The Secret to a Successful Cyber Risk Program: Control the Chaos of Vendor Risk Management

Atlanta RIMS 2022

Mary Guzman

CEO, Crown Jewel Insurance

Meet the Speaker: Mary Guzman

Mary Guzman is an insurance industry veteran and pioneer. She has over 30 years experience advising clients on a myriad of risks to their businesses, most recently with a focus on all things related to technology, media, and intellectual property. She is passionate about educating insurers and clients about Intellectual Property Risk.

Mary earned a reputation as an industry trail-blazer and disrupter using her knowledge and reputation in the market to create new insurance products. These included a first of its kind “franchisee” cyber program, the first “Failure to Supply” coverage via a $125 Million line-slip for the utility sector, and the first cyber-driven bodily injury/property damage coverage for oil and gas companies. Mary was one of the first in the industry to develop and place a cyber insurance policy in 2000.

She is a published author and sought-after speaker, having done over 100 speaking engagements on risks and solutions to threats arising from the convergence of all things intangible. She has been a government liaison as part of the DHS cybersecurity and insurance working group during the Obama administration. Most recently, Mary was honored as one of 2021 Business Insurance Women to Watch.

Mary has provided insurance solutions to an impressive group of Fortune 500 companies.

BUSINESS INSURANCE WOMEN TO WATCH

Vendor Management: By the Numbers

Breach Costs by the numbers:

- Largest Cost: $1.38 billion (Equifax, 2017)
- Average total cost of a data breach: $3.86 million[1].

Weakest link in the chain?

- A 2022 survey by the Ponemon Institute found that over half of organizations (51%) have experienced a data breach caused by third parties that led to the misuse of sensitive or confidential information.
- According to Forrester, 60% of security incidents in 2022 will result from issues with third parties.
- Of the companies that experienced a vendor-driven breach, 32% suffered a loss of PII, 29% payment information, and *24% experienced a loss of proprietary business information*[2].

1. Cost of a Data Breach Report 2020, IBM
2. "Nearly half of firms suffer data breaches at hands of vendors" by Mark Sangster, 2019.

The Problem

- Vendor management has moved from an emerging trend in cyber risk to a robust everyday reality that is increasingly difficult to manage.
- Finding the balance of responsibility between a company and its vendors continues to be a major source of frustration for both parties,
  - Vendors are desperate to cap their costs from a “systemic” issue that affects many customers at once
  - The customer does not want to take on the contingent business interruption losses, extra expenses, and downstream liability or reputation harm associated with hundreds of vendors over whom they have little control
- Most enterprises have a one-size-fits-all approach to vendor security and insurance governance which is not reflective of the exposure a given vendor brings to the organization.
- Current Market Conditions
- Culture

Legislation/Regulatory History

- Several of the more recent privacy laws and/or security guidelines such as:
  - The New York Department of Financial Services (DFS) Cybersecurity Rules (NYCRR 500) requirements for third-party vendors (section 11), or
  - The National Cyber Security Centre (NCSC) Principles of Supply Chain Security specifically lay out what an organization must do to shore up this exposure, and
  - GDPR (European Union)
  - 20+ states have laws requiring "reasonable measures"
  - FTC Act Safeguard Rules, in "Ascension Data & Analytics, LLC" Consent Order held that vendor selection and oversight is a reasonable measure.
- HIPAA has pushed security requirement to Business Associates holding/processing healthcare information for several years now.

Case Studies

- Colonial Pipeline
- SolarWinds
- And more

Colonial Pipeline

The Facts:

- Colonial Pipeline was unable to provide gas to their downstream customers due to a ransomware attack
- It was the first time Colonial had shut down the entirety of its gasoline pipeline system in its 57-year history, and this continued for 7 days
- Colonial paid the hackers, who were an affiliate of a Russia-linked cybercrime group known as DarkSide, a $4.4 million ransom shortly after the hack.
- Decryption key did not work, and company suffered BI and EE losses over the span of the outage.
- Downstream customers (convenience stores) suffered income losses due to major drop in sales during outage.
    - Was there additional downstream liability?

