Cyber Risk Outlook 2018

Centre for **Risk Studies**

UNIVERSITY OF CAMBRIDGE
Judge Business School

RMS®

Cyber Risk Outlook 2018

TABLE OF CONTENTS

SECTION 1

The Evolving Cyber Risk Landscape

Cyber risk is a continuously evolving threat. For insurers of cyber liabilities, it represents a challenging risk to assess, with only a short catalog of historical experience available, and rapidly changing patterns of loss. Recent trends show how the threat is adapting in response to improved levels of security, and reinforce the key principles of cyber insurance risk management.

Trends in Cyber Risk

The RMS Cyber Loss Experience Database

RMS continues to monitor and compile incidents of cyber loss around the world. The RMS Cyber Loss Experience Database (CLED) is a compilation of all known loss events worldwide from cyber hacks, attacks, accidents, and malware occurring to private and public sector organizations in many countries of the world. Records include losses from data exfiltration, malware, financial theft, denial of service attacks, extortion, cyber-physical attacks, and network and cloud service failures. It contains details of several tens of thousands of cyber incidents, dating from 2007 to the present. It is constantly updated with new incidents and is a key resource for tracking the patterns and characteristics of cyber threat. It incorporates cyber claims data generously provided by several RMS client partners.

The RMS Cyber Loss Experience Database shows that cyber losses continue to occur in businesses of all sizes and activities, from a wide variety of causes. The primary causes of cyber loss are broadly consistent with those of previous years, with each loss process seeing new forms of events and techniques being applied, as profiled in the next section.

The internationalization of cyber threats

Cyber risk is becoming increasingly international. Cyber losses are now being reported in almost every country of the industrialized world. Our data gathering for the RMS Cyber Loss Experience Database is now cataloging loss events in over 150 countries, and monitoring large numbers of losses in the 12 principal countries that account for 70% of cyber risk. Figure 1 on page 8 maps the incidence of cyber loss across the world.

Individual malware attacks flow across international borders, and recent attacks have demonstrated the potential for global events of cyber contagion. The WannaCry ransomware in May 2017 (see case study) had reported infections in 150 countries. The NotPetya malware attack a month later (also profiled as a case study) had incidences in 65 countries, demonstrating the far-reaching consequences of a truly global and systemic cyber attack.[1]

Repeat attacks against global financial systems such as SWIFT, hit several countries at once, typically finding entry points into the network of trust through less secure users, with the potential to threaten global financial stability.[2]

The commoditization of cyber criminal tools, such as Ransomware-as-a-Service, Malware-as-a-Service and DDoS-for-Hire, have made the tools for global extortion and business disruption campaigns accessible to the less experienced. Proliferations of crypto-currencies and methods to anonymize their users are also fueling the spread of cyber crime.

[1] Chappel, 2018.
[2] Boey, 2017.

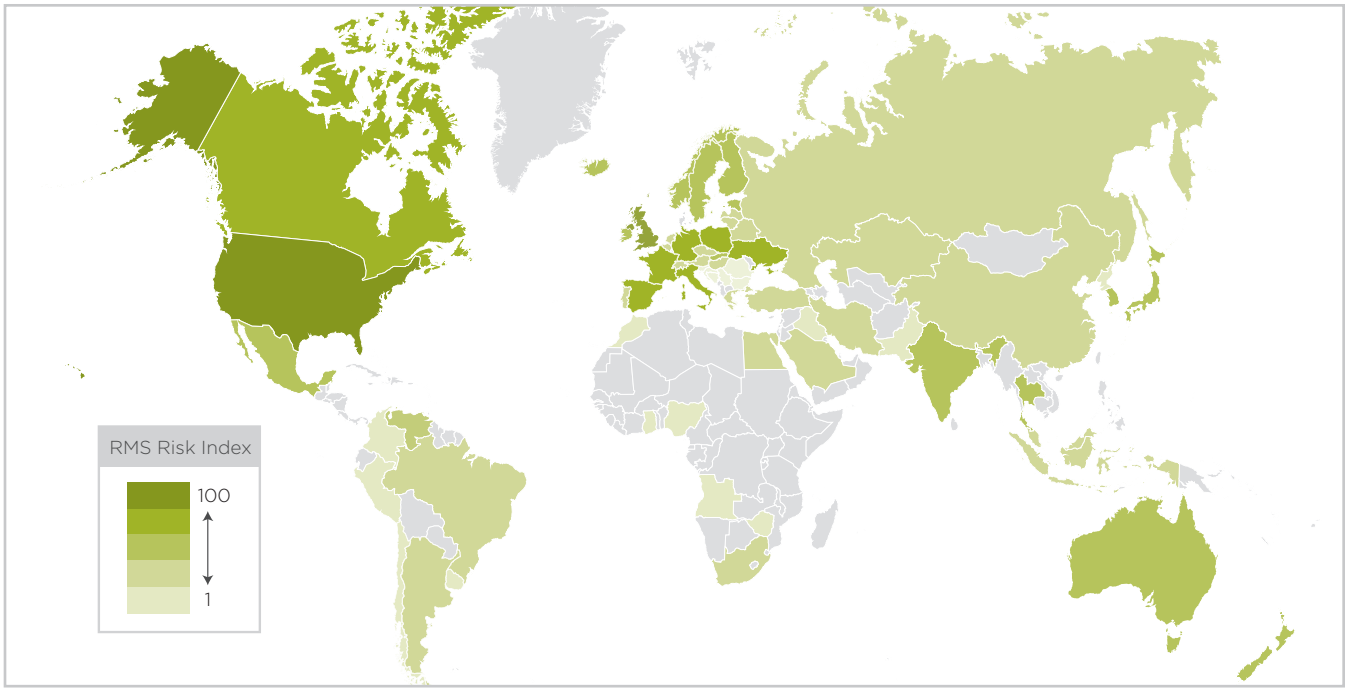


Figure 1: RMS World Map of Cyber Risk

Cyber politics

Cyber is increasingly political, with private sector companies being caught in the cross-fire of internal and geopolitical activities. Election results and social media campaigns are being distorted by cyber interference. Data exfiltrations, server take-downs, and destructive malware attacks on thousands of businesses are suspected as originating from external nation state cyber teams.

Nation States are leveraging disruptive cyber capabilities to achieve geopolitical aims. Attacks on Ukraine's physical and business infrastructure are attributed to a likely nation state.[3] These attacks, like NotPetya, have spilled out far beyond the borders of the conflict target area to cause business loss across many countries and companies. Attacks like these even raise the prospect of triggering a future kinetic war.[4]

Cyber continues to be at the forefront of geopolitical tensions. North Korean cyber actors claim they have exfiltrated the joint U.S. and South Korean Operational Plan 5015, top secret war plans for the invasion of North Korea.[5] increasing the tensions in the greatest nuclear standoff since the Cuban Missile Crisis.

[3] Greenberg (1), 2018.
[4] Oliphant and McGoogan, 2017.
[5] Jun and Youssef,, 2017.
[6] BBC (1), 2017.
[7] Viner, 2016.
[8] Solon, and Siddiqui, 2017.
[9] Solon, and Siddiqui, 2017.

Conflicts in the Middle East are also being fought out in the cyber theater, with data exfiltration and leaking of diplomatic correspondence fueling the disputes between UAE, Qatar, and Saudi Arabia.[6]

Each of these has the potential to provoke military response and wider scale escalation of cyber attacks with the potential for collateral impact on businesses throughout the world.

Deception and misinformation in cyber space

The Internet has increasingly become exploited by nation state intelligence agencies and those who seek to promote dissent. The disruption that new technologies has had on traditional media has resulted in the unintended consequences of amplifying misinformation.[7] Social media has become especially susceptible. During the U.S. presidential election of 2016, the three largest social media companies, Google, Facebook and Twitter, were exploited with both fake accounts and paid advertisements, spreading misinformation that could quickly go viral. This puts the business models of social media companies at risk, because of a dependency on user numbers which drives advertising revenue; incentivizing lax self-regulation.[8] Up to 120 Facebook pages with some 80,000 posts are thought to have been created by actors aligned with the Russian state. These posts are thought to have reached at least 29 million people who then exposed the content to 126 million others.[9] Attributed to Russian intelligence agencies, the misinformation campaign was conducted

in conjunction with the targeted data exfiltration of key campaign officials, the strategic leaking of information to public front organizations and the probing of the electoral infrastructure.[10] The same activities have been observed in elections throughout Western Europe.[11] Besides undermining democratic ideals, a trend in supporting opposing movements throughout the target states has become standard practice.[12] Stoking tensions between extremist groups is inherently irresponsible and has direct repercussions for the insurance industry if violence and destruction ensues.

Fighting Back

Although the cyber threat is increasing, efforts to combat attacks and improve security are also escalating. Security spend is reaching unprecedented levels, international cooperation among cyber protection organizations is improving, and there are initiatives to catch and deter cyber criminals.

Law enforcement's impact on cybercrime

Prosecution and conviction rates for cyber crimes are still low, relative to the incidence, with more than 4,000 ransomware attacks reportedly occurring per day.[13] However prosecutions for cyber offenses have increased rapidly and have reached record levels, after many years of criticism of law enforcement failing to address cyber crime adequately.

Arrests in the past year have included owners of malware cryptor services, malware purchasers, and virus writers. Several high-profile malware writers saw court and jail time, including the case of 'WannaCry hero' Marcus. Hutchins. Hutchins faces up to 40 years in prison for his role in creating and distributing the Kronos banking Trojan between 2014 and 2015.[14] 2017 also saw seven Russians arrested or indicted on U.S. cybercrime charges, a significant increase on previous years.

Encouraging progress is being made on the coordination of legal frameworks and cross-border cooperations to develop global control systems for deterring cybercrime.[15]

[10] Office of the Director of National Intelligence, 2017.
[11] BBC (2), 2017.
[12] Michel, 2017.
[13] Gammons, 2017.
[14] BBC (3), 2017.
[15] Council of Europe. International co-operation under the convention on Cybercrime, 2017.
[16] PYMNTS, 2017.
[17] Greenburg, 2017.
[18] Greenburg, 2017.
[19] Kshetri, and The Conversation, 2017.
[20] Popper and Ruiz, 2017.
[21] The Conversation, 2017.
[22] Ludwin, 2017.
[23] Kshetri and The Conversation, 2017.
[24] United States Department of the Treasury Financial Crimes Enforcement Network, 2017.
[25] Cimpanu, 2017.

Good guys go on the offensive

The take-down of the two biggest dark web marketplaces, AlphaBay (once known as the Amazon of the dark web) and Hansa Market represented a significant victory for the 'Good Guys' in 2017. Online black markets allow cyber criminals to buy cyber-attack tools such as malware and botnets, along with illegal firearms and drugs, using Bitcoin and Tor for transactions.[16] AlphaBay was reported to have daily postings of 300,000 listings of stolen credit cards and digital data thefts, along with drugs and other contraband items, generating up to $800,000 a day in revenue.[17]

Although other black markets are likely to take their place,[18] the disruption of revenue streams to cyber criminals has proven highly effective in reducing their capabilities.

Cryptocurrency for monetizing cybercrime

One of the main barriers for cyber criminals is the process of monetizing the proceeds of their heists. Monetizing the proceeds of a cyber attack often involves a complex money laundering process.[19] The increasing security measures implemented by financial institutions and the closure of black markets[20] changes the equation of the effort-to-reward ratio for cyber crime.

