CEO's Guide to Cybersecurity in 2024

A Free Resource for Business Owners

Are you protected against the growing threat of cyber attacks on businesses like yours? How do you know?

Maybe you are in the difficult position of being *told* that your IT provider is taking all the necessary precautions to protect you, but they provide no proof of those protections. No reports, no checkups, no transparency.

Perhaps you don't have a dedicated IT provider or IT plan yet. If this is the case, you may be spending thousands of dollars every month for break/fix services, waiting hours or days for service, and are still left unprotected against cyber crime.

In these situations, you have two options available to you. The first: continue as you are, and HOPE that you emerge from 2024 as one of the *extremely* lucky businesses that don't experience a cyber attack or breach. The second: bring in an expert to perform a *full* assessment of your cybersecurity posture and provide you a roadmap to cyber resilience.

Some security assessments only provide you with a snapshot of your business's cybersecurity. We go further and show you where you're at right now as well as where you can be with a roadmap and a plan to strengthen your defenses.

Look through the following pages to learn about current cybersecurity statistics and how you can protect yourself. If you need a new IT and cybersecurity partner now or at any point in the future, we hope you will consider Facet.

Dedicated to your success,

Brian Ford

Brian Ford
President of Facet Technologies, Inc.

A GROWING THREAT

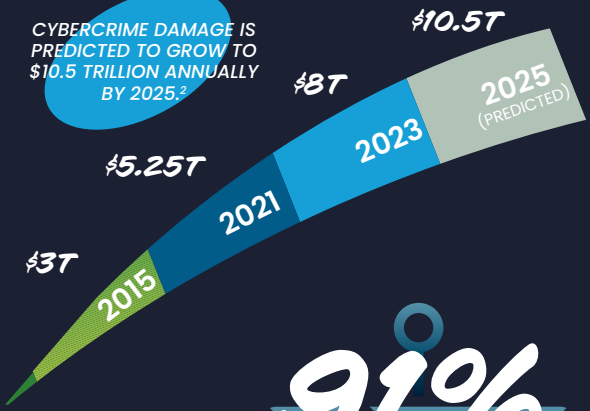
$4.45M

is the average cost of a data breach in 2023, an increase of

15%

year over year since 2020.[1]

CYBERCRIME DAMAGE IS PREDICTED TO GROW TO $10.5 TRILLION ANNUALLY BY 2025.[2]



92% *of companies have passwords for sale on the dark web.*[3]

60% *of companies that experience a cyber attack close their doors within 6 months.*[4]

91%

of cyber attacks begin with a ***phishing email.***[5]

YOUR RESPONSE TO CYBERCRIME MATTERS MORE THAN EVER

GOING RATES OF INFORMATION ON DARK WEB MARKETPLACES[8]

CREDIT CARD NUMBER (MORE IF CVV IS INCLUDED)	$6
SOCIAL SECURITY NUMBER	$25
ONLINE BANKING CREDENTIALS (WITH A BALANCE OF $2,000+)	$35
FACEBOOK ACCOUNT	$45
MICROSOFT OUTLOOK ACCOUNT	$55
FULL DATA SET (ENOUGH FOR IDENTITY THEFT)	$1K

14s

A company falls victim to cyberattack every 14 seconds in the U.S.[6]

82%

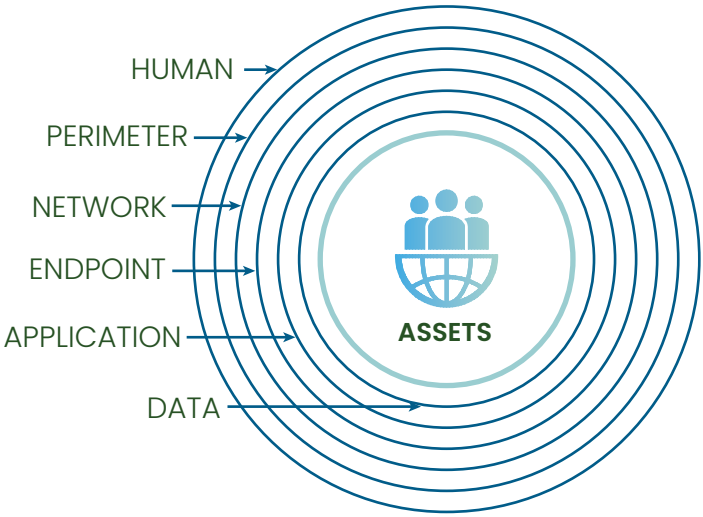
of ransomware attacks target businesses with under 1,000 employees.[7]

[1] IBM, "COST OF A DATA BREACH REPORT 2023." [2] CYBERSECURITY VENTURES, "2023 CYBERSECURITY ALMANAC." [3] DARK READING, "DARK READING ACCOUNT TAKEOVER 2022" [4] NATIONAL CYBERSECU RITY ALLIANCE, "REPORTING CYBERCRIME." [5] KNOWBE4, "CYBER ATTACK TECHNIQUES." [6] UNIVERSITY OF MARYLAND, ASTRA SECURITY [7] FORTINET, "2022 CYBERSECURITY CHALLENGES." [8] EXPRESSVPN, "HOW MUCH IS YOUR DATA WORTH ON THE DARK WEB?"

