EPIPHANY SYSTEMS

Risk Hunting for the **Cyber Insurance Industry**

CYBERCRIME IS GROWING EXPONENTIALLY, ALONG WITH THE REMOTE WORKFORCE.

CYBER POLICIES MAKE UP ONLY A SMALL PART OF THE US PROPERTY & CASUALTY INSURANCE MARKET...FOR NOW.

RANSOMWARE ATTACKS HAVE **DOUBLED**.

ATTACKS ON REMOTE DESKTOPS HAVE **QUADRUPLED**.

PHISHING EMAILS HAVE **TRIPLED**.

AND THE NUMBER OF MALICIOUS FILES CONTAINING THE WORD "ZOOM" HAS **MULTIPLIED TWENTY-FOLD**.

With cyberattacks occurring more often—and inflicting more damage—more organizations want cyber insurance. As a result, cyber is one of the fastest-growing segments of the insurance business. The volume of cyber policy premiums has more than doubled since 2015, according to the Federal Reserve.

And the upside potential for growth is tremendous. A report by the US Council of Economic Advisers estimates that cyberattacks cost the US more than $100 billion annually. Yet the Federal Reserve notes that US insurance companies paid out just $356 million in claims that year, <1% of estimated losses.

Still, for insurers, cyber policies represent significant uncertainty and risk, as well as an opportunity to increase revenue and profits.

CORE CHALLENGES FOR CYBER INSURANCE

To meet the rapidly growing demand for cyber policies, insurers have to grapple with many complex factors:

- **LIMITED HISTORICAL DATA ON WHICH TO BASE PREMIUMS AND LOSS LIMITS.** Cybercrime is a relatively new phenomenon with irregular loss patterns (unlike, say, auto insurance). Adding to the uncertainty, many cybercrime victims do not go public with their losses (to avoid reputational damage).

- **UNPREDICTABILITY OF FUTURE CYBER RISKS.** Digital technology has evolved at light speed, and so has cybercrime. Private hackers share tools and techniques on the Dark Web. Nation-states develop new methods to infiltrate networks. Last year's attacks do not foretell this year's—so the risk posture of insureds changes constantly.

- **RISK OF SIMULTANEOUS, INTERRELATED LOSSES.** Cyberattacks spread at virtually limitless scale. So a single malware program could hit thousands of insureds at the same time. A single attack on a centralized network, like a cloud computing platform, could also affect thousands of policy holders simultaneously.

- **RISK OF MASSIVE, CASCADING LOSSES.** The unchecked spread of malware through critical infrastructure poses a particularly high risk of enormous insurance payouts. For example, Russia's 2015 BlackEnergy and 2017 NotPetya cyberattacks caused, respectively, significant damage to Ukraine's electrical grid and as much as $10 billion in economic costs.

THESE UNCERTAINTIES LEAD TO FUNDAMENTAL QUESTIONS FOR INSURERS

"Should we offer cyber insurance policies at all?

"Can we protect ourselves and still make the policies attractive to clients?"

"If we do write cyber policies, how restrictive should the coverage be?

"Can we set premiums high enough to cover our risk profitably, without making policies prohibitively expensive?"

ADDITIONAL COMPLEXITY FOR CYBER INSURERS

Cyber insurance policies vary widely in what they cover and exclude; there are no industry standards. The industry also lacks a common language to define risks and quantify them. This creates inconsistency and confusion for both insurers and would-be policy buyers.

A 2019 survey cited by the Federal Reserve found that *71% of large-company CFOs thought their policies covered most cyberattack damages*. But they also expected that such attacks would devalue their brands, reduce revenue, undermine investor confidence, and create regulatory compliance issues. *And cyber policies typically do not cover any of those damages.*

Legal liability represents another area of uncertainty for cyber insurers. Laying blame for cyberattacks can create disputes between insurers and policyholders, with relatively little legal precedent. For example, in 2019 the Supreme Court let stand a decision allowing consumers to sue Zappos.com for a 2012 data breach. The impact on Zappos' insurers could obviously be significant.

Another case of particular importance to cyber insurers is Mondelēz v. Zurich Insurance. Mondelēz suffered $100 million in damages from a NotPetya attack. But its insurer, Zurich, withheld payment, claiming that the cyberattack fell under its "act of war" exclusion. As of mid-2020, the case was still unresolved.

Cyber terrorism represents a related legal gray area. The 2002 Terrorism Risk Insurance Act (TRIA) and its 2015 extension enable insurers to offer affordable terrorism risk insurance. But while TRIA includes cyber insurance, no cyberattack has ever been TRIA-certified as an act of terrorism.

