Cyber Insurance Risk&Readiness

ACME Group

Report Generated: 12/08/2025

Overview

We have conducted a comprehensive 360-degree risk assessment of your company and the essential cyber defenses within your supply chain. Through an in-depth analysis of your external attack surface, internal cyber controls, and financial risk impact, we can accurately pinpoint your cybersecurity exposure.

The aim of this report is to provide valuable insights into your company's cybersecurity posture and to support your company's investment strategy in cyber defenses.

360 Risk Assessment

The 360-degree risk assessment involves three core cyber elements tailored to assess your company and your critical supply chain: Attack Surface, Compliance Risk, and Financial Risk Quantification. The integration of these three evaluations provides a comprehensive 360-degree understanding of your cyber exposure, enabling strategic planning and effective mitigation of potential cyber-attacks.

This report combines the observation of your company and supply chain cybersecurity defences, delivering industry-standard insights.

Cyber Rating – Compliance Risk - Financial Exposure - Remediation Plans

Attack Surface, Compliance and Risk Quantification

Attack Surface Management (ASM). ASM is a non-intrusive cybersecurity assessment of a company's internet-facing web servers - web applications, websites, and email systems.

This assessment examines the security settings and potential vulnerabilities within these systems, yielding a comprehensive cybersecurity score and remediation recommendation. Through the implementation of strong cyber controls, the organization can achieve a praiseworthy ASM rating, thereby reducing the likelihood of potential cyber-attacks.

Compliance Risk Management (CRM). CRM ratings reflect the organization's adherence to regulatory requirements and industry-standard controls and policies.

Encompassing aspects such as data protection, privacy regulations, and security frameworks. The assessment reveals that the organization has demonstrated a high level of commitment to compliance, earning a favorable CRM rating.

Financial Risk Quantification (FRQ). The FRQ focuses on the organization's preparedness to handle financial losses in the event of a cybersecurity incident.

Consideration factors such as CRM, ASM ratings, and asset values are calculated to build a loss expectancy and budget requirement to mitigate cyber risks.

In Addition... not rated. We provide an observation of your company's **Threat Intelligence (TI).** TI provides insights into emerging threats, attack vectors, and indicators of compromise. The report includes a comprehensive overview of the threat landscape relevant to the organization, enabling proactive threat detection and response. It also provides recommendations for leveraging threat intelligence to enhance the organization's overall security posture.

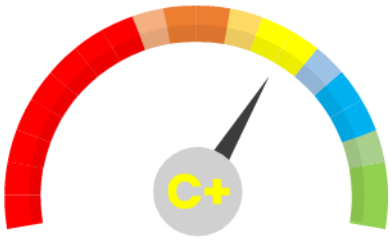
Trusted Cyber Ratings

Our cybersecurity risk ratings are a reliable and trustworthy source of information for assessing the risk profile of any business.
All our ratings are aligned with industry security standards, including the *US Commerce of Trade - **Principles For Fair And Accurate Security Ratings**, *National Institute of Standards and Technology - **NIST NVD CVE** and the *Common Vulnerability Scoring System - **CVSS V3.0**.

Executive Summary

This in-depth report analyzes your internet apps, data, and security controls to give a complete picture of your cybersecurity posture. It prioritizes improvement areas and offers recommendations for strengthening your defenses.

