Jersey Financial Services Commission

JFSC Cyber-Security Survey Results - 2017

JFSC Director General John Harris highlighted in his Dear CEO Letter[1] dated 22 February 2016, that the frequency, sophistication and impact of cyber-attacks is increasing. Such observations are consistent with and supported by assessments from other organisations such as The World Economic Forum who, in their *Global Risk Report 2017*, ranked a "massive incident of data fraud/theft" among their top five Global Risks in terms of likelihood.

46% percentage of UK businesses that had identified at least one cyber security breach in the last 12 months Source: UK Cyber Security Breaches Survey 2017	$21,155 the average cost of a data breach, per day Source: UBM Tech 2016 Cybersecurity Trend Report	$75.4 billion estimated worldwide spending on cybersecurity in 2015 Source: Gartner's Forecast Analysis: Information Security, Worldwide, 2Q15 Update	53 % of all emails are spam, a growing proportion of that spam contains malware. Source: Symantec Internet Security Threat Report, April 2017

When cyber-security incidents occur it is likely to be due, at least in part, to one or more of the causal risks identified in the JFSC's Risk Overview[2]. Firms with ineffectual or inadequate cyber-security therefore have the potential to give rise to some or all of the impact risks identified in the Risk Overview. Such risks can have a direct and negative impact, including customers being defrauded, firms suffering material disruption to their services or loss of control of confidential information.

The growing dependency on technology and adoption of cyber in all areas of daily life and business mean that cyber-security is likely to be an area of international focus for the foreseeable future. The Government of Jersey's draft 'Cyber Security Strategy'[3] highlights the importance of ensuring Jersey has, and maintains a reputation for, sound cyber-security. It is in recognition of the importance of cyber-security for Jersey and financial services in particular that the JFSC Cyber-Security Survey (the **Survey**) was run.

The Survey was based around the standards and principles set out in the US National Institute of Standards and Technology Cyber Security Framework and the International Organisation for

[1] http://www.jerseyfsc.org/pdf/JFSCCyberLetterFeb2016.pdf

[2] http://www.jerseyfsc.org/pdf/JFSC_Approach_to_Risk-based_Supervision_2016.pdf

[3] https://www.gov.je/SiteCollectionDocuments/Government%20and%20administration/C%20Cyber%20Security%20Strategy%2020170215%20VP.pdf

Standardisation ISO/IEC27001:2013. In undertaking the Survey the JFSC sought to:

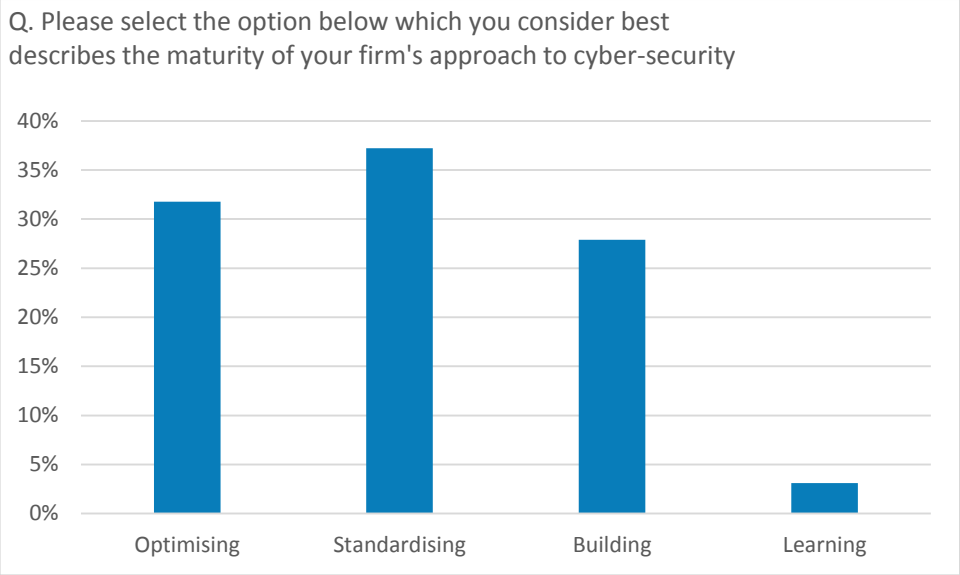
- build a picture of how cyber-security risks are being managed by firms and inform future regulatory activity in this area;
- provide useful feedback to industry; and
- provide useful information to industry on the types of incidents and threats being dealt with by firms.