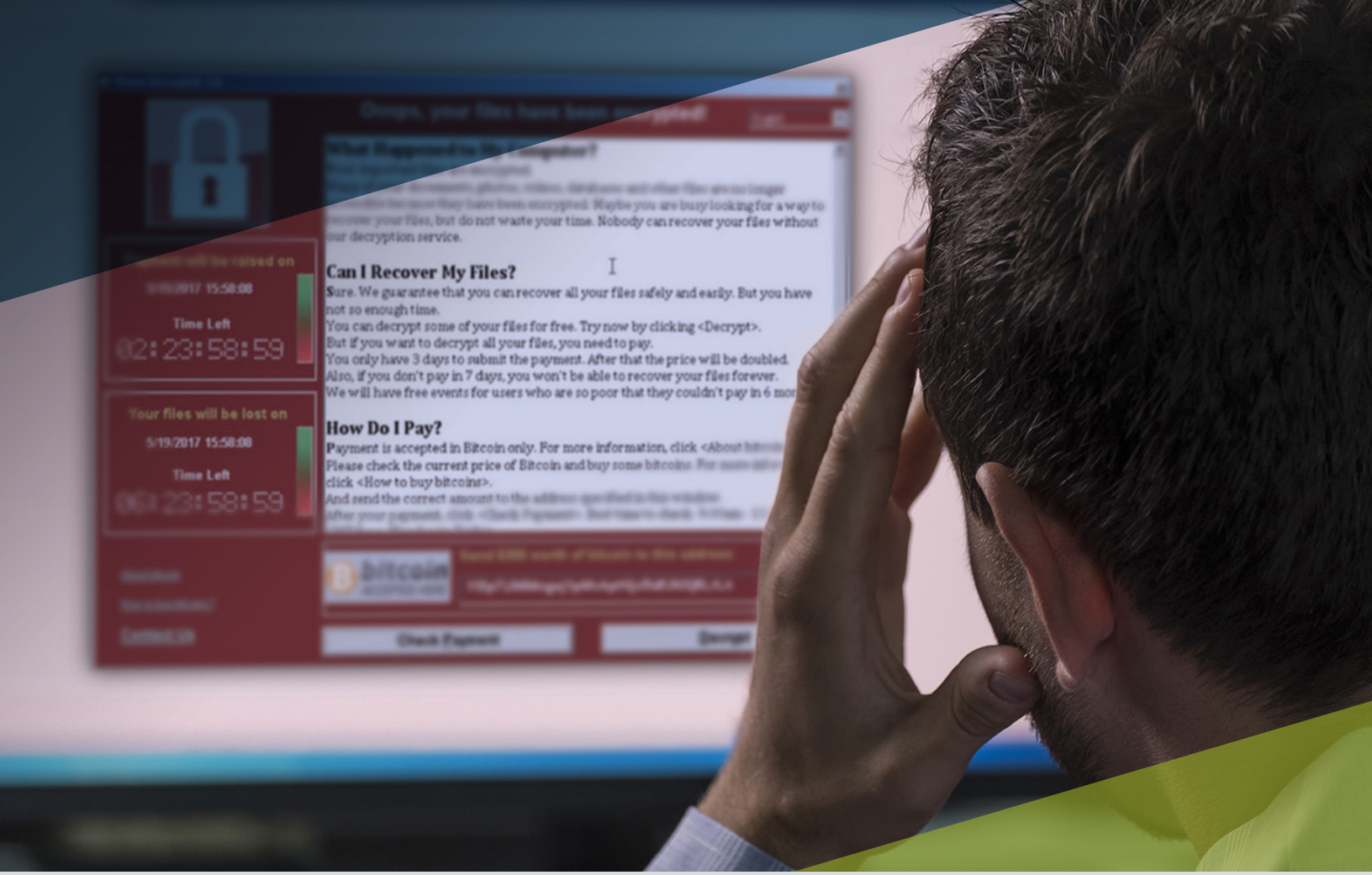
Cryptocurrency has helped hackers profit from cybercrime. Cyber extortion payments often use popular cryptocurrencies such as Bitcoin.[21] Some commentators have attributed the boom in BitCoin valuation to the demand from corporate risk managers to have a manageable supply of BitCoin in case they are held to ransom in the future by a cyber attack.

BitCoin is ultimately traceable, and most crypto-wallets now require ID verification to open an account.[22] Cryptocurrencies that are less traceable, such as Monero, are becoming more popular for use in the cyber black market. Often cyber criminals will launder their extortion payments through multiple cryptocurrency wallets, which makes it more difficult for the cyber security community to track the money trail.[23]

Efforts by U.S. Financial Crimes Enforcement Network (FinCen) resulted in the closure of BTC-e, one of the largest unregulated crypto-currency markets. The CEO of BTC-e was arrested for his part in a 300,000 BitCoin heist.[24] BTC-e handled around 5% of all Bitcoin transactions, but 95% of all ransomware extortion payments.[25]

Understanding the Enemy

Cyber threat actor groups continue to participate in an informal economy, often utilizing collaboration, black markets, and mercenary skills to achieve their aims. Nation state APTs, cyber criminals, and hacktivists draw on a common community of hackers and toolkits, making it



CASE STUDY

Counting the Cost of the ShadowBrokers Release of Cyber-Hacking Weaponry

In last year's Cyber Risk Landscape report we highlighted the theft and release of an NSA arsenal of cyber-hacking weapons by the ShadowBrokers group, and we profiled the tools they had made available to the criminal world.[26] We speculated about the potential impact of these tools in enabling future cyber losses.

We didn't have long to wait to find out. By May 2017, one of the ShadowBrokers' exploits, EternalBlue, had been incorporated as the core penetrating technique for the WannaCry ransomware that infected hundreds of thousands of computers across the world.[27] In June, both the EternalBlue and EternalRomance exploits provided additional vectors for the NotPetya malware to penetrate networks in a large number of major companies, once again taking advantage of unpatched machines for MS-17-010 and open SMB ports.[28]

Throughout the past year, the ShadowBrokers have continuously taunted United States and Western European governments and introduced a monthly subscription service, releasing several more cyber hacking weapons, which allegedly "can penetrate various computers and networks in ways that are not known to the public".[29]

The past year has seen several high profile cases of government employees and contractors indicted for violating national security and secrecy protocols, including stealing or leaking highly classified material. During investigation of the ShadowBrokers leak, the FBI arrested and charged Harold T. Martin III, a contractor for the NSA, with stealing 50 terabytes of classified material. It is alleged that he may have obtained as much as three-quarters of the cyber hacking weapons in the NSA's Tailored Access Operations, considered the United States premier cyber hacking unit.[30]

[26] Greenber (3), 2016.
[27] Johnson, 2017.
[28] Symantec, ISTR Ransomware 2017.
[29] Gibbs, 2017.
[30] Nakashima, 2017.

harder to identify and attribute attacks.[31] Much of the activity is occurring in countries beyond the reach of Western law enforcement.

Blurring lines between threat actors

State-sponsored groups have utilized new types of hacking techniques to further their geopolitical objectives. The suspected state involvement in the NotPetya and WannaCry ransomware attacks are evidence that state-sponsored groups are using new techniques which are global in scale and destructive by nature. This is potentially evidence that state-sponsored groups are using tools and techniques which are traditionally used by financially motivated cyber criminals.[32]

For sale hacking tools remain a threat

The use of common black market or generic open-sourced hacking tools by the spectrum of threat actors makes incident and attribution studies increasingly difficult for the cyber security community.[33] Lower skilled threat actors and cyber criminals continue to utilize resources and skills which can be purchased in the black market to increase their capabilities and covertness.

While there have been some high profile black market closures mentioned previously, the black economy continues to thrive due to the size and nature of the dark web.[34] Ransomware-as-a-service variants have fallen in 2017, but they are more customizable so they can be adapted to particular targets and thus more a threat to organizations.[35] Efforts by law enforcement have reduced the number of exploit kits-software which identifies flaws in networks in the black market. This has resulted in threat actors changing methods to gain access to a company's networks such as social engineering.[36]

Cyber Regulations

General Data Protection Regulation (GDPR) Act

The EU General Data Protection Regulation (GDPR) comes into force on May 25, 2018.[37] This regulation presents a major change for the consequences of breaches in the personal data of European citizens.

GDPR affects not only EU companies but extends to any company offering goods or services (even for free) to EU citizens or any monitoring of EU citizens. Important new obligations under GDPR include notification of breaches within 72 hours, increased requirements in relation to consent for sharing data, storing data, processing data and transferring data as well as the ability to revoke consent.[38]

GDPR aims to combat the growing trends in data exfiltration by standardizing data protection laws across Europe. This regulation builds upon the existing U.K. Data Protection Act 1998 with a new safeguards, requirements, and fines that offer protection to a growing international digital economy.

What information does the GDPR apply to?

GDPR protects 'personal data' which is defined more expansively than its 1998 predecessor:

> "Personal data" means any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.[39]

An important inclusion within this definition is 'Online identifiers', which includes things like IP addresses, to what is considered personal data. This change may create additional compliance obligations as many types of online 'cookies' collect 'personal information' under GDPR. This applies to both automated personal data and manual filing systems.

Additionally, 'Sensitive Personal Data,' such as genetic or biometric data, requires a high standard of protection and access restrictions. This concept will not be novel for many companies as similar standards were required by the U.K. Data Protection Act 1998.[40]

GDPR jurisdiction

Those companies currently subject to the U.K. Data Protection Act 1998 will also fall under GDPR. GDPR affects not only EU companies but extends to any company offering goods or services (even for free) to EU citizens or any monitoring of EU citizens. GDPR does not apply to processes covered by the law Enforcement Directive, processing for national security reasons, and household activities.[41]

U.S. companies are preparing to comply with GDPR in relation to offering goods and services to EU citizens. GDPR offers a significant departure to current U.S. data privacy regulations which focus around specific industries (none relate to computer related industries) and are drafted very broadly to require a 'reasonable' level of security.[42]

[31] Field, 2017.
[32] Accenture Security 2017 Cyber Threat Landscape, 2017.
[33] Kaspersky Lab, APT Trends Report Q2 2017.
[34] BBC (4), 2017.
[35] Symantec, Internet Security Threat Report 2017.
[36] Europol, Internet Organised Crime Threat Assessment, 2017.
[37] ICO, Guide to the General Data Protection Regulation, 2017.
[38] ICO, Guide to the General Data Protection Regulation, 2017.
[39] Gabel and Hickman, Key Definitions-Unlocking the EU General Data Protection Regulation.
[40] European Commission, 2017.
[41] ICO, Guide to the General Data Protection Regulation. 2017.
[42] ICO, Guide to the General Data Protection Regulation, 2017.

GDPR aims to combat the growing trends in data exfiltration by standardizing data protection laws across Europe.

The accountability principle

The accountability principle of the GDPR requires companies to confirm how they comply with the principles of the GDPR which promote transparency and strict governance. Companies are required to implement 'technical and organizational' measures to minimize the risk of breach that include: maintaining relevant documentation, data minimization, pseudonymisation, transparency, allowing individuals to monitor processing and creating and improving security features on an ongoing basis among others.[43]

If data within an organization is not processed correctly, no data protection officer has been assigned, or any of the above measures are not met in concordance with the accountability principle, monetary fines will ensue.[44]

Breach notification

GDPR introduces the obligation to report specified types of data breaches to relevant authorities, and in some cases, to the individuals whose data was affected. Authority notification is required when a breach is likely to result in a 'risk to the rights and freedoms of individuals' i.e. reputation damage, monetary loss, or social disadvantage. When this risk is high, the affected individuals need to be notified.

Fines will be applied to companies who fail to properly notify authorities or individuals when required to which can sum up to 10 million Euros or 2 per cent of company global turnover.[45]

Restrictions on the transfer of data

Increased restrictions have been put on the transfer of personal data outside countries in the European Union. Companies wishing to receive transfers of personal data outside of the EU are required to prove the standardized safeguards for the data as outlined by the GDPR. This includes the transfer of personal data out of the EU in response to a third country's legal requirement.

As with most of the other aspects of the GDPR, failure to comply with these restrictions will result in hefty fines.

The impact of regulation on the cost of data breach

Countries with the strictest regulations make data breaches most expensive, with costs in heavily regulated countries being over twice per record than those in countries with limited data regulation. Figure 2 shows that nearly all the major markets for cyber insurance are now under heavy or robust regulatory regimes, and emerging markets are increasingly regulated.

GDPR regulations will increase the costs of data breaches for companies in Europe and doing business with its citizens. According the PCI Security Standards Council, if data breaches were to continue at the levels of 2015, fines paid to the European regulator could see as much as 'a 90-fold increase, from £1.4bn in 2015 to £122bn [...] based on the maximum fine of 4% of global turnover.'[46]

GDPR & cyber insurance

The increased obligations under GDPR and increased cost of suffering a cyber attack are expected to drive a significant increase in demand for cyber insurance from European countries and for companies who service European markets.

[43] ICO, Guide to the General Data Protection Regulation., 2017.
[44] Burgess, 2017.
[45] ICO, Guide to the General Data Protection Regulation, 2017.
[46] Ashford, 2016.

