QOMPLX:

Mind the Gap:
The Underinsurance of Cyber Risk

Insurance presently covers less than half of companies' cyber exposures. Emerging risk management technology holds the key to closing this gap and reducing cyber risk overall.

DES-470R

In a 2020 poll, global companies voted cyber was their greatest concern, ahead of business interruption and climate change.

Introduction

The Travelex cyber attack has once again demonstrated that ransomware is a real and present threat, even for the most sophisticated organisations. When the foreign exchange giant fell victim to the Sodinokibi ransomware[1] on New Year's Eve 2019, they suffered an extended period of systems interruption as they struggled to restore encrypted files. The ransomware's attack also rippled through to several third-party exchange services that rely on Travelex's systems. End customers are not amused.

In a 2020 poll by Allianz Risk Barometer, global companies voted cyber was their greatest concern, ahead of business interruption and climate change. It is the first time cyber has topped the list of concerns in the annual survey of CEOs, risk managers, brokers and insurance experts spanning 100 countries.

The poll demonstrates that cyber threat awareness is growing, driven by companies' growing reliance on data and IT systems and more damaging and expensive cyber incidents. Dependence and interdependence drives exposure – and it is growing.

The likelihood that breaches will result in lawsuits and litigation is increasing, according to Allianz. It is estimated that up to 90% of the c.$3 billion in insurance claims arising from the 2017 Petya/NotPetya attack came from non-affirmative, or 'silent cyber', coverage. This includes the ongoing litigation between pharmaceutical giant Merck and its carriers, where claims brought under it's property all-risks policy were denied on the basis of war exclusions. While a number of impacted carriers have already settled, the insurance industry will undoubtedly introduce stronger exclusionary language in the future.

Moves by regulators and the insurance industry to tackle some of the issues created by war exclusions and silent cyber have made significant strides in addressing the issues surrounding non-affirmative cover and ensuring cyber insurance is fit for purpose. However, they do not go far enough. Global organisations remain exposed to the cyber threat due to gaps in current approaches to risk management, while at the same time this prevents insurers from gaining any real insight into their underlying exposures and how these risks accumulate within a book of business.

With carriers focusing on reducing their silent cyber exposure, clients will look to the dedicated cyber liability market to hedge their exposures. Unfortunately, dedicated cyber policies are not all created equal. Companies can still find their balance sheets exposed to significant uninsured financial losses. Certain aspects of business interruption, reputational damage, fines and penalties and losses due to management distraction are not indemnified under many cyber policies.

[1] https://www.zdnet.com/article/two-weeks-after-ransomware-attack-travelex-says-some-systems-are-now-back-online/

Data science and telematics are the keys to closing the cyber gap.

Many clients are struggling to quantify the size and nature of their cyber exposure and how much of what kinds of insurance coverage to buy. Insurers are equally uncertain about what they are actually selling and are trading more than they are underwriting. Our QOMPLX Cyber Risk Series offers a new way to look at the problem – better analytics. Data science and telematics are the keys to closing the cyber underinsurance gap and creating a more transparent marketplace for cyber insurance.

Key Points

Current approaches to cyber risk management and insurance are inadequate

A lack of insight is exposing organisations and their insurance carriers to significant cyber losses, potentially systemic in nature

Insurers and brokers must drive awareness of data analytics and telematics, a combined solution that can improve organisations' resilience to cyber threats and shape ongoing responses

By dramatically improving risk insight, data telematics can support the growth of the cyber insurance market

Cyber customers are realising they are not necessarily as confident in what they thought they were buying as they would like to be.

Jason Crabtree
CEO, QOMPLX

Part One: After NotPetya

The disconnect between present cyber insurance policies and the actual exposure faced by global organisations has become increasingly clear over the past two years. The 2017 Petya/NotPetya attack has cost insurers over $3 billion[2], according to Property Claim Services, with a large proportion of the claims paid by the property insurance market.

Some of the losses emanating from the NotPetya ransomware attack were denied by property insurers on the basis of war exclusions. The US government said the malware was released by Russian military hackers, directed at Ukraine, but that several major global companies, including Merck, Mondelez, Reckitt Benckiser, FedEx, and Moller-Maersk, were caught in the firing line.

Insurance companies woke up to the fact that an event on this scale could trigger losses under both standalone cyber insurance as well as property all-risks policies, even where cyber as a peril was not explicitly covered. The potential for these unexpected risk aggregations also began to concern industry regulators.

