SAMPLE REPORT

CYBERPATHWAYS

Leading Cyber Security Education and Training

SAMPLE CLIENT PTY LTD

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

JANUARY 2024

GuardWare

Document intent

- This sample report is indicative of the final report delivered at the end of CyberPathways CyberRisk Audit.
- The assessment covers a 3-4 week assessment period of data flows across your business systems and network.
- 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.
- This sample includes redacted information from a variety of assessments completed throughout 2023. Reports typically span 35-40 pages; this sample includes examples of each report section.

Assessment Scope

The scope of CyberRisk Audit 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.

Executive Summary

SAMPLE CLIENT PTY LTD faces considerable risk of a Data Breach.

Assessment showcased risky handling of PII data.

The assessment has shown that Sample Client 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 Sample Client IP were also detected which need urgent action.

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

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

SAMPLE CLIENT 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

CYBERPATHWAYS GuardWare

SAMPLE REPORT

CYBERPATHWAYS

Leading Cyber Security Education and Training

RISK Summary

GuardWare

IT GOVERNANCE SUMMARY

No	IT Governance Aspect	Implementation Status	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 College 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 2023	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

SAMPLE REPORT

CYBERPATHWAYS

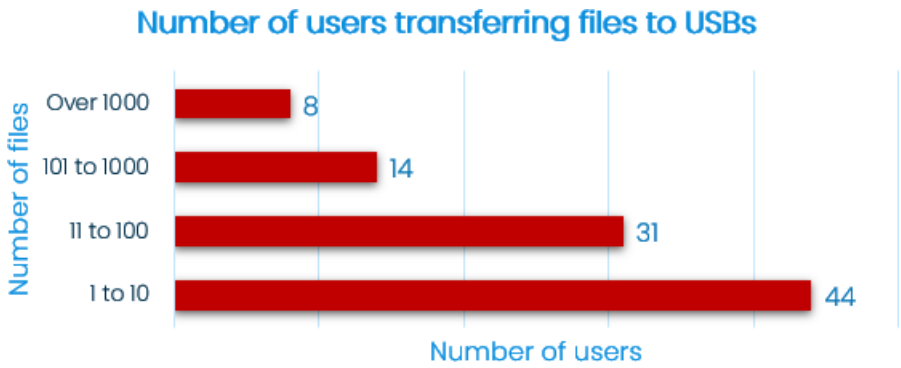
Leading Cyber Security Education and Training

