What is a risk-based approach to cyber security and how do you show evidence of it?

Simon Marvell
Partner
simon.marvell@acuityrm.com
www.acuityrm.com

1. Introduction

Regulations such as EU GDPR, and standards such as ISO 27001 require a risk-based approach to cyber security. But what does this mean and how can you show evidence of a risk-based approach? This is an increasingly important question because organisations that suffer a breach may now face substantial fines and reputational damage unless they can provide evidence of a diligent risk-based approach.

Example: EU General Data Protection Regulation

**Article 32** requires data controllers to ‘ensure a level of security appropriate to the risk’. Controllers can comply with this requirement by implementing ‘technical and organisational measures’ that mitigate the risk.

**Article 83** sets out the factors authorities must consider when imposing penalties for violations of the GDPR and suggests that fines should be imposed in accordance with the risk profile of the operation and the extent to which the controller appropriately addressed the risk. It follows that a controller may face reduced fines or avoid fines altogether by addressing the risk of its activities, even if such measures fail to prevent a data breach.

The Risk-Based Approach in the GDPR, Interpretation and Implications. Gabriel Maldoff, CIPP/US, IAPP Westin Fellow.

There is general agreement within the industry on the aims and requirements for cyber security risk management, however the practical implementations of risk-based approaches often fall below the standard that is likely to be required by regulators.

This paper describes how you can implement, and show evidence of, a truly risk-based approach to cyber security.

2. What is a risk-based approach to cyber security?

Let’s first be clear about what it’s not. It’s not the latest operational cyber security technology, whether it’s artificial intelligence, threat intelligence or data analytics. As much as vendors would like you to believe that you need their technology to comply with GDPR or other regulations (and they may well be a part of the solution) buying these products will not provide evidence of a risk-based approach.
Regulations and standards are consistent in their definition of cyber security risk management, a good example being the NIST Cyber Security Framework.

**Definition: Risk Management**

Risk management is the ongoing process of identifying, assessing, and responding to risk. To manage risk, organisations should understand the likelihood that an event will occur and the resulting impact. With this information, organisations can determine the acceptable level of risk for delivery of services and can express this as their risk tolerance.

With an understanding of risk tolerance, organisations can prioritise cybersecurity activities, enabling organisations to make informed decisions about cybersecurity expenditures.


This relatively simple definition belies a wider range of inter-related information which is required to form a true understanding of cyber security risk:

- **Our objectives** - what we are seeking to achieve and therefore protect, e.g. to achieve business goals and / or to protect the rights and freedoms of individuals in our processing of sensitive personal data
- The **information assets** that we must manage effectively to achieve our objectives and how they inter-relate with each other and with business processes
- The potential **impacts** on the business from a breach involving information assets, or in the case of personal data on the rights and freedoms of individuals
- The **threats and threat actors** that could cause these impacts and the nature and scale of these threats
- The **vulnerabilities** that left open could be exploited by threats to cause the impacts
- The **controls** that are mitigating the risk (prevent, detect, etc.) and their effectiveness and performance
- **Incidents, near-misses and other events** that indicate what is happening in practice
- Based on all of the above, the **current residual risk** to business objectives, targets or indicators (and the rights and freedoms of individuals) and whether or not these are within tolerance and / or can be accepted
- The **actions and risk – based priorities** for addressing unacceptable risks and the extent to which these actions are being implemented in a timely and effective manner.

Some of these variables relating to threats, vulnerabilities, control performance and incidents can change frequently so they need to be easily monitored and whenever necessary easily adjusted. They also interact: the existence of exploitable vulnerabilities on a system which supports a critical business process at a time when we have weak controls and when threat actors are targeting us represents a very high risk.

And since we need to provide evidence of a risk – based approach we need to maintain a history of our assessments, actions and decision making.
3. Managing complexity in risk-based approaches

Authors of standards and regulations have been quick to require a risk-based approach to cyber security, and rightly so, but this doesn’t mean that it is easy. Managing and correlating all of the risk information described above has shown itself to be a non-trivial exercise.

Cyber security risk management is a relatively young discipline and is more complex than other more established risk management disciplines.

Example: Credit Risk Management

Credit risk management has been practised for decades and has a large body of skilled practitioners, but has relatively few variables and a long history of data. This data shows that (within a range of probability) if interest rates go up by X%, loan defaults will increase by Y%. If we predict the interest rates will go up we can reduce the risk of default by tightening our lending criteria.

However, even relatively mature risk management disciplines can struggle to forecast risk, as was evidenced during the 2007/8 financial crisis.

Now consider some of the additional complexities of cyber risk management:

- There are many different potential perpetrators (threat actors) and we don’t know who they all are
- There are many methods of attack with more appearing all the time
- Detection of a breach can be difficult, we may already have been breached and not know it
- Protection against a breach requires a wide range of inter-connected control strategies involving technical, procedural, physical and personnel measures.

