ORIC INTERNATIONAL

TREND WATCH

VOL 1.3

Cyber Risk - Threats, Insights and the Future

INTRODUCTION

Ciaran Hosty
Risk Analyst

The ORIC International Trend Watch series provides an in-depth analysis of the key trends affecting the (re)insurance and investment management industries today.

Covering a range of themes from money laundering to model risk, Trend Watch looks beyond the high level data points to answer the 'So what?' question, carrying out detailed root cause analysis, highlighting common control failings and considering the effects of numerous regulatory, social and economic influences that impact both the frequency and severity of operational risk events.

We hope you find the analysis and insights in this report useful and whilst not designed to be a 'holy grail' for risk management practitioners, we hope this document gives you food for thought to better assess and mitigate operational risks in the future.

TREND IN FOCUS

CYBER RISK

An introduction to cyber risk

The total value at risk from cyber crime over the next five years was projected at US$5.2 trillion in a recent study conducted by Accenture and the Ponemon Institute. This figure not only underlines the sharp rise in cost of cyber incidents over the last decade, but it is also a recognition that firms and academics alike expect cyber risk to evolve over the next few years.

As firms invest millions to improve their security infrastructures, they are having to keep pace with cyber criminals who are constantly evolving. And this evolution is not just in the techniques cyber criminals employ, but also in the targets they pursue and the purpose of their attack. Over the last few years cyber criminals have widened their scope, with data theft no longer the only end goal. Increasingly, cyber criminals attempt to disrupt vital systems, attack data integrity and by doing so, tarnish the reputations of some of the largest financial organisations in the world. And whilst it's irrefutable that cyber criminals are mastering their art of deception and social engineering, ultimately the weakest layer of any security's infrastructure is the human-link. Despite this, many employees lack the appropriate training to identify and act on cyber-attacks, with regular phishing-tests often underutilised as a result of budget constraints in an already price-conscious environment.

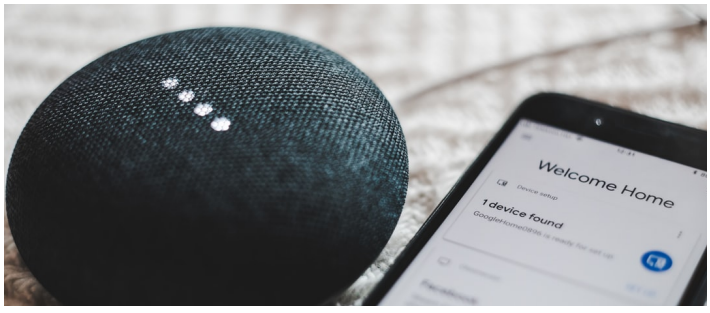
The challenge for firms now is embedding an effective cyber security awareness and identification culture amongst an increasingly flexible workforce (i.e. remote working) who have access to an increasing number of devices.

The Evolving Landscape of Cyber Risk

Use of advanced malware

The AV-Test Institute registers more than 350,000 new malicious programs (malware) and potentially unwanted applications (PUA) each day. In 2010, more than 47 million counts of individual malware were recorded, however, by 2019, this number has grown to more than 950 million. It's the reason why phishing remains one of the most successful tools for cyber criminals. With phishing kits increasingly available on the dark web, even users with very limited technical knowledge can now launch attacks. Furthermore, whilst most views on artificial intelligence and machine learning are positive, particularly for their potential to help organisations be more efficient in their processes and data analysis, artificial intelligence could also be utilised to write phishing emails that are indistinguishable from those written by humans. It's a very likely scenario and one that could bypass the basic filtering controls employed by many firms at present.

Internet of Things (IoT)



The explosion of the Internet of Things (IoT) industry means that there were more than 7 billion IoT devices worldwide in 2018 and a further 10.8 billion non-IoT devices. The number of IoT devices is expected to increase further to 21.5 billion by 2025 and consumers should be wary of the type of data their devices are capturing.