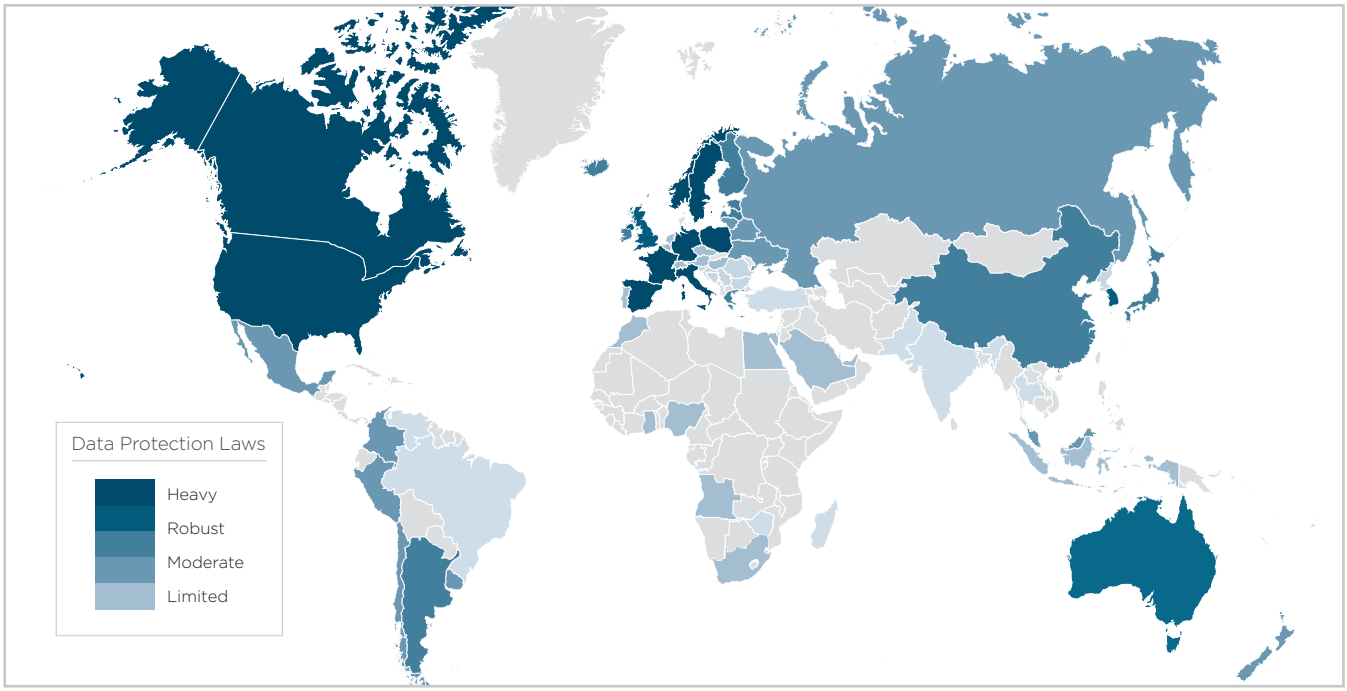


Figure 2: World Map of Data Privacy Regulation (Source: DLA Piper)

SECTION 2

Trends in Cyber Loss Processes

Data Exfiltration

Data exfiltration continues to be the predominant cause of insured losses, with individual companies suffering significant data breaches. While the frequency of smaller data breaches has reduced in United States, incidences are increasing in most other countries. The sizes of successful breaches are increasing, and breaches are becoming more costly in many jurisdictions. There has been a significant shift towards large scale data breaches occurring outside of the U.S., particularly in Asia.

Record-breaking size of data exfiltration events

The past year has seen some of the most severe data breaches occurring in Asia. In May 2017, one of the largest data breaches ever recorded occurred in China, where 2 billion phone records were stolen from the popular Chinese call-blocking tool DU Caller.[47] The U.S. has still suffered from large scale and high-profile data breaches. Equifax, the U.S. based credit reporting agency, was subjected to a high-profile data breach, which resulted in an estimated 143 million U.S. customers personal and financial information stolen (see case study).[48] Yahoo's parent company Verizon, which officially acquired Yahoo in June 2017, announced in a statement that the 2013 data breach has resulted in all 3 billion email accounts being compromised.[49] Evidence that the data is being sold on the black market by an Eastern European hacking collective,[50] may result in an increase in email fraud and account takeovers. The disclosure of further data loss and evidence of fraudulent use of this data could increase financial liabilities in the future.

Decreasing incidence rates of data breaches

Figure 3 shows how data exfiltration incidence in U.S. increased rapidly during the period 2009 to 2014. Events since 2014 have continued to occur at a similar incidence rate, with variation year-on-year, but have not continued the rapid rate of increase of the previous five years, and show signs of declining.

This correlates with major increases in investment in cyber security across many of the companies at risk, and a focus on prevention and awareness in staff that is reducing the number of accidental data loss incidents and smaller breaches. It may also reflect the decreasing 'return on effort' for hackers as black market prices fall for stolen data.

Attackers, finding it harder to steal data, are finding easier ways to make money, including ransomware and extortion. Hackers are making less money out of data exfiltration, as the black market sale price of stolen records from data breaches has fallen with the abundant supply of stolen personal data now being offered for sale.[51]

Cyber attackers may instead be turning to less secure targets in other countries, and to other forms of cyber crime, such as extortion. Data exfiltration remains a very lucrative form of crime for the more professional cyber criminals, who focus on larger scales of thefts from their targets. The median size of successful data exfiltration attacks has continued to increase over time.

Increasing magnitude of global large-scale data breaches

While the overall frequency of data breaches has fallen, the severity of data incidents has grown. The number of records stolen per breach of P3 and higher (greater than 1000 records) has tripled over the past three years. Severity of large scale data breaches have generally increased over

[47] Sputnik News, 2017.
[48] Riley (1) et al., 2017.
[49] Perloth, 2017.
[50] Kan, 2016.
[51] Wolff, 2017.

Company	Country	Number of Records	Date	Severity
Du Group DBA Du Caller	China	2 Billion	2017	P8
River City Media	United States	1.37 Billion	2017	P8
Netease, Inc.	China	1,22 Billion	2017	P8
Emailcar	China	268 Million	01/01/2017	P8
Deep Root Analytics	United States	200 Million	2017	P8
Equifax Inc.	United States	143 Million	2017	P8
National Social Assistance Programme (NSAP), Government of India	India	135 Million	01/11/2016	P8
Tencent Holdings Limited DBA	China	130 Million	2017	P8
Reliance Jio Infocomm Ltd	India	120 Million	2017	P8
Youku	China	91 Million	2017	P7
Edmodo	United States	77 Million	2017	P7
Jigsaw Holdings (Pty) Ltd	South Africa	60 Million	2017	P7
Uber Technologies, Inc.	United States	57 Million	13/10/2016	P7
Republic of The Philippines Commission On Elections	Philippines	55 Million	11/01/2017	P7
Altel Communications	Unknown	50 Million	01/01/2014	P7
Dun & Bradstreet	United States	33 Million	2017	P7
Yahoo Inc.	UK	32 Million	2017	P7
Sina Corporation Dba	China	31 Million	2017	P7
Unitebook Smart Microblogging	China	30 Million	01/01/2017	P7

Table 1: Selected Recent Large Data Breaches

time, with the data being skewed by a few extremely large data loss events. Professional hackers are becoming more sophisticated in their approaches to data exfiltration.

Companies are holding more data

"Data is the new oil": Companies are harvesting data from their customers and mining it for insights in ever increasing volumes. The total amount of business data being stored is estimated to be doubling every 12 to 18 months. This means that the potential for data exfiltration of sensitive information is increasing rapidly, in terms of the amount of data that could potentially be compromised. The size of datasets, and the aspects of people's lives and behaviors that could potentially be exfiltrated, is a constantly increasing trend. The magnitude of data exfiltration losses can be expected to increase in the future.

Data breaches by business sector

Other the past eight years, data exfiltration incidences have been most frequent in organizations involved in public sector, education and healthcare. Certain types of data are worth more than others and personal health records (PHI) and personal identifiable information (PII) are worth more on the black market, relative to credit cards and other personal finance records.[52] The fact that these organizations hold more of these types of data, combined with potentially lower security standards, make these sectors more attractive targets.

Recent incidence rates of data loss for different business sectors remain broadly consistent with previous patterns. Data breach rates have increased in IT services, manufacturing sectors, and have doubled in retail.[53] An emerging recent target for data breaches has been offshore legal firms in tax havens, with a string of incidences of whistleblower tax filings, including another exfiltration, following on from the Panama Papers in 2016, of the so-called 'Paradise Papers' where 1.4TB of sensitive financial and legal information about clients of offshore legal firm Appelby was leaked to the public.[54]

[52] Finkle (1), 2014.
[53] Gemalto, 2014.
[54] Finkel, 2014.

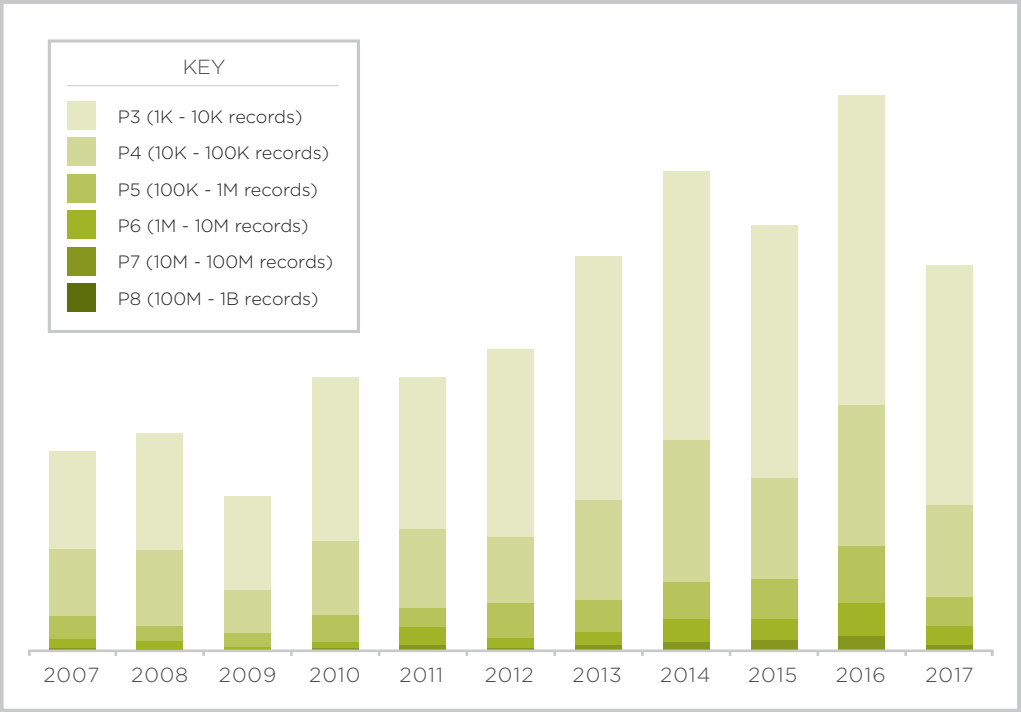


Figure 3: Number of U.S. data exfiltration events (greater than 1000 records) over time. (Source: RMS Cyber Loss Experience Database)