Attack Surface Rating

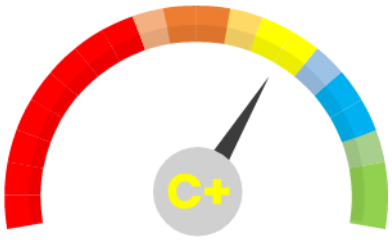


Financial Impact

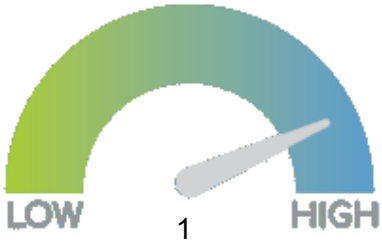
Target Annual Loss

Max Annual Loss

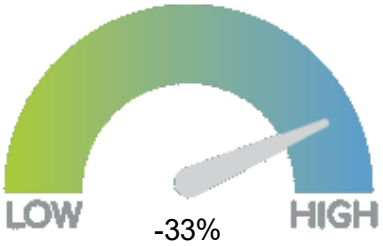
Compliance Rating



Attack Probability

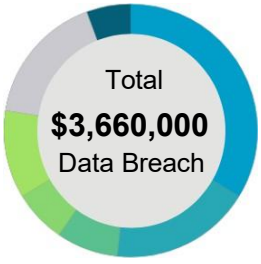


Control Failure Rate



Thresholds

Target Annual Loss



Max Annual Loss

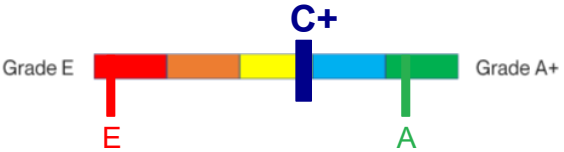
Target Annual Loss

Max Annual Loss

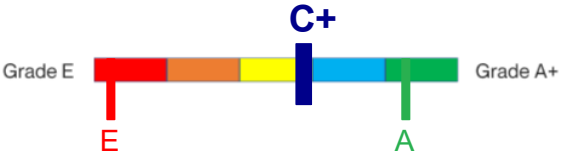
Target Annual Loss

Max Annual Loss

Attack Surface Grade



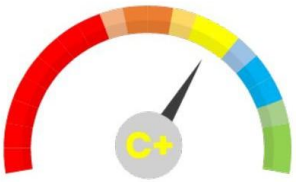
Compliance Grade



Executive Summary Explained

Below is an explanation of how to interpret the executive summary scores and the methodology used to calculate them. Please note that the algorithms may be updated periodically to account for emerging industry profile risks and threats.

Attack Surface



Cygienic evaluates a company's internet assets by thoroughly examining six key checkpoints with fifty-four cyber probes. The grade is assigned using an international rating system ranging from A+ to E, with an A+ indicating that the company's cybersecurity defense is at an industry-leading level.

Checkpoint	# Probes	Weight %
Email Secuirty	6	11
Webpage Security	11	15
Data Privacy	8	14
System Compromised	5	17
System Vulnerability	8	26
Open Network Ports	16	17

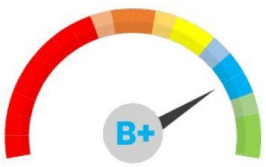
Grades	Pass %	Result
A+	93-100	Leader
A+	85-92	Advanced
B+	79-84	Excellent
B	73-78	Good
C+	62-72	Average
C	55-61	Low
D+	47-54	Poor
D	40-46	V. Poor
E	0-39	Failed

Financial Impact

Financial Impact estimates the expected financial loss from a cyberattack. Additionally, the algorithms calculate the probability of a cyberattack, the likelihood of control failure, and the estimated insurance costs. Below are the formulars used to calculate the impact. A comprehensive report is provided in the financial quantification section of this report.

Financial Quantification	Calculation
Attack Surface Grade weighting for the probability of cyberattack	50%
Security Compliance Grade weighting for the probability of cyberattack	50%
Probability of cyber-attack calculation per year	80%=1 to 40%=3
Insurance calculation = % of event annual loss expectancy	1%
Ransomware calculation = % of total annual sales revenue	2.80%
Total Annual Loss= Data breach + System breach + Ransomware costs	ALE=
Data Breach cost per record	$183
System Breach recovery days	10 days

Security Compliance



Security Compliance grades stem from Cygienic's exclusive audit program, wherein each control is assessed and weighted according to the responder's input. Notably, during onboarding, companies undergo a proprietary cybersecurity survey aligned with ISO27001 standards to gauge their cyber readiness

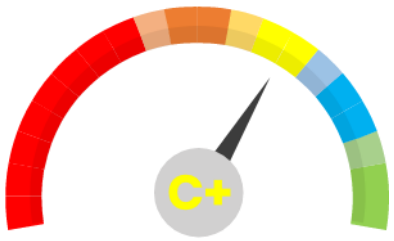
Compliance Control Weighting	Risk Level
8	Critical
6	High
4	Medium
2	Low

Grades	Pass %	Result
A+	93-100	Leader
A+	85-92	Advanced
B+	79-84	Excellent
B	73-78	Good
C+	62-72	Average
C	55-61	Low
D+	47-54	Poor
D	40-46	V. Poor
E	0-39	Failed

