CRIF Submission to the BIS Call for Evidence:

Cyber Organisational Standard

Executive Summary

Cyber risk is a major problem to global business. In the UK the figures vary, but without doubt the standout figure of the overall cost to the UK economy from cybercrime is £27bn per year, reported in 2011, has got the attention of UK Government and UK Business of all shapes and sizes. The Cyber Risk & Insurance Forum (CRIF) was setup in 2012 to help demystify the world of cyber risk and the need for more guidance to organisations and awareness of the issues from micro to global enterprise. The industry forum has representation from leading global insurers and technology brokers, IT assurance leaders, business continuity experts and specialist brokers. The CRIF community and brand has grown over the past year and been involved in discussions around cyber security within UK Government and also wider industry.

The search and selection of a cyber organisational standard by Business Innovation & Skills (BIS) will not be an easy task if the onus is on trying to find a single standard. There is no current standard or specification that meets that criterion or the wider indicators BIS are looking to promote. The intent for any organisational standard should be outcomes based and not a tick-box or a controls heavy assessment. CRIF have outlined their framework approach in this paper, along with themes that a cyber underwriter would look for in the search for a 'good risk', to understanding and addressing the primary cyber risks facing UK business. This framework brings together the world of information assurance and commercial insurance through the facilitation of good risk management.

The role of cyber insurance within an organisations' overall risk strategy and risk appetite needs to be explored. The facilitation of transferring the business risks to this type of product can only be made if the residual risks are known and quantified. Good risk management looks the same in a small business as it does in a large business i.e. it empowers the organisation to make the right decisions about their business so that there is growth and profit. By working through the **Protect>Detect>Respond>Recover>Residual** model, each organisation can measure their IT expenditure, re-align that profile if the 'realisation point' is too heavily dependent on traditional security, and focus on remaining agile in a turbulent market-place.

Introduction

Risk managers, information security practitioners, and continuity specialists all have an appreciation of data assets and their 'currency' to the business. However these approaches are sometimes operated in silos and only converged by the business when there is a need for attaining compliance or for responding to an incident. What the approach below, outlined by the Cyber Risk & Insurance Forum (CRIF), aims to demonstrate is that the risk management domain is intrinsically linked to the successful identification, quantification, management and transfer of cyber risk to cyber insurance.

CRIF have a view that each organisation, regardless of size, should know how to identify their business risks. Therefore our model focuses on the 'what you do today' and drives out the outcomes for 'what you should do tomorrow'.

The CRIF - Cyber Risk & Privacy Framework©

The diagram above demonstrates the innovative organisational approach to managing cyber risk – regardless of the size of that organisation.

Protect and Detect Phases

The traditional phases of **Protect** and **Detect** are where organisations outsource their security requirements to a managed security provider, build an in-house team, or have a trusted independent IT guy they can call if the worst happens. Each of these approaches needs to be cognizant of the changes to the threat actors, their motivation and techniques and how social technology has rapidly altered the attack surface for cyber.

The challenge business owners, risk managers or security managers have in this phase is identifying how best to spend their traditional security budgets e.g. do I keep buying more security technology to tackle the expanding cyber threats or do I look at culture, awareness and training in parallel. UK Government has issued some good guidance in this regard through the BIS Top 10 and the CPNI Top 20, but are these simply viewed as controls and measures of 'what does good look like' or do they actually map to business value and recognised benefits e.g. do X and you will benefit with Y.

Security standards and the wider organisational standards approach to cyber is gaining momentum but they need to be applied where applicable. For example a typical SME will not entertain the lifecycle journey that is ISO27001 but neither should they ignore the threat of cyber to their business. Any standard when applied in principle or taken through to accreditation does help you identify what your security gaps are and the controls that need to be applied to bring you up to 'good standing'.

