Bank Director

Breakout 1:
Bank Against Emerging Cyber and Fraud Risks

Justin Corey
NFP

Lauren Kim
NFP

#BDAudit24

NFP
An Aon Company

Bank Against Emerging Cyber and Fraud Risks

Lauren Kim
Managing Director, FIG

Justin Corey
Senior Vice President, FIG

June 12, 2024

Financial Institutions Group
Current Locations and Client Distribution

By The Numbers

30+ employees
7 offices

50+ global carrier partners

3 dedicated FI coverage attorneys

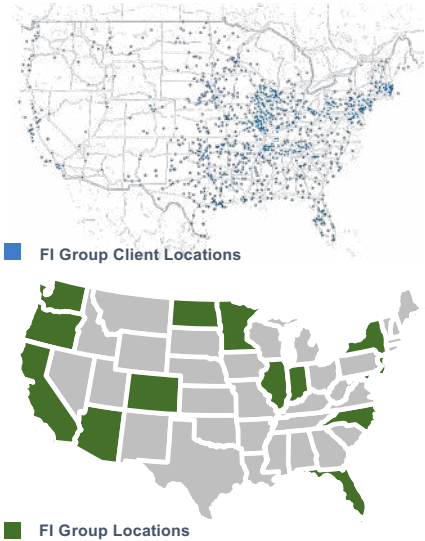
2 FI cyber risk specialists

500+ financial institution clients in all 50 states

190+ loan portfolio clients

350+ commercial bank and credit union clients

Part of NFP: **7000+** employees and **$2.2B** revenue



Cyber and Fraud Risks in 2024

Threats Driving the Cyber Market

Claims severity and frequency has caused underwriters to reevaluate how they approach risk. A client's ability to showcase strong investments to cyber security hygiene is more important than ever. To best showcase controls, it is essential to have an understanding of the top threats driving the market prior to completing a cyber application.

Malicious Attack

- Credential access remains top tactic for network infiltration. Carriers have almost universally adopted MFA as a required security tool to access cyber liability insurance.
- NFP reported 18% of claims in 2023 involved a ransom demand and 50% included a network compromise.
- Read up on the latest large attacks to hit headlines here! (source powered by NFP partner NetDiligence)

The Human Element

- 82% of cyber incidents involve the human element.
- Phishing Links continue to be the most reported access method (Kroll Report 2023).
- Email compromise remains the top threat facing companies.
- Social Engineering tactics continue to enhance with use of Artificial Intelligence. Check out NFP Insight Paper on Company $25M loss due to Deepfake technology.

Privacy Regulation

- BIPA - Litigation and settlements continue to rise.
- Video Privacy Protection Act – litigation gained traction regarding the use of pixel tracking tools on social media websites without user consent.
- SEC issues new Cyber Disclosure requirements
- CCPA announced its second settlement on 2.29.24 for wrongful collection
- Other notable regulations: GDPR, New Jersey Privacy Law (eff. 2025), NY FI Regulation, HIPPA.

Systemic Loss

- Event impacting critical applications, software or infrastructure utilized by organizations.
- 2023 MoveIt breach showcased resurgence in aggregate risk and supply chain vendors are attractive targets.
- A 2023 research study found 98% of organizations have at least one third party vendor that experienced a cyber event.
- Carriers affirmatively define cyber war.

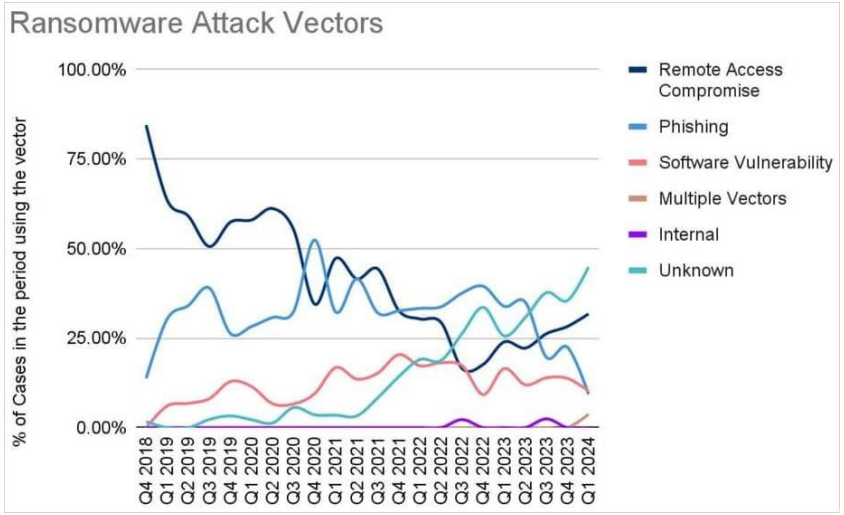
Recent Ransomware Trends

Record Amount Paid to Ransomware Actors in 2023

- The amount paid to ransomware actors is higher than ever before, reaching $1.1 billion last year.
- This is due to ransomware gangs hitting more organizations by escalating their attack frequency and demanding more substantial figures for not exposing stolen secrets and providing victims with a decryption key.

Decreases in 2024

- Ransomware actors have had a rough start this year, as statistics show companies are increasingly refusing to pay extortion demands.
- A record low of 28% of companies paid ransom in Q1 of 2024.
- This decrease is due to organizations implementing more advanced protective measures, mounting legal pressure not to meet the cybercriminals' financial demands, and cybercriminals repeatedly breaching promises not to publish or resale stolen data if a ransom is paid.



