Cyber Risk Engineering

Amanda Draeger

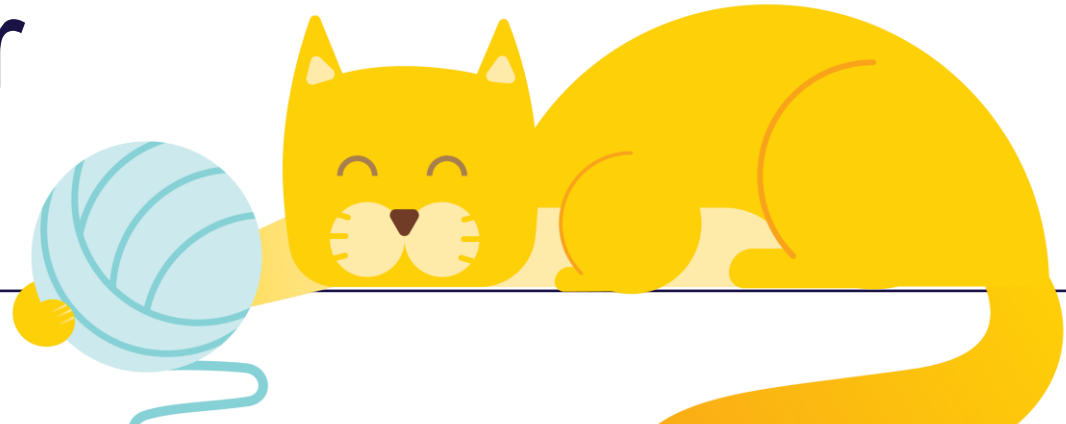
Principal Cyber Risk Engineer @ Liberty Mutual Insurance

Disclaimer

Our risk control services are for informational purposes only. In providing any information or recommending the services of others, we assume no responsibility for management or control of your systems or activities nor for implementation of any recommended corrective measures. Nor do we warrant that any system owned or used by you, directly or indirectly, is secure or that any system or practice complies with any laws, regulations, codes, or standards. We may refer you to one of our trusted service partners. In doing so, we do not warrant or guarantee the work of any provider or third-party. Any information we offer or recommend are not intended to replace any risk control measures you have or should have in place. We will have no liability to you or others in connection with providing or failure to provide information, referring or recommending the services of others, or for your failure to implement any recommended courses of action.

Whoami

- Fiber arts enthusiast
- Cat mom
- Retired Army Sergeant Major
- GIAC Security Expert (GSE)
- Cyber Risk Engineer



Risk Management

- Risk Reduction
- Risk Avoidance
- Risk Acceptance
- Risk Transfer

Risk Transfer

Transfer portion of potential financial consequences from one party to another

Idea started with “mutuals”

Not related to idea of outsourcing risk when you outsource functions

- Still obligated to ensure functioning correctly
- Expertise may reduce risk, but risk inherently yours

Cyber Insurance Process

Players

Insurance customer

Usually CRO, CFO, GC
(not CISO)

Insurance broker

Connect customers to carriers
Advocate for customer

Insurance carrier(s)

Underwriters
Risk engineers (that’s me!)

Insurance Tower

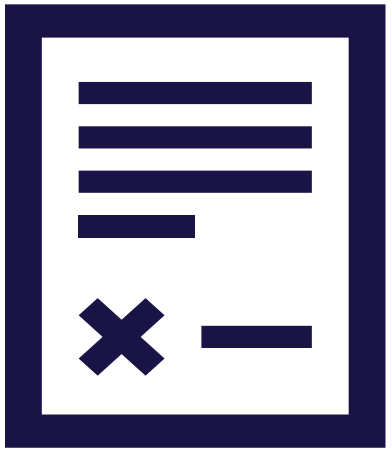
Less risk, premium, influence

More risk, premium, influence

- 3rd Excess (31-41M)
- 2nd Excess (21-31M)
- 1st Excess (11-21M)
- Primary (1-11M)
- Retention (0-1M)

