CYBER METRICS

March 2018 RANT Forum

Post Event Report

Compiled for the Department for Digital, Culture, Media and Sport

Written by Acumin Consulting ltd

Rant FORUM

Department for Digital, Culture Media & Sport

ACUMIN

Introduction

The Department for Digital, Culture, Media and Sport are currently conducting research into how it might provide further support to UK private industry in relation to cyber security resilience. Firstly by looking at how a proposed set of metrics could provide a model by which to standardise a measure of 'good' security but also looking at a wider industrial context of how government can enable organisations to better their approach to security.

The Department has collaborated with RANT to create a trio of events, each designed to collate views from a broad panel of industry professionals and an audience of around 100 senior cyber security professionals representing enterprise, SMB, and public sector end user organisations.
March signalled the final of the three events, posing the question, "What drives business investment decisions around cyber security and what is the role of government in both driving action and reducing barriers?".

Moderated by Acumin Consulting's co-founder Chris Batten, the holistic panel consisted of representatives from an end user organisation, a cyber insurance provider, government, and technology; namely Simon Gilbert (Managing Director, Elmore Insurance Brokers), Charlie Timblin (Senior Director, Europe & APAC Cyber & Technology Risk, Royal Bank of Canada), Dr Mike Lloyd (CTO, RedSeal Networks) and Emma Green (Head of Incentives and Regulation Team, Cyber Security and Data Protection Directorate, DCMS).

The following report is a collection and reflection on feedback from the event.

To what extent are organisations motivated to conduct good cyber security?

One of the focal points for DCMS throughout this industry research has been to understand the usefulness of creating a standardised measurement for cyber security effectiveness. As such it is important to define what 'good' security looks like, and how we establish a best practice baseline. The most obvious approach is in utilising tools that produce an objective measure, such as vendor solutions for scorecards or metrics, or risk assessment and management exercises. Operational data analysis provides insight in to the security posture and resilience of an organisation, but whether those findings are used to improve security or inform processes such as incident handling, is more difficult to measure. As many organisations have discovered, simply producing the data and analytics is not enough if it doesn't inform and improve security.

The level of focus on cyber security is totally dependent on the type of organisation, and the sector it sits within, encompassing factors such as the level of threat and presence of regulation within that industry. Whilst large enterprises are keeping cyber security on the board agenda, for smaller organisations it is hardly a first choice in terms of investment, particularly around areas such as analytics which might be seen as a luxury rather than necessity.

The impact of the human factor as an issue in improving organisation security should not be underestimated. The internal culture and the value employees place in company assets and reputation, can go a long way to improving security posture, it can be said to improve the incident detection capability by building a culture and awareness of security. A further consideration is the expectation of the company's customer base; some products and services have different values placed on them by the end consumer – and so the same goes for the consumers' expectance of customer service and the security of their data.

Some firms or industry sectors are known for exploiting customer information or not placing a huge value on its security, such as online marketplaces, forums and social media where users' data can be heavily processed. Indeed some recent high profile breaches have not been accompanied by a significant loss of users. Incidents such as those experienced by ebay, Ashley Maddison, Under Armour (MyFitnessPal), Uber and the recent privacy concerns around Facebook's sharing of data with third parties (namely Cambridge Analytica) are prime examples of businesses who have maintained a majority share of their customer base despite failing to take their responsibilities to security seriously.

If the organisation in question, believes that its customers are not sufficiently concerned with security to demand investment and risk the business's ability to create profit then there is little motivation to improve the situation. The decision to drive security therefore, has to come from the top and impact every decision in order for change to be actioned. The role of the boardroom is something that comes up time and time again within discussions of effective cyber security strategy, so it is not a surprise that it is symptomatic of either good or bad security strategy in this context.

The question then, is what motivates organisations to become secure. Businesses within the US (92%) and particularly the UK (99%) make decisions that are motivated by regulatory compliance. This is not the same as taking an effective approach to security but rather can be seen as 'underwriting' it to an acceptable benchmark. The role of compliance is not really about security but ensuring you are spending the same, if not more, than your competitors on security. In the event of a breach and potential media focus and criticism, proof of investment and organisational 'good will' in security investment can be used to avoid harsher criticisms and mitigate reputational and financial loss.

Organisations are also motivated to invest more in technology as a 'solution' to reducing cyber risk. Increasingly vendor products position themselves in the market as a multi-issue solution, or even a fix-all to many security questions. These can be tempting to boards, arguably encouraging a principle of 'invest and forget' towards mitigating cyber risks. Alongside this is the narrative of a draining talent pool, and so the cyber security skills gap remains fixed on the radar of HR professionals. If organisations are unable to hire sufficient numbers of subject matter experts, investing in relatively cheap technology solutions can be perceived as a fix (arguably though more akin to a 'Band-Aid' approach than permanent solution), particularly if compliance serves as the lowest common denominator.