Attaining a standard can sometimes give an organisation a false sense of security because it doesn't make you bullet-proof. In fact, keeping the standard and maintaining good security practice is where the real work starts. By assessing your cyber risks and the overall level of maturity against the various published cyber controls, there is an ability to understand your posture and understand what can be done to combat cyber, what investment is needed and where the real gaps lie in people, process, technology and partner. This is what we call the '**realisation point'**, and we find that this crossover between 'keep doing the same, but more of it', against 'do things differently and re-invest your security budget for cyber' is what adds the most value to an organisation. The realisation point is typically between Detect and Respond phases.

Respond and Recover Phases

It is safe to say that without reviewing your cyber risks [via a formal risk assessment] and the appropriateness of your security controls, processes and procedures, then your organisation will not be best placed to **Respond** or **Recover** (R&R) from a cyber attack or data breach. Essentially if you don't **Protect and Detect** effectively i.e. commensurate controls to protect your business assets, then there's limited opportunities for the organisation to actually respond to the cyber attack because you won't know it's happened or still happening. Typical attributes of an adequate Respond strategy are having formal relationships or capability around forensics, crisis management, cyber incident response and first responder training.

Consequently, it's the R&R phases that cause UK business the biggest pain as this is where specialist skills are required and business buy-in that a cyber problem actually exists and the removal of the **'it won't happen to me'** mentality. It's also where the largest proportion of hidden costs (£) are for a business e.g. lost website sales due to a DDoS attack or change in processes and education due to a data breach. A business should not underestimate the total cost of managing a cyber incident, or the impact such an incident may have on its brand, its reputation in the market-place and its customer loyalty.

As with other more traditional forms of risk, organisations need to quantify the impact on its business and its ability to continue normal operations when faced with a cyber-related incident. Part of that quantification process is to identify the likely costs to the organisation, be they legal expenses, potential liabilities, customer notification and public relations (PR) in the event of a hack of personal data, or loss of revenue, increased costs of working and reputational harm in the event of a critical network failure.

It is also important for organisations to understand the possible frequency of such incidents as persistent problems can considerably increase costs and result in greater damage to reputation. Frequency of incidents is also a key concern for insurance underwriters so must form part of any risk assessment.

Only once this exercise is complete can an organisation truly examine its risk appetite in this area and discuss internally how the risks can be mitigated through additional spend on IT services, infrastructure and network security, how much of the risk the business is willing to retain and the possibility of risk transfer through insurance, including being able to determine adequate limits, risk retentions and of course budget for insurance premium.

A cyber risk assessment standard or framework would greatly assist organisations in the all-important quantification process but any such standard or framework would do well to consider that organisations cannot be easily placed into "typical" brackets or categories by their size or industry. Such quantification analysis would however bring a deeper understanding of the often unique risks faced by different organisations and help highlight those risks in a much more coherent fashion to Senior Management, audit and compliance and the insurance industry.

Residual Risk – what does an insurer provider look for?

The questions or elements of an organisation that a cyber underwriter [normally through client dialogue with a broker] would look for to assess the cyber risks are very similar to the risk approach stakeholders' named above would consider. The main purpose of the residual risk exercise is to understand what liability an organisation can insure and how that risk transfer translates to better risk management.

Whilst there are various approaches to underwriting network integrity and privacy exposures, most underwriters attempt to obtain a technical understanding of the flow and type of data, the criticality of a network and the risk management applied. This will enable the insurance market to appropriately discount premiums and improve terms of the contract for organisations that have spent time assessing and understanding the risks to its business and can demonstrate incremental improvements to its network infrastructure, testing environments and employee and vendor management.

"Best Practice" to an insurance market will often incorporate the corporate culture of awareness and best practice rather than only a mapping process to any given "standards". Many standards currently deemed to be in the "cyber" arena less focussed on handling reputational impacts, quantification and understanding of exposures or all-encompassing from an information assurance rather than simply an IT security perspective. Furthermore, there is less focus on the delivery model best practice into the organisation which is imperative to underwriters wishing to see a cultural mentality. Training, delivery and the potential for audit and accreditation by third parties will make the "standards" approach more robust. With insurance coverage responding to the "insider threat" (whether malicious or negligent) as clearly identified by many empirical surveys the focus on culture will only grow.

