Virtual Meeting

CYBERSECURITY (H) WORKING GROUP
Thursday, May 29, 2024
11:00 a.m. ET / 10:00 a.m. CT / 9:00 a.m. MT / 8:00 a.m. PT

ROLL CALL

Cynthia Amann, Chair  Missouri  Jake Martin  Michigan
Michael Peterson, Vice Chair  Virginia  T. J. Patton  Minnesota
Julia Jette  Alaska  Troy Smith  Montana
Bud Leiner/Deian Ousounov  Arizona  Martin Swanson  Nebraska
Mel Anderson  Arkansas  Scott Kipper  Nevada
Damon Diederich  California  D.J. Bettencourt  New Hampshire
Wanchin Chou  Connecticut  Gille Ann Rabbin  New York
Tim Li  Delaware  John Harrison  North Carolina
Matt Kilgallen  Georgia  Colton Schulz  North Dakota
Lance Hirano  Hawaii  Don Layson/Matt Walsh  Ohio
C.J. Metcalf  Illinois  David Buono  Pennsylvania
Daniel Mathis  Iowa  John Haworth  Washington
Shane Mead  Kansas  Andrea Davenport  Wisconsin
Mary Kwei  Maryland  Lela Ladd  Wyoming

NAIC Support Staff: Miguel Romero/Sara Robben

AGENDA

1. Opening Remarks—Cynthia Amann (MO)

2. Hear a Presentation from Coalition, Inc.—Sezaneh Seymour (Coalition, Inc.) & Daniel Woods (University of Edinburgh)  Attachment 1

3. Discuss Any Other Matters Brought Before the Working Group  
   —Cynthia Amann (MO)

4. Adjournment—Cynthia Amann (MO)
Effectiveness of Security Controls: a Meta Analysis

Sezaneh Seymour
Daniel Woods
Table of Contents

1  Context: evolution of cyber insurance
2  Research: effectiveness of security controls
3  Reflections for regulators
4  Questions
The cyber insurance landscape is changing

More believe a cyber insurance policy can serve as a proxy indicator that a firm has met basic cyber hygiene, and this should matter to regulators.

- Cybersecurity is a mainstream national security issue.
- Cyber insurers are evolving to keep pace with cybercrime and price risk.
- Cyber insurers have become a more central part of the security conversation.
Cyber insurance that combines technology and insurance to more accurately price risk, and help policyholders manage digital risks.

All policies include continuous monitoring with personalized alerts and assistance to resolve security issues.

We invest in threat research to stay ahead of trends.

In the event of an incident, we respond in minutes to get businesses back up and running by resolving claims and helping navigate the recovery process.

https://www.coalitioninc.com
Active Insurance

**Active Protection**
Monitoring and alerting to identify and prevent risk before it strikes

**Active Risk Assessment**
Underwriting, quoting, renewals, and digital risk scores powered by real-time data

**Active Response**
Access to in-house resources that accelerate response and coverage if an incident occurs
Research: Effectiveness of Security Controls
Cyber risk science is hard

Systematic review of academic literature reveals an immature body of research [1].

No consensus on basic questions about data breaches (see Table).

Regarding efficacy:

“RQ2: Which security interventions effectively reduce harm?

... Actionable answers are unavailable based on current evidence.”

<table>
<thead>
<tr>
<th>Reference</th>
<th># obs</th>
<th>Years</th>
<th>Breach frequency</th>
<th>Breach size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Curtin et al. (2008)</td>
<td>899</td>
<td>2005–07</td>
<td>▲</td>
<td>?</td>
</tr>
<tr>
<td>Maillart et al. (2010)</td>
<td>956</td>
<td>2000–08</td>
<td>▲</td>
<td>▲</td>
</tr>
<tr>
<td>Wheatley et al. (2016)</td>
<td>5365</td>
<td>2007–15</td>
<td>▲</td>
<td>▲</td>
</tr>
<tr>
<td>Eling et al. (2017)</td>
<td>2266</td>
<td>2005–15</td>
<td>▲</td>
<td>▲</td>
</tr>
<tr>
<td>Xu et al. (2018)</td>
<td>600</td>
<td>2005–17</td>
<td>▲</td>
<td>▲</td>
</tr>
<tr>
<td>Wheatley et al. (2019)</td>
<td>1713</td>
<td>2005–17</td>
<td>▲</td>
<td>▲</td>
</tr>
<tr>
<td>Carfora et al. (2019)</td>
<td>5724</td>
<td>2005–17</td>
<td>▲</td>
<td>?</td>
</tr>
</tbody>
</table>

Insurers also struggle with cyber risk science

Problems during the data breach era

- Data breaches were infrequent outside of mega firms in specific industries
- Cyber insurance penetration was low
  - Again mainly large firms
- Large insureds had complex and heterogeneous networks
  - Statistics abhors heterogeneity
- Insurers relied on questionnaires
  - Asking too many questions impacts sales
  - Self reported answers are unreliable

