The Fundamentals of Cyber Insurance

Tiago Henriques - VP of Research @ Coalition, Inc.

Agenda

- Cyber insurance - What is it and why is it needed?
  - What is covered? What does it include?
- Underwriting - How insurers use data to understand digital risk
- Myth busting
  - Does cyber insurance replace a need for cybersecurity?
  - Is it true that cyber insurance doesn’t pay claims?
  - Is cyber insurance fueling ransomware?
- How cyber insurance can help cybersecurity

What is cyber insurance ?

- Cyber insurance policies safeguard organizations against financial losses stemming from cyber incidents, such as data breaches, ransomware attacks, and network outages.
- What's included in cyber insurance policies varies widely.
  - Some policies cover only specific types of cyber events and may include sub-limits for certain attacks, like ransomware.
- It is **not** a replacement for the need for cybersecurity.
- Parts of the industry care about events affecting an individual organization (e.g., MGAs, and carriers that sell primary insurance), while others only care about big events that affect a lot of people (e.g., reinsurance carriers).

3rd Party Security and Privacy

- Network & Information Security Liability
- Regulatory Defense & Penalties
- PCI Fines & Assessments
- Funds Transfer Liability

Media and Professional Liability

- Multimedia Content Liability
- Technology Errors & Omissions *(available by endorsement)*
- Misc. Professional Liability *(available by endorsement)*

Cyber Crime

- Funds Transfer Fraud, Personal Funds Fraud, and Social Engineering
- Service Fraud including Cryptojacking
- Impersonation Repair & Phishing
- Invoice Manipulation

Event Response

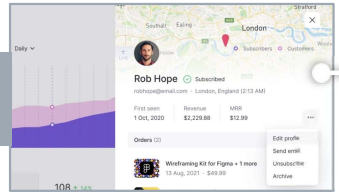
- Breach Response Costs
- Cyber Extortion (Ransomware)
- Business Interruption & Extra Expenses
- Digital Asset Restoration
- Crisis Mgmt & and PR
- Proof of Loss Preparation Expenses
- Computer Replacement & Bricking
- Reputational Harm Loss
- Court Attendance
- Criminal Reward

Other Coverages (available by endorsement)

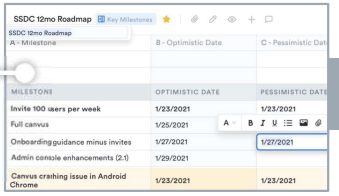
- Bodily Injury & Property Damage 1st Party
- Bodily Injury & Property Damage 3rd Party
- Pollution
- Reputation Repair

