2017 Cyber Risk Landscape

Centre for
Risk Studies

UNIVERSITY OF
CAMBRIDGE
Judge Business School

RMS®

2017 Cyber Risk Landscape

Foreword

The past year has seen unprecedented changes in the cyber risk landscape.

When we at RMS first launched our Cyber Accumulation Management System (CAMS) in February 2016, we provided a new data standard, analytical framework, and a functional platform for our insurance clients to manage this emergent risk.

We have been delighted with the take-up of this solution across the market. And, we continue to innovate to improve your understanding of this dynamic risk so you can approach new opportunities prudently and with confidence in your accumulations. With the release of RMS CAMS Version 2.0, we have enhanced our solution to widen its scope and to reflect the most recent data and trends in the domain.

Recent events have demonstrated just how dynamic the world of cyber risk can be. Records for the most severe incidents have been broken for many of the loss processes we model – the largest volumes of data exfiltrated from companies, the most intense denial of service attacks, the biggest financial theft attempts. Unprecedented numbers of zero-day exploits became freely available to cyber criminals. Systemic cyber heists were carried out on dozens of banks through ingenious corruption of their networks of trust. Cyber risk has become politicized. Regulatory and legal frameworks are changing across the world.

> “modeling cyber risk is core to our mission to create a more resilient and sustainable global society”

Our initial accumulation scenarios anticipated several of these trends and potential surges, and we are committed to remaining up to date with the trends and changes in this volatile risk landscape.

This report summarizes the rapidly changing world of cyber risk, and describes how our analysts and modelers view the current and future risk.

Modeling cyber risk is core to our mission to create a more resilient and sustainable global society by enabling industry solutions to cover the risk responsibly. RMS is committed to investing in world-class cyber risk analytics, working together with industry-leading partners to develop the innovative solutions expected by our clients. We are committed to contributing to the development of a successful cyber insurance market.

Hemant Shah

HEMANT SHAH
Co-Founder and CEO
Risk Management Solutions

Overview

We are in a period where the cyber risk landscape is rapidly changing. Writing cyber insurance means anticipating emerging trends in this landscape. We are seeing new records set for the scale of cyber incidents, escalation in the costs of events, changes in technologies – both offensive and defensive – and shifts in target preferences, activities, and protagonists.

To respond to these changes, the cyber insurance industry is evolving dynamically both in the coverage offered and the risk management practices employed.

In February 2016, RMS released the Cyber Accumulation Management System (CAMS).[1] This has been well received and has been adopted across the industry in a short space of time. RMS has built-out a research and development team that continues to monitor and update its view of risk, and to release new versions of the platform that incorporate these views and improved functionality.

The release of CAMS Version 2.0 marks a major enhancement in the management of cyber risk. It extends accumulation management to “silent” cyber exposure, introducing cyber-physical attack scenarios on operational technology (OT). This is where cyber is the proximate cause for physical damage and consequential loss in other lines of insurance business, such as fires in commercial buildings, explosions in petrochemical facilities, and attacks against marine shipping. Cyber-physical attacks have become a genuine cause of concern in recent years, underscored by the December 2015 cyber-attack on the Ukrainian power grid.

CAMS Version 2.0 also provides an opportunity to update the RMS affirmative IT cyber accumulation scenarios for each loss process, to reflect the changing cyber risk landscape. At the initial launch of RMS CAMS in early 2016, the industry was still debating whether cyber actually posed any systemic threat of correlated loss across multiple accounts. Several events during the year have confirmed that systemic threat convincingly, including the ShadowBrokers making “zero-day” firewall exploits widely available; the Lazarus SWIFT cyber-heists hitting large numbers of banks, and the rapid growth of cloud services putting increasing numbers of companies at risk from failure of a provider.

RMS has updated the CAMS scenarios to reflect the latest trends in cyber risk and provides new recommendations for accumulation stress tests, cost models, and loss footprints to protect portfolios of cyber insurance exposure in the evolving world of cyber risk.

This report provides an update on the cyber insurance market and sets out the landscape of cyber risk in 2017.

[1] CCRS, 2016a.

SECTION 2

Cyber Risk Landscape

Cyber risk is a relatively young phenomenon and is evolving rapidly. The magnitude of known attacks, dissemination of new technologies, compromised IT infrastructures, and security measures put in place to protect against attacks are advancing dynamically. Many of the key assumptions and the understanding on which RMS bases the principles of cyber insurance risk management are subject to significant change, such as fundamental computer science, attack vectors, system vulnerabilities, defenses, and capabilities of the protagonists.

Cyber Threat: Increasingly Professional, International, and Political

Cyber hacking continues to become increasingly professional and international, with growing political dimensions. Amateur hackers and "hacktivists" are still active, but much of the threat to corporate business comes from well-resourced criminal gangs that have professionalized their hacking activities. Much of this activity is organized and hosted from countries beyond the jurisdiction of Western law enforcement. The cybercriminal economy is informal, collaborative, and mercenary. Organized gangs can buy the resources, skills, and tools to perpetrate cybercrime in a thriving black market. Stolen information can be sold and the proceeds of cybercrime laundered through a sophisticated gray economy.

Law Enforcement Lags Behind

Cybercrime is still met with little deterrence, with extremely low conviction rates for perpetrators. Cybercrime statistics published in the U.S. by the FBI in 2015 show that less than 1 in 200 reported cases of cyber identity theft resulted in a criminal case being brought, and only 1 in 50,000 resulted in a conviction.[2] In contrast, armed robbery in the U.S. results in conviction rates of 1 in 5.[3] Convicted cybercriminals face low deterrence as judges struggle to determine reasonable punishments.[4]

This situation may change with the reorganization of law enforcement to provide specialist cyber investigation units, the improvement of international extradition cooperation and a willingness to pursue cybercriminals abroad, the empowerment of national security cyber units to pursue offensive cyber operations against criminals in foreign jurisdictions, and changes in legal prosecution procedures including evidence of harm. Progress is being made in each of these arenas and, over time, it is expected to increase the conviction rate which will be the main control system for deterring cybercrime.

Rapid Growth in Security Investment by Companies

Many companies are investing heavily in their own cybersecurity systems to protect their assets. Global expenditure on cybersecurity is estimated to have grown 14 percent year-on-year, from US$75 billion in 2015, to $86 billion in 2016.[5] On average, U.S. companies now spend around three percent of their capital expenditure budget on cybersecurity.[6] Projections suggest that global cybersecurity expenditure will continue to grow rapidly and will reach hundreds of billions of dollars annually by the end of the decade.

The type of expenditure is also shifting. Traditional purchases of hardware IT security components, such as servers, networking gear, data centers, and physical infrastructure, are being augmented by broader security solutions, such as personnel training, non-computer platforms, and Internet of Things (IoT) security.[7] The cybersecurity industry is becoming more competitive, with many start-ups and a proliferation of security-tech offerings taking an increased

[2] FBI IC3, 2015 Internet Crime Report.
[3] Grimes, 2012.
[4] Williams, 2016.
[5] Cyber Security Ventures, Cybersecurity Market Report Q4 2016.
[6] Pacific Crest Analyst, Rob Ownes, quoted in *Investor's Business Daily News*, 6/10/16.
[7] Cyber Security Ventures, Cybersecurity Market Report Q4 2016.

Cybercrime is still met with little deterrence, with extremely low conviction rates for perpetrators.

share of corporate security expenditure, squeezing the earnings and valuations of the industry leaders in the cybersecurity sector.[8]

The increased level of security expenditure and management focus on cyber protection is apparently reducing the incidence of successful cyber attacks and losses, most noticeably on the frequency of smaller data breach events and accidental losses from staff. But this is countered by increases in scale and ambition of malicious and professional data exfiltration attacks, leading to an increase in the overall risk.

RMS interprets the growing levels of cybersecurity being implemented by larger companies as making it harder for amateur attacks to succeed, and raising the bar of effort, "logistical burden,"and skill levels needed for a cyber-attack to succeed. Determined and well-resourced attackers will still find ways through security defenses.

Cyber-leaks Becoming Increasingly Political

A characteristic of some of the most recent large-scale data exfiltration attacks has been the motivation of the attackers, which is increasingly political rather than financial in nature. This has been dubbed "Leaktivism" by some members of the media. Examples include:

- One of the largest data leaks involved the breach of a 50 million citizen database from the Turkish government in March 2016, apparently by hacktivists protesting against President Recep Tayyip Erdoğan.[9]
- A similar breach was perpetrated against the Philippines' Commission on Elections (COMELEC), leaking 55 million voter details including fingerprint records, posted with anti-government slogans.[10] "The decision of the National Privacy Commission (NPC) finds COMELEC chairman Andres Bautista liable for the March 2016 data breach of the poll body's voters' database" and affected individuals may file suit against him.[11]
- "John Doe,"the anonymous person who leaked the Panama Papers in April 2016 (see page 12) detailing the tax records of wealthy individuals, cited income inequality as the reasons for his actions.[12]
- One of the most controversial cyber incidents was the leaking of emails from the Democratic National Committee during the U.S. presidential election, later concluded by the U.S. Intelligence Community to have been instigated by Russian hackers authorized by the Kremlin to influence the election.[13]

Political motivation – particularly protest and hacktivism – has been a longstanding characteristic of cyber risk, but recent developments suggest that this is becoming more mainstream and increasingly involving well-resourced cyber threat groups.

State-sponsored Cyber-Attacks on Insureds

State-sponsored cyber teams are becoming more active, more visible, and a more significant feature of the commercial risk landscape for cyber, and of the geopolitical risk landscape more generally.

More than 20 countries have national cyber teams as an adjunct of their military capability, at least six of which analysts consider "advanced."[14] Several "cyber-capable" countries are potential adversaries of the United States and other Western powers, including Russia, China, North Korea, and Iran. Cyber incursions by foreign powers into each other's institutions have occurred for many years, but typically these have been restricted to areas of espionage, military and government facilities, and non-damaging activities.

Recent developments have seen suspected attacks by state-sponsored cyber teams cause losses to private sector commerce. Examples include:

- 2014 attack on Sony, alleged by U.S. intelligence officials of being sponsored by North Korea.
- Destructive attacks on civil aviation computers in Saudi Arabia in November 2016, similar to the 2012 Aramco oil company attack, both blamed on Iran's cyber army.
- Allegations that North Korean cyber teams were implicated in the theft of millions of dollars from over a dozen banks in the SWIFT cyber heist.
- Spear-phishing attacks for data breaches on U.S. corporations being blamed by the FBI on Russian government-backed "Cozy Bear" perpetrators.

[8] Investor's Business Daily News, 6/10/2016, 'Security Freeze'.
[9] Murdock 2016.
[10] Temperton 2016.
[11] Ronda, 2017.
[12] Gupta, 2016.
[13] Entous and Nakashima 2016.
[14] Lewis 2012, Centre for Strategic and International Studies.

ShadowBrokers Release a Cyber Arsenal

On August 13, 2016, a previously unknown group called the "ShadowBrokers" released a showcase folder and offered an encrypted folder for sale to the highest Bitcoin bidder. The showcase folder, made publicly available, contained a set of cyber-hacking weapons obtained from "Equation Group,"an elite United States National Security Agency (NSA) cyber-hacking team.[15]

It is widely assumed that these high-quality cyber tools were obtained from the NSA, and that the ShadowBrokers had either hacked the NSA and stole their tools, or an NSA insider had leaked the content. In October 2016, a further message from ShadowBrokers claimed that the auction had been called off, and leaked a further 300 files of IP addresses purportedly revealing NSA targeting and routing.[16]

The released showcase folder contained 15 exploits, 13 implants, and 11 tools, most notably several "zero-day" exploits to penetrate industry standard firewalls such as Cisco ASA, Fortinet FortiGate, and Juniper SRX, along with other corporate penetration tools.[17] The public release meant that unscrupulous hackers could use these tools to access the networks of the many companies running these firewalls. Firewall vendors and corporate security teams scrambled in the following weeks to produce emergency security patches and preventative measures against these exploits.

The proposed RMS "Leakomania" accumulation scenario for data exfiltration is based on the simultaneous availability of multiple "zero-day" exploits enabling a sudden increase in data exfiltration. The ShadowBrokers episode demonstrated how these exploits are hoarded and traded by cyber criminals, and exhibited the potential for clusters of them to trigger a systemic wave of cyber losses.

[15] Greenberg, 2016.
[16] Fox-Brewster, 2016.
[17] CERT, 2016.

- Factories in Ukraine that suffered power outages because of attacks on the Ukrainian power grid, alleged to have been carried out by Russian cyber units.[18]

Good Guys Go on the Offensive

Governments across the world are stepping up their cyber-offensive capabilities, significantly raising the potential for escalation of interstate cyber conflicts. The ShadowBrokers leak revealed NSA Equation Group's aggressive targeting and intrusive activities.[19] The U.K. government established a new National Cyber Security Center in March 2016. In addition to its role in facilitating security, it has a mandate to move to "active cyber defense" – i.e., to hack back against attackers.[20] In April 2016, the German government announced a new cyber and information command in the German military Bundeswehr, controversially including a cyber-attack capability.[21] National security organizations in several advanced economies have ramped up their cybersecurity and counter-cyber activities.

Is Cyber Insurable if Cyber Wars Intensify?

The debate about the insurability of commercial cyber losses originating from state-sponsored cyber groups is intensifying. A potential increase in cyber warfare activity would have significant implications for cyber insurers who pay claims to private sector companies caught up in any international clandestine cyberwar cross-fire. Attribution of attacks is extremely difficult, so it is challenging for cyber insurers to differentiate between criminal and state-sponsored losses. The risk appetite for insurance companies to cover cyber loss is unlikely to be sustainable if losses from state-sponsored attacks become a significant proportion of the risk. The resources of state-sponsored cyber teams pose a threat of major systemic loss across thousands of insured accounts.

Terrorism and Cyber Loss

Assessments of the capabilities of proscribed terrorist groups suggest that they do not currently possess destructive cyber capability, although some groups, such as the United Cyber Caliphate arm of Islamic State, are known to be actively pursuing the strategic increase of their offensive cyber capabilities.

Destructive acts of cyber terrorism could face similar ambiguity in attribution, but mechanisms for determination have been proposed. Cyber terrorism has become a growing topic of concern for terrorism insurance pools around the world. Terrorism insurance is treated as specialist coverage in many countries, and is typically included in government pools or has some level of government backstop. In the U.S., insurers are required to offer terrorism coverage, and it is automatically included in workers compensation coverage.