In addition to the wide range of deliberate threats, there are many other dangers, including failures, errors, failures compounded by errors, disasters and so on.

Against this complexity we have relatively limited comparable data on incidents. Yes, we have some great reports on data breaches from Verizon, Symantec, the Ponemon Institute and others but no two organisations are the same, each has its own ways of doing things and cyber security processes of varying degrees of sophistication which makes it difficult to cross-compare.

Managing complexity is a key issue in the delivery of a practical risk-based approach to cyber security.
4. Beware over-simplified risk-based approaches to cyber security

Most organisations maintain risk registers, most often in spreadsheets, to log and track the Enterprise risks that could impact on the ability of organisations to achieve their objectives and meet their targets. These usually involve simple assessments of perceived impact and likelihood, before and after taking action to mitigate the risks.

**Example: Simple Risk Registers**

Simple risk registers work well when the number of variables is low and there are clear mitigation strategies. If we worry about our top sales team defecting to a competitor we can review their compensation, tie them in contractually, put contingencies in place and monitor the risk. The user can visualise the problem and the solution, make reasonable assessments of the risk and decide whether or not it is tolerable.

This Enterprise risk management approach is increasingly understood and embedded within organisations and is therefore an obvious place for managing and reporting cyber risk. However, problems arise with visualising cyber risks sufficiently well to be able to make reasonable contextualised assessments. Without all relevant information, many users fall back to what can only be described as guesswork. The implications of this are a likely under or over spend on security and the real possibility of damaging incidents still occurring.

In such circumstances, it is unlikely that regulators will be convinced that a diligent risk-based approach is in place.

**Warning! Spreadsheets**

If you are using or contemplating spreadsheets for demonstrating a risk-based approach to cyber security you will almost certainly be driven down the over-simplified route. Spreadsheets can’t link and usefully provide the required visibility of all risk – relevant data and you will be forced to compromise. For further information see the whitepaper:

We need to move on from spreadsheets for compliance and risk management

5. A practical risk-based approach to cyber security

Avoiding the over-simplification trap requires additional visibility of important risk related information but this doesn’t imply capturing masses of additional data – far from it, we need to be selective and focus on what is really important.

Equally important is having the right mind set. We know that if we want to participate in the digital economy then we can’t guarantee to avoid cyber breaches. The saying ‘no risk, no reward’ holds true and organisations that innovate for the greater rewards to be gained will, at the same time, be likely to expose themselves to additional risk.
Key Requirement: Change in mind set

The change in mind set required is to make informed decisions on whether or not we are prepared to accept cyber risk and, very importantly, to recognise as part of this that occasionally these decisions may be wrong.

When we accept a risk, we are doing exactly that; accepting a risk not a guarantee, and if that risk materialises following an informed decision then we shouldn’t fire the person who accepted the risk but instead should learn from the experience to improve our risk management processes.

Clearly there are some pre-requisites – we need good cyber security hygiene, i.e. the cyber security basics should be done well and compliance with an information security management system standard such as ISO 27001 is a very good start. We also need to take account of the law, regulations and good practice relevant to our handling of information, particularly sensitive personal information.

With the pre-requisites in place then what does a practical risk – based approach to cyber security look like? There are 7 important requirements as illustrated in Figure 1:

**Figure 1:** 7 requirements for a risk-based approach to cyber security

1. Set the right scope
2. Capture and correlate relevant risk information
3. Make risk – informed decisions
4. Report in the language of business leaders
5. Maintain evidence and history
6. Accept accountability
7. Monitor and continually improve
1. Set the right scope

Understanding and setting the right scope for cyber risk management is critical. If it’s too detailed we get dragged into over-analysis and unfathomable detail on low-level issues which are really day-to-day IT or security operations activities. Too high-level and we fall into the over-simplified trap discussed earlier and end up with a risk-based approach which isn’t fit for purpose.

There are two important inter-related considerations when setting scope:

- **The scope of business information processing**, which includes:
  - Information assets being processed, stored and communicated in each part of the business
  - Mapping of information assets to business processes and functions, third parties, technology assets and environments.

- **The scope of risks being assessed** – this needs to be set at a level which is relevant and meaningful to business leaders who will be asked to accept or reject risk but of sufficient granularity to allow differences to be identified and resources targeted at the highest risks. GDPR provides a good example of a meaningful yet discrete scope for assessing risk related to the processing of personal data.

Example: GDPR Article 32, Para. 2.

In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

Many risk managers struggle with setting scope but it’s worth taking time over this because if its set correctly, the following requirements will become much easier to deliver.

2. Capture and correlate relevant risk information

The more good information we have, the more likely we are to draw the right conclusions and make the right decisions. As we saw above there are many factors that contribute to our understanding of cyber risk but these only come together to provide valuable information (on which we can make risk-informed decisions) if we can understand them in the right context. Figure 2 provides examples of poor / incomplete and good information on cyber security risk.
In Figure 2, the poor or incomplete examples lack the mappings and context necessary for good information. On the other hand, the good examples correlate relevant risk factors for more valuable contextual information.