This report builds upon and adds to the body of guidance issued by other supervisors around the World and the recent Cyber-Security Masterclass organised by the JFSC.

The JFSC would like to thank all firms who completed the survey and we would urge firms to use this report and the wider Survey results when considering their approach to cyber-security.

Cyber-Resilient?

The Survey sought to gain a picture of the overall maturity of respondents approach to cyber-security by asking firms to assess themselves against a simple maturity scale. Approximately a third of firms rated themselves to each of Building, Standardising or Optimising with a very small percentage assigning themselves to Learning.



The Survey covered a wide spectrum of entities in terms of size and regulated sectors and therefore a spread of maturity was to be expected. While recognising that the results are not necessarily representative of the industry as a whole, they suggest a financial services sector with a reasonably high level of cyber-security maturity. The expectation of the JFSC would therefore be that firms will be able to demonstrate a risk based approach to cyber-security, albeit one that is still developing.

An indication of the level of maturity can be seen in the relatively high proportion of firms (73%) who said they assess their approach to cyber-security against a published standard or framework. This rose to 94% for Banks, which compares favourably to a little under 80% of the Banks examined during the JFSC's 2011 Information Security Thematic who said that they benchmarked their information security policy against an international standard.

The following are the percentage of firms using particular cyber-security standards of frameworks

› 11% Cyber Essentials or Cyber Essentials+
› 36% ISO27001
› 8% NIST
› 17% other (often combination of different frameworks)

While investment in cyber-security can be expensive preventing incidents is often less expensive than responding to them and a high number of firms reported applying some or all of the controls identified in the Survey to protect systems and data.

94% applied one or more of the access controls in the Survey	92% have adopted one or more of the information protection processes or procedures in the Survey	95% had adopted one or more continuous monitoring techniques in the Survey

When considering protective controls firms need know what assets they have and, in recognition of finite resources, target controls towards those assets that are most important to protect. In order to ensure that information assets receive an appropriate level of protection the majority of firms (60%) reported having an inventory of information assets and knowing key data locations. However, only 44% reported that data applications and devices were prioritised based upon their classification of business value.

Case Study

A hacker obtained the username and password belonging to an employee. The attacker used this account to gain remote access to the group's systems and was able to obtain log-in details for an account with administrative privileges. The hacker then had up to five months access to the group's worldwide network and was able to access servers in multiple jurisdictions prior to detection.

The success of the attack above did not require the use of advanced hacking techniques and while additional controls, such as multi factor identification for remote connections might have prevented the attack and greater application of the principle of 'least privilege' to user accounts might have limited the access gained by the attacker, this example demonstrates that it will not always be possible to prevent attacks. Therefore to be truly cyber-resilient a firm must plan for cyber-security incidents.

The Ponemon Institute *2016 Cost of Data Breach Study: Global Analysis* looked at factors that can either increase or decrease the cost of a data breach and the factor that they found reduced the cost most was an incident response team.

The Survey results in this area would appear to suggest that a significant proportion of firms still have further room for development in order to be cyber-resilient.

32% of firms do not have a documented cyber-security incident response plan	40% of firms do not include responding to cyber-security incidents in their disaster recovery and contingency arrangements	63% of firms do not have a dedicated cyber-security insurance policy

The wide range of potential cyber-security incidents make it difficult to plan for specific incidents and at the point an incident is discovered the nature, scale and impact may be unclear. It also may not be possible to immediately identify how long an incident has been occurring, whether it is on-going, what caused it or what systems or data have been compromised. For example, 21% of respondents to 'The 2016 SANS Incident Response Survey' took between 2–7 days from the point of compromise or infection to incident detection and 11% indicated it could take 4 months or longer. It is therefore essential that incident response planning is able to respond and adapt to different types of incidents and is sufficiently flexible to respond as the scale of an incident changes over time.