In May 2018, Amazon's Alexa made headlines after a private conversation between a couple in Portland, Oregon was recorded and sent to a random person in the couple's contact list. There is clearly an inherent trust that consumers place in products provided by Amazon and Google and these could be susceptible to hacking, not just to listen into private conversations but also used as an entry point to then infiltrate the wider network in which the device operates.

Naturally, firms should be very wary of these devices, particularly if they co-exist on the same network as company assets in a remote working environment. The challenge for firms is to ensure that networks are authenticated and protected with valid and unique machine identities (i.e. digital certificates and cryptographic keys which act as a digital handshake between devices) to eliminate the opportunity for unauthorised access.

Mobile devices

With many mobile devices now adopting extensive app stores, how can consumers be sure that companies have been stringent throughout their approval phase, particularly in such a lucrative environment whereby developers will pay substantial fees to have their application hosted in the store?

According to a survey conducted by RSA on the current state of cyber crime, mobile fraud is now larger than web-based fraud, with 80% of mobile fraud coming from mobile applications. It is not just sensitive personal information at stake here either, increasingly mobile phones form the second step in many two-factor authentications and therefore mobile device infiltration opens several security risk considerations for firms, including user lock-out and unauthorised access.

Social Media

It is estimated that more than 2 billion people actively use Facebook on a monthly basis, that's almost 30% of the world population. The platform is fee-free, easy to navigate and global which means it is the perfect playground for cyber criminals. Social media sites like Facebook allow cyber criminals to disseminate stolen financial information with relative ease, identify and contact key business stakeholders and provide tutorials on malware and hacking methods.

Social media is therefore a key source of reputation and data risk. Firms should actively monitor who has administrative rights to their social media platforms and remove those who are not active contributors. Non-active users are often those most susceptible to having their account compromised, potentially exposing sensitive information, particularly if a firm uses social media to interact and solve customer grievances and queries.

Cyber Risk Member Perspectives

Cyber Risk - A Member's Perspective

In October 2019, ORIC International asked three members to answer a short survey about their respective approaches to cyber risk and what the insurance and investment management industries can do to combat common challenges.

How are firms attempting to proactively monitor, assess and mitigate cyber risk?

Vulnerability scanning – An inspection of the potential points of exploit for a computer or network to identify weaknesses in security.

Penetration testing and 'Ethical hacking' exercises – Penetration testing is in some ways the active application of vulnerability scanning, where individuals will attempt to exploit weaknesses in a firm's security and relay the findings back to the organisation for control improvements/fixes.

Threat intelligence – Threat intelligence includes, but is not limited to, industry cyber threats and events (both current and emerging), types of actors and tools used and purpose of attack, i.e. what are cyber criminals trying to achieve. Threat intelligence should be an integral part of any cyber framework.

Engagement within industry and government cyber communities – Learning from your peers is vital and can save firms time, money and the heartbreak of implementing ineffective defences against cyber-attacks. The industry is facing the same problem, so there is power in working together.

Additionally, one firm is starting to draft target operating models based on both current and future threat landscapes which is driven by both internal and external (consultants, benchmarking) views.

What challenges are firms facing in their attempt to proactively monitor, assess and mitigate cyber risk?

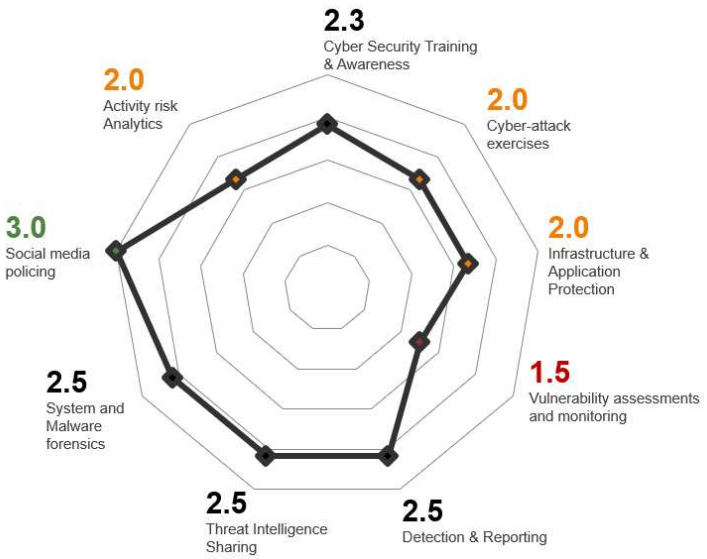
Surveyed firms identified the following challenges associated with monitoring, assessing and mitigating cyber risks:

- Ensuring timely triage of all related information and execution of mitigating actions.
- Ensuring that relevant functions within the firm who have responsibility for managing controls appropriately test their effectiveness so that any issues are identified as early as possible and changes to cyber risk ratings are updated and reported in a timely manner.
- Ensuring the effective co-ordination, assessment and management of sector-wide and supply chain cyber risks.
- Whilst the monitoring of cyber threats via standard indicators is useful and best practice, making this more meaningful for senior management and the board is a challenge – i.e. why should this be prioritised?
- Capturing information from critical outsourcers is often difficult and time consuming.
- Understanding new threats and ensuring these are appropriately considered as part of ongoing risk assessments.

> "**Mitigating** controls for all cyber risks are aligned with the NIST framework and these are assessed on an ongoing basis from a design and performance effectiveness perspective. Any controls deemed not to be fully effective have associated findings recorded with actions to remediate within agreed timescale" - **Surveyed participant**

Cyber framework maturity - Which areas of the framework are considered most mature and where is there still room for improvement?

Firms were asked to indicate which areas of the cyber framework were most reactive (score=1), progressive (score=2) or proactive (score=3). The responses were then averaged to reveal which areas of the framework were deemed least mature.



[Figure 1.1. - Responses of firms who described whether they were reactive, progressive or proactive were averaged with the average score detailed above. A average score of 3 indicates a proactive approach]

The responses revealed that social media policing was deemed the most mature part of the cyber framework with an average score of 3, implying firms took a proactive approach. The most immature area of the cyber framework was vulnerability assessments and monitoring with the majority of firms either carrying out periodic IT asset vulnerability assessments (reactive) or automated IT asset vulnerability assessments (progressive), with none of the participating firms carrying out tailored/integrated business process monitoring (proactive).

Activity Risk Analysis revealed that all surveyed firms were carrying out network and system centric activity profiling (progressive), but none of the surveyed firms were carrying out real-time business risk analytics and decision support (proactive).

Finally, surveyed participants had a progressive approach to cyber-attack exercises which include IT cyber-attack simulations, but none of the surveyed firms had a proactive approach involving sector-wide and supply chain cyber-attack exercises. The full list of reactive, progressive and proactive approaches to all nine indicators is listed in the appendix at the end of this paper.

How can firms better combat the challenges faced by the insurance/investment management industries?

There was a consensus from survey participants that there are opportunities to collaborate more as an industry on cyber risk, particularly with respect to threat intelligence (inc. risk events) and critical 3rd and 4th parties (particularly where similar parties are shared amongst the industry). This is vital to understanding the lessons learnt in other organisations and identifying emerging cyber threats.

Furthermore, firms identified that there was a need to develop an enhanced cyber awareness and training program amongst all staff, with a greater emphasis on malware identification and prevention.

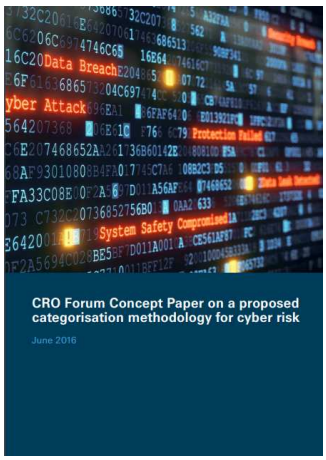
Threat Intelligence Sharing

- ORIC International captures cyber risk events as part of the loss data consortium and newsflash service. Firms should regularly monitor these resources to identify emerging cyber threats and review lessons learned.