Insurance Types

Cyber Insurance
1st Party Coverage



Tech Errors and Omissions (E&O)
3rd Party Coverage

The Challenge

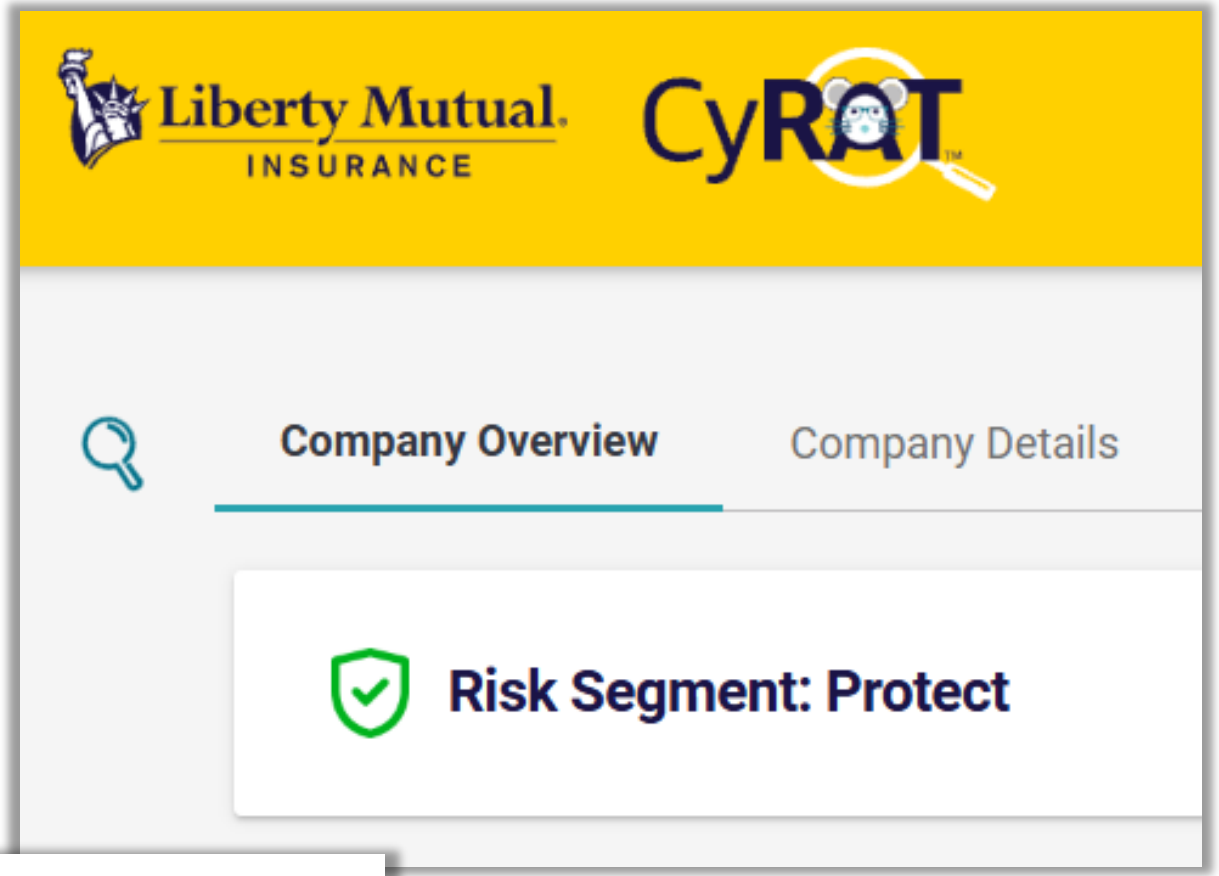
- Data is key for making (risk) decisions
- Data comes in many forms
- Public data vs. Private data
- Data quality issues

How do you use data to make better decisions without blindly following the data?

