Assessing and Managing Your Total Cost of Cyber Risk

December 1, 2021

Tom Hunt, CTP
Director, Treasury Services
AFP

Thomas Reagan
US & Canada Cyber Practice Leader
Marsh

Scott Stransky
Managing Director
Cyber Risk Analytics Center
Marsh McLennan

AGENDA

- Overview of cyber analytic sources
- Loss modeling
- Updates in cyber insurance
- Aligning risk management strategies to cyber exposure
- Q&A

Cyber Ranked the Most Challenging Risks to Manage

ASSOCIATION FOR FINANCIAL PROFESSIONALS

Top ranked risks over a three-year horizon (Percentage of organizations who ranked risks in top three)

47% **CYBER SECURITY**

- Ransomware; Phishing; etc.

37% **STRATEGIC**

- Competitors; Industry disruptions; etc.

34% **BUSINESS OPERATIONS INTERRUPTIONS**

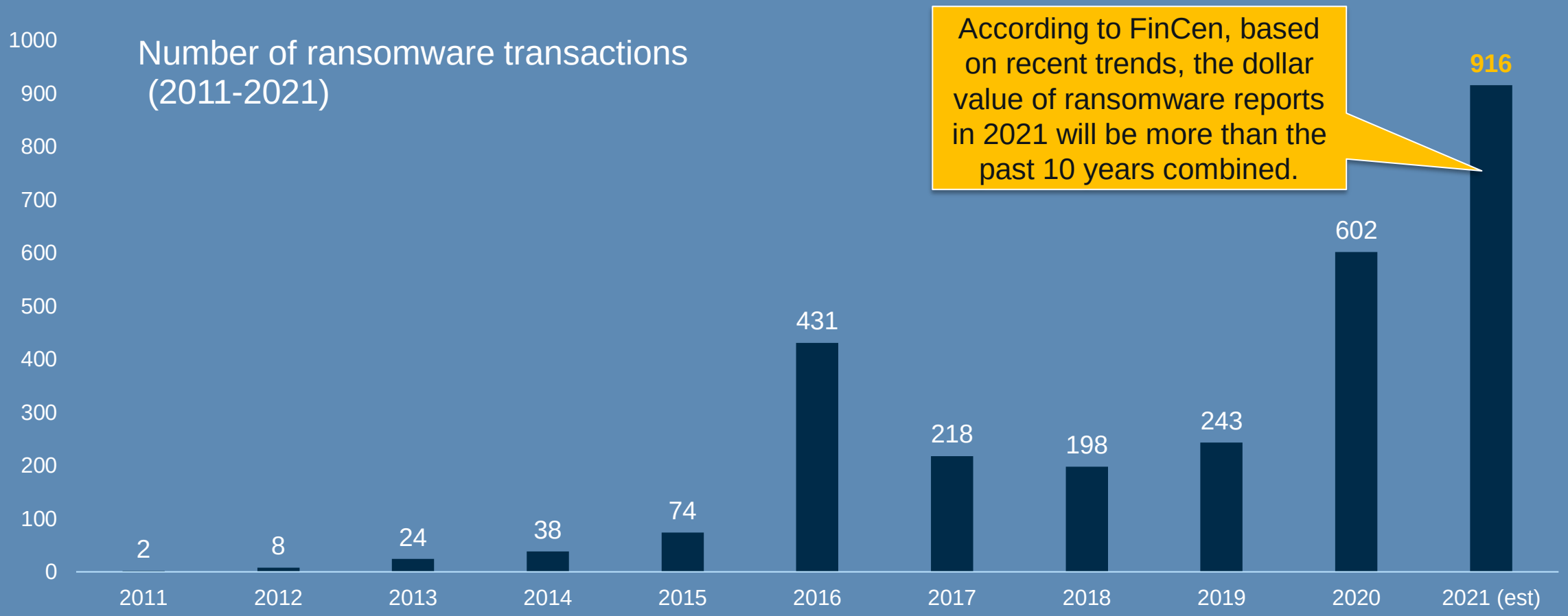
- Supply chain disruptions; Production interruptions; etc.

33% **FINANCIAL**

- Credit; Liquidity; etc.