- Regarding initial infiltration methods, there's a rising number of cases where this is unknown, reaching nearly half of all reported cases in the first quarter of 2024.
- From those that have been determined, remote access and vulnerability exploitation play the largest role in infiltrating systems.

NFP An Aon Company

Social Engineering in Scams and Frauds

Common Methods

Phone call to change accounts, especially spoofing legitimate numbers through enterprise platforms like Zoom, Teams, and Skype.

Email messages to change contact information.

Callback phishing: Threat actor sends a fake invoice with no malicious content other than a phone numbers. Victims call the number and are engineered into downloading a remote access tool the threat actor can use to steal data.

Advanced Methods

- Use of deepfakes for phone calls: In a recent example, LastPass reported an incident where a threat actor created a deepfake voicemail using the voice of their CFO. Luckily, the call came through WhatsApp, which the employee recognized as unusual.
- AI – personal manipulation – generated personas that interact with targets through automated systems like chatbots or virtual assistants
- Bypassing multi-factor authentication by:
  - SIM swapping: Social engineering or using an insider with a phone company to get a phone's SIM transferred to a phone controlled by the threat actor.
  - Push spamming: Sending many push notifications at once, relying on the user to accidentally accept one.

Social Engineering Schemes Involving Email

Bogus/Altered Invoice Scheme

- Fraudster compromises email account
- Business has an established relationship with third-party
- Fraudster asks to wire funds for payment of an invoice to an alternate, fraudulent account

CEO Fraud

- Fraudster identified themselves as a high-level executive (possibly through spoofed email)
- Initiate a wire transfer to an account they control, or request gift cards are sent

Account Compromise with Wire Fraud

- Employee email account is hacked and used to make requests for invoice payments to an account controlled by the fraudster
- Messages can be sent to multiple vendors on the employee's contact list
- Fraud usually discovered when vendors follow up on the invoice that was not paid

Data Theft

- Fraudster compromises an email account with the goal of finding sensitive data
- Targeting employees with specific roles (HR, payroll, etc.)
- May sync account or set up forwarding rule to obtain the contents
- Even without a compromised accounts, fraudsters can request Personal Identifiable Information (PII) from executives/other individuals through spoofing

Credential Harvesters

- After account compromise, fraudster sends spam emails to an individual's entire address book
- Contains a malicious attachment or link to a credential-harvesting website

Focusing on Catastrophic Risk

As the world becomes more dependent on technology, insurer concerns regarding systemic and catastrophic risk has increased. It is important to understand the core catastrophic exclusions in your cyber policy. The war exclusion has the most variability dependent on carrier and syndicate backing.

War Exclusion

To date, the war exclusion has only been used to deny cyber-related coverage on a property policy. That said, we expect the war exclusion to be the most debated and revised by insurers in 2024. Several carriers, including the Lloyd's Market Association, have noted insureds should expect significant changes to the war exclusion language for clients purchasing (or renewing) cyber coverage in 2024. Clients should carefully review changes to the war exclusion language, along with the cyber terrorism carveback on each renewal.

Natural Perils

We tend to not pay too much attention to natural perils on a cyber policy. However, they have come under scrutiny over the past few years. Some insurers are expanding the scope of the exclusion to apply to third-party liability sections, in addition to its traditional application against a first-party insuring agreement. Carvebacks for natural perils are also being challenged or removed given the potential for a catastrophic event.

Infrastructure

Each year, our day-to-day operations have become more dependent on internet and satellite infrastructure to operate. More and more businesses networks are fully cloud based, rather than previous on-premise models. These changes have made revisions to the infrastructure exclusion commonplace on a cyber policy, most notably by broadening the definition to include network services, telecommunications, internet and satellites.

Government Actions

In the wake of the COVID-19 pandemic, there has been scrutiny regarding the implications of widespread government actions, particularly potential orders around computer and network shutdowns. Due to this, some insurers have broadened government action exclusions to affirmatively include the shutdown of computer systems or related networks.

Legal Landscape – Cyber

Hacking Group Behind MGM Attacks Now Targeting Financial Institutions

- The hacking group accused of disrupting casinos and hotels at MGM Resorts International last year is engaged in a new campaign targeting banks and insurance companies, according to cybersecurity researchers. Scattered Spider has targeted 29 companies since April 20 and successfully compromised the systems of at least two insurance companies, including Visa Inc., PNC Financial Services Group Inc., Transamerica, New York Life Insurance Co. and Synchrony Financial.

International Monetary Fund (IMF) Cyber Breach

- The International Monetary Fund (IMF) experienced a cyber incident this year, which was detected on February 16, 2024. The IMF has 190 member countries and works to improve growth and prosperity internationally.
- A subsequent investigation, with the assistance of independent cybersecurity experts, determined that 11 IMF email accounts were compromised. The impacted email accounts were re-secured. While there were no indications of any financial attack or loss, the investigation for the incident is still underway. Microsoft Office 365 accounts were targeted by a Russia-linked intelligence organization in January 2024. However, the IMF has stated that the “incident does not appear to be part of Microsoft targeting.“ and was specifically targeted at individuals.