Technology creates exposures that are part of every organization

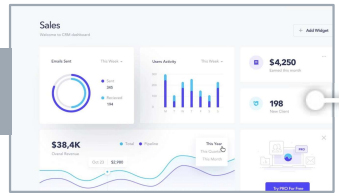
Customer Relationship Management System

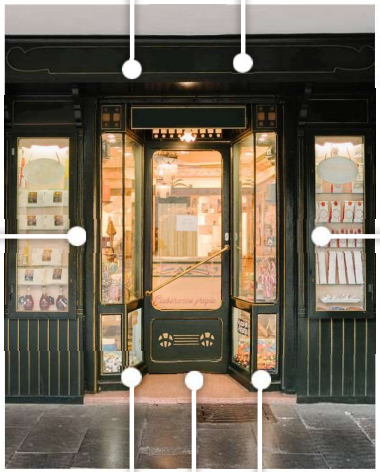


Finances & invoices



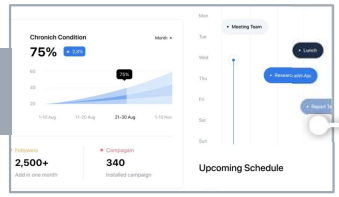
Remote Access, Order & Supplier info





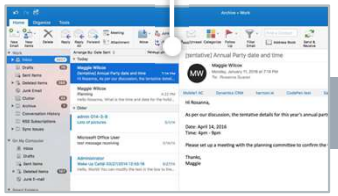
Distributed workforce & employee info

Cloud, Mobile & Web Applications



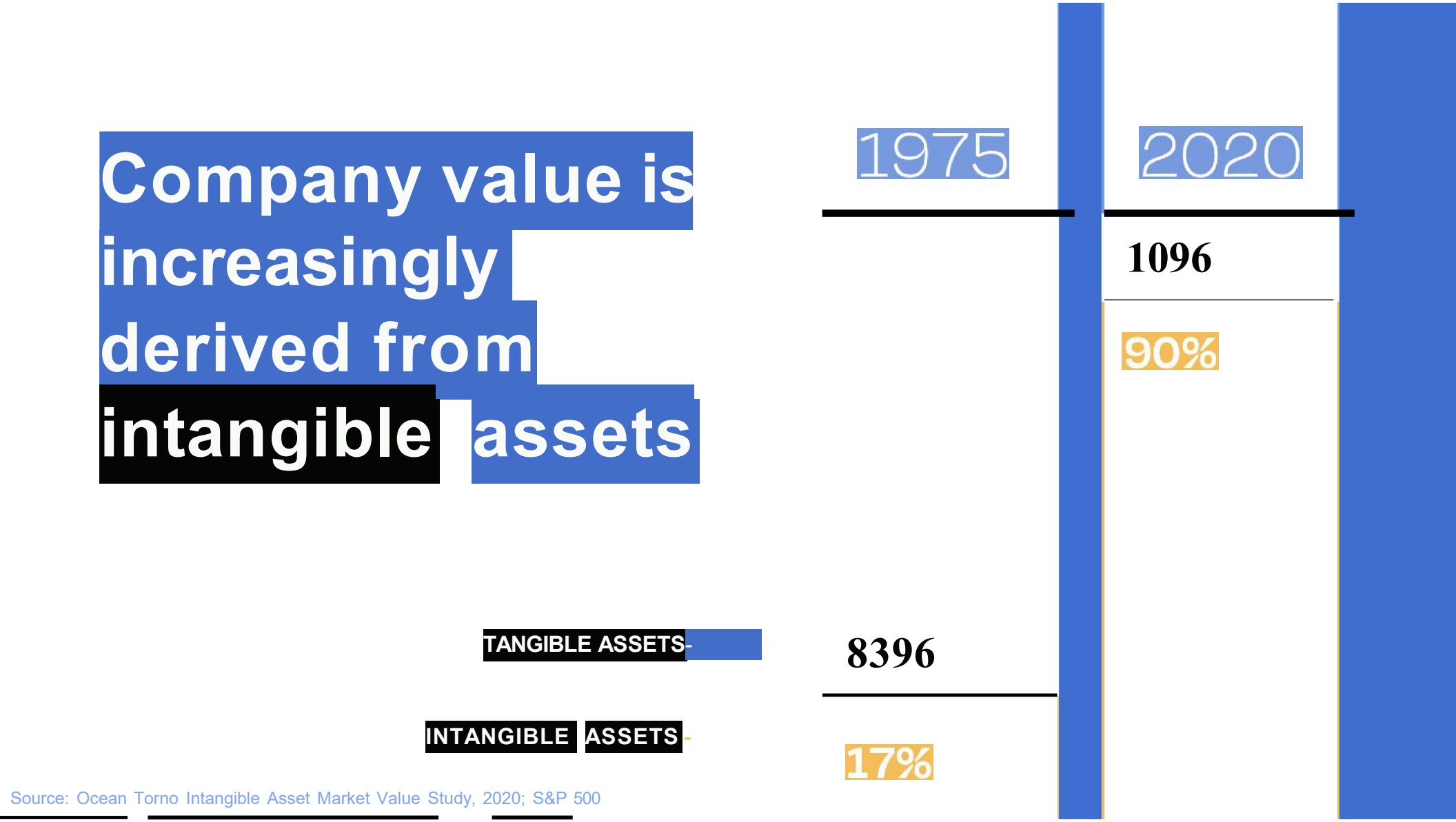
Payroll

Email



*IDC FutureScape: Worldwide Digital Transformation 2021 Predictions

Company value is increasingly derived from intangible assets