The U.S. Terrorism Risk Insurance Program Reauthorization Act 2015 (TRIPRA 2015 or TRIA) backstop does not explicitly cover cyber, and the introduction of a backstop has been the subject of debate for several years.[22] The ambiguity over the level of protection that TRIA provides is a key driver towards the development of a bespoke industry-provided cybersecurity market.

Changes in Extreme Cyber Tail-Risk

The most obvious changes in cyber risk have occurred at the extreme tail. In the past year, the scale of attacks has consistently exceeded the largest attacks previously observed – typically by an order of magnitude. For example, at the start of 2016, the largest data exfiltration events involved hundreds of millions of records. By the end of 2016, events of over a billion (Yahoo!) terabytes of financial data (Mossack Fonseca) had been exfiltrated. Denial of Service attacks had previously been recorded with intensities as high as 600 gigabits per second (Gbps), but by the end of 2016, the Dyn event (page 21) was of an order of magnitude more intense – several terabits per second – enabled by new techniques that utilized the Internet of Things (IoT) for volumetric attacks. Previous financial cyber thefts of tens of millions of dollars were eclipsed by an attempt to steal a billion dollars in a cyber heist involving a compromise of the SWIFT financial transaction system. The pattern of increasingly large extreme events is being repeated in many of the loss processes of cyber risk.

Additionally, we are seeing more cyber-attacks in which multiple companies are impacted in one single event. The Dyn distributed denial of service (DDoS) attack affected web-based services at hundreds of companies, including Amazon, Netflix, Airbnb, Spotify, and PayPal. The Ukraine cyber-grid attack caused power outage to many companies.

The following sections highlight the changing trends in several key IT loss processes.

2.1 Data Exfiltration

Data exfiltration continues to be the predominant cause of insured cyber loss, with many instances of individual companies suffering from data leaks. Companies are at risk of larger data losses; the risk of data exfiltration loss is increasing in severity.

Over the last 18 months, RMS has built out its cyber incident database of historical data exfiltration events.

[18] ICS-CERT, 2016, and Zetter, 2016.
[19] Fox-Brewster, 2016.
[20] The Register, 2016.
[21] ORF, 2016.
[22] For more information on TRIA visit the U.S. Department of Treasury website.

Table 1: Selected Large Data Breach Events Reported in 2016

Organization	No. of Records Lost	Date of Breach	Cause	Jurisdiction	Business Sector	Data Breach Severity
Mossack Fonseca	2.6 terabytes	3/1/2016	Malicious Insider	Panama	Financial Services	P8
Yahoo!	1,000,000,000	2013, reported Dec. 2016	Malicious Outsider	United States	IT Services	P8
Yahoo!	500,000,000	2014, reported Aug. 2016	Malicious Outsider	United States	IT Services	P8
Myspace.com	360,000,000	2016	TBD	United States	IT Services	P8
Yahoo!	200,000,000	2016	TBD	United States	IT Services	P8
U.S. Voter/Amazon/ Google	154,000,000	06/22/16	Accidental Loss	United States	Government	P8
Mexican Voters	93,400,000	04/14/16	Accidental Loss	Mexico	Government	P7
Philippines' Commission on Elections (COMELEC)	55,000,000	03/28/16	Malicious Outsider	Philippines	Government	P7
Turkey General Directorate of Population and Citizenship Affairs	50,000,000	03/28/16	Malicious Outsider	Turkey	Government	P7
Verticalscope/ Techsupportforum.com and others	45,000,000	02/09/16	Malicious Outsider	Canada	Technology	P7
Fling	40,000,000	05/06/16	Malicious Outsider	United Kingdom	IT Services	P7
Twitter, Inc.	32,000,000	2016	TBD	United States	IT Services	P7
17 Media	30,000,000	04/29/16	Malicious Outsider	Asia	Technology	P7
Mate1	27,000,000	02/16/16	Malicious Outsider	United States	IT Services	P7
Alibaba.com	20,000,000	2016	TBD	China	Retail	P7
U.S. Health Insurer	9,300,000	06/27/16	Malicious Outsider	United States	Healthcare	P6
Lifeboat	7,089,395	2016	TBD	United States	IT Software	P6
U.S. Department of Health and Human Services and others	5,000,000	02/05/16	Malicious Outsider	United States	Government	P6
Lightspeed	5,000,000	2016	TBD	United States	IT Software	P6
Adult Friend Finder	3,900,000	2016	TBD	Unknown	IT Services	P6
Banner Health	3,700,000	06/17/16	Malicious Outsider	United States	Healthcare	P6

This information is gathered from various open source data resources and has been heavily enriched by RMS data scientists to provide a historical picture of data exfiltration. This data is a key input into the RMS data exfiltration model and is used to parameterize incident and cost information.

Record-breaking Sizes of Data Exfiltration Events

The past year has seen the largest data exfiltration events ever revealed. In April 2016, the world's largest data leak by volume saw 2.6 terabytes of confidential tax data stolen from Mossack Fonseca (see page 12). Yahoo! broke the record – twice – for the largest number of personal records compromised, first in September 2016 when it revealed that data on 500 million users had been hacked in 2014, and then again in December 2016 when it revealed a data breach of over one billion user accounts dating from 2013.[23] The Yahoo! share price dropped six-and-a-half percent after the December 2016 breach announcement, prejudicing and delaying acquisition negotiations with Verizon.[24]

Because of these increasingly large events, the RMS magnitude scale for data breach has been adjusted. The P8 scale is now extended to include events of more than one billion personal records or more or a terabyte of data lost.

[23] Finkle and Tharakan, 2016.
[24] Moritz and Womack,, 2016.

Panama Papers Data Exfiltration

On April 3, 2016, the world's largest data leak was simultaneously published by 107 news organizations, consisting of 2.6 terabytes of confidential tax data relating to offshore accounts stolen from Panamanian law firm Mossack Fonseca. An anonymous insider apparently leaked the records to highlight "income inequality" by disclosing how high-profile individuals hide income and avoid paying taxes.

The leaks reportedly covered 11.5 million confidential documents dating from the 1970s through to late 2015. The data included 4.8 million emails, 3 million database format files, 2.2 million PDFs, 1.1 million images, and 320,000 text documents.[25] It took news organizations over a year to analyze the volume of data prior to publication.

The leaked information allegedly detailed the ways that many high-profile individuals in more than 40 countries, including U.K., France, Russia, China, and India, set up accounts and shell corporations in Panama to minimize tax payments in their own countries.

The political fallout involved the resignation of the prime minister of Iceland and Spain's minister of industry, and calls for the resignation of the Ukrainian president, the prime minister of Malta, and many other high-profile politicians in other countries. The U.K. prime minister admitted that he benefited from shareholdings in his late father's estate, named in the leak. Seventy-two heads of states were named, and hundreds of high-ranking officials in national governments, as well as wealthy individuals, their relatives, and close associates.[26] High-profile celebrities named included the estate of movie director Stanley Kubrick, and actor Jackie Chan as a shell company shareholder.[27]

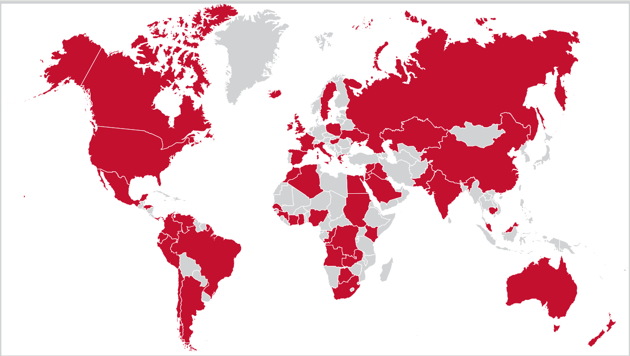


Figure 1: Map of countries impacted by Panama Papers leak.

[25] InfoSEC Institute, 2016.
[26] InfoSEC Institute, 2016.
[27] Palmer, 2016.

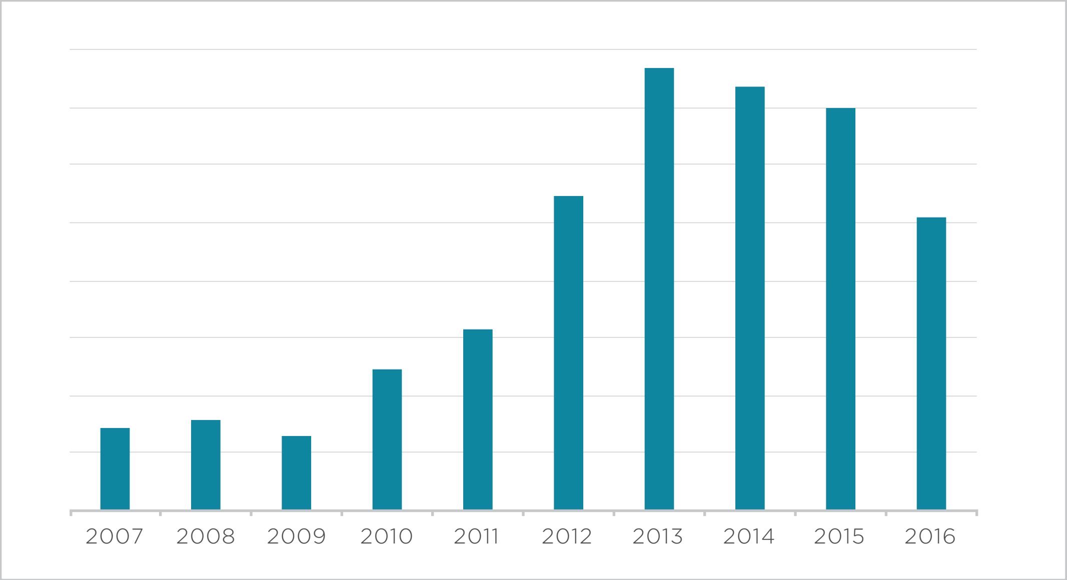


Figure 2: Incident count for all magnitude data exfiltration events from 2006 to 2016[28]

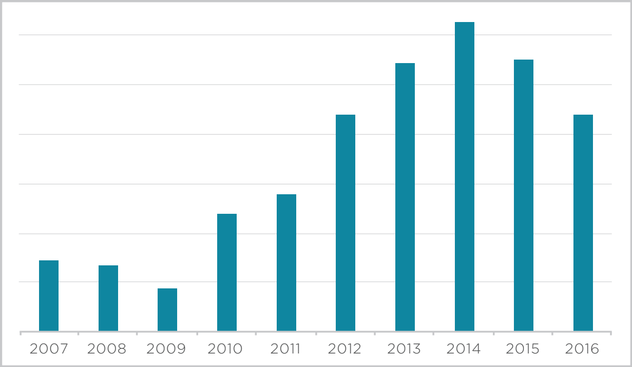


Figure 3: Incident count for magnitude P5 (more than 100,000 records) and smaller

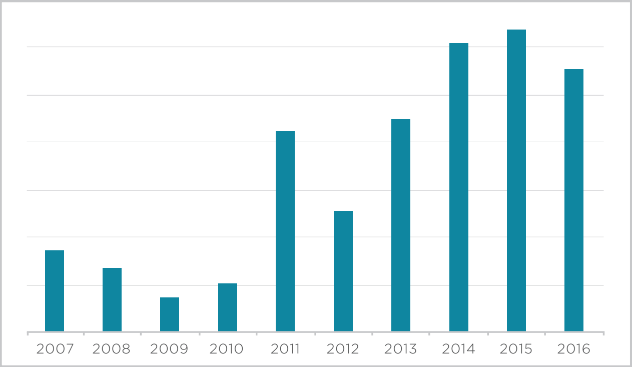


Figure 4: Incident count for magnitude P6 (more than a million records) and larger

Overall Trend for Data Exfiltration Stabilizes

The RMS historical catalog of cyber data breaches shows a substantial increase in reported cyber data exfiltration events in the previous 10 years as shown in Figure 2 (Incident Count – All Magnitude). In 2014 and 2015, the almost exponential growth in attack counts has tapered off. The frequency of occurrence of all sizes of data exfiltration events appears to have decreased since the peak of 2013 - 2015. We will be monitoring incidences in 2017 to see if this reduction continues.

This growth in historical reported attacks is likely caused by two factors: first, an increase in the underlying attack rates and second, because of increased reporting. The cause for the plateau is likely to be a combination of improved corporate security practices, and other attack methods (e.g., extortion) competing for resources with data exfiltration.

Despite the recent flattening of incident rates, data exfiltration remains potentially systemic. A major increase in claims could occur with a shift in attacker resources or availability of exploits, as described in the RMS "Leakomania" accumulation scenario.

Increasing Numbers of Large Magnitude Data Exfiltration Events

While the overall trend of events is flattening, the RMS catalog shows that the number of events of P6 and above – i.e., data exfiltration of more than one million personal records – has grown substantially in the years prior to 2016 for the U.S.

[28] RMS Cyber Incident Database.

One possible explanation is that professional criminals are concentrating their efforts on obtaining larger datasets where they can get a bigger return.

Fewer Small Data Breaches

At the other end of the spectrum, there is a measurable reduction in the incidences of smaller data breaches, as routine security measures prevent the accidental loss of data by employees that caused many of the small loss incidents in the past. The number of incidents of accidental data loss of P5 or smaller (100,000 records) was at its lowest at any point in the past five-year average.

Data Loss is Increasingly Caused by External Attackers

During 2016, the main cause of data breaches and losses was predominantly shown to be malicious interference from outside actors, rather than insider or whistleblower leaks. This continues the recent pattern observed over recent years. As proposed in the RMS "Data Exfiltration" accumulation stress test scenario, malicious outsiders pose more of a systemic threat than either accidental loss or insider leaks. Data exfiltration scenarios now explore more potential vectors for malicious outsiders to impact multiple companies in different attack patterns, sectors, and targeting preferences.

Data Breach by Business Sector

The recent incidents of data loss in different business sectors remains consistent with the previous five years of relativities, with a few notable differences. There has been an increase in data breach incidences in the retail, IT services, and manufacturing sectors that has continued into 2016.

There has been a significant reduction in data breaches from financial services companies – their incident rates are down in 2015 and 2016, compared to previous periods of breach records, reflecting the investment in security and data protection that is being made in this sector. Healthcare, despite some newsworthy events, has also seen a drop in the number of incidents – but this is counterbalanced by the fact that healthcare has seen a significant increase in extortion incidents.

A notable feature of recent data breaches has been the repeated targeting of adult social sites, such as Fling, Mate1, and Ashley Madison, where criminals can add blackmail to their earning potential from the stolen data.