Representative quotes*

- “Every carrier is dying for data, they just don’t know what data they need.”
- “One underwriter said that because so little information about investigations was shared by the lawyers overseeing incident response, insurers often had to rely on their instincts to guide their underwriting more than empirical data”
- “When we got our shirts handed to us by ransomware in 2020, we overhauled our ransomware underwriting model and strategy . . . . But, candidly, it was from my understanding and not from real data,”

The Ransomware Epidemic as a Paradigm Shift

Threat landscape
- Ransomware actors target all kinds of firms
  - Not only those who process payments
- Frequency and severity go up
- Threat actors start to commoditize cyber crime

Insurance market
- Cyber insurance penetration increases
- Adoption of external scans for risk assessment

But this also had implications for cyber risk science
Cyber risk science in the ransomware era

Evidence-based cybersecurity policy? A meta-review of security control effectiveness

Daniel W. Woods and Sezaneh Seymour

School of Informatics, University of Edinburgh, Edinburgh, United Kingdom; Coalition Inc., San Francisco, United States of America

* Publication delays mean our paper’s evidence is relevant up to 2023 or so, but we present studies from 2024 in this talk.
# The emergence of cyber insurance studies

<table>
<thead>
<tr>
<th>Studies (Year)</th>
<th>Outcome Variable</th>
<th>Independent Variables</th>
</tr>
</thead>
<tbody>
<tr>
<td>Marsh (2023)</td>
<td>claims</td>
<td>questionnaire</td>
</tr>
<tr>
<td>GallagherRe (2022)</td>
<td>claims</td>
<td>scans</td>
</tr>
<tr>
<td>AtBay (2023)</td>
<td>claims</td>
<td>scans + questionnaires</td>
</tr>
<tr>
<td>Coalition (2023)</td>
<td>claims</td>
<td>scans</td>
</tr>
<tr>
<td>BitSight and Marsh (2022)</td>
<td>claims</td>
<td>scans</td>
</tr>
<tr>
<td>BitSight (2023)</td>
<td>incidents</td>
<td>scans</td>
</tr>
<tr>
<td>SecurityScorecard and Marsh (2022)</td>
<td>incidents</td>
<td>scans</td>
</tr>
</tbody>
</table>
**Patch management**

### Findings
- Attacks involving the exploitation of vulnerabilities increased by 180% in 2023 ([Verizon, 2024](Verizon, 2024)).
- Speed at which patches are applied is the most important technical variable for predicting whether cyber claims ([GallagherRe, 2023](GallagherRe, 2023)).
- Policyholders with one unresolved critical vulnerability were 33% more likely to claim ([Coalition, 2023](Coalition, 2023)).
- Patch Cadence was the 2nd strongest predictor of cyber claims ([BitSight and Marsh, 2022](BitSight and Marsh, 2022)).
  - Replicated by another scanning provider ([SecurityScorecard and Marsh, 2022](SecurityScorecard and Marsh, 2022)).
- Organizations who patch high severity vulnerabilities within 7 days less likely to file a claim ([Marsh, 2023](Marsh, 2023)).
- Organizations deploying End of Life software were 3.7 times more likely to suffer a claim in 2022 ([Coalition, 2023](Coalition, 2023)).

### Limitations
- Need to measure prioritization and asset coverage
- Causality
  - Signal of broader cyber hygiene
  - We also know cadence matters from root cause claims analysis

**Citrix Bleed Timeline** *(Figure 1.4)*

- **OCT. 10** ⚫ Citrix publishes a bulletin announcing the vulnerability and an available patch.
- **OCT. 10** ⚫ Coalition sends out notifications for policyholders to patch.
- **OCT. 17** ⚫ Citrix first detects threat actors exploiting the vulnerability in the wild.
- **NOV. 21** ⚫ CISA publishes advisory and security researcher Kevin Beaumont publishes evidence that the Lockbit ransomware gang is actively exploiting the vulnerability prioritization.

Extract from Coalition 2023 Cyber Threat Index
Attack Surface Management

Findings

- Number of open ports on a Fortune500 network was a statistically significant predictor of multiple indicators of compromise (Nagle et al., 2017).
- Businesses with internet-exposed RDP are 2.5 times more likely to claim (Coalition, 2024).
- Number of IPs & domains managed by providers explains 71 percent of the variance in network abuse (Tajalizadehkhoob et al., 2017).
- The collection of web-master hardening efforts, including Secure and HTTPOnly cookies, are negatively correlated with both malware and phishing abuse (Tajalizadehkhoob et al., 2017).
- Organizations that employ hardening techniques are 5.58 times less likely to suffer a cyber insurance claim (Marsh, 2023).