ORIC International Data Insights

Between 2016 and 2017, ORIC International collaborated with the CRO Forum to develop an industry taxonomy for capturing cyber-related events. Subsequent to this, ORIC ran a cyber pilot which captured cyber-related events from several submitting entities (consisting of both ORIC and non-ORIC members). Not surprisingly, the results of the pilot revealed that the approaches to capturing cyber-related events varied greatly across the industry and there was a need for firms to develop, capture and assess a uniform set of metrics in order to best capture the essence of the risks faced.

Despite this, cyber-related events are still readily captured as part of ORIC's Basel-II taxonomy for operational risk and event learning should be used as an input into a firm's threat intelligence process that then feeds into the wider cyber framework. Analysis of cyber-related events allows firms to assess new or emerging threats, gauge possible impacts and the scope for loss, as well as review internal control environments. All this analysis should then feed into your firm's penetration testing to identify if similar vulnerabilities exist in your security and if so, what steps should be taken to correct this.



[Figure 2.1. - CRO Forum Concept Paper on a proposed methodology for cyber risk (June 2016).

Common themes in the ORIC dataset

In Q1 2019, a malware attack brought down the website and network of an ORIC member, impacting all head office systems. The event subsequently cost the firm more than GBP £4m comprising IT repair costs (£500k), project-burn costs (£2.5m) and lost revenue (£1.3m). The underlying cause was the exploitation of an outdated test server. This event highlights the importance of server management and in the wider picture an understanding of all assets within the business and how that asset fits within the wider network, i.e. actively (a laptop used by an active employee) or passively (a fax machine used for BCP purposes when primary infrastructure is lost). It Is vitally important that firms have a patching program in place that ensures all network infrastructure is reviewed periodically for having the most up to date software patching to limit the likelihood of exploitation by cyber threat actors.

£4m

in IT repair costs, project burn costs and lost revenue suffered as a result of an outdated test server

Ransomware, a sub type of more general malware, is also increasing in prevalence. In ransomware events, cyber criminals often prevent access to systems, encrypt/damage files or withhold stolen information until a sum of money is paid. In most of these cases, phishing emails are used and opened by employees, thus inadvertently infecting networks, drives and sensitive information. A number of these events exist within the ORIC dataset and whilst a lack of employee training on how to spot malware attempts was apparent, firms' reactive processes were generally good. Those firms who were able to isolate affected data quickly, had multi-layered security, and were able to recover lost data via the use of extensive and periodic backups were able to avoid losses.

Common themes in the ORIC dataset

Within the ORIC data, we've also seen an increase in phishing attempts whereby cyber criminals pose as senior members of staff, most commonly Board Chairs and CEOs. Often these emails ask employees to select a link to provide details which can be harvested, request funds to be sent or in other cases these emails are used as reconnaissance to establish whether a member of staff is inactive (e.g. on holiday, maternity/paternity leave, left the company). In these instances, members of staff should escalate suspicious emails to the IT team who can analyse common phraseology and versing and incorporate these into their spam filters. Furthermore, employees leaving the firm should have their email addresses closed in order to reduce the likelihood of an account takeover.

Finally, the inter-connectedness of a firm and its third parties should be constantly monitored. Firms who may share servers or files with a third party regularly should request confirmation and/or proof on a periodic basis that appropriate review and testing is being carried out on a third party's system infrastructure. The third party in this sense should be an extension of a firm's business, and their network and extensive due diligence should be carried out when on boarding any third parties to ensure they meet certain requirements relating to their system integrity and protection. We've yet to see many losses related to third party compromise, but we have seen near misses whereby firms have had their systems infected after a third-party hack, as well as denial of service attacks on third parties which have affected the operations of firms.

Risk event data from the ORIC International dataset is vital for allowing firms to understand the current landscape of cyber threats. Risk events should be routinely evaluated for root cause analysis, control failures and impacts in order to inform internal frequency and severity assessments of cyber risk events. Coupled with this, ORIC International members should make use of ORIC's recent Emerging Risk report to identify emerging cyber threats and their likely impacts and time horizon.