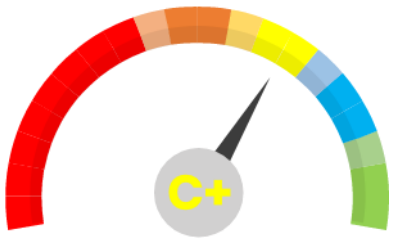
Compliance Weighting		
Fully	Mostly	Partially
100%	75%	50%
Limited	Non	NA
25%	0%	Na

Attack Surface Results

Insured Company Attack Surface Rating



Risk Survey Rating



Insured Client Attack Surface Rating

Leader	0
Advanced	1
Excellent	1
Good	1
Average	3
Low	2
Poor	0
V. Poor	1
Critical	0

Attack Surface Checkpoint Ratings

Email Security	A
Webpage Security	E
System Compromised	A+
Vulnerability	C+
Data Privacy	E
Network Ports	B

Icon	Vulnerability	Domain Failed	Total Vuln
!!!!	Multiple Critical Risk Vulnerabilities	1	14
!!!!	Multiple High Risk Vulnerabilities	1	51
!!!!	Multiple Medium Risk Vulnerabilities	1	49

Bad Network IP

No bad IP found.

ACME Group	Domain Rating	Last Scan
Redacted	A	12/08/2025
Redacted	B+	12/08/2025
Redacted	B	12/08/2025
Redacted	C+	12/08/2025
Redacted	C+	12/08/2025
Redacted	C+	12/08/2025
Redacted	C	12/08/2025
Redacted	C	12/08/2025
Redacted	D	12/08/2025

Email Security

A

Control	Description	Remediation
Email SPF	Email SPF (Sender Policy Framework) is a security protocol used to verify the authenticity of an email sender's domain, helping to prevent email spoofing and phishing attacks. For example, it will detect if an internal company email was sent from a company's email server. If not, the email will be flagged as a spoof or a phishing email - emails are rejected, quarantined, or marked as spam to notify the user.	Redacted

Control	Description	Remediation
Email SPF Treatment	Email SPF (Sender Policy Framework) treatment is a security protocol used to verify the authenticity of an email sender's domain, helping to prevent email spoofing and phishing attacks. For example, it will detect if an internal company email was sent from a company's email server. If not, the email will be flagged as a spoof or a phishing email - emails are rejected, quarantined, or marked as spam to notify the user.	Redacted

Control	Description	Remediation
DMARC Authentication	DMARC authentication is a robust email security protocol that helps prevent email spoofing and phishing attacks by verifying the authenticity of email senders and their domains.	Redacted .

Domains Failed
Redacted

Control	Description	Remediation
DMARC Treatment	A Dmarc blocked email must be appropriately managed by either rejecting, quarantining or marking the message as spam or phishing - failure to manage the message will not truly block or notify the user that this is a phishing email.	Redacted

Domains Failed
Redacted

Control	Description	Remediation
Open Relay Security	An email open relay is a misconfigured or unauthorized mail server that allows third parties to send emails through it without proper authentication, potentially leading to spam and security vulnerabilities	Redacted

Control	Description	Remediation

Email Encryption-STARTTLS	SMTP email servers are not secured by default, which means that if you were to send email over SMTP without StartTLS protocol the email could be intercepted and easily interpreted. STARTTLS is an email protocol command that tells the receiving email server it wants to upgrade to a secure connection and that the content must be encrypted.	Redacted

Webpage Security

E

Control	Description	Remediation
HSTS-Enabled	HSTS-Enabled refers to a secure web browsing feature that enforces the use of HTTPS (HyperText Transfer Protocol Secure) for all communication between a web browser and a website, thereby enhancing online security by preventing unencrypted connections	Redacted

Domains Failed
Redacted

ReControl	Description	Remediation
XFrame-Option	The "X-Frame-Options" is a security HTTP header that allows a website to control whether or not its content can be displayed within a frame or iframe on another website, thereby helping to prevent clickjacking attacks.	Redacted

Domains Failed
Redacted

Control	Description	Remediation
XSS-Protection	XSS-Protection is a security mechanism designed to safeguard web applications by detecting and mitigating cross-site scripting (XSS) vulnerabilities. The web pages are protected from malicious code injections between the server and the user's browser.	Redacted