In fact, TRIA may never apply to a cyberattack. The Act was aimed at physical damage to infrastructure and loss of human life, not financial impact. And the nation-states that carry out cyberattacks are not defined as "terrorist organizations." So a state-sponsored cyberattack could be an "act of war" exclusion for insurers, not an act protected under TRIA.

CYBERATTACKS GROW DESPITE IT EFFORTS

IT organizations do their best to improve cybersecurity with the tools at their disposal. They segment networks to isolate key systems, use configuration management tools, and scan and patch vulnerabilities.

But these approaches focus on a limited number of technical issues, which account for only about one-quarter of all cyber risks. They do not fully cover wider-ranging problems with misconfigurations, permissions, data exposures, and simple IT oversights that cause security "drift."

Also, most security tools do not understand technical issues in context with their real-world impacts. So IT teams get bogged down in triage. Overwhelmed with alerts, security analysts cannot prioritize issues by the impact they might actually have on core business functions.

Analysts can only react to the latest tactical "fires." They can't proactively hunt for strategic risks that pose the gravest consequences to revenue, brand value, business relationships, infrastructure, and other critical assets.

AS A RESULT, CYBERATTACKS CONTINUE TO PROLIFERATE—AND SUCCEED—IN EVERY BUSINESS AND GOVERNMENT ENVIRONMENT.

WHAT CYBER INSURERS NEED

With limited historical cyber risk data, constantly changing attack surfaces, and the potential for interrelated or cascading losses, the cyber insurance industry needs a better way to understand risk conditions and their potential downstream impacts.

More specifically, insurers and their clients need a way to hunt for risks—and mitigate them—before cyberattacks occur. That includes:

Empirical data on the risk postures of potential policyholders

Quantified values for policyholders' business risks

Common visualizations & language for risk across industries

Predictive models prioritizing risks by business value

The ability to assess, quantify, and prioritize business risks is especially important in light of legal uncertainties. To reduce the chance of disputes, insurers need greater clarity when underwriting cyber policies. As the Federal Reserve noted:

> *"Better modeling of cyberattacks should help insurers measure their accumulation of interrelated risks, and improved cybersecurity standards and practices may help businesses avoid such catastrophic attacks."*

Cyber insurers should be able to answer questions like these:

- Do we understand the potential entry points for attacks on client networks?
- Where do ransomware and other attacks have the highest probability of entry?
- Do we understand the combinations of technical conditions that allow attacks to succeed?
- What is the likelihood that particular mitigations will effectively correct those conditions?
- Do we understand how attacks can spread?
- Have we modeled the interrelationships of assets throughout each environment?
- Do we understand which types of attacks have the highest probability of success?
- If an attack occurs, do we understand what mitigations would minimize the impact?

NEW RISK HUNTING TECHNIQUES OFFER A SOLUTION FOR CYBER INSURERS

"Risk Hunting" tools, like Digitalware's Epiphany Intelligence Platform™, provide answers to these kinds of questions.

A Risk Hunting platform absorbs data from existing network, security, and domain sources. (Epiphany is agentless; it doesn't directly interrogate data sources, so it doesn't disrupt any processes or operations.)

Risk Hunting looks at the current state of all technical risks—including those common IT issues that cause security drift. Risk Hunting also analyzes how those risks could potentially migrate across network paths. And Risk Hunting integrates an understanding of the business value of each node on the network.

THAT ALL TRANSLATES INTO AN ABILITY TO QUANTIFY CYBER RISK IN CONTEXT WITH WHAT IS MOST VALUABLE TO AN ORGANIZATION.

For cyber insurance providers, that means:

- Assessing current cyber risks in client environments—and guiding fast mitigation
  - Understanding critical risk areas (cloud, endpoint, email, etc.)
  - Pinpointing the most urgent risks (by business value)
  - Showing the most effective way to reduce risks
- Enabling clients to continuously enforce security policies, monitor regulatory compliance, control cyber hygiene, and improve risk posture
- Developing better cyber risk metrics for industry benchmarks, trends, and predictive modeling
- Communicating and visualizing cyber risks with a common data set for all parties
- Improving policy-writing with more informed decisions, value-added offerings, and incentives for client retention

For cyber insurers, the need for better risk management has never been more urgent.

RISK HUNTING WITH EPIPHANY ANSWERS THE CALL.

Awareness powers protection.

Contact us today to get started with Epiphany.

Contact Us

ABOUT EPIPHANY SYSTEMS

Epiphany delivers world-class cybersecurity solutions for enterprises in every sector of government and industry, including the Fortune 500. We are dedicated to reducing technical and business risks through innovative technologies, including artificial intelligence and machine learning.

Our mission is to safeguard our clients' data, assets, and operations across the globe. We assess each client's unique needs and challenges to ensure that their risks are visible, managed, and mitigated. If it's connected, it must be protected.