Screwloose
Professional IT Solutions

01 Aug - 31 Aug

Security Business Review

Generated For

[redacted]

[redacted] | Analyzed domain

Internet Software & Services | Industry

34 | Employees

This assessment report was prepared by

Screwloose IT

☎ 1300 794 777 | screwlooseit.com.au | cyber@screwlooseit.com.au

Summary

Screwloose Professional IT Solutions

SECURED ASSETS

305 IPs & Domains — No Changes	**34** Employees 2 Increase	**16** Devices — No Changes
59 Cloud Drives	**32** Mailboxes	**2** Browsers

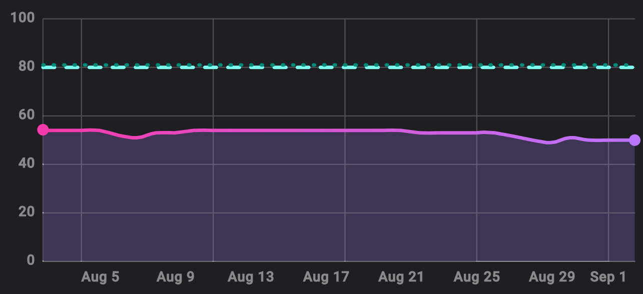
FINANCIAL EXPOSURE

~ $132,000
Possible Financial Loss

2% increase from last period
$3,000

Possible Financial Loss - This data estimates potential financial losses based on internal and external scans, user risk, vulnerabilities and overall security posture, factoring in industry, company size, digital assets and attack surface.

SECURITY SCORE



50
Current Score
4 Decrease

81
Industry benchmark

54
Starting Score

80
Insurance threshold

Security Score - The Security Score is based on coverage (activated security controls) and the volume and severity of issues within each control.

Financial loss due to cybersecurity incidents in Internet Software & Services

In the Internet Software & Services industry, with its valuable user and corporate data services, Cyberattacks can have an average cost per breach estimated around 8.64 million.

Beyond the direct fiscal impact, non-compliance with data protection regulations (e.g. GDPR) can lead to severe penalties with fines up to €20 million, or 4% of their global turnover if user data has been mishandled. Significant instances, such as the data breach suffered by LinkedIn revealing confidential data of millions, highlight the consequences of cybersecurity threats.

DETECTIONS & RESPONSES

425
Total Detection

8 ✓
Fixed

0
Ignored

0
In Progress

417
Open

Cloud Data	50%	4
Cloud Directory Posture	25%	2
Endpoint Protection	13%	1
Email Protection	13%	1
Phishing Simulations	0%	
Awareness	0%	
Dark Web Monitoring	0%	
External Footprint Scan	0%	
Secure Browsing	0%	

User Posture

SAFE VS RISKY USERS

34 Total

100%
34 safe users

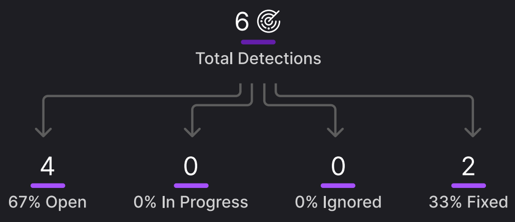
0%
0 unsafe users

2 Increase from last period

TOP RISKY USERS

No risky users to report

CLOUD DIRECTORY DETECTIONS & RESPONSES



6
Total Detections

4
67% Open

0
0% In Progress

0
0% Ignored

2
33% Fixed

CLOUD DIRECTORY DETECTIONS BY TYPE

0
Multi Factor Authentication

0
Suspicious Mailbox Rules

1
Inactive User

5
Suspicious Login
8 Decrease

TOP SUSPICIOUS LOGINS

Cebu City Philippines
7 Logins | Closed

Elizabeth United States, New Jersey
5 Logins | Closed

San Juan City Philippines
4 Logins | Closed

Tuguegarao City Philippines
6 Logins | Closed

Singapore (Queenstown Estate) Singapore
5 Logins | Open

*The above is a subset of security detections, highlighted based on the severity and recency of the detections.