Domains Failed
Redacted

Control	Description	Remediation
MIME X-Content	Servers without standard MIME file format policy fail to protect attackers from uploading malicious executable programmes within a different file type, also known as MIME Sniffing. Mime x-content refers to the specialized format or content associated with a MIME (Multipurpose Internet Mail Extensions) message, typically used for encoding and transmitting multimedia data	Redacted

Domains Failed
Redacted

Control	Description	Remediation
Content Security Policy	Content Security Policy (CSP) is a security feature implemented in web applications to mitigate the risks of cross-site scripting (XSS) attacks by controlling which resources can be loaded and executed in a web page.	Redacted

Domains Failed
Redacted

Control	Description	Remediation
Referrer Policy	The Referrer policy is a security feature in web browsers that determines how much information about the user's current web page is shared with the destination website when a link is clicked. Webpages that DO NOT secure with a referrer policy fail to protect the user's identity and data when being redirected to another website	Redacted

Domains Failed
Redacted

Control	Description	Remediation
Cache-Control	A Server Cache-Control allows webpage data storage management policies to block exposure of server memory data loss. A server cache-control policy determines how long and under what conditions a server's cached data can be stored and reused	Redacted

Domains Failed
Redacted

Control	Description	Remediation
X Domain permission	X Domain permissions allow webpages to use approved whitelists to control content from other domains and web services to stop fake or malicious data from other websites.	Redacted

Domains Failed

Control	Description	Remediation
Except-CT TLS	Website encryption certificates should be verified by the CT Public Log - a trusted public database subscription service.	Redacted

Domains Failed
Redacted

Control	Description	Remediation
Web-Server Version	A server that displays the web server hostname and version can be useful for hackers during their reconnaissance stage. e.g Server: Apache v1.2 can be used to check for known vulnerabilities on Apache.	Redacted

Control	Description	Remediation
X-Powered-By	A Server that displays an X-powered service & version is exposing critical system information that the attacker can use against them e.g displaying X-powered 'ASP.net v1.0' could be used to find known vulnerabilities in ASP	Redacted

Domains Failed
Redacted

System Compromised

Control	Description	Remediation
Open Proxy Services	A webserver hosting and distributing anonymous open web proxy services poses a grave threat to online safety. It can infect unsuspecting visitors' devices, compromise sensitive data, and contribute to the spread of cyber threats, endangering both individuals and businesses. Such malicious activities undermine trust and security on the internet. An anonymous open proxy service allows ANY internet user online anonymity and privacy. It can help users hide their IP address from web servers since the server requests appear to originate from the proxy server.	Redacted

Control	Description	Remediation
Malware Hosting	A web server registered for hosting and distributing malware poses a severe threat to online security. It jeopardizes user data, compromises privacy, and undermines trust in online interactions, making it a dangerous breeding ground for cybercriminal activities.	Redacted

Control	Description	Remediation
Bot Net Services	A webserver hosting and distributing Bot Net Services poses a grave threat to online safety. It can infect unsuspecting visitors' devices, compromise sensitive data, and contribute to the spread of cyber threats, endangering both individuals and businesses. Such malicious activities undermine trust and security on the internet.	Redacted

Control	Description	Remediation

Spam Host	A webserver hosting and distributing illegal email spam messages poses a grave threat to online safety. It can infect unsuspecting visitors' devices, compromise sensitive data, and contribute to the spread of cyber threats, endangering both individuals and businesses. Such malicious activities undermine trust and security on the internet.	Redacted

Vulnerability

Control	Description	Remediation

Multiple Critical Risk Vulnerabilities	Exposing a web server with CRITICAL vulnerabilities poses a severe security risk, leaving it susceptible to malicious attacks. Unaddressed vulnerabilities can lead to unauthorized access, data breaches, and potential compromise of sensitive information, emphasizing the urgency of timely security patching and proactive measures.	Redacted

Domains Failed
Redacted

Control	Description	Remediation
Multiple High Risk Vulnerabilities	Exposing a web server with HIGH vulnerabilities poses a severe security risk, leaving it susceptible to malicious attacks. Unaddressed vulnerabilities can lead to unauthorized access, data breaches, and potential compromise of sensitive information, emphasizing the urgency of timely security patching and proactive measures.	Redacted

