Death by Cyber Attack

Web Cast Report July 2020

Introduction

This report is based on the ISITC EUROPE CIC webinar entitled "Death by Cyber Attack. The webinar was kindly hosted by the CISI and moderated by senior industry professional, published author, speaker and industry commentator Gary Wright, Director, ISITC EUROPE CIC. The speakers were [i]Aman Sood, Chair ISITC EUROPE Cybersecurity Forum and [ii]Jeremy Samide.

ISITC EUROPE CIC would like to thank Aman, who undertook to write up this document in conjunction with ISITC Europe.

About

The ability of cyber threats to compromise information systems is an ongoing danger to all organisations, an emerging threat presents a new challenge, cyber-attacks that may cause harm to systems with the potential to kill the business.

Financial services are amongst the most attractive targets for cyber attackers as industry reports rank FS as the premier industry risk. Adversaries offering their customisable malware strains or services-for-hire on the dark web are contributing to a rise in the adoption of more modern Tactics, Techniques, and Procedures (TTPs) by attackers.

Despite these acute threats, cyber security remains as much as a black art as a science with those who lead, manage and operate the business, delegating either internally to a select few IT security specialists or contracting with an external Service Provider. As with other strategic risks, this is an area that the Board and Management teams need to have a thorough understanding of.

IGNORANCE IS NO DEFENCE!

What Are Cyber Risks?

There are several cyber risks in existence today, which broadly speaking, could fall into 4 categories:

- Regulatory
- Reputational
- Operational
- Financial.

As our reliance and demand for robust, high-performing and flexible technology is significantly increasing, this has led to a sharp rise of cyber-crime across all industries, for every business, as well as individuals. However, cyber security risks are not purely technology vulnerabilities. Cyber spans across the entire business and at every technological, process or human touch point will lie potential risks which, when exploited, could seriously disrupt your organisation.

Never assume safety; today's Internet is a digital cyclone with highly sophisticated cybercriminals fast becoming well-organised and well-funded. Combine this with the increasingly new types of malware and the expansion of cheap hacking tools, it is easier today than ever before for cybercriminals to discover new target opportunities.

YOU COULD EASILY BE NEXT!

Who Is Responsible?

Cyber and information security is solely the responsibility of the technology departments, right? No - this is a common misconception! Cyber is the number #1 risk to any organisation, therefore it must be the responsibility of every individual to become cyber aware, in order for the organisation to remain as secure as possible. Think of cyber security as a "team sport", it is not limited to one department or one individual - every single one of us has a part to play.

Who Is Accountable?

Whilst responsibility sits on everybody's shoulders, ultimate accountability will fall on the Board of Directors. As the most senior level executives within the company, the Board supports and sponsors the cyber security strategy using a top-down approach. The Board should be aware of all cyber risks, their impact and likelihood, using that information to decide the risk appetite helping to formulate the governance and security culture, to permeate throughout the organisation.

'Most, if not all, organisations today are constantly challenged with balancing key business priorities and managing risks. This is especially difficult in today's VUCA World of continuous change. Managing cybersecurity is no different.'

What Is The Definition Of Cyber Risk Management?

Cyber risk is a highly complex, challenging function. It is very much a living, breathing 24x7 function, without a defined finish line. **Managing cyber security is like playing a game of whack-a-mole!** An overarching risk management framework and appropriate controls need to be implemented to mitigate against potential cyber risks.

How Much Will This Cost?

Unfortunately, cyber security cannot be solved with financial investments alone. It is an expensive function: technology, resources, education, 3rd parties, partner support, infrastructure, the list is endless. The firm should allocate an appropriate yearly budget to manage cyber security, understanding it is not a cost-centre. If managed well, it can become a business enabler and a differentiator in the market. Despite the high expense, the more secure an organisation can be can also prove to be a significant competitive advantage, increasing both viability and profitability. The cost of recovering from a catastrophic breach will, almost certainly, be astronomically more expensive than the initial investment.

Are Cyber Security Challenges For Asset Managers, Hedge Funds, Brokers Any Less Than The Big Banks?

Most, if not all, organisations today are constantly challenged with balancing key business priorities and managing risks. This is especially difficult in today's [1]VUCA World of continuous change. Managing cyber security is no different.

However, in smaller firms, the RTB (Run-the-Business) and CTB (Change-the-Business) functions are often intertwined, with the same group of individuals running the day to day BAU execution and performing the strategic, change innovations.

The smaller investment managers simply do not have the budgets, resources or skillsets to have the luxury of separate RTB and CTB teams. Often the in-house IT resource or external MSP, are expected to co-manage cyber security.

As Regulators such as the FCA and SEC are quickly prioritising cyber security assessments, smaller firms must treat cyber risk management separately to IT. Although there may be some cross-over between the functions, the IT teams will simply not have the resources nor the capacity to manage numerous cyber risks across the wider business. The small consolation is, however, the attack-surface of a wealth manager or hedge fund, is significantly less when compared to a tier-one Global bank.

Where Are The Biggest Attacks Coming From?