Limitations

- Reducible vs irreducible attack surface
  - How much of this is controllable
- ASM is nebulous
  - We see tiny slices of a broad process
- Variables differ across studies
Multi-Factor Authentication

Findings

- Multi-factor authentication (MFA) is associated with a 98.56% reduction in Active Directory account compromise in cases of leaked credentials (Meyer et al., 2023).
- Using SMS as the 2nd factor was 41% less effective than a dedicated authenticator app at protecting accounts with leaked passwords (Meyer et al., 2023).
- MFA blocked 100% of automated Gmail account takeover attempts, but using SMS as a 2nd factor blocked only 76% of targeted attacks (Doerfler et al., 2019).
- Implementing MFA was associated with the lowest reduction in claims likelihood compared to 10 other controls (Marsh, 2023).

Limitations

- MFA highly effective at protecting individual accounts, but loses efficacy when rolled out across an org
- Effective relative to a fixed threat level
  - Global companies face adversaries who can overcome SMS-MFA
- Configuration details matter and are hard to measure unless you run the infrastructure
  - In contrast to say vaccine studies where a doctor administers a uniform substance with a reliable instrument (needle)
Cloud Migration

Findings

- Businesses with more than $100 million in revenue with on-premise Exchange are 260 per cent more likely to make a claim (Coalition, 2023).
- Firms running on-premises Microsoft Exchange have a claims frequency of 0.19 per cent compared to 0.14 per cent for Microsoft’s cloud email solution (Office365) and 0.07 per cent for Google’s cloud email solution (AtBay, 2023).

Limitations

- Organizations who haven’t migrated likely haven’t done so for a reason
  - Tech debt, complex use cases
- Univariate analysis cannot capture interdependencies
  - E.g. cloud provider manages patches
Boundary Devices

Findings

- These are the largest effect sizes
- Businesses with internet-exposed Cisco ASA devices are 4.7 times more likely to claim \(\text{(Coalition, 2024)}\).
- Firms with exposed Fortinet devices three times as likely to file a claim \(\text{(Coalition, 2023)}\).
- Organizations exposed to a group of vulnerabilities associated with PulseSecure VPN devices are 2.6 times more likely to suffer a ransomware incident \(\text{(Bitsight, 2023)}\).
- Firms using two self-managed VPNs, Cisco ASA and Citrix SSL, were 11X more likely to claim than those who use no/cloud VP \(\text{(AtBay, 2024)}\).

Limitations

- Causal link can be seen from claims data
  - Ransomware gangs scan the Internet following CVEs
- But is it because of security?
  - Perhaps VPNs are targeted because they are popular?
    - E.g. there’s more windows malware than mac malware
- Problem of underwriting impacting effect sizes
  - Once you detect an effect, you underwriter away from it OR require controls
Summary

Findings

- No silver bullets
  - Configuration and maintenance seem to be key
- Patch management highly effective
  - Investment in info infrastructure?
    - CERT/CC since 1990s
    - NVD since 2000s
    - CISA’s KEV since 2020s etc
- Emergence of actuarial evidence about insecure tech
  - Edge device manufacturers

Limitations

- Causality
  - No modern econometrics
  - Correlation is still valuable
- Streetlight effects
  - Only so much can be seen with external scans
Future of cyber risk science

Opportunities

- New streetlights — data directly from vendors
- Using NLP to process historic unstructured data
- Bigger n as the industry grows
- Partnerships with Govt?

Challenges

- Traditional insurers don’t run/share analysis
- Technological flux
  - Will ransomware gangs target VPNs in 3 years?
- Correlation vs causation
  - Correlation is fine for passive insurance
  - Need to understand causation for active (e.g. discounts)
Reflections for Regulators
Rate without filing: Insurers navigate constantly evolving tech risk. Appropriately, many states allow rating without filing. Where that’s not an option, a faster approval process needed.

Insurance and security services: Anti-rebating and anti-tying rules must allow cyber insurers to offer premium and services discounts when policyholders implement risk reduction measures.

Data Privacy: Ensure goals of transparency and data minimization don’t inadvertently undermine ongoing cyber threat research and information sharing.

Cyber insurance is a market tool to drive digital resilience: Ongoing federal and international conversations are focused on our industry.
Questions?
You are advised to read this disclosure carefully before reading or making any other use of this presentation and related material. The content of this presentation is (i) not all-encompassing or comprehensive; (ii) solely for informational purposes; (iii) not be construed as advice of any kind or the rendering of consulting, financial, legal, or other professional services from Coalition; and (iv) not in any way intended to create or establish a contractual relationship. Any action you take upon the information contained herein is strictly at your own risk and Coalition will not be liable for any losses and damages in connection with your use or reliance upon the information. The content of this presentation may not apply directly to specific circumstances and professional advice should be sought before any action is taken in relation to the information disseminated herewith. Coalition makes no representation or warranties about the accuracy or suitability of information provided in the presentation or related materials. The presentation may include links to other resources or websites which are provided for your convenience only and do not signify that Coalition endorses, approves or makes any representation or claim regarding the accuracy of copyright compliance, legality, or any other aspects of the resources or websites cited.

Copyright © 2023. All Rights Reserved. Coalition and the Coalition logo are trademarks of Coalition, Inc.