SEC Cyber Enforcement Top Concerns for Compliance Pros

- More than 40% of compliance personnel from asset management, investment adviser and private markets firms are concerned about how the U.S. Securities and Exchange Commission will enforce its new cybersecurity rules, according to findings from a recent survey.
- Results from the 2024 Cyber Benchmarking survey indicated that almost half of respondents listed uncertainty about enforcement as one of their top two concerns about the rules, which was the top choice in a list that also included compliance, costs and increased risk of cyber attacks, among others.
- In July 2023, the SEC adopted a final rule requiring public companies to make certain public disclosures regarding material cybersecurity incidents. The rule covers incident-specific disclosures of significant cybersecurity breaches and annual disclosures about companies' cybersecurity risk management, strategy and governance practices. The final rule gives companies four business days to disclose material cybersecurity incidents from the time the companies determine that an incident was material.

Healthcare Cyber Attacks Showing Vulnerability

- In February of 2024, UnitedHealth suffered a major DDoS cyber attack on their systems forcing the company to disconnect more than 100 systems. The hacking groups BlackCat and RansomHub have claimed responsibility for the attacks thus far, claiming to have taken over 10 Terabytes of UnitedHealth data. The attack capitalized on the cyber vulnerabilities across the company’s systems, with Sen. Bob Casey (D., Pa.). remarking “I think it’s clear that if United had stronger defenses, like MFA, then this could have gone very differently.”
- The attack is expected to cost UnitedHealth around $1.6 Billion throughout the 2024 year, excluding further potential litigation costs or regulatory fines. It is essential for Insureds to make sure all systems are up to date with proper cyber safeguards and that their 3rd party vendors are establishing their own protections with sensitive data.

New SEC Rules

The SEC approved new cybersecurity rules in July 2023.

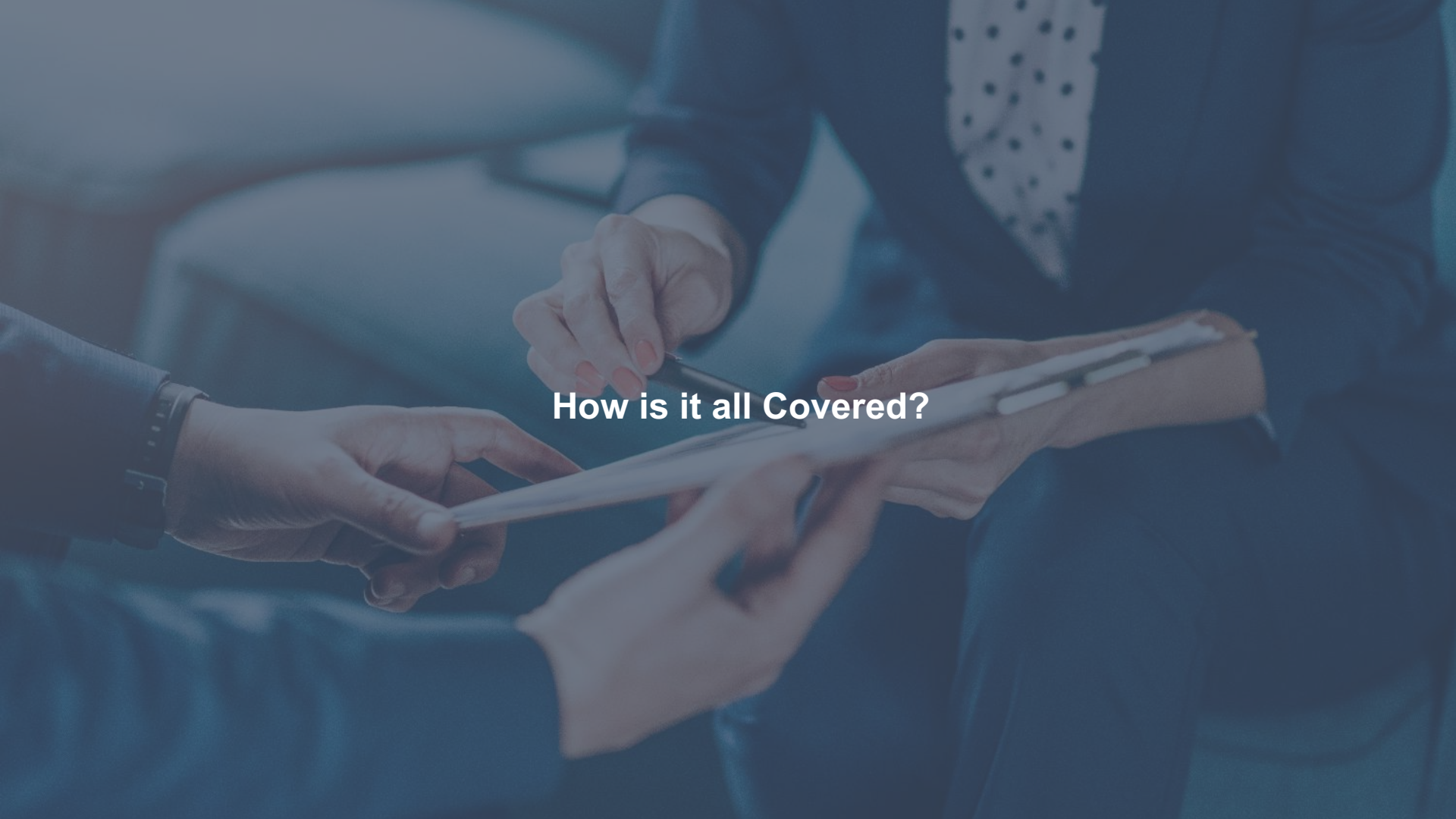
The key features of the guidelines require that companies:

(i) disclose material cybersecurity incidents they experience within four days

(ii) disclose on an annual basis material information regarding their cybersecurity risk management and governance.