Source: Ocean Torno Intangible Asset Market Value Study, 2020; S&P 500

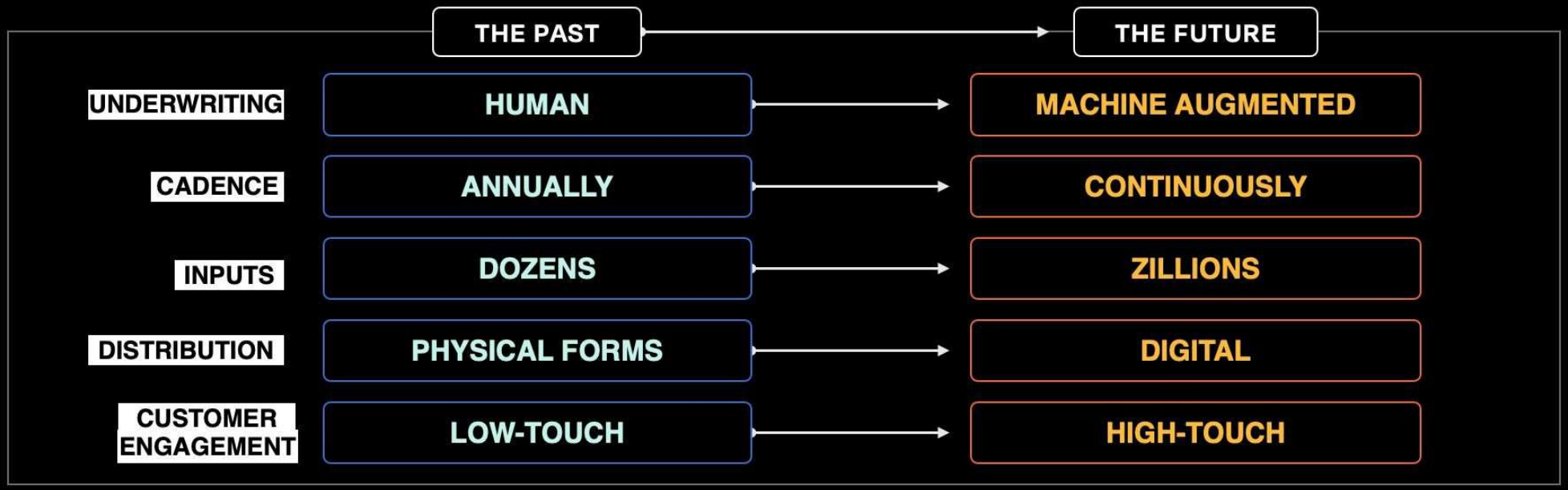
Then… along came cyber…

- Technology evolution is dynamic and changes risk exposure.
- Risk itself is incredibly dynamic since new vulnerabilities appear on a daily basis.
- A single individual can cause a widespread amount of damage.
- The types of threats depend on heterogeneity of the technology stack and every single company is different.
- There is a lot of noise in the industry (vendors selling solutions for risk that isn't exploited by attackers, attackers continuously leveraging basic techniques).

