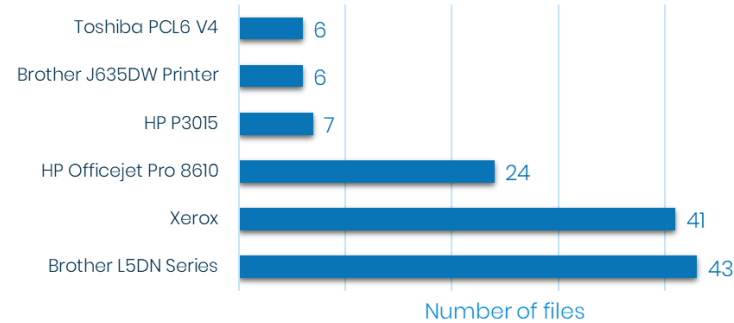
Printing of PII Information

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

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.

Top 6 Printers – Potential Sensitive File Printed



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

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	Number of	Number of Files
	79	1086
Document Access	146	19567

File Name	User Name	Date	Time	File Path
mp-23 project brief.doc		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

Recommendation to Reduce Risk

High Priority

The company's users are exhibiting several risky behaviours when dealing with Company data. These are putting company IP at serious risk and can easily result in a Breach. There is a need to monitor and control these activities.

Implement a User activity Monitoring, Data Egress/leak Monitoring solution which can monitor and alert "sensitive data" in the following use cases:

- Access of sensitive files
- Transfer using corporate channels like emails and cloud.
- Transfer using any personal online sources like free emails, cloud, and web uploads.
- Transfers using encrypted personal chats like WhatsApp.
- Data shared out directly from cloud shares.
- Printed using corporate and personal printers.
- Transfer using offline sources like USBs, phone sync etc.
- Locate laptops containing Sensitive PII data
- Monitor and control syncing of data using wireless methods like Bluetooth and Mobile Sync apps.
- Ability to monitor when user's circumvent company policy.
- Monitor use of unauthorized company applications.
- Monitor access of risky websites.
- Ability to monitor 24/7 even not connected to corporate network or offline.

Recommendation to Reduce Risk

High Priority

- Implement a staff awareness program around the identified risks. The OAIC's **Guide to Securing Personal Information** sets out expectations that Entities should ensure they foster a privacy and security aware culture, such as through staff training and awareness exercises.

High Priority

- The company is recommended to complete their IT Security Policy. It is recommended that the IT Security policy covers the following areas:

- Privacy Policy
- Acceptable Use Policy
- Authenticity Policy
 - Password Policy
 - MFA Policy
- Access control and Authorisation Policy
- Data Protection Policy
 - Data classification
 - Asset register
 - Protection of assets
- Communication and Data Transfer Policy
 - Email Policy
 - Chat
 - Media transfer
 - Other communication mechanisms.
- Mobile Device Protection and Management Policy
 - Mobile device management
 - Mobile device encryption
- Configuration and Vulnerability Management
 - Patching (which will include OS, and applications)
 - Application Control
 - User application hardening
 - MACRO management
 - AV configuration
- IT equipment Purchase, Deployment and Disposal Policy
- Clean Desk Policy
- Business Continuity Policy
 - Business Continuity Plan.
 - Backup and recovery strategy
- Supplier Management Policy
- User education and awareness policy
- Data Breach Response Plan

Recommendation to Reduce Risk

High Priority

- Company should aim to meet a minimum maturity of level 1 for ACSC essential 8 controls. The following essential 8 controls are considered of higher importance:
 - Application control
 - Patch applications
 - Patch Operating System
 - Restrict administrative privileges

Medium Priority

- The following essential 8 controls are considered of medium importance:
 - Backup
 - Configure Microsoft Office macro settings
 - User application hardening

GuardWare offers 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