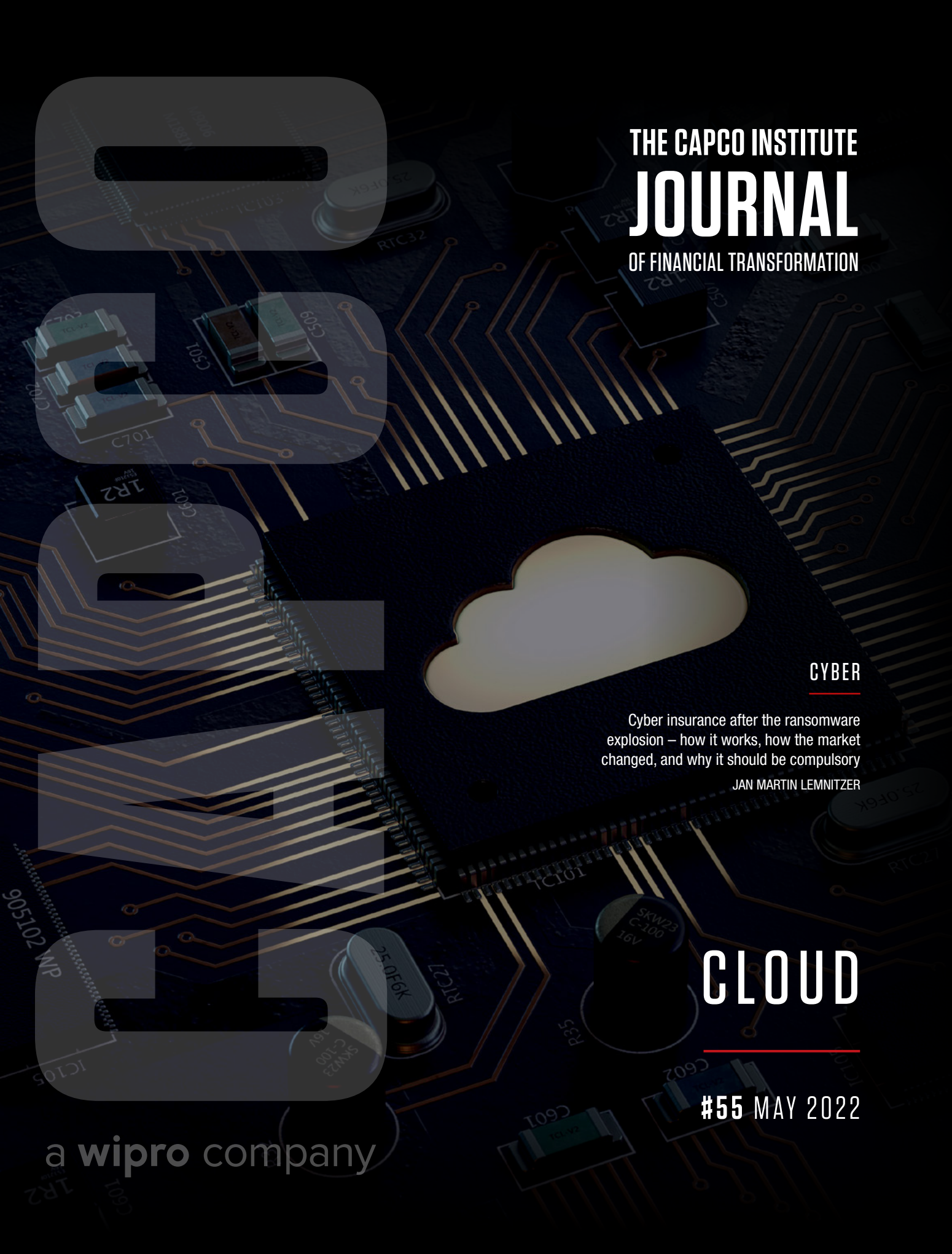

THE CAPCO INSTITUTE

JOURNAL

OF FINANCIAL TRANSFORMATION

CYBER

Cyber insurance after the ransomware explosion – how it works, how the market changed, and why it should be compulsory

JAN MARTIN LEMNITZER

CLOUD

#55 MAY 2022

a **wipro** company

THE CAPCO INSTITUTE

JOURNAL OF FINANCIAL TRANSFORMATION

RECIPIENT OF THE APEX AWARD FOR PUBLICATION EXCELLENCE

CONTENTS

CLOUD

CRYPTO

CYBER

DEAR READER,

Welcome to edition 55 of the Capco Institute Journal of Financial Transformation. Our central theme is cloud computing, which has transformed from an efficiency initiative for our clients, to an indispensable growth driver for financial services.

The pandemic has changed consumer expectations, with consumers now demanding 24/7 access to their financial resources from anywhere, as well as hyper-personalized products that reflect their lifestyle choices.

In this edition of the Journal, we explore the power of cloud and its potential applications through the lens of a joint Capco and Wipro global study, and take a deeper look at the financial services data collected in Wipro FullStride Cloud Services' 2021 Global Survey. The survey was focused on perceptions of cloud and its importance to business strategy from over 1,300 C-level executives and key decision-makers across 11 industries.