PREMERA BLUE CROSS AGREES TO $74m SETTLEMENT AFTER DATA EXPOSURE

What happened?

In 2015, Premera Blue Cross, a health insurance company based in Washington, United States fell victim to a cyber attack which exposed approximately of 11 million customer records. These records included credit card numbers, social security numbers and sensitive information relating to patients. It is believed that Premera Blue Cross may have fallen victim to the same hackers who targeted Anthem, another health insurer, who in February 2015 had more than 37.5m records stolen from its server. Premera was subject to a class action lawsuit in the U.S. District Court of Oregon, which the company later agreed to resolve by paying USD $32m. Throughout the lawsuit, the plaintiffs accused the organisation of 'wilfully destroying' evidence that was crucial for establishing accurate details in a security breach incident.

It was stated that the USD $32m would be used to provide cash payments for patients who file claims, as well as two additional years of credit monitoring and identity protection services. In addition to this, Premera pledged that it would invest a further USD $42m to fund a new information security program over the next three years.

ROOT CAUSES

It is believed that the Premera attack may have been a state-sponsored attack following the arrest of two Chinese men attributed with hacking health insurer Anthem. A security audit carried out by the US Office of Personnel Management in April 2014 revealed that Premera's security infrastructure was inadequate and the monitoring of cyber threats was minimal. Following the incident, Premera hired security firm Mandiant as well as the FBI to support its investigation which revealed 35 infected computers. The 35th computer allegedly contained evidence proving that hackers used customised malware to download sensitive data, however this computer was destroyed by the firm after being marked as an 'end-of-life' asset in 2016. It is believed that the 35th computer was a developer computer which afforded security clearance to Premera's most sensitive databases.

IMPACTS

Premera advised that they would be incorporating the following changes:

- Strengthening specified data security controls.
- Encrypting certain personal information.
- Increased network monitoring and logging of monitored activity.
- Annual third-party security audits
- Stronger passwords, reduced employee access to sensitive data and enhanced email protections.
- Moving certain data into archived databases with strict access controls.

RISK CATEGORY External Fraud / Hacking & Systems Disruption

TAGS Cyber Security; Cybercrime; Hacking; Identity Theft; Inadequate Internal Controls

The Future & Final Thoughts

Formal Data Privacy Regulation

In the last few years, the way data is used and the rights of the users that provide it has been subject to countless new regulations across the globe. And considering emerging cyber threats and the possibility of unprecedented data breaches, firms are having to conform to a new set of data regulations aimed at bringing consistency to regulation in a previously 'wild-west' landscape.

In Europe, the General Data Protection Regulation (GDPR) was introduced in May 2018, with violators facing the prospect of being fined up to €20m or 4% of annual worldwide turnover, whichever is greater. GDPR's main principle involves ensuring that the data subject has given consent to the processing of his or her data and could ask a firm what data is held for them. There have already been several high-profile non-conformities including, but not limited to, Google (GBP £44m) over lack of transparency in advertisement personalisation and British Airways (GBP £183m) after a data breach in 2018. GDPR also requires that firms report all data breaches to relevant regulators within 72 hours of the event, a significant undertaking for any firm.

In the United States, the New York State Department of Financial Services was the first state in the US to launch a cyber security regulation which requires CISOs to prepare an annual report that includes:

- An organisation's cyber security policies and procedures
- An organisation's security risk
- The effectiveness of an organisation's existing cyber security measures

California has since launched its Consumer Privacy Act, which, similarly to GDPR, gives residents of California the right to know what personal data is collected about them, what personal data is sold and to whom. It is likely that more states will adopt similar regulation in the upcoming months and years as regulators attempt to force firms to get a better grip and overview of the data they receive and use from their customers.

Conclusions

The cyber landscape is evolving. Cyber threats are becoming increasingly commonplace and financial services firms have the challenge of monitoring, assessing and mitigating a risk that is constantly changing and manifesting itself in different ways.

There is a need for firms to invest heavily in cyber awareness and training. People remain the weakest link in a security infrastructure and there is a need to enhance vulnerability assessments and monitoring through industry-wide sharing of information. This allows firms to better understand the threats and the lessons learned.

