RANT+ DCMS: THE REPORTS

WRITTEN BY  ACUMIN

CULTURE OF SECURITY

The Department for Digital, Culture, Media and Sport are currently researching how to support UK private industry in relation to cyber security. One area of that research is understanding the importance of engaging a strong culture of security within organisaitons as a form of resilience, comparitive to using technical controls to measure and protect the organisation.

The Department sponsored a trio of events hosted by RANT Events and supported by Acumin Consulting that brought together a group of 100 cyber security professionals. Each event was designed to collate views and experiencesthat could be later used to support government.

In the February event the question was posed:

'What is more important, a culture of security or technical controls?'

The discussion was moderated by Geordie Stuart (Head of Security Governance, Risk and Controls, Nationwide Building Society) with a panel of speakers consisting of Prudence Smith (Head of User Behaviour and Awareness, Barclays), David Cook (Solicitor Advocate, Eversheds Sutherland), Erica Constance (EO Cyber Portfolio Manager, QBE Insurance) and Chris Hodson (Board Member, IISP).

The following report is a collection and reflection of feedback from the event, it was later sent to the Department to aid their research.

This report was written by Martha Tonks, with support from Daniel Beresford.

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.

WHAT DO WE MEAN BY TECHNICAL CONTROLS?

Technical controls can provide automated protection from unauthorised access or misuse, facilitate detection of security violations, and support security requirements for applications and data.

Information from technical systems needs to drive risk assessments in order to protect organisations from threats, and develop insights into how to build out a strategy for creating an effective security culture. Metrics from these products can identify or highlight threats (an example being which employees are clicking on malicious links in emails), but how is that changing organisational culture in making it less likely to make the same mistake again?
If we look at technical controls in isolation, there is a deficit in the information they present and an outcome of improving security. Metrics from technical controls must be included in communications within the business to have any real effect.

WHAT EXTERNAL INFLUENCES NEED TO IMPACT TECHNICAL CONTROLS?

AI has a potentially massive future influence on technical controls and organisational resilience against cyber threats. Employees have never been more powerful in terms of data they both create and have access to, the margin for error continues to increase and there is an argument to suggest that there will come a point where human monitoring and intervention will not be able to minimise risks against the wider organisation and its customers. Is AI really the answer to our risk management problems?

Regulatory compliance and the legal sector are also influencing the metrics required from technical solutions to gain an understanding and managerial response to threats affecting the organisation. If we consider the impact GDPR is having, and will continue to have on organisations this point is given context. The GDPR states that it's not in the data subject's interest for organisations to store and process data indefinitely. Therefore, an important metric that needs to come out of our technical controls is in correctly mapping the current data within the organisational network. Technical controls can play an important role in providing visibility across an organisation as to the types of data and processing taking place, providing insights in to not only its location but also data flows and uses. Having an unbiased and real-time update on the data and its usage across the organisation is vital in understanding where and how threats surface, and succeed.

GDPR recommends data minimisation as a way of reducing the impact of a breach and maintaining fairness of processing, and privacy by design is inherent to this. The challenge with this approach of course is that, data minimisation goes against the grain of other business objectives. Sales and Marketing functions are dependent on gathering data but at what point do they stop – how much of this is really useful? Cyber security and data protection professionals therefore, have to embrace security- and privacy-by-design, and the data gathering and usage across the organisational network with a compromising and fair attitude if they want to succeed in mitigating, or at least limiting, data risk.

HOW DO WE KNOW TECHNICAL CONTROLS ARE WORKING?

The first step is investing in the right technologies to prevent users from making mistakes and getting the basics right combined with some effective monitoring.

From an insurance perspective, the management of risk needs to be considered in all senses. Technology controls are the first layer but by no means the only element considered. A lot of claims in the market are driven by human error, which is no surprise. Examples of this could include individuals turning off or circumventing end point security controls, or poor configuration of IT platforms. Removing the dependency on controls in isolation is a necessity of a strong security culture, they are most effective as part of a joined-up approach to risk mitigation and management.

Culture is instrumental in preventing incidents in the first place but also, if and when incidents do occur the response time can be much faster, and the information about the extent of the breach much more likely to be captured. This is not necessarily an easy thing to measure however, insurers are not agreed on common metrics as there is huge diversification in cyber security insurance packages out there in the market. The growing competition in the market for cyber insurance products reflects the maturity of the offering, the cyber insurance market has been around for 20 years and yet only in the last 7 has there been an influx of insurers and propositions entering the market.