These new rules could create circumstances that could increase the litigation risk for banks experiencing a cybersecurity incident.

The mandated disclosures concerning board cybersecurity governance practices, particularly with respect to **board oversight processes concerning cybersecurity**, could also contribute to securities litigation.

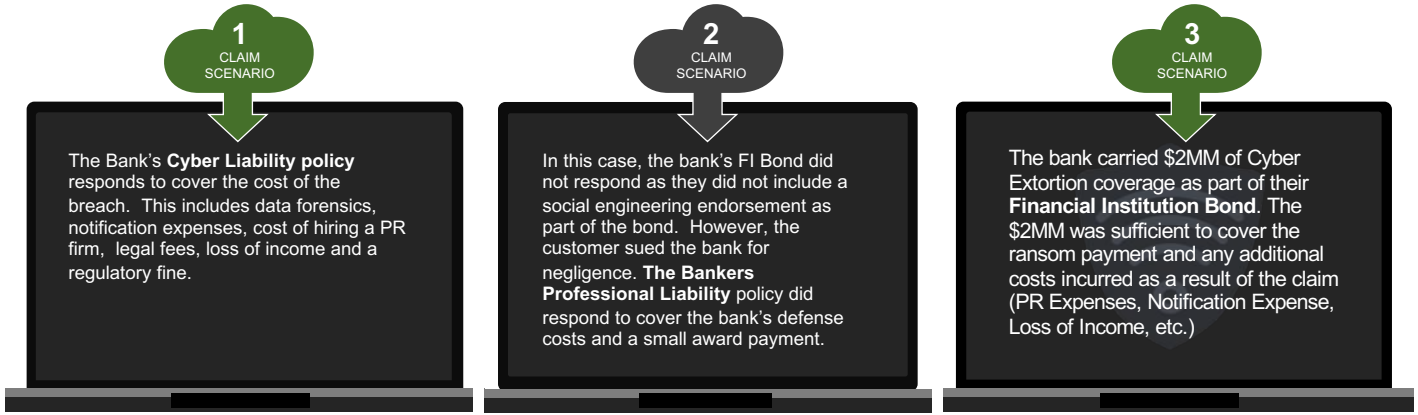

How is it all Covered?

Cyber Crime, Cyber Liability, or Professional Liability?

So, what's the difference? When compared to most other industries, Banks have more policies and variables to consider when assessing their cyber insurance. Depending on the details of the claim, coverage could potentially be found within 3 different policies. Here are 3 claim examples to help illustrate the difference.

Cyber Crime, Cyber Liability, or Professional Liability?

OUTCOME: Each claim was covered under a different policy! The bank needs to focus on their whole insurance program (not just the Cyber Liability policy) when addressing Cyber risk. Cyber Liability, Bankers Professional Liability and FI Bond policies are all critical components of a strong Cyber Insurance program. In fact, the majority of Computer Systems/Cyber claims are related to cyber crime and covered on the FI Bond.



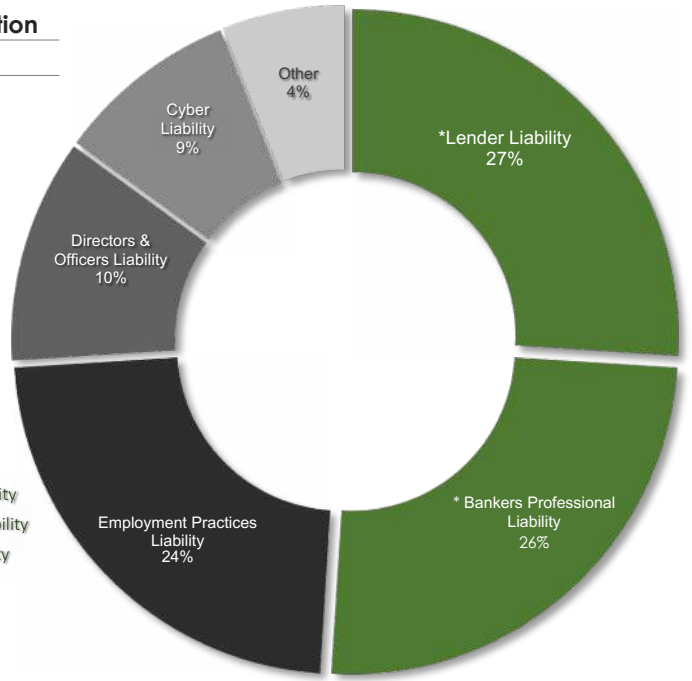
2023 Bank Claims Distribution: Management Liability

Management Liability Claims Distribution

Per Lines of Coverage

*SOURCE: ABAIS, NFP, TRAVELERS, INTACT, HALES REPORT

Bankers Professional Liability, which includes Lender Liability and Wire Transfer Liability, accounted for 53% of all Management Liability claims in 2023. Because BPL encompasses such a broad range of exposures, we ask that our customers review this coverage at each renewal to ensure they are comfortable with their limit.