Costs of Data Loss

Since 2010, the average cost per record of a data loss of over 100,000 records has more than doubled.[29] This reflects increasing regulatory fines and procedures, growing costs

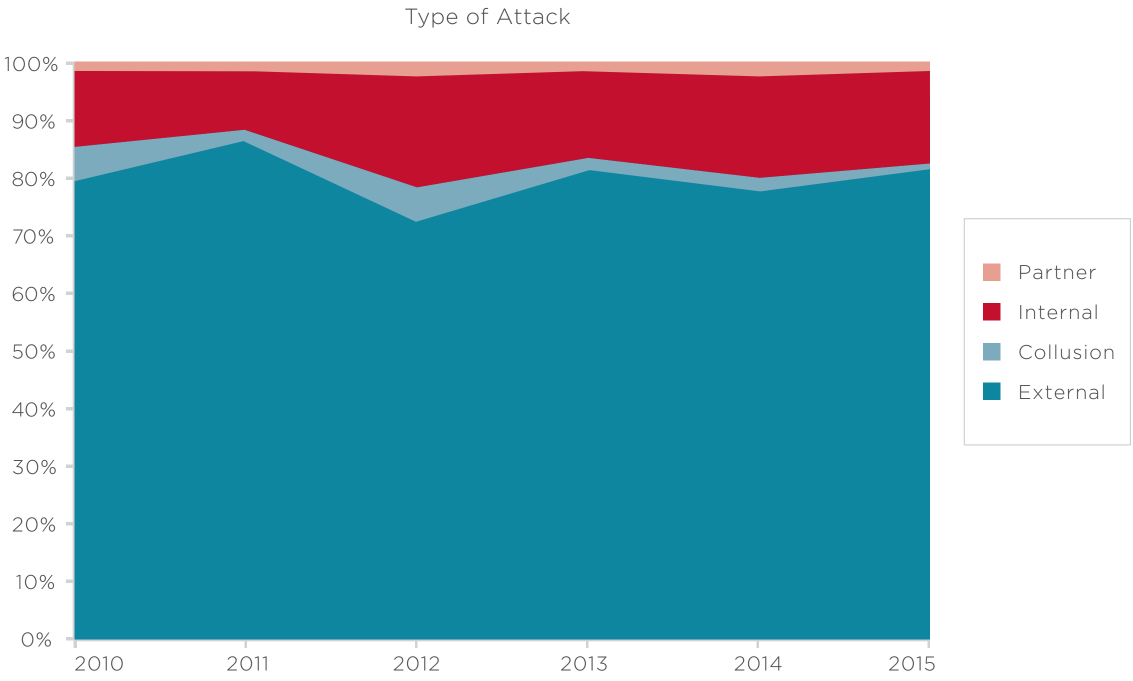


Figure 5: Percent of breaches per threat actor category over time[30]

[29] RMS Cyber Incident Database.
[30] Verizon 2016 Data Breach Investigations Report.

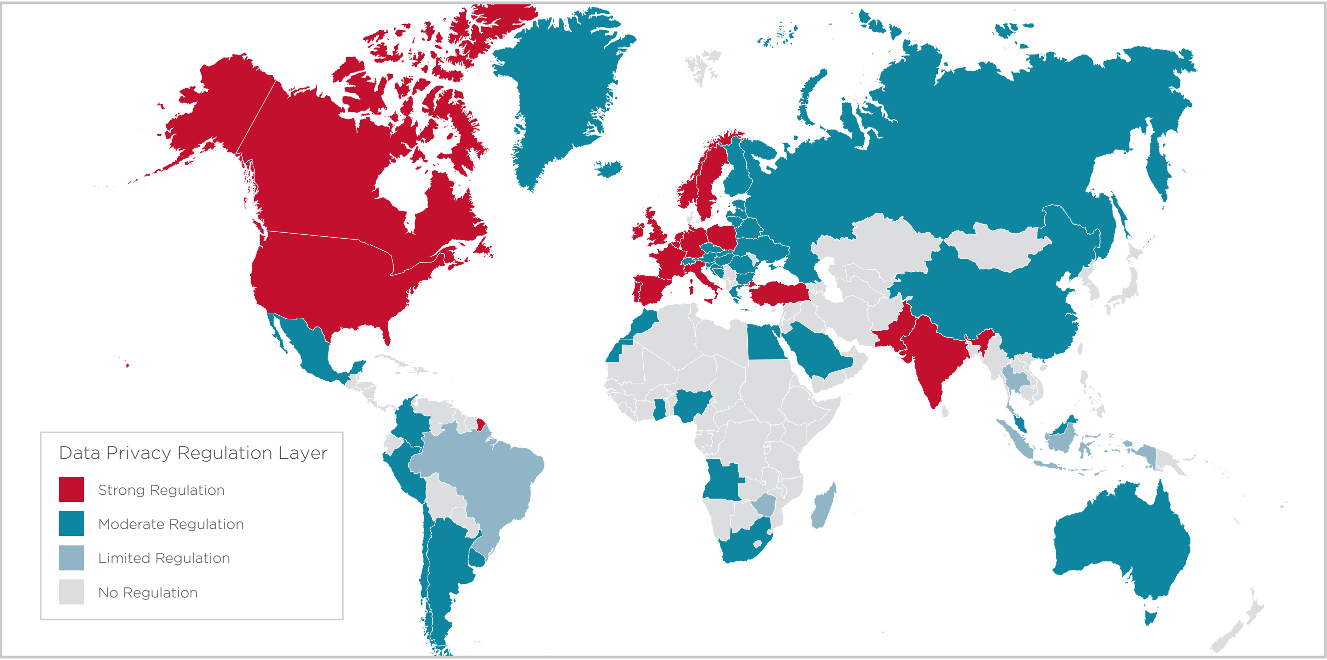


Figure 4: Data breach of privacy regulation heatmap[31]

of compensation, and escalation of legal complexities in dealing with identity loss. Projecting forward for 2017, a further inflation of costs by 15 to 25 percent could be expected.

Data Exfiltration Risk is Increasingly International

Although the U.S. remains a major source of data breach loss, sizeable data loss events were reported in many other countries in 2016. It is becoming common practice for responsible large companies in many countries to publicly disclose a data breach and to notify the individuals affected, although mandatory reporting requirements in many countries is still some way behind the United States. Statutes are currently in preparation to require mandatory reporting of data breaches in many countries, including the European Union (EU) and several other countries that are developing markets for cyber insurance.[32] The EU General Data Protection Regulation (GDPR) will require notification within 72 hours from when a breach is discovered with maximum fines of four percent of annual global turnover or €20 million, whichever is greater.[33]

Costs of data breaches to companies in other countries are broadly similar to those in the United States, although when tort actions are brought, these make U.S. data breaches more expensive than in other countries.

Implication for RMS Modeling

This shift in the pattern of data breach sizes – increased targeting of larger data sets and reductions in the incidence rate of small data breaches – is represented in the release of the "Leakomania" data exfiltration accumulation stress test scenarios in CAMS Version 2.0, with adjusted frequency-severity distributions of sizes of data leaks and the addition of a risk potential for companies in some sectors to suffer data breaches of over a billion records.

The recent trends of relativities across business sectors of data breach incidences is reflected in the CAMS Version 2.0 release of data exfiltration accumulation stress test scenarios.

The relative risk levels of cyber data exfiltration loss remain consistent with the country risk parameterizations for frequency and cost modeling in Version 1.0, with minor changes in RMS CAMS Version 2.0.

2.2 Financial Theft

Financial theft has continued to be a major source of cyber attacks and cyber-enabled fraud. The most common manifestation of financial theft is credit card misappropriation. Some of the recent higher-profile credit card misappropriations have involved hotel chains, with the

[31] Based on data from Forrester Research Data Privacy Map 2015 and DLA Piper, 2017.
[32] Forrester Research Data Privacy Map 2015 and DLA Piper, 2017.
[33] European Commission General Data Protection Directive.

Mandarin Oriental[34], Hilton[35], and Starwood[36] hotel chains each hit in separate theft campaigns involving data harvesting from their point-of-sale systems. Point-of-sale systems remain targets, particularly with legacy systems that are slow to be updated and widely distributed.

The growing use of chip and pin (EMV) credit cards is reducing theft levels in many countries. Barclays attributes EMV technology for reducing credit card-related thefts in the U.K. by 70 percent since its introduction in 2003.[37] EMV now has an 81 percent adoption rate in Europe and is in use in Australia, Russia, and several other countries. However, EMV uptake in the U.S. is slow, resulting in higher credit card misappropriation levels than in countries where this is standard. In 2015, Barclays noted that although the U.S. accounts for 24 percent of total credit card transactions worldwide, it represents 47 percent of global credit card fraud.[38]

Shift of Liability for Credit Card Thefts to Non-EMV Retailers

In 2016, Visa, Mastercard, and Europay credit card companies introduced new rules requiring retailers in Europe to upgrade their point-of-sale systems to EMV and – importantly – requiring retailers to bear the liability for fraudulent card transactions if they do not do so. This move could potentially result in increased or shifted exposure for insurance companies with retail cyber insurance policyholders if their coverage includes liabilities that were previously indemnified by the credit card companies. This has the potential to create a new route for systemic loss for cyber insurers, where many retailers suffer theft losses from non-EMV point-of-sale system cyber compromise that is not indemnified by the credit card companies.

Because of this change, RMS strongly recommends that in the CAMS cyber exposure data schema, insurers should ensure they capture data in the "Financial Loss Potential: Named Payment System Provider(s)"[39] field for retail insureds specifically for EMV compliance. The ability to report on this will become increasingly more important over time, especially for those in Europe who could otherwise potentially face liabilities from future credit card thefts, deferred from the credit card companies who have previously held this risk.

Financial Transaction Theft

The source of systemic tail-risk from cyber attack in the financial services sector is the penetration of banks internal systems and the transaction systems that link with them. There have been recent individual cyber bank robberies; in November 2016, Tesco Bank in the U.K. lost US$2.5 million from 9,000 accounts, showing that online banking systems are still vulnerable.[40] Several new types of point-of-sale and ATM malware were discovered in 2016.[41]

A truly systemic cyber bank heist involving many banks occurred in 2016, with the Lazarus SWIFT campaign (page 17). This campaign appears to have successfully stolen hundreds of millions of dollars, and to have narrowly failed to secure a transfer request for one billion dollars. Dozens of banks were compromised across several different countries by a sophisticated and well-resourced cyber hacking gang. Investigators have found similarities in the malware computer code with previous malware attributed to North Korean cyber teams. The scale of the operation was considerable, involving local bank infiltration activities in at least seven countries, the creation of a sophisticated suite of malware with many tricks to disguise its presence, and an untraceable central monitoring system to gather data transmitted from the malware. The plot was also notable for the sophistication of the money laundering operations put in place to prevent the funds from being recovered once the transaction compromise was discovered.

Networks of Trust

The key feature of this criminal gang was its ability to break into a network of trust used for financial transactions and then to use legitimate authentication protocols to syphon money out of the system.

The accumulation management of cyber insurance coverage for financial theft loss requires identification of these networks of trust as key potential sources of future correlation of loss between numbers of financial services companies.

Research is ongoing to map these networks of trust as variants of potential financial transaction cyber compromise scenarios, including:

- Consumer financial transaction systems, point-of-sale systems, online payment processing, credit and debit card purchasing and reconciliation systems, electronic funds transfers, and check clearing
- Interbank payment and lending systems, clearing houses, debit and credit systems, wire networks, settlement and reconciliation systems, credit transfer systems, and loan management
- Currency exchanges: foreign currency payment, settlement, and clearing exchanges, forex currency trading systems

[34] ComputerWeekly, 2015. 45 hotels of Mandarin Oriental hotel chain reported compromised.
[35] ComputerWeekly, 2016.
[36] Starwood, 2016.
[37] Security, 2015.
[38] Security, 2015.
[39] Cyber Insurance Exposure Data Schema Version 1.0; See CCRS (2016a).
[40] Guardian, 2016.
[41] Emm, Unuchek and Kruglov, 2016.

Lazarus SWIFT Financial Theft: The Billion Dollar Cyber Heist That Nearly Succeeded

In 2016, the SWIFT interbank financial transaction system was hit repeatedly, using specially-crafted software from a criminal gang called the “Lazarus Group.”[42] The software provided a sophisticated method of enabling the criminals to gather information on standard practices and send fraudulent requests through the SWIFT system for financial transfers disguised as legitimate transactions, from software that had been infiltrated into a number of banks with many layers of subterfuge to prevent discovery. The fraud was combined with a complex money laundering process that obscured the proceeds of the theft from investigators.

To break into the trusted SWIFT network, the gang found lower-security banks in many different countries around the world and found a variety of ways of secretly infiltrating their malicious software onto the SWIFT transaction servers. Banks were reported compromised in Ukraine, Bangladesh, the Philippines, Ecuador, Vietnam, and potentially other Southeast Asian countries.[43]

Over a period of months these banks requested other banks, including the U.S. Federal Reserve, to transfer funds via the SWIFT system with fully credentialed authentication protocols. The money was then diverted through laundering operations, including casinos in the Philippines and cover accounts in Sri Lanka and Hong Kong. The full extent of the operation and the total amount stolen remain undisclosed, but reports include US$81 million unrecovered from Bangladesh National Bank, a $10 million loss from a Ukrainian bank, a bank in Ecuador with a $12 million loss, and a dozen more potential losses to Southeast Asian banks.[44]

At one point, the gang issued 30 transfer requests totaling $951 million to be withdrawn from the Bangladesh National Bank account with the U.S. Federal Reserve. Security alerts, including reported typo errors in the requests and triggering flags on money laundering blacklists, blocked $850 million of the transfers.[45]

The discovery of the attempted billion-dollar heist has resulted in a radical overhaul of the SWIFT system and new security systems put into place.

The RMS accumulation management stress test scenario “Financial Transaction Interference Scenario” includes many of the features that were seen in the Lazarus SWIFT campaign, particularly the multimillion dollar thefts from dozens of banks in trusted financial transaction networks.

[42] Symantec Security Response, 2016.
[43] van der Walt, 2016.
[44] Riley and Katz, 2016 and van der Walt, 2016.
[45] Zetter, 2016.

> The potential is evidently growing for high-intensity attacks to be sustained for very long durations and to exceed the eight-hour threshold to cause significant insurance loss.

