



FTC Safeguards Rule

IT Provider Selection

Cyber Liability Insurance



\$1.5
MILLION

**AVG RANSOMWARE PAYOUT IN
2023**

\$4.35
MILLION

**GLOBAL AVG COST OF A DATA
BREACH IN 2023**

Source: <https://www.cobalt.io/blog/cybersecurity-statistics-2024>

\$9.5
TRILLION

**COST OF CYBERCRIME IN
2024**

\$13.8 TRILLION BY 2028


THE ULTIMATE GUARDIAN: YOU - THE HUMAN FIREWALL

First Line of Defense


Security-Conscious Culture

Continuous Training





What is the FTC Safeguards Rule?



FTC Safeguards Rule – June 2023

Objective: protect the security,
confidentiality, and integrity of
customer information.



November 12, 1999

Congress passed the Gramm-Leach-Bliley Act (GBLA)

- Meant to modernize financial industry
- FTC responsible for implementation
- Went into effect May 23rd, 2003



The technology landscape is
radically different from 2000's.



**In December 2021, the FTC
Safeguards Rule was revised.**

Dramatic Change in Scope – “Financial Institutions”

Original 2002 Verbiage:

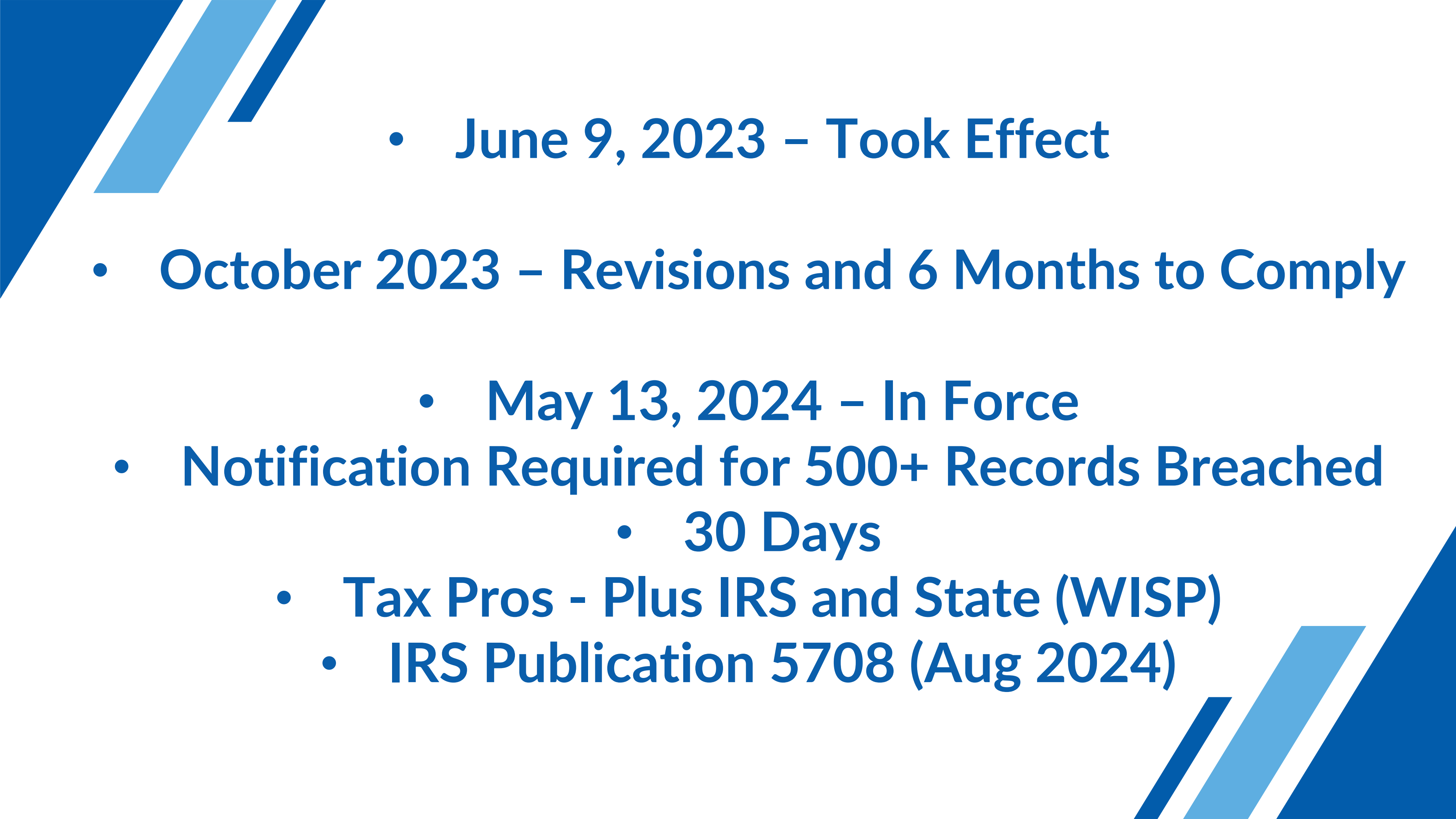
Scope. This part applies to the handling of customer information by all financial institutions over which the Federal Trade Commission (“FTC” or “Commission”) has jurisdiction. This part refers to such entities as “you.” This part applies to all customer information in your possession, regardless of whether such information pertains to individuals with whom you have a customer relationship, or pertains to the customers of other financial institutions that have provided such information to you.

After Dec 2021 revision:

Scope. This part applies to the handling of customer information by all financial institutions over which the Federal Trade Commission (“FTC” or “Commission”) has jurisdiction. Namely, this part applies to those “financial institutions” over which the Commission has rulemaking authority pursuant to section 501(b) of the Gramm-Leach-Bliley Act. An entity is a “financial institution” if its business is engaging in an activity that is financial in nature or incidental to such financial activities as described in section 4(k) of the Bank Holding Company Act of 1956, 12 U.S.C. 1843(k), which incorporates activities enumerated by the Federal Reserve Board in 12 CFR 225.28 and 225.86. The “financial institutions” subject to the Commission's enforcement authority are those that are not otherwise subject to the enforcement authority of another regulator under section 505 of the Gramm-Leach-Bliley Act, 15 U.S.C. 6805. **More specifically, those entities include, but are not limited to, mortgage lenders, “pay day” lenders, finance companies, mortgage brokers, account servicers, check cashers, wire transferors, travel agencies operated in connection with financial services, collection agencies, credit counselors and other financial advisors, tax preparation firms, non-federally insured credit unions, investment advisors that are not required to register with the Securities and Exchange Commission, and entities acting as finders.** They are referred to in this part as “You.” This part applies to all customer information in your possession, regardless of whether such information pertains to individuals with whom you have a customer relationship, or pertains to the customers of other financial institutions that have provided such information to you.

Section 314.2(h) of the Rule

(h) (1) ***Financial institution*** means any institution the business of which is engaging in an activity that is financial in nature or incidental to such financial activities as described in section 4(k) of the Bank Holding Company Act of 1956, [12 U.S.C. 1843\(k\)](#). An institution that is significantly engaged in financial activities, or significantly engaged in activities incidental to such financial activities, is a financial institution.

- 
- June 9, 2023 – Took Effect
 - October 2023 – Revisions and 6 Months to Comply
 - May 13, 2024 – In Force
 - Notification Required for 500+ Records Breached
 - 30 Days
 - Tax Pros - Plus IRS and State (WISP)
 - IRS Publication 5708 (Aug 2024)



Also created punitive
consequences for failing to
adhere to these parameters.

Civil penalties can help the FTC deter conduct that harms consumers.

- Up to **\$100,000 per violation** for Institutions
- Up to **\$10,000 per person** for Board Members, CEO and Owners.
- **Loss of business license**
- **5-year prison sentence**



Examples of Covered Entities

- Mortgage lenders
- Pay day lenders
- Finance companies
- Mortgage brokers
- Account servicers
- Check cashers
- Wire transferers
- Some travel agencies
- Real estate appraisers
- Credit counselors
- Automotive dealerships
- Tax preparation firms
- Non-federally insured credit unions
- Some investment advisors

Examples of Exemptions

(4) Examples of entities that are not significantly engaged in financial activities are as follows:

(i) A retailer is not a financial institution if its only means of extending credit are occasional “lay away” and deferred payment plans or accepting payment by means of credit cards issued by others.

(ii) A retailer is not a financial institution merely because it accepts payment in the form of cash, checks, or credit cards that it did not issue.

(iii) A merchant is not a financial institution merely because it allows an individual to “run a tab.”

(iv) A grocery store is not a financial institution merely because it allows individuals to whom it sells groceries to cash a check, or write a check for a higher amount than the grocery purchase and obtain cash in return.

Safeguards Rule Requirements



Covered Entities are required to:

1. Designate a Qualified Individual
2. Document Risk Assessments
3. Apply Controls
4. Validate Controls
5. Develop Training and Auditing Program
6. Monitor Service Providers
7. Develop Continuous Improvement Cadence
8. Document Incident Response Plan
9. Provide Annual Reporting to Senior Leadership

1. Designate a Qualified Individual to implement and supervise your company's information security program.

- In charge of overseeing/implementing
- Can be employee, affiliate, or service provider of the client
- Client retains responsibility if delegated outside of their organization



2. *Conduct a Risk Assessment.*



- Must be a written assessment
- Must include criteria for evaluating risks and assessment of systems and customer information (PII)
- Requires periodic refresh
- Identifies all assets

Sample Risk Assessment

NIST Risk Assessment Template: Adversarial

Refer to the guidance before completing this sheet.

Entity Being Assessed ABC Company

Tie

Assessment Date

Assessor

[illegible]

Source: <https://www.securityscientist.net/>

Sample Risk Assessment

NIST Risk Assessment Template: non-Adversarial

Refer to the guidance before completing this sheet.