The study indicates that cloud is becoming ever more intelligent, hyperconnected, and pervasive, and enables companies to offer their end users the personalized, user-centric experience that they have come to expect. It's clear that only the financial services firms that can successfully leverage cloud, will thrive.

In addition, this edition of the Journal examines important topics around digital assets and decentralized finance, including central bank digital currencies, and bitcoin's impact on the environment, and cybersecurity and resilience.

As ever, you can expect the highest calibre of research and practical guidance from our distinguished contributors, and I trust that this will prove useful in informing your own thinking and decision-making.

Thank you to all our contributors and thank you for reading. I look forward to sharing future editions of the Journal with you.

Lance Levy, **Capco CEO**

CYBER INSURANCE AFTER THE RANSOMWARE EXPLOSION – HOW IT WORKS, HOW THE MARKET CHANGED, AND WHY IT SHOULD BE COMPULSORY

JAN MARTIN LEMNITZER | Department of Digitalization, Copenhagen Business School

ABSTRACT

For two decades, the cyber insurance sector had been a niche sector of the insurance industry: tiny but boasting strong growth rates and enormous profit ratios. Yet, between 2019 and 2022, the cyber insurance industry has been devastated by the impact of the explosion in ransomware, causing huge payouts and escalating losses. Some insurers are now fleeing from the sector entirely. This article will shine some light on how the cyber insurance industry works and how it has responded to the ransomware impact. After discussing why insurers struggle with accurately pricing the cyber risks posed by the companies in their portfolios, it will explore the evidence in support of the claim that having cyber insurance improves a company's IT security. The final section offers a radical proposal to make cyber insurance compulsory for small- and medium-sized companies (SMEs) to tackle their known and longstanding issues with IT security. If combined with an externally established minimum IT security standard developed for SMEs and light regulation on insurance policies, this measure could transform IT security in thousands of companies and vastly improve their resilience against ransomware and other cyberattacks.

1. INTRODUCTION

For two decades, the cyber insurance sector had been a niche sector of the insurance industry: tiny, at less than 1 percent of the size of the greater property and casualty insurance market but boasting strong growth rates and enormous profit ratios [IST (2021)]. This growth accelerated further as many more businesses sought cover after the double shock of NotPetya and WannaCry in 2017. Yet, between 2019 and 2022, the cyber insurance industry has been devastated by the impact of the explosion in ransomware, causing huge payouts and escalating losses. Some insurers are now fleeing from the sector entirely.

This article will explain what the cyber insurance industry offers to clients, how it was hit by ransomware, and how it is responding. To explain how an entire branch of insurance could end up mispricing its products and underestimating risks, section 3 will look at how insurers set premiums and measure the cyber risks posed by the companies in their portfolios, and why they find the task extremely challenging. Section 4 will explore the evidence to support the claim that having cyber insurance improves a company's IT security. The final section will develop a radical proposal to make cyber insurance compulsory for small- and medium-sized companies (SMEs) to tackle their known and longstanding issues with IT security. If combined with an externally set IT

security minimum standard developed for SMEs and light regulation on insurance policies, this measure could transform IT security in thousands of companies and vastly improve their resilience against ransomware and other cyberattacks.

2. WHAT IS CYBER INSURANCE?

Insurance policies covering cyber risk offer companies protection against the escalating costs related to a network breach or successful cyberattack and are sold either as part of a company insurance policy or (as is increasingly common) as a standalone cyber insurance policy. As such, cyber insurance is a risk management practice that transfers residual risk after all other available sensible measures to reduce an organization's cyber risk have been exhausted. Used wisely in conjunction with sensible IT security practices, cyber insurance can provide crucial cover against catastrophic breaches whose consequences might otherwise endanger the survival of the company.

Moreover, good cyber insurance policies offer much more than simply the chance to claim back damages. Next to the financial coverage, they provide access to support services that can be critical in containing and overcoming a cyberattack. Companies will be able to call a specific phone number 24/7 and request the immediate support of a team of sophisticated cybersecurity professionals at the insurer's expense. While the details vary between policies, an increasing number of them are also offering the services of specialists dealing with client data, GDPR exposure, and client management, as well as consultants for branding and media reputation that can support communications with the public and clients about the incident. Moreover, insurers provide quality control for incident responders: they will only call in IT companies who have proven themselves in previous assignments, while a single company looking for post-breach support will find it much harder to decide which IT service providers they can trust in their moment of crisis [Woods and Böhme (2021)]. SMEs will find it impossible to assemble a similar support set-up at short notice and at their own expense.

