

BREAKOUT SESSION

KROLL

Managing Ransomware Attacks

MODERATED BY

Jeannette Ramirez-Clay

Underwriting Officer – AEGIS

Christopher Ballod

Managing Director, Cyber Risk – Kroll

Mark Henderson

*Assistant Vice President,
Underwriting – AEGIS*



22 Policyholders'
Conference

The Current Landscape



22 Policyholders'
Conference

THREAT ACTOR MONETIZATION METHODS – WHAT THEY ARE DOING

Extortionate Attacks

- Ransomware (with or without data theft)
- Data theft
- DDoS attacks
- Shaming emails

Social Engineering Attacks

- Business email compromises
- W-2 fraud
- Tech support scams

Others

- Insider threats
- Hacktivists



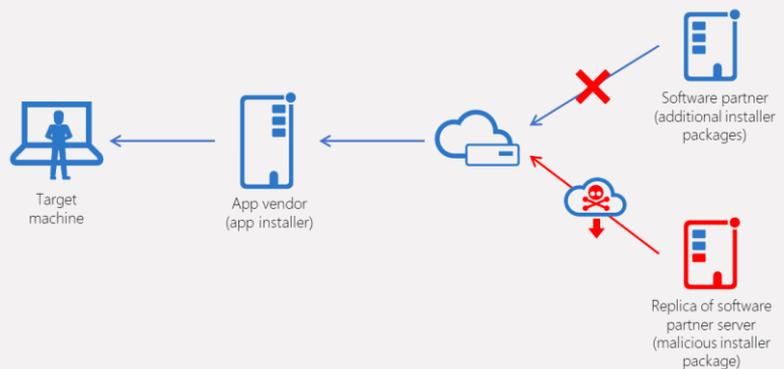
THREAT ACTOR ATTACK METHODS – HOW THEY DO IT

Intrusions

- CVEs and Zero Days
- Supply Chain Attacks
- Misconfigurations/Inadequate Configurations
- Phishing

Communications Channels

- Phishing and Spear Phishing
- Phone calls



Focus on Ransomware



22 Policyholders' Conference

FOCUS ON RANSOMWARE

Overview

- Trended down in February and March. Sharp increases in April and May.
- Manufacturing is most frequent target.
- Demands are lower and groups are more nebulous.
- War in Ukraine
- 2021 shrinking cyber insurance market
- Less-hardened environments
- Professional services continues to be close second
- Good platforms/targets for supply chain attacks
- U.S. defense activity and Ukrainian affiliate operations
- Decline in cyber insurance
- War in Ukraine



22 Policyholders' Conference

FOCUS ON RANSOMWARE

Intelligence Coming Out of the War in Ukraine

- Ransomware groups and affiliates have differing loyalties.
- Internal working of the groups were revealed.
- Warnings from .gov suggest close relationship with intelligence services.
- Conti, the largest operator in 2021, declared loyalty to Russia
- Conti affiliates in Ukraine “doxed” Conti actors
- Purchased all major EDR products to develop new countermeasures
- Organization of groups into access and abuse departments confirmed
- “Playbooks” obtained and translated
- Warnings of averted and still-impending “wiper” malware attacks
- Concerns about targeting critical infrastructure and financial sector targets



22 Policyholders' Conference

FOCUS ON RANSOMWARE

Costs

- Regulatory and enforcement actions are trending up.
- Increase in litigation and threats of litigation stemming from incidents.
- U.S. regulators are requiring more information and are more likely to levy a fine
- Increased scrutiny of cross-border data incidents
- Law enforcement inquiries into reported incidents are more assertive
- Business email compromise payment redirects are increasingly resulting in aggressive legal action
- Incidents are resulting in claims for breach of contract based on data protection provisions
- Business interruption claims against third-parties increased



22 Policyholders' Conference

THE FUTURE

- Resurgence of extortionate attacks.
- Cybercriminals have a revenue shortfall in the first half of 2022
- “Cash out” facilities have been relocated to new countries
- Sub-\$1 million demands and no infrastructure targets
- Less encryption and business interruption
- Cloud tenancies and applications will be increasingly targeted.
- We already see subversion of cloud migration tools to steal data
- Previously too much work for too little reward
- Could yield more diffuse claims if the infrastructure is impacted as a result of the insured’s incident



22 Policyholders'
Conference

Impact on the Cyber Insurance Market



22 Policyholders'
Conference

IMPACT ON THE CYBER INSURANCE MARKET

Cyber Threats and Trends

Evolving Threat Environment

- Threat actor are maximizing their ability to monetize network disruption
- Average breach costs for energy sector = \$5.6M on average*

Uncertain Geopolitical Environment

- War in Ukraine and proxy conflicts

Rising Compliance Costs

- State data privacy notification laws evolving into consumer protection laws
- Cyber Incident Reporting for Critical Infrastructure Act of 2021
- Multiple regulators considering incident notification requirements