Entity Being Assessed	ABC Company
Tier	0
Assessment Date	00 January 1900
Assessor	0

[illegible]

Source: <https://www.securityscientist.net/>

Sample Risk Assessment

NIST SP 800-30 Risk Assessment Report

Entity Being Assessed ABC Company
Tier 0
Assessment Date 00 January 1900
Assessor 0

Threat	Very High					
	High					
	Moderate			Unauthorized Access to Sensitive Data	Phishing Attacks Data Theft by Employee	Spear Phishing Attacks
	Low			Deliver modified malware to internal organizational information systems.	Fire at Primary Facility	
	Very Low				Flood at Primary Facility	
		Very Low	Low	Moderate	High	Very High
Impact						

Adversarial Threat List

Phishing Attacks
Spear Phishing Attacks
Deliver modified malware to internal organizational information systems.
Data Theft by Employee

Non-Adversarial Threat List

Unauthorized Access to Sensitive Data
Fire at Primary Facility
Flood at Primary Facility

3. Design and implement safeguards to control the risks identified through your risk assessment.

1. Implement and periodically review access controls. Determine who has access to customer information and reconsider on a regular basis whether they still have a legitimate business need for it.





3. Design and implement safeguards to control the risks identified through your risk assessment.

2. Know what you have and where you have it.

A fundamental step to effective security is understanding your company's information ecosystem. Conduct a periodic inventory of data, noting where it's collected, stored, or transmitted. Keep an accurate list of all systems, devices, platforms, and personnel. Design your safeguards to respond with resilience.

3. Design and implement safeguards to control the risks identified through your risk assessment.

3. Encrypt customer information on your system and when it's in transit. If it's not feasible to use [encryption](#), secure it by using effective alternative controls approved by the Qualified Individual who supervises your information security program.



3. Design and implement safeguards to control the risks identified through your risk assessment.

4. Assess your apps. If your company develops its own apps to store, access, or transmit customer information – or if you use third-party apps for those purposes – implement procedures for evaluating their security.

3. Design and implement safeguards to control the risks identified through your risk assessment.

5. Implement multi-factor authentication for anyone accessing customer information on your system. For [multi-factor authentication](#), the Rule requires **at least two** of these authentication factors: a knowledge factor (for example, a password); a possession factor (for example, a token), and an inherence factor (for example, biometric characteristics). The only exception would be if your Qualified Individual has approved in writing the use of another equivalent form of secure access controls.

Know. Have. Are.

3. Design and implement safeguards to control the risks identified through your risk assessment.

6. Dispose of customer information securely. Securely dispose of customer information no later than two years after your most recent use of it to serve the customer. The only exceptions: if you have a legitimate business need or legal requirement to hold on to it or if targeted disposal isn't feasible because of the way the information is maintained.

3. Design and implement safeguards to control the risks identified through your risk assessment.

7. Anticipate and evaluate changes to your information system or network. Changes to an [information system](#) or network can undermine existing security measures. For example, if your company adds a new server, has that created a new security risk? Because your systems and networks change to accommodate new business processes, your safeguards can't be static. The Safeguards Rule requires financial institutions to build change management into their information security program.

3. Design and implement safeguards to control the risks identified through your risk assessment.

8. Maintain a log of authorized users' activity and keep an eye out for unauthorized access. Implement procedures and controls to monitor when [authorized users](#) are accessing customer information on your system and to detect unauthorized access.

4. Regularly monitor and test the effectiveness of your safeguards.



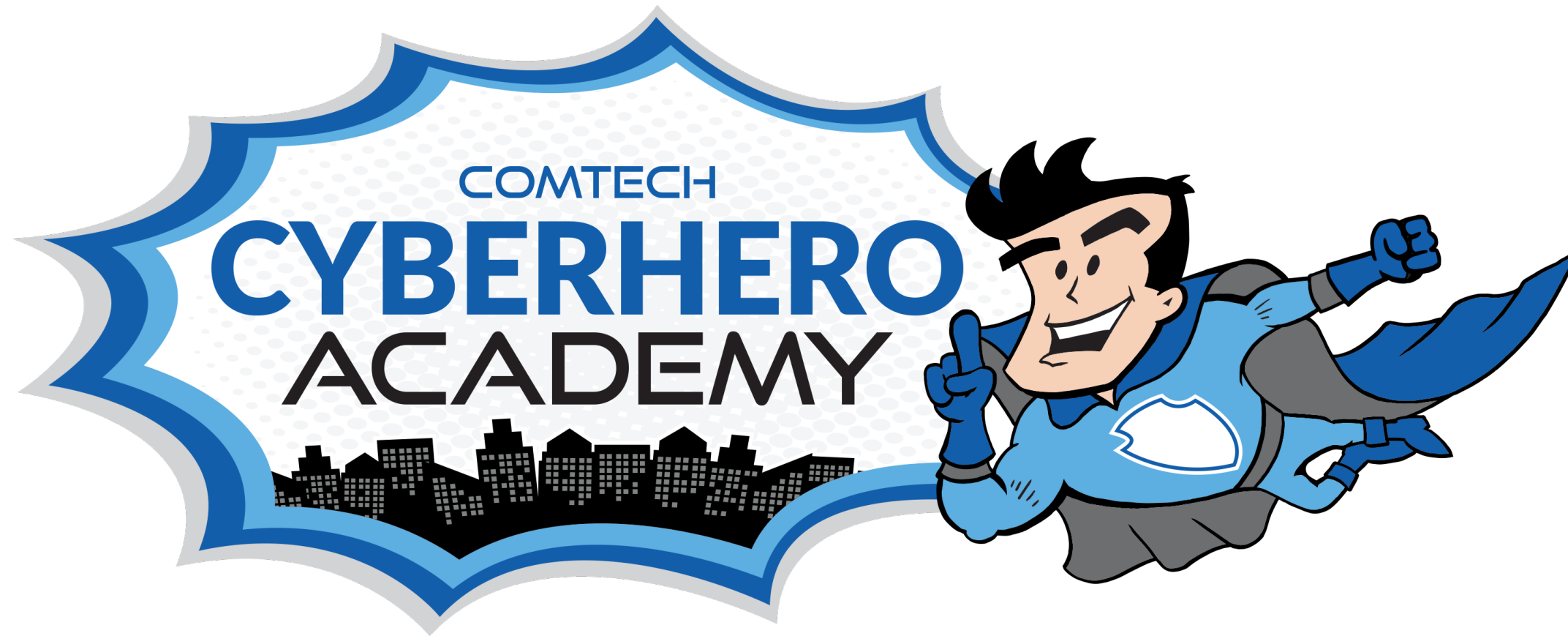
- Regularly test and monitor controls' effectiveness – ex: test backups, restoring
- Information systems require continuous monitoring – vulnerability scans
- Annual penetration tests

5. *Train your staff*

- Implement security awareness training explaining risk assessment findings
- Maintain sufficient staffing to run the security program
- Verify that security personnel are staying current on security threats



Training Programs



PII Protect

6. Monitor Your Service Providers



- Engage service providers that can maintain appropriate safeguards
- Make sure service provider contracts include safeguard implementation
- Periodically assess service providers

7. Keep your information security program current

Evaluate information security program based on:

- Testing
- Material changes in your organization
- The results of a risk assessment



8. Create a written incident response plan



Your “What if?”
Response and Recovery Plan

Incident Response Plan Goals



- Clear roles, responsibilities and levels of decision-making authority
- Communications and information sharing both inside and outside your company
- A process to fix any identified weaknesses in your systems and controls
- Procedures for documenting and reporting security events and your company's response
- A post mortem of what happened and a revision of your incident response plan and information security program based on what you learned

9. Require your Qualified Individual to report to your Board of Directors.

- Designated Qualified Individual must provide annual report to leadership body
- Include overall status of security program and compliance
- Must also have material matters related to the information security program (assessments, incident reports, improvement recommendations, etc.)

314.6 Exceptions

- Section 314.4(b)(1), (d)(2), (h), and (i) do not apply to financial institutions that maintain customer information concerning **fewer than five thousand consumers**.
- 314.4 (b)(1) requiring a **written** risk assessment
- 314.4 (d)(2) requiring **continuous** monitoring, annual penetration testing and bi-annual vulnerability assessment
- 314.4 (h) requiring a **written** incident response plan
- 314.4 (i) requiring an annual **written** report by Qualified individual to the board of directors

Takeaways – FTC Safeguards

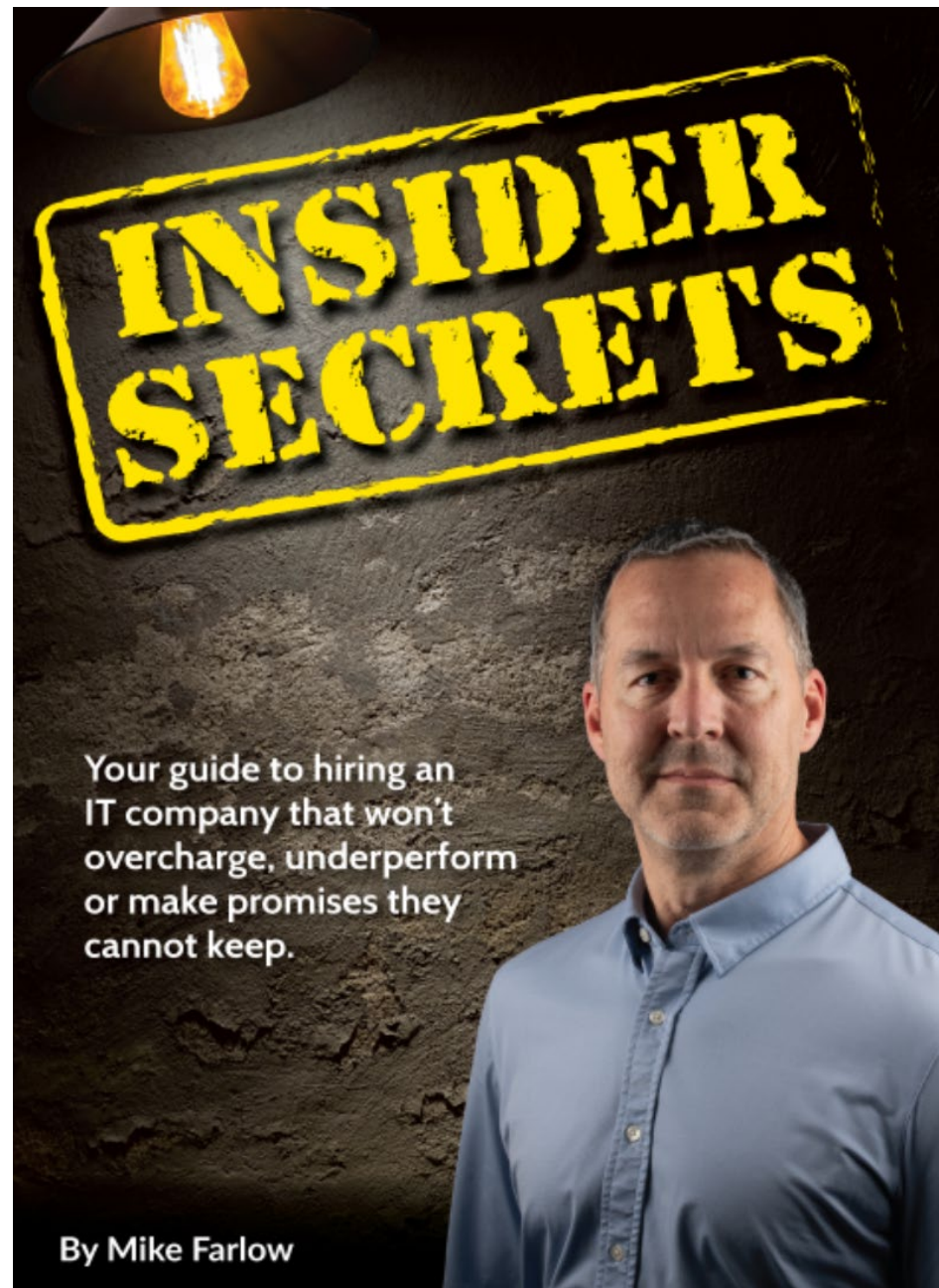
- Objective is designed to protect consumer information
- Expands the definition of financial institution
- 9 key requirements
- New penalties for non-compliance
- **Notification Requirements:** Effective May 13, 2024, for certain incidents affecting 500+ consumers.