- Investment trading systems and exchanges, bourses, electronic trading systems and platforms, stock market data systems; automated trading systems, investment bank exchanges

High Standards of Cybersecurity in Financial Companies

Banks and financial service companies are fully aware of their susceptibility to attempted hacks and are leaders in the implementation of security systems and measures for preventing cyber theft. Expenditure on cybersecurity by banks has been high profile and extensive; the banking industry is the single largest sector of cybersecurity expenditure.[46] Bank of America disclosed that it spent $400 million on cybersecurity in 2015 and, in January 2016, its CEO said that its cybersecurity budget was unconstrained.[47] JP Morgan Chase and Co. announced the doubling of its cybersecurity budget from $250 million in 2015 to $500 million in 2016, and reported levels of expenditure by other banks reached record levels, including Citibank with $300 million and Wells Fargo with $250 million.[48]

Changes in RMS Modeling of Financial Transaction Cyber Compromise

The scale of potential losses from individual financial services institutions is clearly growing. The RMS magnitude scale for loss from a single company has been extended to include FT4, representing a loss from $1 billion to $10 billion, and a representative value of $5 billion.

The accumulation scenario, in which many financial services companies incur theft losses from a campaign of a criminal gang compromising a network of trust, has been increased in severity to reflect the fact that the Lazarus SWIFT campaign came close to replicating the scenario released in Version 1.0.

The increasing levels of security in financial services enterprises means that cyber theft events should become less likely, but the extreme case of many severe losses from within a network of trust remains an important stress test for insurers to run on their financial services accounts.

2.3 Cloud Service Provider Failure

The market for cloud services has grown by 53 percent since last year.[49] Major companies are making cloud services more of a central part of their business operations and migrating more services to the cloud. If a cloud service provider (CSP) were to interrupt its service, business operations in many companies would be impacted more significantly than they would have been just a year ago. This represents a major increase in exposure to any potential failure of cloud service providers in cyber-affirmative IT insurance portfolios.

Increased Concentration Risk in Big Four CSPs

There is also an increasing concentration of risk in the "Big 4" CSPs: Amazon Web Services, Microsoft, IBM, and Google. The "Big Four" CSPs have grown by a combined 68 year-on-year percent, and have significantly increased their collective market share from 47 to 54 percent compared to the previous year.[50]

High Resilience Standards of CSPs

The CSPs however remain resilient – their business depends on continuity of service – and they are improving their reliability performance even as they grow. Analysts consider the key goal of CSPs to be "five nines" – i.e., 99.999% of uptime. In 2014, both Amazon and Google got close to this statistic in several of their service areas.[51] In 2015, Amazon improved on this even further and managed only two and a half hours of downtime across its four major services: virtual computing, storage, content delivery network, and domain name service.[52] Each of the Big Four are improving their reliability significantly year-on-year.

[46] IDC Report 2016, reported in Forbes Tech, 2016.
[47] Forbes, 2016.
[48] Forbes, 2015.
[49] Specifically Infrastructure-as-a-Service (IaaS) such as Amazon Web Services. Richman, 2017.
[50] Sullivan, 2016.
[51] NetworkWorld, 2015. Amazon's EC2 achieved 99.9974% and Google Cloud Platform Storage System exceeding the five nines with 99.9996% uptime.
[52] NetworkWorld, 2016.

Table 2: Example of recent cloud service outages

Platform Outages (IaaS)	Date
Amazon Web Services (AWS) suffered a five-hour outage	February 2017
Amazon Web Services (AWS) suffered a five-hour outage	September 2015
Google cloud outage: Compute Engine down for 18 minutes everywhere, compensated its customers with 10-25% off their monthly bill	April 2016
Applications Outages	
Microsoft Office 365 users suffered a multiday outage	January 2016
Yahoo Mail was disrupted for several days by an outage	December 2013
Cloud SaaS Outages	
Symantec cloud-based security services down for 24 hours	April 2016

That is not to say that outages have not occurred. Table 2 lists some examples of the more significant recent CSP outages. Most outages are short and only impact part of the services or individual application areas. Services are structured into Platform as a Service (PaaS), Infrastructure as a Service (IaaS), and Software as a Service (SaaS), and failures could potentially occur in any of these service areas.

Potential for Disruption from CSP Failure

Cyber insurance policy retentions ensure that outages less than 12 hours are unlikely to trigger claims, but any CSP failures longer than this will be systemic and cause multiple claims from companies that are covered against cloud provider downtime. Most companies who have a significant part of their business operations in the cloud have increasingly sophisticated engineering approaches to maintain their own resilience and structuring contingency for individual CSP failures, but there are vulnerabilities in these systems and these present potential for widespread business interruption resulting from CSP failures. The mechanisms for potential failures continue to be those represented in the RMS accumulation management stress test scenarios – systemic and contagious hub and data center faults or malware, combined with complex repair and restoration paths.

Changes in System Architecture of CSPs

Full systemic failures of cloud providers are rare but possible. Most of the Big Four serve their customers through regional structures and individual compartments of operation, to isolate any potential failure into a single compartment. The RMS scenario for CSP failure in 2015 simulated the failure of a representative CSP in the United States that loses three regions out of the five from which it serves its U.S. customers. The regions and technical structure of CSPs is constantly evolving and becoming more sophisticated and diversified. For example, in early 2016, Amazon Web Services served its global customer base through 30 geographical "Availability Zones" in 11 regions. By early 2017, the AWS cloud infrastructure has expanded to 42 Availability Zones and 16 regions. It expects to bring another five Availability Zones and two more regions online within the next year.[53] The structural architecture of CSPs is an important factor in determining potential outage footprints, and constrains the extent of systemic impacts of CSP failure accumulation scenarios.

Updates to CSP Failure Accumulation Scenarios

In RMS CAMS Version 2.0, the "Cloud Service Provider Failure" accumulation scenarios have been updated to reflect the growing uptake of cloud services by insured companies. They model the latest structural architecture of the cloud service providers. The assumptions about time taken to restore service to customers have been updated in the light of latest examples of restoration capabilities following outages. Costing assumptions have been improved from recent examples.

2.4 Denial of Service Attacks

Denial of service attacks have continued to be a major component of the cyber risk landscape. The number of attacks has increased, with businesses reporting DDoS attacks up by as much as 130 percent year-on-year[54] and the intensity of attacks breaking new records.

[53] AWS, 2017.
[54] Digital Trends, 2015.

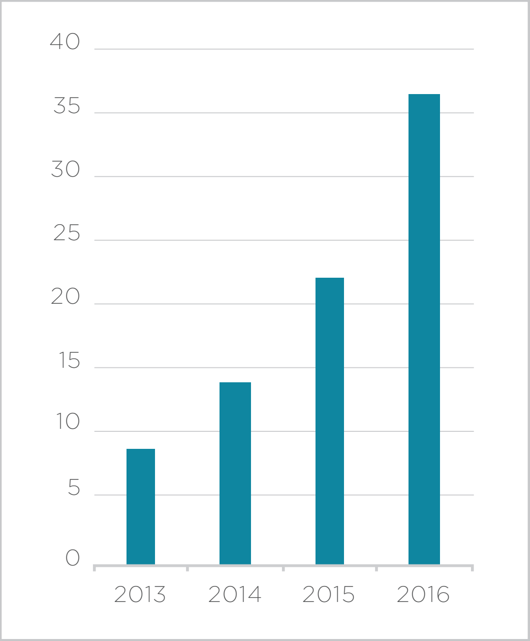


Figure 5. Average DDOS attack intensity in gigabits per second[55]

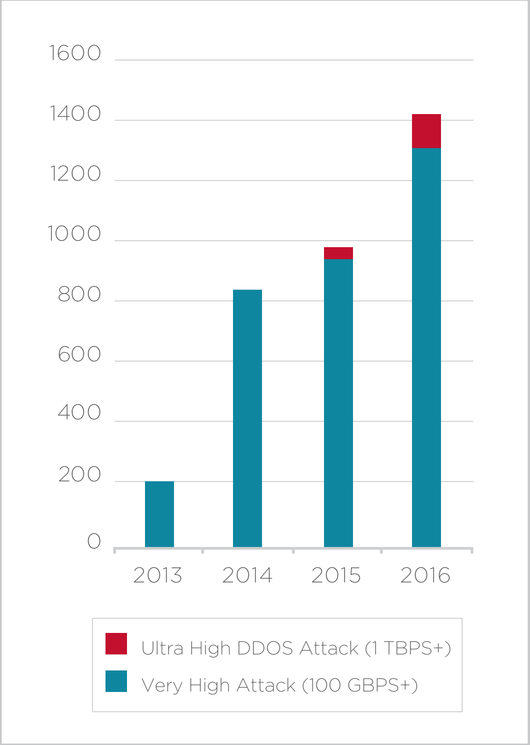


Figure 6: Frequency of "very high" and "ultra-high" DDoS attacks[56]

Increasing Intensity of DDoS attacks

In the 2015 RMS review of DDoS attacks, the largest attack intensity rate observed at that time was 600 gigabits per second, classified as a "Very-High Intensity DDoS." By the end of 2016, attacks of over 1,000 gigabits per second (a terabit per second) were being recorded, such as an attack on France-based hosting provider OVH in September 2016,[57] and now attacks of that intensity are being observed several times a month.[58] Attacks of this intensity require a new classification of "Ultra-High Intensity DDoS Attacks."

In addition to these ultra-high intensity DDoS attacks, even the "average" attack has seen a significant increase in intensity. The average attack intensity increased by 60 percent between 2014 and 2015, and in 2016 increased a further 70 percent to 37 gigabits per second.

The significance of the intensity levels of these attacks is that large commercial servers designed to deal with high traffic volumes are resilient against attacks of low intensity, but very-high intensity and ultra-high intensity attacks can bring down even the strongest websites. It is possible that there are not any web servers available that are not currently vulnerable to disruption of DDoS attacks if the intensity of potential attacks continues to scale up. The Dyn attack (see page 21) is one example of an attack on a piece of Internet infrastructure called the domain name system (DNS) that connects web addresses with IP addresses, for servers hosting the web addresses.[59] This type of attack has systemic impacts as many seemingly unrelated companies use this service, such as Airbnb, Netflix, and Amazon.[60]

Internet of Things: A New Technology for DDoS Attacks

The technological innovation in creating DDoS attacks has helped increase the intensity of these attacks. The "Internet of Things" (IoT) has brought many devices online with low security levels. An HP Fortify study found that as many as 70 percent of IoT devices are vulnerable to attacks due to weak passwords, insecure web interfaces, and poor authorization, with new vulnerabilities being discovered each year.[61] These devices can be "enslaved" easily to create volumes of traffic to fire against a target. The Dyn attack in October 2016 utilized freely distributed software to infect online IoT devices to control their use in the attack. Until the security of online devices is improved, these types of attacks will become more common, likely in greater and greater intensities as the number of online devices proliferates.

[55] Akamai 2016.
[56] Akamai 2016.
[57] The Hacker News, 2016.
[58] Akamai, 2016.
[59] Newman, 2016.
[60] Woolf, 2016.
[61] Rawlinson, 2014 and Constantin, 2016.

Dyn DDOS Attack

On October 21, 2016 Dyn suffered two separate outages when hit by a massive DDoS attack, reaching intensities of 1,200 gigabits per second.[62]

Dyn is an Internet traffic management product managing domain name system (DNS) infrastructure. Among its services, it provides protection to companies from DDoS attacks. It optimizes web traffic and provides servers that are located geographically close to customers to enhance user experience.

Because Dyn optimizes server traffic for other companies delivering web services, many Dyn customers were affected, including some of the largest names in web-commerce, including Amazon.com, Netflix, Airbnb, Spotify, PayPal, PlayStation Network, GitHub, and DirecTV, as well as many corporate and government web services.[63]

Attackers used a botnet from the Internet of Things (IoT), using online devices with low embedded security, such as printers, cameras, baby monitors, and residential hubs. An estimated 100,000 malicious endpoints were involved in the attack. They were coordinated into a botnet using Mirai malware, freely distributed software, used to infect the IoT devices.[64]

The attack also had specific geographical attributes, with 18 points of presence attacked in the densest population regions of United States and parts of Western Europe (see map). Although cyber-attacks typically do not have a strong geographical footprint, this attack is notable for the geographic clustering of the customers who lost service from their various providers.

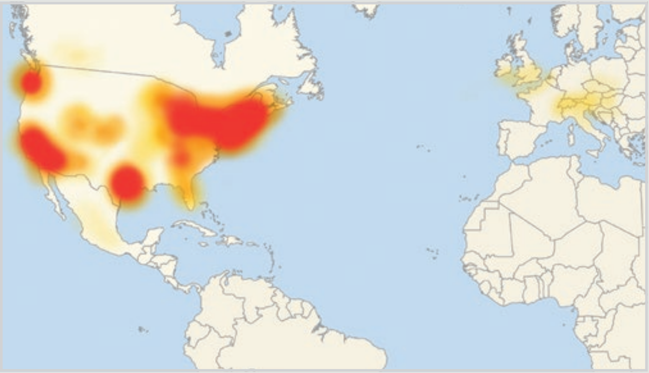


Figure 7: Map of Internet outages in Europe and North America caused by the Dyn cyber attack (as of October 21, 2016 1:45 p.m. PT)[65]

[62] Ibid.
[63] Woolf, 2016.
[64] Ibid.
[65] Source: DownDetector, Wikipedia Commons.

> Very-high intensity and ultra-high intensity attacks can bring down even the strongest of websites.

Increasing Frequency of DDoS Attacks

Sites that monitor web traffic and denial of service attacks are observing significant increases in numbers of attacks, quarter-on-quarter. Akamai, for example, has detected increases in the number of DDoS attacks of between 15 and 30 percent each quarter for the past year.[66]

Attacks are increasingly multivectored (over half in 2016), making them more difficult to mitigate. Attacks most commonly originate from or are routed through servers in China, although attacks are directed via servers in many countries, including the U.S., Turkey, Brazil, South Korea, and other territories.

Repeat Attacks on Targets

Repeat attacks on targets are a common characteristic of DDoS attacks. The average number of DDoS attacks per target is increasing, from 17 in the third quarter of 2015 to 30 by late 2016.[67] There is a wide variation in number of attacks per target, with some companies reporting many hundreds of repeated attacks.

Sectoral Preferences in DDoS Targeting

Profiling the business sectors that experience the highest number of DDOS attempts shows that the targeting has remained relatively consistent with the background relativities proposed for Version 1.[68] Software and technology companies are targeted in a quarter of attacks. Over half of all attacks are directed against gaming companies and their servers. Media and entertainment companies are the next most popular targets, followed by Internet and telecom companies.[69] Financial services companies have seen reductions in attacks – previously they were attacked more than media and entertainment, and Internet and telecom companies. Other sectors, such as retail, education, public sector, business services, and hotel and travel, continue to receive a significant, though smaller, proportion of all attacks.