The implications:

- Colonial's insurance coverage
- Customer's insurance coverage

SolarWinds

Facts

- The hackers used a method known as a supply chain attack to insert malicious code into the Orion system.
- More than 18,000 SolarWinds customers installed the malicious updates, with the malware spreading undetected.
- At least 9 Federal Government Agencies were impacted

Implications:

- IronNet's 2021 Survey, 90% of respondents said cyber security had improved over the last 2 years, yet 86% of them suffered attacks that required a C-Suite Executives or Board Member Response.
- Board Duty Failures Enabled Breach
- On average, the SolarWinds hack cost companies 11% of their annual revenues or $12 million.
- 9 out of 10 companies have reevaluated their Supply Chain Cyber Security following the attack.
- The White House Executive Order on Cyber Security
- Insurance Response?

And the list goes on…

2 Vendor Hacking Incidents Affect Over 600,000 Individuals

At Least 32 Providers Affected by Ciox Vendor Email Breach

Vendor's Ransomware Attack Is Latest Supply Chain Warning

Vendor's Ransomware Attack Is Latest Supply Chain Warning

K-12 vendor breach spreads across New York State

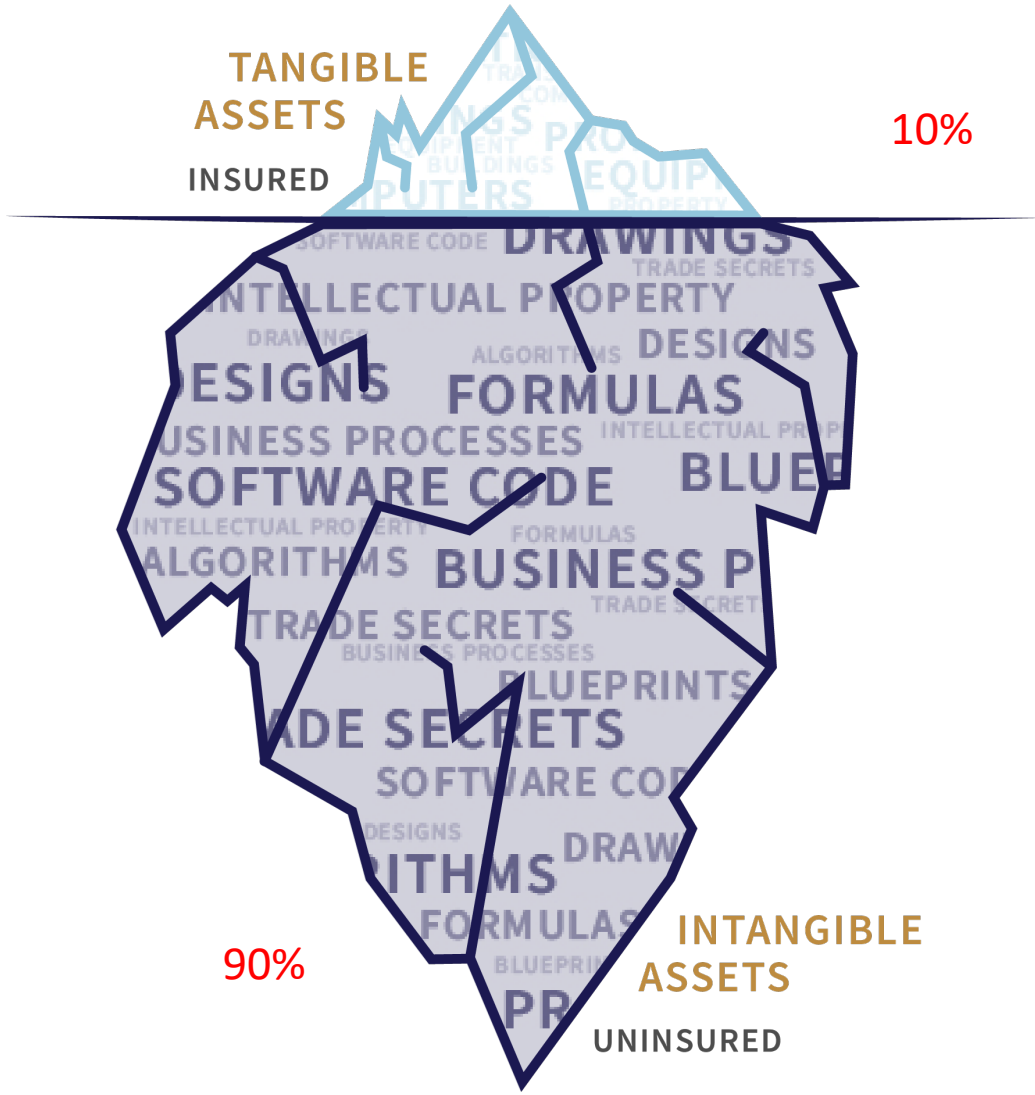
Whose insurance pays? If any..