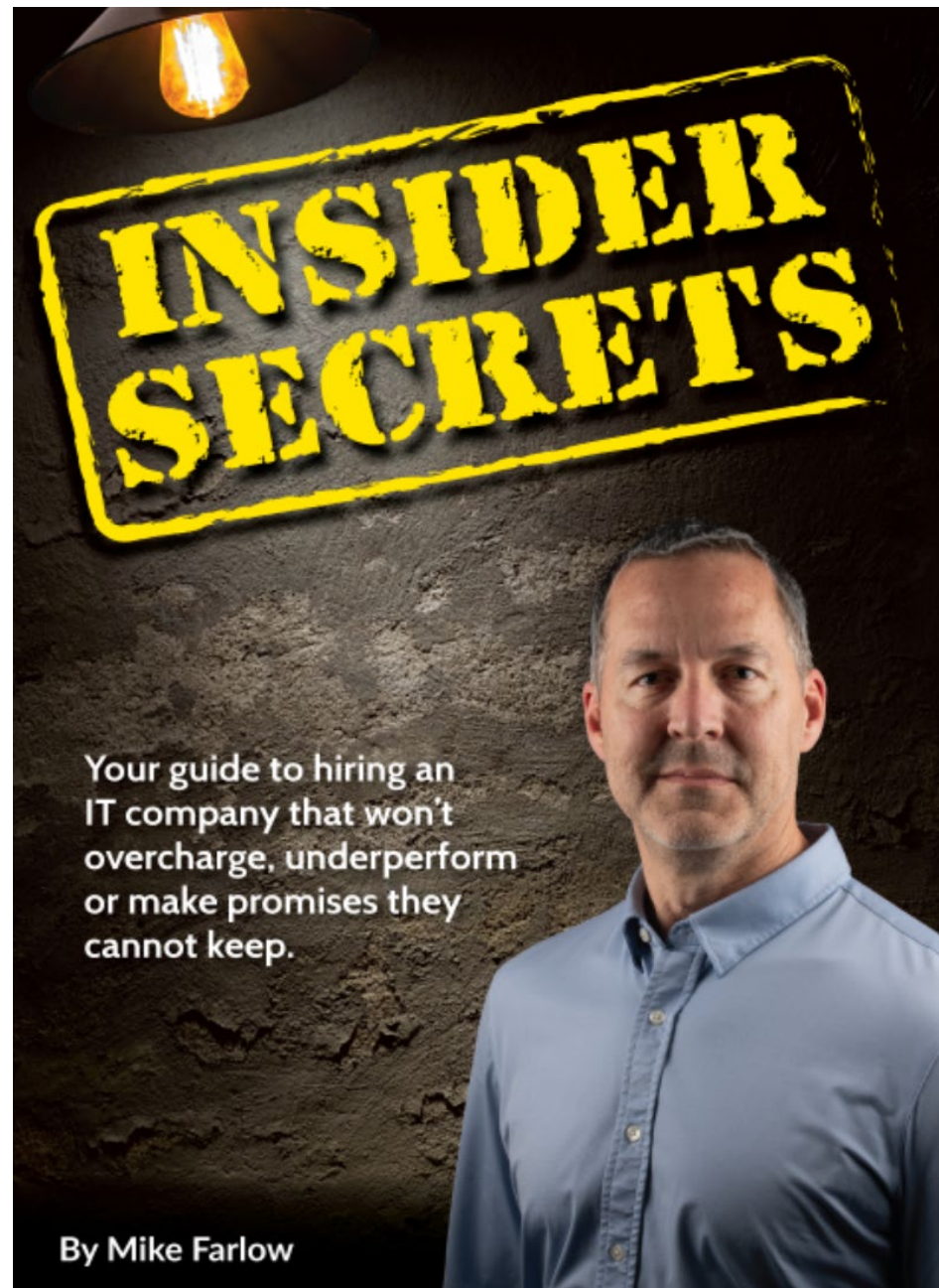
IT Vendor Selection and Internal Team Recommendations

Critical Factors for Compliance and Security:



1. Cybersecurity Expertise
Ask about Cybersecurity certifications such as CISSP, CEH, or CompTIA Security+
2. Zero-Trust Cybersecurity Framework
User, Device, Apps, Data, Network
3. Ensure IT vendor or team is well-versed in security standards, regulatory compliance (FTC), and safeguarding client data.

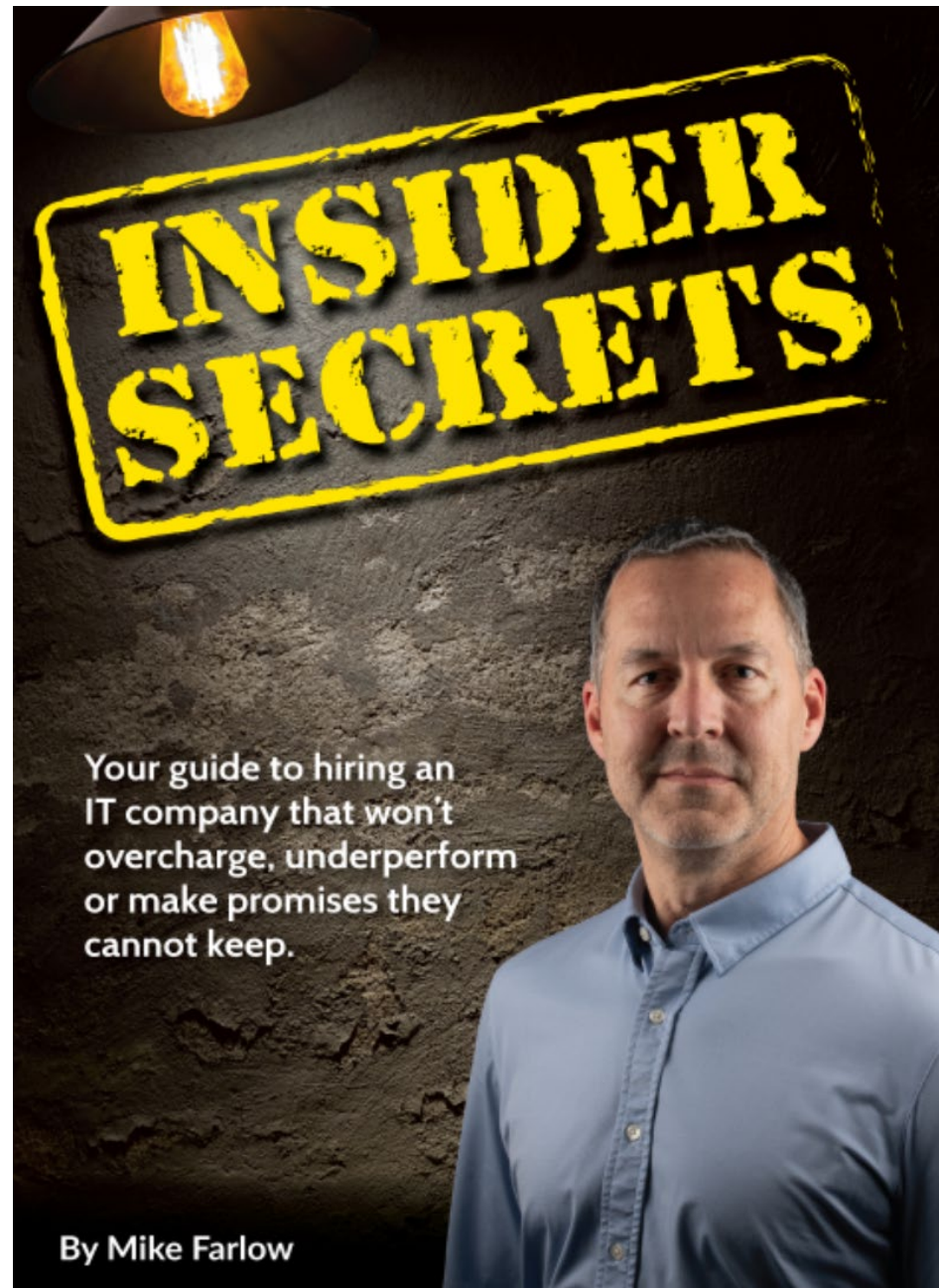
Critical Factors for Compliance and Security:



3. Data Backup and Disaster Recovery
 - Where is Data backed up?
 - How many different places?
 - How quickly can data be recovered?
4. Ensure IT conducts full network assessments for themselves and for you. Ask how often network assessments are completed

Critical Factors for Compliance and Security:

5. Ask about Third-Party Audits
6. Cyber Liability Insurance
7. Response Time and After-Hours Support
Avg US MSP Response Time = 16 Hours
8. Network Documentation and Transparency





Zero-Trust Strategy

layers multiple protections to provide

defense against modern threats. Continuous verification of applications and controls keep systems safe.