Duration

The duration of attacks and the time that servers can be interrupted is a key component of potential insurance loss. The typical deductible level for cyber insurance coverage is eight hours, and most of the high-intensity attacks being observed are still well below this eight-hour threshold. The most severe DDoS attack recorded in 2016 lasted for a total of three hours at 1,200 gigabits per second.[70] Long-duration attacks of low intensity and multiple repeat attacks are more common. The potential is evidently growing for high-intensity attacks to be sustained for very long durations and to exceed the eight-hour threshold to cause significant insurance loss, but this is not yet a common characteristic of DDoS attacks.

Property Business Interruption Due to DDoS Attack

A DDoS attack was responsible for the loss of control of a central heating system in two tower blocks in Lappeenranta, Finland, in an example of potential new types of attacks on connected operational technology (OT) systems.[71] This attack raises the possibility of commercial property being rendered unusable by DDoS attacks and potentially incurring insured loss if coverages are ambiguous. This attack is also scalable to similar building management systems, with a vulnerability in one system allowing hackers to cause disruption or even damage to multiple buildings are a time. It also presages more general potential for loss from attacks on OT systems in industrial control systems and other areas of potential insurance exposure.

Updating of RMS Mass DDoS Scenarios

The accumulation scenarios for mass DDoS in RMS CAMS Version 2.0 incorporate the current trends in DDoS attacks. The attacks reflect the use of IoT botnets to create higher-intensity and longer sustained duration of attacks across a broad number of commercial targets as well as including constraints on the total DDoS traffic the Internet can support at a single point in time.

2.5 Cyber Extortion

Attempts to extort major companies using cyber attacks are still relatively rare, but events are growing in frequency and the scope of their ambition. The issue is common in personal computing and is occasionally seen in attacks on companies. There have been recent examples of cyber

[66] Akamai, 2016.
[67] Akamai, 2015 and Akamai, 2016.
[68] Akamai, 2016.
[69] Ibid.
[70] York, 2016.
[71] Rounela, 2016, and Paul, 2016.

extortion demands on corporations resulting from data exfiltration, in which confidential data is threatened to be released, and as part of denial of service attacks. These elements are likely to become more common components of these loss processes in the future.

Ransomware Attacks on the Rise

The use of ransomware, where malware is infiltrated into the networks of a company and disables servers or locks-up data until a ransom is paid, has become more of a concern for cybersecurity specialists. Beazley handled four times as many ransomware incidents in 2016 compared to 2015, and expects the rate of incidents to double in 2017.[72] Advisen data also shows a marked increase in ransomware events (see Figure 7). In the past year, there have been several examples of companies disabled by extortion malware attacks.

Cyber Extortion Attacks on Hospitals

Notably, cyber attackers have repeatedly targeted hospitals, with multiple facilities and clinics in the U.S., Germany, and elsewhere experiencing potentially life-threatening computer systems failures accompanied by demands for payment to restore IT functionality.[73] Payments in the range of thousands of dollars and tens of thousands of dollars (E1 and E2 in the scale of cyber extortion levels used in RMS CAMS) have been made, usually in Bitcoin. Examples include the Hollywood Presbyterian Medical Center in California, which paid a $17,000 Bitcoin ransom in February 2016 for the decryption key to unlock their patient data.[74] Several MedStar Health hospitals and clinics in the Baltimore-Washington area were reportedly hit with ransomware in March 2016, leading to patients being turned away.[76]

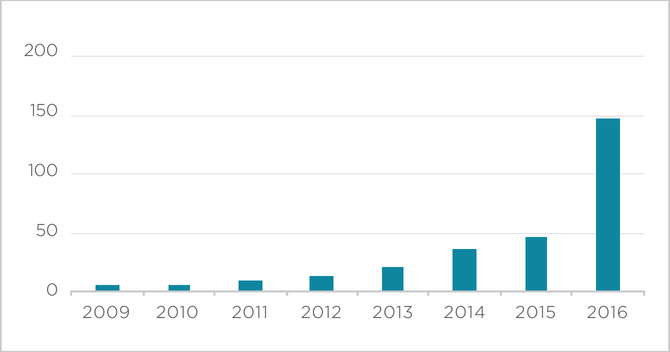


Figure 7. Cyber ransomware annual incidents[75]

Few companies admit to being targeted by ransomware or paying ransom demands and so historical data is scant. The costs of business disruption are typically much higher than the ransom payments, which may constitute the most significant exposure for insurers in covering cyber extortion.

Not all companies give in to demands. A ransomware attack that froze the payment system of the San Francisco Municipal railway system, accompanied by a demand for $73,000 in November 2016, was dealt with by allowing customers to ride for free while the system was rebuilt instead of paying the ransom.[77]

Locky: A New Suite of Ransomware

The cyber extortion industry for personal computers is expanding. In addition to the families of ransomware cataloged last year,[78] a new suite of ransomware called "Locky," has come into circulation.[79] Locky is typically spread by email (often in an invoice requiring payment) and is international in nature, presenting in several languages with the ransom demand tailored to the country and possibly other user characteristics. The Dridex gang is suspected to be behind the Locky software and is thought to be responsible for several early ransomware and malware packages, including a banking trojan. Analysts suspect that the Dridex gang is now well-resourced with gains from earlier criminal campaigns and is becoming more ambitious, scaling up its distribution and targeting, including targeting small and medium-sized businesses. It is possible that the Hollywood Presbyterian Medical Center ransomware attack was the Locky payload.

Updating of RMS Extortion Spree Scenarios

The accumulation scenarios for Cyber Extortion originally released in RMS CAMS Version 1.0 anticipated an increase in extortion incidents in commercial businesses, envisioning a campaign of ransomware that could potentially impact thousands of small and medium companies, paying sizable ransom amounts and suffering business disruption. The increases in cyber extortion incidents on businesses reported during the past year supports this view of the growing importance of this loss process and the need for an accumulation scenario of systemic campaigns of extortion.

[72] Beazley, 2017.
[73] Beazley, 2017 and Zetter, 2016.
[74] Advisen, 2017.
[75] Los Angeles Times, 2016.
[76] Cox, 2016.
[77] The Merkle, 2016.
[78] CCRS, 2016.
[79] Malwarebytes Labs, 2016.

The ransom payouts incorporated in the Version 1.0 scenario were drawn from previous extortion examples over the past decade, but typical ransom payouts reported over the past year have not sustained these substantial amounts. In CAMS Version 2.0, we redefine the magnitude scale of ransom payouts to match recent experience, and use this new scale to define distributions of increased incidence of these payouts across insured companies. We no longer constrain extortion incidents to small and medium-sized enterprises, and now include a low incidence for large companies. Ransom demand levels have been reduced to align with the latest trends. Business interruption consequences have been expanded to reflect recent evidence.

CAMS Version 1.0 Scenarios

Cyber Data Exfiltration

Three rare "zero-day" vulnerabilities provide a criminal gang with the capability to scale data exfiltration attacks across thousands of companies. Billions of confidential data records are leaked in a few months, more than the total number of confidential data records leaked in the past 10 years.

Denial-of-Service Attack

Hacktivists build the largest DDoS capability yet seen and target it at capitalist corporate websites to disrupt e-commerce. They generate DDoS traffic at many multiples of the most extreme peak rates seen on the Internet, which is concentrated on insured businesses.

Cloud Service Provider Failure

A technical error leads to an outage at a leading cloud service provider, causing its customers to lose service for many hours until they are gradually reconnected. The outage is on a scale never experienced by a commercial CSP, in terms of proportion of its customers affected and reconnection times.

Financial Transaction Cyber Compromise

A coordinated cyber heist operation on many financial services companies to syphon funds from transactions, obtain cash from ATMs, and carry out insider trading using stolen information. It is carried out on a scale that is orders of magnitude larger than any known cyber theft to date.

Cyber Extortion

Hackers graduate from personal computer ransomware to create a sophisticated system of encrypting small and mid-sized business corporate servers. They attack large numbers of enterprises, and demand high ransom payments, on a scale far beyond anything seen even in the PC environment to date.

SECTION 3

Silent Cyber Insurance Exposure

CAMS Version 1.0 focused on affirmative cyber insurance scenarios and identified loss processes from cyber attacks that target information technology (IT) systems such as databases, software, and websites.

It is also becoming apparent that there is potential for cyber attacks to cause disruption and damage that could trigger insurance payouts in traditional non cyber-specific lines of business. For example, if a cyber attack causes physical damage, destruction of property, fires or explosions, deaths, injuries, loss of services, or other harms that are covered in policies without excluding cyber as a cause, then insurers could suffer losses under these policies.

The policies in these lines of business may be silent on whether they would pay out if cyber was the proximate cause. "Silent" exposure to the peril of cyber is a growing concern. Many insurers have instigated reviews of the lines of business that may contain silent exposure to identify ambiguities in the terms and conditions of policies, and to identify the amount of risk that this may represent.

CAMS Version 2.0 contains an additional suite of scenarios that enable an insurer to review the exposure it may face from silent coverages in other lines of insurance business, described on page 28. These scenarios enable insurers to identify potential losses from lines of business including property – commercial and residential – marine, energy, industrial, facultative, specialty, casualty/liability, and other lines.

3.1 Operational Technology (OT) Attacks

Cyber attacks can cause property damage and disruption when they are targeted on interfering with the computerized systems that control physical processes, known as operational technology (OT) attacks.

There have been several examples of cyber attacks on OT, including:

- "Stuxnet" is the most prominent example of a cyber attack causing physical damage to centrifuges that separate nuclear materials.[80]
- Researchers demonstrated that a cyber attack on a 2.25 megawatt (MW) electricity generator could cause physical damage to the unit. The vulnerability in the generator software was called "Aurora."[81] This vulnerability not only has the potential to cause damage to the generator and surrounding buildings from fire, but also a lengthy blackout that could cause significant business interruption.[82]
- A cyber attack on Ukrainian power companies caused a power outage for thousands of customers for several hours in December 2015, and another suspected event in December 2016 (see page 30).[83]
- Iranian hackers gained remote access to a 20-foot dam north of New York City in 2013.[84] While no damage was done, this attack demonstrates the potential vulnerability of critical national infrastructure to cyber attacks.

[80] Zetter, 2014.
[81] Meserve, 2007.
[82] See CCRS report on Lloyd's Business Blackout Scenario, 2015.
[83] ICS-CERT, 2016.
[84] Strohm, 2016.

3.2 Smart Devices and the Internet of Things

There is a concern about potential attacks on various types of physical control systems that can be controlled electronically, particularly where they are connected to networks and could be accessed by unauthorized third parties. These smart devices and "cyber-physical" systems[85] consist of a wide range of sensors, actuators, valves, switches, mechanical devices, and electronic controls sometimes known as supervisory control and data acquisition (SCADA) systems, and perhaps most crucially in industrial control systems (ICS). Many electronic systems now contain elements of connectivity for diagnostic read-outs, upgrading and programming uploads, data transmission, and signal processing.

The proliferation of devices that are connected to the Internet has given rise to the term the "Internet of Things" (IoT). This is also described as "the infrastructure of the information society." It is estimated that there are currently around 28 billion devices connected to the Internet, and various projections suggest that the number could reach 50 billion by 2020.[86] The number of devices connected to the Internet is currently increasing by 30 percent year-on-year.[87] There are many studies that describe the growing potential for the transformative power of IoT including smart grids, smart homes, intelligent transportation, and smart cities.

It is evident that the IoT has significant vulnerability to malicious manipulation. The increasing ubiquity of connected devices causes concerns for the insurance exposure that it could potentially represent. Connected and smart devices are a growing part of the everyday world and cybersecurity issues have been raised around products varying from household appliances, industrial process control systems, building heating and ventilation systems, webcams, drones, autonomous cars, medical devices and heart pacemakers, and entertainment systems.

Many of these systems were originally designed with poor attention to security, and have relatively low levels of anti-hacking protection. This is likely to change over time as manufacturers are held to higher standards of security, but low costs and volumes of products constrain the levels of protection that can be expected. The January 2017 filing by the United States Federal Trade Commission against the D-Link Corporation[88] because its devices were used in the Dyn attack (see page 21) is the first example of a lawsuit against a manufacturer of IoT devices for poor cybersecurity, and this may prove influential in improving the security standards of IoT devices in the future. Improvements in security are unlikely to occur rapidly, so society and insurers may have to accept vulnerabilities in these systems and their potential for use in cyber-physical attacks for some time to come.

3.3 How Can Cyber Attacks Cause Physical Damage?

Examples have been seen of using cyber attacks in several ways to trigger physical damage. They broadly follow the following types of interference processes.

Spoofing – Sending False Data to a Sensor

When a sensor is vital to the safe performance of a system, spoofing the sensor can trick the system into unsafe activities. An example would include thermostat readings that normally prevent a process overheating, so by spoofing the thermostat, the system could be forced into overheating. Other examples would include spoofing GPS interpretation, electronic map systems, or beacons that guide aircraft navigation systems. Sending false data can potentially be a damaging attack mechanism.

Hysteresis – Forcing Cyclical Behavior

Once an unauthorized hacker has control of a physical system, damage can sometime be caused by forcing the system to start and stop in rapid cycles. This causes machinery to wear out, damage bearings and misalign, overheat, blow electrical fuses, and potentially trigger uncontrolled positive feedback. The "Aurora" vulnerability in power generators and thermal runaway in lithium batteries are examples of hysteresis damage in cyber-physical attacks.

Disconnection – Stopping the Function of a Device

Simply preventing a physical system from connecting to its control system may be enough to cause damage and loss. A denial of service attack on a system that requires connectivity to operate can shut down a process. Examples include disabling a building management system with a DoS attack; by making it unable to connect to the Internet it was unable to start a heating system for an apartment building.[89]

Draining the battery of a device by forcing it into constant activity is also a method for causing the failure of connected battery-powered systems.

[85] Loukas (2015).
[86] Statistica, 2017.
[87] Gartner, 2015, reports 6.4 billion connected devices in 2016, up 30 percent from 2015.
[88] FTC, 2017.
[89] SC Media, 2016.

Cyber Insurance Exclusions

Many exclusion clauses have been developed for traditional general liability and property policies to help insurers prevent loss accumulation from cyber events. Two of the exclusions (CL 380 and LMA 3030) prevent claims from cyber events committed with malicious intent or deemed acts of war, while NMA 2912, 2914, and 2915 exclusions prevent property damage claims from cyber events unless caused by fire or explosion.

