RANT+ DCMS: THE REPORTS

WRITTEN BY ACUMIN

CYBER METRICS

The Department for Digital, Culture, Media and Sport are currently researching how to support UK private industry in relation to cyber security. One proposition is defining a set of metrics that organisations could adopt that would display a holistic view of cyber resilience.

The department sponsored an event hosted by RANT Events and supported by Acumin Consulting that brought together a group of 100 cyber security professionals to discuss the potential benefits and drawbacks of implementing an industry standard of metrics, and an action plan of how this could be achieved in the future. The question posed for the evening was:

"How can we provide a snapshot of an organisation's cyber resilience to external stakeholders?"

The January RANT Forum had a panel consisting of Dr Rachel Anne Carter (Cyber Innovation, AmTrust), Peter Church (Solicitor, Linklaters LLP), Alex Holmes (Deputy Director of Cyber Security, Department for Digital, Culture, Media and Sport) and John Noble (National Cyber Security Centre). The Panel was chaired by Geordie Stewart (Head of Cyber Security, Nationwide Building Society).

The following report is a consolidation of responses to questions posed by the panel, and answers by both the panel and audience from the event. This forum is due to be the first of 3 discussing how to take this idea into a working practice. It was sent to DCMS post event to help with their research.

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

WHY DO WE NEED METRICS?

Metrics can be used to measure, assess and cost cyber risks. They can also be used to demonstrate what losses look like, both to an organisation's board and then to the wider public and government to help build up a better picture of the risks currently affecting organisations.

However, there is yet an agreement on which metrics are universally important to organisations to measure. In order for there to be an industry standard metrics need to be worked on collaboratively by a range of stakeholders.

It is especially important for organisations to share accurate information when they do suffer a breach and that that information is validated by multiple parties. Mandatory breach notifications is enshrined in the forthcoming GDPR and reinforced by the Network Information Security (NIS) Directive, which requires critical infrastructure providers to notify competent authorities of substantial impacts to public services.

How metrics are positive with regards to information gathering is certain, but there still needs to be a discussion of how this information is a) protected and b) used. Information relating to organisations vulnerability is a risk in itself. Therefore if the government are wanting to implement a standardised type of cyber risk reporting to UK businesses, then there must be an action plan of how they can intervene to alleviate some of that risk/ the effects of breaches to organisations.

Recent cyber breaches like the ones carried out against the National Health Service, Coincheck and Equifax illustrate the need for public and private sector organisations to adopt a more robust cyber security posture in terms of vulnerability management and incident response. Cyber Security is going through a market maturity where consumers are more considerate of a company's reputation during their own buying decision. If this is not incentive enough for organisations to become more critical of their own technical infrastructure, regulations such as GDPR will also cause market upheaval. Penalties for not taking care of customer's personal data at any point within an organisation's supply chain means that the board needs to make cyber security strategy a priority moving forward.

WHY ARE METRICS IMPORTANT TO ORGANISATIONS?

The argument for metrics giving power to the CISO. Having a standard of criteria that an organisation needs to achieve in comparison to its industry peers gives the CISO a level of leverage in the boardroom in terms of team performance and business investment decisions to plug any shortfalls.

Organisations who are breached can develop a better appreciation of how to manage their infrastructure against future attacks. The information from a metrics dashboard can be fed into the discovery stages of a brief as additional support.

Considering how only half of all UK companies currently have basic cyber security hygiene, metrics should be adopted in conjunction with other regulations such as GDPR. Having a set type of reporting will also help organisations benchmark themselves against meeting other related regulations including GDPR.

For certain industry sectors, or SME's that currently do not have a legacy of prioritising cyber security, having a standardised set of metrics could greatly contribute to overall industry cyber awareness and individual organisations could benefit from the experiences of others.

Cyber metrics need to be able to provide transparency on risks in real time, both inside and outside of the organisation.

Metrics can alleviate the pain of the skills gap by giving organisations a better view of their current optimisation of resources. A standardised set of metrics will be able to help organisations see patterns and trends over time and to focus spend or talent acquisition accordingly.

WHY ARE METRICS IMPORTANT TO GOVERNMENT?

The case for greater visibility of industries overall security status is obvious.

When we consider the amount of UK organisations that currently don't take substantial cyber security measures, how much responsibility can we attribute to the government in not educating and expressing the importance of taking a more constructed approach? In order for the government to be able to deliver effective campaigns and policies, more intel must first be gathered so that the government can see the extent of the problem.

There is a general distrust in the current available market data on breaches and incidents, as it is down to the organisation in what they share. Examples where firms who have suffered breaches have been slow in sharing information to the public displays the lack of incentive for firms to do so. The government can play an important role in reporting on incidents and how tacit the private sector's cyber security is, and advising organisations on how to manage their risk.

It is important to consider how the government can use data gathered from GDPR as part of the reporting on cyber security. The government has access to far more data than the average organisation, and therefore should be looking to create something substantial to different markets.