Ransomware Detection and Isolation

We use special detection

software that identifies active ransomware activity. It stops the process and isolates the computer from the network.



Application Controls

for installing & running programs. By

locking down the systems to only allowed programs and processes. Simply put - if it can't execute then the threat level is greatly reduced.



Microsoft 365 Risk Watch

includes SOC monitoring for threats in

your Office 365 cloud. Unusual activity, forwarding rules, international logins and more are monitored.



SIEM

advanced logging for firewalls, servers and

Office 365 meets insurance and compliance requirements.



Employee Self-Paced CyberSecurity Training

Human error is the primary cause of cybersecurity events. A properly trained staff helps eliminate errors.



Password Manager

company managed credentials are

a challenge to maintain. Our password manager solves this nagging problem.



Ring Fencing

puts a fence around your applications and data so

hackers or malware can not access them in an unauthorized manner.



24/7 Monitoring

by a live security operation center (SOC). If a security event is

detected on critical assets, then action can be taken immediately to isolate or remediate the threat.

Adopt a Framework



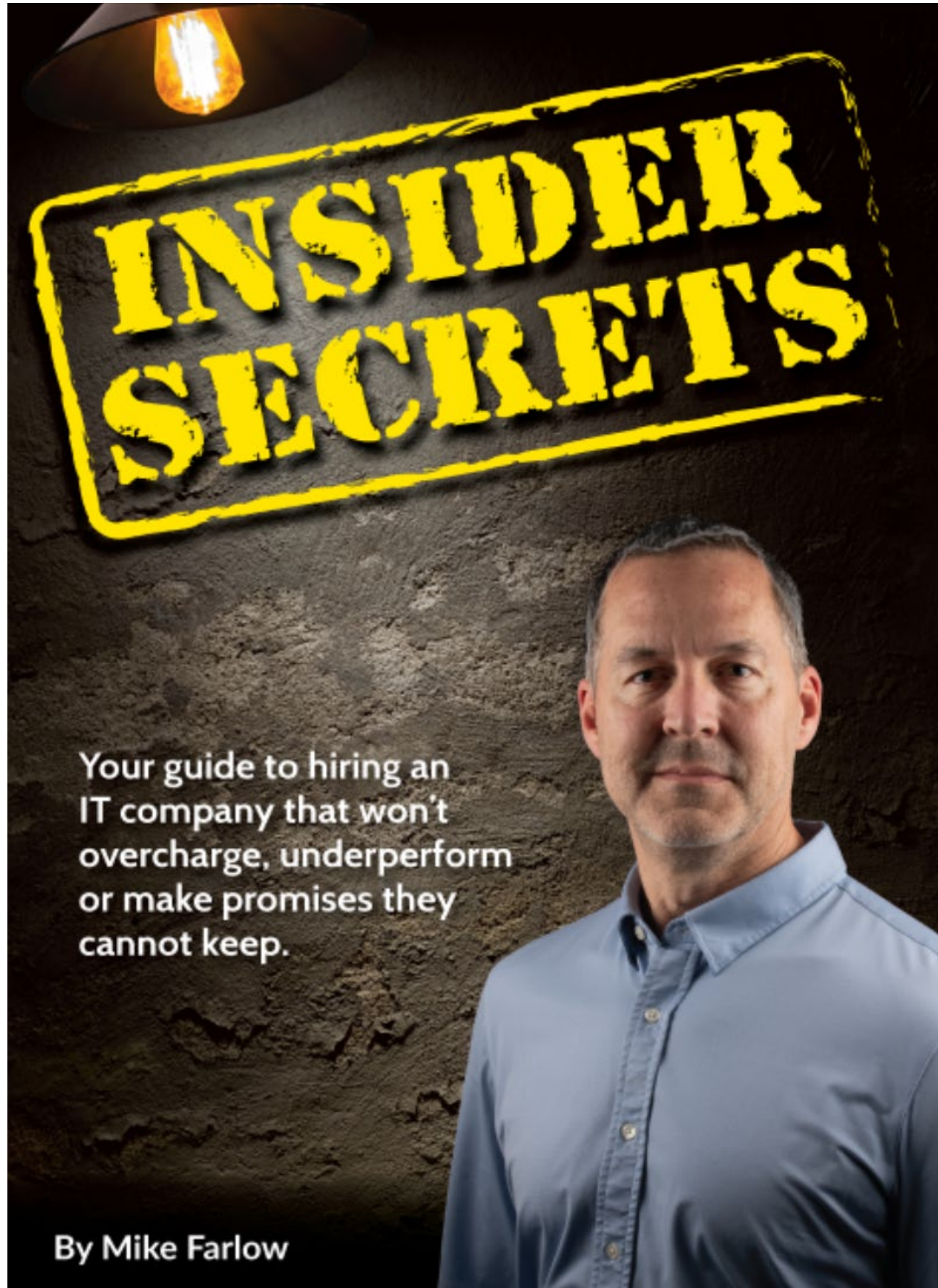
Cyber Defense Matrix

	Identify	Protect	Detect	Respond	Recover
Devices					
Applications					
Networks					
Data					
Users					
Degree of Dependency	<div><div>Technology</div><div>Process/Govern</div><div>People</div></div>				

Beware!

Common Surprises:

- Auto-renewing Contracts
- Surprise Invoices
 - Software Licenses
 - Hardware Licenses
- What You Own vs “Managed” Devices
- Remediation Charges
- Trip Charges
- Projects vs Standard Support



Come Visit the
ComTech Booth
for a free copy!



Cyber Liability Insurance

COMTECH

Key Pillars of a Cyber Insurance Policy



Prevention

- Pre-breach assessments
- Access to pre-vetted vendors
- Cybersecurity information



Assistance

- Forensic Investigators
- Legal Services
- Notification
- Credit Monitoring
- Call Center Services
- Crisis Management
- Public Relations



Operations

- Costs incurred to keep or return the business to operational
- Loss of revenue, income, turnover
- Costs incurred to recreate/restore data and information



Liability

- Legal costs and damages from claims alleging privacy breach or network security failure

What is Cyber Insurance?

- Containing the Breach
- Remediation
- Cyber Forensics
- Recovering Data
- Customer Notifications
- PR Costs
- Credit Monitoring
- Legal Expenses
- Regulatory Fines
- Extortion Costs
- Business Interruption

What's Covered?

First-party coverage – Intends to cover damages a business suffers because of a cyber breach. This can include things like investigative services, business interruption coverage and data recovery.

Third-party coverage – Intends to cover damages if a business' customers or partners are affected by a cyber attack. This can include legal fees, settlement costs, security failures and media liabilities.

Cyber crime — Intends to cover damage due to any type of illegal activity that occurs using digital means. Examples of cybercrime are extortion/ransomware, phishing, social engineering, and wire transfer fraud.



**Do Small Businesses Need Cyber Insurance If
They Practice Good Cyber Hygiene?**

YES!

Do Hackers Really Bother with Attacking Small Businesses?

Yes! A recent Verizon report notes that 43% of all cyber attacks are against small businesses. Worse, 63% of small businesses had experienced a breach in the last 12 months.

Any business with a computer and an internet connection is at risk.



Doesn't My Current Business Insurance Cover Cyber Attacks?

Maybe





What Should I Consider When Choosing Between Purchasing a Stand-Alone Cyber Policy vs. Adding an Endorsement to an Existing Policy?

Aggregate Limit/Retention
Business Interruption/Loss of Revenue
Extortion/Ransomware
Regulatory Fines
1st Party, 3rd Party, Cyber Crime

Look Inside a Cyber Liability Policy

First-Party Insuring Agreements

Breach Response

- Following a system breach, provides coverage for activities such as forensic and legal review, notifications to affected parties, public relations, etc.

Business Interruption & Extra Expenses

- Provides coverage for lost revenue due to an interruption in business caused by breach of internal systems or those of a third-party provider.

Digital Restoration

- Aimed at covering the costs to recover, re-create, and restore affected data.

Cyber Extortion

- Intended to provide coverage if a ransom payment is made and/or the expenses incurred to recover data/system control without paying the ransom.

Cyber Crime

- Coverage that targets fraudulent payments via Social Engineering or Funds Transfer Fraud.

Look Inside a Cyber Liability Policy

Third-Party Insuring Agreements

Network & Information Security Liability

- Designed to provide protection in the event of claims for failing to protect client or third party personally identifiable information (PII), including but not limited to SSN, credit card numbers, medical information, passwords, etc.

Regulatory Defense & Penalties

- Covers defense expenses and penalties levied by regulatory agencies due to a data breach.

Multimedia Liability

- Leveraged to cover claims that allege invasion of privacy, copyright/trademark infringement, and other Wrongful Media Communications Acts.

PCI Fines & Assessments

- Designed to cover fines and assessments imposed by credit card companies or banks for issues of non-compliance with Payment Card Industry Data Security Standard (PCI DSS).

FIRST PARTY COVERAGE	VALID UNTIL	12/24/24	12/24/24	12/24/24	11/29/24
	ADMISSION STATUS	Non-Admitted	Admitted	Non-Admitted	Admitted
	ISSUING INSURER	See quote letter	Coalition Insurance...	Certain Underwriters at...	Spinnaker Insurance...
	AM BEST RATING Financial strength rating	A+ (Superior) A- (Excellent)	A- (Excellent)	A (Excellent)	A- (Excellent)
	AGGREGATE LIMIT / RETENTION <small>(DEDUCTIBLE)</small> Maximum amount paid by the Insurer / The amount of a claim you pay	\$1,000,000 / \$2,500'	\$1,000,000 / \$2,500'	\$1,000,000 / \$2,500'	\$1,000,000 / \$1,000'
	NOTIFICATION COSTS Cost to notify affected individuals after a data breach	\$1,000,000	\$1,000,000	\$100,000	\$1,000,000
	BREACH COSTS INSIDE/OUTSIDE Will the breach costs erode the aggregate limit (Inside) or are separate (outside)	Outside	Inside	Outside	Inside
	BUSINESS INTERRUPTION Covers lost profits Incurred due to not operating	\$1,000,000	\$1,000,000	\$1,000,000	\$1,000,000
	BI WAITING PERIOD Minimum duration of business interruption before coverage starts	8 hours	8 hours	10 hours	6 hours
	CONTINGENT BUSINESS INTERRUPTION Losses from an interruption in 3rd party computer services or software	\$1,000,000	\$1,000,000	\$1,000,000	Refer to quote letter
	DATA RECOVERY The cost of recovering lost data	\$1,000,000	\$1,000,000	\$1,000,000	\$1,000,000
	EXTORTION/RANSOMWARE Covers damage and ransom payments from an attack	\$1,000,000	\$1,000,000	\$1,000,000	\$1,000,000
	BRICKING When computers and electronic hardware are damaged beyond repair	\$1,000,000	\$1,000,000	\$1,000,000	\$50,000