"There are a lot of questions about terrorism or nation state exclusions, attribution-related issues that are exceedingly problematic for a whole host of reasons," says Jason Crabtree, CEO and Co-Founder of QOMPLX. "Cyber customers are realising they are not necessarily as confident in what they thought they were buying as they would like to be, and they are recognising that they are experiencing more of these events."

"Insurers and regulators are recognising there is now material capital at risk," he continues. "The market has now got enough exposure to this risk that we have to start having a quantitatively-grounded discussion on the degree to which it is both systemically important and the degree to which it impacts specific relationships between insureds and their carriers on an ongoing basis."

In January 2019, the UK Prudential Regulation Authority (PRA) called on insurers to produce an "action plan" setting out their plans to reduce unintended exposure to silent cyber risk. Lloyd's of London called for its syndicates to provide clarity on cyber coverage under property policies by 1 January 2020, with other classes of business set to follow.

Major commercial insurance companies, including Allianz and AIG, have committed to providing explicit coverage with property and cyber underwriters joining forces in many instances. Others, however, have reacted by withdrawing or limiting cyber coverage amid fears over risk aggregations. This is despite the fact that cyber as a class of business has become an important source of income. Lacking more sophisticated tools with which to measure and monitor the underlying risk, these insurance carriers are becoming more sceptical[3].

[2] https://www.verisk.com/siteassets/media/pcs/original-risk-when-cyber-hits-a-beaten-balance-sheet.pdf
[3] https://bit.ly/2HAwBsv

There is anticipation cyber could become the next peak catastrophic peril.

There is concern over the prospect of major property catastrophe and cyber catastrophe losses in the same year and the pressure this will exert on insurer balance sheets. "Business interruption/system failure continues to be an area of concern for underwriters," notes broker Willis Towers Watson. "Heavily exposed industry classes, such as aviation, manufacturing and transportation, have seen increased underwriting scrutiny."

The Next Peak Peril

Standalone cyber premiums currently account for less than 1% of the international commercial property and casualty insurance market. However, there is anticipation cyber could become the next peak catastrophic peril, alongside Florida wind and California earthquake, with the market growing from its current level of around $6 billion to over $20 billion by 2025. As more businesses and devices become network enabled, the total economic exposure continues to outpace insurance growth.

Some market commentators have speculated that ultimately the insurance industry will consist of three main sectors: property, casualty and cyber (PC&C)[4]. However, what should be a significant opportunity has not yet materialised and total limits for standalone cyber insurance remain low. Meanwhile, the increased prevalence of ransomware losses is influencing the overall profitability of cyber as a class of business and exerting upward pressure on rates, according to Willis Re[5].

Following NotPetya, insurance consultancy Mactavish[6] controversially questioned the value of cyber insurance. It focused on eight coverage flaws it said were prevalent across the burgeoning market (see box-out) and argued that "policies failed to meet the client needs for which they were sold". However, it acknowledged that cyber insurance is a growing necessity in a technology-reliant business landscape in which cyber risks are escalating and recommended that underwriters do more to tailor their coverage to the insured.

Indeed, the value of bespoke cyber insurance is irrefutable when the coverage is written with the correct wordings and proper transparency. Cyber claims are growing in both frequency and severity, according to AIG[7], reflecting an increase over time in the carrier's cyber book of business but also demonstrating "the product is responding to clients' needs". It notes a shift towards a preference for affirmative cyber cover.

Amid a lack of understanding over the risk accumulations presented by some of the more challenging catastrophe scenarios (see box), there has been a

[4] https://www.capsicumre.com/wp-content/uploads/2018/10/Capsicum-Re-Evolutionary-Drive-of-Non-Affirmative-Cyber.pdf
[5] https://bit.ly/2HEqaEA
[6] https://www.mactavishgroup.com/wp-content/uploads/2018/11/Mactavish-Cyber-Risk-Insurance-Report-November-2018.pdf
[7] https://www.aig.co.uk/content/dam/aig/emea/regional-assets/documents/aig-cyber-claims-2019.pdf

retrenchment on both the insurance and reinsurance side. As a man-made peril that transcends geographies, classes of business and types of industry, it is becoming apparent to carriers and regulators that normal aggregation methodologies do not apply to cyber catastrophic losses.

"Unlike anything the insurance industry has had to deal with up until the arrival of terrorism, you're insuring against a peril where you have a sentient attacker for the most part," explains Alastair Speare-Cole, president of insurance at QOMPLX. "How does the insurance industry model, price and issue policies for a peril where the attack types are constantly altering? It's an arms race."