An incident response team should consist of individuals from across a firm who have the capability to understand the issues and respond appropriately to the incident. Many firms will not have the specialist skills in-house for responding to an incident and the development of such capability may be uneconomic or impractical. In such cases firms should consider the types of external resource they may need to call on in the event of an incident. Such advisors might include IT experts with specialisms in cyber-security or forensic analysis but could also include software providers, lawyers or public relations firms.

The evolving nature of cyber-security threats means that incident and disaster recovery planning needs to be regularly reviewed. 64% of respondents to the Survey tested their disaster recovery on an annual basis and 23% said they tested their arrangements more often. When determining the frequency of reviews and testing firms should factor in the speed of evolution of threats in the external environment.

The potential complexity of cyber-security incidents and their impact on core business functions can mean that the time and cost of remediating incidents is significant. One approach to mitigate the financial impact is the use of insurance. Cyber-security insurance is a relatively new concept for many and the Survey results indicated that it is not something the majority of firms currently use.

Firms considering cyber-security insurance should first establish what, if any, coverage they have through existing insurance policies. They will also need to be clear about the coverage they require. For example, policies generally distinguish between first-party costs such as direct costs incurred by a firm when dealing with an incident and third party liabilities such as claims arising from a failure to protect the confidential information of others.

The Survey results show that cyber-security has a significant profile in financial services firms in Jersey

<table>
<tr><td rowspan="2">86%</td><td colspan="2">70%
of boards signed off their firm's cyber-security policy</td></tr>
<tr><td>66%</td><td>80%</td></tr>
</table>

of boards regularly receive reports on cyber-security	of those boards were involved in the development of the policy	of those firms review their policy at least annually

And the profile is rising:

31% of firms are still implementing or building their framework to manage cyber-security	68% of firms expect their spending to increase in their next financial year

Firms are also actively evaluating their approach to cyber-security

71% of firms monitor external threat and vulnerability intelligence sources

Respondents referenced a large number of intelligence sources for cyber-security. The organisation referred to by the most number of firms was the UK's National Cyber Security Centre 'Cyber Security Information Sharing partnership' or CiSP[4]. Also referred to were various national CERTs such as CERT-EU[5], UKCERT[6] and US-CERT[7]. Other sources of intelligence were software vendor websites, external IT and security service providers, social media as well as news and industry sites. The JFSC has also issued guidance to firms about cyber-attacks which contain valuable information for firms.[8]

Intelligence monitoring enables firms to protect themselves against known and new attacks such as the recent high profile ransomware attacks (Wannacry and Petya/NotPetya) experienced across the World in 2017. The monitoring of intelligence around such attacks enables firms to proactively take action to protect themselves by raising awareness amongst staff and adopting technical measures to remedy vulnerabilities to attacks.

However, sound intelligence can only be produced if information on threats is available which requires firms to share information and to report cyber-attacks to law enforcement, regulators and other relevant parties. It is therefore of some concern that the majority of firms (73%) reported not sharing information on cyber-security threats and vulnerabilities externally.

---

4 https://www.ncsc.gov.uk/cisp

5 https://cert.europa.eu/cert/filteredition/en/CERT-LatestNews.html

6 http://www.ukcert.org.uk/

7 https://www.us-cert.gov/

8 https://www.jerseyfsc.org/pdf/30-06-17_Press_Statement_re_Petya.NotPetya_Cyberattack.pdf

https://www.jerseyfsc.org/pdf/05-05-15_Press_Statement_re_WannaCry_Cyberattack.pdf

Jersey's draft 'Cyber Security Strategy' has a strategic objective to establish trusted information sharing and reporting mechanisms. In the meantime there are various governmental and industry bodies through which information can be exchanged and firms are urged to consider how they might share information externally.

Monitoring and testing

78% of firms perform regular automated vulnerability scanning and penetration testing to identify vulnerabilities	91% of whom conduct testing at least every 12 months with many doing so on a monthly, weekly or even daily basis

Case Study

Extract of results of an external security assessment of a multi-licensed firm by security consultants:

- Software update patches were missing which would enable an attacker to bypass security features in order to intercept communications.
- Over 50 employees were tricked in to clicking on to a malicious link in a phishing email and to enter their log-in details (some employees did this more than once). The absence of multi factor identification meant that with the details obtained it was possible to log-in, view and send emails from those accounts.
- A number of user accounts were identified as having the same passwords meaning that if an account with lower permissions was compromised an attacker could use the password to access accounts with higher permissions
- The firm had a flat network with no segregation making it possible to connect in a meeting room and then access the firm's entire network.
- A tester obtained unauthorised access to the building via tailgating and was able to move around the office unchallenged.
- Secure areas containing IT equipment were found unlocked with keys left in the locks making it possible to plug in malicious devices.