THIRD PARTY COVERAGE	NETWORK SECURITY AND PRIVACY LIABILITY Third party liability costs	\$1,000,000	\$1,000,000	\$1,000,000	\$1,000,000
	PCI Covers fines or penalties imposed by banks or credit card companies	\$1,000,000	\$1,000,000	\$1,000,000	\$1,000,000
	REGULATORY In case you're fined by regulators (e.g., for breaching consumer privacy)	\$1,000,000	\$1,000,000	\$1,000,000	\$1,000,000
	MEDIA When your content triggers legal action against you (e.g. - libel, plagiarism)	\$1,000,000	\$1,000,000	\$1,000,000	\$1,000,000
CYBER CRIME	COMPUTER FRAUD Covers funds or property stolen resulting from a hack	\$250,000,	\$250,000,	\$250,000,	\$1,000,000,
	FUNDS TRANSFER FRAUD When a criminal deceives a bank/institution to transfer funds	\$250,000,	\$250,000,	\$250,000,	\$1,000,000,
	SOCIAL ENGINEERING When cyber criminals deceive a business to transfer funds willingly	\$250,000,	\$250,000,	\$250,000,	\$100,000,
	INVOICE MANIPULATION Invoice Manipulation means the release or distribution of any fraudulent invoice	\$250,000,	\$250,000,	\$250,000,	Refer to quote letter,
	TOTAL	(Approximate²) \$875.78	(Approximate²) \$1,479	(Approximate²) \$1,598.66	(Approximate²) \$1,703

Cyber Liability Claims Scenarios

Ransomware

An employee at a small business accidentally clicked a malware link, resulting in a ransomware attack that encrypted **2,500 customer records containing sensitive information**. The hackers demanded **\$38,000 in Bitcoin within 48 hours to unlock the files**. The business contacted its cyber insurance provider, which assigned a breach coach to oversee a forensics team. This team assessed the damage and paid the ransom demand, while the insurer confirmed coverage and helped file a claim to minimize business interruption impacts.

INCIDENT RESPONSE	
Incident response manager ("breach coach") fees	\$8,000
Forensic investigation costs to locate malware, analyze damage, ensure containment and calculate loss	\$7,150
Legal fees	\$5,100
NOTIFICATION COSTS	
	\$1,425
BUSINESS INTERRUPTION	
	\$25,433
DATA RECOVERY	
Costs associated with replacing lost or corrupted data	\$13,200
EXTORTION/RANSOMWARE	
Ransom payment	\$38,000
BRICKING	
Damage to computer and hardware systems	\$13,800
TOTAL POTENTIAL CLAIM	
	\$109,908

Resolution: Although the business had regular online backups, the hackers also encrypted these, leaving no recovery option. The insurance company and breach coach determined that paying the ransom was the quickest way to restore operations. Using their Bitcoin account, the insurer paid the ransom, swiftly unlocking the files and minimizing business interruption, allowing the business to resume quickly.

Cyber Liability Claims Scenarios

Outdated Software

INCIDENT RESPONSE

Forensic investigation costs to isolate vulnerability, analyze damage, ensure containment and calculate loss

\$7,500

Identity theft and credit monitoring services

\$4,140

Incident response fees

\$5,650

Public relations fees to minimize reputational impact

\$8,000

Call center set up and operation to field inquiries

\$8,000

NOTIFICATION COSTS

\$1,000

DATA RECOVERY

Costs associated with replacing lost or corrupted data

\$9,200

REGULATORY

Legal expenses arising from regulatory investigation due to mismanagement of private information

\$10,925

Legal expenses and settlement costs for claims

\$7,950

Business Interruption

\$19,376

TOTAL POTENTIAL CLAIM

\$79,741

Hackers exploited outdated software at a small automobile dealership, compromising **1,150 records** containing names, emails, credit card, and banking details. Local authorities alerted the dealership after multiple complaints of suspicious activity. Upon discovery, the dealership's insurance carrier brought in forensic experts to start the IT recovery and notification process.

Resolution: The dealership's cyber policy activated, providing immediate response services. A forensic team isolated the breach, while a claim was filed to cover legal, consulting, and media costs. The insurance and IT teams strengthened the dealership's cyber defenses with updated firewalls, intrusion detection, and encryption. Local media informed affected customers, offering credit monitoring, and legal teams managed responses. Finally, forensic consultants helped establish a new plan with regular updates, testing, and staff training to prevent future incidents.

Cyber Liability Claims Scenarios

Social Engineering

An attacker accessed a medical equipment company's emails, posing as the General Manager to trick an employee into transferring funds to the hacker's account. **Upon discovering \$244,600 in unauthorized payments, the company froze the funds and alerted their cyber insurer, recovering \$220,000 of the losses.**

INCIDENT RESPONSE	
Forensic investigation costs to locate the breach, analyze damage, and ensure containment	\$8,800
Legal fees	\$8,200
FUNDS TRANSFER FRAUD	
Transferred funds not recovered	\$24,600
TOTAL POTENTIAL CLAIM	\$39,600

Resolution: The medical company's stand-alone cyber policy covered social engineering and included essential response services. After notifying their insurer, an IT forensic consultant helped repair the system and enhance security. With expanded cyber crime coverage, the company was reimbursed for the financial loss, less the deductible, as well as forensic and legal costs.

Cyber Liability Claims Scenarios

Lost Hardware

An employee at a copy machine company **lost a laptop containing an Excel file with records of 4,100 customers, including sensitive information.** Upon discovery, the company notified their insurer, which provided a breach coach to assess the damage and ensure compliance with regulatory and notification requirements.

INCIDENT RESPONSE

Forensic costs to assess and contain damage

\$7,600

Legal fees

\$11,930

Public relations fees to minimize reputational impact

\$8,600

NOTIFICATION COSTS

\$1,075

DATA RECOVERY

Costs associated with replacing lost or corrupted data

\$9,200

REGULATORY

Settlement fine

\$19,665

Patient liability settlements

\$41,113

TOTAL POTENTIAL CLAIM

\$99,183

Resolution: The breach coach assigned a forensic team to assess the potential data exposure, confirming that customer records were compromised. Affected customers were notified and offered credit monitoring. To manage reputational impact, a PR agency was engaged, and legal counsel addressed customer claims. The company also proactively contacted the Department of Health and Human Services, reaching a settlement that included a corrective action plan and employee cybersecurity training.

Cyber Liability Claims Scenarios

Former Employee

A financial institution was hacked by a former employee whose credentials were not revoked upon termination. **The ex-employee sold 1,050 customer records, including names, contact information, and credit card details, on the dark web.** The institution promptly informed their insurer, which provided forensic, legal, and media support to control the impact, along with a breach coach to manage both financial and reputational damage.

INCIDENT RESPONSE	
Forensic investigation costs to analyze damage and ensure containment	\$7,800
Identity theft and credit monitoring services	\$3,780
Legal fees	\$8,900
Public relations fees to minimize reputational impact	\$8,100
Call center set up and operation to field inquiries	\$5,700
NOTIFICATION COSTS	
DATA RECOVERY	
Costs associated with replacing lost or corrupted data	\$8,300
TOTAL POTENTIAL CLAIM	\$43,380

Resolution: The forensic team quickly identified the breach and coordinated with the financial institution's IT department to make repairs. Guided by the breach coach, the institution informed affected customers, offering identity protection and credit monitoring. Legal counsel was advised to pursue action against the former employee. Working with media relations, the institution responded transparently to the press. The insurer and forensic team also recommended updates to the cyber response plan, enhancing IT policies and technology. This swift response minimized both costs and reputational damage.

Cyber Liability Market Overview

2024 Trends

Rates Expected To Remain Stable In 2024

- Ample carrier capacity
- Competitive market environment

Ransomware Events

- Up 1281% over last 5 years
- Increased 214% alone in Q4 '23

Claims Activity

- Up 65% Year over Year
- Top claims by type
 - Ransomware
 - Funds Transfer Fraud (FTF)
 - Business Email Compromise

Source: Aon Cyber Solutions



Cyber Liability in the Financial Services Industry

In the News

B Bloomberg.com

Davos 2024: JPMorgan Says Hacker Attempts Have Increased This Year

JPMorgan Chase & Co. has seen an increase in hackers attempting to infiltrate its systems as the Wall Street giant and its rivals continue...

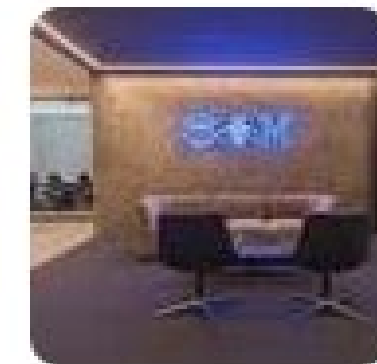
Jan 17, 2024

F FinTech Magazine

IBM: Finance and Insurance is Second-Most Attacked Industry

By Tom Chapman. February 21, 2024. 4 mins. Research from IBM has Laid Bare the Cyber Challenges Facing Financial Institutions. Picture: IBM.