2.1 Why do so many companies choose not to have cyber insurance?

Although cyber insurance policies have been commercially available for more than two decades, less than 15 percent of organizations globally buy cyber insurance [IST (2021)]. The market is still lopsided and unsettled: the U.S. is by far the largest market for cyber insurance policies, with about 90 percent of all premiums written there, and Europe and Asia making up the remaining 10 percent [OECD (2017)]. One key reason for this difference is that starting with California in 2003, all U.S. states have introduced laws requiring notification of data breaches [Lubin (2019)]. Recent increases in European companies seeking coverage might, therefore, be as much driven by the introduction of E.U. data protection legislation in May 2018 (especially since GDPR comes with huge potential fines for data breaches) as it is by the increasing cyber threat.

One important caveat is that while cyber insurance is a widely used tool among large companies for managing their cyber risks, it remains a niche product for the many smaller- and medium-sized companies (SMEs) that make up a large part of the economy. There are several reasons for that: firstly, small company boards tend to believe that cyberattacks are something that happen to large companies and not to them. Unfortunately, the common view that SMEs are not targeted by ransomware gangs is manifestly false: in the first half of 2020, almost half of all cyber insurance claims came from SMEs [Cimpanu (2020)]. Predictably, direct personal experience of a cyberattack has been identified as a key driver of insurance uptake in this group [Bernard (2020)]. Moreover, company leaders find the wording and coverage details of cyber insurance policies highly confusing – privately, insurance brokers will agree [Insurance Journal (2017)]. Insurers are acutely aware that there are serious problems with the definitions used in the various policies to describe what kind of damage is covered and what is not, especially given the fast-changing market conditions [Rawlings (2014), Kesan and Hayes (2017)]. For example, the terms "data loss" or "data breach" may have different meanings in different policies, making them quite hard to compare [ENISA (2016b)]. Other terms, such as "cyber terrorism", are completely undefined [GAO (2021)]. Insurers know that a more unified approach to policy language would be preferable, but are wary of the huge, concerted effort that would be necessary across the industry. Moreover, a global solution is especially complex since different countries also have their own legal traditions, with specific legal concepts and insurance industry terms based on decades of court precedents. The wide variations of coverage and policy terms suggest a market that is still unsettled [Xie et al. (2020)].

Moreover, many policies list so many exclusions and duties for the policyholder that businesses get concerned about how easy it would be for an insurance provider to find negligence or other behavior breaching the policy [the model policy provided

by the German insurance industry is a good example, see GDV (2017)]. This contributes to a general skepticism among smaller companies about whether such policies can be trusted and will pay out in full in the hour of need. There is some hope that the ransomware epidemic might provide some assurance here: cyber insurers ran into trouble with their portfolios because they paid out so much, not because furious hacked companies canceled their policies [Woods (2022)].

Crucially for budget-strapped small companies, signing up to cyber insurance can require serious effort. This is especially true if the company has never previously conducted a systematic assessment of its own network, patching procedures, and cyber risk exposure. In addition, company leaders know that insurers might demand the replacement of outdated software or IT infrastructure, which can result in considerable expenses. Taken together, these factors mean that while bigger companies have IT departments and usually at least some cyber insurance policy in place, many small companies that would benefit the most from IT guidance, support services, and financial cover do not.

2.2 Cyber insurance and the ransomware impact

Today, the daily reports of companies falling victim to ransomware are persuading companies of all sizes to apply for cyber insurance for the first time or raise the coverage limits on existing policies. Unfortunately, the escalating payouts caused by the ransomware problem have led insurers to make drastic changes to their portfolios. While the first wave of ransomware, targeting companies by encrypting all their data, could be countered by better backup practices, the second wave is practicing a double extortion approach: by threatening to leak stolen internal or client data (which may lead to substantial fines under data protection law, not to mention upset clients) the ransomware gangs are persuading companies to pay up even if they have recent backups. As it turned out, there is no easy fix to counter this extortion scam. In the first half of 2020, insurer Coalition experienced an increase in ransomware claims of 260 percent, with the average ransom demand rising by almost 50 percent [IST (2021)].

That meant that insurers had to adjust their business models. Most of them raised premiums by 30-40 percent or more in the first half of 2021, decreased the maximum coverage limits on offer, or included new sub-limits for ransomware damage [Cohn (2021)]. In the third quarter of 2021, the price rises reported by Marsh reached an astonishing 96 percent for the U.S. market and 76 percent in the U.K., strongly suggesting that we have not as yet reached the peak of the ransomware epidemic [Marsh (2021)]. A report by the U.S. Government's General Accounting Office, published in May 2021, confirms this picture: while there is an increasing demand for policies by businesses and organizations, prices are much higher and coverage limits lower than they were in recent years. Some sectors that have been hit especially hard by ransomware attacks due to their highly sensitive data and known poor IT security practices, such as healthcare and education, are having real difficulties finding insurers that will cover them [GAO (2021)]. Following the highly publicized Solarwinds and Kaseya hacks, "managed service providers" (MSPs) are also experiencing similar problems. Given that they offer remote IT security management services for multiple clients' networks, the payouts when they are being hacked will be enormous. Consequently, they now face extremely high insurance premiums [Bay and Pruger (2021)].