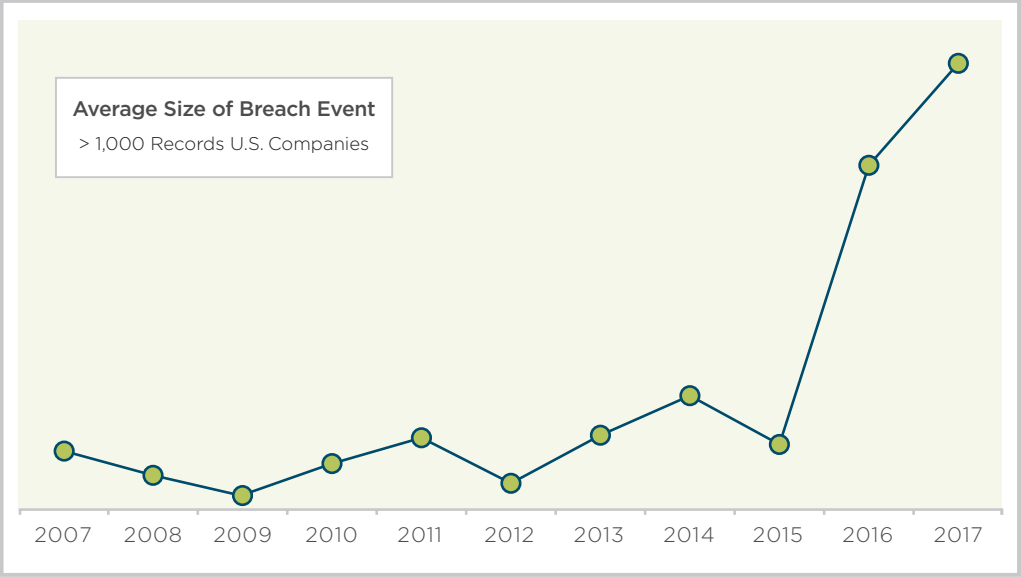


Figure 4: Increasing size of U.S. data exfiltration events over time

Cost trends in data breaches

There has been an increasing trend in the average cost per record of data loss for incidents over 100,000 records.[55] This is attributed to the regulatory costs, escalating legal complexity and growing cost of compensation. Costs of data exfiltration attacks vary significantly between countries,[56] and increases in incident rates in countries with lower compensation costs have resulted in average costs worldwide apparently decreasing, but costs are generally increasing over time in many countries, as regulations tighten. The highest cost per record remains in the U.S. due to the increasing notification costs.[57] Average costs per record are reported to have decreased recently in Western Europe, particularly in the U.K., Austria and Denmark. Costs of data breaches are expected to increase in Europe with the implementation of GDPR. Costs in other countries are likely to rise, such as Asia-Pacific countries as they move towards tougher data breach laws including the new Cyber Security Laws introduced in China.[58]

Cyber insurers are increasingly moving their larger insured accounts to 'managed response' relationships, where they control the claim costs when they occur, and this is managing to reduce the cost of data breaches in those client accounts.

The business impact of a data breach has reduced, with some of the consequences having diminished, such as churn (number of customers lost due to a data breach) which has reduced in Western Europe.

Data loss mainly caused by external outsiders

The main cause of data breaches is attacks from malicious outsiders rather than accidental losses or 'whistle-blower' leaks from internal employees. While external actors remain the most pertinent threat, internal threats are still a concern to most corporations. The escalating use of third-parties such as sub-contractors is responsible for a growing proportion of loss events. Contractor-breaches result from bushinesses being granted, access to vital systems within a company's network.[59] One of the higher profile 'contractor-breaches' was from National Security Agency (NSA), which demands the highest level of vetting for employees.[60]

Accidental data loss remains significant

Unintended disclosure of data remains a significant loss process.[61] While the forensic costs are often less when data is unintentionally disclosed, cost to insurers can still be substantial due to the high notification and credit monitoring costs.[62]

Contagious Malware

Malware that can replicate and spread through networks of communication has been one of the longest-standing cyber threats. Recent events have shown that malware remains a potent trigger for loss, even in companies with high standards of security. Most significantly WannaCry and NotPetya demonstrated that contagious malware has the ability to scale and to cause systemic loss to thousands of companies.

WannaCry and NotPetya

WannaCry and NotPetya demonstrated the disruptive capabilities of viruses, worms, and trojan horses to spread through populations of organizations, see case studies. Many of these infections affected organizations of different geographical location, industry and size.[63]

Cyber contagion and cyber physical

These contagious cyber attacks have had significant effects on physical operating environments. They have affected critical infrastructure and public services, imperilling public safety. Previous extortion attacks, for example on hospitals remained compartmentalized to an individual hospital or specific department. The WannaCry event threatened public safety across large numbers of hospitals. WannaCry affected 81 out of 236 National Healthcare System Trusts throughout United Kingdom, and 603 primary care providers. The disruption locked up important medical equipment such as MRI scanners, and caused the diversion of patients, the canceling of appointments and surgeries, and forced a reversion to manual record keeping.[64]

WannaCry affected over 300,000 machines, many critical to national infrastructure such as power stations and transportation hubs, localized and international banking systems, global manufacturing networks and logistics and delivery centers.[65]

[55] RMS CLED Database.
[56] Wolfram et al., 2017.
[57] Wolfram et al., 2017.
[58] JLT, 2017.
[59] Gogan, 2017.
[60] Gerstein, 2017.
[61] Beazley (1), 2017.
[62] Beazley (1), 2017.
[63] Kaspersky, KSN Report: Ransomware in 2016-2017, 2017.
[64] Comptroller and Auditor General, 2017.
[65] Graham, 2017.

CASE STUDY – JULY 2017

Equifax Data Breach

In July 2017, credit reporting agency Equifax were the victims of a significant data breach which resulted in an estimated 143 million U.S. records containing customer information being stolen by hackers.[66] This included social security numbers, dates of birth, and the credit card details of over 209,000 Americans.[67] The breach also impacted other countries, with Equifax admitting that 15.2 million records of British citizens and 8000 Canadians were stolen in the breach.[68] There was over a month's delay in disclosing the data breach. Senior executives were criticized for selling shares in the days before the breach was announced to the public.[69]

The intruders managed to gain access to the records using a weakness in a popular back-end website application. The vulnerability was made public in March 2017, but Equifax were slow to fix the bug in their networks, highlighting the importance of maintaining the latest patches.[70]

The Equifax hack had the markings of a sophisticated cyber attack, leading to speculation about attribution, with some in the cyber security community blaming Chinese-backed groups due to similarities with other attacks such as the U.S. Office of Personnel hack in 2017.[71]

The potential for the stolen Equifax data to be used in financial fraud has caused U.S. banks such as Citi Group and Wells Fargo to step up anti-fraud controls.[72]

[66] Turner, 2017.
[67] Jolly, 2017.
[68] McCrank (1), 2017.
[69] McCrank (2), 2017.
[70] Shepardson, 2017.
[71] Riley (2), 2017.
[72] Gray, 2017.

CASE STUDY – MAY 2017

WannaCry Malware Attack

WannaCryptor ransomware spread via file-sharing network protocols on computers using outdated Windows XP and v8 OS. It resulted in 300,000 infections of computers across 150 countries. WannaCry used a NSA exploit codenamed EternalBlue (made available the previous August by ShadowBrokers). It predominantly affected personal users, public sector organizations, and SME-scale companies, affecting unpatched boxes and equipment on dedicated older operating systems. Several dozens of large companies also reported disruption and losses from infections of their systems. Of the roughly 400 million actively-used Windows computers running version 8 or earlier operating system, approximately 0.1 percent were infected. The great majority of the Windows computers running version 8 or earlier were protected by a Microsoft patch MS17-010 issued two months earlier, in March 2017.

The event highlighted the issue of equipment software latency, i.e. that machines and sub-networks within organizations may rely on specific versions of operating system that render them vulnerable. In these cases, although the majority of systems within organizations ran more up-to-date operating systems, certain departments and activities were maintaining the older versions that contained the vulnerability. Machines such as medical MRI scanners and X-Ray machines that were certified on XP and v8 and maintained on those operating systems, were among those that were crippled by the attack.[73] Businesses reported substantial losses from lock-outs of systems around the world, such as manufacturing processes, dispatch and ordering systems, gas pump payment applications, and telephone exchange equipment. We estimate the direct costs and indirect business disruption losses from WannaCry to be around half a billion dollars.

If the WannaCry malware was created to generate ransom payments then it was remarkably unsuccessful. The BitCoin accounts that it requested payments into received less than $150,000 in payments and may not have been claimed by the criminals. No company that paid a ransom got its data back. The motivation was more likely to sabotage some of the affected companies, rather than generate funds for the hackers. It is possible that the widespread economic disruption was collateral damage to mask a targeted destructive attack.

The propagation of WannaCry was stopped after four days by a researcher finding a kill-switch within the software. Otherwise the infection could have spread to many more machines and had a more severe impact. RMS counterfactual analysis suggests that if the kill-switch had not been triggered, and if the attack had occurred prior to the issuing of the MS17-010 patch for Windows 8, the infection rates and losses could have been an order of magnitude higher, perhaps reaching $3 to $6 billion.[74]

[73] National Audit Office 2017.
[74] Woo, Counterfactual Analysis of WannaCry Malware Attack. RMS Webinar Nov 2017.

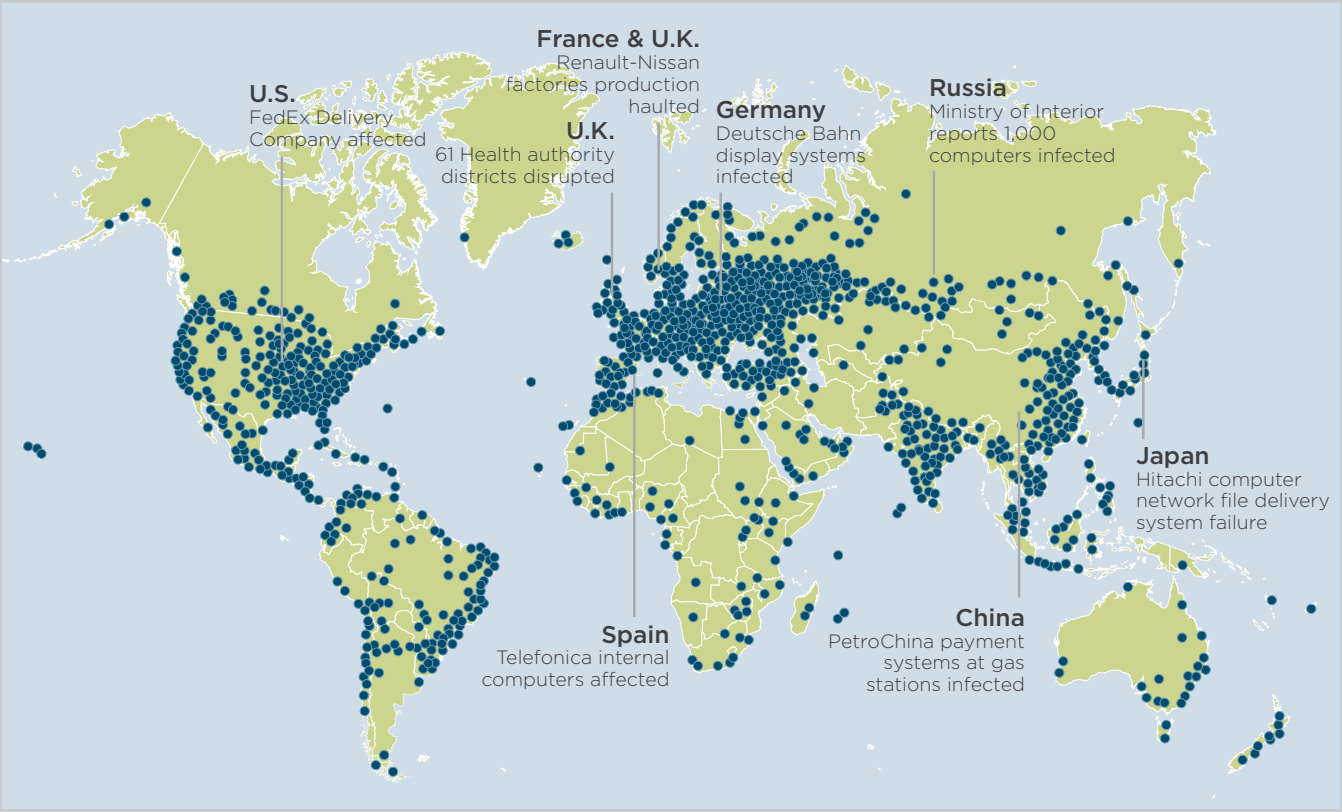


Figure 5: WannaCry infections across the world and example business impacts, May 2017 (Source: intel.malwaretech.com)

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 one of the most pressing concerns for cyber security specialists. Attempts to extort major companies using cyber attacks have grown in frequency, scope and ambition. Many companies have developed contingencies for ransomware attacks in the future. Some commentators have suggested that companies stockpiling BitCoin in case of extortion attacks may have fueled the recent surges in BitCoin demand.