Feb 21, 2024



Cyber Liability in the Financial Services Industry

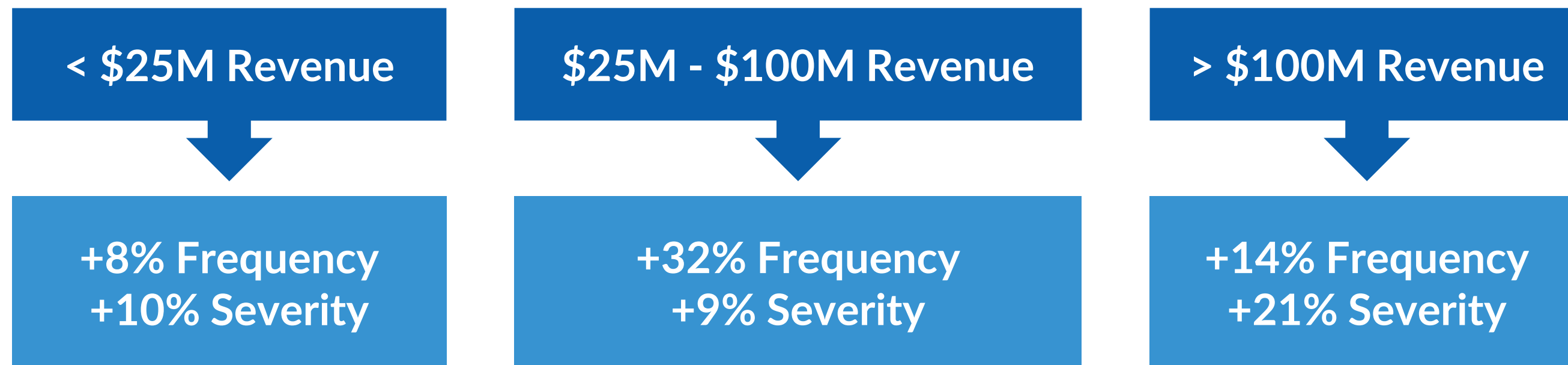
Why are financial institutions targeted?

- Client files/access to sensitive information
 - Personally Identifiable Information (PII)
 - Payment Card Information (PCI)
- Frequent transactions between clients, vendors, and financial firms
- Key link in economic infrastructure → Breach of financial institutions can cause massive downstream effect



Cybersecurity Statistics

99% Of All Cyber Claims Come From Companies
With Annual Revenue Under \$2 Billion



- Average ransomware claim: \$812,360 across all organization sizes
- Ransomware claims account for nearly 30% of all filed cyber claims
- 27% of data breach claims and 24% of first-party claims contained exclusionary language in the policy, which prevented payout

Perspective of a Cyber Liability Carrier

The 2024 Travelers Risk Index

Overview

- Over 1,200 business decision makers surveyed
- Representative of all business sizes and industries

Cyber Preparedness by the Numbers

- 20% of businesses are not implementing basic tools – firewall, antivirus, data backups, password updates, etc.
- 53% do not utilize an endpoint detection and response (EDR) tool
- 51% of businesses do not have an incident response (IR) plan
- 37% do not use multifactor authentication (MFA) for remote or admin access
 - According to Microsoft, 99.9% of attacks can be blocked by MFA

Small Business Focus - Even Less Prepared

- 81% do not use EDR
- 69% do not have an IR plan
- 52% do not use MFA for remote or admin access

80% Of Business Leaders Think Having Cyber Insurance Is Critical...

Perspective of a Cyber Liability Carrier

No matter the size or industry of the business,
many are left vulnerable without cyber insurance.

53%

of small businesses lack
cyber insurance

18%

of midsize businesses
lack cyber insurance

17%

of large businesses lack
cyber insurance

15% Of Banks Have Not Purchased Cyber Liability Insurance...

Source: Travelers Cyber Risk Index

Perspective of a Cyber Liability Carrier

Future Market Outlook

Cyber Incident Costs on the Rise

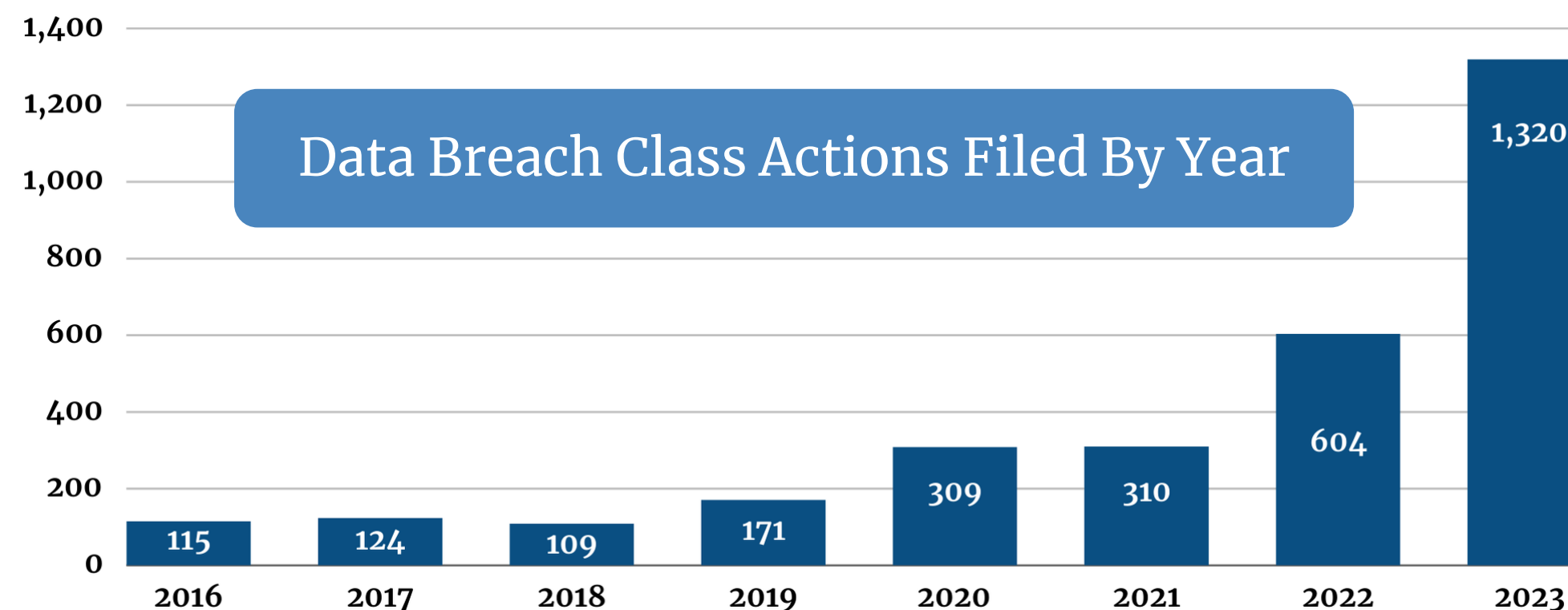
- Single Business Email Compromise: Six figures in forensic investigation/notification costs

Data Breach Class Action Lawsuits Increasing

- More than doubled 2022 to 2023
- Defense costs to follow

Financial Sector Remains Top Target

- Substantial Personally Identifiable Information (PII) maintained



Businesses at Risk

Should All Businesses Be Worried About Cyber Risks?

YES, But Why?

- Most have simpler IT infrastructure than financial institutions
- Fewer cybersecurity controls in place, lack of resources
- Smaller (or outsourced) IT team to respond to issues

Cyber Attacks Often Lead To Weeks/Months Long Delays In Business

- Forensic investigations
- Data/asset recovery and restoration
- This process can cost hundreds of thousands of dollars

60% of businesses that are victims of a cyber attack, go out of business within 6 months of the incident
(Source: Forbes)

Cybersecurity Best Practices

How to Safeguard Your Firm

1. PROVIDE CYBERSECURITY TRAINING

Conduct regular Cybersecurity Training for all associates including internet use guidelines, phishing testing, and social engineering protocols.

2. PREPARE AN INCIDENT RESPONSE (IR) PLAN

A clearly defined, focused, and coordinated approach for responding to cyber incidents. Test this plan annually.

3. KEEP SYSTEMS UP TO DATE

Regularly install updates, patches, and fixes. Enable automatic updates where possible and replace unsupported systems. Set antivirus software to run scans following updates.

4. IMPLEMENT THE 3-2-1 BACKUP STRATEGY

3) Create one primary backup and two copies of your data, 2) Save your backups to two different types of media, and 1) keep at least one backup file off-site and offline.

5. CONTROL ACCESS TO SYSTEMS AND DATA

Lock laptops when unattended, ensure all employees use strong and unique passwords, and only grant administrative privileges to trusted IT staff.

Cybersecurity Best Practices

How to Safeguard Your Firm

6. REQUIRE FIREWALL SECURITY

Ensure the office operating system is firewall enabled. If employees work remotely, require their home systems are protected by a firewall.

7. SECURE WI-FI NETWORKS

Make sure that Wi-Fi is secure, encrypted, and hidden.

8. ENABLE MULTI-FACTOR AUTHENTICATION (MFA)

Most email platforms allow you to adjust your settings to enable MFA at no cost.

9. CREATE A MOBILE DEVICE ACTION PLAN

Require users to password protect their devices, encrypt data, and install security applications. Be sure to have reporting protocols for lost or stolen equipment.

10. DEFEND AGAINST SOCIAL ENGINEERING THREATS

Implement Endpoint Detection and Response (EDR), set spam filters, and establish multi-step verification communication protocols.

