



Company

Cybersecurity Risk Report

Enterprise

Report Generated: 15/08/2023

Executive Summary

This executive summary provides an overview of the cybersecurity risk report, highlighting key findings and ratings across various risk management categories. The report focuses on assessing the organization's cybersecurity posture, identifying vulnerabilities and threats, and providing recommendations for mitigating risks. The following sections present ratings for Attack Surface Management (ASM), Compliance Risk Management (CRM), Third-Party Risk Management (TPRM), Financial Impact Management (FIM), Bad Network IPs, and Threat Intelligence.

1. **Attack Surface Management Rating (ASM):** The ASM rating evaluates the organization's ability to manage and reduce its attack surface. The assessment considers factors such as network infrastructure, software vulnerabilities, and configuration management. Based on the analysis, the organization has achieved a commendable ASM rating, indicating effective controls and measures in place to minimize potential attack vectors.
2. **Compliance Risk Management Rating (CRM):** The CRM rating reflects the organization's adherence to regulatory requirements and industry standards. It encompasses 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.
3. **Third-Party Risk Management Rating (TPRM):** The TPRM rating assesses the organization's ability to identify and manage risks associated with third-party vendors, suppliers, and partners. It evaluates the effectiveness of security controls and governance practices in mitigating potential vulnerabilities introduced through third-party relationships. The analysis shows that the organization has implemented robust TPRM processes, resulting in a positive rating.

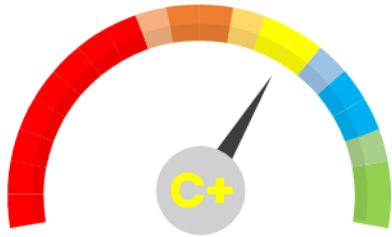
4. Financial Impact Management (FIM): The FIM rating focuses on the organization's preparedness to handle financial losses in the event of a cybersecurity incident. It considers factors such as insurance coverage, incident response plans, and business continuity strategies. The evaluation indicates that the organization has taken significant steps to manage financial impact, resulting in a favorable FIM rating.

5. Threat Intelligence: Threat intelligence 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.

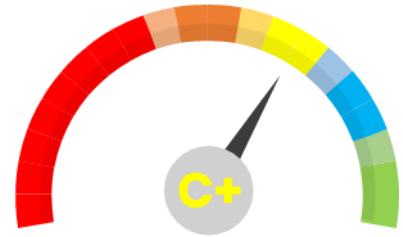
In conclusion, the organization has demonstrated a strong commitment to cybersecurity risk management, as evidenced by the positive ratings across ASM, CRM, TPRM, and FIM.

Company Result

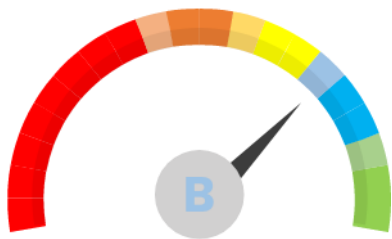
Company Attack Surface Rating



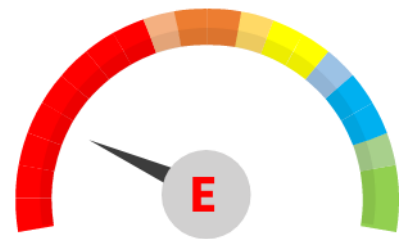
Company Compliance Rating



Third-Party Average Attack Surface Rating



Third-Party Average Compliance Rating






Company Domains





ACME Bank Sub1	Domain Rating	Last Scan
Domain Hidden	B	21/07/2023
Domain Hidden	B	21/07/2023
Domain Hidden	D+	24/07/2023




ACME Bank Sub2	Domain Rating	Last Scan
Domain Hidden	B+	21/07/2023
Domain Hidden	B+	23/07/2023
Domain Hidden	C+	23/07/2023
Domain Hidden	C+	21/07/2023






ACME Bank1	Domain Rating	Last Scan
Domain Hidden	B	21/07/2023
Domain Hidden	B	23/07/2023

Domain Hidden		21/07/2023
Domain Hidden		21/07/2023
Domain Hidden		24/07/2023
Domain Hidden		23/07/2023

ACME Bank Sub1	Domain Rating	Last Scan
Domain Hidden		21/07/2023
Domain Hidden		21/07/2023
Domain Hidden		24/07/2023

ACME Bank Sub2	Domain Rating	Last Scan
Domain Hidden		21/07/2023
Domain Hidden		23/07/2023
Domain Hidden		23/07/2023
Domain Hidden		21/07/2023