Firms' approaches are risk based

68% have a documented risk assessment process
90% of which use one or more of Threats, Vulnerabilities, Likelihood, Impact
However, only 43% of firms have a documented Risk Appetite for cyber-security

A firm that has established its appetite for a particular risk can compare this to its assessment of exposure to that risk. In cases where exposure exceeds appetite a consideration of the control environment may identify areas for enhancement, for example, supplementing technical controls by increasing staff awareness of cyber-security risks.

The role of people in cyber-security

A consistent factor in many cyber-security threats are the actions or inactions of people.

43% of businesses able to identify contributing factors for their most disruptive breaches identify factors relating to staff Source: UK Cyber Security Breaches Survey 2017	In 2015 60% of attacks were carried out by insiders Source: IBM 2016 Cyber Security Intelligence Index

While the focus is often on preventing malicious external attackers, the actions of insiders, both deliberate and inadvertent, can result in cyber-security incidents. This can clearly be seen from the top five threats identified by respondents to the Survey. Cyber-security breaches are often the result of or depend on employees clicking on a malicious link, acting on the instructions of a fraudster or being manipulated through social engineering into disclosing passwords or other confidential information.

Case Study

IT systems and software typically have a variety of functionality to assist users which can lead to data breaches.

In the case of email this can be functions such as:

- ‘Auto-Complete’ of email addresses
- ‘Reply all’
- The ability to attach and send externally large amounts of unsecured data
- Email chains containing confidential information

Employees sending to their personal email addresses confidential business or customer information such as customer lists, contact details and CDD documentation can also result in incidents. On occasions this has been with the intention of using the information in a new employment or even to provide services to a firm’s customers on the employees own account. Even where there may be no malicious intent such actions can place confidential information at risk and possibly cause firms to be in breach of their legal and regulatory obligations.

Another method by which insiders may seek to steal confidential information is the use of USB or other mass storage devices which can be used to download information from a firm’s systems.

While there are benefits to all of these functions there are also risks which firms should assess and manage proportionately through techniques such as email and system scanning and monitoring, restricted access/permissions, user education or, where appropriate, disablement.

Case Study

A Jersey regulated firm inadvertently transferred data relating to employees and customers to an unauthorised third party via an automated file transfer process.

The issue occurred as a result of an error by an employee with access permissions in excess of those that were appropri*ate* for their role.

Case Study

An employee of a Jersey based Fund Services Business received an email with an attached file which the employee opened. The attachment contained malicious ransomware which the firm only became aware of when corrupted files were discovered.

The firm immediately notified its IT service provider and recovered the situation by identifying the time at which the servers had become infected and switching to backup servers which were verified as being virus free.

In response to the issue an incident report was produced and steps taken to upgrade the firm's security measures including additional intrusion and integrity monitoring and email protections.

In response to these threats:

77% of all employees receive cyber-security training appropriate to their role	82% have a documented process for managing access for joiners, leavers and internal movers	85% have a process to manage access permissions for privileged users	87% of firms monitor their networks to detect potential cyber-security events

When considering cyber-security risk presented by people firms need to look beyond just their permanent staff and consider risks posed by contractors/temporary staff and customers.

57% of organisations consider that Contractors/Consultants/Temporary Workers pose the biggest insider threat Source: Information Security Committee on LinkedIn "Insider Threat Spotlight Report 2016"	63% of Banks believe that customers are the weakest link in their IT security Source: The Kaspersky Lab Report 2017 "New Technologies, New Cyberthreats

However, only:

40% of firms said all contractors receive cyber-security awareness training appropriate to their role	43% of firms provide guidance to external users on good security practices	41% of firms place contractual cyber-risk management requirements on service providers

Cyber-security cannot be addressed in isolation and firms need to consider all individuals who may have access to their systems which includes third party service providers, contractors and customers.

