2023

Cybersecurity Risk Assessment Report
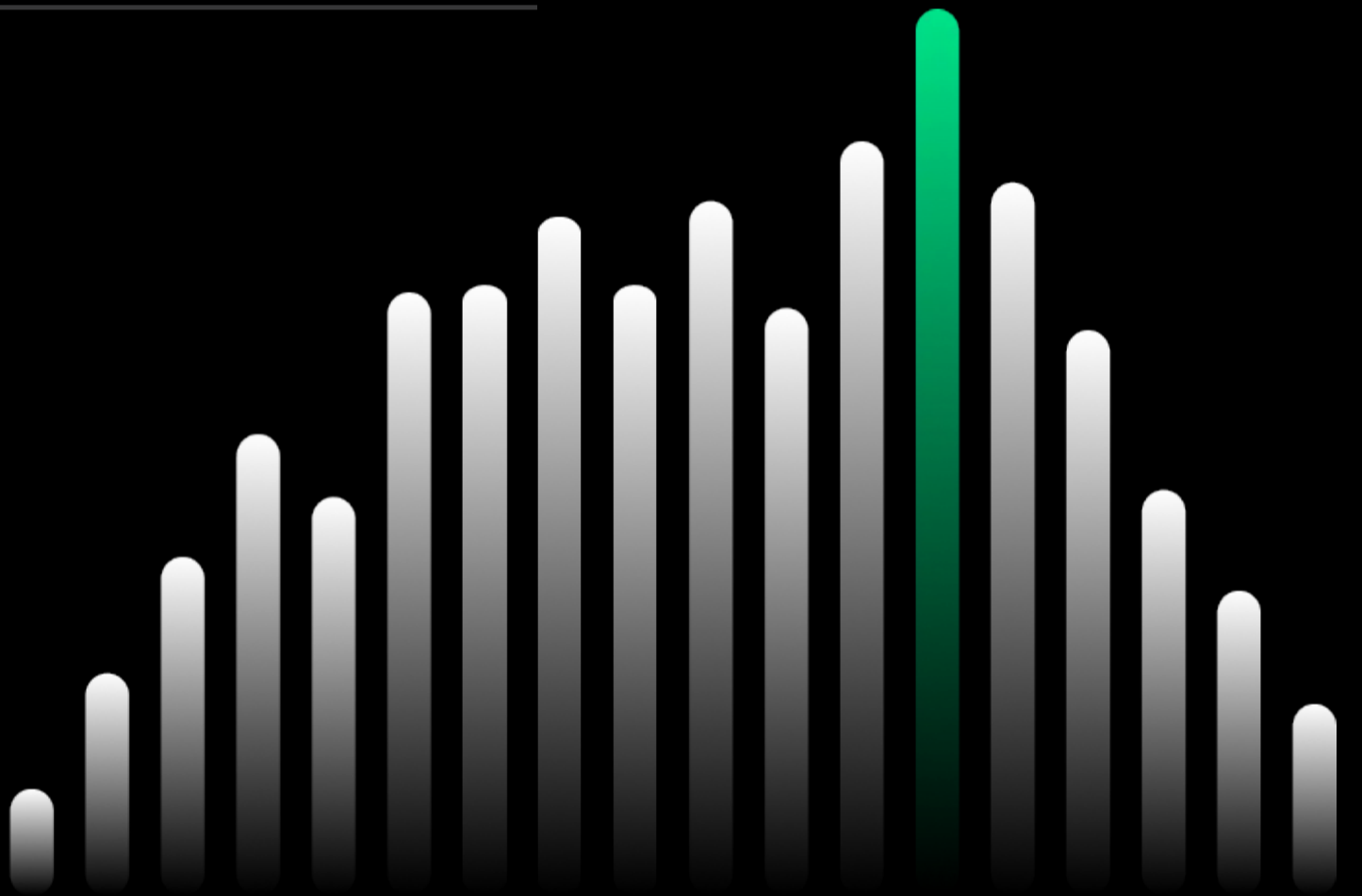
Generated For