Data-Informed Risk Management

Correlation

Predictive Modeling: five years of data trained to predict claims so that we can learn how things we can see predict the things we can’t



Indicator	Weighting	Findings
TIscert No Revocation	5.9%	99
TIs Weak Cipher	5.7%	67

Correlation Challenges

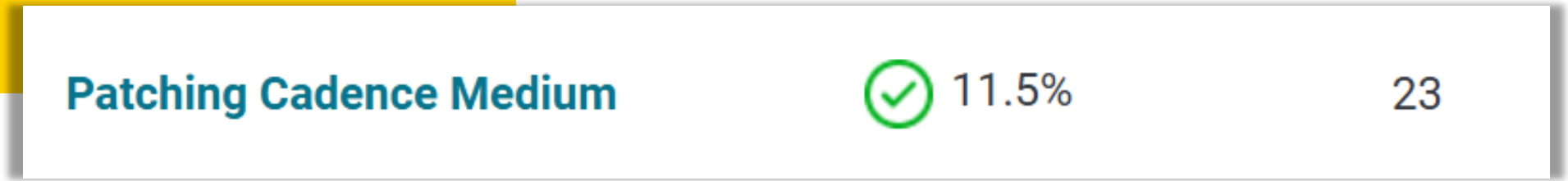
Firmographics Impact: revenue, industry, employee count often the most predictive factors

Indicator	Weighting	Findings
Industry	17.8%	hospitality (Value Used)
Employee Count	15.3%	5804 (Value Used)

Correlation Challenges

Lack of Direction: can be difficult to say what organizations should do based on this data, inconsistent model weightings

Visibility: limited to the data that is currently being collected



Causation

Cyber Hazard Flags

Status	Flag/Control	Definition
	High Risk Vulnerabilities	The organization has vulnerabilities that are being actively exploited by threat actors.
	Organization Likely Compromised	There are not indicators that the organization has suffered or is likely to suffer some type of cyber incident.
	Exposed remote access services	The organization has exposed ports commonly associated with remote network access.
	High-risk open ports	The organization does not have exposed ports that are known to pose a significant risk.
	Asset Inventory Process	The organization does not have an adequate asset inventory.