Demo1	Domain Rating	Last Scan
Domain Hidden		23/04/2023
Domain Hidden		23/04/2023
Domain Hidden		09/05/2023







Demobv3	Domain Rating	Last Scan
Domain Hidden		20/07/2023
Domain Hidden		20/07/2023
Domain Hidden		20/07/2023
Domain Hidden		20/07/2023
Domain Hidden		20/07/2023



Attack Surface Management (ASM)




Domains By Attack Surface Rating

Leader	1
Advanced	0
Excellent	5
Good	5
Average	6
Low	1
Poor	3
V. Poor	0
Critical	0

Email Security	
Webpage Security	
System Compromised	
Vulnerabilities	
Data Privacy	
Network Ports	

Bad Network IP

No bad IP found.

Icon	Vulnerability	Domain Failed	Total Vuln
	Multiple Critical Risk Vulnerabilities	2	50
	Multiple High Risk Vulnerabilities	5	373
	Multiple Medium Risk Vulnerabilities	7	995

Email Security

Probe Name	Domain Failed
Email Spoof	3
Email SPF Treatment	3
DMARC Authentication	10
DMARC Treatment	20
Open Relay Security	0
Email Encryption-STARTTLS	0

Webpage Security

Probe Name	Domain Failed
HTTPS only	19
Clickjack Protection	18
Malicious XSS Code Injection	20
MIME X-Content type	17
Content Security Policy	20
Referrer Policy	20
Server Cache-Control	12
Cross Domain permission	21
Except-CT TLS	21
Server-Service Version	2
Hide X Powered Services	4

System Compromised

Probe Name	Domain Failed
Open Proxy Services	1
Malware Hosting	1
Bot site	1
Spam Host	0

Vulnerabilities

Probe Name	Domain Failed
Multiple Critical Risk Vulnerabilities	2
Multiple High Risk Vulnerabilities	5
Multiple Medium Risk Vulnerabilities	7
SSL Cert Heartbleed Vulnerability	4

TLS CCS Injection Vulnerability	4
SSL Ticketbleed Vulnerability	4
SSL Renegotiation Vulnerability	10
TLS Fallback Vul	7

Data Privacy

Probe Name	Domain Failed
SSL Cert Date Valid	4
SSL Cert Cipher Suite	11
SSL Cert Weak	4
Cookie Sucure Flag	16
Cookie Samesite	20
Cookie HttpFlag Protection	18
Cookie Notification	19
Privacy Notification	19
Cookie Consent	0

Network Ports

Probe Name	Domain Failed
SMB Services 139	1
Mongo dbase open 27017	1
Microsoft dbase open 1433	1
MySQL 3306	2
PostgreSQL Db open 5432	1
RDP Access 3389	1
SSH Access 22	4
FTP Open 21	2
IP Camera 8000	1
IP Camera 7998	1
Telnet 23	1
IMAP email 143	1
Network devices 2000	2
Pop3 server 110	1



Financial Impact Management



Annual Revenue US \$

Personal Records

\$1,107,000,000

212,722

Estimated Insurance Cost

\$15,954

Industry Dependency

Ransomware Cost

Business Interruption Cost

Medium

\$30,996,000

\$21,230,137

High

\$55,350,000

\$30,328,767

Low

\$11,070,000

\$15,164,384

Data Breach Breakdown

Data Breach Cost

Data Breach Cost

\$10,636,100

Notification-Email, Calls, PR agency letters, Regulators Commas

\$744,527

Post Breach Response Helpdesk Credit, Monitor legal costs

\$2,871,747

Detaction & Escalation-Forensic, Audit, Crisis, Mgmt Teams

\$3,509,913

Lost Business Cost-Loss of Revenue, Loss of Clients, Rebuild Reputa




\$3,403,552



Analyst Commentary






Analyst Commentary

Icon	Company Name	Comment
	Demobv3	<p>JULY 2003 EXECUTIVE SUMMARY</p> <p>The overall digital footprint for the company is very small and the security for domains is mostly managed by Cloudflare. There are some issues that need to be reviewed for the attack surface security, as per the systems report.</p> <p>No further risks found in data leaks for this month.</p>
	ACME Bank1	<p>JULY 2023 EXECUTIVE SUMMARY</p> <p>THE ATTACK SURFACE MGT RESULTS</p> <ol style="list-style-type: none">1. [C+] Attack Surface Cyber Rating2. [13] Domains and Subdomains active3. [2000] Checkpoint failures <p>VULNERABILITY VALIDATION [1500+] Critical/High/Med confirmed on [7] servers</p> <p>COMPROMISED SERVERS [3] servers identified as compromised</p> <p>EMAIL CREDENTIAL LEAK [7] email credential leaks found</p> <p>DATA DISCOVERY Search Term 'Acme'</p> <p>[200] Github Code Repository found. refer links below [25] Pastebin data found. refer to links below</p>
	Demo1	<p>JULY 2023 EXECUTIVE SUMMARY</p> <p>No major issues to report this month.</p>