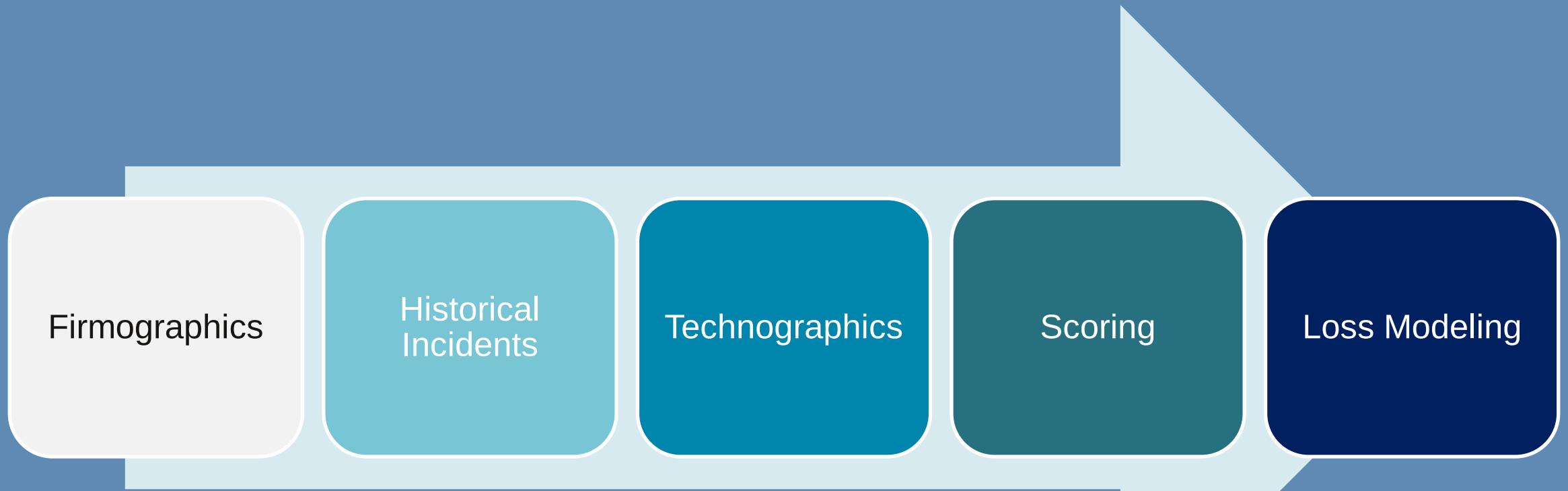
Source: 2021 AFP Risk Survey, Association for Financial Professionals with support of Marsh McLennan

Rising financial impact of cyber crime



Source: Financial Trend Analysis (fincen.gov), Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021

Five Sources of Cyber Analytics Data



Firmographics

Metrics including:

- Revenue
- Employee count
- Industry
- Geographic location(s)
- Company hierarchy