So if effective security is not inherent through regulation, why then is the idea of compliance so important to organisations? The psychology lies in the notion that by meeting a set of criteria you should be rewarded with a level of assurance that you have guaranteed a level of safety and security. Cyber threats by their very nature are fluid, constantly evolving and therefore both difficult to identify and prevent – not least because the nature of understanding and mapping how threats enter and permeate the business is a substantial and complex undertaking. Investing in solutions either by design or via human processes feeds into and informs the business' risk management processes.

How able are organisations' in providing effective internal cyber resilience? What are the barriers?

Regulation drives behaviour – but that does not necessarily drive security. Striving for too many compliance factors and 'ticking the box' can actually increase risk because it causes organisations to try and meet too many standards and expectations, which can potentially offer conflicting guidance. If all the resource is taken in meeting contradictory regulatory standards, where is the room to actually think critically about how secure your business is, or indeed the resource to address it?

Regulation is also being used to shift the blame from the organisational to the individual level, namely on to the CISO, should anything go wrong. Regulation is being treated as a means through which to shift liability and so for many large US companies the CISO is becoming the 'Chief Blame Officer.' Why is this scapegoating seen as acceptable and if the practice continues, what kind of candidate is going to be willing to take on the job? Regulation is the driver now, but it's being used against the security function. We all remember the stories about Lehman Brothers in Administration, hiring a CISO in preparation for the FBI, and likewise off the back of large-scale breaches, too many times the CISO has found themselves beholden to the consequences of organisational rather than individual failures.

There is a significant and logical demand to have someone in the role but the scapegoat element is built-in. It eliminates the gross incompetence of doing nothing at all but doesn't lead to good security, it undermines it. There is no strategy, little understanding of specific risk, and too many regulations.

As an industry we should share data more, but how do we do this in a collaborative and constructive manner. This was something highlighted in the feedback around the Waking Shark II war games in 2014, and we still haven't solved the issue of collaboration. Sharing data will enable insurance businesses to make more informed decisions through objective benchmarking but any efforts lack maturity.

Currently risk management techniques are not up to scratch but internally managing risk could still be a huge advantage. Organisations should move away from regulation and use risk management to encourage investment. £100ms are invested off the back of risk assessments but the methodologies involved can often be too clunky to allow a business to make such investment decisions effectively. How can we improve this approach? Risk assessments are inconsistent, they bring in bias or rely on poor knowledge, it would be better to join up all capabilities and models. We fail in cyber because we lose the context of what's important to the CEO or CIO; what is the value of what is at risk, what is the potential impact rather than the technical issue? Risk assessments are not holistic enough, they're conducted in isolation, this has to change if the industry is to mature further and become a ubiquitous element of business processes. The board don't want to address these issues at an individual level, a comprehensive approach for risk exposure is needed.

Despite many organisations showing that an incident does not need to have a substantial impact on the commercial side of a business, the risk of press exposure revealing corporate mistakes or shortfalls is a massive driver for the C-suite in pushing toward effective security; "The fear of the media drumbeat" reverberates hard in boardrooms. Yet as Uber have shown us, this can be an inhibitor of honest and timely breach notifications, where ultimately the main victims are the subjects whose data has been compromised; arguably this may be an area where regulation mandates better practice.

Information security now has a greater presence at board level but is this because of awareness over high-profile breaches or as a result of regulation? Boards are paying attention, regulation has been around for a long time but didn't gain traction, e.g. PCI-DSS. The media are driving awareness. DCMS – How can government do better at communicating the impact of a breach? An amplification network? They already work with the third sector on an initiative like this. How can government help to understand the need for cyber investment and improve inter-company collaboration? Bad behaviour is often driven some of the major consultancies and any others who could be argued to value service delivery and box-ticking over pragmatism and enablement. CxO awareness and investment is definitely a positive but the industry is and for the foreseeable future will continue to fail at collaboration; what is the organisation outside of CxO doing about collaboration, can security learn lessons?

How can government reduce barriers?

Government needs to work on awareness campaigns to break down the reputational risk of being associated with suffering an attack or data breach. We need to move towards a model of understanding that breaches and incidents will happen, even to those who are best prepared against them.

If gathering information on how attacks originate, there should be a consideration of providing a safe-haven for those who come forward with information. Where there are not regulated requirements for disclosure, those organisations who trade within the UK and who choose to do so, should arguably be rewarded for their honesty.

Industry needs to be better protected from the insurance industry. The government has a role to play in working with the insurance companies to generate better information that can be passed on to help as many organisations that are at risk – so that they may benefit from realistic insurance policies. In a time where it's not 'if' you will be attacked but 'when', the insurance industry has a long way to catch up in providing effective support in setting policies that enable prevention and not just pay-out (which is hard to come by in itself).