Insurance
wasn't built for
a digital world

The insurance industry must shift too

Insurance ecosystem of tomorrow will look very different



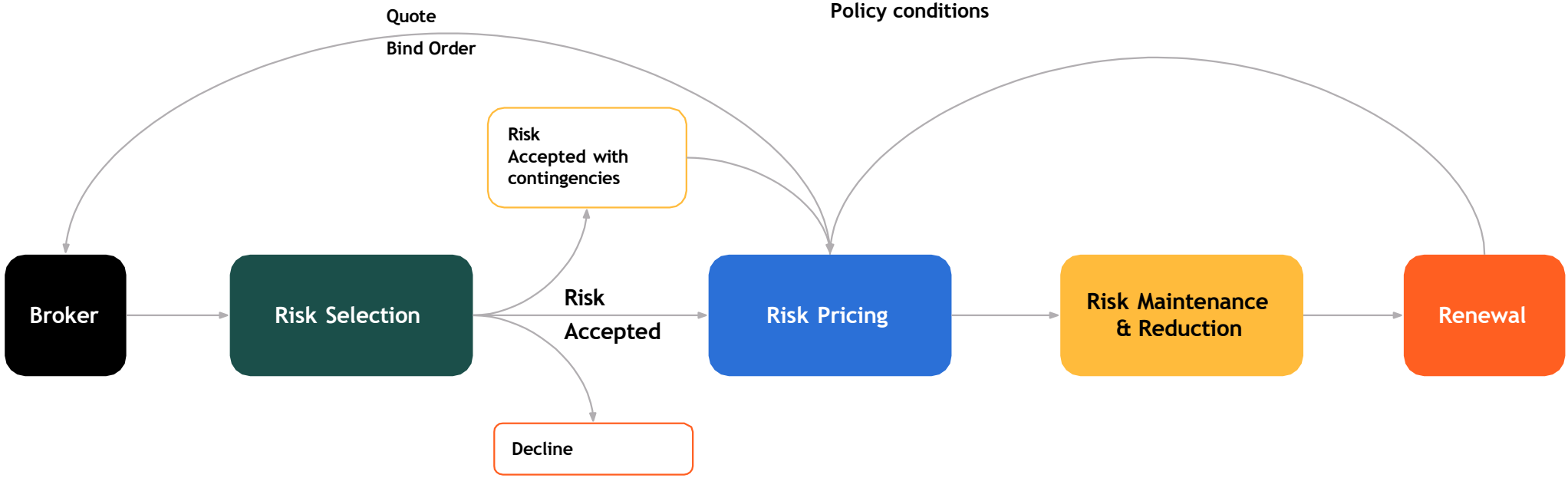
How underwriting works… at a modern cyber insurance provider!

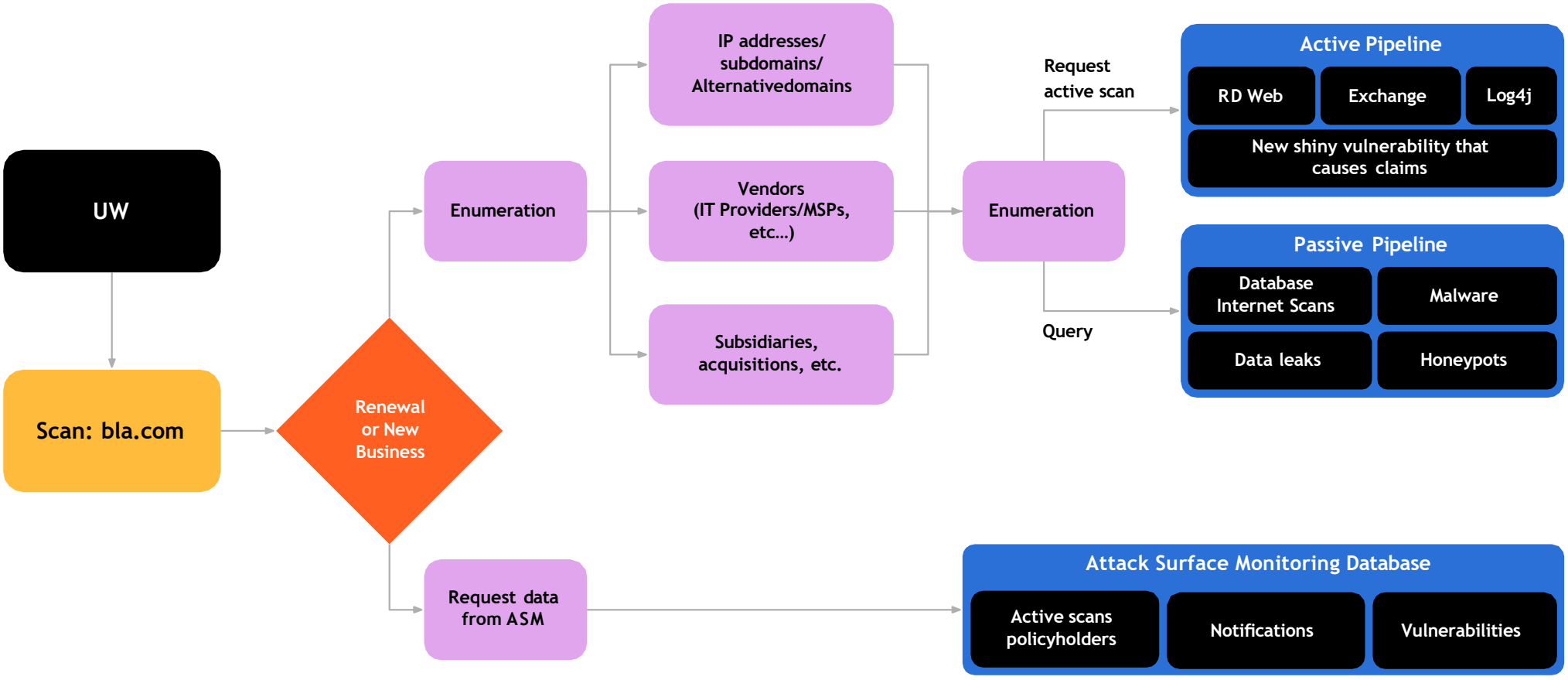
- Not all cyber insurance providers are modern… sometimes, filling out a piece of paper gets you a policy.