Therefore, it is difficult to ascertain what individual organisations should be working towards in order to show their resilience against cyber threats towards insurers, as there is not necessarily a best practice put forward. What is true, is that most insurers expect their customers to have a cyber security claim at some point or another.

Therefore we need to consider how metrics from technical controls can assist insurers in accurately costing the risk from which to base an organisation's potential premiums. The insurance market are not experts in technical security, but there are indicators of effective cyber security management. Questions about basic controls in situ are commonplace, as well as an understanding of the vendor technologies in place that look at encryption and patching for example. Insurers will need to understand the policies, procedures and controls that are put around the technical solutions and their application in mitigating risk in order to get a clearer picture of resilience.

In terms of the information security professionals' responsibility in making sure that technical controls are working toward mitigating risk, the use of KPIs incurred an animated response -should the KPIs of IT and cyber professionals be a mirror of business goals? For the most part, information security staff work in silo within the organisation and are presenting data that does not necessarily look related to revenue generation. The number of malware alerts each month does not give senior management an indication if they are closer or further from meeting business objectives. For cyber security to be taken seriously across organisations, it needs to correlate to the language of business – financials. But there is also argument to say that the purpose of an information security professional is somewhat different than other operational roles. Finding the balance between what technical controls are telling us and what that tells us of the information security professionals' proficiency in their role needs to be carefully considered.

If the cyber security team are not correctly linked with the board and there are technical control failures, it's not the fault of the IT people or the technical controls themselves, it's a communication and maturity issue.

CONCLUSION

Technical controls and building a culture of security are not exclusive in their impact on mitigating risks. In order to survive, businesses need to have a balance of both, and one should inform and support each other. Indeed, in many respects, the use of technical controls helps to facilitate cultural change. On balance, however, we feel the result of the RANT was that achieving a culture of security is fundamentally important, but is a utopian "Nirvana". Whereas conversely, solely implementing technical controls alone will not suffice in the long-term.

The disparate nature and cross-department coverage of cyber security's focus means that it must be embedded throughout the business and its culture to succeed. Technical controls perhaps should be redefined as tools through which to support staff and security, rather than the final 'solution'.

Ultimately users must have some responsibility for their actions but they should equally be empowered to make informed decisions rather than facilitating a blame culture. If (and we should) expect security-ley staff to act as eyes and ears for the business, we must provision them to be that line of defence. Openness, collaboration, and education are paramount in fostering a strong security culture.

The upcoming deadlines for the GDPR bring in to focus the need for connected processes and systems, connected with the people and the business, offering transparency and a culture of a shared responsibility.

If we take the tried and tested security analogy of the fortified castle with its high walls and ramparts, the masonry will quickly deteriorate unless those it protects work to maintain and reinforce it. Protection is the raison d'etre of the security function, but it should be the responsibility of all those who work across the business; for this to happen it must become familiar, embedded, and empowering rather than threatening, confusing, or overwhelming.

Most important controls in 12 months' time:

- Technical controls that stop threats at the gate.
- Cultural controls more able to affect management and boardroom change.
- Network monitoring, endpoint protection, threat intelligence.
- Metrics around time to detect, time to respond.
- Cultural and technical controls that stop users walking away with data e.g. data classification.

ABOUT ACUMIN

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.

Our unique understanding of the market and of the specific skill sets necessary across a range of role disciplines mean that we are the first choice amongst our network for placing talent in the right opportunities across permanent, contract and temporary staff across the contingency and retained models of recruitment.

Acumin's approach comes from a firm understanding of the market, we work with industry leading analysts and partner with content experts to continuously build on our knowledge resources. Acumin also spend the time to get know our clients' businesses and their cultural nuances to ensure that we deliver with the clients overall organisational goals in mind.

CONTACT ACUMIN:

+44 (0) 20 3119 3333

INFO@ACUMIN.CO.UK

WWW.ACUMIN.CO.UK

ABOUT RANT

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.

CONTACT RANT:

+44 (0) 20 3119 3387

CONTACT@RANTEVENTS.COM

WWW.RANTEVENTS.COM