What is required of government so industry can be enabled to support smarter decisions around security?

From what we know of the government's current stance, the 2016 report did a lot to suggest that for many the current strategy is to wait on the impact of GDPR, NIST, and other inbound regulations to measure the market's and competitors' reactions before responding. Government already acknowledges regulation is not, and should not be, the sole driver and want to learn what else is driving the security market. Better intelligence sharing and communications between organisations is essential to give those assigning budget the full picture, and go some way in providing a more representative set of benchmarks.

In a lot of cases (likely not enterprise businesses) organisations are not implementing basic cyber security procedures; SME's in particular are guilty of not investing in cyber security, as is the third sector. Where government has been writing reports to drive awareness to charities in the recent year; they should consider widening such initiatives to include advertising and gathering information on effective business protection for sectors that need it most.

Another aspect that government should consider addressing is the difficulty organisations have in knowing where to turn when they require information, support, or need to report a breach. Having a centralised function would be far simpler for the private sector, and may break down barriers toward honest communication. Hiding security behind the DCMS doesn't work; do we need a specialist agency solely for cyber? It is currently admittedly disjointed, not just for businesses but also victims of cybercrime within the general public; government understand this and that there needs to be clear point of contact regarding cyber, there is a more joined up centralised approach coming.

A question from the end users: Who shares incident data outside of regulatory requirements? "We share with the NCSC". Most who share do so within regulated industries, otherwise they are often not allowed. There's an argument that at board level such intelligence is seen as an investment and therefore represents competitive advantage. Why should government be doing more, with the information gathered by the NSCS? How should the information be used to drive awareness to prevent similar situations occurring in the future?

The government should also consider how to incentivise organisations to implement an effective cyber security strategy. Regulation doesn't work. A risk becomes company-specific or regulatory; the risk drives behaviour but not security. Has the government considered offering tax incentives for security investment rather than regulation; what are the alternatives to incentivise investment?

There's an awareness in government that not enough has been provided in terms of support to now which is why they are undertaking initiatives like RANT. Government want to grow the security ecosystem and support start-ups to create a constructive business model, and they are trying to use companies not government to drive the buried skills pipeline for new and existing professionals. They had a scheme at one point for micro-SMEs, offering a £5k cyber security grant to implement Cyber Essentials. Eight audience members raise their hands to demonstrate a prior knowledge of this. Being pragmatic, DCMS understand something like this would not be scalable, but could consider something like vouchers towards certifications, indeed a similar initiative has been rolled out in Scotland, but odds are against it seeing wider integration.

Conclusions

Organisations want a clearer strategy on what government is going to do about the nature of cyber threats against the country, and how it intends to support industry in its endeavours.

Although awareness of cyber threats and investment are both increasing, many organisations value tax breaks or monetary incentives as a motivation for prioritising cyber security, particularly when this is not against a backdrop of regulation. Collaboration creates realistic and useful threat intelligence that can guide security methodologies, yet this is only ever going to be good as the volume or quality of data, as well as the number and breadth of contributors.

Cyber security is definitely a growing concern at board level and only gaining further traction, the question of how effectively risks are managed varies wildly though. Organisations need to harness their own risk management processes and usage of security product data to understand the risks they face and to impact behavioural change in their organisations to stand a chance.

GDPR and the data privacy argument is both a help and a hindrance to cyber security professionals in terms of managing information security priorities. Regulations and compliance continue to be huge impacts on behaviour and can create narratives of necessity and urgency; it brings the conversation to the board-room table. Too often though these regulations are seen as a minimum requirement by which to pass under and achieve a false sense of being secure. Government needs to take that seriously and think critically about how that is managed, it needs to drive best practice benchmarks as well as an organisation-specific risk-based approach to identifying and managing security risks.

RANT was established in 2007 as a unique open networking and discussion event for Information Security Managers, Directors, CISO's and other influential information security, cybersecurity and risk professionals who work within End User organisations.

RANT works to provide a platform for all members to discuss and debate Information Security related issues in an open format. RANT supports the cyber security industry with monthly discussion forums, bespoke conferences and CISO roundtables based predominantly in London, but also UK wide.

This report was written for the DCMS post the March 2018 RANT Forum in conjunction with Acumin Consulting by Martha Tonks and Ryan Farmer.

Acumin is an internationally established Cyber Security recruitment specialist. Operating since 1998, Acumin consulting has been working exclusively in the cyber security landscape with the world's leading talent.

Contact Us:

+44 (0) 20 3119 3387

contact@rantevents.com

www.rantevents.com

Rant FORUM