- A modern insurance provider:
  - Uses internet-wide scans
  - Collects security controls data (via questionnaires or integrations)
  - Continuously scans, alerts and monitors
  - Has security engineers that meet with customers (usually for companies with revenue >$100M)
  - Ensures everything is data-driven
  - Constantly evolves their understanding and view of digital risk

Lifetime of a Quote and Phases of Risk

Company name:	Bla
Domain:	bla.com
Industry:	Industrials
Employee number:	10
Revenue:	$10,000,000
Policy conditions	




UW
Scan: bla.com
Renewal or New Business
Enumeration
Request data from ASM
IP addresses/ subdomains/ Alternativedomains
Vendors (IT Providers/MSPs, etc...)
Subsidiaries, acquisitions, etc.
Enumeration
Request active scan
Query
Active Pipeline
RD Web
Exchange
Log4j
New shiny vulnerability that causes claims
Passive Pipeline
Database Internet Scans
Malware
Data leaks
Honeypots
Attack Surface Monitoring Database
Active scans policyholders
Notifications
Vulnerabilities

Our risk view: 2023

Our risk view: 2024

Myth: If I buy cyber insurance, I don't need to invest in cybersecurity!

Answer: Wrong ❌

The reality:

- Cyber insurance actually requires you to have a minimum set of security controls or issues addressed before your policy is active (and some technical issues need to be addressed within a certain time window of notification).
- It continuously gives extra incentives for companies to keep updating, patching, and to practice defense-in-depth.
- These days, many companies have a contractual need to have cyber insurance, so it’s one way to enforce good practices.
- And when it all goes wrong (and eventually it does…) you have a partner to financially help you recover.