- A dramatically hardened cyber insurance market for large global enterprises is forcing higher retentions for customers, and narrowing coverage is a driver for increased scrutiny of vendor insurance programs.
- Meanwhile third party service providers (vendors) are buying less insurance than they did two years ago, citing cost and a lack of capacity as impediments to their need/desire to purchase more coverage (particularly public companies).
- Key considerations:

Customer/Enterprise	Third Party Service Provider/Vendor
Contingent BI limits, retentions, waiting periods	Definition of Security Breach
Definition of Third Party Service Provider	Definition of Damages
Ransomware or other exclusions/limitations	Limits! Remember, most Tech companies buy cyber and E&O combined. They have to account for their own losses and that of their customers under one aggregate!
Contractual liability/breach of contract exclusions	Breach of contract/contractual liability exclusions

What about Trade Secrets?

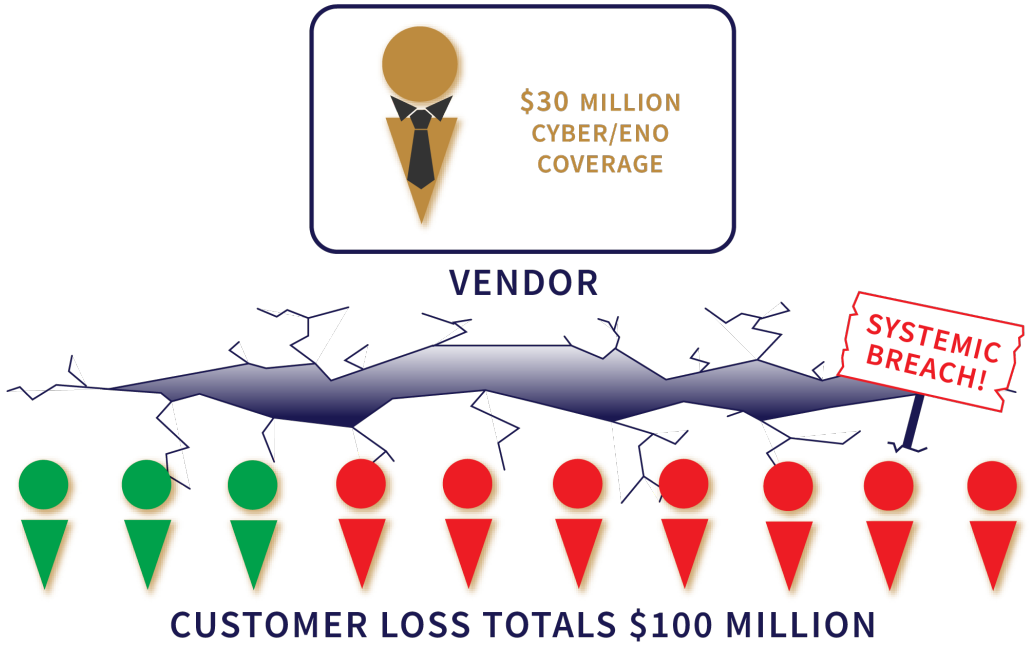
- Trade secrets are generally defined as financial, business, scientific, technical, economic, or engineering information that has actual or potential independent economic value, and the information is kept confidential, not generally known or ascertainable by others who could obtain economic value from the disclosure or use of that information.
- Federal law (18 U.S.C. §1831 et seq.) makes it a crime to wrongfully disclose, copy, steal, etc. a trade secret (with a few narrow exceptions) or to receive or accept trade secrets that were stolen and allows a court to impose significant fines and jail sentences for such activities.
- Both state and Federal statutes require that the owner take "reasonable steps" to keep the information secret in order to be protected under the law.
- Important factors:
  - Identification and marking of Trade Secret Assets
  - Require employees, contractors, vendors, and any other people who may have access to a company's trade secrets to execute specific non-disclosure agreements
  - Information security policies and procedures specific to these assets
  - "need to know" access
  - Exit interviews
  - Mitigation plan
  - Evidence of all of the above