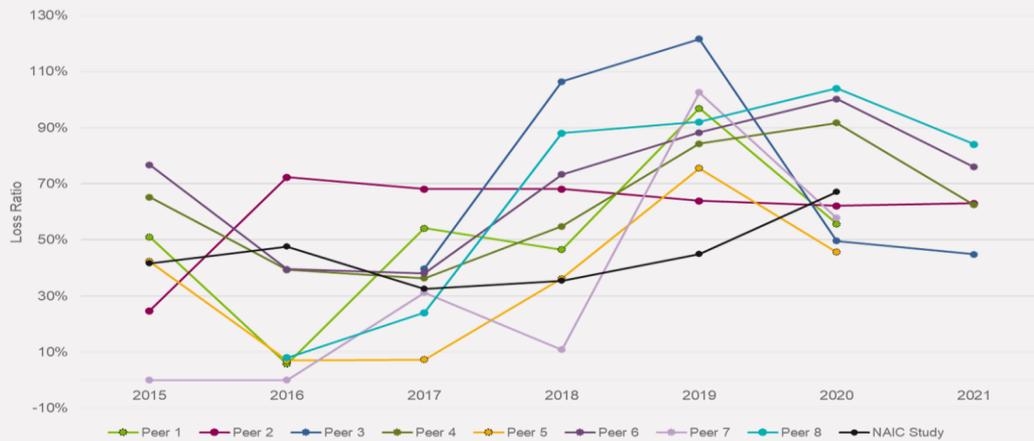
*Guidehouse Inc., "Cyber Insurance for the Energy Industry," Research Report, February 10, 2022, <http://www.guidehouseinsights.com>



22 Policyholders' Conference

IMPACT ON THE CYBER INSURANCE MARKET

Growing Exposures and Deteriorating Results



Peer groups consist of anonymized US, International and Global Mid/Large commercial carriers



22 Policyholders' Conference

IMPACT ON THE CYBER INSURANCE MARKET

Commercial Market Reaction

Dramatic Rate Increases

- Publicly available rate information ranges from 50% - 400%!

Restricting Coverage

- Sublimits, exclusions, split SIRs

Cutting Capacity

- Halving limits, quota-shares, mandatory co-insurance requirements

Non-Renewing

- Limited appetite of utility/public power segment or exiting cyber altogether



22 Policyholders'
Conference

IMPACT ON THE CYBER INSURANCE MARKET

AEGIS – Fulfilling its Mission

Moderate Rate Increases

- Pricing for long-term stability

Maintaining Coverage

- Full limits coverage, war exclusion clarification not restriction

Maintaining Capacity

- More limit available for our members than any other market

Committed to Cyber and our Members

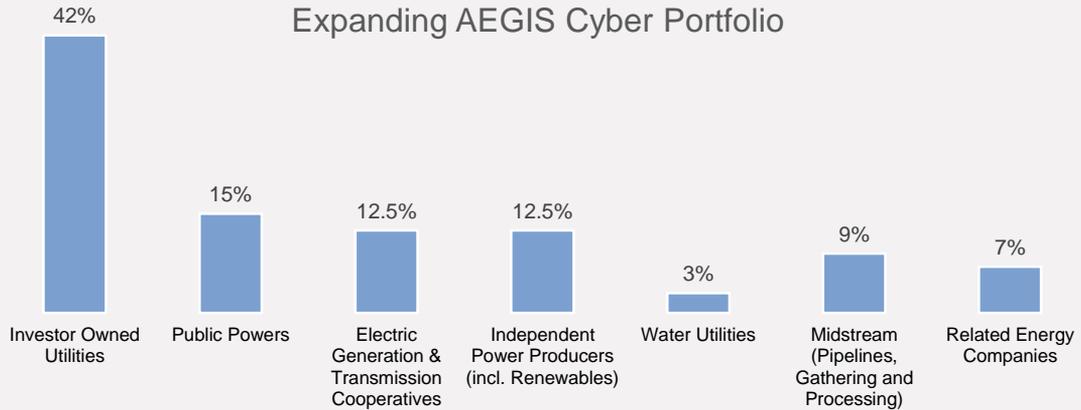
- Doubling Cyber credit to \$2,000,000.



22 Policyholders'
Conference

IMPACT ON THE CYBER INSURANCE MARKET

AEGIS – Fulfilling its Mission



22 Policyholders' Conference

WELCOME TO THE AEGIS ERISKHUB®

Key Features of the eRiskHub® Portal

- **Incident Roadmap** – Includes suggested steps to take following a network or data breach incident, free consultation with a BreachCoach® and access to a breach response team
- **News Center** – Cyber risk stories, security and compliance blogs, security news, risk management events and helpful industry links
- **Learning Center** – Best practices articles, white papers and webinars from leading technical and legal practitioners
- **Risk Manager Tools** – Assist you in managing your cyber risk including a self-assessment and state breach notification laws
- **eRisk Resources** – A directory to quickly find external resources with expertise in pre- and post-breach disciplines
- Go to <http://www.eriskhub.com/aegis>
- Complete the New User Registration form and use the Access Code 12752.
- No user registration caps – please give your whole team access!



22 Policyholders' Conference

Chris Ballod



Managing Director,
Cyber Risk, Kroll

Chris.Ballod@kroll.com

- Christopher Ballod is a Managing Director in the Cyber Risk practice of Kroll, based in Philadelphia. He leverages over 15 years of experience in data privacy and cyber security, counseling clients in the preparation for a cyber incident, and during the response and notification process after an incident occurs.
- Before joining Kroll, Chris was a partner and vice chair of the Data Privacy & Cybersecurity practice at Lewis Brisbois Bisgaard & Smith LLP, which received the Advisen Cyber Risk Award for Best Legal Practice in 2019 and 2020. He also served as a member of the firm's Corporate and Complex Business and Commercial Litigation practices.
- Christopher holds a Juris Doctor from the Delaware Law School. Additionally, he is a Certified Information Privacy Professional/U.S. (CIPP/U.S.) and Certified Information Privacy Professional/Europe (CIPP/E).



22 Policyholders'
Conference

Thank You



22 Policyholders'
Conference



22^{AEGIS}
Policyholders[®]
Conference