Some insurers are even questioning the viability of the entire product, have stopped adding new customers to their portfolios, or decided to leave the market entirely [IST (2021)]. However, this phenomenon seems to be limited to smaller insurers who saw cyber insurance as an easy way to create income and growth by offering policies written and backed by major reinsurers and without investing in their own cyber expertise. As Woods (2022) states, "for the first two decades, the cyber insurance market rewarded entrepreneurial insurers who embraced uncertainty (or ignorance) while offering innovative insurance products." In other words, the ignorant got rich insuring the careless while the sun was shining. Then it rained, and hard, forcing many of these types of players to leave the market. That is why we might ultimately come to view these large ransomware events as a healthy moment for the cyber insurance market, when it matured and providers without deep knowledge of cyber risk who had previously pulled down prices or security requirements were weeded out.

Yet, this new, more mature market suggests that increased security requirements and higher prices are here to stay, as those insurers that stayed on have fundamentally reevaluated the risks they are taking on [IST (2021)]. In this new environment, it will become increasingly harder for small businesses to persuade insurers to provide them with the protection they need. The recommendations in the final section will address this problem, offering suggestions on how an externally set minimum cybersecurity standard for SMEs could provide the necessary clarity about mutual expectations. However, even if it might turn out to be a good thing for the market in the long run, this market contraction certainly raises

questions regarding why cyber insurers were unable to see the wave of ransomware claims coming in advance. The next section will look at how insurers evaluate and price the cyber risks posed by the companies in their portfolios.

3. CYBER RISK ASSESSMENT

While it is not something usually mentioned in sales pitches, insurers have long known that company cyber risk is a very different beast to many of the other risk categories that they traditionally deal with. A key concern is that the usual approach of predicting future risks by amassing historical claims data has limited utility in cyber insurance. Companies only report network breaches if legislations force them to do so, and insurers do not share their claims data with competitors. Even if you have industry-leading knowledge about which industries were facing what chance of being hit by a cyberattack between 2005 and 2015, how much value does this information have for predicting the likelihood that a specific company will file a huge claim on their cyber insurance policy in 2023? Unsurprisingly, a key concern of the literature on cyber insurance is how to accurately price and manage cyber risk [Romanowski et al (2019), Khalili et al. (2019), Xu and Hua (2017)] given the lack, and limited reliability, of data on historic or recent claims and losses [Boyer (2020), Eling (2018), Marotta et al. (2017)].

Looking at how insurers gather data on their clients reveals a market split in two, with a high-end section offering bespoke arrangements for large businesses but demanding considerable scrutiny, and a budget product that is offered off the shelf to smaller customers who only need to undergo a very superficial audit before receiving their policies. At the high-end level, companies often buy so-called stacks or towers of insurance, where a huge coverage sum, reaching hundreds of millions of euros, is jointly guaranteed by multiple insurers and/or re-insurers. Consequently, insurers must make three separate decisions: 1) Do we want to insure this company; 2) what is the right price for insuring this company; and 3) where would we like to be in the tower: near the top, were we only need to pay out once the client claims their maximum coverage, or near the bottom, where we would be among the first to pay out but can command higher premiums?

Insurers collect data from multiple public or private sources on the company, send them detailed questionnaires about IT security practices and governance, and discuss the answers with the board and the IT department leadership. In some cases, they will also send one of their senior cyber underwriters to conduct an onsite audit [MacColl et al. (2021)]. This approach makes no economic sense for smaller companies, as the insurer would have to invest several years' worth of premiums to pay for this kind of extensive audit. Usually, smaller companies simply fill out a questionnaire, but insurance industry insiders do not like to discuss the level of scrutiny with which their answers are treated. After conducting dozens of interviews, as part of a wider research project on cyber insurance, Sullivan and Nurse (2020) conclude that almost no meaningful data on the IT security practices of small companies is gathered when signing them up for cyber insurance.

Insurers also use so-called outside-in rating agencies to assess company cyber risk. These companies will run a "vulnerability scanner" to scan a company network from the outside to identify vulnerabilities, patching regularity, open ports, and email security. This is in principle a very useful thing to do, as it mirrors the behavior of hackers and cyber criminals who run similar scans to identify potential victims. The rating agencies then employ an algorithm to quantify the results and combine them with data about the company from commercial providers or the dark web. The result is a "cyber risk rating score", which in theory allows the insurer or third-party risk manager to understand the company's cyber risk at a glance and base business decisions on this score [MacColl et al. (2021)].

Companies offering this kind of technology (such as BitSight, Security Scorecard, and RiskRecon) have seen huge growth in the insurance sector in recent years as their ratings offer a more comprehensive and reliable picture of a company's cyber risks than a short questionnaire. Moreover, the products are designed to be run at scale, meaning the cost of checking on an individual company is low. This explains why insurers were pioneer customers of these products before they began to become more popular in third-party risk and supply chain management.