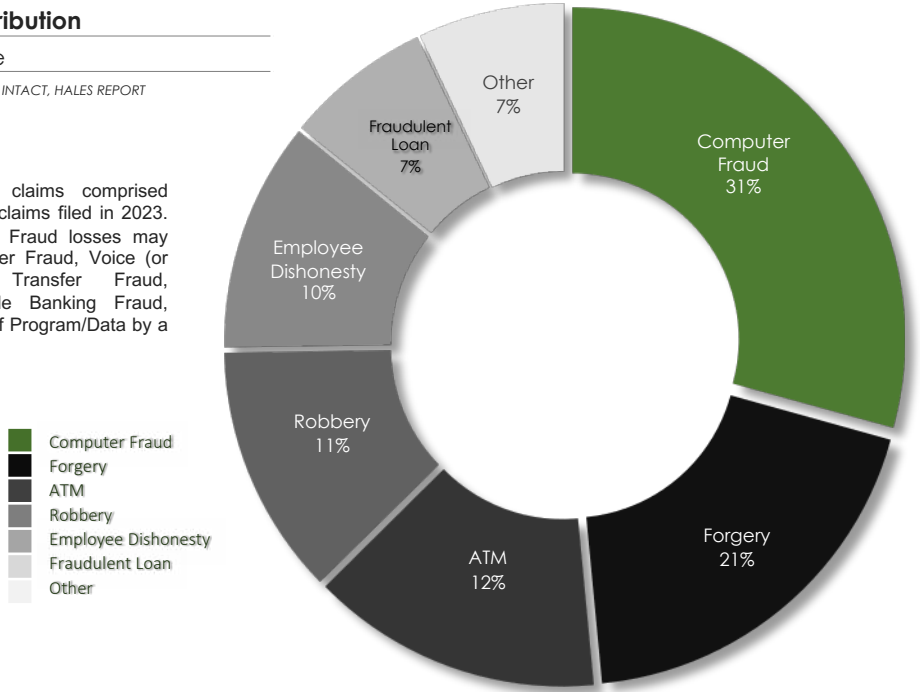
2023 Bank Claims Distribution: Financial Institution BOND

FI Bond Claims Distribution

Per Lines of Coverage

*SOURCE: ABAIS, NFP, TRAVELERS, INTACT, HALES REPORT

Computer Fraud claims comprised 31% of all FI Bond claims filed in 2023. Common Computer Fraud losses may include Wire Transfer Fraud, Voice (or Email) Initiated Transfer Fraud, Unauthorized Mobile Banking Fraud, and/or Destruction of Program/Data by a Hacker or Virus.



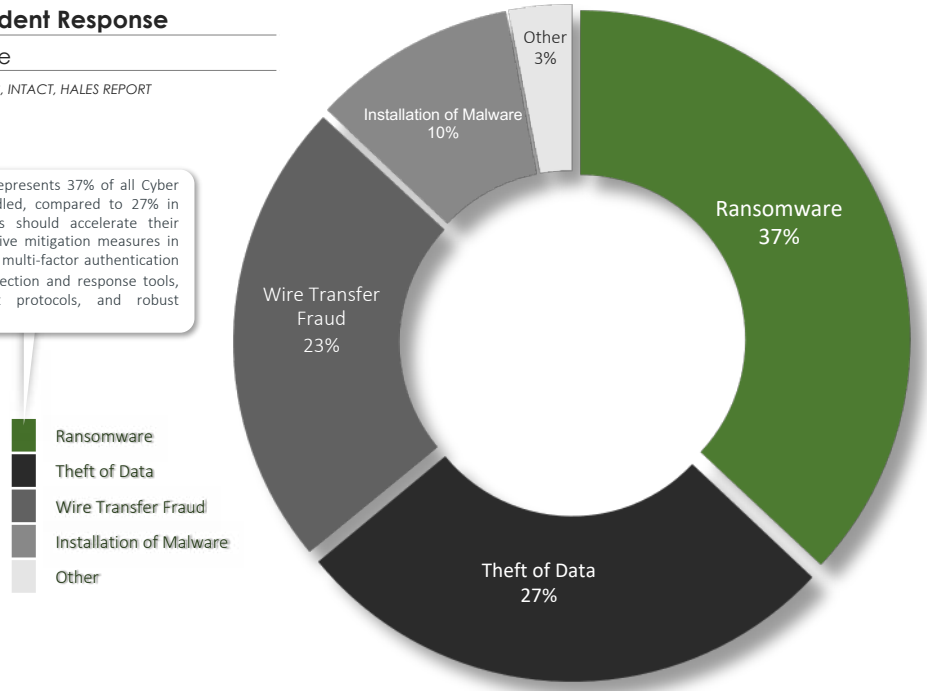
2023 FI Cyber Incident Response Trends

Cyber Liability Incident Response

Per Lines of Coverage

*SOURCE: ABAIS, NFP, TRAVELERS, INTACT, HALES REPORT

Ransomware now represents 37% of all Cyber Liability claims handled, compared to 27% in 2020. Credit Unions should accelerate their efforts to put effective mitigation measures in place. These include multi-factor authentication (MFA), endpoint detection and response tools, patch management protocols, and robust backup plans.



