MARSH & McLENNAN COMPANIES

Global Risk Center

EVOLVING CHALLENGES IN CYBER RISK MANAGEMENT

PROTECTING ASSETS AND OPTIMIZING EXPENDITURES

AUTHORS

Richard Smith-Bingham

Raj Bector

Claus Herbolzheimer

- ANTICIPATE TOMORROW'S THREATS
- INVIGORATE RISK ANALYTICS
- OPTIMIZE SECURITY INVESTMENTS
- MEET GOVERNANCE EXPECTATIONS

MARSH GUY CARPENTER MERCER OLIVER WYMAN

The integrity of corporate information technology (IT) systems is vital for business success. However, perfect cybersecurity can rarely be achieved without unacceptable commercial constraints, and companies that underestimate their risks or misjudge the effectiveness of their controls may endure significant operational disruption, financial loss, strategy compromise and reputational damage.

In October 2015, Marsh & McLennan Companies' Global Risk Center and Oliver Wyman worked with the International Risk Governance Council to bring together risk experts and cybersecurity experts from both industry and academia for a two-day workshop in Zurich. Under the Chatham House rule, the 35 participants discussed how companies can better protect core assets and optimize security expenditures against the backdrop of an evolving cyber threat landscape and skyrocketing costs.

This short paper contains our key takeaways from the event and additional reflections. For the full report and more detailed observations, please visit here.

THE CYBER THREAT LANDSCAPE IS BECOMING MORE COMPLEX...

Despite the recent surge in cyberattacks, companies should accept that the coming years will most likely bring an even greater rise in criminal activity. These cyber crimes will become manifest for a wider range of targets, with constantly shifting attack vectors and more sophisticated execution. Advantage will continue to lie with the "offense" rather than the "defense" due to technological innovation and the challenges associated with attributing attacks, accessing perpetrators and appropriately punishing them. No company will be below the radar, no company will be safe.

The agenda of cyber criminals will extend far beyond simple data theft as attackers continually re-evaluate the most rewarding and least risky ways of deploying their capabilities for strategic and financial advantage – either their own or that of their backers. Security threats will impact not just the safety of corporate and customer data, but also the resilience of product innovation, corporate strategy, physical operations and supply chains.

Two points of evidence stand out. First, the dark net is increasingly awash with commoditized attack vectors and payloads that enable opportunistic criminals to infiltrate companies with outdated defenses and weak capacities for detecting an incursion. This library of attack tools is lowering the bar for cyber criminals. Second, highly sophisticated, multimodal strikes targeted at specific corporate assets are becoming more common, with a rise in attacks that involve multiple phases of action and layers of deception to conceal both incursion and exfiltration.

The year 2015 will probably be remembered most for the revelation of large-scale data breaches in the US (think Anthem, the U.S. Office of Personnel Management and Ashley Madison). The year also saw a leap in the severity of Distributed Denial-of-Service (DDoS) attacks, with consequent business disruption. While these events will no doubt continue to occur in large numbers in 2016 and beyond, other types of incidents will probably rise in significance: corporate extortion hacks (threats to release customer or company data to the world if certain demands are not met); intellectual property theft (for use by a competitor); and data sabotage (where digital data is manipulated to compromise its integrity, thereby causing high levels of uncertainty).

Over time, we should also expect more cyberattacks that carry physical consequences, as hackers find a stronger rationale for undermining industrial control systems and exploiting the growing Internet of Things (IoT). Vulnerabilities to these attacks have certainly been demonstrated (recall last year's successful penetration of the Ukrainian power system and multiple hacks of connected cars), and this likely presages further incursions to come.

Any single attack may have any combination of the above characteristics. Indeed, the growing scope for contingent business interruption due to cyberattacks on third parties (such as supply-chain nodes or critical infrastructure) makes for a whole new set of risk considerations for companies. This all suggests that the risk for organizations operating outside the US will become more evident.