Analyzed domain

Industrials & Manufacturing | Industry

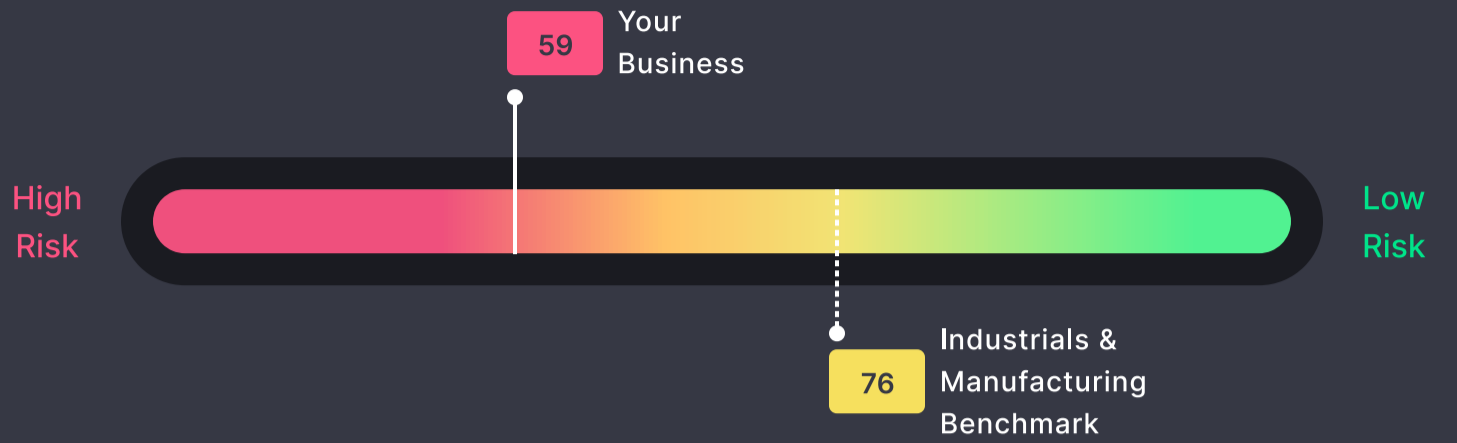11-50 | Employees

This assessment report was prepared by

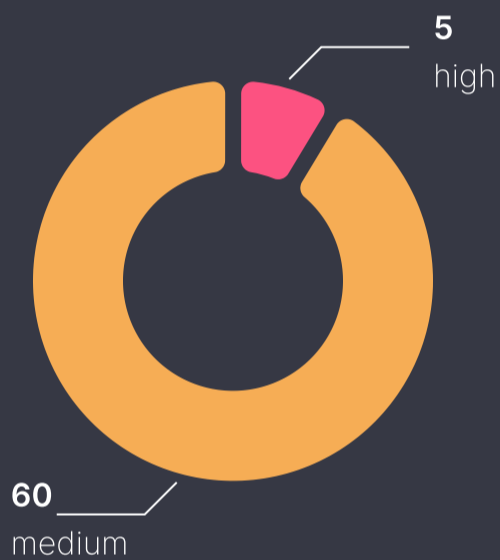## H2 Cyber Risk Advisory Services Ltd

Risk Analysis

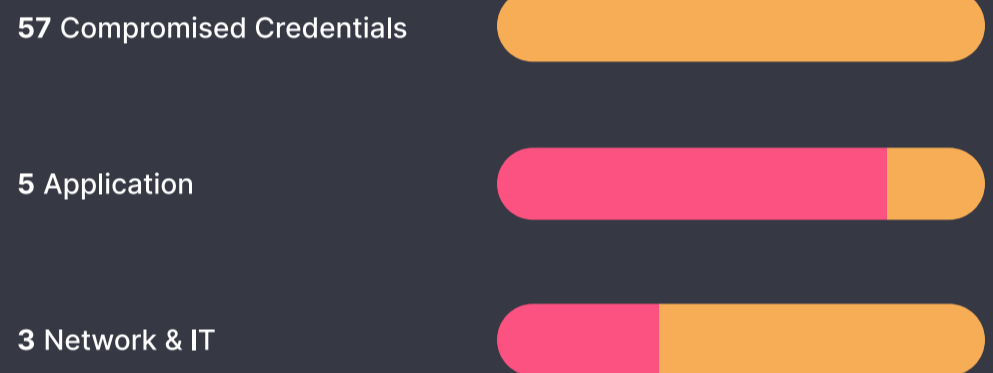## Cyber Posture Rating

59

Cyber Posture Rating

Risk Scale

59 Your Business

High Risk — Low Risk

76 Industrials & Manufacturing Benchmark

Risk Status Legend: ●High | ●Medium | ●Low | ●Secured

65 Security Findings by Severity

- 5 high
- 60 medium

Security Issues by Category

- **57** Compromised Credentials
- **5** Application
- **3** Network & IT

Dark Web Findings

57

Compromised Credentials

External Surface Findings

8

Publicly Exposed Vulnerable Assets

Assets	Employees
10	11-50

Industry	Issues
Industrials & Manufacturing	65

Possible Financial Loss

~ £27,000

Possible Financial Loss- this data aims to estimate the potential financial loss that can occur based on the scan results, taking into account the industry, the findings, the size of the digital footprint (number of discovered assets), and the company's size.