Domains Failed
Redacted

Control	Description	Remediation
Multiple Medium Risk Vulnerabilities	Exposing a web server with MEDIUM vulnerabilities poses a considerable security risk, leaving it susceptible to malicious attacks. Unaddressed vulnerabilities can lead to unauthorized access, data breaches, and potential compromise of sensitive information, emphasizing the urgency of timely security patching and proactive measures.	Redacted

Domains Failed
Redacted

Control	Description	Remediation
SSL Cert Heartbleed Vuln	TLS Heartbleed is a critical security vulnerability that affected the OpenSSL cryptographic software library, allowing attackers to exploit a flaw in the TLS (Transport Layer Security) protocol to steal sensitive information from servers, such as private keys and user data. OpenSSL below version 1.0.1g does not properly handle Heartbleed Extension packets.	Redacted

Domains Failed

Control	Description	Remediation
TLS CCS Injection Vuln	TLS CCS Injection is a security vulnerability that occurs when an attacker manipulates the Change Cipher Spec (CCS) protocol within a Transport Layer Security (TLS) connection to disrupt or compromise the encryption and integrity of data being exchanged. - CCS allows hijack sessions to obtain sensitive information via a crafted TLS handshake, aka the "CCS Injection"	Redacted

Domains Failed

Control	Description	Remediation
SSL Renegotiation	The SSL/TLS renegotiation vulnerability, a longstanding security issue, empowers malicious actors to execute Distributed Denial of Service (DDoS) attacks and infiltrate established SSL/TLS sessions between clients and servers. Through this exploit, they gain the potential to intercept and manipulate the transmitted data. This vulnerability is typically not a concern when servers are utilizing the latest TLS certs and web server engines.	Redacted

Domains Failed

Redacted

Control	Description	Remediation
TLS Fallback Vuln	TLS-Fallback is a security mechanism that allows a system to gracefully switch to an older, less secure version of the TLS (Transport Layer Security) protocol in case of compatibility issues, but it is generally discouraged due to its potential vulnerabilities. a downgrade the SSL standard e.g. SSL 3.0, allows the attacker to decrypt all communication and inject malicious code into the website.	Redacted

Domains Failed
Redacted

Data Privacy

E

Control	Description	Remediation
SSL Expiry	A website SSL certificate must not expire otherwise users cannot verify the authenticity and trustworthiness of the site. You cannot renew an expired SSL certificate, but you can renew it prior to the expiry date.	Redacted

Domains Failed
Redacted

Control	Description	Remediation

SSL Cert Cipher Suite	The SSL encryption certificate must meet the latest encryption standards to protect user data. Data being transferred between the browser and the site is at risk of being breached if there is a weak SSL cipher.	Redacted

Domains Failed
Redacted

Control	Description	Remediation
SSL Encryption Version 1.3	An SSL certificate with the latest encryption version (1.3 or 1.2) will secure and protect the data during transit between the browser and the site - any encryption version below v1.2 is no longer considered safe.	Redacted

Domains Failed

Control	Description	Remediation

Secure Cookie	Cookie Secure flag will only allow the user's browser to share cookie data if the transmission is encrypted or via https only - any http requests (unencrypted) transmissions will be ignored by the browser.	Redacted

Domains Failed

Control	Description	Remediation
Samesite Cookie	HTTP Same-Site prevents the browser from sending cookie data to a hacker - the security features will block domains (other than the original cookies domain) from receiving the user's cookie data.	Redacted

Domains Failed

Control	Description	Remediation
Http-Only Cookie	Cookie HTTP-Only flag configuration protects the cookie data stored in the user's browser from being viewed or stolen by a hacker. This will help to prevent man-in-the-middle and cross-site scripting cyber attacks.	Redacted

Domains Failed

Control	Description	Remediation
Cookie Notification	A cookie notification page found on a website or web application allows the user to understand how their cookie data is managed by the website owner - without such a notification, the trustworthiness of the website is lowered. A cookie policy is required to conform with the EU GDPR regulations.	Redacted

Domains Failed

Control	Description	Remediation
Privacy Notification	A website without a Data Privacy notification page is deemed as untrustworthy. If you handle data about identifiable individuals, you very likely come under at least one privacy law. Many of these laws directly or indirectly require that you publish a Privacy Policy on your website. You do not need to physically reside in a country to be regulated by its privacy law. The notification must explain how data is collected and managed. In many countries this is now a regulatory requirement and failure to do this will lower the trustworthiness of the website.	Redacted