Treat cyber like other business risks

AVOID

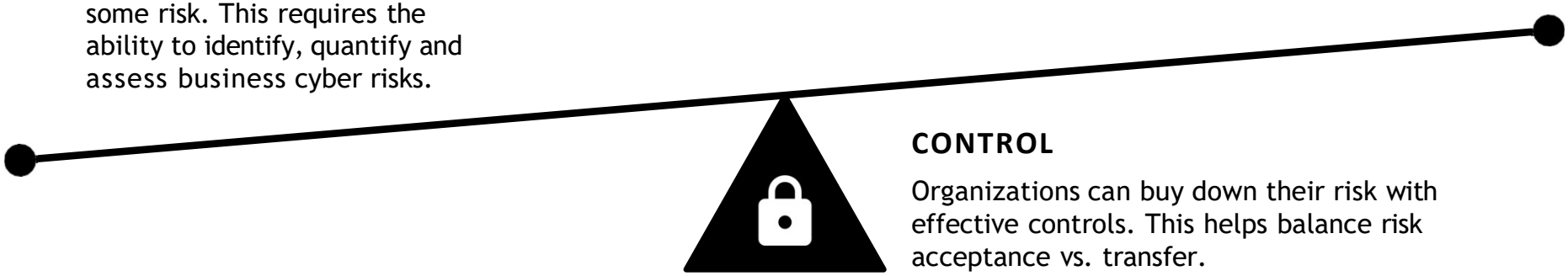
Not always an option, but some risks can and should be avoided.

TRANSFER

Residual risk the organization can't accept, control or avoid can be transferred. This is where cyber insurance comes in.

ACCEPT

All organizations must accept some risk. This requires the ability to identify, quantify and assess business cyber risks.



CONTROL

Organizations can buy down their risk with effective controls. This helps balance risk acceptance vs. transfer.

Myth: Cyber Insurance claims aren't paid.

Answer: Wrong ❌

The reality:

- This comes mostly from the now famous Mondelez case, where the company filed for damages with Zürich Insurance due to a NotPetya attack in 2017 and were refused payment.

- Here is an important fact often overlooked about that case: At that time, Mondelez **DID NOT** have cyber insurance.
  - They tried filing their claim under their property insurance and got denied, but due to information dilution overtime and hearsay, cyber insurance ended up targeted by people reading the news about this case.

- The reality is that the large majority of cyber insurance claims **do** get paid.

Cyber Insurance is proven at scale

74,000

Critical vulnerabilities fixed[1]

64%

Fewer cyber claims[2]

$86M

Stolen funds recovered[1]

$285M

Claims paid[1]

52%

Incidents handled at no cost[3]

1. Coalition claims and incident data. 2. 2023 Coalition Claims Report. 3. 2024 Coalition Claims Report.

Myth: Cyber Insurance is fueling ransomware.

Answer: Wrong ❌

The reality:

- Critics say cyber insurers pay ransoms because it's cheaper than incurring other business disruption costs. However, insurers often incur higher incident costs than the initial ransom demand, spending more on crisis response and recovery expenses.

- Data shows that **a fraction of claims costs go toward ransom payments** because insurance providers prioritize and fund strategies to avoid paying[1].

- We always try to find solutions for the customers not to pay ransom demands (paying is always the last resort).

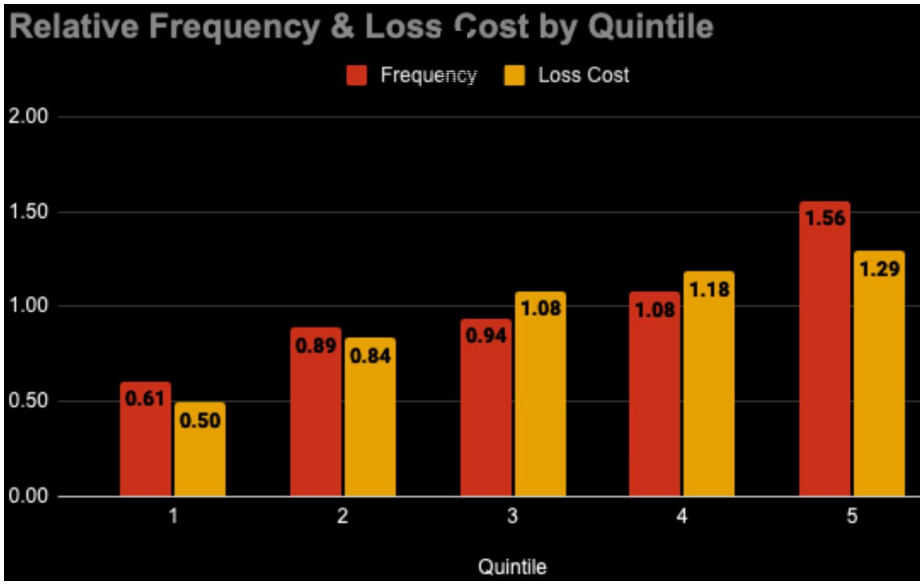
- If anything, insurers have been actively reducing the rate of compromise to prevent infections that force the payment decision.