It is also worth mentioning the concept that cyber-crime is also a national risk, not just one that relates to individual organisations. Most current risk assessments don't include war, and yet cybercrime is an evolving threat from entire nations. The government needs to understand the risk to its country, and take a level of responsibility in protecting companies. In practice, cyber attacks have many differing scales of likelihood. There needs to be a way of attributing value to the different types of attack (motive included), in order for information gathering to be successful.

This ties into the argument that in economics terms, cyber security is a market failing. To what extent should the government intervene to gather resources to aid organisations engage with practical solutions?

HOW WILL METRICS HELP ORGANISATIONS WHO HAVE BEEN BREACHED?

A key consideration for most organisations, if they are expected to spend more in order to develop a set of metrics looking at cyber security, is the return on this investment.

If metrics display a negative outlook for an organisation, then there may be little incentive to start on adopting. However, for some organisations they will likely see the potential in linking metric displays and insurance premiums.

Organisations will likely go through a period of change with regards to insurance deals once information on cyber security status becomes more visible.

Moreover, it may be that insurance pay outs benefit if it is shown that organisations took reasonable measures to protect their infrastructure. Metrics can act as a form of 'guarantee' if they show a consistent standard of organisational security.

Metrics themselves may be able to help insurance companies develop a better understanding of cyber risk, which is transformative in nature. Increasing regulations such as GDPR and the provision of standardised data across industry sectors helps insurer's benchmark organisations against their peers, and gives better insights into the likelihood of certain attacks/ security flaws.

Therefore, metrics may be able to give an objective view of organisational cyber security 'health' to better delineate how insurance companies work with them.

HOW SHOULD METRICS BE IMPLEMENTED CONSIDERING DIFFERENT ORGANISATION'S STRUCTURES AND INDUSTRY FEATURES?

The reality is, currently there is no agreed view of what an ideal dashboard of metrics would look like. There may be certain methodologies that can be used to create a common approach across government and enterprise.

Some breaches are more fatalistic depending on a myriad of factors such as; example of data entries, how many records are breached, costs associated, how has the data been sold, what kinds of organisations been targeted. Other considerations would also be the nature of the information taken and the organisation's reputation in the market as being trustworthy. A similar size breach on one organisation could cause a vastly different reaction in another if it were to greatly effect customer loyalty.

Metrics need to be neutral in terms of valuing brand reputation, but sensitive to the complexity of breaches comparative to one another. How organisations are judged when they experience a breach needs to be flexible to the situation. The challenge to government is in introducing metrics that are supportive of that reality.

A large commonality across many sectors is that human behaviour is a major cause of why breaches occur and how they end up being dealt with. Metrics need to be able to assess the human risk within organisations and look at internal cultures in order to give a fair representation of how well an organisation would be able to cope with a cyber-attack.

Cyber metrics should also make reporting on cyber security easier, not harder. Cyber risk is in the marketplace already, and it's important that a government initiative does not create a reverse incentive for organisations. The format should be reflective for regulations already existing in the market such as GDPR. Metrics must be a natural progression from what a board room is looking for, and not be abstract to the information a business would value. Therefore, a good metric dashboard structure would break down the need for duplication or lengthy internal processes. This approach should work well across any size or scope of organisation.

WHAT ARE THE POTENTIAL PITFALLS OF ORGANISATIONS PUBLISHING METRICS ON THEIR CYBER SECURITY STATUS?

Namely, how can government effectively respond to more incident reporting? Currently, there is a lack of clarity in the private sector as to where and how they can report an incident to the government. The NCSC states that only 20% of cyber-attacks are reported by victims. If this is partially because some organisations are not aware, if they do start a process of measuring their risk factors and take a more active interest in their cyber security, would it lead to more support from the NCSC being demanded?

There needs to be a routine in which the government protects organisations and incentivises them to come forward about data breaches rather than punish those who do.

The government also needs to manage expectations, which only the most serious breaches will be responded to, as there are not enough resources to deal with everyone.

Also, for organisations, creating public records of vulnerabilities is a risky venture. Metrics can potentially provide criminal parties with an insight into their security weaknesses.

Organisations should have a voice in deciding what types of metrics should be included, and how much information should be gathered depending on the type of organisation they are.

CONCLUSIONS

The discussion on the topic needs to delve further into what types of metrics should be universally important to organisations regardless of sector.

The government should strive to research how it can be of use to victims, and how it could potentially utilise the reporting in a way that drives long term benefits to the private sector. This would be in both reducing cyber-crime, and enabling organisations to be better armed with information to defend themselves.

Metrics will likely provide a platform for information sharing and change within individual sectors. SME's and lower technology focused businesses will likely be most influenced if cyber security metrics were adopted nationwide, as they are less likely to be aware of cyber principles to begin with. Adoption may be an issue if the government is not able to educate smaller businesses on the importance of measuring cyber security resilience. Additionally, lack of available resources to invest in practical measures may inhibit some businesses.

Larger organisations with complex supply chains will most likely benefit from cyber security metrics being adopted. However, they could be slower to adopt it, as it brings in additional risk to the organisation and opens up strategic management to criticism.

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