WAVESTONE

SECURE BY DESIGN : TAKING A STRATEGIC APPROACH TO CYBERSECURITY

THE CYBERSECURITY MARKET IS OVERLY FOCUSED ON AUDITING POLICY COMPLIANCE AND PERFORMING VULNERABILITY TESTING WHEN THE LEVEL OF BUSINESS RISK PRESENTED DEMANDS A HOLISTIC RISK ASSESSMENT AND AGILE SECURITY ARCHITECTURE TO BE PROACTIVELY DEVELOPED.

INSIGHTS

1 THE THREAT FROM CYBERATTACKS IS CLEAR AND ACKNOWLEDGED

Nearly all UK corporations have seen hackers successfully penetrate their IT systems in an attempt to steal, change or make public their sensitive data[1]. Criminals are not only targeting financial institutions or looking for financial data, they are also now seeking personal data of employees and customers, corporate intelligence and to hijack IT infrastructure for criminal use.

The UK Government's National Security Council recently announced that attacks on computer networks are among the biggest emerging threats to the UK, ranking them alongside terrorism and flu pandemic as the key dangers to the UK's security.

Recent high-profile attacks reported across a variety of industries include:

- Fiat Chrysler, who had to recall 1.4 million vehicles in the US for an upgrade to the computer systems, after security researchers demonstrated they could take full control of a Jeep Cherokee from 10 miles away by hacking into its on-board computer system[2]
- Carphone Warehouse, who acknowledged a serious data breach that may have seen the banking details of 2.4 million customers stolen by hackers[3]
- Hacking rings that have targeted three pharmaceutical companies in the last 18 months to get access to details for their financial gain[4]
- Telstra's newly acquired Asian subsidiary, Pacnet, had its IT network hacked into, just before the acquisition took place[5].

Whilst the majority of firms are actively engaged in setting up security governance policies and carrying out security audits to aim to safeguard themselves against cybercrime, almost one tenth of UK firms have not acted in any way at all to protect themselves from hacking[6].

That aside, cybersecurity is starting to get the right level of attention within large corporates. It is no longer just seen as a policy issue, a compliance issue, or an IT issue. Instead, it is now seen much more as a strategic and corporate risk issue, which has to be considered throughout all internal project lifecycles and as part of 'business-as-usual', not just as a one-off activity. Board members of many firms now hold the CEO primarily responsible for cybersecurity, with the CIO as the second-most responsible executive, showing the importance of cybersecurity within the organisation.

2 THE ELEVATING PROFILE OF CYBERSECURITY HAS YET TO TAKE REAL EFFECT

In a recent survey on behalf of the UK Department for Business Innovation and Skills and contributed to by 200 corporate directors, just over one third said cybersecurity in some capacity was discussed at every board meeting and nearly half said it was discussed at most meetings[7]. This is likely to be a significant increase from comparable responses 12 months ago. However, two thirds of board members are not confident of their companies' in-house ability to fully defend themselves against cyberattacks with only 4% being "very" confident of their defences. Despite this lack of confidence, integration of security into the design of new products ranked second to last in priority when considering the development of new products and services.