1. *NetDiligence Cyber Claims Study 2023 Report*

- Only **40%** of policyholders who experienced a ransomware attack paid ransom demands.
- We helped negotiate down ransom demands by **64%** of the original demand.
- As ransom payments hit $1B globally Coalition ransomware severity dropped **54%** in 2H 2023.
- Yet, **myths** persist that about ransomware and cyber insurance.

How can cyber insurance help cybersecurity?

- The cybersecurity market has a “vendor overload” problem and a “solutions looking for a problem” problem.
- Insurance plays the big number game, we get data across thousands of customers.
- This allows us to gather data about which security solutions, products, and vulnerabilities actually make a difference.
  - This is part of the process of creating a pricing model and measuring underwriting efficiency.
- Bringing a bit of science to the art of infosec…



Data-driven insights...

EXPOSED FORTINET DEVICES

"Businesses with internet-exposed Fortinet devices were **twice as likely** to experience a claim in 2023"

- 2024 CYBER CLAIMS REPORT

REMOTE DESKTOP PROTOCOL (RDP)

"Policyholders using internet-exposed RDP were **2.5 times** more likely to experience a claim in 2023"

- 2024 CYBER CLAIMS REPORT

ANY CRITICAL VULNERABILITY

"Policyholders with one unresolved critical vulnerability of any kind were **33% more likely** to experience a claim."

