CYBER METRICS

2

February 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 researching how to support UK private industry by proposing a set of metrics that organisations could adopt to provide a holistic view of cyber security.

The Department are sponsoring a trio of events run by RANT, each designed to collate views and experiences from a group of senior cyber security professionals.

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.

Can we define a 'good' culture of security?

Building a culture of security is challenging. It is not the same as enforcing training plans or strategies to improve employee awareness of cyber security issues.

Creating an effective security culture has to start from the boardroom. If you expect processes to be adopted you need to ensure you have a strong communications strategy to go alongside well-meaning protocols. To change user behaviour, it seems logical to communicate in a way that relates cyber security to their own personal wellbeing, and their responsibility to the company. One way of approaching this is to use metrics collated from the various technologies used to monitor risk and threats, as proof of the ongoing challenges the organisation is facing. Rather than rely on sending out awareness messages or mandatory training, perhaps the best way to engage employees is to demonstrate a direct correlation between their behaviour and the impact on the business.

We can take this concept of personalisation for creating a culture of security by thinking critically about how we can tailor awareness strategy to individuals, and teams.

A clever approach to improving security culture could start with identifying your highest risk employees. By understanding who is most likely to be targeted, as well as why and how, an organisation can start to develop a model of best practice in response to more specific risks.. Disseminating such a pragmatic model in response to targeted risks will enable a more responsive and focused strategy of informed defence to develop.

Another way of creating a culture of security is to look at individual teams, and their processing abilities and general security awareness. By taking a case-by-case approach the outcome is a set of behavioural processes that have been born out of direct contact and buy-in from teams. By consulting with employees you are engaging them in the process of creating a culture of communication and openness, and therefore security.

These are traits that we would expect of a positive culture. It is widely accepted common sense that threats will continue to grow within firms, and so we can't expect that mistakes will never happen. A more useful metric may be to define how many mistakes we find acceptable. Knowing if your organisational culture values security is surely indicated by the way in which individuals respond to a potential breach or issue.

A good culture of security therefore, is not likely to be based on fearmongering. Phishing metrics for example, should not be considered a particularly effective benchmark for an effective security culture.

Greater societal awareness of cyber attacks and the necessity to secure against them means that board-level and organisational buy-in have increased significantly in recent years; if security have not yet gained such traction within your company, a good culture of security and organisational maturity will prove challenging.

What are the challenges to maintaining a strong culture of security?

Maintaining a culture of security requires discipline from every level of management.

Some argue that successful information security is a matter of getting the technology right. Others contend that it's more about training and education. Both views are valid, but neither is complete. Good information security is about technology design and deployment, to be sure, but it's also about people and the right processes being in place. It's clear that good security will always be about the old trio: people, process and technology. The issue for most organisations, is that cyber security is not yet a priority. Creating a culture of security is nigh on impossible if companies are doing relatively little to arm themselves against cyber attacks in the first place. For many organisations developing and delivering bespoke employee awareness training programmes is beyond their level of maturity in managing security issues, with a surprising amount not offer training programmes at all. How we treat employees is probably the biggest influence on how much respect they pay to our business, so how can senior management effectively deal with the reality that employees will make mistakes. Without a culture of openness, the impact of those mistakes is much greater. But allowing employees to be relaxed enough to make mistakes in the first place only increases the chance of risk itself. The amount of mistakes from the general employee workforce that the average information security professional would deem acceptable is likely much lower than say a manager who recognises that the offending employee is a productive team member. How a company can find a standard to which everyone should be held to account is a challenging standard to implement.

When looking critically at weaknesses in user behaviour, should the IT staff themselves be put under similar scrutiny as a potential cyber security risk. It's necessary to take into account the different risks specific teams are most likely to face, what systems may be attractive to attackers and the routes through which they may be attacked.

Some organisations have a paranoid security culture, which can lead to paralysis. A culture of openness is vital to ensure people feel confident in alerting the business about breaches, however, cultural measures are not a solution in themselves – human error will always prevail.

Arguably, there is also a concern that if an organisation is public in heavily investing in technological solutions that should mitigate some cyber risk then the employees of that organisation will get lax about ensuring their behaviour is vigilant; there is perhaps a false sense of over-assurance and so reliance in such technical fail-safes. Companies need to find the balance of not guaranteeing a security blanket – nor solely placing the blame on the information security professional when there is a problem and they expect technical controls to have prevented it – part of the responsibility also lies in company culture.

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.

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 February 2018 RANT Forum in conjunction with Acumin Consulting by Martha Tonks, with support from Daniel Beresford.

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