Sample: Management Liability Benchmarking
Based on ABA and NFP 2022 Peer Data*

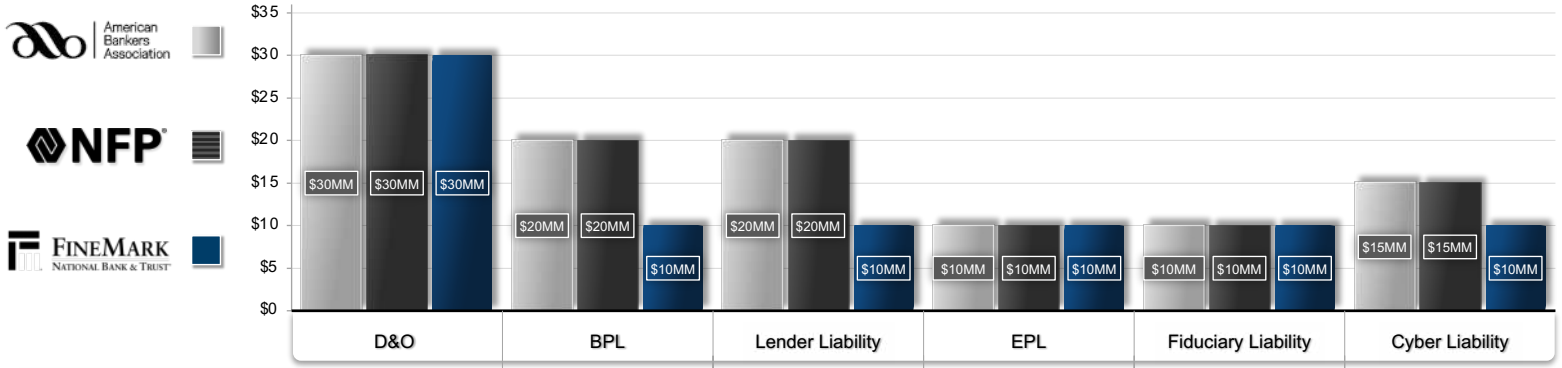
Management and Professional Liability

Peer Group Average Limits

***FDIC ASSET PEER GROUP: $3 Billion - $5 Billion**

**SOURCE: FDIC, AMERICAN BANKERS ASSOCIATION, NFP*

TOTAL ASSETS :	$3,800,338,000
ASSET PEER GROUP:	$3B - $5B
NUMBER OF PEERS:	113
PEER AVERAGE ASSETS	$4,043,077,000



	D&O	BPL	Lender Liability	EPL	Fiduciary Liability	Cyber Liability
American Bankers Association	$30,000,000	$20,000,000	$20,000,000	$10,000,000	$10,000,000	$15,000,000
NFP Recommended	$30,000,000	$20,000,000	$20,000,000	$10,000,000	$10,000,000	$15,000,000
FineMark National	$30,000,000	$10,000,000	$10,000,000	$10,000,000	$10,000,000	$10,000,000