STORAGE MEDIA ANALYSIS

GuardWare

DATA TRANSFER – PII & STORAGE DEVICES

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

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

SAMPLE REPORT

CYBERPATHWAYS

Leading Cyber Security Education and Training

SUSPICIOUS USER ANALYSIS

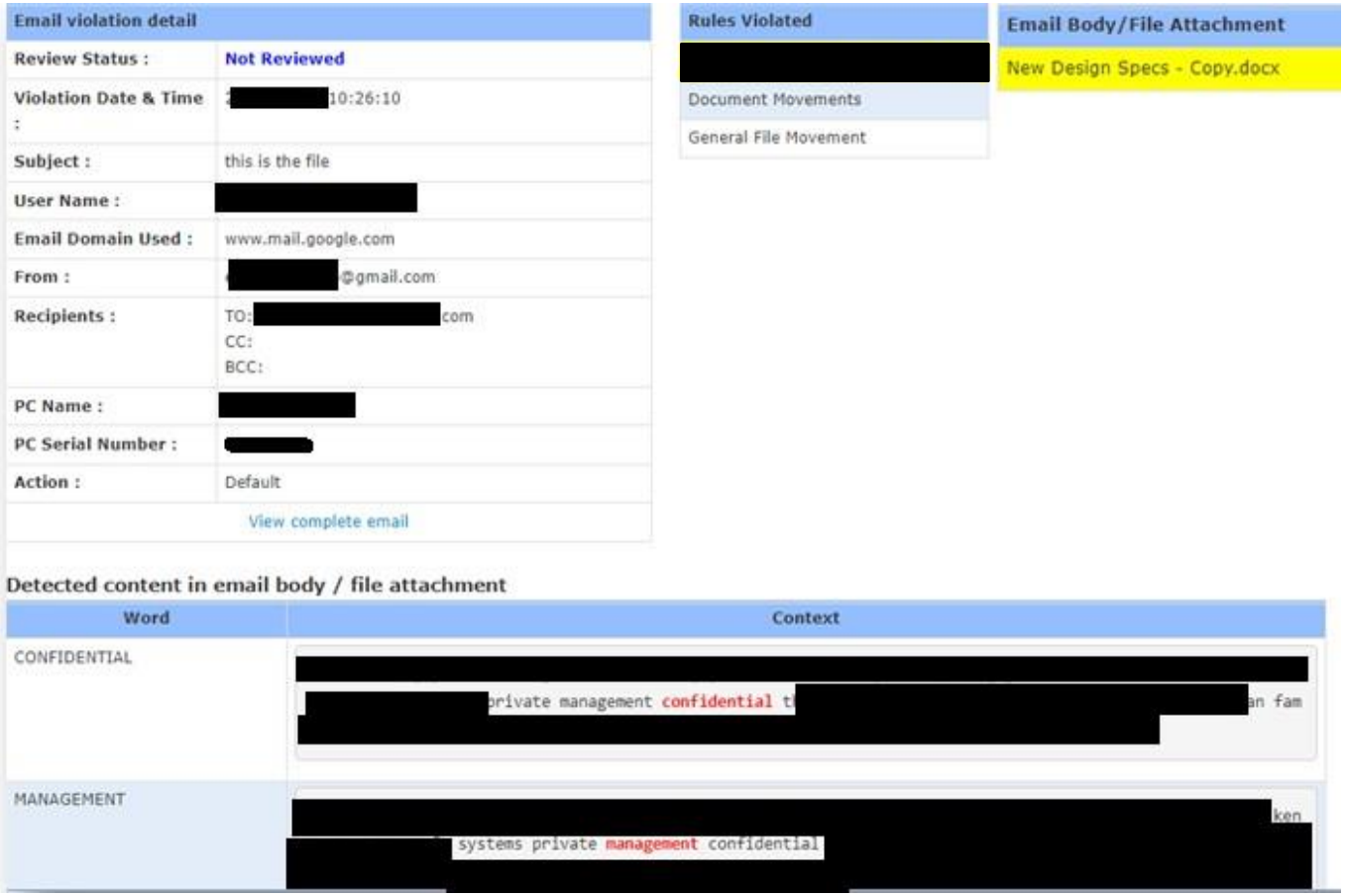
GuardWare

USER 1 – Personal email usage

Suspicious User Activity		
Potential Insider Risk. 1. User detected using his personal email to send highly sensitive sample client data to unauthorised 3rd 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	
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	Email Body/File Attachment
[redacted]	New Design Specs - Copy.docx
Document Movements	
General File Movement	

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

USER 2 –Data transfer

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 SAMPLE CLIENT 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 SAMPLE CLIENT 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	[redacted]	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

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

SAMPLE REPORT

CYBERPATHWAYS

Leading Cyber Security Education and Training

EMAIL ANALYSIS

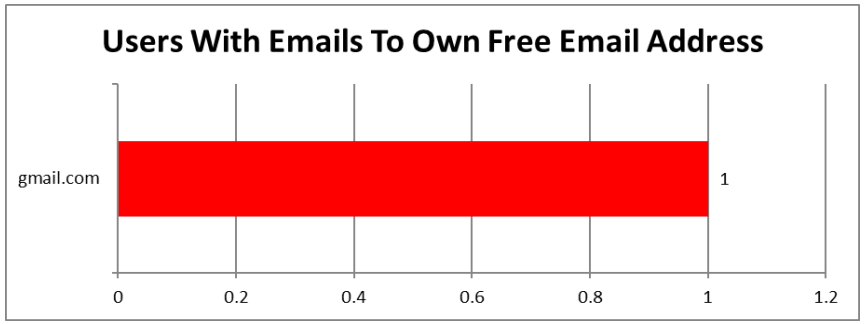
GuardWare

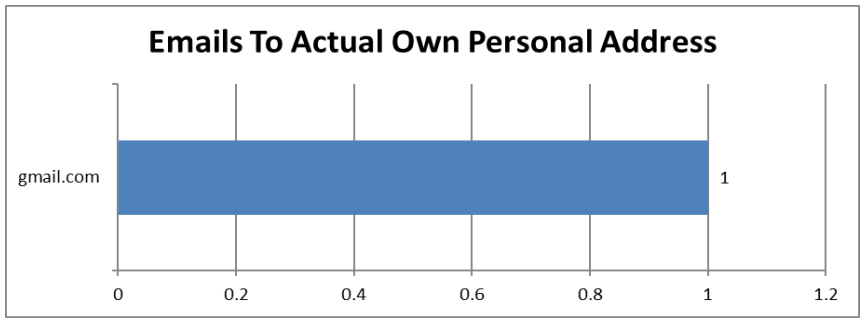
Customer data forwarded to personal email

