briefing note 366 March 2018

FS-ISAC 2018 Cybersecurity Trends

By Tahiry Rabehaja
Email: tahiry.rabehaja@riskfrontiers.com

Figure 1: Snapshot from the FS-ISAC report ranking the key priorities to improve cyber security postures in 2018.

2017 was not a good year for cyber security. Victims ranged from small businesses to corporate giants such as Equifax, Deloitte and Kmart with the impacts of 'improved' ransomware such as WannaCry and NotPetya just two well-publicised examples. Such breaches emphasise that cybersecurity poses not just a headache for IT departments but is an issue warranting a top-down solution, starting with C-level executives. To this end, the *Financial Services Information Sharing and Analysis Center* (FS-ISAC), have recently published a report summarising the thoughts of over 100 financial sector Chief Information Security Officers (CISO) regarding key priorities to improve digital security postures for 2018 (FS-ISAC, 2018). This survey shows most executives focused on improving their defensive strategies against cyber attacks.

[FS-ISAC is a non-profit global organisation providing a platform for sharing and analysing cyber and physical security information and intelligence. It currently has approximately 7000 members from 39 different countries. It was an initiative established by the financial service sector in response to the 1998 US Presidential Directive 63.]

For more than a third (35%) of the executives, improving employees' awareness about digital threats ranks top of the list. This comes as no surprise given employees have always been on the front line of defence against cyber attacks while remaining the weakest link. Indeed, most attacks against financial services companies exploit human weaknesses using social engineering, spear phishing and account take-over due to weak and reused passwords, etc. In 2017, Verizon reported that 1 in 14 employees were opening attachments or links sent through phishing emails and 1 in 4 were giving out account credentials or personal information (Verizon, 2017).

Investment into modern cyber resilient infrastructures (25%) comes in as runner up. Such an investment includes a progressive upgrade of existing network defence hardware and software as well as the creation of specialised departments that ensure digital information security.

Another recent study shows that subscription to Threat Intelligence, the emergent use of defence systems based on Machine Learning as well as strategic use of Cyber Analytics rank

amongst the more cost-effective security investments (Accenture, 2017). That same study shows many companies over-investing in technologies that fail to deliver the desired cost-benefit ratios. These include extensive applications of Advanced Perimeter Controls and incongruous use of data loss prevention such as full disk encryption. Thus, efficient security programs should be implemented by ensuring an optimal cost-benefit ratio. This can be achieved by prioritizing the security of critical assets and related infrastructures.

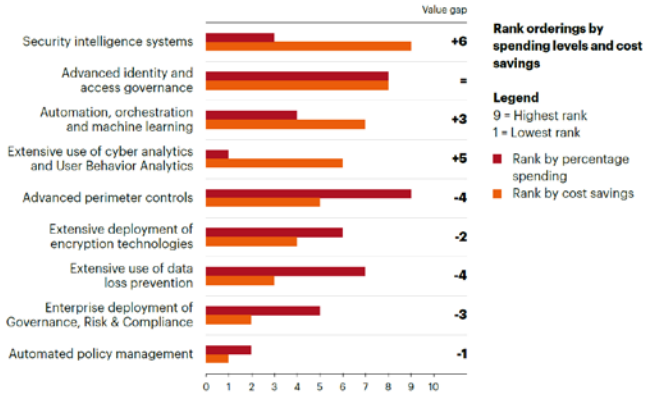

Figure 2: Snapshot from the Accenture report showing spending in security technology and the associated business benefit value.

2018 will also mark a long-awaited ratification of various breach notification regulatory laws. These include changes to the General Data Protection Regulation in Europe, the Notifiable Data Breaches scheme that has just come into effect in Australia, and upcoming changes to China's Cybersecurity and Data Protection laws. These entail that compliance, explicitly voted by 2% of the surveyed executives, will also play an important role in shaping digital security especially for companies dealing with personally identifiable information.

The focus towards defensive solutions (FS-ISAC, 2018) is disturbing. The report also investigates the impact of hierarchical organization on reporting frequency but nothing is said about responses. This may be due to the fact that those executives interviewed were mainly from the financial industry. However, historical breaches shows response is equally as important as is defence. In fact, it is very likely that a resourceful hacker interested in a particular asset of a certain company will be able to hack in and extract or destroy the targeted information.

Targeted attacks are amongst the most costly and usually affect critical assets such as Intellectual Property. A successful attack on these key assets can have destructive impacts on the victim's business model itself. Expenses incurred during a cyber event will span from direct costs -- forensic and remediation cost, customer protection, regulatory penalty, etc. -- to collateral damages -- loss of customers, damage to reputation and brand name, increased cost of capital, etc. These costs can be considerably reduced using efficient incident response and mitigation policies as well as cyber insurance.

The White House Council of Economic Advisers estimate the average cost of a breach to be as high as $330 million when an event negatively affects the market value of the victim (Advisers, 2018). For instance, Equifax's stock price dropped by more than 35% within 7 days of last year's massive data breach disclosure. The emergence of cyber insurance is anticipated to provide cover against some of the financial losses. Various vendors are already providing cyber insurance products and it is expected this market will grow to over $7 billion within the next three years (PwC, 2015).

References

Accenture. (2017). *Cost of Cybercrime Study*. Retrieved from Accenture: https://www.accenture.com/au-en/insight-cost-of-cybercrime-2017

Advisers, W. H. (2018, February 16). *Cost of malicious cyber activity to the US economy*. Retrieved from https://www.whitehouse.gov/articles/cea-report-cost-malicious-cyber-activity-u-s-economy/

FS-ISAC. (2018, February 12). *FS-ISAC Unveils 2018 Cybersecurity Trends According to Top Financial CISOs*. Retrieved from FS-ISAC: https://www.fsisac.com/article/fs-isac-unveils-2018-cybersecurity-trends-according-top-financial-cisos

PwC. (2015). *Insurance 2020 and beyond: Reaping the dividends of cyber resilience*. Retrieved from https://www.pwc.com/gx/en/industries/financial-services/publications/insurance-2020-cyber.html

Verizon. (2017). *Verizon Data Breach Investigation Report*. Retrieved from Verizon: http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/