Sample: Management Liability Benchmarking
Based on ABA and NFP 2022 Peer Data*

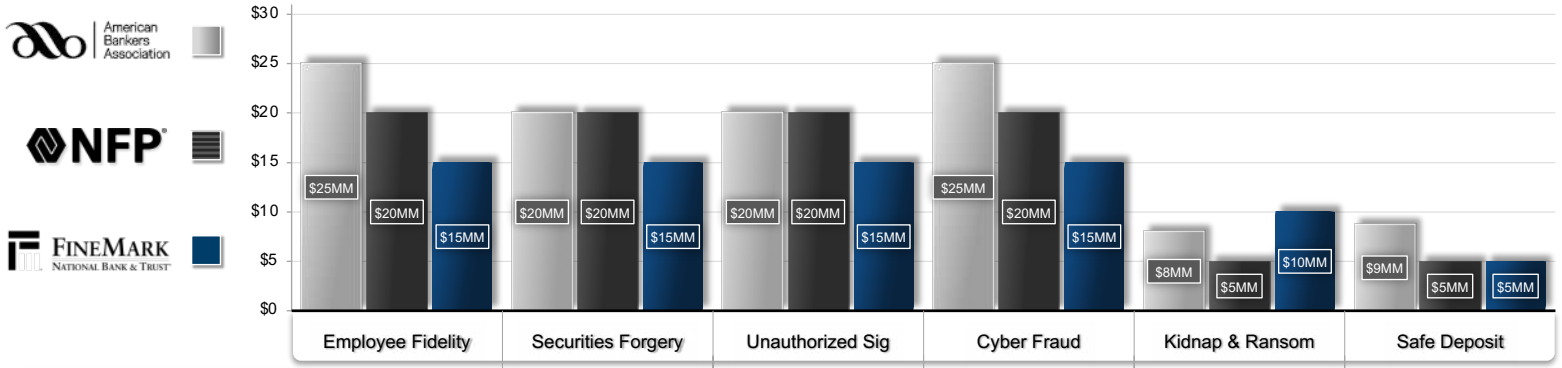
Financial Institution Bond

Peer Group Average Limits

***FDIC ASSET PEER GROUP: $3 Billion - $5 Billion**

**SOURCE: FDIC, AMERICAN BANKERS ASSOCIATION, NFP*

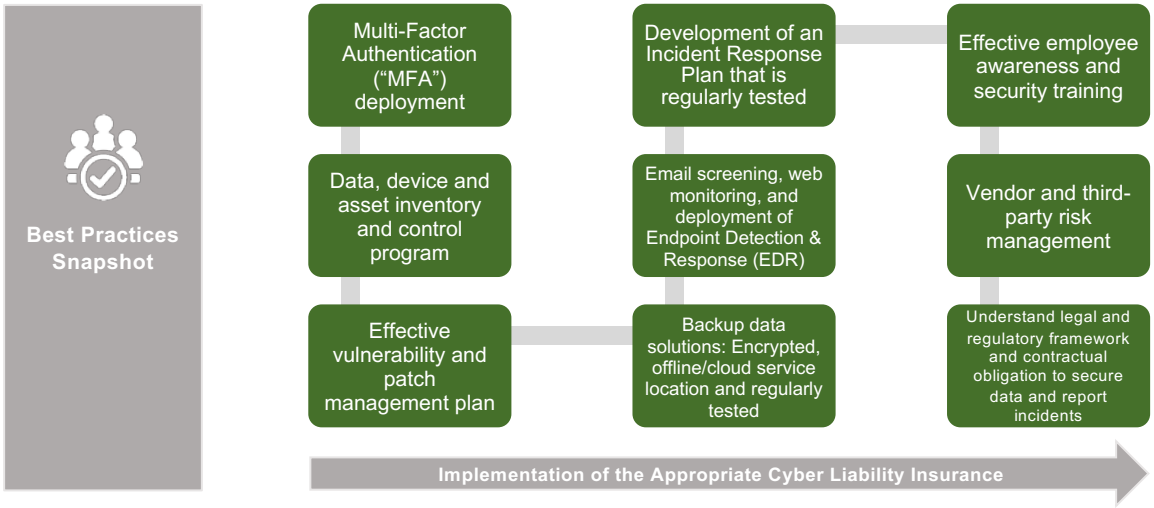
TOTAL ASSETS :	$3,800,338,000
ASSET PEER GROUP:	$3B - $5B
NUMBER OF PEERS:	113
PEER AVERAGE ASSETS	$4,043,077,000



	Employee Fidelity	Securities Forgery	Unauthorized Sig	Cyber Fraud	Kidnap & Ransom	Safe Deposit
American Bankers Association	$25,000,000	$20,000,000	$20,000,000	$25,000,000	$8,000,000	$8,700,000
NFP Recommended	$20,000,000	$20,000,000	$20,000,000	$20,000,000	$5,000,000	$5,000,000
LiveOak Bank	$15,000,000	$15,000,000	$15,000,000	$15,000,000	$10,000,000	$5,000,000


The Basics of Cyber Insurance

Market Focus - Risk Mitigation and Controls



Cyber Security and Internal Controls

1

Minimum standard of security required by all Cyber Liability insurance carriers at start of 2024. If any of these basic risk controls have not been implemented, we strongly recommend this be completed ASAP (before your next Cyber Liability renewal at the very latest).

2

Additional controls that are not currently a requirement but areas worth considering. These will make the bank a more attractive risk to an underwriter which would likely lead to a savings in premium.

3

Controls over and above level 2 and well above industry standards. Not critical today but constitutes the highest level of security measures currently available. Ensures the most favorable Cyber Liability terms and premium.

Cyber Security and Internal Controls

1

- Multifactor authentication (MFA) for employee email
- MFA for remote access
- MFA for privileged accounts/privileged access
- Offsite (preferably offline) backups of critical data.
- Deploy an endpoint detection and response (EDR) solution on all managed endpoints
- Employee cybersecurity training, including phishing simulations

2

- Strong email filtering tools
- Privileged access account security measures
- End-of-life (EOL)/unsupported software and hardware segregated from the network,
- Segmentation of your computer network by operational function, data classification and operational risk
- Local domain control turned off on all owned managed endpoints

3

- Password management
- Detailed asset footprint of particular service accounts with domain credentials, services and monitoring
- Security information and event monitoring (SIEM) tool
- Data loss prevention (DLP) tool
- Follow an information security framework
- Maintain 24/7 Security Operations Center internally or externally

Cyber Security and Internal Controls

Baseline Requirements Of Cyber Liability Insurers In 2024

1. Secure remote network access via MFA for all remote access
   a) Remote access to your network, applications, systems by employees, contractors and network service providers
   b) Remote access to your data on cloud-hosted systems (i.e., software as a service, backups, etc.)
   c) Remote access to your email, O365, Google, etc.
   d) To access your VPN
   e) On-premises access for privileged users
2. Backup and recovery assessment
   a) Air-gapped backups, taking into account cadence, segregation, testing and redundancy
3. Conducting regular employee infosec training, including quarterly phishing simulations
4. Endpoint protection (endpoint detection and response or EDR)
5. Incident response plans that include ransomware readiness (underwriters will want to know the plans have been tested as well)
6. Timely, consistent patch management protocols
7. Secure email configurations — DMARC, SPF, DKIM
8. Filtering inbound web traffic
9. Implementing least-privilege administrative models
10. Internal and external vulnerability scanning and secure remote desktop configurations
11. Segregating unsupported end-of-life software from primary network
12. Requiring callback verification for authorization of wire payments and any requested changes in routing information by third parties (call the previously known number on file, not a number provided via email request)