Whilst a proposal form is the typical manner in which to obtain high level information, the following themes (not exhaustive) can be expected to improve the countenance of the risk faced by underwriters:

The typical questions are as follows: -

- Staggered Expectancies – "Benchmarking"
    - SME
    - Large or Global multinational

Insurers should at all times take into account the commercial realities of the costs for higher risk management within an organisation. Therefore it may be typical for companies to be benchmarked against each other within certain industry sectors or revenue thresholds with regards to IT spend and

quality of risk management. A small law firm would not be expected to have the same standards as a large bank, despite the exposures to that business. However underwriters must bear in mind that such decisions can lead to insurance profitability being marginalised as often small businesses have a higher frequency of small claims, and large businesses having fewer claims but of a more 'catastrophic' nature. To ensure the insurance risk transfer process works for business insurers must ensure policies are adequately priced whilst taking account of the clients' ability to pay for the insurance. Any use of a delivery model for the incorporation of standards and best practices within a business which can map one organisation against its peers (complex in theory) will assist in this regard.

- Quality of Risk Management
    - Generally (non-silo)
    - Specifically (Standards, PCI, Vendor Management etc.)

The risk management approach is to be considered from both a Specific of "technical" perspective and also from the General co-ordination and approach to risk within an organisation. The General approach includes ensuring that a company operates in a "cyber-savvy" manner by way of not throwing the burden of cyber/data risk management upon one individual silo but to ensure that legal, compliance, marketing, the Board and IT (amongst others) are all in discussion and aware of their roles and responsibilities. The Specific risk management an insurance market will look for are typically more aligned to the compliance, legal and IT functions and are inclusive of documented policies and controls, the awareness of appropriate standards or certifications and the management of exposures arising from third parties.

- Focus on data
    - Type, Security, Distribution, Points of Access
    - Policies & Controls

Liabilities arising out of data breaches, or indeed first party damage to an Insured, are rarely perfectly aligned to the turnover/revenue of a business and the exposure is better matched to the quality and type of data, an analysis of the points of failure and the protections in place.

- BCM, Incident Response, Security Policy, Privacy Policy
    - "on the ball?" e.g. Cookie policy

Aligned to the quality of risk management are the quality of policy and procedure around privacy and security matters and the robustness of contingency plans. However, insurance markets will be aware of documents that are produced that are not tested, updated or fit for purpose. The use of a downloaded template which has been vaguely tailored to an organisation is easy to spot for a seasoned underwriter. Furthermore an underwriter can be impressed if a client has policies in place that might go above and beyond the standard "set" of policies that may be seen amongst the company's peers, e.g. Cookie policies or Bring Your Own Device policies for smaller businesses.

- Industry Sector

Much empirical data on claims history in this area of insurance is still closely aligned to the threat environment and "typical" exposures of various industry sectors. A financial institution, telecommunications company or critical national infrastructure obviously considered having a higher

exposure base than a cash-only company or B2B. Broad assumptions should not be made by the insurance market but their data will often be driven by such a split.

A key issue however is how large organisations interact with smaller organisations through supply chains and how a breach of personal or business confidential information or a system intrusion or critical failure could be the result of poor practices at the smaller partner organisation.

- Revenue

Considered of more importance to some underwriters than others, the revenue can still be a useful guide to the potential exposures whereby larger organisations are more visible targets, have more data of value and potentially larger quantum of exposure or loss.

- Network Dependency
    - Online revenue? Critical infrastructure?

As with the discussion on Data above, the ability to correctly underwrite business interruption losses following a network integrity issue must focus on the dependence and type of network in place. Many organisations are critically dependent upon IT infrastructure without necessarily selling products online due to procurement, supply chain, logistics, computer aided design and manufacturing, to name but a few.

- Operational Jurisdiction
    - E.g. USA? Spain?

The privacy and security liability exposures to an Insured are very much dependent upon the geographic scope of their operations and the jurisdictions under which organisations find themselves accountable. The regulatory environment of the USA at a State level and with regards to federal healthcare legislation, combined with the aggressive plaintiff bar, naturally lead to a higher degree of exposure to those with operations in the US. Another example might be that of the Spanish regulator for privacy breaches being funded by the fines it issues which leads to a more volatile risk environment.