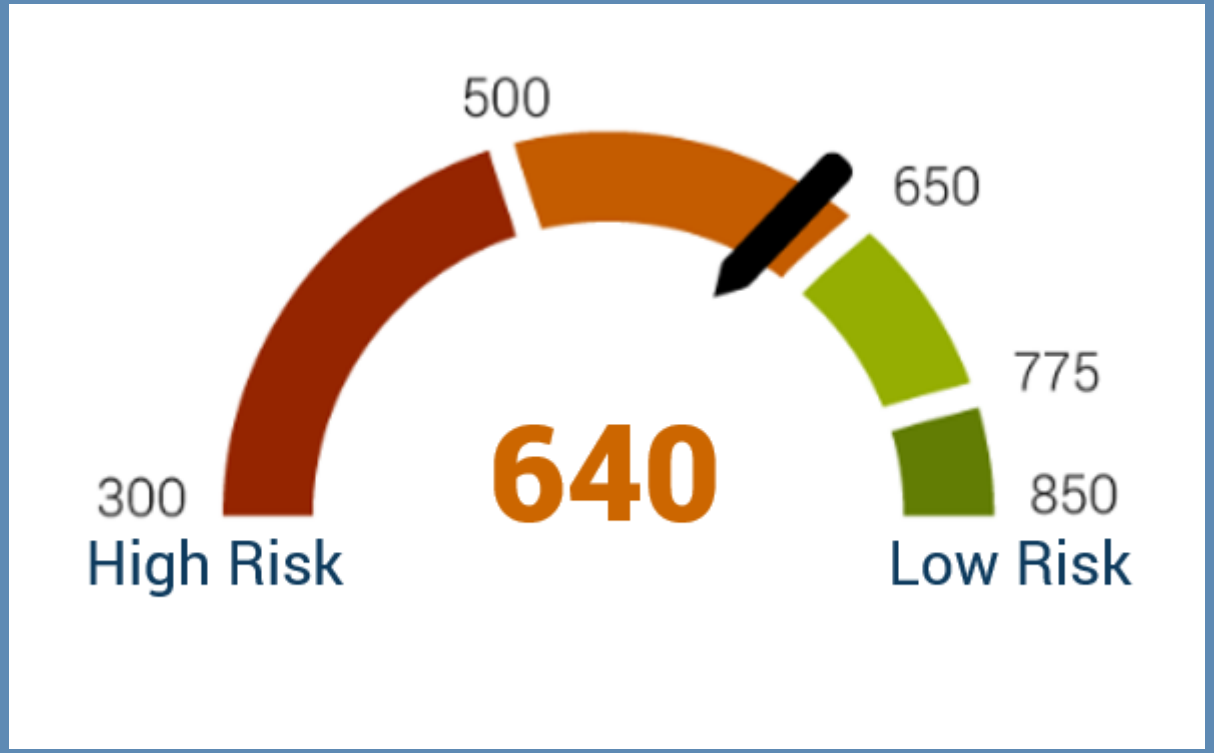
Historical Incident Data

Technographics

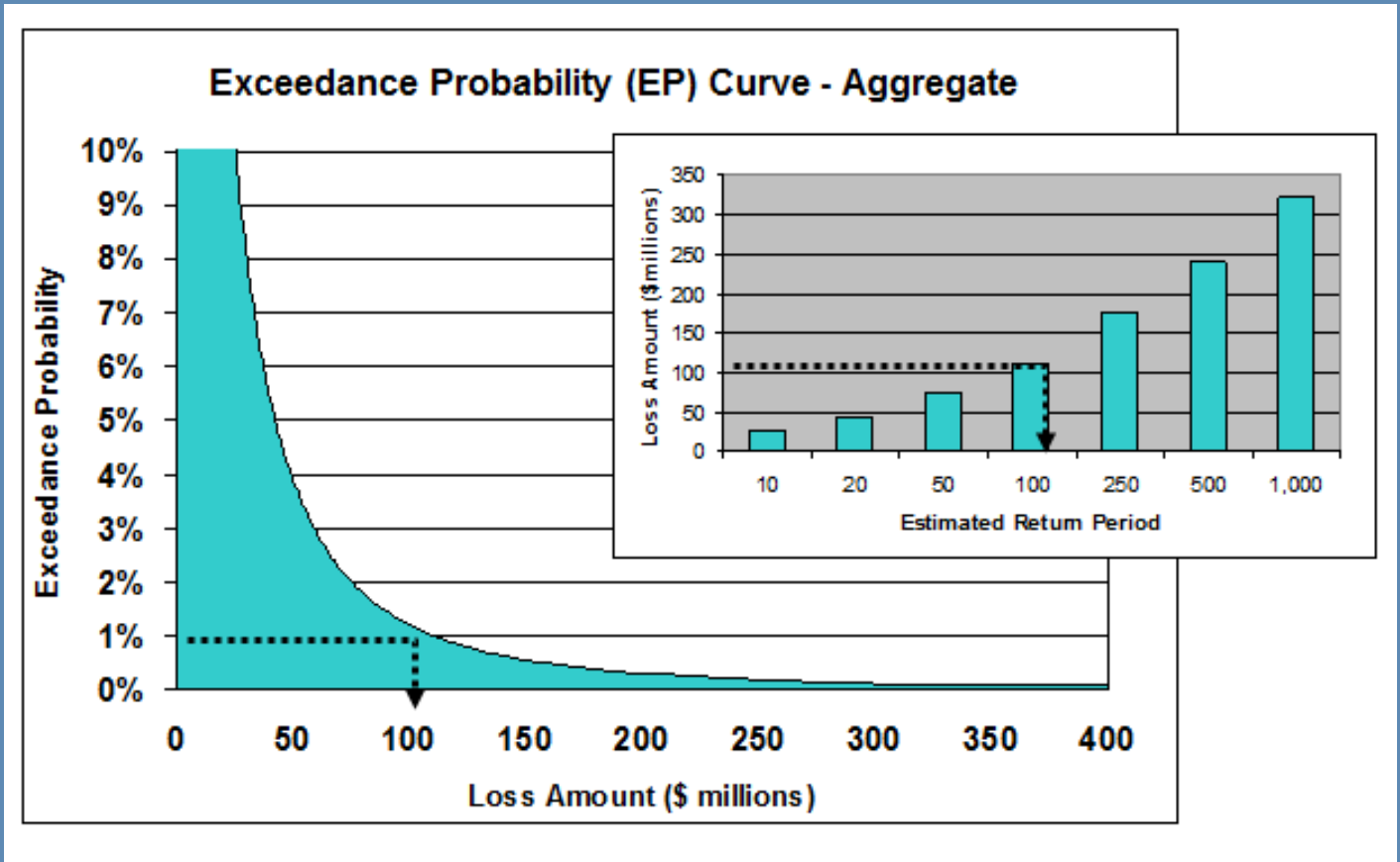
Outside-in

Inside-out

Scoring



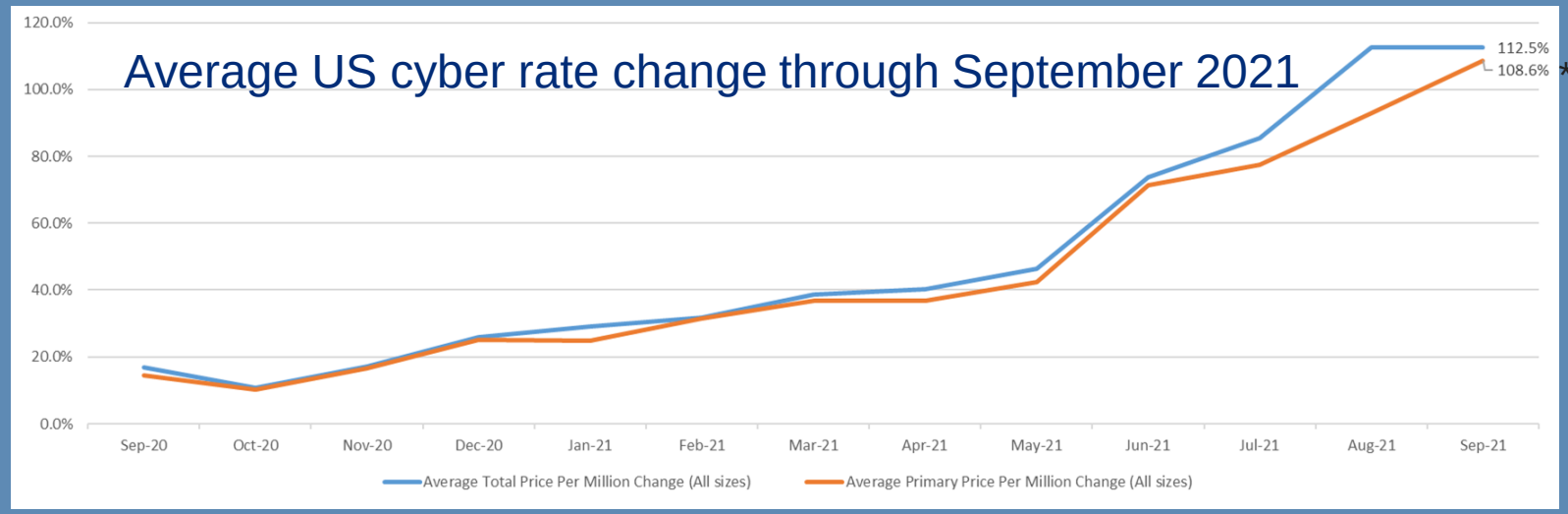
Bringing it together: Loss Modeling



Various types of loss models:

- Scenario models
- Probabilistic models
- Losses for individual cyber perils (ex: ransomware)
- Correlated models
- Aggregation models

Cyber Insurance: Rising Rates Drive Hard Decisions



Sept 2021 renewals*	1st Quartile	Median	Average	3rd Quartile
Total price per mil	46.2%	88.3%	112.5%	128.3%
Primary price per mil	38.9%	78.1%	108.6%	126.6%

*Programs that renewed with expiring limits | Excludes 30% of Sept. renewals due to limit changes.