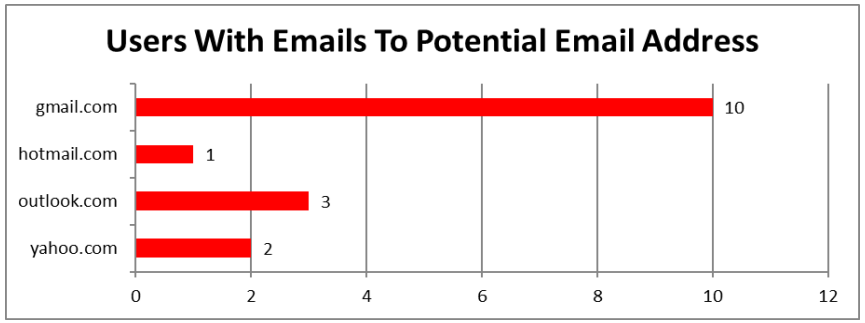
Corporate Email Analysis		
Customer data forwarded to personal emails by staff. Email detected being forwarded to user own personal email.	**Technical control not implemented**	**Medium**
Visibility of email forwards. Visibility of what files have been forwarded by users to personal and free emails to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

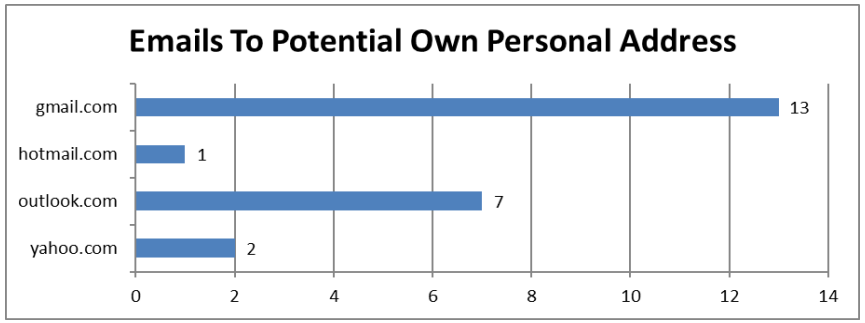
Forwarding emails to personal and other free emails is a common cause of leakage and non-compliance

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.









SAMPLE REPORT

CYBERPATHWAYS

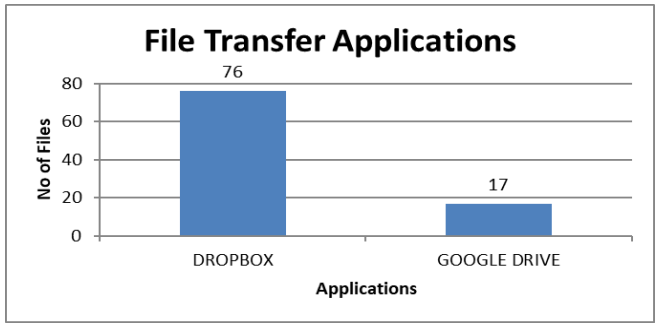
Leading Cyber Security Education and Training

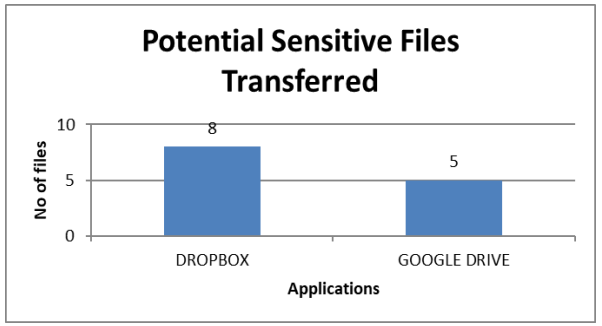
DATA TRANSFER ANALYSIS

GuardWare

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 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 College 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 College, which could result in the loss of sensitive information.

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

SAMPLE REPORT

CYBERPATHWAYS

Leading Cyber Security Education and Training

PRINTING ANALYSIS

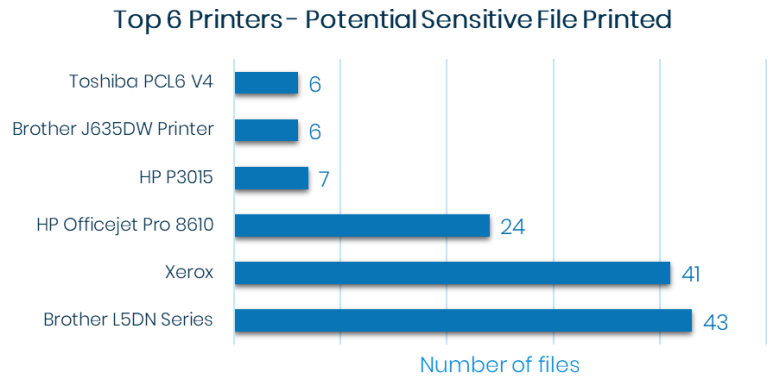
GuardWare

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.



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