Actuators – Controlling Physical Components

Actuators open and close valves, lock and unlock doors, control robot arms, change the pitch of ailerons, drive car accelerators, apply brakes, and control many other processes. The remote control of actuators has significant potential to cause damage, either by preventing them from operating or causing them to operate unsafely. Cyber attacks have opened valves and manipulated pumps to maliciously release water, sewage, and gas supplies, for example. There is obvious potential for deliberate accidents to be caused in transportation systems, manufacturing, industrial processes, and other systems where remotely-managed actuators are an integral part of the operation. Industrial and manufacturing systems tend to have security systems and fail-safe mechanisms, but these may not have always been designed against malicious intent, and determined hackers have found ways to penetrate even well-designed security systems.

3.4 Cyber-Physical Attack Scenarios in RMS CAMS Version 2.0

The greatest concerns for insurers are the potential for cyber-physical attacks to trigger fires, explosions, or to cause major industrial accidents or system failures that could lead to large losses or systemic claims across multiple insureds.

Cyber-physical attacks have the potential to cause claims on traditional policies that do not explicitly exclude cyber as a proximate cause, but include the consequential perils of fire and explosion, water escape, or other destructive processes. Lines of business that could potentially be impacted include marine, aviation, energy, casualty liability, and property.

RMS CAMS Version 2.0 includes an additional suite of scenarios, listed on page 31, that can be used by insurers to test their exposure to cyber-physical attacks and identify their silent exposure in policies in several lines of business, including commercial and residential property, marine cargo, industrial facilities, offshore energy, and a variety of other lines impacted by cyber-induced power outage scenarios.

Cyber Attack on Ukrainian Power Grid

On December 23, 2015, three regional electricity distribution companies in Ukraine reported service outages to an estimated 225,000 customers.[90] The outages were caused by external agencies that delivered malware via a phishing attack, gaining access to the companies' computers and remotely controlling the industrial control systems (ICS) to disconnect the substation power breakers, disabling power supply. At least 30 110kV and 35kV substations were disconnected for three hours.[91] Ukrainian government officials blamed Russian security services for the incident.[92]

The event has highlighted the potential for OT cyber attacks and the vulnerability of national critical infrastructure, a threat that is being taken seriously by Western governments and national cybersecurity agencies worldwide.

Investigators are reviewing another suspected cyber attack on the SCADA systems of the 330 kW Kiev substation grid, which caused a 75-minute outage for the northern part of Kiev in December 2016, during one of the colder months in Ukraine.[93]

RMS CAMS Version 2.0 includes a suite of accumulation scenarios of potential OT attacks for insurers to manage their silent OT cyber exposures.

[90] ICS-CERT, 2016.
[91] Lee, Asante and Conway, 2016.
[92] Zetter, 2016.
[93] Constantin, 2016.

Scenarios added in CAMS Version 2.0

Cyber-Induced Fires in Commercial Office Buildings

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. The attack is coordinated to occur on a specific night. A small proportion of the infected laptops left on charge overnight then overheat and catch fire; some unattended fires in commercial office buildings spread to cause major losses. Insurers face claims for a large number of fires in their commercial property and homeowner portfolios.

Cyber-Enabled Marine Cargo Theft from Port

Cyber criminals gain access to a port management system in use at several major ports. They identify high-value cargo shipments and systematically switch and steal containers passing through the ports over many months. When the process of theft is finally discovered, the hackers scramble the data in the system, disabling the ports from operating for several days. Insurers face claims for cargo loss and business interruption in their marine lines.

ICS-Triggered Fires in Industrial Processing Plants

External saboteurs gain access to the process control network of large processing plants, and spoof the temperature and pressure set points of the ICS, causing heat-sensitive processes to overheat and ignite flammable materials in storage facilities. Insurers face sizeable claims for fire and explosions at several major industrial facilities in their large accounts and facultative portfolios.

PCS-Triggered Explosions on Oil Rigs

A disgruntled employee gains access to a network operations center (NOC) controlling a field of oil rigs and manipulates several of the platform control systems (PCS) to cause structural misalignment of wellheads, damage to several rigs, release of oil and/or gas, and fires. At least one platform has a catastrophic explosion. Insurers face significant claims to multiple production facilities in their offshore energy book.

Regional Power Outage from Cyber Attack on U.S. Power Generation

A well-resourced cyber team introduces malware into the control systems of U.S. power generating companies that creates de-synchronization in certain types of generators. A sufficient number of generators are damaged to cause a cascading regional power outage that is complex to repair. Restoration of power to 90 percent of customers takes two weeks. Insurers face claims in many lines of business, including large commercial accounts, energy, homeowners, and specialty lines. The scenario is published as a Lloyd's Emerging Risk Report "Business Blackout" by Cambridge Centre for Risk Studies, and was released in RMS CAMS Version 1.1.

Regional Power Outage from Cyber Attack on U.K. Power Distribution

A nation state plants "Trojan Horse" rogue hardware in electricity distribution substations and activates it remotely to curtail power distribution and cause rolling blackouts intermittently over a multi-week campaign. Insurers face claims in many lines of business, including large commercial accounts, energy, homeowners, and specialty lines. The scenario is published as "Integrated Infrastructure: Cyber Resiliency in Society" by the Cambridge Centre for Risk Studies, and was released in RMS CAMS Version 1.1.

SECTION 4

What's New in RMS CAMS Version 2.0

The cyber risk landscape is changing dramatically, and the insurance industry is reacting quickly with adaptations of its products and services to help its insureds with the protection they need and to meet the growing demand. RMS is serving our insurance clients by keeping abreast of this dynamic peril and providing analytical tools for managing accumulations of cyber exposure.

4.1 Updates of Affirmative Cyber Insurance Accumulation Scenarios

Data Exfiltration

The revised Data Exfiltration Version 2 scenarios reflect the increase in the number of large data sets being targeted by professional criminals and the systemic nature of multiple large-magnitude data thefts that could occur if cyber penetration toolkits, such as those released by ShadowBrokers, find their way into criminal hands. The shifting targeting pattern of criminals stealing data from different business sectors is reflected in the new scenario footprints. An important new enhancement is the differentiation in the scenario suite among different types of personal data, with the addition of separate stress test scenarios for personal identifiable information (PII), payment card information (PCI), and personal health information (PHI). The scenarios have been updated to reflect the trend of increasing costs and the emerging picture of international incidence rates and relative costs.

Financial Theft

The updates of the Financial Transaction Interference Version 2 stress test scenarios incorporate the lessons from the SWIFT cyber heist in confirming the potential for a single campaign to steal large financial sums from multiple financial services providers. The stress test suite is updated to incorporate larger campaigns than those seen to date. The loss magnitude scale is extended to incorporate larger losses per bank and reflects the significant improvements in security being implemented in the networks of trust being used by the financial services community.

Cloud Service Provider Failure

Cloud Compromise Version 2 stress test scenarios have been updated to incorporate the substantial growth in cloud usage by companies, the increasing domination of the market by the big four providers, and the restructuring of the cloud service provider (CSP) infrastructure that is being developed and expanded to meet this growth. Outages are analyzed by restoration curves: the proportion of customers reliant on regions and availability zones in the CSP's architecture who have services reconnected over time. These are updated to reflect the potential for complex technical failures to deprive customers of their cloud functionality for periods of time and the zonal dependencies of the CSP customer base. Insurers are encouraged to capture CSP information about their insureds in the CAMS system to improve their exposure risk management.

Denial of Service Attacks

The updating of Mass DDoS Version 2 scenarios incorporates the increase in DDoS firepower that has become available to attackers through harnessing IoT devices and includes new intensity levels for attacks. The maximum volume of attacks in the stress test scenario is now informed by analysis of the total firepower that could be obtained by a campaign that succeeded in harnessing all devices available on the Internet. The targeting pattern of DDoS attackers reflects recent patterns of targeting as well as those that would have the most severe impacts on cyber insurance portfolios.

> The shifting targeting pattern of criminals stealing data from different business sectors is reflected in the new scenario footprints.

Cyber Extortion

Stress test scenarios for the Cyber Extortion Version 2 now include incidence of extortion on larger companies as seen in the past year as part of a systemic campaign with ransom payment amounts recalibrated to recent experience. The targeting incorporates the recent trend of targeting the healthcare sector. Business interruption consequences have been expanded to reflect evidence of the impact of extortion events.

4.2 Expected Loss Baselines

In addition to stress test scenarios, RMS CAMS Version 2 introduces an expected loss baseline for U.S. businesses for data exfiltration. Data exfiltration accounts for a large proportion of the insurance costs of typical affirmative cyber insurance products. The data exfiltration expected loss baseline provides average annual industry loss values, before insurance is applied, for incidence rates of different magnitudes of data exfiltration events by business sector and company size. It enables clients to benchmark their own loss experience to industry averages, to set expected loss levels and burn rate assumptions, and to explore potential market expansion strategies for safe diversification of new business.

The expected loss baseline is calibrated from the historical average annual incident rates experienced in U.S. businesses over the past six years. We augment this to apply cost levels that are trended to estimate likely claims values for 2017/18. This provides a portfolio-specific estimation of burn rate for data exfiltration incidents for cyber insurance accounts across businesses of different sectors and sizes, if incident rates continue their historical average levels.

4.3 Cyber-Physical Attack Scenarios

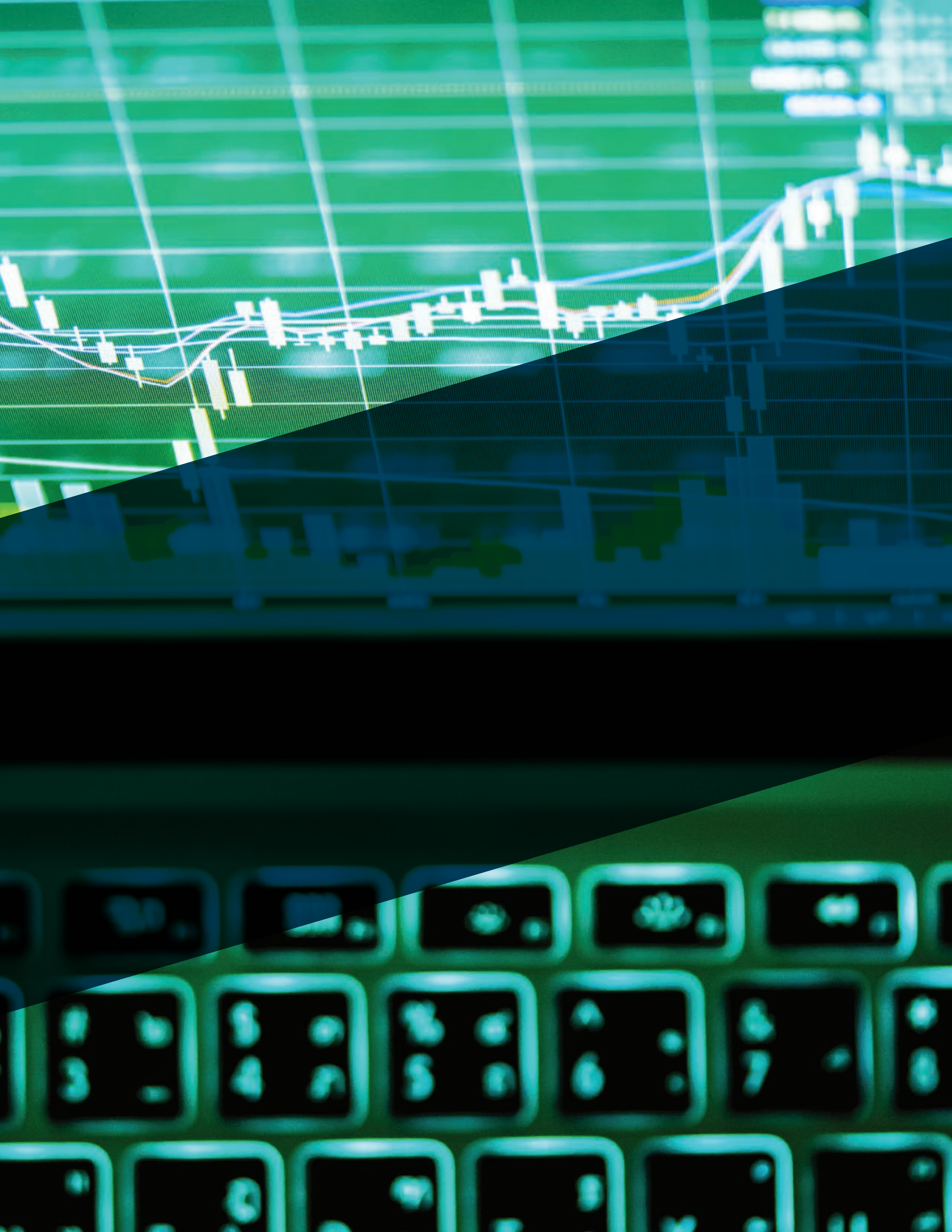
To respond to client demand for stress tests for silent cyber exposure in other lines of business, CAMS Version 2 provides a suite of cyber-physical attack scenarios. These are described above (see page 31), and more detailed technical specifications are available to clients.

4.4 Improvements in Functionality

RMS CAMS Version 2.0 has been rebuilt on a new software platform to improve the ability to add future features and functionality. It incorporates a new user interface designed to help clients in their workflows and incorporates additional report generation to aid risk management decision making.

RMS CAMS Version 2.0 Scenarios

- **Cyber-Induced Fires in Commercial Office Buildings**
- **ICS-Triggered Fires in Industrial Processing Plants**
- **Cyber-Enabled Marine Cargo Theft from Port**
- **PCS-Triggered Explosions on Oil Rigs**
- **Regional Power Outage from Cyber Attack on U.S. Power Generation**
- **Regional Power Outage from Cyber Attack on U.K. Power Distribution**



SECTION 5

Cyber Insurance Market Update

As a result of the new pressures in the cyber risk landscape, the insurance industry has continued to evolve and grow.

5.1 Rapid Growth

The global cyber insurance market continues to experience strong growth. The affirmative cyber insurance market is estimated to have increased in premium volume from around $2 billion in 2015 to up to $3.5 billion in 2016. The large majority of this insurance is purchased in the U.S. and is focused on cover against breach of privacy.

Several analysts forecast the market growing rapidly, with some predictions stating that the global cyber insurance market will reach $7.5 billion by 2020.[94] Others predict estimates of over $20 billion by 2025.[95]

Even the more conservative growth forecasts expect annual cyber premium growth rates of over 20 percent. With the context of a wider P&C soft market, many insurers are making cyber insurance a key area of focus.