3rd

How large-scale cyberattacks rank as a business threat, according to executives in advanced economies

Source: World Economic Forum, Global Risks Report, 2016

Note: Focus was on global risks to doing business in their country. Cyber was the top-ranked risk in the USA, Germany, Switzerland, the Netherlands, Japan and Singapore, among other countries

BUT COMPANIES CAN INCREASINGLY OBTAIN A CLEARER PICTURE OF THEIR EXPOSURES...

Good situational awareness and cyber risk analytics are vital in helping firms identify weaknesses, rank threat scenarios, identify countermeasures and set priorities for intelligence gathering.

Too few companies have properly documented their core information technology assets – their databases, intellectual property or computing resources, for example. Without this information, it is hard to form a firm view on critical dependencies within the network for short- and long-term business success. A review of assets may also reveal parts of the network that are adding limited commercial value but giving rise to significant cyber risk.

Building on this, it is important to adopt the perspective of likely adversaries: What might they want, and why? How sophisticated are they? Many will just want to steal easily tradable data or siphon off funds. Others may scent more niche value in intellectual property, such as confidential pricing data and innovation research, or early intelligence on strategy direction, acquisition targets, decisive legal disputes or pivotal regulatory negotiations. A third group may want to cripple operations, either because they have an aversion to the company or to fulfill more strategic, if obscure, objectives.

Clarity on the company's assets and the possible ambitions of intelligent, adaptive adversaries helps focus analysis into where the firm might be exposed and the potential cost of that vulnerability. Establishing how easy it is to penetrate a company system – through its web presence, stolen mobile devices and emails via firewall breaches, encryption failures, the exploitation of privileged accounts and general network porosity – provides insight into how badly it might be compromised.

Understanding the scope of the threat is vital, but robust risk quantification is also essential for communicating risk, prioritizing security safeguards and allocating resources. For too many companies, this currently means little more than a heat map representation of potential damage, which is often misleading, as it combines frequent small losses with rare large losses for each type of incident in the form of a single expectation of likelihood and impact.

A more reliable and functional approach is to build distributions, or risk curves, from whatever company-specific and industry-wide incident data is available by means of a Monte Carlo simulation. This has a number of benefits. It helps companies understand the range of outcomes and associated costs for each attack vector on a probabilistic basis. Application across attack vectors makes it possible to compare the different cost profiles and to determine which are causing the most losses overall. It may transpire that attack vectors that are low on the C-suite radar are in fact more troublesome than those that are of high concern. Moreover, the ability to adjust cost and incidence assumptions in a transparent way gives risk managers the opportunity to future-proof analyses in the light of current known trends.

Not only can this type of modeling properly compare attack vectors on a like-for-like basis, it can also support the aggregation of all cyber risks to quantify impact at an identified level of confidence. This provides an analytical foundation for considering the acceptability of cyber risk levels for the firm and discussing the value of risk transfer and mitigation investments.

Scenario analyses can be deployed using the same modeling technique to examine extreme events and emerging threats for which little data is available and where "what if" type thinking is required to explore second- and third-order consequences, such as reputational impacts.

MAKING THE MOST OF AVAILABLE INTELLIGENCE

Good data is certainly a challenge, but more is available than ever before for careful use. Multiple reports and articles from the security industry and governments record attack trends, prevailing forms of malware, average corporate expenditures and incident costs. Insurers and brokers sometimes publish data based on trends in claims. Informal peer group networks in more cyber-mature industries shed light on emerging cyber threats in a noncompetitive way, as do industry-government forums. Individual security experts have compelling anecdotes based on disguised client experiences. The dark web is a valuable, if underused, resource for understanding criminal agenda and the price of traded items and activities.

Admittedly, all this intelligence needs to be calibrated. Some of it is overstated, partial or hard to access. Well-publicized attack vectors (such as customer data breaches) are not necessarily the most prevalent risk for a company, or the most damaging. Many mundane attacks are never reported, and rarely can one read articles about extortion attempts and critical infrastructure breaches, where there are vested interests in concealment.