HOW WE PROTECT YOUR DATA

We work to stop hackers at every stage to secure critical assets. One way we approach this is by envisioning the "layers" standing between attackers and your assets.

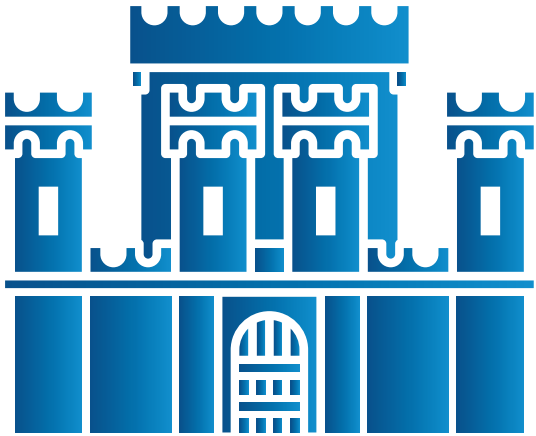
7-LAYER
SECURITY FRAMEWORK



LAYERED SECURITY: THE CASTLE

Defense in depth is an age-old concept. Think of a fortress with moats, drawbridges, guard towers, secret passageways, and sentries posted throughout.

Nothing can prevent bad actors from attempting to breach the "gates" of your company's digital defense, but a multi-layered approach can keep them at bay.



HUMAN ELEMENT: TRAINING AND AWARENESS

Most cyber attacks occur due to human error. Cyber criminals use social engineering tactics to gain access to your network via phishing and other attacks on your employees. Studies show that **security awareness training** is the most effective way to combat these vulnerabilities in your organization.

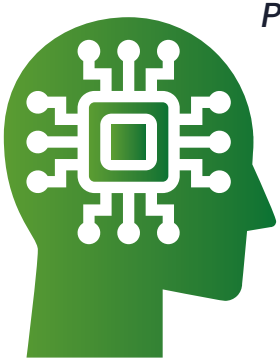
- **Phishing Simulations**
- **Reporting**
- **Employee Training and Resources**

Our library of videos, quizzes, and other resources for employee security awareness is available to all Security Suite clients.

98% *of cyber attacks rely on social engineering.*

ARTIFICIAL INTELLIGENCE
AND THE FUTURE OF CYBERSECURITY

A.I HAS BEEN PROVEN TO CRAFT MORE CONVINCING PHISHING EMAILS THAN HUMANS ALONE.



How? Hackers use A.I. to scan the web for information about your employees and craft a more effective email. Examples include job titles, spouses' names, years at the company, and recent promotions.

Through an automated process, an email is generated with personalized details that make phishing scams harder to spot.

THE GOOD NEWS? *Even as cybercrime advances by harnessing A.I., our defenses advance using the same technology for good. Modern security essentials include A.I.-driven and assisted software to identify patterns of behavior to prevent breaches.*

THE UPSHOT: AS HACKERS ADVANCE, SO DO SECURITY EXPERTS

PERIMETER: BUSINESS-GRADE SECURITY APPLIANCE

More than just basic security, a **next-generation firewall** provides essential services all from a single appliance. Businesses benefit from protection that integrates with threat intelligence services and analyzes traffic comprehensively to stop malware before it enters your network.

- Web Filtering
- Intrusion Prevention System
- Application Control
- Antimalware
- Data Loss Prevention
- Security Analytics
- Internet Load Balancing & Failover
- Secure Remote VPN Capabilities

CHANGES IN COMPLIANCE

REGULATIONS, INSURANCE, AND MORE

Looking at cyber liability insurance as an extra safeguard against ransomware losses?
More companies than ever are being denied cyber liability coverage due to an incomplete security stack.

We developed the Facet Security Suite to provide best-in-class protections that ensure our clients meet compliance regulations in their industries and the requirements of insurance policies.