- Relevant Laws & Regulations
    - Telco? Data owner or data processor?

Any industry that may attract greater regulatory scrutiny or be subject to additional legal requirements will attract a more significant underwriting premium but also will be expected to have strong risk management.

- Claims experience
    - No claims vs. managed to success

It will not be well accepted by the insurance market if companies falsely state that they have had no circumstances or possible claims that would have been covered by cyber insurance. The majority of companies, even SME's, face attacks from external threats annually if not weekly or daily. It provides greater credibility if the risk environment of an Insured's business is known, rather than management being oblivious of matters that have passed. Issues that have been managed to success will be

underwritten to the advantage of the Insured for the most part over statements that there have been no claims.

- Visibility/Exposure
    - Crime/hacktivist/plaintiff bar threat

Certain businesses have a greater visibility than others to the “threat” environment. Large businesses may gain the attention of the plaintiff bar due to the deep pockets of the company. Companies supporting large events, holding themselves out to be of outstanding security or of questionable ethical standing may be the targets of “hacktivist” organisations. These matters will be considered by insurers.

Conclusion

Any cyber standard of framework would be well minded to strongly consider the motivational drivers for organisations to implement recommendations and best practice. The cyber insurance market may act as one driver if it were able to offer cheaper premiums where organisations had acted beyond what might be expected of a similar organisation according to the standard or framework. Incorporating quantitative measurements of potential exposures and frequency at an organisation-specific level will also drive further investment in improved best practices as the CFO, CEO and others within the organisation will be able to more accurately understand what risk management and insurance might actually be worth.

Whilst cyber insurance is somewhat nascent to UK/EU markets as opposed to the US market, what CRIF has seen over the last 12 months is more organisations enquire and take up cyber insurance to manage their residual risk. At the SME sector, new products and affordable premiums are being launched constantly so that the ‘pain and doubt’ around cyber is alleviated. For larger organisations, the BIS Cyber Organisational Standard if followed would no doubt lead to a reduction in premiums if cyber assurance can be demonstrated.

About the Authors:

==========

Daljitt Barn is the chairman of the Cyber Risk and Insurance Forum (CRIF), and Associate Director at NCC Group plc.

At NCC Group, Daljitt works directly with insurers, brokers and systems integrators on various areas relating to Cyber Security and Information Assurance. Daljitt has considerable technical and market expertise that has helped many organizations develop integrated operational and business controls to deliver cyber resilience.

Daljitt previously worked at BT, Capgemini, Fujitsu, EDS and HP in a multitude of information security roles; specialising in security strategy, architecture, risk management and business development. Daljitt is CISSP certified.

==========

Matthew Hogg, Vice President of Liberty Specialty Markets, is also the vice chair of the Cyber Risk & Insurance Forum (CRIF).

His division underwrites specialist risks in the classes of intellectual property, reputation, cyber, privacy and non-material damage business interruption.

Prior to joining Liberty, Matthew was the EMEA Technology Leader for international insurance broker Marsh and before that an underwriter at Lloyd's of London where he created a number of niche products in the intangible assets space. He holds a degree in law, a Masters in Law & Economics and an Advanced Diploma in Insurance.

Matthew is also Chairman of the Risk Committee of the Intangible Asset Finance Society (IAFS), on the Membership Committee of the IAFS, a member of the Information Assurance Advisory Council (IAAC). He is also an Associate of the Chartered Insurance Institute. Matthew is also the recently past Chairman of the UK charity BELS (Business & Education for London South) where he remains a trustee.

==========

Iain Ainslie, is an underwriter at ACE European Group where he is responsible for Technology Professional Indemnity, Cyber and Privacy Insurance, predominantly for the UK, Ireland, US & Canadian markets albeit with a worldwide territorial scope.

Iain is a Certified Project Manager and a Master of Business Administration (MBA) and has worked in the London Insurance Market for more than 27 years, 21 of which were within information technology where his roles included application development, project management, infrastructure management, Head of IT and consultancy.