Anatomy of a Cyber Liability Claim

Insuring Agreement	Security & Privacy Liability	Privacy Regulatory Defense, Awards and Fines	Media Content	Event Management	Cyber Extortion	Network Interruption
What is Covered?	Defense costs and damages arising out of a data security or privacy incident to a third party, including fines and/or penalties arising out of PCI-DSS non-compliance.	Coverage for claim expenses and regulatory damages as a result of a privacy regulatory action (violations of GDPR, CCPA, and/or BIPA).	Defense costs and damages for third party claims alleging libel, slander, copyright/trademark infringement, invasion of privacy, etc. arising out of all content distributed by a company.	Costs incurred arising from a cyber incident, including costs to hire expert privacy counsel to determine any legal obligations, costs to retain a forensic firm to investigate the cause of the event, notification and call center costs as well as public relations.	Money paid by you, including cryptocurrency with the insurer's consent to resolve a cyber security threat and costs to investigate the cause of the threat.	Loss of income and extra expenses incurred by you following a security or system failure of your computer systems, subject to a waiting period and/or monetary retention.
Types of Claims	Privacy Class Actions: • Neiman Marcus • Anthem PCI-DSS Related Litigation / Demands • Target • Home Depot	Regulatory Actions including: • State Attorneys Office of Civil Rights under HIPAA • EU Countries under GDPR	Most common examples include demands to cease and desist using imagery and/or claims for copyright or trademark infringement.	Most common examples include hiring a forensic investigation specialist to conduct an investigation at an hourly rate. Setup and implementation costs of notifying individual consumers, including setting up new call centers to handle volume.	Most common examples include extortion demands following a ransomware attack.	Merck and Maersk impacted by NotPetya ransomware Nation-state attacks against Sony Pictures Entertainment Royal Bank of Scotland 2012 outage Azure or AWS or other data center outage impacts your operations

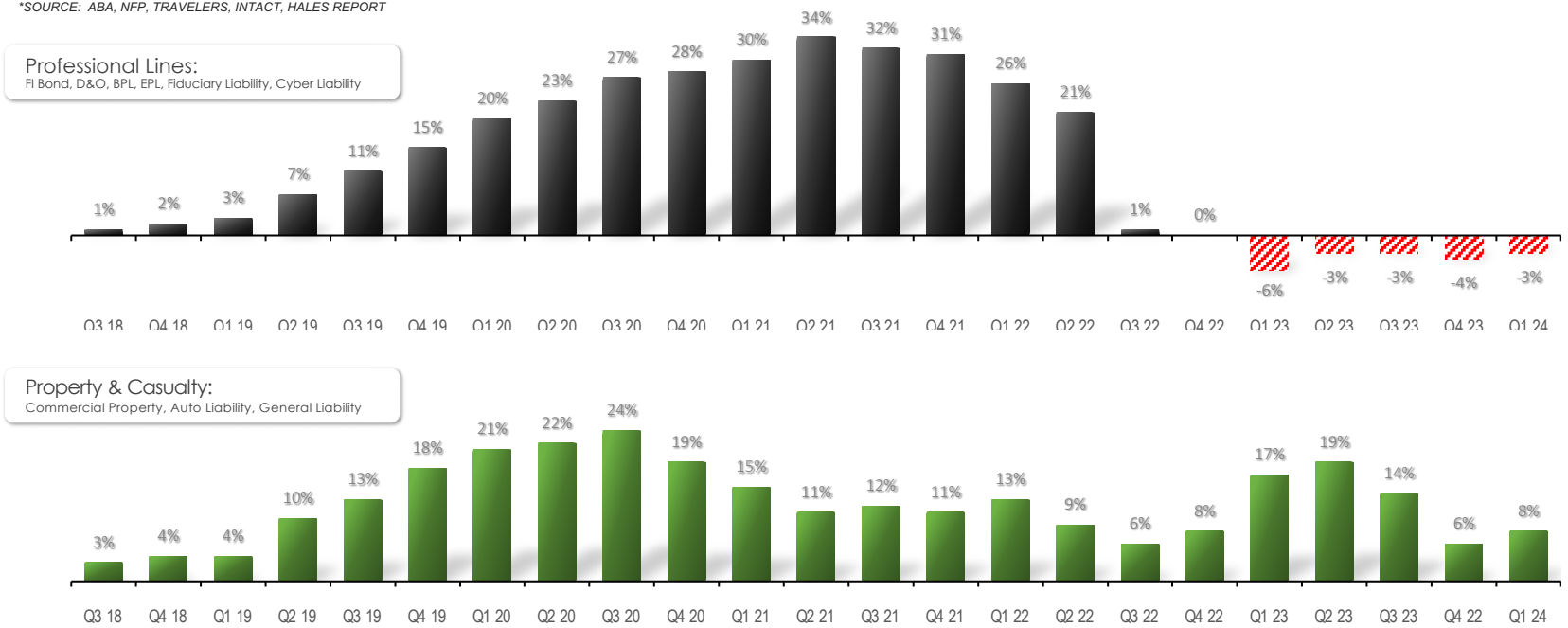
SOURCE: ABA, NFP

Premium Trends
Historical FI Pricing by Core Coverage Line (3Q18 – 1Q24)

Financial Lines Pricing Trends

Per Lines of Coverage

SOURCE: ABA, NFP, TRAVELERS, INTACT, HALES REPORT



NFP.com