Cybersecurity Best Practices

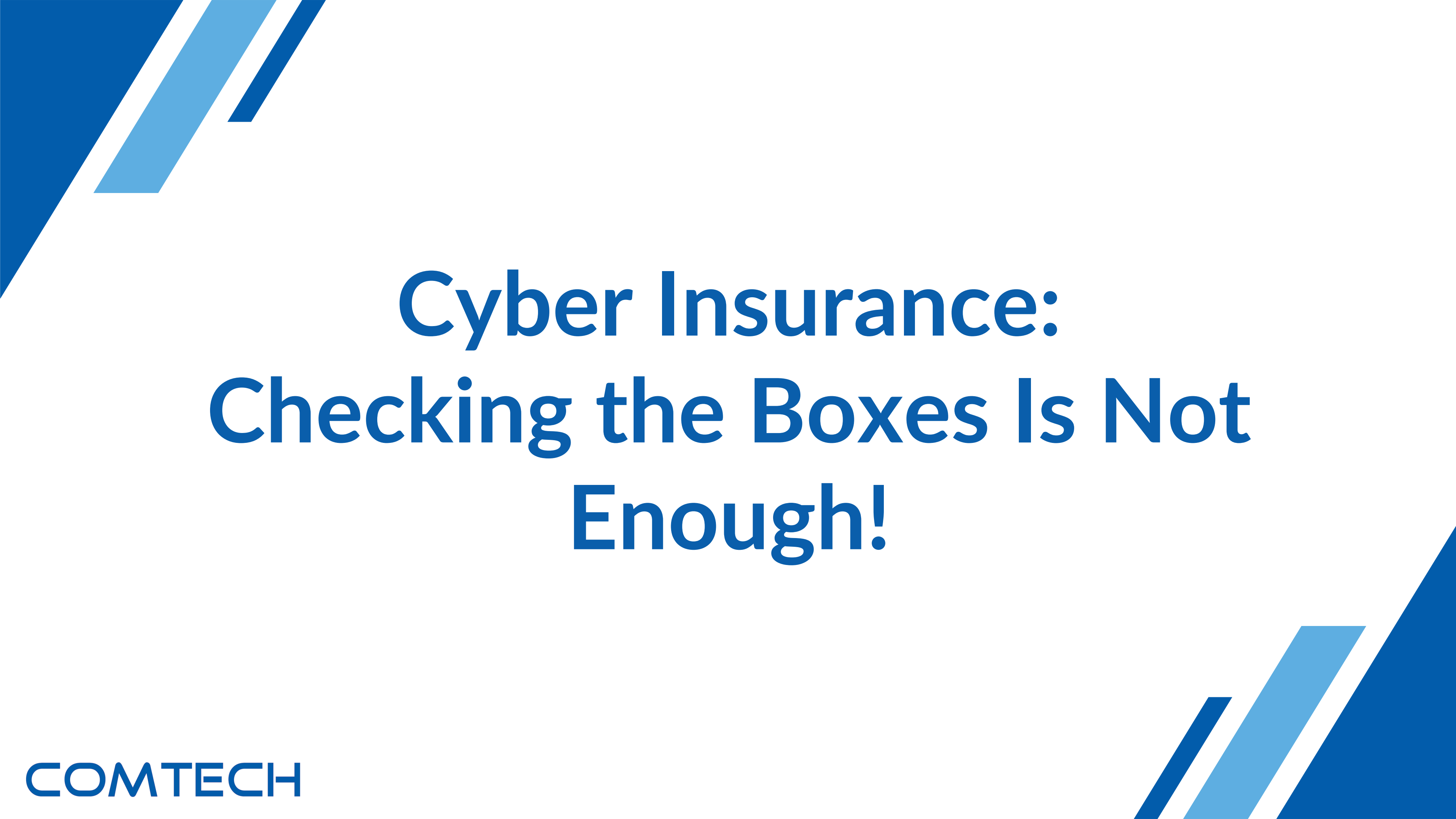
It Takes EVERY Employee – A Few Simple Steps

Password Hygiene

- What NOT to do...?
 - Keep an electronic list of usernames and passwords
- Best Practices
 - Update passwords regularly
 - Utilize password generation capabilities

Email Encryption

- If an email contains Personally Identifiable Information (PII):
 - Type the word ***encrypt*** into the subject line or body of the email
 - Expand tags menu and change sensitivity level to ***confidential***



Cyber Insurance: Checking the Boxes Is Not Enough!

UNDERWRITING INFORMATION

DATA INVENTORY

1. Indicate whether the Applicant or a third party on the Applicant's behalf, collects, receives, processes, transmits, or maintains the following types of data as part of its business activities:
 - a. Credit/Debit Card Data ☐ Yes ☐ No
If Yes:
 - i. Is the Applicant currently compliant with Payment Card Industry Data Security Standards (PCI-DSS)? ☐ Yes ☐ No
 - ii. How many credit card transactions are processed or accepted for payment in a typical year?
 - iii. What is the Applicant's reporting level? ☐ 1 ☐ 2 ☐ 3 ☐ 4
 - iv. Was the Applicant's last PCI assessment conducted within the past 12 months? ☐ Yes ☐ No
 - b. Medical information, other than that of the Applicant's own employees ☐ Yes ☐ No
 - c. Non-employee Social Security Numbers ☐ Yes ☐ No
 - d. Employee/HR Information ☐ Yes ☐ No
2. What is the approximate number of unique individuals for whom the Applicant, or a third party on the Applicant's behalf, collects, stores, or processes any amount of personal information as outlined in Question 1?
☐ fewer than 100,000 ☐ 100,000 – 250,000 ☐ 250,001 – 500,000 ☐ 500,001 – 1,000,000
☐ 1,000,001 – 2,500,000 ☐ 2,500,001 – 5,000,000 ☐ > 5,000,000
3. Indicate whether the data indicated in Question 1 is encrypted:
 - a. While at rest in the Applicant's databases or on the Applicant's network ☐ Yes ☐ No ☐ N/A
 - b. While in transit in electronic form ☐ Yes ☐ No ☐ N/A
 - c. While on mobile devices ☐ Yes ☐ No ☐ N/A

PRIVACY CONTROLS

6. Indicate whether the Applicant currently has the following in place:
- | | | |
|--|------------------------------|-----------------------------|
| a. A Chief Privacy Officer or other individual assigned responsibility for monitoring changes in statutes and regulations related to handling and use of sensitive information | <input type="checkbox"/> Yes | <input type="checkbox"/> No |
| b. A publicly available privacy policy which has been reviewed by an attorney | <input type="checkbox"/> Yes | <input type="checkbox"/> No |
| c. Sensitive data classification and inventory procedures | <input type="checkbox"/> Yes | <input type="checkbox"/> No |
| d. Data retention, destruction, and recordkeeping procedures | <input type="checkbox"/> Yes | <input type="checkbox"/> No |
| e. Annual privacy and information security training for employees | <input type="checkbox"/> Yes | <input type="checkbox"/> No |
| f. Restricted access to sensitive data and systems based on job function | <input type="checkbox"/> Yes | <input type="checkbox"/> No |

NETWORK SECURITY CONTROLS

7. Indicate whether the Applicant currently has the following in place:
- | | | | |
|---|------------------------------|-----------------------------|------------------------------|
| a. A Chief Information Security Officer or other individual assigned responsibility for privacy and security practices | <input type="checkbox"/> Yes | <input type="checkbox"/> No | |
| b. Up-to-date, active firewall technology | <input type="checkbox"/> Yes | <input type="checkbox"/> No | |
| c. Up-to-date, active anti-virus software on all computers, networks, and mobile devices | <input type="checkbox"/> Yes | <input type="checkbox"/> No | |
| d. A process in place to regularly download, test, and install patches | <input type="checkbox"/> Yes | <input type="checkbox"/> No | |
| <i>If Yes, is this process automated?</i> | <input type="checkbox"/> Yes | <input type="checkbox"/> No | |
| <i>If Yes, are critical patches installed within 30 days of release?</i> | <input type="checkbox"/> Yes | <input type="checkbox"/> No | |
| e. Intrusion Detection System (IDS) | <input type="checkbox"/> Yes | <input type="checkbox"/> No | |
| f. Intrusion Prevention System (IPS) | <input type="checkbox"/> Yes | <input type="checkbox"/> No | |
| g. Data Loss Prevention System (DLP) | <input type="checkbox"/> Yes | <input type="checkbox"/> No | |
| h. Multi-factor authentication for administrative or privileged access | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> N/A |
| i. Multi-factor authentication for remote access to the Applicant's network and other systems and programs that contain private or sensitive data in bulk | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> N/A |
| j. Multi-factor authentication for remote access to email | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> N/A |
| k. Remote access to the Applicant's network limited to VPN | <input type="checkbox"/> Yes | <input type="checkbox"/> No | <input type="checkbox"/> N/A |
| l. Backup and recovery procedures in place for all important business and customer data | <input type="checkbox"/> Yes | <input type="checkbox"/> No | |
| <i>If Yes, are such procedures automated?</i> | <input type="checkbox"/> Yes | <input type="checkbox"/> No | |
| <i>If Yes, are such procedures tested on an annual basis?</i> | <input type="checkbox"/> Yes | <input type="checkbox"/> No | |
| m. Annual penetration testing | <input type="checkbox"/> Yes | <input type="checkbox"/> No | |
| <i>If Yes, is such testing conducted by a third party service provider?</i> | <input type="checkbox"/> Yes | <input type="checkbox"/> No | |
| n. Annual network security assessments | <input type="checkbox"/> Yes | <input type="checkbox"/> No | |
| <i>If Yes, are such assessments conducted by a third party service provider?</i> | <input type="checkbox"/> Yes | <input type="checkbox"/> No | |
| o. Systematic storage and monitoring of network and security logs | <input type="checkbox"/> Yes | <input type="checkbox"/> No | |
| p. Enforced password complexity requirements | <input type="checkbox"/> Yes | <input type="checkbox"/> No | |
| q. Procedures in place to terminate user access rights as part of the employee exit process | <input type="checkbox"/> Yes | <input type="checkbox"/> No | |

VENDOR CONTROLS

14. For vendors with access to the Applicant's computer system or confidential information, indicate whether the Applicant has the following in place:

- | | | |
|---|------------------------------|-----------------------------|
| a. Written policies which specify appropriate vendor information security controls | <input type="checkbox"/> Yes | <input type="checkbox"/> No |
| b. Periodic review of, and updates to, vendor access rights | <input type="checkbox"/> Yes | <input type="checkbox"/> No |
| c. Prompt revocation of vendor access rights when access is no longer needed | <input type="checkbox"/> Yes | <input type="checkbox"/> No |
| d. Logging and monitoring of vendor access to the Applicant's system | <input type="checkbox"/> Yes | <input type="checkbox"/> No |
| e. A requirement that vendors carry their own Professional Liability or Cyber Liability insurance | <input type="checkbox"/> Yes | <input type="checkbox"/> No |
| f. Hold harmless / indemnity clauses that benefit the Applicant in contracts with vendors | <input type="checkbox"/> Yes | <input type="checkbox"/> No |

15. Indicate which of the following services are outsourced:

Data back up ☐ Yes ☐ No ☐ N/A

Provider:

Data center hosting ☐ Yes ☐ No ☐ N/A

Provider:

IT infrastructure ☐ Yes ☐ No ☐ N/A

Provider:

IT security ☐ Yes ☐ No ☐ N/A

Provider:

Web hosting ☐ Yes ☐ No ☐ N/A

Provider:

Payment processing ☐ Yes ☐ No ☐ N/A

Provider:

Physical security ☐ Yes ☐ No ☐ N/A

Provider:

Software development ☐ Yes ☐ No ☐ N/A

Provider:

Customer marketing ☐ Yes ☐ No ☐ N/A

Provider:

Data processing ☐ Yes ☐ No ☐ N/A

Provider:

If Data center hosting or IT infrastructure is answered Yes above:

a. What is the likely impact to the organization if these services become unavailable?

b. Does the Applicant have an alternative solution in the event of a failure or outage to one of these service providers?