The most cyber-mature companies are already mining their own data to understand what is driving the most risk. A well set-up cyber incident log linked to cost data can be the foundation for identifying the prevalence of attack vectors and the range of impacts from each. Tracking provides a lagging indicator of key threats and known tail events, and how overall incident numbers and costs have varied over time. While valuable, this historic data does not, of course, represent the full scope of attack types and possible damage in a constantly evolving threat landscape.

68%

Companies in Europe that have not estimated the financial impact of a cyberattack

Source: Marsh, European Cyber Risk Survey Report, 2015

Note: Survey of large and medium-sized corporations

ENABLING INVESTMENT DECISIONS THAT BETTER BALANCE SECURITY AND COMMERCIAL NEEDS...

Concern has risen among senior management and boards that higher budgets for cybersecurity are not necessarily delivering better corporate resilience in either the short or the long term. As cyber risk and associated expenditures are more visible at senior level, the situation is no longer sustainable.

The analytics referred to above offer a platform for assessing the value of different security safeguards. If, for example, it is clear that a certain countermeasure will impede the ability of an adversary to move through a network to find assets of interest, it should be possible to compare the cost of that intervention against the amount of risk that is reduced, and therefore against alternative expenditure options. In conducting such an analysis, it is important to assess whether there are any material second-order costs, such as constraints on commercial activity.

Likewise, and where appropriate, companies should bring cyber risk into the assessment of new commercial ventures, along with the consideration of other risks. If expected returns, taking into account mitigation costs, insurance premiums and residual risk do not meet the hurdle rate, investment might not justify approval.

Indeed, with cyber risk now presenting as a critical and expensive business risk rather than merely as a technological irritant, security efforts should be considered both in a strategic manner and on a risk-return basis. Solutions are imperfect, resources are finite, insurance capacity remains limited, and the threat environment is changing. Resilience options need to be prioritized with the right level of senior oversight and endorsement. It may be the case that firms have to accept a higher level of cyber risk if mitigation and transfer opportunities are limited or unaffordable.

Technologically, companies should at first aim to close vulnerabilities by putting current best practices in place. This can be achieved by compartmentalizing the network and instituting key security controls such as full disk encryption, whitelisting certain software, careful network monitoring, strong authentication, routine incident logging and periodic forensics. Strengthening corporate risk culture with regard to cybersecurity is also critical. Personnel should be encouraged to feel both more accountable and more empowered, actively supporting company efforts by adhering to company policy and also reporting suspicious website and email activity – without being blamed for flagging their own failures in meeting recommended security standards.

But just as technological barriers can often be penetrated by the most determined and sophisticated attackers, so human error is inevitable in the face of sustained attempts at deception. More importantly, a balance needs to be struck between short-term needs and long-term requirements – between pragmatic fixes and strategic solutions. Likewise, tradeoffs between security and business objectives are inevitable, which may also clash with expectations that personnel have of the company's IT infrastructure. The necessary outcome (at least in the short term) may be sub-optimal capabilities, slower product and service development, and more restricted network access.

32%

Increase in US-based Marsh clients purchasing cyber insurance H1 2015 versus H1 2014

Source: Marsh, Benchmarking Trends: Cyber-Attacks Drive Insurance Purchases For New and Existing Buyers, 2015

Note: Across all sectors. Greatest rises in Education, Power and Utilities, and Manufacturing

THEREBY ALIGNING THE ORGANIZATION EFFECTIVELY AND SATISFYING GOVERNANCE CONCERNS

It is widely understood in most industries that risk management should be a partner to the business as well as a control function. While front-line, risk-taking roles act as the first line of defense for risk management, risk managers need a risk-return mentality to appreciate the commercial imperatives that underpin the business. In the case of cyber, this becomes a three-way interaction additionally involving those responsible for information technology infrastructure. Each group must learn to speak the language of the other two to reduce friction and failed effort. Only in this way can companies develop a strategic approach to cyber threats that effectively balances security with commercial needs and that bases decisions on insights into the possible damage from action and inaction.