There are 3 levels of threat actors. Cyber criminals are no longer the one individual looking to create a little mayhem. Whilst those still do exist, the three levels broadly are:-

1) Hacker collective groups – anywhere from amateurs to relatively skilled, reusing tools readily available on the dark web
2) State-organised criminals – often Russian and Chinese groups, closely affiliated by state-sponsored organisations, can be self-funded
3) State-sponsored groups – purely state backed organisations, mandated to target large organisations.

[1] VUCA stands for Volatility, Uncertainty, Complexity and Ambiguity

Statistically, the FBI reported losses from cyber-attacks to be estimated at $3.5bn for 2019, up from $2.7bn in the previous year; the prediction being even higher for 2020. However, these figures are purely what has been disclosed.

In our estimations, however, the actual real number of losses is significantly higher. There are several organisations which have suffered a breach who are still dealing with ransomware and paying real sums of cash – *via crypto currency of course!* –as they find themselves in a compromised position attempting to recover from a cyber breach.

Is There A Time Of Year / Month / Week Which Is The Window Attackers Are Likely To Be Successful?

A highly sophisticated, targeted attack is often the result of deliberate reconnaissance, whereby the criminals have gained a foothold inside of your network, harvesting information and patterns over a number of months, to identify the most opportune time to launch an attack. This can be anytime, after-hours, on a weekend, or even Christmas day.

Back in 2013, a Friday-afternoon scam cost a hedge fund $1.2m and a CFO to lose his job. The financial chief received a phone call just as he about to head home. The caller claimed he was calling from Coutts, the hedge funds main bank, warning the CFO of suspicious activity which needed further investigation ASAP. Though the CFO was somewhat hesitant, he eventually agreed to create and share the access codes to cancel the suspicious payments.

By Monday morning, $1.2m (£742,000) was gone. The CFO was terminated due to *"breaching his duties and failure to protect the assets"* and was also sued by his former employer. The CFO argued no wrongdoing, denying negligence, saying he was acting in the company's best interests. Messy stuff! When you begin to look at the anatomy of this particular cyber-attack, it demonstrates why cyber security is a human risk. The criminals knew when to strike, understood the internal processes, and identified exactly who to call and when. Improved internal verifications, better user awareness training and tighter banking controls were absent. Although this was over seven years ago, many organisations today are still highly likely fall for the same scam.

What Are The Increased Cyber Risks Of Working Remotely?

Covid 19 has caused a sudden radical shift, globally, to many workforces now having to work from home. This has presented additional cyber and operational risks, as well as data privacy challenges, many of which are very likely to remain for quite some time. The ISITC EUROPE Cybersecurity Forum will discuss this topic in greater detail in the future.

In addition, we will also be discussing remote connectivity, technical infrastructure, policy & governance, staff culture, video-platforms, physical challenges and also some blind-spots which are always forgotten about.

As The UK Government Has Withdrawn Huawei From Its 5g Network, How Will This Impact 5g Going Forward:

Prudent decision for Governments to distance themselves from Huawei and their technologies. The People's Republic of China (PRC) has a long history of espionage and more specifically, a history of spying through technology manufactured in country.

The UK and other jurisdictional Five Eye (FVEY) countries in the 5G space need to focus on collaboration in order to compete and maintain an edge in the next frontier for telecommunications. As 5G emerges as the next generation of communications, it is important for the UK and its allies to come together to create a ubiquitous 5G network. Giving control to a state-sponsored country, such as China, carries an inherent number of risks and challenges for the UK and its allies.

The UK and other collaborative countries need to accelerate the development and implementation of its 5G capabilities in order to maintain its position in the global telecommunications stage.

How Do We Evolve Cyber Defences?

Cybersecurity is a critical business function. A continuous commitment towards cyber security is necessary for firms to continue to remain protected. Conducting risk assessments, developing a strategic cyber programme and strong incident response all help evolve the threat intelligence and improve reaction speeds.

Continued monitoring of the threat landscape to discover what threats are out there is critical. Enlist the help of a specialist that can educate your firm on the latest techniques, tactics, and procedures that are being used by cybercriminals to help proactively defend your enterprise.

About ISITC EUROPE CIC

ISITC EUROPE CIC is a totally inclusive, registered, not-for-profit Community Interest Company for all types of organisation within the Financial Services community. Its mission is to promote operational efficiency in the global financial markets through; Education, Innovation and Exchange of Information, via a program of events, publications and educational activities.

---

[i] Aman Sood has over twenty years' experience working within Infrastructure Technology and Cyber Security focused roles. He has held senior leadership positions within Financial Services, managing teams and building programmes within highly regulated organisations, such as Wadhwani Asset Management, Caxton Associates, The London Stock Exchange and Barclays Capital. Aman recently created a strategic Global cybersecurity roadmap for MeDirect Bank of Malta, to effectively reduce operational risk and strengthen cyber resilience, spanning across both 1st and 2nd Lines of Defence.

[ii] Jeremy Samide is a highly-sought after, global cybersecurity expert and speaker in the areas of cyber threat intelligence, next-generation security threats and cyber risk for governments, insurance, financial, healthcare, retail and legal vertical markets as well as family offices. As a trusted cybersecurity expert, Jeremy leverages his 18 years in cybersecurity supporting clandestine operations for the US Intelligence, Department of Défense, Federal Law Enforcement, allied foreign governments as well as the private sector advising organizations around the world on how to protect themselves.