If Payment processing is answered Yes above, does the Applicant have an alternative means of processing card data in the event of an outsourced provider failure or outage?

☐ Yes ☐ No

Provide details:

LOSS INFORMATION

16. In the past three years, has the Applicant experienced a network or computer system disruption due to an intentional attack or system failure; an actual or suspected data breach; an actual or attempted extortion demand; or received any complaints, claims, or been subject to litigation involving matters or privacy injury, identity theft, denial-of-service attacks, computer virus infections, theft of information, damage to third party networks, or the Applicant’s customer’s ability to rely on the Applicant’s network?

☐ Yes ☐ No
17. Is the Applicant, any Subsidiary, or any person proposed for this insurance aware of any circumstance that could give rise to a claim against them under this CyberRisk Coverage?

☐ Yes ☐ No
- If the Applicant answered Yes to any part of Question 16 or Question 17, attach details of each claim, complaint, allegation, or incident, including costs, losses, or damages incurred or paid, any corrective procedures to avoid such allegations in the future, and any amounts paid as loss under any insurance policy.

REQUESTED INSURANCE TERMS

Requested Terms:

Insuring Agreement	Limit Requested	Retention Requested
Privacy And Security	\$	\$
Media	\$	\$
Regulatory Proceedings	\$	\$
Privacy Breach Notification	\$	\$
Computer And Legal Experts	\$	\$
Betterment	\$	\$
Cyber Extortion	\$	\$
Data Restoration	\$	\$
Public Relations	\$	\$
Computer Fraud	\$	\$
Funds Transfer Fraud	\$	\$
Social Engineering Fraud	\$	\$
Telecom Fraud	\$	\$
Business Interruption	\$	\$
Dependent Business Interruption	\$	\$
Reputation Harm	\$	\$

18. Requested Terms:

Aggregate Limit Requested:

Effective Date Requested:
19. Does the Applicant currently purchase CyberRisk coverage?

☐ Yes ☐ No
- If Yes, provide the following:

Expiring Carrier:

Expiring Limit:

Date coverage first purchased?

Takeaways – Cyber Liability Insurance

- Assess Coverage Needs
- Compare Policy Options
- Plan for Incident Response
- Implement Risk Mitigation Measures
- Prepare for Renewal and Premium Management

YOU ARE THE HUMAN FIREWALL

Empower Your People

Your team is your first line of defense. Training is key.

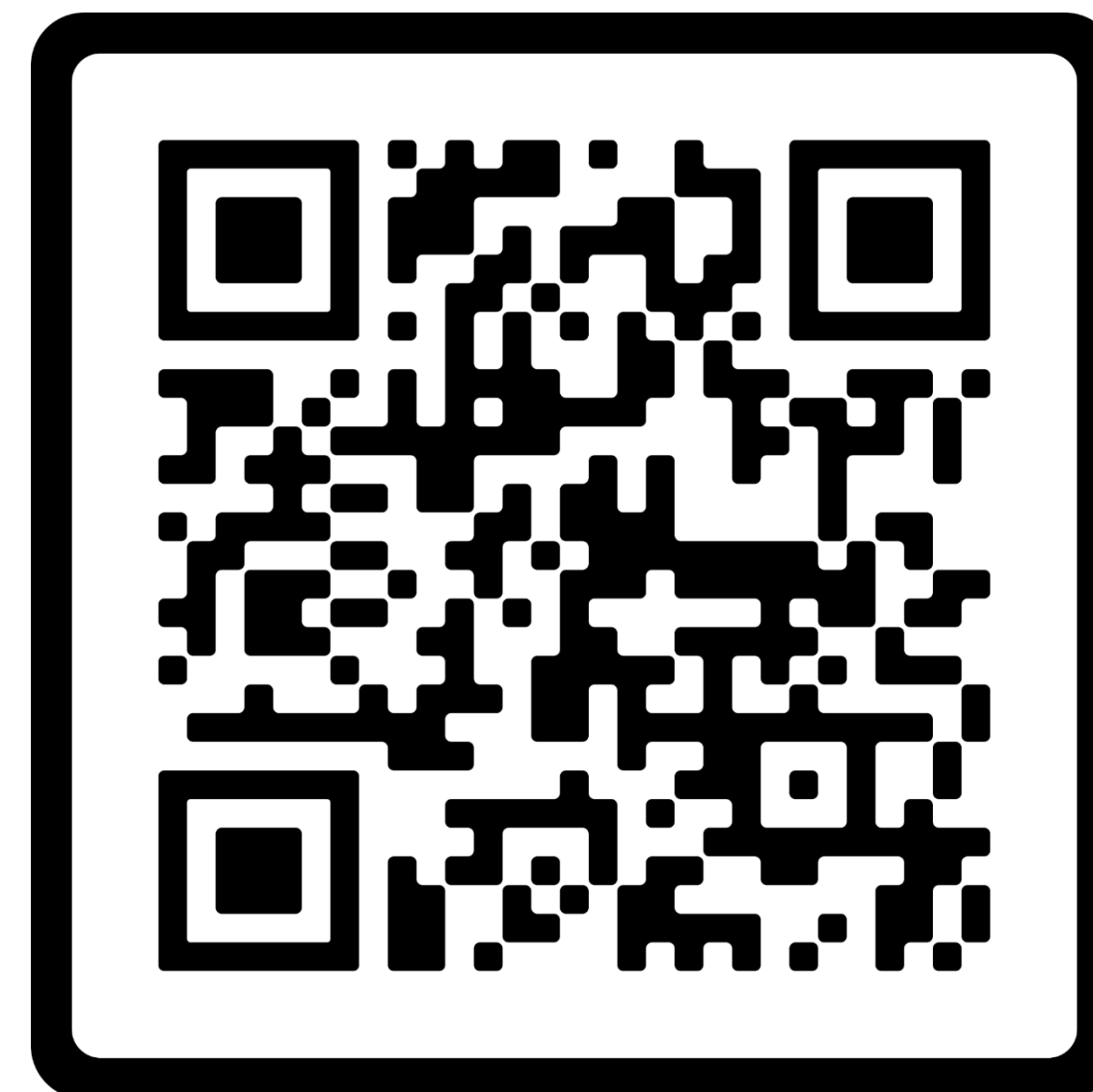
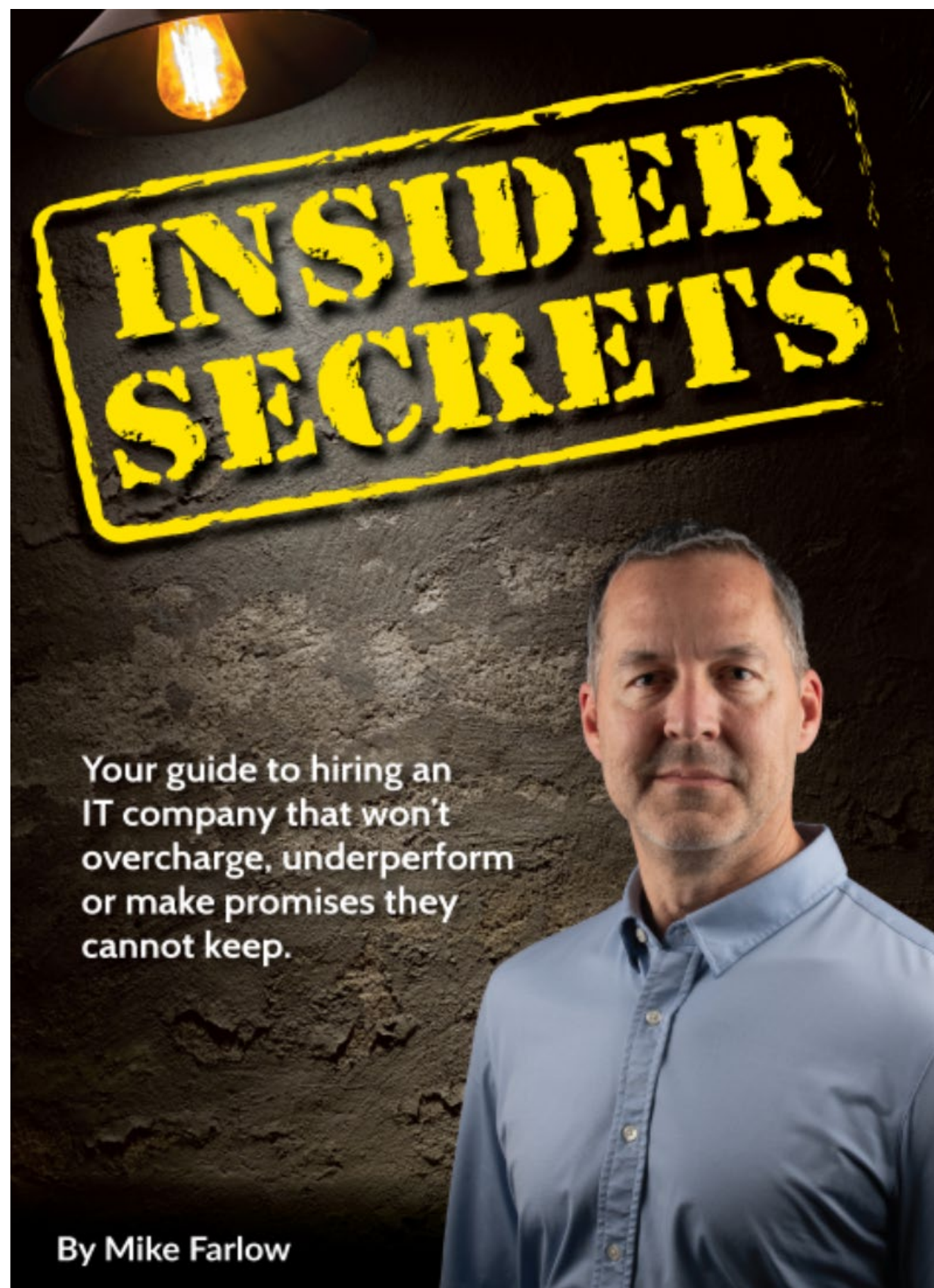
Adopt a Zero Trust Mindset

Never trust. Always verify.

Stay Vigilant

Review and update policies.
Adopt a Cybersecurity Culture.





The 9 Elements of FTC Safeguards Rule

Thank You!



Rafe Martin

CRO, CCRP

rafe@comtechnnc.com

336 -338 -7328