The current drivers of cyber insurance premium growth are:

- Existing customers purchasing greater limits and additional coverages: In business sectors where customers have already purchased cyber insurance, customers are looking for more cover, increasing their limits, and adding further coverages, such as business and contingent interruption, to complement the breach of privacy coverage they already have.
- Strong growth from small and mid-sized (SME) companies: Many SMEs are required to purchase cyber insurance, which is a common stipulation under the terms and conditions when SMEs work with other companies. More SMEs are now aware of the cyber risk posed, their obligation to their customers, and the availability of appropriate insurance coverage.
- Strong growth from other sectors: Currently, cyber insurance take-up is largely within a relatively concentrated set of business sectors, but cyber insurance premium growth is expected to become more mainstream, with take-up from more sectors outside of this current core.
- New regulations to drive international demand: With most cyber premiums currently generated in the U.S., growth is likely to accelerate in non-U.S. markets driven by new regulatory requirements. One such area of growth will be the European Union (EU) where EU-wide legislation for cybersecurity is due to be ratified during 2018. The EU directive sees providers of critical infrastructure and essential physical and digital services adopting strengthened cyber defense measures, along with heightened reporting requirements for security incidents.

5.2 Market Participants

The growing market is attracting an increasing number of market participants. More than 50 companies now offer affirmative cyber policies, up from around 35 in 2015, a 43 percent increase.

Most of the cyber insurance premium written today originates from around ten of the largest cyber writers, who each write more than $100 million of premiums annually; a similar number are writing between $25-$100 million. Most of the market participants are responsible for writing less than $25 million in annual cyber insurance premiums, and typically represent newer entrants who are gaining experience in the market with low exposure.[96]

[94] PWC, 2015.
[95] Allianz.
[96] The Betterly Report, 2016.

In addition, more insurers are integrating cyber cover in the policies of their traditional business lines. This increase in the number of market entrants, together with extension of cyber into traditional policies, both present significant challenges to cyber risk management.

Most cyber premiums still originate from the U.S. where data privacy laws have been in place for over 10 years, though an increasing amount of cyber risk is being written internationally, with the London market making a significant play to increase its cyber expertise.[97]

For reinsurance, though the market for cyber is comparatively small, reinsurers are playing an active role in increasing the capacity available for the primary carriers. Most reinsurance being written today is placed as per-risk quota share, with some agreements having an aggregate stop loss term in place. There is a move towards excess of loss agreements; however this is still a nascent market for cyber and RMS expects per-risk agreements to remain as the mainstay for 2017.

The reinsurance market is expected to continue to grow as the primary market increases and insurers look to cede out a portion of the risk. Improved cyber exposure data capture techniques and improved risk quantification is also expected to lead to additional forms of reinsurance becoming more commonplace.

5.3 Available Insurance Coverage

Cyber insurance products and coverages are likely to evolve over time, as this area attracts more focus from corporate risk management functions.

Wide Variety of Available Coverage

As part of its market review, RMS explored the types of cyber coverage being offered by re-examining the range of cyber policies currently available. This assessment revealed that the 19 coverage categories outlined in the RMS Cyber Exposure Data Schema generally continued to be consistent with the range of coverage available on the market.

It is evident that the insurance industry is slowly taking steps towards standardization around specific coverage terms, but variations in coverage among products continues to be prevalent. RMS research shows that for the second year in a row, only two reviewed products offered the same mix of coverages. This lack of product standardization continues to pose a challenge for companies looking to navigate the cyber insurance market, making it difficult to conduct product comparisons or to find a product that matches their exposure.

While the existing types of cyber coverage available has remained broadly consistent, RMS has seen that more insurers are now offering network service liability, regulatory defense costs, and business interruption coverage. There has also been a decline in the number of insurers offering intellectual property (IP) theft, directors and officers insurance, and contingent business interruption coverage.

Several new affirmative cyber insurance products were launched in the market during 2016, with existing market players extending the range of products they offer, as well as new market entrants.

An increasing number of insurers now offer breach response services alongside their insurance offerings. Having an established incident response plan and team in advance of any data breach reduces the average breach costs by as much as $16 per record.[98]

Increasing Limits Being Purchased

Insurers are making more limit available, and insureds are purchasing cover to higher levels. Limits purchased are reported to have increased by more than 10 percent in the past year, with the average cyber insurance limit passing US$20 million for the first time in the third quarter of 2016.[99]

5.4 Cyber Risk Management Practices

A combination of factors, from the evolution and increasing prevalence of cyber risk, through to growing regulatory interest, is driving insurers to focus on improving cyber risk management practices.

Data Standards

RMS has worked with many of the cyber market leaders over the past year, and during that time we have seen a big improvement in the quality and completeness of data capture. RMS and the industry are continuing to emphasize data standard initiatives, but data continues to be a significant issue in the market. Issues include missing data attributes, and inconsistencies in recording and usage.

Underwriting and Risk Selection Processes

Underwriting and risk selection techniques continue to be highly varied across the market. Many companies are taking actuarial approaches to extrapolate from historical trends. Given the limited presence of large “tail” events, insurers are adding a significant load onto premiums to account for the large uncertainty leading to high prices. Many other companies are buying their experience in the market through consortiums or by taking small lines on bigger risks.

[97] Lloyd's Report.
[98] 2016 Cost of Data Breach Study, Ponemon Institute and IBM.
[99] Marsh, 2016.

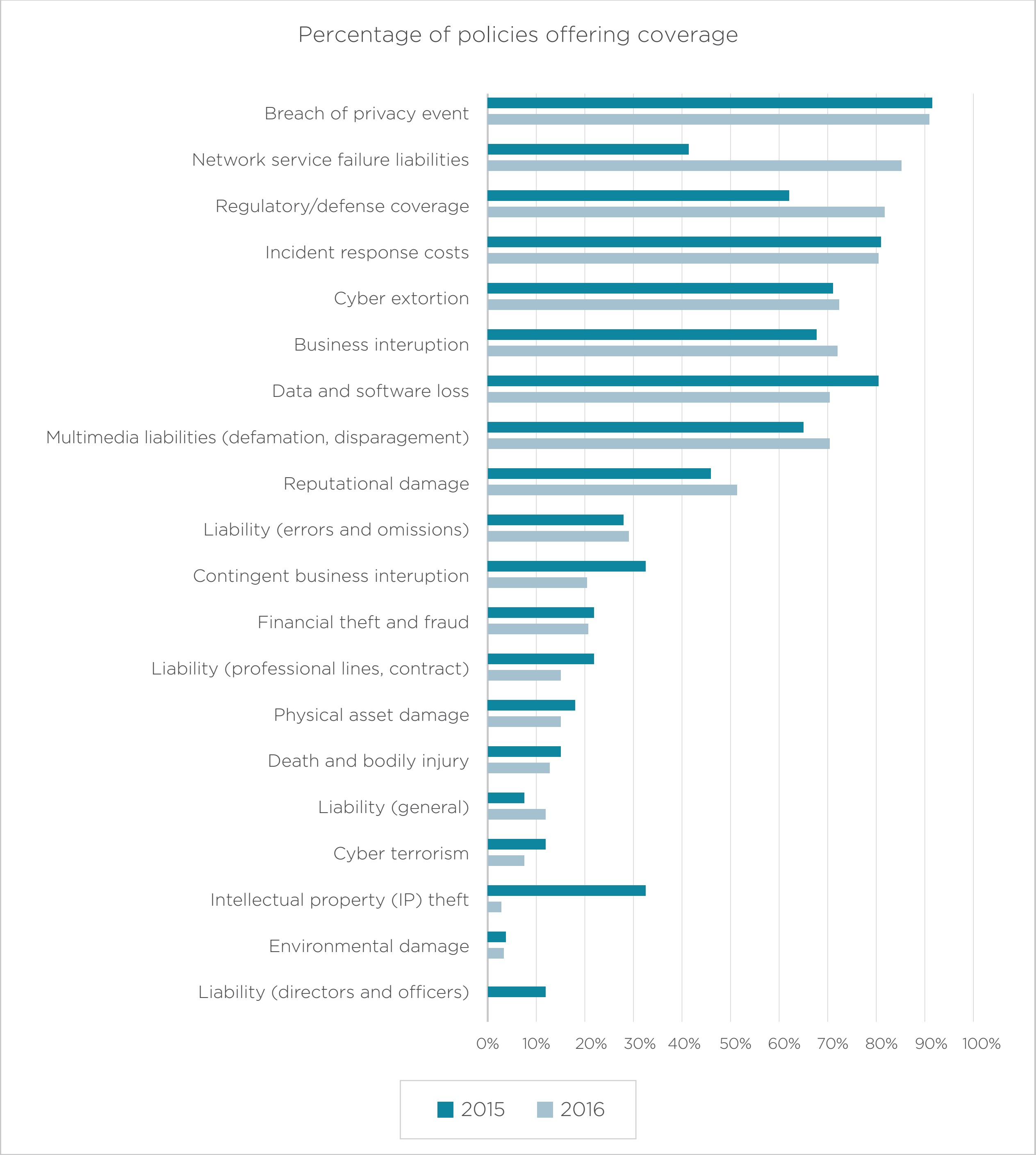


Figure 8. Change in proportion of cyber-affirmative policies on the market offering different types of coverage, comparing 26 products in 2015 to 50 products in 2016

The reinsurance market is expected to continue to grow as the primary market increases and insurers look to cede out a portion of the risk.

As the market continues to grow, and the risk landscape shifts, RMS expects to see continued price volatility.

An increasing trend has been toward companies leveraging Cyber Hygiene Scores as a method of quantifying the IT security maturity of a company. While undoubtedly a valuable tool, RMS would encourage organizations relying on these types of products to fully understand the underlying factors that go into these scores.

Accumulation Management

Managing the accumulations of risk in a cyber portfolio is one of the key challenges of growing a resilient cyber insurance portfolio. With the growth in cyber insurance and the corresponding increase in exposure, insurance companies are increasingly focused on managing their portfolio accumulation risk. Where cyber is added to other lines, this is often intended rather than "silent," but insurers are concerned that it may not be adequately priced and constrained by soft market conditions and limited historical data.

Exposure management is challenging for cyber, as correlations of cyber risk are complex. The more mature cyber insurers have developed cyber stress tests over the last few years to assess their probable maximum loss to cyber catastrophes. These scenarios vary in their sophistication, ranging from a simplistic approach through to the construction of complex systems with the assistance of outside expertise.

Newer cyber market entrants, without the historical experience to effectively price and manage cyber, have taken a conservative approach, with many using exposed limit as a measure of cyber catastrophe potential. But this is changing. Driven by regulatory pressures as well as the availability of commercial solutions such as RMS CAMS, more companies are adopting an integrated approach to establish their cyber risk appetite. For the first time, this is enabling a more consistent view of the risk and a more efficient use of capital across the market.

5.5 Insurance Regulations

Regulators have made significant steps to push the insurance industry towards better cyber risk management.

In the London market in 2016, Lloyd's has taken an active role by adding cyber scenarios to the mandatory reporting requirements of their managing agents.

The U.K. financial services regulator, the Prudential Regulatory Authority (PRA), has begun instigating regulatory approaches for insurers to improve their management of cyber risk, with a supervisory statement for consultation highlighting preferred best practices.

RMS was pleased to be able to contribute scenarios for the Lloyd's RDS requirement, and to provide inputs to the PRA's regulatory best-practice consultation.

The U.S. National Association of Insurance Commissioners (NAIC) has convened a task force for cybersecurity to create model laws that will provide minimum standards for insurance company security. The model laws will also spell out how insurance departments will monitor companies' cybersecurity practices. NAIC also commissioned a data call on types of policies and relative premium sizes being underwritten in the private market.

U.S. rating agencies, such as AM Best, are not yet requiring quantitative analysis of cyber risk in their assessments but have added questions about a company's preparedness and disaster plan for responding to cyber attacks as part of assessing an overall enterprise risk management framework.

5.6 The RMS Commitment to the Future

As the economy increasingly relies on the digital world to drive innovation and foster growth, the transfer of cyber risk will become more critical for businesses. This new type of risk transfer offers the insurance industry a huge growth opportunity – one which RMS is committed to helping insurers capitalize on.

The information in this report will provide you with the knowledge to better understand cyber risk and how it impacts the insurance market. It also helps demonstrate the great steps the industry is taking to provide coverage of this important peril to the economy.

The RMS commitment to the future of cyber security will continue, as the RMS cyber risk team works to develop and provide the analytical tools, newest technologies, and models the insurance industry needs to address emerging and evolving global cyber and terrorism threats. These will enable us to provide valuable insights into the evolving cyber landscape; identify the type of attacks to expect and how far-reaching they might be; anticipate the shifts in target preferences; and state the potential for cyber to trigger physical damage.

We look forward to a continued partnership with our clients in the development of a cyber insurance market that serves the enterprises at risk, and enables insurers to understand and diversify portfolio risk, while managing your capital adequacy.

References

Advisen, “Cyber Risk Trends: 2016 Year in Review.” 24 January 2017, Advisen Webinar.

Akamai, 2015. Quarterly Security Reports, Q3 2015.

Akamai, 2016. Quarterly Security Reports, Q3 2016.

Ali, M.A., Arief, B., Emms, M., van Moorsel, A., “Does The Online Card Payment Landscape Unwittingly Facilitate Fraud?”

Allianz, 2015, Cyber Risk 2015 – the next 10 years, Allianz Insights, Expert Risk Articles.

Arnold, M., “Tesco Bank ‘ignored warnings’ about cyber weakness.” Financial Times. November 13, 2016.

Ashok, I., “Tesco Bank under investigation for possibly ignoring warning of potential cyberattack.” International Business Times, November 28, 2016.

Assante, M. and R. Lee., “The Industrial Control System Cyber Kill Chain,” SANS Institute, October 2015.

AWS, 2017, AWS Global Infrastructure, Amazon Web Service, January 2017.

Bakir, N. (2007), A Brief Analysis of Threats and Vulnerabilities in the Maritime Domain, Create Research Archive, Los Angeles, USA: Create Homeland Security Center, pp.1-30.

Bateman, T., (2013), Police warning after drug traffickers' cyber-attackcyber attack - BBC News, [online] BBC News.

Beazley Breach Insights Report, January 2017.

Betterly, Richard S., The Betterly Report: Cyber/Privacy Insurance Market Survey, June 2016.

CCRS, 2015, Lloyd's Business Blackout Scenario, Cambridge Centre for Risk Studies and Lloyd’s, June 2015.

CCRS, 2016a, Cyber Insurance Exposure Data Schema Version 1.0, Cambridge Centre for Risk Studies and Risk Management Solutions, Inc. January 2016.