Estimates of ransomware extorted in 2017 exceed five billion dollars, a 15-fold increase over the previous two years.[75] Ransomware has historically afflicted personal computers and small and medium sized enterprises, but recent developments have seen large multinational corporations affected, with security companies seeing some 42 percent of all ransomware infections in the first half of 2017 targeting organizations in an interconnected and networked environment.[76]

Cyber extortion from large companies

Ransomware is not the only method of cyber attacks that has been used for extortion. There have been several high profile instances where data exfiltration attacks have resulted in ransom demands. In the July 2017 HBO breach, hackers threatened to release upcoming episodes of hit shows if a price was not met.[77] Another targeted attack, utilizing the ransomware Erebus against a South Korean web hosting company, Nayana, in which all of its servers were encrypted, resulted in a $1 M ransom being paid and the bankruptcy of the company.[78] Increasingly, the interconnectedness of things has been exploited by cyber criminals. The past year has seen a rise in targeted attempts to extort major multinational corporations, often compromising thousands of machines across these organizations.

[75] Morgan, 2017.
[76] Symantec, 2017.
[77] Gibbs, 2017.
[78] BBC (5), 2017.

REUTERS/Phil Noble

CASE STUDY – JUNE 2017

NotPetya Malware Attack

On June 27, 2017, a virus that became known as 'NotPetya', to distinguish it from its antecedent versions of the 'Petya' virus, caused over 2,000 infections in organizations across 65 countries. Although disguised as ransomware, it was actually a destructive disk wiper. It was hidden in the software update mechanism of M.E.Doc (U.K.), a Ukrainian tax preparation program which is an industry standard for tax filing in Ukraine. As a result, 80% of the infections occurred in Russia and Ukraine, where more than 80 organizations initially reported being affected, including the National Bank of Ukraine, Kiev's Boryspil International airport, and the radiation monitoring system at Ukraine's Chernobyl Nuclear Power Plant.[79] 9% of the infections occurred in Germany, but also reached France, Italy, Poland, the United Kingdom, and the United States. NotPetya utilized the exploit of EternalBlue, similarly to WannaCry, but enhanced it with multiple techniques to propagate throughout internal networks, including harvesting passwords, and running PSExec code on other local computers. The data encryption payload was irreversible, and the ransom demand was a hoax.

A number of large multinational organizations reported significant costs and losses from business disruption. Maersk, one of the largest shipping operations, reported that infections of the NotPetya virus had caused it to suspend operations in parts of its organization, causing congestion in at the 76 ports it operates worldwide, and resulting in business losses of up to $300 million in the initial quarter after the attack. FedEx suspended its share dealings on the New York stock exchange after reporting $300 million costs from its TNT Express division in lost business and clean-up costs.[80] Pharmaceutical giant Merck reported losses of $300 million a quarter for two successive quarters, from lost sales resulting from production shut-downs and failure of internal IT systems.[81] French construction materials company Saint Gobain reported a business impact of $393 million from the virus impacting its systems. Over a dozen multinational companies announced losses to quarterly earnings following the attack,[82] and there are reports of disruption to more than 30 international companies, and many Ukrainian national organizations.

In total we estimate that the NotPetya malware caused losses of around $2.5 to $3 billion.

[79] ZDNet, 2017.
[80] Register, 2017.
[81] TechRepublic, 2017.
[82] Cybereason, 2017.

Financial Theft

Financial theft has continued to be a major source of cyber attacks and cyber-enabled fraud. Compromising networks of trust to misappropriate financial transfers remains a significant threat, despite major efforts to improve security. Cyber attacks on customer systems continue to be a major cause of loss.

Customer side financial theft

Cyber attacks on the customer side of financial institutions continue to dominate, with online fraud plaguing the e-commerce, airline and retail industries.[83] Physical fraud on ATM's and point-of-sale (POS) terminals also remain a key threat.

An emerging threat is complex attacks on the financial institutions and their company's internal systems (back-end systems) and key counterparty networks of trust, involving sophisticated threat actors. This is evident from the Bangladeshi and Taiwanese SWIFT attacks (see case study) and the Polish financial regulator attack in early 2017.[84] which are both linked to the North Korean hacking group Lazarus.[85] Cyber attacks for financial theft and fraud are still a more significant element of cyber loss than ransomware, with 2.5 times the annual detection of cyber attacks involving financial malware.[86]

Muted EMV implementation in the U.S.

The U.S. remains a key location for credit card fraud, accounting for 24 percent of total credit card use, but 47 percent of global credit card fraud.[87] In 2016, Visa, Mastercard, and Europay credit card companies introduced new rules in the U.S. requiring retailers to upgrade their point-of-sale terminals to accept EMV-chip enabled cards. These rules are accompanied by a EMV fraud liability shift requiring retailers to bear the costs for card-present and other point-of-sale (POS) fraudulent card transactions if merchants did not upgrade their systems.

Implementation of the EMV post-liability shift has been slow, with only 52% of U.S. card-accepting merchants upgraded to EMV technology[88] compared with 84.9% of European vendors.[89] Sluggish rollout of EMV in the U.S. has been attributed to the cost of implementing EMV technology, regulatory confusion, and lack of awareness of the risk of cyber-fraud, particularly for small-medium sized enterprises.[90] U.S. continues to see many types of card-present and point-of-sale fraud, including cashing counterfeit EU payment cards.[91]

Digital currency and financial theft

Cyber attacks have increased against third-party cryptocurrency wallets to steal digital currency, exploiting weaknesses in factor security verification in wallets. Reports of financial theft from wallets is wide-spread, with at least 36 major heists on cryptocurrency exchanges since 2011.[92] In July 2017, three separate cyber attacks occurred across cryptocurrency platforms, including 153,000 Ethereum worth $30 million stolen from the widely used Parity Wallet.[93] Cyber attacks in cryptocurrency markets undermines attempts to validate digital currency, and impedes the introduction of insurance against digital financial theft.[94]

Financial transaction theft remains key threat

A major source of large loss from cyber-attacks is the emergence of cyber criminals targeting financial institutions by penetrating banks internal systems, including inter-bank transaction networks. The Lazarus SWIFT financial theft in early 2016 was one of the most audacious cyber bank heists of its kind, which could have resulted in a theft of more than a billion dollars.[95] The 2016 campaign successfully stole $81 million, with dozens of banks and central banks compromised including the U.S. Federal Reserve. The hackers hit the SWIFT network by repeatedly using specially-crafted software which allowed them to gather information on standard practices and send fraudulent requests for funds across the network.

In response to the cyber-attack, SWIFT in 2017 announced an updated security protocol.[96] The vulnerability was not in the SWIFT technology itself, but a weakness in the security of some of the member banks, so SWIFT introduced the Customer Security Control policy which gives advice on how to segregate SWIFT and critical systems from a member bank's general framework. Further security measures include a new real-time payment controls service to reinforce existing fraud controls and cyber-crime prevention.

The security update in 2017 has become more pertinent because of a further attack on the SWIFT network involving Taiwanese banks (see case study). Although the amount stolen was smaller, the risk of large losses from compromises of financial transaction systems remains significant.

[83] Europol, Internet Organised Crime Threat Assessment. 2017.
[84] Symantec Blog. 2017.
[85] Kaspersky Lab, 2017.
[86] Symantec, Internet Security Threat Report: Financial Threats Review 2017.
[87] Security Magazine, 2015.
[88] EMVco, 2017.
[89] EMVco, 2017.
[90] Kar, 2017.
[91] Europol, Internet Organised Crime Threat Assessment, 2017.
[92] Stecklow et al., 2017.
[93] Khandewal, 2017.
[94] Lloyds, Bitcoin: Risk Factors for Insurance, 2015.
[95] Symantec, Internet Security Threat Report, 2017.
[96] SWIFT, 2017.

CASE STUDY

The Return of Lazarus: More SWIFT Financial Thefts in 2017

Sophisticated cyber attacks continued to enable financial thefts from the SWIFT inter-banking financial transaction system, following on from the major attacks in 2016. The victim of the 2017 attack was Far Eastern International Bank (FEIB) based in Taiwan. The gang used a vulnerability in the banks security, which allowed the group to secretly implant their malicious malware onto the bank's computers and servers.[97] This lead to a SWIFT terminal operated by the bank becoming compromised.

Once the group gained access to the SWIFT network and acquired the credentials necessary for payment transfers, the group attempted to fraudulently transfer $60 million to accounts in United States, Cambodia and Sri Lanka.[98] Due to a mistake by the criminals causing an error in the specific fields of the SWIFT transfer, banking officials were alerted and all but $500,000 was recovered.

As with previous attacks on the SWIFT network, the attackers used a specifically-crafted malware with many layers of subterfuge to avoid discovery. The sophistication of the attack is highlighted due to the incorporation of ransomware in the attack, which is likely to have been used to mislead the cyber security community. However, the money laundering process was less sophisticated than in previous attacks on the SWIFT network, and two 'money mules' were arrested attempting to physically withdraw stolen funds from a bank account in Sri Lanka.[99]

Some have attributed this attack to the North Korean state-sponsored hacking group Lazarus due to the similarities in the method of attack.[100] This group is a sophisticated advanced persistent threat (APT) group which has been associated with many high profile financial thefts including Bangladeshi SWIFT attack in 2016 and the 2017 attack on Polish banks.[101]

The continuation of attacks on financial network highlights that these are attractive targets offering big rewards to cyber criminals. Systems in place continue to manage to stop the criminals extracting the full potential from the initial penetration, although other attacks are known to succeed.

[97] Shevcheko et al., 2017.
[98] Finkle (2), 2017.
[99] Lin and Ondaatjie, 2017.
[100] BAE, 2017.
[101] Symantec, 2017.

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. 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. JP Morgan Chase and Co. announced the doubling of its cybersecurity budget from $250 million in 2015 to $500 million. Financial services continue to be the largest investors in cyber security.[102]

Cloud Outage

Cloud computing is being adopted increasingly rapidly. The failure of a cloud service provider, while very unlikely, represents a potential cyber insurance systemic exposure as many cyber policies include coverage for outages. Failures of individual services or availability regions have the potential to cause losses to thousands of users.

Cloud computing has successfully inundated the global markets, creating a utility-like service for over 90% of companies.[103] Adoption rates for use of the public cloud reached an estimated 18% with up to $246 Billion in revenue worldwide.[104] Large numbers of companies depend on the cloud, particularly in the ecommerce sector which accounts of 8.9% of total sales in the U.S. This represents a significant exposure to a potential failure of cloud service providers in cyber-affirmative IT insurance portfolios.[105]

Concentration risks in big four cloud service providers (CSPs)

The global market of CSPs continues to be dominated by Amazon Web Services (AWS) at 47%, followed by Microsoft Azure at 10%, Google Cloud Platform with 4%, & IBM Softlayer with 3%.[106]

While Amazon's position of market leader has yet to be seriously threatened by its competitors, the highest cloud adoption rates went to Microsoft Azure, particularly in application workloads. Azure adoption grew from 20 to 34 percent in a single year, while AWS maintained a steady 57 percent.[107] While this could be due to the size of AWS relative to Microsoft Azure, Azure's marketability to companies aiming to work in hybrid cloud may have begun to tip the scales. Azure's infrastructure is marketed to support data within a company's data center and within the Azure cloud, which may catch the attention of prospective clients. 67% of cloud users currently report using a hybrid cloud strategy which allows processes in-house and on the cloud.[108]

High resilience standards of CSPs

To be competitive in the public CSP market, providers need to minimize downtime and deliver on promised reliability ratings. While companies can state that their products are designed to deliver '99.999999999% durability',[109] the Service Level Agreements (SLAs) for AWS' compute service 'EC2', and Microsoft Azure's cloud services, dictate an official commitment to their customers of 99.95% reliability for each region.[110]

To maintain such high levels of reliability, the architecture of CSPs focuses on strategic isolation to protect the spread of malicious software and geographic redundancies for datacenters to reduce downtime. With plans for continued growth across the industry, the AWS Cloud operates 44 Availability Zones within 16 geographic Regions around the world, Microsoft with 36 regions, Google with as 13 regions, 39 zones, and IBM with 60 IBM Cloud data centers.[111]

Potential disruption from CSP failure

While agreements of 99.95% reliability are impressive, anything less than 100% translates to damaging downtime. The critical minutes or hours of downtime have proven to be costly to both the CSPs and their clients. The committed 99.95% reliability of the top 4 CSPs would legally allow for roughly four and a half hours of downtime for customers. The cost of downtime for 98% of organizations for a single hour totals $100,000, with 33% of those enterprises reporting that one hour of downtime costs their firms $1-5 million.[112]

Downtime for a CSP rarely translates to a shut down of the entire cloud. Rather, CSP downtime often manifests in service interruption to a single service, or, in the case of interdependent services, all those associated with the single service. Interruption to 'compute' and 'storage' services have the potential to cause greatest impact on customers as interdependencies within the cloud are often traced back to these essential services. Isolation between CSP availability zones limits the impact of the down service(s) - aiming to prevent global interruption.