The percentage of firms providing guidance to external users on good security practices such as strong passwords, anti-virus measures and phishing awareness rose to 62% among those firms that provide services to customers through the internet and was a measure adopted by 88% of Banks. Providing guidance to customers seems most relevant for these types of firms; however, it is of note that 59% of firms reported having received a fraudulent email purporting to be from a customer in the last twelve months. There may therefore be steps that firms can take to educate customers on cyber-security which could also protect firms from threats being realised through their customers

Case Study

The private email account of a Jersey Trust Company Business' customer was hacked and fraudulent emails sent over two weeks requesting three separate payments all in excess of £10,000.

No call back was made to the customer to confirm the payment requests and when the bank queried the third payment, confirmation was sought and received from the customer by email.

A subsequent Internal Audit review of the incident identified a number of 'red flags'

- The payments were not in line with the customer's previous pattern of activity, being to unknown 3rd parties and unusual jurisdictions;
- There was a lack of supporting information to be able to fully understand the rationale for the payments;
- Bad spelling and grammar in the emails was out of character for the customer.

Although the firm had procedures for making payments including call backs and dual authorisations, none of the authorisers challenged the lack of CDD information or the lack of evidence of any call backs to the customer.

The fraud was finally detected when a fourth payment request was received and, alerted by the payment being to a high risk jurisdiction, the customer was telephoned and the payment request confirmed as fraudulent.

Conclusion

Cyber technology continues to be a fast moving and developing area where the opportunities are considerable and the threats numerous and diverse. Many of the advantages and convenience that new technologies provide to firms and their customers, through greater connectivity and mobility, may also increase vulnerability to those threats. Firms responding to the Survey that provide services to clients through the internet were significantly more likely to have experienced a cyber-security event than those that do not provide such services.

Cyber-security is often perceived as a technical subject (something to be dealt with by specialists). However, Boards should recognise that cyber-risk is an enterprise wide issue that can, and has to be, addressed at all levels together with other risk management activity. The Survey results illustrate this by highlighting the key role of people as a potential vector through which threats may be realised. Conversely, through a process of training and awareness raising people can also be a key part of a firm's cyber-defences.

The rate of change and number of potential threats mean that firms should be thinking in terms of "When" rather than "If" they have a cyber-security incident, to ensure they are in a position to respond effectively. The Survey results suggest that while firms have adopted a wide range of controls designed to prevent incidents occurring a significant minority appear to be less well prepared to respond to cyber-security incidents.

Best practice, with the aim of moving beyond just cyber-security and towards cyber-resilience, requires firms to understand where they are vulnerable and the threats they face, develop defences against those threats and plan such that they have the resources available to mitigate the impact of a cyber-security incident.

The following are a few high level questions Boards and senior managers might ask themselves when considering their firm's cyber-resilience:

- *Does the Board take ownership of and understand the critical assumptions underlying the firm's cyber-security strategy?*
- *Is one individual, with sufficient authority, knowledge, experience and resources, accountable for reporting on the firm's cyber-security? Does that individual have regular board access*?
- *Does the firm pro-actively identify and act upon cyber-security risk inherent in its strategy and structure as well as have a process for identifying and responding to emerging cyber-security risks?*
- *Does the firm have a cyber-security incident response plan which ensures a consistent and effective response to cyber-security incidents?*
- *Does the firm regularly evaluate its approach to cyber-security and its level of resilience to provide the Board with adequate assurance regarding the management of cyber-security risk?*
- *Does the firm have a process for identifying and taking advantage of cyber-opportunities?*

Limitations

- The Survey sample was made up of firms who were required to respond and those who responded voluntarily. The mandatory sample was selected in order to include a range of firms across the various regulated sectors. However, statistical inferences, margins of error and confidence intervals cannot be applied to this data given our sample was not statistically selected.
- 42% of firms completing the Survey did so on a voluntary and anonymous basis and it is therefore possible that those firms that chose not to respond may be substantially different from those that chose to respond.
- The conclusions in this report are based on the data available to the authors. All data is based upon the responses provided by firms and no attempt has been made to validate or seek evidence for the responses given.
- The JFSC cannot accept any liability for reliance by any person on this report or any of the information, opinions or conclusions herein.
- Third party sources are quoted as appropriate and the authors of the report are not responsible for the content of the external sources including external websites referenced.