Potential Solution: Contract Specific Coverage

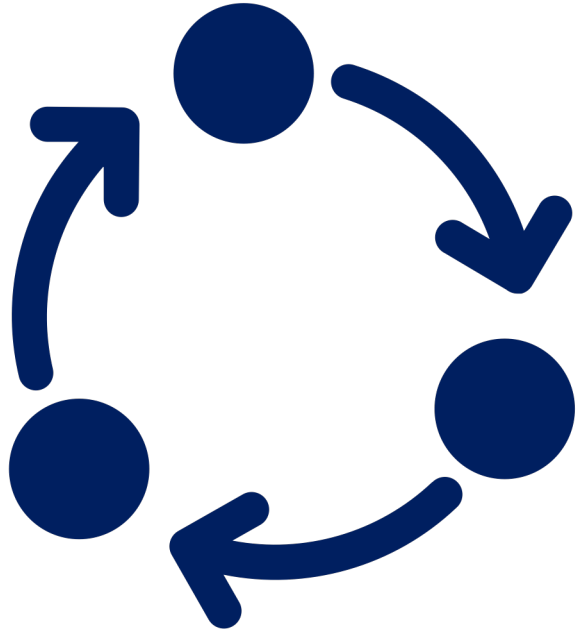
This approach does several things for both parties:

- Reduces frictional cost and frustration on the part of both parties because the vendor can now agree to reasonable indemnity and limitation of liability wording and can evidence excellent coverage with limits (up to capacity) that reflect actual risk created by specific vendor.
- Does not matter if the breach is caused by error or omission or by breach, as policy response should be the same.
- Guarantees to the Enterprise that at least the dedicated limits will be available to them in the event of a catastrophic, systemic event caused by or suffered by the vendor.
- Insulates the Board from D&O risk and insulated company from regulatory and reputation risk.
- The Enterprise could deduct the cost of the insurance from the price they would have otherwise paid for the contracted services, therefore, neither party must come "out of pocket" to pay the premium.
- Enterprise could negotiate that its own cyber insurance carrier(s) would allow any payment by the vendor's insurance to erode the retention of its program? And/or their own insurance should cost significantly less since 60% of the exposure is mitigated.

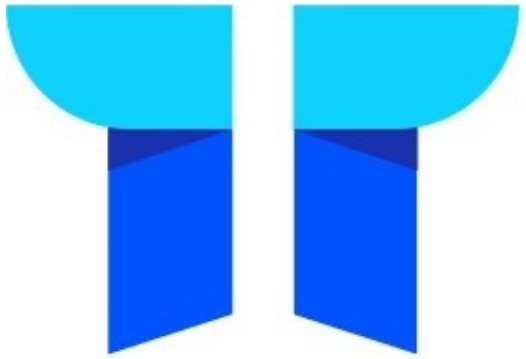


Automated Vendor Governance

- Creates efficiency, a road map for improvement, and objective information from which to leverage contract terms. Game changer for Risk Managers, Compliance, Information Security, Legal, and Procurement Professionals who struggle to dedicate sufficient time and resources toward vendor governance
- Solves for regulatory challenges by creating dashboard reporting evidencing much more that “check the box” assessment questionnaires
- Insulates Board of Directors (and insurance limits)
- Allows for pro-active, strategic management of vendors using risk-based assessment tools; can and should become an integral part of procurement process



Cyberwrite



Torii

Accountable

Looking into the crystal ball

- Capacity crunch will become such an issue that market dynamics are forced to change
- Customers will view control of vendor insurance coverage as part of the cost of doing business; vendors will include cost of contract/customer-specific insurance in their bids…period.
- Aggregation risk to insurance market will be laid off to reinsurers via stop-loss and/or parametric vehicle and/or
- Federal backstop for only the largest of TPSP breaches and only for TPSPs that have acted according to much tougher standards/regulations around security
- Tax incentives for companies that spend more time and money on information security and availability/reliability in the supply chain
- SEC and plaintiffs bar will hold Directors and Officers accountable for inaction, penalties will have to be much stronger than today

Questions?

info@crownjewelinsurance.com

+1-833-999-9981

@CrownJewel_Ins

@Crown Jewel Insurance

@Crown Jewel Insurance