Domains Failed

Control	Description	Remediation

Cookie Consent	The website must provide a cookie consent option for the user to approve or reject their cookie data being accessed by the website owner - this is required for all websites to meet GDPR and EU data privacy laws.	Redacted

Domains Failed

Network Ports

Control	Description	Remediation
SMB: 139	SMB Port 139 provides network file and printer-sharing capabilities in Windows-based environments. When a server port is accessible from the public internet, it becomes a potential entry point for malicious actors seeking to exploit vulnerabilities in the system. These vulnerabilities can range from known software weaknesses to zero-day exploits, and they can lead to unauthorized access, data breaches, and even the compromise of the entire server. Moreover, open server ports can be susceptible to brute force attacks, DDoS attacks, and other malicious activities.	Redacted

Domains Failed

Control	Description	Remediation

Mongo db: 27017	Mongo db Port 27017 is a relational database management system for storing application and server data. When a server port is accessible from the public internet, it becomes a potential entry point for malicious actors seeking to exploit vulnerabilities in the system. These vulnerabilities can range from known software weaknesses to zero-day exploits, and they can lead to unauthorized access, data breaches, and even the compromise of the entire server. Moreover, open server ports can be susceptible to brute force attacks, DDoS attacks, and other malicious activities.	Redacted

Control	Description	Remediation
MS SQL: 1433	MS SQL port 1433 is a Microsoft relational database management system for storing application and server data. When a server port is accessible from the public internet, it becomes a potential entry point for malicious actors seeking to exploit vulnerabilities in the system. These vulnerabilities can range from known software weaknesses to zero-day exploits, and they can lead to unauthorized access, data breaches, and even the compromise of the entire server. Moreover, open server ports can be susceptible to brute force attacks, DDoS attacks, and other malicious activities.	Redacted

Domains Failed

Control	Description	Remediation

MySQL: 3306	MySQL is an open-source relational database management system for storing application and server data which could be targeted by a hackers. When a server port is accessible from the public internet, it becomes a potential entry point for malicious actors seeking to exploit vulnerabilities in the system. These vulnerabilities can range from known software weaknesses to zero-day exploits, and they can lead to unauthorized access, data breaches, and even the compromise of the entire server. Moreover, open server ports can be susceptible to brute force attacks, DDoS attacks, and other malicious activities.	Redacted

Domains Failed

Control	Description	Remediation
PostgreSQL Db: 5432	PostgreSQL Port 5432 is a relational database management system for storing application and server data. When a server port is accessible from the public internet, it becomes a potential entry point for malicious actors seeking to exploit vulnerabilities in the system. These vulnerabilities can range from known software weaknesses to zero-day exploits, and they can lead to unauthorized access, data breaches, and even the compromise of the entire server. Moreover, open server ports can be susceptible to brute force attacks, DDoS attacks, and other malicious activities.	Redacted

Domains Failed

Control	Description	Remediation

RDP: 3389	RDP Port 3389 (Remote Desktop Protocol) uses port 3389 to facilitate remote access and control of a computer or server over a network connection. When a server port is accessible from the public internet, it becomes a potential entry point for malicious actors seeking to exploit vulnerabilities in the system. These vulnerabilities can range from known software weaknesses to zero-day exploits, and they can lead to unauthorized access, data breaches, and even the compromise of the entire server. Moreover, open server ports can be susceptible to brute force attacks, DDoS attacks, and other malicious activities.	Redacted

Domains Failed

Control	Description	Remediation

SSH: 22	SSH Port 22 refers to the use of the Secure Shell (SSH) protocol on port 22, which is a secure and encrypted method for remote access and communication with a computer or server. When a server port is accessible from the public internet, it becomes a potential entry point for malicious actors seeking to exploit vulnerabilities in the system. These vulnerabilities can range from known software weaknesses to zero-day exploits, and they can lead to unauthorized access, data breaches, and even the compromise of the entire server. Moreover, open server ports can be susceptible to brute force attacks, DDoS attacks, and other malicious activities.	Redacted