CCRS, 2016b, Managing Cyber Insurance Accumulation Risk, Cambridge Centre for Risk Studies and Risk Management Solutions, Inc. February 2016.

CCRS, 2016c, Integrated Infrastructure: Cyber Resiliency in Society, Cambridge Centre for Risk Studies and Lockheed Martin, January 2016.

CERT, “The Shadow Brokers auctions cyber weapons from Equation Group,” TLP: White, Version 1.5, August 26, 2016.

Chen, K., “Reversing and Exploiting an Apple Firmware Update.”

Collette, M. L. Olsen and J. Malewitz, “Ten years after a Texas City refinery blast killed 15 and rattled a community, workers keep dying,” Houston Chronicle, March 21, 2015.

ComputerWeekly, 2015, “Mandarin Oriental hack highlights security risk of legacy point of sale systems,” Warwick Ashford, March 6, 2015.

ComputerWeekly, 2016, “Data breach hits Hilton Worldwide hotel chain,” Warwick Ashford, November 25, 2016.

Constantin, L., “Cyberattack suspected in Ukraine power outage,” PC World, December 20, 2016.

Constantin, L., “Hackers found 47 new vulnerabilities in 23 IoT devices at DEF CON,” CSO, September 13, 2016.

Costin, A., Zaddach, J., Francillon, A., Balzarotti, D., “A Large-Scale Analysis of Security of Embedded Firmwares,” 23rd USENIX Security Symposium.

Cox, J.W., “MedStar Health turns away patients after likely ransomware cyberattack,” The Washington Post, March 29, 2016.

Cui, A., Costello, M., and S. J. Stolfo, “When Firmware Modifications Attack: A Case Study of Embedded Exploitation,” Columbia University.

CyberSecurity Ventures, 2016, CyberSecurity Market Report Q4 2016.

Department for Transport, (2015), “Maritime Growth Study: Keeping the UK competitive in a global market. Moving Britain Ahead,” [online] London: The Department for Transport, pp.5-12.

Digital Trends, 2015, “DoS Attacks hit Record Numbers in Q2 2015,” August 19, 2015.

DiRenzo, J., Goward, D. and Roberts, F., “The Little-known Challenge of Maritime Cyber Security,” Rutgers University, November 2015.

DLA Piper, “Data Protection Laws of the World,” 2017. Quarterly Security Reports, Q3, 2016.

Emm, D., Unuchek, R. and K. Kruglov, “Kaspersky Security Bulletin 2016: Review of the Year.”

Entous, A. and E. Nakashima, E., “FBI in agreement with CIA that Russia aimed to help Trump win White House,” Washington Post., December 16, 2016.

Gartner, 2015, “Value and Impact of IoT on Business,” Symposium/ITxpo, November 8-12, Barcelona, Spain.

FBI IC3, 2016, 2015 Internet Crime Report; Internet Crime Complaint Center, Federal Bureau of Investigation; US Bureau of Justice Assistance.

Finkle, J. and A. G. Tharakan, “Yahoo says one billion accounts exposed in newly discovered security breach,” Reuters, Technology News, December 15, 2016.

Forbes Tech, 2016, “Here’s How Much Businesses Worldwide Will Spend on Cybersecurity by 2020,” Market Intelligence, October 13, 2016.

Forbes, 2015, “J.P. Morgan, Bank of America, Citibank And Wells Fargo Spending $1.5 Billion To Battle Cyber Crime,” December 13, 2015.

Forbes, 2016, “Bank of America's Unlimited Cybersecurity Budget Sums Up Spending Plans In A War Against Hackers,” January 27, 2016.

Forrester, 2015, Sherman et al., Forrester Research Data Privacy Heat Map 2015, FTI Consulting, October 13, 2015.

Fox-Brewster, Thomas, “Shadow Brokers Give NSA Halloween Surprise With Leak Of Hacked Servers,” Forbes, October 31, 2016.

FTC, 2017, “FTC Charges D-Link Put Consumers’ Privacy at Risk Due to the Inadequate Security of Its Computer Routers and Cameras,” Federal Trade Commission, January 5, 2017.

Gartner, “Gartner Says Worldwide PC Shipments Declined 8.3 Percent in Fourth Quarter of 2015,” Gartner Newsroom, January 12, 2016.

GDPR Key Changes.

Greenberg, A., “Hackers Claim to Auction Data They Stole From NSA-Linked Spies,” Wired, August 15, 2016.

Grimes, Roger, A., 2012, “Why Internet crime goes unpunished,” InfoWorld, January 10, 2012.

Gupta, R., “The Panama Papers Signal A New Kind of Cyber Attack,” Fortune, July 28, 2016.

ICS-CERT, “Alert (IR-ALERT-H-16-056-01): Cyber-AttackCyber attack against Ukrainian Critical Infrastructure,” February 26, 2016.

InfoSEC Institute, “Panama Papers – How Hackers Breached the Mossack Fonseca Firm,” April 20, 2016.

Investor’s Business Daily News, 2016, “Security Freeze: Giants IBM, Cisco 'Squeeze' Palo Alto, Check Point,” 6/10/2016.

Karvets, D., “Feds: Hacker Disabled Offshore Oil Platforms’ Leak-Detection System,” March 18, 2009.

Kaspersky, “Energetic Bear – Crouching Yeti.”

Keane, J., “Apple Gains Notebook Market Share in 2015, Can’t Top HP and Lenovo,” Digital Trends, February 16, 2016

Klahr, R., Amili, S., Shah, J.N., Button, M., Wang, V., “Cyber Security Breachers Survey 2016,” HM Government, Ipsos MORI and University of Portsmouth, May 2016.

Kramek, J. (2013), “The critical infrastructure gap: U.S. Port Facilities and Cyber Vulnerabilities,” Washington D.C.: Brookings Institution, pp.1-35.

Lee, R. M. Assante and T. Conway, “German Steel Mill Cyber Attack,” SANS Industrial Control Systems, December 30, 2014.

Lee, R., Assante, M. and T Conway. “Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case,” TLP: White. Electricity Information Sharing and Analysis Center and SANS Industrial Control Systems, Washington D.C., March 18, 2016.

Lewis, James A., 2012, "Cybersecurity, Threats to Communications Networks, and Private-sector Responses," Testimony to House Committee on Energy and Commerce, Subcommittee on Communications and Technology, February 8, 2012, submission by Center for Strategic and International Studies.

Loukas, George, 2015, "Cyber-Physical Attacks: A Growing Invisible Threat," Butterworth-Heinemann, ISBN 978-0-12-801290-1.

Los Angeles Times, 2016, "Hollywood hospital pays $17,000 in bitcoin to hackers," FBI investigating, February 18, 2016.

Malwarebytes Lab, 2016, "Look Into Locky Ransomware," March 1, 2016.

Marsh, Global Insurance Market Index, Q3 2016.

Meserv, J. "Staged cyber attack reveals vulnerability in power grid," CNN, September 26, 2007.

Miller, C. (a), "Battery Firmware Hacking: Inside the innards of a Smart Battery," July 27, 2011.

Miller, C. (b), "Battery Firmware Hacking."

Millman, Rene, "How Vulnerable are Smart Buildings to Cyber Hacks?" IFSEC Global, March 29, 2016.

Moritz, S. and Womack, B., "Verizon Explores Lower Price or Even Exit From Yahoo Deal," Bloomberg Technology, December 15, 2016.

Murdock, J., "Turkey: Political hacktivist leaks 'citizen database' containing 50 million personal records," International Business Times, April 4, 2016.

NetworkWorld, 2015, "Which cloud providers had the best uptime last year?" Cloud providers are becoming more reliable, but some still had downtime issues," Jan 12, 2015.

NetworkWorld, 2016, "And the cloud provider with the best uptime in 2015 is…Amazon's cloud bests those of Microsoft and Google by this reliability test," Jan 7, 2016.

Newman, L.H., "What We Know About Friday's Massive East Coast Internet Outage," Wired, October 21, 2016.

Oregon State University, "Lithium Battery Safety and Handling Guide," Enterprise Risk Services, Environmental Health & Safety, December 2013.

ORF, 2016, Bundeswehr: Cyber security, the German way, Observer Research Foundation, Isabel Skierka, October 20, 2016.

Palmer, E., "Panama Papers: Simon Cowell and Jackie Chan among celebs named in Mossack Fonseca leak," International Business Times., April 7, 2016.

Paul, "Industrial Control Vendors Identified in Dragonfly Attack," The Security Ledger, July 4, 2014.

Paul, "Update: Let's Get Cyberphysical: Internet Attack shuts off the Heat in Finland," The Security Ledger, November 8, 2016.

Polityuk, P., Vukmanovic, O. and Jewkes, S., "Kiev power outage in December was cyber attack: Ukrenergo," Reuters, January 18, 2017.

Positive Technologies, "Security Trends & Vulnerabilities Review: Industrial Control Systems," 2016.

PwC, 2015, "Cyber insurance market set to reach $7.5 billion by 2020," September 15, 2015.

Rawlinson, K., "HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack," HP, July 29, 2014.

Response, S. S. (2014, 06 30), "Dragonfly: Western Energy Companies Under Sabotage Threat," Retrieved February 11, 2015, from Symantec.

Richman, D., "Cloud computing revenues jumped 25% in 2016, with strong growth ahead, researcher says," Geek Wire, January 4, 2017.

Rigzone, Worldwide Offshore Rig Utilization.

Riley, M. and Katz, A., "Swift Hack Probe Expands to Up to a Dozen Banks Beyond Bangladesh," Bloomberg Technology.

Ronda, R. A., "NPC: Victims of data leak may file suit," Philstar Global, January 8, 2017.

Rounela, S., "English summary about DDOS attacks," Valtia, 2016.

SC Media, 2016, "Finns have their heating systems knocked offline by a DDoS attack," November 9, 2016.

Security News Desk, "Securing critical infrastructure from virtual and physical threats," November 24, 2016.

Security, 2015, “47% of the World’s Credit Card Fraud Happens in the US,” June 1, 2015.

Starwood, 2016, Letter From Our President, January 22, 2016.

Statistica, 2017, IoT Number of Connected Devices Worldwide.

Strohm, C., “New York's Little Dam Sends Super-Sized Warning of Cyber-AttackCyber attacks,” Bloomberg Technology, March 20, 2016.

Sullivan. B., “Amazon, Microsoft, IBM And Google Growing 30 Percent Faster Than Next 20 Cloud Providers,” Silicon, August 1, 2016.

Symantec Security Response, “SWIFT attackers’ malware linked to more financial attacks,” Symantec Official Blog, May 26, 2016.

Temperton, J., “The Philippines election hack is 'freaking huge',” Wired, April 14, 2016.

The Guardian, 2016, “Tesco cyber-raid raises serious questions over UK banks’ security,” November 12, 2016.

The Hacker News, 2016, World’s largest 1 Tbps DDoS Attack launched from 152,000 hacked Smart Devices; Sept 27, 2016.

The Merkle, 2016; “Muni First Targeted By Ransomware, Now Faces Extortion Demand By Same Hackers,” November 29, 2016.

The Register, 2016, “National Cyber Security Centre to shift UK to 'active' defence: Cyber chief calls for 'offensive' weapons,” September 19, 2016.

U.S. Energy Information Administration (2016), “Commercial Buildings Energy Consumption Survey (CBECS) – 2012 CBECS Preliminary Results,” [Online].

United States District Court For the Central District of California February 2009 Grand Jury.

US Department of Energy, “Transforming the Nation’s Electricity System: The Second Installment of the Quadrennial Energy Review,” January 2017.

US Department of Homeland Security, National Cybersecurity and Communications Integration Center, ICS-CERT Year in Review, Industrial Control Systems Cyber Emergency Response Team, 2015.

Van der Walt, C., “Four Lessons to Learn From the SWIFT Hacks,” Info Security, August 3, 2016.

Williams, Katie, 2016, “Judges struggle with cyber crime punishment,” The Hill, 01/09/16.

Woolf, N., “DDoS attack that disrupted internet was largest of its kind in history, experts say,” The Guardian, October 26, 2016.

World Shipping Council, (2016a), “Global Trade | World Shipping Council,” [online] Worldshipping.org.

World Shipping Council, (2016b), “Ports | World Shipping Council,” [online] Worldshipping.org.

York, K., “Dyn Statement on 10/21/2016 DDoS Attack,” Dyn.

Zetter, K., (2014), “Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon,” New York, NY, USA: Crown Publishing Group.

Zetter, K., “Everything We Know About Ukraine’s Power Plant Hack,” Wired, January 20, 2016.

Zetter, K., “That Insane, $81M Bangladesh Bank Heist? Here’s What We Know,” Wired, May 17, 2016.

Zetter, K., “Why Hospitals Are the Perfect Targets for Ransomware,” Wired, March 30, 2016.

Acknowledgements

Risk Management Solutions, Inc; 2017; Cyber Risk Landscape Update; report prepared by RMS in collaboration with the Centre for Risk Studies, University of Cambridge.

Risk Management Solutions, Inc

Dr. Andrew Coburn, Senior Vice President

Dr. Christos Mitas, Vice President

Tom Harvey, Senior Product Manager

Peter Ulrich, Senior Vice President

Dr. Gordon Woo, Catastrophist

Simon Bennet, Content Manager

Carol Hackett, Senior Graphic Designer

Edwina Lister, Principal Consultant

Chris Vos, Senior Consulting Analyst

Hicham Boudali, Senior Cyber Risk Modeler

Malik Awan, Cyber Risk Modeler

Simon Arnold, Senior Manager

John Agorgianitis, Modeler

Gates Maus, Senior Consultant

Kate Grove, Consultant Analyst

Cambridge Centre for Risk Studies

Simon Ruffle, Director of Research and Innovation

Jennifer Copic, Research Associate

Kayla Strong, Research Assistant

Shahzeb Malik, Research Assistant

Éireann Leverett, Senior Risk Researcher

Dr Andrew Skelton, Research Associate

Tamara Evan, Coordinating Editor

Ali Rais-Shaghagi, Research Assistant

Professor Daniel Ralph, Academic Director

Dr. Michelle Tuveson, Executive Director

RMS solutions help insurers, financial markets, corporations, and public agencies evaluate and manage risks throughout the world, promoting resilient societies and a sustainable global economy.

Risk Management Solutions, Inc.
7575 Gateway Blvd.
Newark, CA 94560, USA
www.rms.com

Centre for
Risk Studies

UNIVERSITY OF
CAMBRIDGE
Judge Business School

RMS®