Common Cyber Insurance Limitations

Based on Mactavish analysis of market-leading standard cyber insurance wordings, there are at least eight common flaws, meaning buyers need to negotiate bespoke cover.

1 Cover can be limited to events triggered by attacks or unauthorized activity—excluding cover for issues caused by accidental errors or omissions

2 Data breach costs can be limited, e.g. covering only costs that the business is strictly legally required to incur (as opposed to much greater costs which would be incurred in practice)

3 Systems interruption cover can be limited to only the brief period of actual network interruption, providing no cover for the more significant knock-on revenue impact in the period after IT systems are restored but the business is still disrupted

4 Cover for systems delivered by outsourced service providers (many businesses' most significant exposure) varies significantly and is often limited or excluded

5 Exclusions for software in development or systems being rolled out are common and can be unclear or in the worst cases exclude events relating to any recently updated systems

6 Where contractors cause issues (e.g. a data breach) but the business is legally responsible, policies will sometimes not respond

7 Notification requirements are often complex and onerous

8 During a cyber incident, businesses often have no freedom to choose their IT, PR, or legal specialists, as the policy only covers insurer appointed advisors[8]

[8] https://www.mactavishgroup.com/wp-content/uploads/2018/11/Mactavish-Cyber-Risk-Insurance-Report-November-2018.pdf

Examples of Systemic Cyber Scenarios

Source: Capsicum Re

Northeast Blackout

A piece of malware infects electricity generation control rooms in parts of the Northeastern United States.

SWIFT Attack

Vast messaging network used by banks and other financial institutions to securely send and receive money transfer instructions is hacked.

Cyber Induced Fire

Hackers exploit vulnerabilities in the smart-battery management system of a common brand of laptop, sending their lithium-ion batteries into a thermal runaway state.

PCS Explosion

Manipulation of platform control systems to cause a structural misalignment of wellheads, release of oil and gas and fire.

Offshore Energy

Offshore drilling units are hit by a malware targeting their programmable logic controllers used to control systems of mobile drilling units.

Cloud Provider

A global CSP with a major market share has a disgruntled employee who releases malware into the CSP network causing extended service outage to several of its hubs.

Ransomware

A criminal cyber gang infects multiple companies with ransomware demanding a ransom payment for each company within a time limit, otherwise files may be deleted.

Logic Bomb

A logic bomb causes a bank to suffer financial data corruption, causing stock markets to be impacted as access to bank accounts and cash machines freeze[9].

> The prolonged outage of a major cloud provider could cost the industry in excess of $14 billion in claims, with other scenarios as high as $20 billion[10].

[9] https://www.capsicumre.com/wp-content/uploads/2018/10/Capsicum-Re-Evolutionary-Drive-of-Non-Affirmative-Cyber.pdf

[10] http://www.guycarp.com/insights/2019-guy-carpenter-cybercube-cyber-catastrophe-loss-study.html

Part Two: Cyber Risk Management

A major factor hindering the growth and development of the cyber insurance market are current approaches to risk management and how underwriters are using this as a tool for pricing and aggregate risk management. Neither of the two present methods of measuring companies' sophistication in relation to cyber risk management reveal the complete picture or directly seeks to improve the underlying risk.

The Questionnaire Approach

At its crudest level, the underwriting, or risk assessment, questionnaire approach is used to gather information about prospective insureds. Risk and control self-assessments (RCSAs), which organisations administer to themselves in order to meet regulatory requirements, are a close cousin of questionnaires.

Risk questionnaires are provided by insurers to the applicant and consist of a series of questions relating to the company's use of IT and information assets in supporting the business. Self-attestation is most common but auditors or third-party evaluators are also increasingly common.

Questionnaires are used to gain a reasonable approximation of the overall security profile of the applicant but are fraught with limitations - including weakness and inaccuracy stemming from wordings, user expertise, limited scope, and self-attestation incentives/bias. This is because they do not offer a complete and accurate picture of potential loss.

For instance, many questionnaires are overly focused on compliance or maturity models – not actual security. Defending an organisation against real attackers is distinct from gaining and maintaining compliance certifications or attaining maturity model scores, but many industry models are incapable of handling these distinct constructs. "To best assess the true risk of loss, especially for business disruption, it is necessary to 'score' a prospective insured using the mindset of an attacker not an auditor," explains QOMPLX's Jason Crabtree.