Domains Failed

Control	Description	Remediation
FTP: 21	FTP Port 21 (File Transfer Protocol) typically uses port 21 to establish connections for transferring files over a network. When a server port is accessible from the public internet, it becomes a potential entry point for malicious actors seeking to exploit vulnerabilities in the system. These vulnerabilities can range from known software weaknesses to zero-day exploits, and they can lead to unauthorized access, data breaches, and even the compromise of the entire server. Moreover, open server ports can be susceptible to brute force attacks, DDoS attacks, and other malicious activities.	Redacted

Domains Failed

Control	Description	Remediation

IP Camera: 8000	IP Camera 8000 services is a surveillance device that streams video and data over the internet using the specific network port 8000 for communication. When a server port is accessible from the public internet, it becomes a potential entry point for malicious actors seeking to exploit vulnerabilities in the system. These vulnerabilities can range from known software weaknesses to zero-day exploits, and they can lead to unauthorized access, data breaches, and even the compromise of the entire server. Moreover, open server ports can be susceptible to brute force attacks, DDoS attacks, and other malicious activities.	Redacted

Domains Failed

Control	Description	Remediation
IP Camera 7998	IP Camera 7998 services is a surveillance device that streams video and data over the internet using the specific network port 8000 for communication. When a server port is accessible from the public internet, it becomes a potential entry point for malicious actors seeking to exploit vulnerabilities in the system. These vulnerabilities can range from known software weaknesses to zero-day exploits, and they can lead to unauthorized access, data breaches, and even the compromise of the entire server. Moreover, open server ports can be susceptible to brute force attacks, DDoS attacks, and other malicious activities.	Redacted

Domains Failed

Control	Description	Remediation

Telnet: 23	Telnet Port 23 services is a network protocol allowing remote terminal access and communication with other devices over a network. When a server port is accessible from the public internet, it becomes a potential entry point for malicious actors seeking to exploit vulnerabilities in the system. These vulnerabilities can range from known software weaknesses to zero-day exploits, and they can lead to unauthorized access, data breaches, and even the compromise of the entire server. Moreover, open server ports can be susceptible to brute force attacks, DDoS attacks, and other malicious activities.	Redacted

Domains Failed

Control	Description	Remediation
IMAP: 143	IMAP Port 143 (Internet Message Access Protocol) on port 143 is a standard email protocol used for retrieving emails from a mail server, typically over a non-encrypted connection. When a server port is accessible from the public internet, it becomes a potential entry point for malicious actors seeking to exploit vulnerabilities in the system. These vulnerabilities can range from known software weaknesses to zero-day exploits, and they can lead to unauthorized access, data breaches, and even the compromise of the entire server. Moreover, open server ports can be susceptible to brute force attacks, DDoS attacks, and other malicious activities.	Redacted

Domains Failed

Control	Description	Remediation

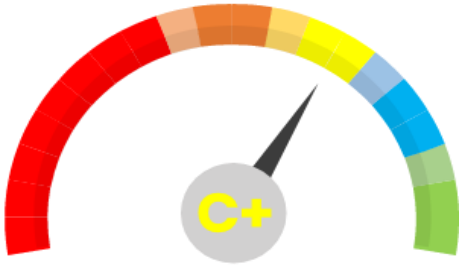
Network: 2000	Network Device Port 2000 services is a crucial component within the infrastructure, facilitating seamless communication and data transfer across the network. When a server port is accessible from the public internet, it becomes a potential entry point for malicious actors seeking to exploit vulnerabilities in the system. These vulnerabilities can range from known software weaknesses to zero-day exploits, and they can lead to unauthorized access, data breaches, and even the compromise of the entire server. Moreover, open server ports can be susceptible to brute force attacks, DDoS attacks, and other malicious activities.	Redacted

Domains Failed

Control	Description	Remediation
Pop3: 110	Pop3 Port 110 which stands for Post Office Protocol 3, is a commonly used email retrieval protocol that operates on port 110. When a server port is accessible from the public internet, it becomes a potential entry point for malicious actors seeking to exploit vulnerabilities in the system. These vulnerabilities can range from known software weaknesses to zero-day exploits, and they can lead to unauthorized access, data breaches, and even the compromise of the entire server. Moreover, open server ports can be susceptible to brute force attacks, DDoS attacks, and other malicious activities.	Redacted