[102] IDC, 2017.
[103] Rightscale, State of the Cloud, 2017.
[104] Gartner, 2017.
[105] U.S. Census Bureau, 2017.
[106] Coles, 2017.
[107] Rightscale, State of the Cloud, 2017.
[108] Rightscale, State of the Cloud, 2017.
[109] Amazon (1), 2017.
[110] Google (1); Azure ; IBM: Blue Mix; Amazon (2). 2017.
[111] Amazon Web Services ; Google (2); IBM Blue Mix.
[112] Woodward.

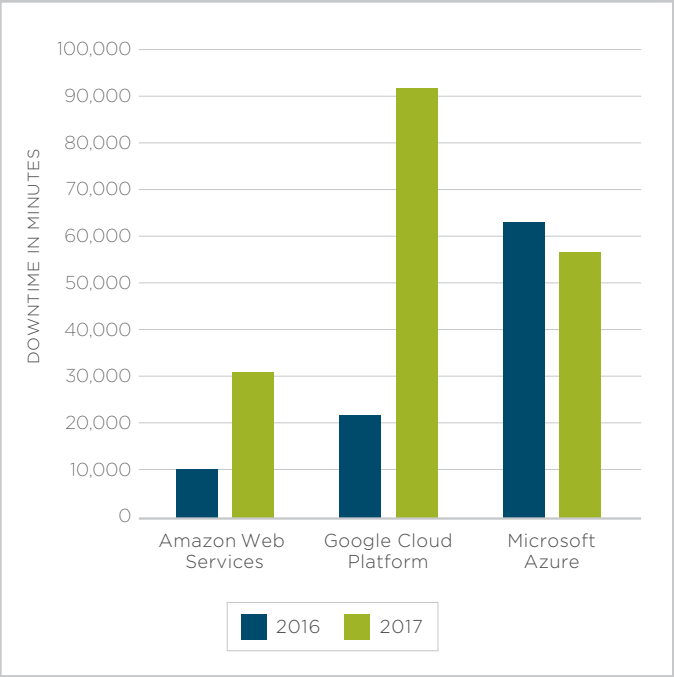


Figure 6: Recent Downtime Trends for Major Cloud Service Providers

Depending on the services provided by the cloud and the down service, downtime for a client could range from missing files from a website (as in the AWS S3 Outage in March 2017), denied access to a website (as in the case of the global Twitter cloud outage in January 2017), denied access to customer data (as in the case of the Salesforce.com outage in May 2017) and loss of revenue (AWS S3 outage in March 2017). While CSPs have been able to recover and restore access to customers after an outage, some outages can result in the permanent loss of data as in the Amazon EC2 crash in 2011.[113]

While stop gaps are standard for all major service providers, downtime continues to increase annually. The complete shut down of a CSP is not necessary for large financial losses. As more companies depend on the cloud, the interruption of an essential service in a single availability zone inevitably puts thousands of customers, and potentially millions of dollars at risk.

Cyber insurance and CSP outages

Cyber insurance policy retentions ensure that outages less than 12 hours are unlikely to trigger claims, but with companies more dependent on the cloud than ever, shorter outages are costing more to cloud customers with increasing dependencies. Any CSP failures longer than retention times will be systemic and cause multiple claims from companies that are covered against cloud provider downtime. Most companies who have a significant portion of their business operations in the cloud have increasingly sophisticated engineering approaches to maintain their own resilience and structuring continency from 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 RMS modeling: systemic and contagious hub and data center faults or malware, combine with complex repair and restoration paths.

Denial of Service Attacks

Distributed Denial of Service (DDos) attacks continue to be a major component in the cyber risk landscape. A third of all organizations reportedly experience DDoS attacks, twice as many as a year ago. This trend of growing likelihood of attack is likely to continue across sectors, geographies, and activity areas, as the firepower capacity of attackers increases, and they seek out new targets.

Increasing complexity of DDoS attacks

A Distributed Denial of Service attack uses internet traffic to overwhelm servers forcing a shut-down of the system or a slowing of services. This increased traffic denies access and limits usability to legitimate users or systems. Not only is the number of DDoS attacks increasing,[114] but so too is the complexity.

Instead of tactics focused on single aspect of a company's infrastructure, DDoS attacks are taking a more diversified approach, alternating targets within a single attack including web application servers, firewalls, and other infrastructure components. Additionally, by varying the modes within of attack, an additional layer of complexity can be added. Attack types are broadly categorized into Volume Based Attacks, Protocol Attacks, and Application Layer Attacks each with a different method of overwhelming site bandwidth. The increased complexity of a multi-modal attack makes these attacks difficult for a company to defend its networks both proactively and reactively.

[113] Blodget, 2011.
[114] Rayome, 2017.

CASE STUDY – FEBRUARY 2017

AWS S3 Outage

The Amazon Simple Storage Service (S3) is an object built storage system hosted on the Amazon cloud where clients can 'collect, store, and analyze data'. While AWS advertises its S3 service as the 'most supported storage platform available', disruptions to this service on Tuesday, 28 February 2017, saw "high error rates" in multiple AWS services in the U.S. eastern region.

Disruptions to the S3 Service, which allows clients to store and retrieve data from AWS servers, left numerous websites devoid of product images and company logos. Additionally, many IOT devices which relied on the S3 buckets were unable to operate normally[115] Ironically, the Amazon Health dashboard, which reports the working status of services was offline globally, preventing all clients, regardless of S3 usage, from access to updates about service status and downed regions.

Amazon reported that the outage occurred while members of the S3 team were attempting to debug the billing system and unfortunately entered an incorrect command. This slip took down more servers than intended, including two which support the S3 subsystems. The restart required to bring these services online took down other additional services in the process.[116] While these began in the S3 service provided by the U.S.-East-1 North Virginia site they spread to other services hosted by U.S.-East-1 including CloudWatch, EC2, Storage Gateway, and WAF (web application firewall). This case study brings to light the vulnerability of cloud service ecosystems where services within the cloud rely on each other.

During the four-hour disruption, we estimate that large and premier-sized IT, Retail, & Finance Companies lost a total of $150 million. E-commerce companies specifically felt the downtime as 54 of the top 100 internet retailers were affected with a reported decreased processing speeds or websites down entirely. It is essential to have redundancies within a cloud infrastructure and within cloud service ecosystems to protect against downtime and the resulting financial losses.

[115] Nichols, 2017.
[116] Cassey, 2017.

Pulse DDoS attacks

The typical attack pattern of DDoS attacks has also grown in complexity. While previously a DDoS attack pattern was pictured as a prolonged wave leading to a peak in activity followed by a rapid descent, a new tactic known as the 'pulse wave attack' has changed the timing of attacks. A pulse wave attack is a rapid succession of attacks with the interval between each attack being used to mount the next attack on a different target. It may take attackers only minutes to bring down a server which will take hours to reinstate. Pulse DDoS attacks can extend for days at a time and thus pose a significant risk to the accessibility of a company's network.[117]

The significance of complex successive attacks is that large commercial servers designed to deal with high traffic volumes are resilient against attacks of low intensity, but very-high intensity attacks with frequently changing targets within a network's infrastructure can bring down even the strongest websites. It is possible that no web server will be resilient to disruption from DDoS attacks if the intensity of attacks continues to scale up.

Repeated attacks on targets

Repeat attacks on targets are a common characteristic of DDoS attacks. The average number of DDoS attacks per target is increasing. Over 75% of targets are reportedly hit multiple times, an increase from 43.2% in 2016.[118] There is a wide variation in number of attacks per target, with some companies reporting several hundreds of attacks.

Internet of Things: A technology for DDoS attacks

Much of the firepower from recent DDoS attacks has been drawn from Internet of Things (IoT) devices connected to the web. In addition, IoT devices can also become vulnerable targets for DDoS attacks: computers, mobile devices, tea-kettles, fish tanks, all being used in recent DDoS attacks. IoT devices serve as an ideal platform for DDoS attacks. Networks for IoT devices are notoriously vulnerable and offer high speed connections on a consistently switched on network.[119] Until manufacturers of IoT devices address network security, these devices will continue to pose an increasingly large threat as a platform for DDoS attacks as IoT devices are projected to account for more than two-thirds of the 34 billion internet connected devices by 2020.[120]

Political use of DDoS attacks

The motivations for recent DDoS attacks have been evolving, with politically-motivated DDoS attacks gaining the focus of the media globally. DDoS attacks accompanied the Qatar Crisis, with an attack on Al Jazeera, the largest news network in the area, the presidential elections in France where Le Monde and Le Figaro websites were targeted, and voter registration for Brexit in U.K. among others.[121]

Sectoral preferences in DDoS targeting

Profiling the business sectors that experience the highest number of DDoS attacks has consistently indicated that the Gaming Industry, with its need for reliable, high-speed connections, is a preferred target for DDoS cybercriminals. Other popular targets for DDoS attacks for 2017 included the Software & Technology Sector as well as Internet & Telecom and Financial Services. Other sectors including Media & Entertainment, Retail & Consumer Goods, and Education sectors have all reported frequent DDoS attacks.[122]

Business disruption from DDoS attack

For most competitive companies, internet access is as essential as basic utilities. A DDoS attack, regardless of platform threatens the accessibility of network traffic from legitimate customers and thereby the bottom line of web-based sales. Business interruption loss poses one of the most severe financial outcomes of a DDoS attack as without reliable access to internet functionality, significant financial losses can result. A DDoS attack which is designed to cause such disturbances to essential network infrastructure has recently been estimated to cost companies up to $2.5 million per attack.[123] Insurance agencies have paid out Business Interruption claims specifically for DDoS and DDoS extortion attacks with pay-outs nearing half a million dollars.[124]

DDoS protection

Many cyber security companies offer DDoS protection and tracking software which create intelligent resilience solutions for customers. These solutions include protective firewalls, large networks which can absorb DDoS attacks, and monitoring software to keep track of network traffic. By monitoring the internal and external network traffic, and defining 'normal' traffic patterns, companies can be alerted when they deviate from the norm. DDoS traffic can usually be traced to bots or hijacked web-browser rather than personnel, so it is important to monitor signatures and identifiable attributes of network traffic. The best protection for a company is to diversify protection techniques. An internal understanding of the norm for a company's network, paired with the software to monitor and protect this norm allows for expedited mitigation techniques from emergency response services in the event of a DDoS attack.

[117] Imperva, 2017.Global DDoS Threat Landscape Q1 2017.
[118] Paganini, 2017.
[119] IBM X-Force, The weaponization of IoT devices: Rise of the thingbots, 2017.
[120] Greenough, 2014.
[121] Khaliimonenkon et al., DDoS attacks in Q2 2017.
[122] Akami, State of the internet security report Q2, 2017.
[123] Brook, 2017.
[124] Beazley (2).

CASE STUDY – OCTOBER 2017

Denial of Service Attack on Swedish Transport System

DDoS attacks not only threaten the internal infrastructure of a company but also pose a threat to physical structures which rely on working networks. Starting on October 11, 2017 DDoS attacks disrupted the Swedish Transport Administration (Trafikverket) which sent the IT system that monitors the company's train locations, email systems, and road traffic maps off-line. This network disruption brought Sweden's transportation services to a standstill. The Transportation agency was forced to stop or delay trains during the attack and the traffic maps were affected into the upcoming days.