Assets & Findings

Top Assets With Potential Risk (5 / 10)

Asset	Asset Type	Geolocation	Findings
	Domain	United Kingdom	2
	Domain	United Kingdom	2
	Domain	United Kingdom	1
	Domain	United Kingdom	1
	IP	United Kingdom	1

External surface scan - Top Vulnerabilities (5 / 8)

Vulnerability	Risk	Findings
⚠️ Exposed management services	High	2
⚠️ Technologies with high severity vulnerabilities	High	2
⚠️ Missing email protection record (SPF)	High	1
⚠️ Missing email protection records (DMARC)	Medium	2
⚠️ WordPress exposed users via author url	Medium	1

Impact: Vulnerable Assets
Publicly exposed vulnerable assets can be exploited by hackers to launch attacks against your company.

Dark Web Scan Findings (5 / 57)

Users Compromised	Password
⚠️	N*********1
⚠️	p******a
⚠️	p*******※
⚠️	8******w
⚠️	m*******1

Impact: Compromised Credentials
Business email compromise can result in email spoofing and the hacking of your company's accounts.

External Risk Posture

Your complete risk posture offers an extensive overview of your organization's cyber exposure, covering assets, data vulnerabilities, and technologies that could be exploited, as identified by our External Surface Scan.

Categories - Secured / At Risk		Findings / # of Assets Impacted
At Risk	Employee Attack Surface	57 / 1 Assets
At Risk	Mail Server	3 / 2 Assets
At Risk	Exposed Services	2 / 1 Assets
At Risk	Technologies	2 / 1 Assets
At Risk	Application Security	1 / 1 Assets
Secured	Cloud	0 / 0 Assets
Secured	TLS	0 / 0 Assets
Secured	DNS	0 / 0 Assets
Secured	Domain Attacks	0 / 0 Assets
Secured	Web Server	0 / 0 Assets
Secured	Asset Reputation	0 / 0 Assets
Secured	Endpoint	0 / 0 Assets
Secured	Social Posture	0 / 0 Assets
Secured	Responsiveness	0 / 0 Assets
Secured	Security Team	0 / 0 Assets

Financial loss due to cybersecurity incidents in Industrials & Manufacturing

In the Industrials & Manufacturing industry, where complex supply chains and industrial control systems are commonplace, the impact of a data breach averages approximately $5.41 million.

Lapses in data security can have regulatory implications where violations of legislation such as NIST or GDPR could result in fines up to €20 million or 4% of a company's global revenue. The breach at steel manufacturing giant ThyssenKrupp, potentially disrupting their production lines, serves as a sobering example of the potential adverse effects of security vulnerabilities.

Powered by Guardz

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.
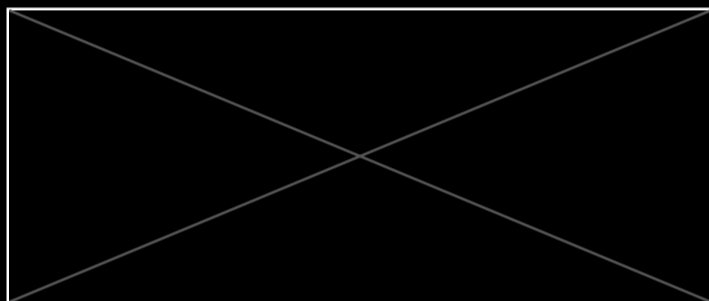
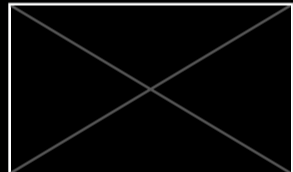was prepared by

H2 Cyber Risk Advisory Services Ltd

📞 0845 5443742

✉ kevin_hawkins@hah2.co.uk

🌐 www.hah2.co.uk

Generated For

🛡 **Industrials & Manufacturing** | Industry

 | Employees

Secure Your Business Today

Powerful Cybersecurity in Action