Unfortunately, out-side in rating scores come with important inherent limitations to their scope and reliability. While a bad rating score makes it highly likely that there are serious cybersecurity issues at the company, a good rating does not necessarily mean that company IT security is handled well, and that the company poses a low cyber risk. The rating score can only include what is observable from the outside, or available in public or private databases. It reveals next to nothing about a vast range of key IT security issues within the company, ranging from systems and network configuration to staff training or incident response planning. Insurers need to know whether cybersecurity is something that is taken

seriously by the company board and operationalized with clearly attributed responsibilities. Consequently, cyber risk ratings should not be used as the single data point to drive a business decision, especially since there are also issues with occasionally incorrect attributions of IP addresses to companies (so-called false positives) that are not rectified because the company in question does not know this rating exists. Yet, insurers will privately admit that this is happening for insurance decisions relating to small companies. Once cyber risk ratings are accepted as a de facto standard for third party risk management, financial, or investment decisions, we might even see a situation reminiscent of the corporate credit rating market where a small number of U.S. companies dominate the markets and set the standards for how companies are measured and evaluated [Lemnitzer (2020)].

4. DOES CYBER INSURANCE IMPROVE COMPANY IT SECURITY?

Having established how hard it is for insurers to assess company cyber risk and why companies struggle to find and buy the right cyber insurance policy for themselves, the question arises whether having cyber insurance has a measurable positive effect on company cybersecurity. Does having cyber insurance simply mean a company pays money to transfer risk and receive access to support services, or does it also tend to initiate a process that leads to improved cybersecurity performance? This paper is far from the first to pose that question, and as Woods and Moore (2020) note, there are two decades' worth of research on whether insurance improves security. In the absence of universally agreed and comparable measurements of company IT security performance, what researchers attempt to do is to find out whether a company is less likely to experience a network breach when it is insured.

Unfortunately, conducting such research comes with inherent methodological difficulties: there are no public registers of insured or uninsured companies, and the vast majority of company breaches are never reported to regulators or the public. Both insurers and their clients have good reasons to be rather private about data regarding market reach, insurance claims, or their experience with security breaches. It is also difficult to do comparative work since there are practical, as well as ethical, issues regarding maintaining a control group of uninsured companies to measure their susceptibility to cyber-attacks while trying to identify whether the sample of insured companies do better.

As a result, it becomes difficult to replicate, or even evaluate, the results of studies conducted internally by insurers, even if they are published and not reserved for internal use. For example, the U.S. insurer Corvus recently reported that a vulnerability scanning tool it makes available to its clients had led to a 65 percent drop in ransomware-related claims from April to September 2020 [Abrams (2020)], which would be a direct improvement in security performance as a result of an insurance policy, but this is not a peer-reviewed study tested for its methodology. Many similar studies exist, but insurers usually chose not to make them publicly available. For these reasons, an extensive discussion on whether cyber insurance improves IT security concluded that the lack of data meant that the question could not be resolved with any degree of certainty. However, MacColl et al. (2021) found "a solid body of theoretical arguments that cyber insurance could play a meaningful role in improving cybersecurity among businesses."

Most experts agree and point to a number of factors: firstly, the mere act of applying for insurance cover usually entails a requirement to fully consider a company's cyber risk exposure and conduct an audit of its IT infrastructure and network configuration. It is recommended that companies should regularly conduct such exercises, though not all companies do it in practice. Secondly, some insurance policies also provide free access to IT security products or advice, which could potentially mean a marked improvement in company IT security, especially if implemented properly. Thirdly, the biggest benefit of a good cyber insurance policy are the support services that are available to clients in the event of a breach. Employed successfully, they benefit three different groups at once: the company stands a much better chance of dealing with the breach successfully, the insurer invests in these support services to limit the size of the eventual claim, and the economy as a whole is more secure as a cyberattack that is quickly contained by professionals is less likely to spread to other companies or institutions. This example also highlights the methodological problem that arises when we use the likelihood of being breached as the key variable to determine whether having an insurance policy improves company IT security. If the only "success" parameter of cyber insurance is reducing breaches, every breach is a fail. However, companies will get breached and limiting the damage and preventing the spread down the supply chains can be a key benefit of a good insurance policy. This effect is not captured by just looking at how many insured companies still get breached.

Most recently, there is anecdotal evidence that companies that have been denied insurance due to the recent hardening of the market have responded by improving their IT security measures before returning to re-apply for coverage. This is a recent observation and there is no solid empirical study of it yet, but it supports the view that this mechanism might be exploited systematically to improve company IT security by making cyber insurance compulsory.