Data Discovery

Icon	Company Name	Comment
	Demobv3	<p>JULY 2023 DATA LEAKS</p> <p>No data leaks were discovered this month for the company</p>
	ACME Bank1	<p>JULY 2023 DATA LEAKS</p> <p>Search Terms 'Acme'</p> <p>[2] Deepweb leaks (links redacted) [5].Google shares leaks (links redacted) [200] Github repositories leaks (links redacted) [12] Paste sites leaks (links redacted)</p> <p>[55] EMAIL CREDENTIAL LEAKS</p> <p>sample below</p> <p>Email - john@acme.com Source(s) - Twitter.com (scraping data) Date of Breach - Jan 2022 Email - lee@acme.com Source(s) - Twitter.com (scraping data) Date of Breach - Jan 2022 Email - sue@acme.com Source(s) - Twitter.com (scraping data) Date of Breach - Jan 2022 Email - alf@acme.com Source(s) - Twitter.com (scraping data) Date of Breach - Jan 2022 More links sent to company contact</p>
	Demo1	<p>JULY 2023 DATA LEAKS</p> <p>No Data leaks discovered this month.</p>



Adversary Threat

Icon	Company Name	Comment
	Demobv3	<p data-bbox="555 210 975 241">JULY 2023 ADVSEARY THREATS</p> <p data-bbox="555 286 1453 353">We believe the enigmatic group is targeting your industry. Our advisory is to review their TTP and counter with security controls.</p> <p data-bbox="555 398 1517 801">The enigmatic group known as "ShadowNet" has emerged as a formidable adversary within the realm of American cybersecurity. Operating with a combination of sophisticated techniques and a cloak-and-dagger ethos, ShadowNet has left a trail of digital disruption and uncertainty in its wake. With a reputation for targeting high-profile institutions, ranging from government agencies to critical infrastructure, their motivations remain shrouded in mystery. Experts believe that ShadowNet employs a potent blend of cutting-edge malware, social engineering tactics, and a deep understanding of system vulnerabilities, allowing them to breach even the most fortified networks. As authorities scramble to decipher the group's origins and objectives, the ongoing game of cat and mouse between ShadowNet and American cybersecurity forces has e</p>
	ACME Bank1	<p data-bbox="555 1055 1010 1086">JULY - 2023 ADVERSARY THREATS</p> <p data-bbox="555 1131 1453 1198">We believe the enigmatic group is targeting your industry. Our advisory is to review their TTP and counter with security controls.</p> <p data-bbox="555 1243 1517 1646">The enigmatic group known as "ShadowNet" has emerged as a formidable adversary within the realm of American cybersecurity. Operating with a combination of sophisticated techniques and a cloak-and-dagger ethos, ShadowNet has left a trail of digital disruption and uncertainty in its wake. With a reputation for targeting high-profile institutions, ranging from government agencies to critical infrastructure, their motivations remain shrouded in mystery. Experts believe that ShadowNet employs a potent blend of cutting-edge malware, social engineering tactics, and a deep understanding of system vulnerabilities, allowing them to breach even the most fortified networks. As authorities scramble to decipher the group's origins and objectives, the ongoing game of cat and mouse between ShadowNet and American cybersecurity forces</p>





Demo1

JULY 2023 ADVERSARY THREATS

We believe the enigmatic group is targeting your industry. Our advisory is to review their TTP and counter with security controls.

The enigmatic group known as "ShadowNet" has emerged as a formidable adversary within the realm of American cybersecurity. Operating with a combination of sophisticated techniques and a cloak-and-dagger ethos, ShadowNet has left a trail of digital disruption and uncertainty in its wake. With a reputation for targeting high-profile institutions, ranging from government agencies to critical infrastructure, their motivations remain shrouded in mystery. Experts believe that ShadowNet employs a potent blend of cutting-edge malware, social engineering tactics, and a deep understanding of system vulnerabilities, allowing them to breach even the most fortified networks. As authorities scramble to decipher the group's origins and objectives, the ongoing game of cat and mouse between ShadowNet and American cybersecurity forces has