Domains Failed

Compliance Risk Report



The results ranged between 62-72% of the assessment

Questionnaire Cyber Risk Survey

User Email - demotd1@hotmail.com

Audit Date - 12/08/2025

Tier - 1

Due Date - 12/08/2025

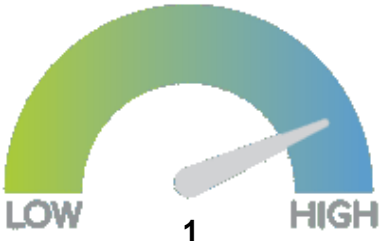
Compliance Control	Result	Recommendation	Response	Priority	Fix Date
Does the company have an up-to-date and recently (annually) tested technology disaster recovery plan?	Mostly	All company systems and data is registered against their criticality - and prioritization for recovery. There should be a record for recovery testing of data and systems conducted annually.		0	0000-00-00
Do you have an antivirus solution in place that is regularly updated with the latest virus and malware signatures?	Partially	An up-to-date antivirus solution is key to ensuring your systems are protected against the latest viruses.		0	0000-00-00
Do you have an Endpoint Detection and Response (EDR) solution on all company systems? e.g. MS Defender.	Mostly	EDR Endpoint Detection and Response solutions are the next generation of malware protection to be considered for this control.		0	0000-00-00
Are firewalls in place to protect all company systems and endpoints?	Mostly	A standard Microsoft OS firewall could be considered for all laptops. A Next Gen firewall with IDS/IPS could be considered as the main corporate firewall protecting cloud / on-premises servers.		0	0000-00-00

Does the company enforce a strong password policy for all systems and privileged accounts? for example, Administrative passwords should be at least 15 characters long and include both letters and numbers and change regularly.	Partially	A robust password policy is essential to defend against brute force attacks, password spraying, and guessing attempts, ensuring secure access to company systems.		0	0000-00-00
Is MFA (multifactor authentication) required for company system remote access, and all system access containing confidential company information?	Mostly	MFA via authentication token via mobile or email is desirable. As example, Google and Microsoft offer free authentication tools and the app code. Alternatively, paid tools like OKTA are good MFA options.		0	0000-00-00
Do you maintain a patch management strategy to ensure timely updates for all applications and operating systems?	Mostly	Automatic patch updates are recommended for OS systems and standard office applications. All other applications that support critical systems should be tested manually before any patch is deployed. Vulnerability scans should be conducted regularly (min. monthly) to ensure your system's security patches are up-to-date.		0	0000-00-00
Does the company have a Cyber Incident Response Process for Cyber Attacks?	Mostly	The incident response process should ensure all security events are researched thoroughly to isolate the incidentÂ and to remediate the control failure.		0	0000-00-00
Do the backups reside in a geographically separate location from the source data to ensure physical redundancy?	Partially	Ensuring your data is backed up in a separate physical location is key to resilience and recovery plans.		0	0000-00-00
Has the company experienced a system outage or ransomware caused by a supplier or partner in the past year? e.g. CrowdStrike Outages, Blue Yonder Ransomware, TCS M&S System Breach.	Partially	Third-party risks cause a significant number of cyber events - it's important to know the security posture of your supply chain and partners.		0	0000-00-00
Does the company back up critical data daily?	Mostly	Daily backup of critical data is key to ensuring resilience and recovery from cyber events, ransomware, and system failure.		0	0000-00-00

Financial Risk Quantification

Executive Summary

Company Exposure



Company Revenue	$10,000,000
Control Failure	-33%
Attack Surface	68%
Compliance	66%
Likelihood of Breach	1

Data Breach

Single Loss	$3,660,000
Insurance	$36,600
PII Records	10,000
Health Records	5,000
Credit Cards	5,000

Data Privacy Notification: Emails, PR, Regulator fees	$256,200
Data Privacy Response: Helpdesk, Credit Monitoring, Legal	$988,200
Data Privacy Audit: Forensics, Auditors, Engineers, Crisis	$1,207,800
Data Privacy Recovery: Customer Incentives, System	$1,171,200

System Breach

Single Loss	$275,000
Insurance	$2,750
Non Systems	5
Revenue Loss Per Day	$5,000
Recovery Per Days	10

Ransomware

Single Loss	$280,000
Insurance	$2,800