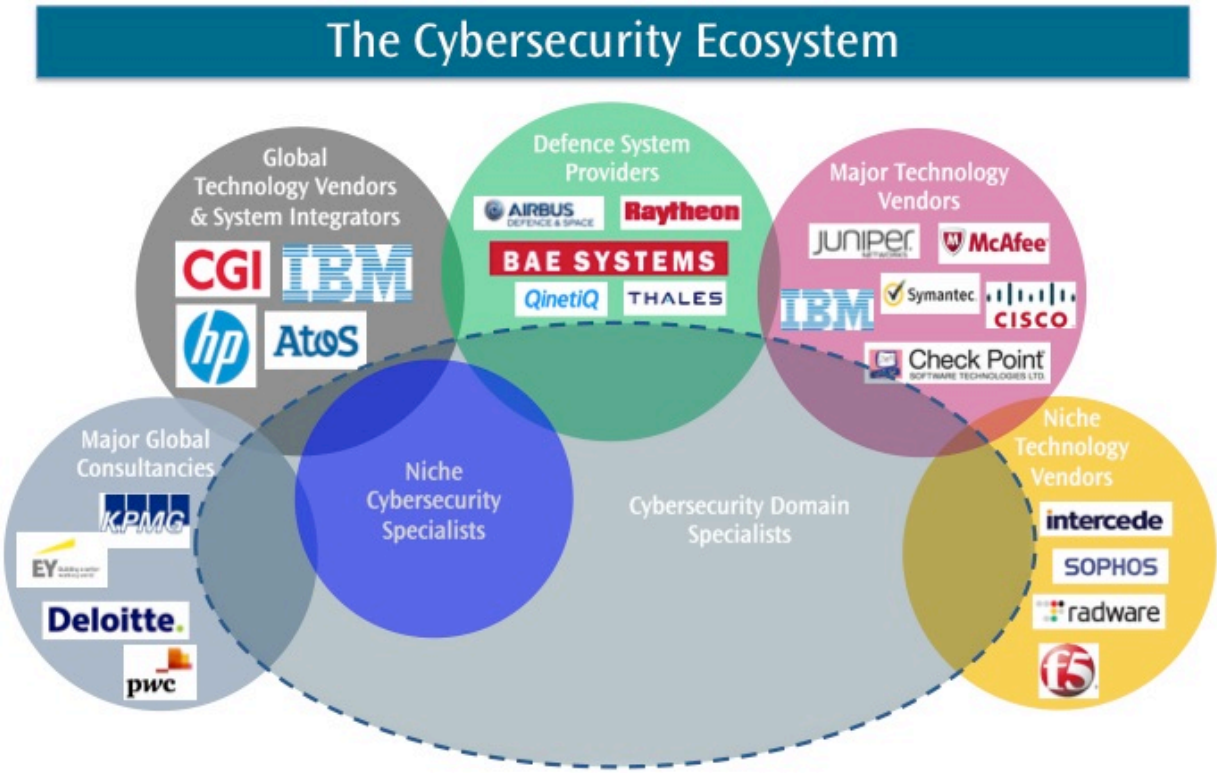
The limited amount of new products being released within the security area, together with the rapid increase in volume and criticality of the threats in recent times shows that the level and availability of technical knowledge of the cybersecurity field as a whole has not grown at the same pace as demand.

3 A STRATEGIC AND HOLISTIC APPROACH IS NEEDED TO ADDRESS THE THREAT EFFECTIVELY

The cybersecurity ecosystem is disparate and encompasses professional services firms, technology vendors, defence system providers, IT systems integrators as well as niche cybersecurity specialists. However in most examples the focus of these organisations can be traced back to their roots; for instance many of the professional services firms offer security audit services, building on their financial audit experience into a new market to fill an emerging gap. As a result, many services in the cybersecurity advisory market tend to be based on audit and compliance checks against industry and government standards including ISO27001 and CESG Assured Service (CAS).

Technology vendors and defence system providers have also been able to offer cybersecurity advice but this has predominantly been focused on whether the hardware and software within the IT environment of a company and its security architecture is fit for purpose at that point in time or at the point of installation. Only a few have developed genuine creative capabilities by addressing both the business and the technical risk perspectives and therefore offering advice in a more rounded holistic way. This holistic approach requires knowledge of business risks and the security standards and how these can be applied to the technical architecture and end-user business environment. This must be underpinned by knowledge and learning gained from recent industry cyber-attacks to determine the best prevention strategies to manage risk.

The diagram below illustrates the complexity of the 'cybersecurity industry' and the diversity of companies that are within it, all offering slightly different services and advice to businesses from their own individual perspectives. Wavestone believes organisations need 'Cybersecurity Domain Specialists' that offer a more holistic approach to cybersecurity by drawing in the knowledge and expertise across all areas of the domain.