The following day, the attacks on the Swedish Transportation System continued. On October 12, 2017, the DDoS attacks focused on the website of the Swedish Transport Administration who is responsible for regulating and inspection systems and the transport operator Vasttrafik – taking down both their online booking and travel planning services for trains, buses, ferries, and tram transports.[125]

The perpetrator for these attacks has yet to be named, but presumed motivations of disrupted transportation services were successful. This cyber-attack was the second in a four-month span for Sweden's Transport Administration, with a previous attack targeting Sweden's air traffic control center. Swedish officials attributed this November 2015 attack which grounded flights, to Russian cybercriminals.[126]

[125] Barth, 2017.
[126] Cimpanu, 2017.

SECTION 3

A Growing Cyber Insurance Market

The growing cyber insurance market is continuing to be profitable, but has had some near misses that could have substantially impacted the industry loss ratio. Growth is coming from new sectors and markets. Implementing growth and loss control strategies is a major priority.

Rapid Growth

The cyber insurance market continues to demonstrate consistent growth at around 30% year on year. Estimates for 2020 range from between $5 to 10 billion,[127] with several analysts expecting by 2025 the market could be as large as $20 billion.[128]

While this represents substantial growth, it remains modest in comparison with the overall commercial insurance market of $247 billion.[129] It is also relatively small in comparison with the overall corporate cyber risk management spend, with Gartner reporting worldwide cybersecurity spending at over $75.4 billion.[130]

Drivers of growth

A review of a large number of cyber insurance policies seen by RMS suggests the growth in the U.S. has been driven by increased take up from non-traditional purchases of cyber insurance (outside healthcare, technology and retail), as well as additional premiums generated from the availability of larger limits. International growth has also played a key part, with several markets demonstrating strong growth including Australia, Japan, and the United Kingdom.

Looking more long term, RMS expects substantial growth for the industry driven by not just cyber but a broader category of digital risks. Businesses are becoming increasingly reliant on technology to run their operations and while this brings obvious benefits, it also means they are increasingly vulnerable to system failures, data losses and cyber attacks. As the rate of technology change continues apace, the digital environment is likely to become even more complex and the amount of digital information will grow exponentially.

Corporate risk managers need to develop comprehensive digital risk management strategies that involve a range of mitigations with risk transfer solutions through insurance being critical. Given the pervasive nature of technology as the foundation of the modern economy, digital risk provides a once in a generation opportunity for the insurance industry.

Market participants and increased competition

The market continues to see a substantial concentration of premium within a handful of insurers. In the U.S. just 4 domestic writers and one Lloyd's insurer generate almost 60% of all premium, according to an analysis of the NAIC statutory filings. This market leading position has allowed these organizations to develop a wealth of experience and data, affording them a substantial competitive advantage.

However, a key trend observed over the last two years has been the entrance of many new carriers. There are now more than 140 insurers reporting cyber premiums, although their participation remains limited. In 2016, 68 insurers reported premiums greater than a million dollars, and of these only 28 had more than $5 million.[131]

The increased competition is having an impact, with rates reportedly down over the last 12 months as well as a

[127] Swiss Re Sigma Report, 2016
[128] Allianz, *A Guide to Cyber Risk*, 2017.
[129] Romansky et al. *Content Analysis on Cyber Insurance*, 2017
[130] Gartner (2), 2017.
[131] Aon, Global Cyber Market Overview, 2017.

> The market continues to see a substantial concentration of premium within a handful of insurers.

general loosening of coverage terms. Despite high profile systemic cyber events over the last 12 months, the limited impact on the cyber insurance industry has likely only exacerbated this issue.

International growth

While the clear majority of premium continues to be emanate from the U.S., there are substantial signs of growth internationally, with Europe, Japan and Australia all seeing significant rises in GWP, albeit from a relatively small base.

New data protection regulations coming in to place in Australia appear to be stimulating the market, and it is expected that GDPR will have a similar impact for the EU.

Profitability of Cyber Lines

RMS estimates the industry loss ratio for 2016 at 54.6%. This is based on an extensive review into the occurred events and insurance penetration for 2016. This is slightly higher than the 47.6% reported from the admitted business in the U.S.[132] However, it is still healthy return compared with more mature insurance markets.

Loss processes

RMS analysis shows that breach of privacy events (such as data exfiltration) continue to contribute the largest financial impact to losses. As has been widely reported, the proliferation of ransomware (see previous section) has resulted a large spike in the frequency of extortion and BI claims.

To date the costliest losses have been driven by individual large loss events rather than more systemic events. This has had the impact of spreading the losses unevenly across insurers, with loss ratios varying substantially between carriers, with writers of larger corporates seeing volatile losses. Some have been fortunate enough to return single digit loss ratios while others have ratios greater than 150%.[133]

Near misses

But it is fair to say it could have been a very different picture had the WannaCry and NotPetya events played out differently. An analysis of the WannaCry incident carried out by RMS calculated that with just a few small variations in the way it played out, insured losses for the industry would have exceeded $3 billion.

Cyber Reinsurance

The cyber reinsurance market has continued to develop over the last 12 months. Insurers are now more aware of the potential for systemic incidents to trigger substantial losses and are looking to the reinsurance market to transfer some of this risk off their balance sheets.

The majority of reinsurance contracts remain as per risk quota share with some aggregate stop loss terms adding additional protection for the reinsurer. However, over the last 12 months RMS is seeing several brokers structuring more complex treaties including excess of loss.

Managing Cyber Exposure

Driven by increased regulatory pressures and improved awareness at the board level, insurers have looked to implement practices to manage cyber risk. However, substantial challenges exist in providing the clear visibility required.

As many commentators have stated, cyber coverage can be found in numerous other lines of business, including property, general liability, crime, kidnap and ransom, and potentially many others. This is either through endorsements or silent 'non-affirmative' coverage.

Consistent approaches

Implementing a consistent approach to managing risk across these diverse classes of business is a challenge for many insurers. Some of the main challenges are with the inconsistency in policy wordings, ambiguity in the strength of exclusions, and varying data quality approaches to data capture across multiple often legacy systems.

The clear need for visibility into cyber risk has led insurers to tackle these challenges head on. RMS has worked with many insurers over the last 12 months to implement robust but practical exposure management approaches leading to significantly improved visibility.

[132] Aon, Global Cyber Market Overview, 2017.
[133] NAIC, 2017.

Pricing Cyber Risk

Approaches to pricing cyber risk have yet to come to a consensus across the industry. A review of the rate fillings provided to insurance commissioners in the U.S. highlight the challenges of pricing cyber risk given the limited historical data and the relatively dynamic peril. Among the approaches documented includes borrowing from other classes; "we chose to use fiduciary liability data because it has a similar limit profile and expected development pattern [as cyber losses]", and "factors are taken from our Miscellaneous Professional Liability product"[134]– a less than ideal approach.

Risk capital allocation

At the portfolio level, the potential impact of cyber catastrophe risk is predominantly monitored through deterministic models. This has led to increased awareness of the potential for systemic risk to have a material impact on a cyber portfolio and provides insurers with an approach to identify and mitigate risk accumulations. However, approaches to assigning return periods to losses, and thereby supporting the inclusion of modeled results within capital modeling applications have to date been limited.

These challenges highlight the need for improved data and risk models to support the industry's growth in a resilient manner.

[134] Romansky et al. *Content Analysis on Cyber Insurance*, 2017

References

Accenture Security. *2017 Cyber Threatscape Report: Midyear Cybersecurity Risk Review-Forecast and Remediation's*. Accenture Security, 2017.

Advisen. *Information Security and Cyber Risk Management*. Seventh Annual Survey, 2017.

Akamai. *State of the internet/security: Q2 2017 Report*.

Allianz. *A Guide to Cyber Risk*. Allianz Global Corporate & Specialty White Paper, 2017.

Amazon (1). "Amazon Simple Storage Service (S3) — Cloud Storage — AWS". Amazon Web Services, Inc. 2018.

Amazon (2). "Amazon EC2".

Aon. *Global Cyber Market Overview*, June 2017.

BAE. "When cyber attacks meet financial crime".

Barth, Bradley. "DDoS attacks delay trains, halt transportation services in Sweden". SC Magazine. October 16, 2017.

BBC (1). "Qatar Crisis: What you need to know." July 19, 2017.

BBC (2). "Theresa May accuses Vladimir Putin of election meddling." November 14, 2017.

BBC (3). "NHS cyber-defender Marcus Hutchins to appear in U.S. court." August 4, 2017.

BBC (4). "Dark web markets boom after AlphaBay and Hansa Busts". August 1, 2017.

BBC (5). "South Korean firm's 'record' ransom payment", June 20, 2017.

Berr, Jonathan. "'WannaCry' ransomware attack losses could reach $4 billion". *CBS Moneywatch*. May 16, 2017.

Beazley (1). "Ransomware attacks steal headlines, but accidental data breaches remain a major cause of loss". August 1, 2017.

Beazley (2). "Technology, Media & Business Services First Party Computer Claims".

Blodget, Henry. "Amazon's Cloud Crash Disaster Permanently Destroyed Many Customers' Data". *Business Insider*. April 28, 2011.

Boey, Darren. "North Korean Hacker Group Linked to Taiwan Bank Cyber Heist." *Bloomberg Technology*. October 17, 2017.

Brook, Chris. "DDOS Attacks Can Cost Businesses up to $2.5 Million per Attack, Report Says". *Threat Pos*t. May 2, 2017.

Burgess, M. "What is GDPR? WIRED explains what you need to know". *Wired*, January 2, 2018.

Chappell, Bill. "'Petya' Ransomware Hits at Least 65 Countries; Microsoft Trace it to Tax Software." *NPR*. June 28, 2018.

Cimpanu, Catalin. "95% of All Ransomware Payments were Cashed out via BTC-e Platform". *Bleeping Computer*. July 27, 2017.

Coles, Cameron. "Overview of Cloud Market in 2017 And Beyond". *Skyhigh*.

Comptroller and Auditor General. Investigation: *WannaCry cyber attack and the NHS*. National Audit Office. Department of Health. October 27, 2017.

Council of Europe. *International Co-operation under the Convention on Cybercrime*. Project on Cybercrime. 18 August, 2017.

Cybereason. *Paying the Price of Destructive Cyber Attacks*. Whitepaper, 2017.

EMVco. "EMVCo Reports 6.1 Billion EMV Chip Payment Cards in Global Circulation". June 5, 2017.

European Commission. "Protection of personal data". *Europa*, 2017.

Europol. *Internet Organised Crime Threat Assessment*. 2017.

Field, Tom. "The Blurred Lines Between Criminals and Nation-States". *Bank Info Security*. June 19, 2017.

Forester, Conner. "NotPetya ransomware outbreak cost Merck more than $300M per quarter". *Tech Republic*.

Finkle, Jim (1). "Your medical record is worth more to hackers than your credit card". *Reuters*. September 24, 2014.

Finkle, Jim.(2) "Cybersecurity Firm: North Korea Was Likely Behind Cyber Heist In Taiwan". *Business Insider*. October 16, 2017.

Gabel, Detlev and Hickman, Tim. K. *Key definitions-Unlocking the EU General Data Protection Regulation*. Whitecase publications, September 2017.

Gammons, Brianna. "6 Must-Know Cybersecurity Statistics for 2017". *Barkly* (Blog), January, 2017.

Gartner (1). "Gartner Says Worldwide Public Cloud Services Market to Grow 18% in 2017". 2017.

Gartner (2). "Gartner Says Worldwide Information Security Spending Will Grow 7 Percent to Reach $86.4 Billion in 2017". August 16, 2017.

Gerstein, Josh. "Alleged leaker Reality Winner said she stuffed NSA report in her pantyhose". *Politico*. September 27, 2017.

Gibbs, Samuel (1). "Shadow Brokers threaten to unleash more hacking tools". *The Guardian*. May 17, 2017.

Gibbs, Samuel (2). "Game of Thrones: HBO hackers threaten leak of season finale". *The Guardian*. August 21, 2017.

Gogan, Marcell. "Insider Threat as the Main Security Threat in 2017". *TRIPWIRE*. April 11, 2017.

Google (1). "Google Cloud Computing, Hosting Services & Apis". *Google Cloud Platform*.

Google (2). "Cloud Locations".

Graham, Chris. "NHS cyber attack: Everything you need to know about 'biggest ransomware' offensive in history". *The Telegraph*. May 20, 2017.

Gray, Alistair. "U.S. banks to introduce new anti-fraud measures after Equifax Hack". *Financial Times*. October 15, 2017.

Greenberg, Andy (1). "How An Entire Nation Became Russia's Test Lab for Cyberwar." *Wired*. June 19, 2017.