100%

OF FACET SECURITY SUITE CLIENTS' CYBER LIABILITY INSURANCE APPLICATIONS HAVE BEEN APPROVED

AS OF OCTOBER 2023

NETWORK: MULTI-FACTOR AUTHENTICATION

MFA should be enabled wherever possible, including:

Email Accounts • Server Access • Remote Connections • Administrative Access

Malicious actors often get around passwords and other "baseline" security measures. One way we prevent these compromises is through **multi-factor authentication**. One quick tap on your mobile device adds a layer of protection even when passwords fail.

MFA BLOCKS UP TO 99% OF AUTOMATED ATTACKS.

ENDPOINT: ENDPOINT DETECTION AND RESPONSE

Endpoint, cloud and identity threat protection enhanced with A.I.: your business is better protected with detection and investigation beyond known malware.

AV (ANTIVIRUS)	EDR (ENDPOINT DETECTION AND RESPONSE)
Works to prevent only identified threats;	Prevents known and unknown threats using pattern detection;
Relies on exact "signatures" to find issues;	Goes the "extra mile" to contain threats;
High resource usage;	Returns endpoints to pre-infected state; and
Not proven to be effective endpoint protection for 2024.	Provides data on threats and network.

A CHANGING INDUSTRY: STILL USING AN ANTIVIRUS? IT'S TIME TO SWITCH TO EDR.

APPLICATION: DEDICATED EMAIL SECURITY

Dedicated third-party email security filters inbound and outbound email to reduce spam, block malicious links and attachments, and identify imposter emails.

As cyber criminals' tactics become more sophisticated with A.I. and other tools, preventing these emails from reaching the end-user's inbox is critical.

- Spam Filtering
- Phishing Defense
- Imposter Prevention
- Content Filtering
- Outbound Filtering
- URL Defense
- Attachment Defense
- Email Encryption
- Reporting

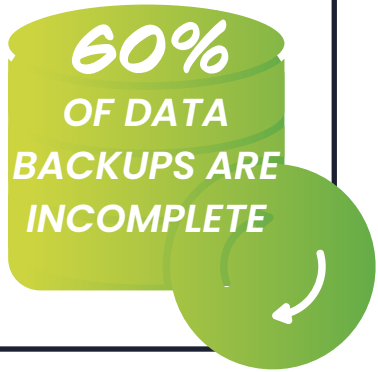
5 STEPS TO BUSINESS CONTINUITY

1. EVALUATE RISK
2. IDENTIFY CRITICAL ASSETS
3. BACK UP DATA
4. TEST PLAN
5. OPTIMIZE PLAN

DATA: EFFECTIVE BACKUP STRATEGY

Data Backups: the final layer protecting your assets. Most compliance standards require backups be automated, encrypted, and stored in an offsite location.

Cyber attack and user error can result in the need to deploy a disaster recovery plan. Isolated backups and instant recovery can save your company in an emergency.



FACET TECHNOLOGIES, INC.

TRUE TECH PEACE OF MIND

is our commitment to you.

THE BIG PICTURE
Straightforward assessment of your cybersecurity situation

STRATEGY
We learn your business and industry-specific needs, plus compliance requirements.

CREATION
We present your roadmap tailored to meet your needs.

PEACE OF MIND
Our expert team works to continually protect your business and livelihood.

READY TO FIND YOUR TRUE TECH PEACE OF MIND?

Request Your Custom Cyber Resilience Roadmap Today

FACET

FACETTECH.COM
(309) 689-3900
INFO@FACETTECH.COM

WHAT CAN FACET DO FOR MY BUSINESS?

MANAGED SERVICES AND IT SUPPORT

In-House Helpdesk
Provoptix, Facet's Monitoring System
Staffed Repair Bench
Cloud Servers/Virtual Desktops
Backups/Instant Recovery/Backup Isolation
Work-From-Home Security
24/7/365 Support Line
Network Upgrades/Refreshes
Hardware Sales
Domain and Email Hosting

CYBERSECURITY & THE FACET SECURITY SUITE

A.I.-Assisted Autonomous Endpoint Protection
Managed Firewall – Next-Gen Security Appliances
Employee Training/Phishing Simulations
24/7 SOC (Security Operations Center)
Managed Detection and Response
Dark Web Monitoring
Compromised Credentials Reporting
Office 365 Backups
Email Security and Spam Filter
Multi-Factor Authentication
Third-Party Audits
Zero Trust
Admin Password Rotation

INTERESTED IN ANY OF THE ABOVE SERVICES OR NEED A CUSTOM SOLUTION?

facettech.com | info@facettech.com | (309) 689-3900
Facet Technologies, Inc.: 3024 W. Lake Ave., Peoria, IL 61615