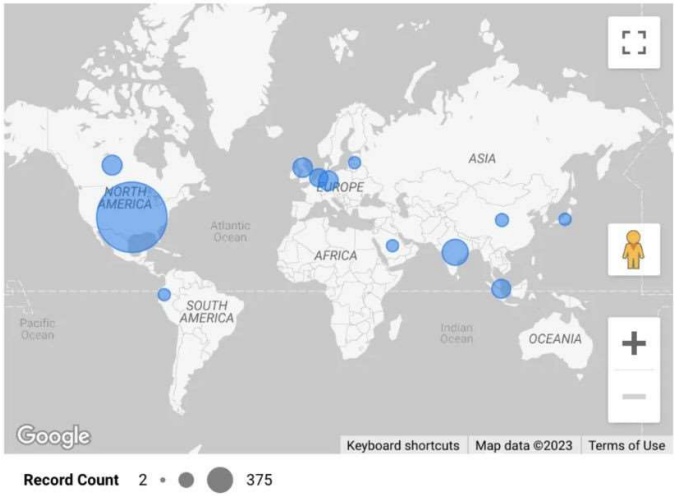
- 2023 CYBER CLAIMS REPORT

CASE STUDY: Unpacking the MOVEit Vulnerability

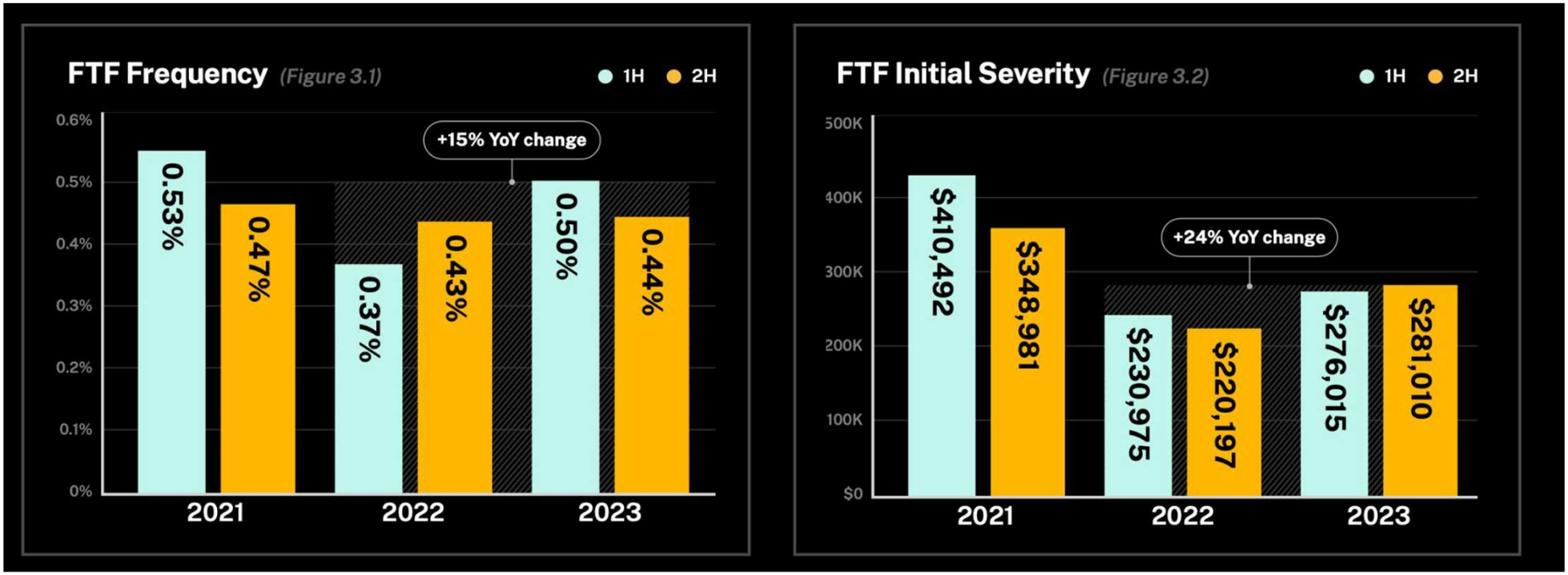
- **November 2022:** We observed threat actor scanning activity for MOVEit software through our honeypot network - **6+ months before the vulnerability was publicly disclosed.**
    - Honeypot activity caused us to start proactively scanning for the technology in all applicants and policyholders.
- **June 2023:** When the vulnerability was publicly disclosed, we already knew which policyholders were affected and notified them within minutes of the announcement. Most of our policyholders had patched by July 2. No claims arose.
- **Now**: Any new applicant receives a technical contingency on their quote if they are using MOVEit to ensure they patch it and where possible put it behind a Zero Trust solution.

# of times honeypots were scanned for MOVEit

	Date (Year Month) ▲	Count
1.	Nov 2022	4
2.	Dec 2022	2
3.	Jan 2023	2
4.	Feb 2023	6
5.	Mar 2023	2
6.	May 2023	88
7.	Jun 2023	615



We talk a lot about ransomware, but funds transfer fraud (FTF) is also incredibly painful.



And the modern cyber insurance providers have great track records in funds recovery…

Clawbacks in 2023

$38M

Total FTF recovery

$470K

Average amount recovered per FTF claim when recovery was successful

46%

FTF events with a full recovery when recovery was successful

102%

Increase in total FTF recovery amount since 2022

Final Thoughts

- The future will see the lines between cybersecurity and cyber insurance blend.
- Cyber insurance providers are big fans of MDR and many of them offer their own MDR services
- Incident response is already a pretty big tool in pretty much every insurer's toolkit.
- Modern cyber insurance providers usually offer TPRM and external scanning with monitoring/notification. We will continue to see more products being offered (and even products being built by cyber insurance providers).
- Insurers are perfectly placed to help with risk quantification (lots of technical data and loss data), and they are always looking for partners, creating an interesting channel and opportunities for security startups/companies.