5. RECOMMENDATIONS: REGULATED POLICIES, EXTERNAL STANDARDS, COMPULSORY INSURANCE FOR SMES

While fire insurance or third-party car insurance is compulsory in most countries, cyber insurance is not. Outside of tightly regulated industries, such as finance or critical infrastructure, company owners can largely handle their IT infrastructure as they see fit. As states are unwilling or unable to take the matter of corporate IT security under direct control, the idea of using the insurance industry as a regulator in this field has emerged [Trang (2017)]. To overcome the issue that not all private companies might want to buy the insurance policies offered by their new "regulators", it was proposed to simply make cyber insurance compulsory [Miller (2019)]. A recent RUSI report suggested that the U.K. government should promote the sector by making cyber insurance compulsory for all companies competing for government contracts [MacColl et al. (2021)]. Interestingly, these demands tend to come from researchers rather than insurers, who fear the aggregate risk of large cyberattacks hitting many insured parties at once. The Danish market leader Tryg is an exception in this regard and published a white paper calling for compulsory cyber insurance in December 2019 [Hübbe (2019)]. Indeed, the greatest potential in using cyber insurance to improve company IT performance lies in making it compulsory for small- and medium-sized companies (SMEs). While large companies with sophisticated IT departments will be able to look after themselves in case of a network breach, the audit function and support services that come with cyber insurance can make a fundamental difference to the ability of SMEs to prevent, contain, or survive being hacked [Lemnitzer (2021)].

We have known for a long time that SME cybersecurity is typically poor, and that despite the well-publicized hacks of businesses across the world and numerous government awareness campaigns, the vast majority of SMEs do not practice proper cybersecurity. A recent Hiscox report on cyber readiness puts about 75 percent of companies into its politely-worded "novice" category [Hiscox (2019)]. Data from Germany suggests that half of all small companies still have no incident response plans or any staff members explicitly responsible for IT security, and over 70 percent conduct no IT security training for their staff. Only a fifth of the companies surveyed fulfil the most basic requirements for secure IT systems [GDV (2020)]. This is a major issue since any attempt to achieve resilience within a modern digital economy will fall flat if such a large percentage of companies remain vulnerable to the most basic malware. After many years of relying on awareness campaigns, we know full well that they will not cause the drastic change of approach by SME company boards that is necessary.

> *"Requiring SMEs to sign up to cyber insurance offers the best solution for changing the practices at a huge number of companies in a relatively short period of time."*

We need to try something new and requiring SMEs to sign up to cyber insurance offers the best solution for changing the practices at a huge number of companies in a relatively short period of time. Once insurance becomes compulsory, companies must meet the required minimum IT security necessary to obtain cover or face a fine. Consequently, the key element necessary for the success of compulsory cyber insurance is to accompany it with a clear, externally set minimum IT security standard that both insurers and companies can refer to. This task should not be left to the insurers – variation between providers creates confusion and unpredictability for clients, and insurers might find economic incentives to water down standards to win market share or arbitrarily exclude certain groups of companies perceived as too risky.

Instead, the standard should be set by a trusted external body. The procedures and controls established by the various cybersecurity standards developed by the U.S. National Institute of Standards and Technology or the International Organization for Standardization (esp. ISO 27001) are a challenge to fully implement even for large companies with skilled IT departments. For SMEs they are simply too demanding in organizational scope and technological sophistication. The

measures required by this new standard must be feasible to implement without extensive specialist IT knowledge, and they must come at a cost point that is manageable for smaller companies. At the same time, they must be carefully chosen to achieve the highest security gains at the lowest price.

The U.K. National Cyber Security Centre attempted to provide such a universal minimum standard with its "Cyber Essentials" certification program for small businesses, which is already used as a reference point by U.K. insurers. It has just been updated and will now demand multi-factor authorization, password management, and tighter security regarding the use of cloud services [Hill (2022)]. Combined with least privilege principles, network segmentation, breach response, and mandatory staff training it could serve as a good starting point for any country considering a minimum standard for SMEs. Australia's National Cyber Security Centre has embraced a much more ambitious approach with three different levels of cyber maturity adapted to company size. An alternative route would be to build up a nationwide cyber risk rating system like the one currently set up in Austria, which combines a vulnerability scan, an onsite audit, and a bespoke standard to rate and compare companies [Cyber Trust Austria (2021)]. Originally created to allow critical infrastructure companies to monitor their suppliers, the ultimate intention is to cover all Austrian businesses.

Moreover, the clarity and uniformity that this new standard needs to achieve should be matched by corresponding improvements to the wording of cyber insurance policies. The E.U.'s insurance oversight organization, European Insurance and Occupational Pensions Authority (EIOPA), is now on record demanding that minimum standards for policies should be set externally (in other words, by regulators), with insurers then competing over price or by providing extra coverage and features [EIOPA (2020)]. Next to clear language, policies must also offer clear guarantees: first, a company meeting the minimum standard must be able to rely on their claims being paid out in full once they are hit by malware. That excludes common tricks such as hiding a much lower sublimit for ransomware-related damages deep in the small print. Second, policies must include quick, easy, and reliable access to support services once a breach has occurred. This is a point that has been overlooked in the relevant reports and the specialist literature but is vital if we look at the insurance sector from a public policy or national security perspective. Some policies still do not include such services, while others put access to them at the discretion of the insurer. Neither should remain since easy access to professional tech support is one of the main advantages cyber insurance offers to SMEs. Finally, it should no longer be legal for insurers to cover ransom payments made by their clients. With some states already moving in this direction, it would make no sense to extend compulsory cyber insurance to many thousands of companies while allowing these policies to be used to pay off cyber criminals.

