MODULE 9:
CYBER LOSS PROCESS & CYBER INSURANCE

Trends in Cyber Loss Processes. The environment of cyber threats has led to a shift in how organizations manage cyber losses. This dynamic field is experiencing trends in incident response, mitigation, and recovery. Cyber loss processes now focus on swift detection, effective containment, and resilient recovery strategies. Understanding these trends is crucial for organizations to adapt and safeguard their digital assets.

Cyber Insurance. With the increasing frequency and sophistication of cyberattacks, cyber insurance has emerged as a critical tool in risk management. This insurance provides coverage for losses resulting from data breaches, ransomware attacks, and other cyber incidents. It plays a vital role in helping organizations recover financially from the fallout of cyberattacks. As a key component of a comprehensive cybersecurity strategy, cyber insurance is essential for mitigating the financial risks associated with cyber threats. Understanding its principles and benefits is crucial for businesses in today's digital landscape.

9.1 TRENDS IN CYBER LOSS PROCESSES

Several trends have emerged in cyber loss processes as organizations seek to improve their cyber risk management and response capabilities. These trends include:

- **Incident Response Automation** - organizations are adopting automation tools and technologies to improve their incident response capabilities. Automated incident response systems can detect and respond to cyber threats in real-time, reducing response times, minimizing the impact of attacks, and improving overall cyber resilience.
- **Threat Intelligence Sharing** - collaboration and sharing of threat intelligence between organizations, industries, and even across national borders has become crucial. By sharing information on emerging threats, attack techniques, and vulnerabilities, organizations can proactively defend against cyber threats and better protect their systems and networks.
- **Cyber Insurance** - demand for cyber insurance has been on the rise as organizations recognize the financial risks associated with cyber incidents. Cyber insurance policies help mitigate potential financial losses by covering costs such as incident response, legal expenses, customer notifications, and business interruption.
- **Focus on Cyber Resilience** - rather than solely relying on prevention measures, organizations are shifting their focus towards building cyber resilience. This involves implementing strategies and technologies to enable quick recovery and continuity of operations in the face of a cyber

incident. Cyber resilience includes measures such as regular data backups, incident response planning, and robust business continuity management.

- **Regulatory Compliance and Data Privacy** - with the increasing number of data protection regulations worldwide (e.g., GDPR, CCPA), organizations are prioritizing compliance efforts. This includes implementing strong data privacy practices, conducting privacy impact assessments, and ensuring secure data handling and processing.
- **Cloud Security and Third-Party Risk Management** - as organizations embrace cloud computing and rely on third-party vendors for various services, managing cloud security risks and assessing third-party cyber risk have become critical. Organizations are implementing robust security measures, conducting thorough due diligence on vendors, and establishing clear contractual agreements to mitigate potential risks.
- **Cybersecurity Training and Awareness** - recognizing that human error is a significant factor in cyber incidents, organizations are investing in cybersecurity training and awareness programs for their employees. These programs aim to educate staff about common cyber threats, best practices for data protection, and the importance of maintaining good cyber hygiene.
- **Cyber Exercise and Simulation** - organizations are conducting regular cyber exercises and simulations to test their incident response plans and identify potential gaps. These exercises involve simulating realistic cyber-attack scenarios to assess the effectiveness of response processes, train incident response teams, and improve overall preparedness.

By staying informed and adapting to these trends, organizations can enhance their cyber loss processes, better mitigate cyber risks, and respond effectively to cyber incidents.

DATA EXFILTRATION

Data exfiltration is the unauthorized extraction or theft of data from a computer network, system, or device. It involves the unauthorized transfer of sensitive, confidential, or valuable data from an organization's internal network to an external location or unauthorized recipient.

Data exfiltration can occur through various methods, such as exploiting vulnerabilities in the network, using malware or malicious software, leveraging social engineering techniques, or unauthorized physical access to devices. The stolen data can include intellectual property, financial information, personally identifiable information (PII), trade secrets, or any other valuable data assets. Data exfiltration is a significant risk to organizations, including financial loss, reputational damage, regulatory compliance issues, and potential legal repercussions.

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 costlier 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

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. 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. 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. Evidence that the data is being sold on the black market by an Eastern European hacking collective 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

Data exfiltration events 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.

Cyber-criminals 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.

Cyber attackers may instead be turning to less secure targets in other countries, and to other forms of cybercrime, 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 numbers of data breaches has fallen due to improved methods of prevention, the severity of data incidents has nonetheless 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 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.

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),	India	135 Million	01/11/2016	P8
Tencent Holdings Limited	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	China	30 Million	01/01/2017	P7

Selected Recent Large Data Breaches

COMPANIES ARE HOLDING MORE DATA

"Data is the new gold": 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. The size of datasets, and the aspects of people's lives and behaviours that could potentially be exfiltrated, is a constantly upward 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 (Private Health Insurance)) and personal identifiable information (PII) are worth more on

the black market, relative to credit cards and other personal finance records. 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. An emerging recent target for data breaches has been offshore legal firms in tax havens, with a string of incidences of whistle-blower 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.

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. This is attributed to the regulatory costs, escalating legal complexity and growing cost of compensation. Costs of data exfiltration attacks vary significantly between countries and increases 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. 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.

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 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 businesses being granted, access to vital systems within a company's network. One of the higher profile 'contractor- breaches' was from National Security Agency (NSA), which demands the highest level of vetting for employees.

ACCIDENTAL DATA LOSS REMAINS SIGNIFICANT

Unintended disclosure of data remains a significant loss process. 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.

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 can 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.

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 cancelling of appointments and surgeries, and forced a reversion to manual record keeping.

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 centres.

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 fuelled 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. 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.

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. Another targeted attack, utilizing the ransomware Erebus against a South Korean web hosting company, Nayana, in which all its servers were encrypted, resulted in a $1 M ransom being paid and the bankruptcy of the company. 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

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. 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. 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.

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. 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 an 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 technology88 compared with 84.9% of European vendors. 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. U.S. continues to see many types of card-present and point-of-sale fraud, including cashing counterfeit EU payment cards.

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. 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. Cyber-attacks in cryptocurrency markets undermines attempts to validate digital currency and impedes the introduction of insurance against digital financial theft.

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. 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. 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

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.

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. 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.

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%.

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. 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 centre 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.

HIGH RESILIENCE STANDARDS OF CLOUD SERVICE PROVIDERS

To be competitive in the public CSP (Cloud Service Providers) 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', 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.

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 datacentres 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 centres.

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.

Downtime for a CSP rarely translates to a shutdown 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.

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, 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.

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.

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. 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.

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.

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.

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. Insurance agencies have paid out Business Interruption claims specifically for DDoS and DDoS extortion attacks with pay- outs nearing half a million dollars.

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.

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 bank's 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.

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.

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

9.2 CYBER INSURANCE

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, with several analysts expecting by 2025 the market could be as large as $20 billion.

While this represents substantial growth, it remains modest in comparison with the overall commercial insurance market of $247 billion. 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.

DRIVERS OF GROWTH

A review of many 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 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.

The increased competition is having an impact, with rates reportedly down over the last 12 months as well as a 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 most premiums 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) continues 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%.

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.

Most 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.

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”– 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 modelled results within capital modelling 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.

9.3 CASE STUDY: 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 (released the previous August by ShadowBrokers). It mainly affected personal users, public sector organizations, and SME-sized 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 most 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.