Greenberg, Andy (2). "The Biggest Dark Web Takedown Yet Sends Black Markets Reeling". *Wired*. July 14, 2017.

Greenberg, Andy (3). "No One Wants to Buy Those Stolen NSA-Linked 'Cyberweapons'". *Wired*. August 16, 2016.

Greenough, J. "The 'Internet of Things' Will Be The World's Most Massive Device Market And Save Companies Billions Of Dollars". *Business Insider*. November 18, 2014.

IBM. "IBM Blue Mix". IBM.

IBM X-Force Research. *The weaponization of IoT devices: Rise of the thingbots*. New York: IBM, 2017.

IDC. "Worldwide Spending On Security Technology Forecast To Reach $81.7 Billion In 2017, According To New IDC Spending". *Research Press Release*. March 29, 2017.

Imperva. *Global DDoS Threat Landscape Q1 2017*. 2017

Information Commissioner's Office. *Guide to the General Data Protection Regulation*. ICO, 2017.

Jolly, Jasper. "Massive hack at Equifax exposes personal records of Brits and 142m Americans". *CITY A.M*. September 8, 2017.

JLT. "Asia Moves Towards Tougher Data Breach Rules". December 8, 2017.

Johnson, Tim. "Here's one tally of the losses from WannaCry ransomware attack". *McClatchy*.

Jun, Kwanwoo and Yousef, Nancy. "North Korea Suspected of Hacking U.S.- South Korean War Plans." *The Wall Street Journal*. October 10, 2017.

Kan, Michael. "Yahoo uncovered breach after probing a black market sale". *CIO*. September 22, 2016.

Kar, Ian. "The chip card transition in the U.S. has been a disaster". *Quartz*. July 29, 2016.

Kaspersky Lab (1). *APT Trends Report Q2 2017*. SECURELIST, 2017.

Kaspersky Lab (2). *KSN Report: Ransomware in 2016-2017*. Security List,2017.

Khalimonenko, Alexander, Oleg Kupreev, and Timur Ibragimov. *DDoS attacks in Q2 2017*. SecureList DDOS Reports.

Khandelwal, Swati. "Hackers Stole $32 Million in Ethereum; 3rd Heist in 20 days". *The Hacker News*. July 19. 2017.

Kshetri, Nir and The Conversation. "Cryptocurrencies May Be a Dream Come True for Cyber-Extortionists". *Fortune*. September 19, 2017.

Lin, Adela, and Ondaatjie, Anusha. "Sri Lanka Makes Arrests In $60 Million Taiwanese Bank Cyberheist". *Bloomberg*. October 12, 2017.

Lloyds. *Bitcoin: Risk Factors for Insurance*. London: Lloyd's Innovation Series, 2015.

Ludwin, Adam. "How Anonymous is Bitcoin? A Backgrounder for Policymakers". *Coindesk*. January 25, 2015.

Morgan, Steve. "Global ransomware damage costs predicted to exceed $5 billion in 2017, up from $325 million in 2015". *CSO*. May 23, 2017.

McCrank (1), John. "Equifax says 15.2 million U.K. records exposed in cyber breach". *Reuters*. October 10, 2017.

McCrank (2), John and Saxena, Aparajita. "Equifax clears executives who sold shares after hack". *Reuters*. November 3, 2017.

Michael, Casey. "The Kremlin's California Dream." *Slate*. May 4, 2017.

Microsoft Azure. "Cloud Locations". *Google Cloud Platform*.

National Association of Insurance Commissioners. "The National System of State Regulation and Cybersecurity". December 12, 2017.

Nakashima, Ellen. "Prosecutors to seek indictment against former NSA contractor as early as this week". *The Washington Post*. February 6, 2017.

National Audit Office. *Investigation: WannaCry Cyber Attack and the NHS*. Report by the Comptroller and Auditor General, Department of Health. HC 414 Session 2017–2019 October 27, 2017.

Newton, Casey. "How A Typo Took Down S3, The Backbone Of The Internet". *The Verge*. March 2, 2017.

Nichols, Shaun. "AWS's S3 Outage Was So Bad Amazon Couldn't Get Into Its Own Dashboard To Warn The World". *The Register*. March 1, 2017

O'Conner, Fred. "NotPetya Still Roils Company's Finances, Costing Organizations $1.2 Billion In Revenue". *Cybereason*. November 9, 2017.

Office of the Director of National Intelligence. "Assessing Russian Activities and Intentions in Recent U.S. Elections". ICA, 2017-01D. January 6, 2017.

Oliphant, Roland and McGoogan, Cara. "NATO warns cyber attacks 'could trigger article 5' as world reels from Ukraine hack." *The Telegraph*. June 28, 2017.

Paganini, Pierluigi. "Imperva Report Q2 2017- Over 75% Of DDoS Targets Were Hit Multiple Times". *Security Affairs*. October 3, 2017.

Palmer, Danny. "A massive cyberattack is hitting organizations around the world". *ZD Net*. June 27, 2017.

Perlroth, Nicole. "All 3 Billion Yahoo Accounts Were Affected by 2013 Attack". *New York Times*. October 3, 2017.

Popper, Nathaniel and Ruiz, Rebecca. "2 Leading Online Black Markets Are Shut Down by Authorities". *New York Times*. July 20, 2017.

PYMNTS. "Dark Web Down But Not Out". August 21, 2017

Rayome, Alison. "33% of businesses hit by DDoS attack in 2017, double that of 2016". *Tech Republic*. October 11, 2017.

Right Scale. 2017. State Of The Cloud Report.

Riley, Michael (1), Anita Sharpe and Jordan Robertson. "Equifax Suffered a Hack Almost Five Months Earlier Than the Date It Disclosed". *Bloomberg*. September 18, 2017.

Riley, Michael (2), Jordan Robertson and Anita Sharpe. "The Equifax Hack Has the Hallmarks of State-Sponsored Pros". *Bloomberg*. September 29, 2017.

Romanosky, Sasha, Lillian Ablonm Andreas Kuehn and Therese Jones. *Content Analysis on Cyber Insurance*. RAND Working Paper, September 2017.

Shepardson, David. "Equifax failed to patch security vulnerability in March: former CEO". *Reuters*. October 2, 2017.

Shevchenko, Sergei, Hirman Muhammad bin Abu Bakar, and James Wong. "Taiwan Heist: Lazarus Tools And Ransomware". *BAE Threat Research* (Blog). October 16, 2017.

Solon, Olivia and Siddiqui, Sabrina. "Russia-backed Facebook posts 'reached 126m Americans' during U.S. election." *The Guardian*. October 31, 2017.

Sputnik News. "Chinese Phone App Leaks 2 Billion Private Numbers, High Officials' Among Them". May 14, 2017.

Stecklow, Steve, Alexandra Harney, Anna Irrera and Jemima Kelly. "Chaos and hackers stalk investors on cryptocurrency exchanges". *Reuters*. September 29, 2017.

SWIFT. "Release Timeline".

Symantec. *Internet Security Threat Report*. ISTR, 2017.

Symantec. *ISTR Ransomware 2017*. July 2017.

Symantec. "Attackers target dozens of global banks with new malware". *Symantec Official Blog*. February 12, 2017.

Symantec. *Internet Security Threat Report*: *Financial Threats Review 2017*. 2017.

Symantec. "Attackers Target Dozens Of Global Banks With New Malware". *Symantec Official Blog* (Blog).

The Conversation. "By concealing identities, cryptocurrencies fuel cybercrime". *Editorial*. September 26, 2017.

Thomson, Iain. "Virus (cough, cough Petya) goes postal at FedEx, shares halted". *The Register*. June 28, 2017.

Turner, Karen. "The Equifax hacks are a case study in why we need better data breach laws". *Vox*. September 14, 2017.

United State Department of the Treasury Financial Crimes Enforcement Network. "FinCEN Fines BTC-e Virtual Currency Exchange $110 Million for Facilitating Ransomware, Dark Net Drugs Sales". *FinCen*. July 26, 2017.

Viner, K. "How technology disrupted the truth." *The Guardian*. July 12, 2016.

Wolff, Josephine. "The New Economics of Cybercrime". *The Atlantic*. June 7, 2017.

Wolfram, Hedrick, Gerald Wong and Jaclyn Yeo. *Cyber Risk in Asia-Pacific: The Case For Greater Transparency*. OLIVER WYMAN, 2017.

Woo, G.; 2017; Counterfactual Analysis of WannaCry Malware Attack. RMS Webinar, Nov 2017; and blog 'Reimagining the WannaCry Cyberattack'

Woodward, Matt. "How Much Does 1 Hour of Downtime Cost the Average Business?". RAND Group.

Acknowledgements

Report prepared by Cambridge Centre for Risk Studies, in collaboration with Risk Management Solutions, Inc.

Report Citation

Coburn, A.W.; Daffron, J.; Smith, A.; Bordeau, J.; Leverett, É.; Sweeney, S.; Harvey, T.; 2018. Cyber Risk Outlook; Centre for Risk Studies, University of Cambridge, in collaboration with Risk Management Solutions, Inc.

Risk Management Solutions, Inc

Dr Andrew Coburn, *Senior Vice President*
Dr Christos Mitas, *Vice President*
Adam Sandler, *Managing Director*
Tom Harvey, *Senior Product Manager*
Peter Ulrich, *Senior Vice President*
Dr Hichem Boudali, *Senior Modeler*
Chris Vos, *Senior Modeler*
Dr Malik Awan, *Modeler*
Simon Arnold, *Senior Modeler*
John Agorgianitis, *Senior Modeler*
Dr Gordon Woo, *Catastrophist*
Bob Owen, *Marketing Director*
Simon Bennet, *Content Manager*
Carol Hackett, *Senior Graphic Consultant*
Kate Grove, *Consultant Analyst*

Cambridge Centre for Risk Studies

Simon Ruffle, *Director of Research and Innovation*
Dr Jennifer Daffron, *Research Associate*
Éireann Leverett, *Senior Cyber Risk Researcher*
Andrew Smith, *Research Assistant*
James Bordeau, *Research Assistant*
Kelly Quantrill, *Research Assistant*
Jennifer Copic, *Research Associate*
Kayla Strong, *Research Assistant*
Siobhan Sweeney, *Risk Fellow*
Professor Daniel Ralph, *Academic Director*
Dr. Michelle Tuveson, *Executive Director*


function MM_preloadImages() { //v2.0
if (document.images) {
var imgFiles = MM_preloadImages.arguments;
if (document.preloadArray==null) document.preloadArray = new Array();
var i = document.preloadArray.length;
with (document) for (var j=0; j<imgFiles.length; j++) if (imgFiles[j].charAt(0)!="#"){
preloadArray[i] = new Image;
preloadArray[i++].src = imgFiles[j];
function MM_swapImgRestore() { //v2.0
if (document.MM_swapImgData != null)
for (var i=0; i<(document.MM_swapImgData.length-1); i+=2)
document.MM_swapImgData[i].src = document.MM_swapImgData[i+1];
function MM_swapImage() { //v2.0
var i,j=0,objStr,obj,swapArray=new Array,oldArray=document.MM_swapImgData;
for (i=0; i < (MM_swapImage.arguments.length-2); i+=3) {
objStr = MM_swapImage.arguments[(navigator.appName == 'Netscape')?i:i+1];
if ((objStr.indexOf("document.layers[")==0 && document.layers==null) ||
(objStr.indexOf("document.all[") ==0 && document.all ==null))
objStr = 'document'+objStr.substring(objStr.lastIndexOf('.'),objStr.length);
obj = eval(objStr);
if (obj != null) {
swapArray[j++] = obj;
swapArray[j++] = (oldArray==null || oldArray[j-1]!=obj)?obj.src:oldArray[j];
obj.src = MM_swapImage.arguments[i+2];
document.MM_swapImgData = swapArray; //used for restore
function MM_controlShockwave(objStrNS,objStrIE,cmdName,frameNum) { //v2.0
var objStr = (navigator.appName=='Netscape')?objStrNS:objStrIE;
if ((objStr.indexOf("document.layers[")==0 && document.layers==null) ||
(objStr.indexOf("document.all[") ==0 && document.all ==null))
objStr = 'document'+objStr.substring(objStr.lastIndexOf('.'),objStr.length);

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®