3. Make risk – informed decisions

With good correlated and contextual information, we can make risk – informed judgements and decisions:

- Which risks are currently acceptable with no further action needed for now, other than monitoring?
- Which risks are currently unacceptable and require action?
• What actions will be most effective in addressing unacceptable risks, to what degree and, therefore what is the risk – based order of priority for completing these actions?

Individual actions can, at the same time, help to address multiple risks so we again need good visibility to identify and prioritise actions across our complete risk landscape.

4. Report in the language of business leaders

Ultimately risk owners in the business are responsible for accepting cyber risk, often with the assistance of cyber risk specialists. To make decisions, business leaders need good, credible information in a language that they understand, i.e. that relates to business objectives or legal obligations, such as protecting the rights and freedoms of individuals.

Business leaders are not interested in technical data, such as the number of vulnerabilities patched last month. They are interested in the top 10 cyber security risks, what these mean in business terms, what’s being done about them and who’s responsible. And then they want to see progress at the next update.

Business leaders understand risk registers and use these for tracking Enterprise risks so a series of risk registers showing summary data with drill-down for more detail is a good way to present cyber security risk in the language of business leaders, but only where conclusions and decisions are based on good visibility of relevant correlated information.

5. Maintain evidence and history

We make better decisions when they are based on evidence rather than theory so we should capture evidence and maintain historical records to back up our decisions, for example the maturity and effectiveness of controls at the point when risks were accepted, how we assessed the risks and our reasoning behind risk acceptance. Evidence of a diligent risk – based approach with risks identified and appropriately addressed will be important in mitigating damages that could result in the event of a breach.

6. Accept accountability

Since we can’t completely avoid risk there will always be a point at which we must accept risk and this will balance varying trade-offs, such as:

• business benefits versus the rights and freedoms of individuals
• less secure but greater user experience versus more secure but impaired user experience
• cost versus benefit.

The ability to accept risk increases with seniority and the highest risks need to be accepted by business leaders, based on full visibility of risk information, supplemented with evidence and historical records.
Those accepting risk need to accept accountability for their decisions and be prepared to respond in the event that the risk materialises and a breach occurs.

7. Monitor and continually improve

Risk is accepted at a point in time and we can capture evidence of the risk status at the point of acceptance, however the acceptance is out of date almost as soon as it has been made. The performance of controls can deteriorate, new vulnerabilities can be identified, new threat intelligence can appear and incidents can occur which throw a new light on our understanding of risk. We therefore need to monitor our risk status and be alerted when changes result in risk increasing to above the level at which it was accepted, so that we can initiate actions to bring risk back within tolerance.

Also by monitoring and learning from our risk assessments compared to what happens in practice we can adjust our processes and continually improve our cyber risk management.

6. The need for automation in a risk – based approach to cyber security

Automated tools play an essential role in cyber risk management. As we saw above, spreadsheets will drive you down an over – simplified path because they can’t manage, correlate, aggregate and report on the many cyber risk variables described in this paper.

Automation can provide real benefits in the following areas:

- Holding and correlating all relevant risk information providing easy visibility of the information required to assess and accept risk
- Maintaining a history of assessments and decisions with evidence to show auditors and regulators
- Aggregation and reporting of risk in the language of business leaders
- Action management with workflow, alerting and reminders.

These requirements can only be delivered by a software solution designed exactly for this purpose which ideally is also quick to deploy and easy to use.

Acuity’s STREAM Cyber Risk Platform is such a solution, with editions for small, medium and large organisations. Some examples are illustrated below.

Users with complex compliance obligations and / or complex organisational structures, will often benefit from the expertise of third party cyber security risk specialists. Acuity works in partnership with a number of Professional Services organisations, such as CGI UK, to deliver this specialist expertise, together with integrated ‘compliance profiles’ and risk data for users to adopt and adapt.

Figure 3 below illustrates how through having easy access to relevant correlated information, we can make informed decisions on whether or not we can accept risk.
Figure 3 – Correlated information on risk status

Figures 4 and 5 show, respectively an example cyber security risk register and an example of an aggregate view across multiple cyber security risk registers for one part of an organisation.

Figure 4 – Example cyber security risk register

Figure 5 – Example aggregate view across multiple registers for one part of the business

Further information on STREAM is available on the Acuity Risk Management website.
7. Conclusion

A risk-based approach to cyber security is increasingly being mandated by regulations and standards and provides significant benefits to organisations by: reducing the risk of damaging security breaches; optimising cyber security activities; and, in the event of a breach mitigating damages through demonstration of a diligent approach.

A risk-based approach can be complex but over-simplification must be avoided. The 7 key requirements described in this paper form the basis for a practical risk-based approach to cyber security.