4 CORPORATIONS AND THEIR ADVISORS NEED TO ADDRESS AND MITIGATE RISK AT A BUSINESS LEVEL

The cybersecurity market can become overly focussed on auditing policy compliance and performing one off vulnerability tests when the level of business risks demands a more holistic risk assessment across its entire estate and an agile security architecture to be developed in defence, which is monitored and reviewed on an on-going basis.

Some companies have independent audits carried out which confirm that they have fully met security compliance standards. They may even have had their IT network redesigned or upgraded to make it harder for a cybersecurity attacks to occur. However, it is not unusual to find that a few months later they have been subject to a cyberattack. To be cyber-secure requires hitting a moving target: the assessment and mitigation of cyber-attacks requires continuous and proactive risk management to be part of the security strategy.

We advocate that organisations shouldn't build a castle without internal protection within its walls, instead they should build along the lines of the airport model with multiple layers of security that monitor and adapt to threats as needed. They should seek specialist professional support to ensure that 'secure by design' principles are adopted across the business and permeate through all business processes, products and services. The objective of this approach is to proactively build security into the design of services instead of adding layers of security at a later stage in reaction to events.

5 HOW TO INITIATE THE "SECURE BY DESIGN" APPROACH

To address the challenge of "secure by design", the Chief Information Security Officer (CISO) should organise their team to provide expert support to all projects and product development activities. Their objective should be to build mutualised security services and to increase the security competencies of project managers, developers and architects:

- The first step should be to ensure that any project management process includes an initial

"information security assessment to identify whether the project involves a number of security-critical areas. For example, does the project require the usage of personal data, of payment information, confidential data or a direct connection to Internet? Each affirmative answer will increase the level of attention required by the project. Projects requiring a high level of focus will often benefit from the including a security expert in the project team.

- To ease the integration of security in the project, the CISO should also consider building security commodities. Capabilities such as database encryption or strong authentication will be required by many projects. The ability to standardise security services is a keystone to ensure security will be really integrated into all projects.
- Finally, to enhance the security by default, the training of the developers and architects is required. As of today, many project team members have a limited awareness of security threats – as a result applications are built without security embedded. Often, just before being put in production, audits show numerous security flaws, adding delay to the project and increasing the cost as remediation is put in place.

To fully implement a global, integrated "secure by design" culture in a large organisation is a long-term strategic activity and may take between 3 and 5 years. However, the first quick wins can be obtained in around 3 months with the support of a 'Cybersecurity Domain Specialist'. It could deliver considerable cost savings as information security related costs can range from 2% to 20% of total project cost.

ABOUT US

Wavestone is an international consultancy that provides connected thinking, insight and capability to industry leading organisations. We work collaboratively with our clients to plan strategic business transformation and seamlessly turn strategy into action.

FIND OUT MORE

If you'd like to find out more, please contact us by calling at +44 20 7947 4176, or via email at **enquiries@wavestone-advisors.com** or visit our website at **www.wavestone-advisors.com**

[1] http://www.computerweekly.com/news/4500248063/Nearly-all-UK-corporations-have-been-hacked-a-survey-shows
[2] http://www.computerweekly.com/news/4500250565/Fiat-Chrysler-recall-highlights-importance-of-security-by-design
[3] http://www.finextra.com/news/fullstory.aspx?newsitemid=27707
[4] http://www.fiercebiotechit.com/story/financially-motivated-hackers-break-3-major-pharma-companies-18-months/2015-07-10
[5] http://www.computerweekly.com/news/4500246705/Telstra-Pacnet-hack-shows-telcos-are-a-prime-targets-say-security-experts
[6] http://www.computerweekly.com/news/4500248063/Nearly-all-UK-corporations-have-been-hacked-a-survey-shows
[7] http://www.computerworlduk.com/news/security/cybersecurity-now-being-discussed-at-most-board-meetings-survey-shows-3613503/

WAVESTONE

www.wavestone-advisors.com