All Sept 2021 renewals**	Median	Average
Total price per mil	97%	174%
Primary price per mil	83%	155%

**Data includes 30% of renewals with limit changes:
23% reduced limits
7% increased limits

Takeaways:

1. Capacity changes are driven by insureds minimizing increases as well as less available capacity.
2. Clients who saw outsized increases were forced to consider reduced limits.

Source: Marsh Global Placement & Specialties, Data and Analytics, PlaceMAP Marsh Clients

Cyber insurance market summary

ASSOCIATION FOR FINANCIAL PROFESSIONALS

Claims

Claims frequency and severity remain high

Ransomware, systemic risk, and regulations continue to drive concern

Tech E&O and Media now also a concern

Rates

Losses accelerating pricing pressure even on loss free accounts with good controls

Expect increases to continue into 2022

Capacity & Attachment

Insurers aggressively managing global capacity and increasing SIRs

Distressed classes and large towers may see capacity challenges

Underwriting

3rd parties being used to externally scan environments

Expect inquiries on recent supply chain events, biometric info, and operational technology

Coverage

Carriers scaling back or not offering ransomware-related coverages if a client has poor controls

More scrutiny on CBI and regulatory cover

Robust cybersecurity controls are key to risk mitigation, resilience, and insurability

ASSOCIATION FOR FINANCIAL PROFESSIONALS

Multifactor authentication (MFA) for remote access and admin/privileged controls

Endpoint Detection and Response (EDR)

Secured, encrypted, and tested backups

Privileged Access Management (PAM)

Email filtering and web security

Patch management and vulnerability management

Cyber incident response planning and testing

Cybersecurity awareness training and phishing testing

Hardening techniques, including Remote Desktop Protocol (RDP) mitigation

Logging and monitoring/ network protections

End-of-life systems replaced or protected

Vendor/digital supply chain risk management

Note: Each insurance carrier has their own specific control requirements that may differ by company revenue size & industry class.
For more on the Cyber hygiene see: Cyber hygiene controls critical as cyber threats intensify (marsh.com)

Strategize for renewals

Excellent controls are baseline to access cyber insurance coverage

ASSOCIATION FOR FINANCIAL PROFESSIONALS

Controls

Improve security and claims posture:

- Address potential security gaps prior to underwriting to achieve optimal results.
- Leverage carrier preferred vendors and access solutions to improve security posture.
- Update and practice incident response plan specific to ransomware scenarios.
- Identify vendor and legal counsel partners you might engage and evaluate against insurer's panel.
- Identify any problematic IP addresses & remote desktop protocols (RDP).

Structure

Explore structure options:

- Prioritize program components and goals: carrier partners, limits, attachment, coverage, overall structure, and consider ability to retain risk.
- Consider alternative terms and conditions to minimize increases and maximize coverage, including increased retentions and alternative limit options.
- Use of insurers in the US, London, and Bermuda may increase terms available.

Underwriting

Provide robust underwriting data:

- Leverage assessment tools to minimize need for multiple supplemental applications (includes ransomware questions and provides additional insights).
- Prepare for additional questions and applications; ransomware supplemental will still be required.
- Highlight significant cybersecurity updates and improvements over past year – especially those in the top 12!

ASSOCIATION FOR FINANCIAL PROFESSIONALS

Q & A

Contacts

Tom Hunt, CTP
Director of Treasury Services
AFP

thunt@afponline.org

Thomas Reagan
US & Canada Cyber Practice Leader
Marsh

thomas.reagan@marsh.com

Scott Stransky
Managing Director
Cyber Risk Analytics Center
Marsh McLennan

scott.stransky@mmc.com

Appendix: Additional reading and resources

[2021 AFP Risk Survey]

[2020 AFP Strategic Role of Treasury Survey]

[The State of the Us Cyber Insurance Market]

[The Marsh McLennan Cyber Handbook]