A 2017 study by the European Union Agency for Network and Information Security (ENISA)[11] found very little standardisation between carriers when it came to question sets used. Moreover, there was a significant difference between the security standards used by carriers and the wording of underwriting questionnaires.

Among other things, the researchers attribute the lack of consistency between risk questionnaires to the emerging nature of the cyber insurance market and differing claims histories from one carrier to the next. "Insurers who have rich information from claims history adapt their questionnaire to allow them to focus on mitigating those risks where they historically have had the most claims," was noted in the study.

[11] https://eiopa.europa.eu/Publications/Reports/

In 2019, the widespread abuse and weaponisation of Active Directory and privileges enabled mass ransomware and data exfiltration.

Jason Crabtree
CEO, QOMPLX

The use of claims history in informing underwriting and risk questionnaires is in itself problematic. The kinds of tactics and techniques used by attackers vary in response to defenders' choices and the state of computer security across the industry, explains Crabtree.

"We see far too much emphasis on the need for historical claims data and historical scan data. That's completely negligent. The reality is that networks are changing all the time and the risk is both sentient and dynamic."

"In 2019, the widespread abuse and weaponisation of Active Directory (AD) and privileges enabled mass ransomware and data exfiltration," he continues. "This was further facilitated by low-cost access to tools like Mimikatz and the widespread use of AD as a common part of virtually every IT environment. Ten years earlier, AD exploits were artisan-level skills and no tools were available to make it easy."

External Scanning

External scanning is a maturity-based vulnerability assessment, which attempts to confirm whether the company's controls covering its externally facing services have been implemented in the right way, and there are no obvious vulnerabilities. While external scanning, vulnerability scanning and Open Source Intelligence (OSINT) are related methods of penetration testing, each is also distinct.

Vulnerability scanning has some predictive power and Security Ratings uses observable data to infer that deeper problems exist. Scans are typically carried out in order to achieve regulatory compliance, such as with payment card industry data security standards (PCI DSS), as well as for risk maturity and insurance purposes.

Contrary to general belief, external scans are not a thorough enough approach to cyber risk management. The internals of businesses are at least as important to understand. Disciplined carriers and regulators need a clear guide on what assertions can be made about a given business from its exterior appearance versus those which require an inside look.

"Scanning is the equivalent of walking around the walls of a fortified castle and looking for chinks in its armament," explains Speare-Cole. "OSINT tools are used to look at a company's external features - to find out how many domains they've got, what software appears to be interacting with these domains and how secure they are. External scanning will undoubtedly get more sophisticated over the next six to 12 months, but current approaches do not provide the complete picture."

> *Just as telematics works in a smart home or connected car environment, cyber telematics offers access to real-time data sources.*

'Outside-in' techniques utilise the 'broken windows' theory of security. "They are useful, but both have flaws," says Andy Jaquith, chief information security officer and general manager, Cyber at QOMPLX. "Vulnerability management scans are mostly limited to cyber hygiene issues, such as patching, and while security ratings supply valuable signals, they say little about what's really going on inside."

The majority of organisations continue to take a compliance-driven approach to risk assessment. However, this is moving towards a maturity-based approach. Together, risk questionnaires and external scans give a reasonable indication of the overall security maturity of an organisation. But on their own however, they are insufficient for tracking, measuring and pricing cyber risk on an ongoing and dynamic basis.

"This combination of self-attested and external data can be further refined by incorporating additional sources of information to establish ground truth as viewed from the inside," says Crabtree. "Gaining insight into the vantage point from which a given company's defenders will engage their foe."

"A number of vendors in cyber risk modelling have made outsized claims about their ability to fully assess and monitor organisations from this single external viewpoint, but scepticism is well advised," he adds.

Cyber Telematics

Dynamic risk management is where cyber telematics will become a powerful tool in the future, offering continuous control monitoring and validation and providing actionable intelligence to core business operations. Such a proactive approach to cyber security can support the overall resilience of an organisation by spotting and patching potential issues before they become actual problems.

It is more than identifying vulnerabilities in specific tools or components. Rather, telematics can help defenders and insurers by providing a continuous map of an environment with annotation of potential potholes and pitfalls that lay along the route. "A digital co-pilot for operating the network is a far more complex task, but similar to services like Waze used by millions of drivers when navigating the physical world," says Crabtree.

Just as telematics works in a smart home or connected car environment, cyber telematics offers access to real-time data sources from a wide variety of internal and external sensors. Together these offer a comprehensive understanding of security maturity on an ongoing basis to support event characterisation, current vulnerabilities, ongoing actions from threat actors, and ultimately impact analysis.