There is some debate currently about the optimal reporting line of the Chief Information Security Officer (CISO) – whether the role should report to the Chief Risk Officer, the Chief Information Officer or the Chief Security Officer. While organizational culture will always be a significant factor (and many firms do not have all these positions), the trend appears to be toward reporting to the Chief Risk Officer, especially in companies with a wide-ranging risk function. In our view, this is often helpful in aligning different capabilities and focusing on cyber as a risk to be dynamically managed rather than on security as an outcome to be delivered. Much is currently expected of the CISO and their tenure in a company is often short.

Better ex-ante justification of security investments may be the top priority, but ex-post monitoring is of increasing interest to support future decision making. Metrics and data that can show progress over time with regards to both incidents and their handling will be increasingly demanded by senior management and the board. Boards are gradually becoming more familiar with cyber issues, through greater prominence of the topic on meeting agenda and the recruitment of members with appropriate expertise. Gone are the days when IT could do its job largely unchecked by the C-suite and subject to minimal reporting requirements on operational issues. Transparency and effectiveness are now the order of the day.

As a result, these principles are informing governance beyond the individual company. It is almost ironic, given the nature of cyber crime, that information sharing – with company leaders, other companies, insurers and governments – is increasingly central to the development of cyber resilience. But a maturing dialogue is helping in a number of ways. Through it, companies can better understand how to allocate resources and identify risk transfer opportunities; insurers can provide greater coverage and protect themselves against accumulation risk; and governments can target policy efforts and strategic support more productively. We hope that our workshop with the International Risk Governance Council helped inch that conversation forward. But the challenges of building widespread resilience remain immense, and, mindful of one salutary observation from the event, “let’s not forget that bad guys have their conferences too.”

AUTHORS AND CONTRIBUTORS

Richard Smith-Bingham
Director, Global Risk Center, Marsh & McLennan Companies
richard.smithbingham@mmc.com
+44 207 852 7828

Raj Bector
Partner, Oliver Wyman, and a member of the firm's Strategic IT and Operations practice
raj.bector@oliverwyman.com
+1 (646) 364 8519

Claus Herbolzheimer
Partner, Oliver Wyman, and a member of the firm's Strategic IT and Operations practice
claus.herbolzheimer@oliverwyman.com
+49 (30) 399 94563

Additional insights came from Tom Reagan, Cyber Practice Leader for Marsh USA, and David Christensen, Cyber Risk Task Force Leader for Marsh UK and Ireland.

Marsh & McLennan Companies and Oliver Wyman are grateful for the opportunity to partner with the International Risk Governance Council on the workshop, which was additionally supported by Swiss Re and AXA Technology Services.

ABOUT

This paper was developed by Marsh & McLennan Companies' Global Risk Center. The Global Risk Center generates insights and explores solutions for addressing major threats facing industries, governments, and societies. Drawing on the combined expertise of our companies and in collaboration with research partners around the world, the Center aims to highlight critical challenges and bring together leaders from different sectors to stimulate new thinking and practices.

Marsh & McLennan Companies (NYSE: MMC) is a global professional services firm offering clients advice and solutions in the areas of risk, strategy, and human capital. Marsh is a global leader in insurance broking and risk management; Guy Carpenter is a global leader in providing risk and reinsurance intermediary services; Mercer is a global leader in talent, health, retirement, and investment consulting; and Oliver Wyman is a global leader in management consulting. With annual revenue just short of $13 billion, Marsh & McLennan Companies' 57,000 colleagues worldwide provide analysis, advice, and transactional capabilities to clients in more than 130 countries. The Company prides itself on being a responsible corporate citizen and making a positive impact in the communities in which it operates. Visit www.mmc.com for more information.

MARSH & McLENNAN COMPANIES