Third party risk should also be considered, and third parties should be seen as extensions of the business, with periodic confirmation/proof that appropriate review and testing have been carried out on third party systems.

Regulation worldwide will continue to drive better practices in data management and impose greater scrutiny on those that do not act in the best interests of their customers. This should play some role in ensuring firms continue to invest in infrastructure that treats customer data as a priority.

Bibliography

[1] The Cost of Cybercrime, Accenture Security, 2019 - https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf

[2] Insurance CRO Survey - Shifting from defense to offense, EY, 2018 - https://www.ey.com/Publication/vwLUAssets/ey-insurance-cro-survey-2017/$FILE/ey-insurance-cro-survey.pdf

[3] AV-Test, The Independent IT-Security Institute - https://www.av-test.org/en/statistics/malware/

[4] State of the IoT 2018, IoT Analytics, 2018 - https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/#targetText=The%20number%20of%20connected%20devices,laptops%20or%20fixed%20line%20phones)

[5] Hackers could use Google Home or Amazon Echo to listen in to your conversations, Tech Radar, 2019 - https://www.techradar.com/news/hackers-could-use-google-home-or-amazon-echo-to-listen-in-to-your-conversations

[6] The current state of Cyber Crime, RSA, 2018 - https://www.rsa.com/content/dam/premium/en/white-paper/2018-current-state-of-cybercrime.pdf

[7] 2019 Insurance Industry Outlook, Deloitte, 2019 - https://www2.deloitte.com/content/dam/Deloitte/us/Documents/financial-services/us-fsi-dcfs-2019-insurance-industry-outlook.pdf

[8] What is the NYDFS Cyber-security Regulation? A Cyber-security compliance requirement for financial institutions, Digital Guardian, 2019 - https://digitalguardian.com/blog/what-nydfs-cybersecurity-regulation-new-cybersecurity-compliance-requirement-financial

[9] Premera Blue Cross hacker victims claim insurer trashed server to hide data-slurp clues, The Register, 2018 - https://www.theregister.co.uk/2018/09/06/premema_breach_lawsuit/

[10] Machine Identity Protection for Dummies, Venafi, 2018

Appendix 1 - Cyber Framework Maturity

Participants of the survey were asked to identify where they were most reactive or pro-active in their cyber framework defined by 10 key indicators.

Indicator	Reactive	Progressive	Proactive
1	Acceptable usage policies	General information security training & awareness	Business partner cyber security awareness
2	IT BC & DR Exercises	IT cyber-attack simulations	Sector-wide & supply chain cyber-attack exercises
3	Ad hoc: Infrastructure & Application protection	Enterprise-wide infrastructure & application protection	Adaptive & automated security control updates
4	Periodic IT asset vulnerability assessments	Automated IT asset vulnerability assessments	Tailored/integrated business process monitoring
5	Security log collection & reporting	24x7 Technology centric security event reporting	Cross-channel malicious activity detection
			Global cross-sector threat intelligence

[11] Global Cyber Security Outlook, Deloitte, 2014

OUR RESOURCES

CONTACT US

Trend Watch forms part of ORIC International's extensive library of resources, which spans a number of key themes affecting the (re)insurance and investment management industries. In addition to this, ORIC International have a range of thought leadership studies, member-led surveys, working group and forum outputs and industry analysis.

If you are interested in getting access to these resources or have any questions about ORIC International and our services, please contact:

Ciaran Hosty
Risk Analyst

+44 (0)203 917 1733

ciaran.hosty@oricinternational.com

Chris Watson
Senior Manager

+44 (0)203 917 1735

chris.watson@oricinternational.com

Paul Dolman
Senior Manager

+44 (0)203 917 1736

paul.dolman@oricinternational.com

Follow us on LinkedIn
https://www.linkedin.com/company/oric-international.com/

www.oricinternational.com
enquiries@oricinternational.com
+44 (0) 203 917 1750
Find us on

Published by ORIC International. One America Square, 17 Crosswall, London, EC3N 2LB