Cyber telematics needs to do two things really well in order to be really effective, explains Speare-Cole. "First, it needs to detect at speed," he says.

Insureds may only have a matter of minutes to prevent a hacker before some real damage is done.

Alastair Speare-Cole
President & General Manager, Insurance, QOMPLX

"Insureds may only have a matter of minutes to prevent a hacker before some real damage is done. Second, telematics needs to work with the minimum of false positives. If a fire alarm goes off every day with a false alarm it undermines the response and requires resource to continually investigate issues."

For underwriters and modellers, cyber telematics offers a quantitative risk-based approach for assessing cyber risk, enabling accurate risk pricing and aggregate management. While still in its infancy, such a data-driven approach is essential to the future development of the cyber insurance market as it scales. A rich and exponentially growing pool of internal and external data can offer real-time insight, necessary for carriers to stay on top of a uniquely dynamic exposure with large accumulation potential.

Using advanced analytics to determine how the risk varies from client to client and across a book of business, along with intelligence to predict how the exposure is changing, underwriters will ultimately be empowered to make informed decisions and spread and diversify risk throughout their portfolio. Crucially, this will allow insurers to bring more capacity to bear at a time when the appreciation of the value of affirmative cyber coverage is growing.

The Future: Carrot or Stick?

At present, only a small number of organisations are using cyber telematics to monitor the security maturity of their company networks and to keep track of their changing vulnerability, as these networks and the threat landscape continuously evolve. What will drive wider take-up of this highly sophisticated and effective approach to cyber risk management depends on a number of factors.

Companies and their management will certainly see the value in putting in place an infrastructure that supports a risk-based approach, as it means their overall vulnerability is reduced, including the potential impact of a breach. This will see a shift towards graceful, rather than catastrophic, failure and the growth in importance of independent third-party data analytics providers.

An added incentive for companies adopting cyber telematics will be provided by improved insurance pricing and terms, if their efforts are rewarded with more competitive cyber insurance rates and better, broader coverage. By improving insurers' understanding of the underlying risk, cyber telematics will enable the growth of a class of business that promises to one day be as large and important as mainstream property and casualty insurance.

Unfortunately, it could also be the case that it takes another major and systemic cyber attack to awaken global corporates and their insurers to the need for a more data-driven approach to risk management. Just as the Petya/NotPetya attacks revealed the true extent of the silent cyber exposure (and were nearly much worse), another major loss is likely to unveil unexpected and costly risk

Creating efficient and stable markets in insurance requires a common language and understanding of what the risk is.

accumulations, triggering a second (more severe) wave of claims litigation.

Creating efficient and stable markets in insurance requires a common language and understanding of what the risk is. Before Hurricane Andrew, there was blissful ignorance about the catastrophe potential buried in insurers balance sheets. The resulting losses were astronomically higher than anyone had realised and markets were massively disrupted.

A similar market disruption in cyber is inevitable if we continue business as usual. In order to avoid an Andrew-style market implosion, both buyers and sellers will need to operate differently. Buyers will need to give insurers more access to their physical networks, and insurers will need better technical skills to understand what that network data is telling them.

With QOMPLX's analytical, data, and telematics tools, we can bridge the current market gap and bring buyers and sellers closer together in understanding the nature of cyber risk. Without doubt, generating real underwriting data will be more work than the status quo, but it is far superior to a decade of litigation on a claim that can put a company out of business, or a reactionary insurance market.

The demands of regulators are already playing an important role. Certainly, it is true that regulation has driven markets in the past, albeit at an occasional cost to innovation. If the market does not evolve quickly enough, supervisors will be forced to step in (most likely following adverse losses) and mandate a risk-based approach to cyber in the future, beginning within the financial services sector.

At QOMPLX, we believe the risk and insurance industry is at critical crossroads. There is a recognition that the market has to change the nature of its approach to cyber and that a different toolkit is required. Certainly, if the cyber insurance market is to reach its full potential, cyber underwriters will require richer and more accurate sources of data to support real-time probabilistic modelling.

QOMPLX makes it faster and easier for organisations to integrate disparate internal and external data sources across the enterprise via a unified analytics infrastructure that supports better decision-making at scale. This enterprise data-fabric is called QOMPLX:OS, an enterprise operating system that powers QOMPLX's decision platforms in cybersecurity, insurance, and quantitative finance. Headquartered in Reston, VA, QOMPLX also has offices in New York, Denver, and London. More information about QOMPLX can be found at www.qomplx.com/.