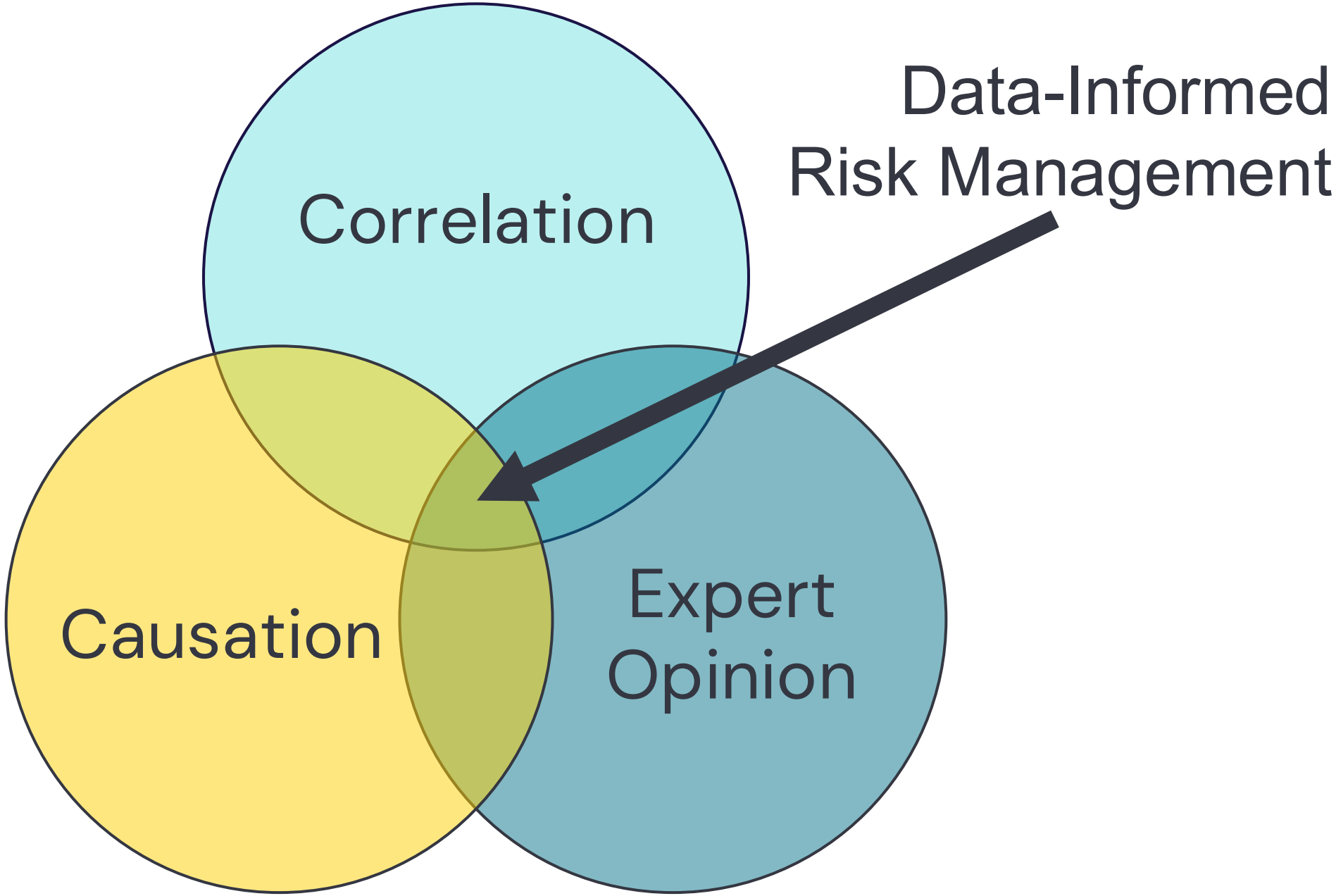
Consider both Frequency and Severity

Causation Challenges

Automatability: Different data sources are more or less automatable depending on their consistency and format

Expert Opinion

- Data exists in conflict with itself; correlation and causation may give different answers
- Data lives in the context in which it was generated
- Organizational features
- Data collection method
- Qualitative data (e.g., leadership attitudes)


Data-Informed
Risk Management
Correlation
Causation
Expert
Opinion

What does the data say???

Frequency

Root cause: read any of the major industry reports

Marsh self-assessment questionnaire: ability to apply critical vulnerabilities in less than 1 week

Firmographics count for a lot

Modeling based on outside-in scans (e.g., by Gallagher Re) tend to focus on correlation, not causation

Severity

Business Interruption

- Extended downtime
- Fragile supply lines
- Consider billing, ERP, other support systems

Data Breach

- Regulatory fine vs. trial w/ jury (especially US)
- Costs of notification, credit monitoring per person
- Possible wrongful collection

How I look at organizations

Liberty Lenses

Threat access

Culture

Security Ops & Resilience

Security Planning & Engineering

Partner Security

Focus Areas

Threat access

- Credentials
- Phishing
- Asset Mgmt. Vulns
- Bots

Culture

- Corporate Culture
- Corporate Capability
- Errors

Security Ops & Resilience

- Incident Response
- Disaster Recovery
- Tactical Intelligence

Security Planning & Engineering

- Standards
- Plan to Standard
- Measurement to Plan
- Security Engineering

Partner Security

- Who you rely on
- Who relies on you

Observables

- Keeping in mind our limited inputs
  - What can we observe?
  - Self reported vs. externally observable
- Correlation vs. causation
- Not mutually exclusive
- Expectations based on org type, size

- Examples:
  - MFA use
  - Exposed ports
  - Exposed vulnerabilities
  - Security Leader
  - Budget
  - IR, BC, DR plans exercised
  - Policies up-to-date
  - Roadmap

Conclusions

- Risk Management all the way down
- Data is a liability
- Important to be able to make decisions in the absence of perfect data
- Never stop learning

Questions?

 https://www.linkedin.com/in/adraeger
 @TindrasGrove@infosec.exchange
 @tindrasgrove.com
 https://tindrasgrove.com/pages/links.html


Liberty Mutual®
INSURANCE