Setting professional standards for cyber risk management

Why recognition is needed for cyber security professionals and why companies need the assurance of a quality professional standard

By: Andy Watkin-Child

Cyber, cyber security and cyber risk management regularly make the headlines in the context of countries hacking countries, data breaches, states and companies being held to ransom and individuals having personal data stolen. Cyber is a complex risk to manage. The World Economic Forums (WEF) annual report of global risks identified cyber-attacks as one of the top 5 global risks for good reason. It is a diverse risk which touches society in many ways. The NATO alliance positions cyber as a legitimate weapon, sitting alongside conventional military assets, and nation states use cyber as a tool to target national infrastructure such as power networks. Cyber is a well-funded criminal activity, with the global cost of cybercrime estimated to be approaching $1trn a year. The NotPetya attack in 2017 caused heavy corporate losses, Maersk reported that the cost to the company following the attack was around $300Mn and Merck over $2Bn. Cyber has had an interesting relationship with M&A, with both Marriott Hotels being impacted following their acquisition of the Starwood and the Verizon Yahoo deal, which dropped the acquisition price by around £350Mn. Cyber has also been a contributory factor in a class action lawsuit launched on Fed Ex; investors claim that the board miss-led shareholders on the impact of NotPetya on TNT Express, acquired by Fed Ex in 2016. A ransomware attack in March 2019 on Norsk Hydro is reported to have cost the company in excess of $75Mn and 2019 has to date been the worst year on record for data breaches.

The systemic nature or cyber-attacks, the complexity of cyber risk management and a lack of corporate focus on cyber risk management has led governments globally to respond with tougher regulation. The European Union's General Data Protection Regulation (EU-GDPR) was enforced in 2018 and has resulted in some notable intentions to fine for British Airways £183Mn and Marriott Hotels £99Mn. Equifax recently agreed to pay out $575Mn to settle outstanding claims in response to their hack in 2017. Cyber has had a noticeable impact CapitalOne reported a data breach in July 2019, setting aside $150Mn to compensate clients and manage the legal response. The Security and Exchange Commission established guidance in 2018 requesting companies to inform the markets of material cyber risks. Congressional members are pushing through the 'Cybersecurity Disclosure Act of 2019' to amend the Securities and Exchange Act of 1934 with the aim of mandating boards to have cyber aware executives sitting on the board table.

There are substantial costs to fix the fallout of a cyber-attack, such as communicating to and compensating customers, lost sales, associated brand and reputational damage, regulatory and on-going legal costs and the unpredictable impact to future profits, creating financial uncertainty which can last several years. There is growing evidence that a cyber-attack can have a material impact on the share price of companies affected. The credit rating agencies now include in their evaluations the potential impact and effectiveness of cyber security. There is an additional burden to the balance sheet when a company has to include provisions for the costs to implement the appropriate level of cyber security following a successful attack. It is reported that Equifax are spending $1.25Bn to fix security issues following their 2017 incident.

The evidence demonstrates that the consequences of a cyberattack are far reaching, complex and expensive to manage. That the corporate focus on cyber risk management is low, that financial markets want boards to clarify their approach to cyber risk management and there is a high probability for more costly cyber regulation. The challenge all boards face is how will they address these concerns?

Traditionally cyber security has been treated as a technology issue. It is not, it is a board-level shareholder value issue. We live in a global, digital and data dependent economy, where data touches all aspects of corporate operations, this makes cyber risk management an enterprise wide risk. Wherever data is required there is a cyber risk to be managed and the board has the collective responsibility for data management and security, one which is generally delegated to the Chief Information Security Officer (CISO). A question for boards is how do they place assurance that the CISO is able to take on such a complex role?

Cyber Security qualifications?

There are a broad range of cyber related security qualifications, with some mature certifications and some new entrants. At the time of writing there were over 120 qualifications licensed through a mix of schools and universities,

vendors, associations and government agencies. Representing generalist certifications aimed at security practitioners and security management; specialist qualifications; or industry related qualifications for example in the healthcare sector. All achieved through a mixture of examination, classroom and remote learning. Not all qualifications require continual professional development, or a practical assessment of their application in the context of the business environment. There are no universally agreed qualifications for cyber security, and it is difficult to identify which are the most appropriate qualifications for cyber leadership. With no universally agreed professional standards I believe this makes it difficult for boards to identify whether their security teams have the appropriate skills.

Why are professional standards important?

Many professions set standards for membership which in general require approved academic qualifications, competency assessments, oversight within the work environment and continual professional development (CPD). Some professions require registration in order to practice: to be a practicing solicitor in the UK you must be member of the 'Solicitors regulatory body', who require its members to have completed the appropriate academic qualifications, have met additional professional standards and undertaken practical skills training with a qualified solicitor. Legal entities in the UK are required to have qualified accountants and audits of UK legal entities cannot be completed unless the auditor holds a certificate from a recognised professional body. For doctors to practise medicine in the UK they must be registered with the General Medical Council (GMC), demonstrating that they have acceptable medical qualifications, practical skills and capabilities. For professions like engineering, human resources, architecture, nursing and teaching membership of professional bodies is either required or recommended to practice or operate at the highest levels.