6. CONCLUSION

While the story of cyber insurance has long been one of continuous growth, the sector is now experiencing its first proper crisis as ransomware claims led to huge losses on formerly profitable portfolios. This has caused a spike in prices and a hardening of market conditions, which has unfortunately inhibited the increased take-up of cyber insurance policies among smaller companies that we might have expected following the introduction of GDPR in 2018 and the escalating ransomware threat. However, this new "harder" market will almost certainly be a healthier market where more insurers will have a deep understanding of cyber risk and establish specific security requirements for their clients without the fear of losing business to more lenient competitors.

This is a good development, but it also makes it harder for SMEs to obtain cyber insurance just when they need it most. While it has proven difficult to show a direct empirical connection between having cyber insurance and improvements in company IT security due to data and methodological constraints, a good case can be made that the financial cover, technical support, and post-breach incident response services offered by cyber insurance would be hugely helpful to SMEs in particular. At the same time, the increasing focus on cyber risk supply chain monitoring in larger companies, particularly those that are part of critical infrastructure, means it is becoming increasingly common to demand proof of cyber insurance before signing a contract with a supplier, just at a time when many SMEs find it harder to access cyber risk coverage as conditions tighten [Glover (2022)].

Frankly, this group of companies is struggling to meet basic IT security standards and will struggle to obtain insurance in the new market conditions. Yet, this is not just a problem for the individual companies: as long as a large number of SMEs remain so vulnerable, their connections to business partners and clients of all sizes means the security of the digital economy as a whole remains compromised. Something needs be done to support them in an environment where

the threat from ransomware and state hackers is so severe, and if done the right way, making cyber insurance compulsory for this group of businesses might be the game changer that is required.

Compulsory cyber insurance for SMEs is a radical idea, but given that none of the awareness campaigns that were tried over the years has had a significant impact on security standards in smaller companies and the threat level due to ransomware and supply chain hacks keeps rising, something radical must be done. Moreover, compulsory insurance is accepted without controversy in other parts of business life, such as fire insurance or third-party car insurance. If compulsory cyber insurance is combined with an externally set minimum security standard designed with SMEs in mind and appropriate regulation of cyber insurance policies, it might well be the single best lever there is to significantly improve IT security in many thousands of companies in a short period of time.

REFERENCES

Abrams, L., 2020, "Cyber insurer's security scans reduced ransomware claims by 65%," Bleeping Computer, September 22, https://bit.ly/3sOBbvH

Bay, K., and M. Pruger, 2021, "The future of cyber insurance: what to expect in 2022," https://bit.ly/3MttMtq

Bernard, J., 2020, "Overcoming challenges to cyber insurance growth: expanding stand-alone policy adoption among middle market business," Deloitte, March 16, https://bit.ly/3HJhfi5

Boyer, M., 2020, "Cyber insurance demand, supply, contracts and cases," The Geneva Papers on Risk and Insurance – Issues and Practice 45: 559–563

Cimpanu, C., 2020, "Ransomware accounted for 41% of all cyber insurance claims in H1 2020." ZDNet.com, September 10, https://zd.net/3vFREUO

Cohn, C., 2021, "Insurers run from ransomware cover as losses mount," Reuters, November 11, https://reut.rs/3sY7TLj

Cyber Trust Austria, 2021, https://bit.ly/3pLgC15

Eling, M., 2018, "Cyber risk and cyber risk insurance: Status quo and future research," The Geneva Papers on Risk and Insurance – Issues and Practice 43: 175–179

EIOPA, 2020, "Cyber underwriting strategy," European Insurance and Occupational Pensions Authority, February 11, https://bit.ly/36Zcwfg

ENISA, 2016, "Cyber insurance: recent advances, good practices and challenges," European Union Agency for Cyber Security, https://bit.ly/3IPYtXr

ENISA, 2016b, "Commonality of risk assessment language in cyber insurance," European Union Agency for Cyber Security, https://bit.ly/3HPP1IB

GAO, 2021, "Cyber insurance: insurers and policyholders face challenges in an evolving market," U.S. Government Accountability Office, May 20, https://bit.ly/3KVCaAv

GDV, 2017, "Allgemeine versicherungsbedingungen für die cyberrisiko-versicherung (General insurance conditions for cyber risk insurance)," Gesamtverband der deutschen Versicherungswirtschaft, https://bit.ly/373EG8V

GDV, 2020, "Cyber-Risiken im Mittelstand 2020, (Cyber risks in SMEs)," Gesamtverband der deutschen Versicherungswirtschaft, https://bit.ly/35vDHy9

Glover, C., 2022, "The ransomware crisis is making cyber insurance harder to buy," TechMonitor, January 24, https://bit.ly/3IPZw9P

Hill, M., 2022, "UK NCSC updates Cyber Essentials technical controls requirements and pricing structure," CSO Online, January 7, https://bit.ly/3CmZZ0X