PHISHING SIMULATIONS

No phishing simulation to report

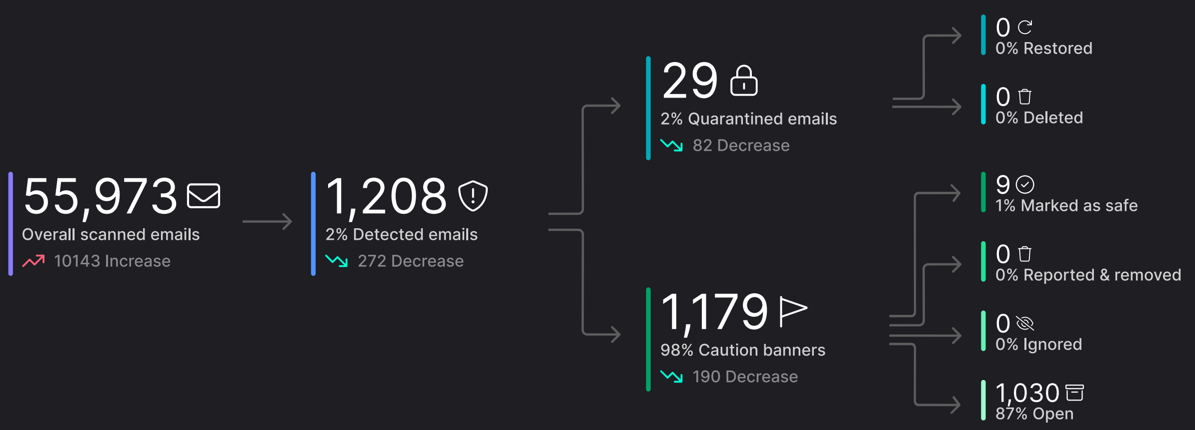
AWARENESS CAMPAIGNS

07 Aug
30 Assignees
33% Completed

USERS WITH MOST INCOMPLETE CAMPAIGNS	#
[redacted]	1
[redacted]	1
[redacted]	1

Email Protection

DETECTIONS & RESPONSES



55,973 Overall scanned emails — 10143 Increase

1,208 — 2% Detected emails — 272 Decrease

29 — 2% Quarantined emails — 82 Decrease

- 0 — 0% Restored
- 0 — 0% Deleted

1,179 — 98% Caution banners — 190 Decrease

- 9 — 1% Marked as safe
- 0 — 0% Reported & removed
- 0 — 0% Ignored
- 1,030 — 87% Open

ATTACK TYPE BREAKDOWN

285 ⚠ Spam — 193 Increase

15 Phishing — 13 Increase

674 Impersonation — 44 Decrease

10 Virus — 9 Increase

1 Scam

10 Other — 386 Decrease

TOP TARGETED USERS

	# of detections
[redacted]	519
[redacted]	142
[redacted]	86
[redacted]	7
[redacted]	5

External Assets

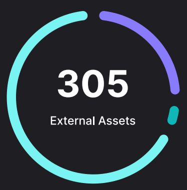
TOP RISKY ASSETS

Asset	Type	Geo-Location	Issues
[redacted]	IP	Australia	151
[redacted]	IP	Australia	99
[redacted]	IP	Australia	99
[redacted]	IP	Australia	27

EXTERNAL FOOTPRINT DETECTIONS & RESPONSES

No detections to report

INTERNET ASSETS TYPES



77 — 25% IP — No Changes

14 — 5% Domain — No Changes

214 — 70% Sub-domain — No Changes

Risk: 40 Unsafe — No Changes

13 Unsafe — No Changes

155 Unsafe — No Changes

Endpoint Protection

SECURED DEVICES

16

13 Unsafe Devices

OPERATING SYSTEM BREAKDOWN

15 ⊞	1 ▦	0
94% Windows	6% Windows Server	0% MacOS
12 Unsafe	1 Unsafe	

DEVICE DETECTION BY TYPE

11 Decrease

0 Antivirus Threat
2 Decrease

0 Antivirus Policy
6 Decrease

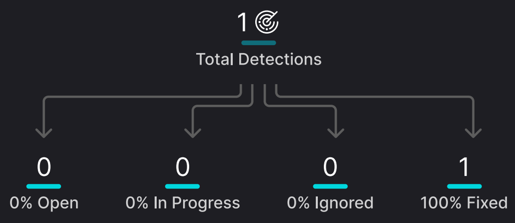
1 Endpoint Posture
3 Decrease

0 Endpoint Ransomware

TOP RISKY DEVICES

Identifier	Count	Status	OS
[redacted]	8	Medium	▦
[redacted]	7	Medium	⊞
[redacted]	7	Medium	⊞
[redacted]	5	Medium	⊞

ENDPOINT DETECTIONS & RESPONSES


1
Total Detections

0	0	0	1
0% Open	0% In Progress	0% Ignored	100% Fixed

Cloud Data Protection

CLOUD DRIVES

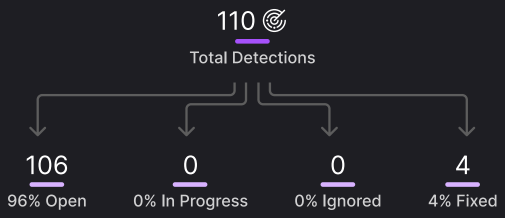
59

EXPOSURE BY TYPE

4 External Share
2 Increase

94 Public Link
54 Increase

CLOUD DATA DETECTIONS & RESPONSES


110
Total Detections

106	0	0	4
96% Open	0% In Progress	0% Ignored	4% Fixed

TOP RISKIEST PATHS

Path	Issues	App
[redacted]	1	☁
[redacted]	1	☁
[redacted]	1	☁
[redacted]	1	☁
[redacted]	1	☁

Glossary

IP Address

An IP address is a distinct numerical label, unique to a device, server or website, serving as a specific online location. It's vital for all online activities, and should be protected as a valuable 'digital asset'.