Professional bodies set the bar for professional standards, which are independent of academic institutions and organizations. They level the competency playing field, setting holistic international and agreed standards for professionals wherever they live or work in the world. They require members to commit to continuous professional development (CPD) and continuous learning and they also require their members to demonstrate professional competency, integrity and display ethical standards. Professional bodies like the Law Society, General Medical Council, Engineering council, Chartered Institute of Personnel Development and Association of Chartered Certified Accountants define and apply the standards they expect their members to achieve and apply. By achieving professional recognition members demonstrate that they have had their competence independently assessed and credentials verified to practice.

Professional standards in cyber security.

Successful cyber risk management requires proven competencies across a range of management and technical disciplines including cyber strategy, cyber security, risk management, project management, leadership, regulation, communications and reporting to name some. No single qualification in the list of 120 appears to address all these competencies in addition to peer review and CPD. In the UK there is no independent professional assessments carried out and assessed within the working environment. This is of no surprise as there are no professional standards which have been universally recognised and meet the same levels of attainment as a doctor, nurse, chartered accountant, lawyer, chartered engineer or teacher.

Whilst there are no formal professional standards for cyber security in the UK there are professional security standards. The UK's 'Security Institute' manages the process for being accepted onto the register of Chartered Security Professionals (CSyP), a professional standards accepted by the UK Governments Centre for the protection of National Infrastructure. Inclusion on the register follows an assessment of academic qualifications, competency and peer review and confers on an individual the recognition that they have met the highest security standards. Registration is recognised by the UKs Centre for the Protection of National Infrastructure (CPNI) a government agency sitting under MI5.

The UK Government is in the process is implementing a programme to define the standards for cyber security professionals in the UK. As part of the UK governments commitment to develop its National Cyber Security Strategy and the cyber security profession, the Department for Culture Media and Sport (DCMS) has awarded a contract to the Institute of Engineering and Technology (IET) to develop the UK Cyber Security Council. A body which will oversee the development of cyber security professional standards, set the appropriate pathways for qualifications, deliver a Royal Charter for cyber security and a governing body like that of other professions. The challenge will be to implement these into cyber security marketplace so that cyber security professionals are recognised in the same way as engineers, doctors, teachers, nurses and accountants.

Professional accountability on the board table.

In the UK there are no legal requirements for board members to hold and maintain professional qualifications. But there is clear duty of care for board members to maintain professional standards, integrity and competency in their chosen fields. The CFO should be a member of a professional body to manage the finances, the group General Counsel should be a registered lawyer. The Human Resources Director should be a member of the Chartered Institute of Personal Development. The head of Engineering should be a member of a recognised engineering institute and the chief marketing officer, the Chartered Institute of Marketing. The CISO, a critical role for securing corporate value does not have to have any formal qualifications or the opportunity for professional recognition.

Recent cyber events demonstrate the significant impact on shareholder value for the companies that have been hacked. A trend which will only continue to increase as the regulatory environment gets tougher, big data and corporate digital strategies take effect, society becomes more digitally enabled and cyber develops into a fully utilised geopolitical tool. The complexity of managing cyber risks creates a strong argument for setting professional standards for the cyber security community. But cyber is not like the 'older' professions of law or accountancy. It's a profession which has grown in many directions through market forces over a very short time period (less than 20 years) with a diverse suite of qualifications.

Overcoming the obstacles of implementing professional standards

The biggest challenge I believe in implementing a professional standard for cyber security is one of developing a road map which recognises some of the current qualifications, professional experience and develops a professional standard over them. Any new professional standard will take time to implement. Engagement by governments, companies and individuals will be key and recognise all levels of security professionals. This is not unsurmountable, for example the engineering profession has many routes to recognise engineers at all levels from apprentices, associates and professional engineers with academic qualifications and industry experience. The same can be applied to cyber security, where there are many qualifications and levels of industrial experience in the marketplace to be considered.

There can be no qualification 'light-switch', or 'cliff edge', but a road map which will take time to implement. To reach a point whereby standards are agreed and universally recognised for cyber security professionals. With the UK Cyber Security Council taking the lead, putting in place standards for cyber professionals for UK PLC. Once in place it will formalise what a cyber security professional look like, in line with other professions. It will enable boards to place assurance over the quality of the cyber security professionals they employee and all of this must be positive news for the cyber security profession. This conversation has some way to go, but in the UK the direction of travel is being set by DCMS and the UKs Cyber Security Council and one which isn't going away.