Hiscox, 2019, "Cyber readiness report," https://bit.ly/3IKtJap

Hübbe, M., 2019, "Lovpligtig forsikring mod cyber-angreb," Jyllands-Posten, December 2, https://bit.ly/3ISto5o

IST, 2021, "Combating ransomware – a comprehensive framework for action: key recommendations from the ransomware task force," Institute for Security and Technology, https://bit.ly/3MuUyBx

Insurance Journal, 2017, "Why 27% of U.S. firms have no plans to buy cyber insurance," May 31, https://bit.ly/3IPi2z3

Kesan, J. P., and C. M. Hayes, 2017, "Strengthening cybersecurity with cyberinsurance markets and better risk assessment," Minnesota Law Review 102: 191

Khalili, M. M., M. Liu, and S. Romanosky, 2019, "Embracing and controlling risk dependency in cyber-insurance policy underwriting," Journal of Cybersecurity 5:1

Lemnitzer, J. M., 2020, "Do we need and EU cybersecurity ratings agency?" EU CyberDirect Blog, November 10, https://bit.ly/3pJcqPz

Lemnitzer, J. M., 2021, "Why cybersecurity insurance should be regulated and compulsory," Journal of Cyber Policy, 1-19

Lubin, A., 2019, "The insurability of cyber risk," SSRN, https://bit.ly/3pNfha7

MacColl, J., J. R. C. Nurse, and J. Sullivan, 2021, "Cyber insurance and the cyber security challenge," Royal United Services Institute (RUSI) occasional papers, June 28, https://bit.ly/3MunidP

Marotta, A., F. Martinelli, S. Nannia, A. Orlando, and A. Yautsiukhin, 2017, "Cyber-insurance survey," Computer Science Review 24, 35-61

Marsh, 2021, "Marsh global insurance market index – 2021 Q3," https://bit.ly/3MuCAPP

Miller, L., 2019, "Cyber insurance: an incentive alignment solution to corporate cyber-insecurity," Journal of Law and Cyber Warfare 7, 147-182

OECD, 2017, "Enhancing the role of insurance in cyber risk management," Organisation for Economic Cooperation and Development

Rawlings, P., 2014, "Cyber risk: insuring the digital age," Journal of the British Insurance Law Association 128:1

Romanosky, S., L. Ablon, A. Kuehn, and T. Jones, 2019, "Content analysis of cyber insurance policies: how do carriers price cyber risk?" Journal of Cyber Security 5, 1-19

Sullivan, J., and J. R. C. Nurse, 2020, "Cyber security incentives and the role of cyber insurance," Royal United Services Institute (RUSI) Emerging Insights series, https://bit.ly/3sR1Fg9

Trang, M., 2017, "Compulsory corporate cyber-liability insurance: outsourcing data privacy regulation to prevent and mitigate data breaches," Minnesota Journal of Law, Science and Technology 18: 389-425

Woods, D. W., 2022, "The evolutionary promise of cyber insurance," The FinRegBlog (Duke University School of Law), https://bit.ly/3vLXrs3

Woods, D. W., and R. Böhme, 2021, "How cyber insurance shapes incident response: a mixed methods study," 20th Workshop on the Economics of Information Security (WEIS 2021), https://bit.ly/35Du54b

Woods, D. W., and T. Moore, 2020, "Does insurance have a future in governing cybersecurity?" IEEE Security and Privacy Magazine 18:1, 21-27

Xie, X., C. Lee, and M. Eling, 2020, "Cyber insurance offering and performance: an analysis of the U.S. cyber insurance market," The Geneva Papers on Risk and Insurance – Issues and Practice 45, 690-736

Xu, M., and A. Lei Hua, 2017, "Cybersecurity insurance: modeling and pricing," Society of Actuaries, https://bit.ly/3Cn5VHh

ABOUT CAPCO

Capco, a Wipro company, is a global technology and management consultancy specializing in driving digital transformation in the financial services industry. With a growing client portfolio comprising of over 100 global organizations, Capco operates at the intersection of business and technology by combining innovative thinking with unrivalled industry knowledge to deliver end-to-end data-driven solutions and fast-track digital initiatives for banking and payments, capital markets, wealth and asset management, insurance, and the energy sector. Capco's cutting-edge ingenuity is brought to life through its Innovation Labs and award-winning Be Yourself At Work culture and diverse talent.

To learn more, visit www.capco.com or follow us on Twitter, Facebook, YouTube, LinkedIn Instagram, and Xing.

WORLDWIDE OFFICES

APAC
Bangalore
Bangkok
Gurgaon
Hong Kong
Kuala Lumpur
Mumbai
Pune
Singapore

EUROPE
Berlin
Bratislava
Brussels
Dusseldorf
Edinburgh
Frankfurt
Geneva
London
Munich
Paris
Vienna
Warsaw
Zurich

NORTH AMERICA
Charlotte
Chicago
Dallas
Hartford
Houston
New York
Orlando
Toronto
Tysons Corner
Washington, DC

SOUTH AMERICA
São Paulo

WWW.CAPCO.COM

CAPCO
a wipro company