Cyber Posture Rating

Based on the results of a non-intrusive external surface attack scan and dark web monitoring, a cyber posture rating is calculated from 0-100 which represents the level of risk allocated to a company's external digital footprint.

Security Findings

Security findings refer to identified vulnerabilities or weaknesses discovered during the risk assessment, highlighting security issues that organizations need to address. The findings in this report cover; Network & IT, Application, Human, and Compromised Credentials.

Dark Web

The Dark Web is a hidden part of the internet, commonly used by cybercriminals for illegal activities. A dark web scan identifies leaked credentials indicating the potential for unauthorized access of personal data, eventually leading to the risk of security breaches.

External Surface

The external surface refers to an organization's digital footprint that is visible and accessible to the public. This includes company websites, email systems, servers, protocols and other exposed services.

Assets

For the purposes of this report, a digital asset refers to company owned domains, subdomains, servers, and IP addresses. These assets often carry a lot of value, as they form a part of an organization's digital identity and operations which should be protected against cyberthreats.

Domain

A domain is a unique identifier that represents the web address or URL which is crucial for people to find and interact with a website. Domains are essential digital assets because of the traffic they attract, requiring protection to prevent misuse or unauthorized changes.

Web Server

A web server is a system that stores, processes, and delivers web pages to users. These servers require regular maintenance and if not updated can open up publicly accessible vulnerabilities.

TLS/SSL

TLS and SSL are protocols designed to provide secure communication by encrypting data between a browser and a website. It's crucial to ensure up-to-date versions of TLS or SSL to avoid vulnerabilities in the system.

Web Certificate

A web certificate authenticates a website’s identity and enables an encrypted connection. When it is outdated, site traffic may be compromised.

Common Threats

Phishing

Hackers use phishing to trick people into giving away sensitive information, such as passwords, by posing as a trustworthy entity or person. Holistic protection against phishing combines email security, browsing, endpoint protection, perimeter posture, and awareness culture in one native solution.

Ransomware

This malware encrypts a victim's files or data and demands payment in exchange for the decryption key, causing damage to businesses.A managed anti-virus solution should detect and isolate infected systems in parallel with monitoring of vulnerable servers, email attachments, and abnormal activity.

Data Loss

Unauthorized loss of sensitive information, can have severe consequences, including financial losses, reputational damage, and legal implications. Data loss protection includes data in the cloud and secures several vectors of attack while exposing the risks of negligent and intentional data exfiltration.

User Risk

Users are the first line of defense against a cyber attack but are often also the weakest link, so in addition to ongoing security training, employees should be protected through monitoring for leaked credentials, spear-phishing prevention, as well as cloud and device posture analysis.

Common Threats FAQ

How can I identify a phishing email?

Looking for suspicious senders or sloppy formatting are quick indicators you can catch with your eye. But hackers are getting more sophisticated, and it is recommended by regulation and industry best practices to utilize email security with other detection tools.

How can I protect my computer or network from ransomware attacks?

To defend against ransomware, keep software updated, use reputable antivirus software, be cautious with email attachments/links, regularly back up important files offline/cloud, enable automatic backups/versioning, and educate about phishing and safe browsing. Bottom line employees need to be actively involved in security, and systems need to be in place to quickly detect and prevent ransomware attacks.

How to prevent data loss?

In a world where we are focused on collaboration, the same tools that allow us to be productive open up vectors of attack for external exposure of confidential data. It's about being diligent regarding cloud posture and sharing best practices to avoid accidental data leakage.

How to prevent user risk in cybersecurity?

To prevent user risk in cybersecurity, implement comprehensive user awareness and training programs to educate employees about common cyber threats, phishing attacks, and safe online practices as well as having the right tools in place to automate user access policies and mitigate common vectors of risk.

Screwloose
Professional IT Solutions

This assessment report was prepared by

Screwloose IT

☎ 1300 794 777

🌐 screwlooseit.com.au

✉ cyber@screwlooseit.com.au

Generated For

[redacted]

[redacted] | Analyzed domain

Internet Software & Services | Industry

34 | Employees

Secure Your Business Today

Powerful Cybersecurity in Action