John Leach Information Security

JLIS Modelling and Analysis

Examples of analytical tools

February 2018

John Leach, Ph.D.
Director, John Leach Information Security
Tel.: (+44) (0)1225 332 134
Mob.: (+44) (0)7734 311 567
e-mail: john.leach@jlis.co.uk

Introduction

Despite Cyber Security being predominantly about bits and bytes and technologies, security risk management tends to be practised as a craft rather than as a science. Security managers adhere to standard recipes for how to secure business operations, recipes we call 'Best Practices'. And they can follow those recipes without needing to have a deeper understanding of the chemistry that is going on under the covers to give rise to the security risks they are trying to manage. It doesn't need to be this way. What I bring to the table is a rare, if not unique, ability to take a scientific approach to Cyber Security matters. I enable my clients to get objective quantified insights into the components that contribute to their security risk so they can manage those risks in a more informed and confident manner.

The actual deliverables I create come in a wide variety of different forms. I develop bespoke solutions customised to the individual client and their particular need, so the range of possibilities is almost endless. Some of these solutions are relatively straightforward tools that help my clients take the initial steps to becoming more analytical, and some are much more intensive tools that have more demanding data requirements but provide more incisive results. To clarify the sorts of solutions I develop, I have written this short paper describing some of the analytical tools I have created for clients in the past few years.

The first question to ask yourself is this: Would taking a more scientific, analytical approach to your cyber security challenges suit you or not? If yours is a scientific, engineering or technology-intensive organisation, then probably the answer would be Yes. But don't presume the answer always has to be Yes. Taking a scientific approach can help you gain objective actionable security risk insights and manage your security risks more confidently. But as you move beyond the initial steps, it gets less simple than just following Best Practices. The later stages are not for everyone.

If you are interested in knowing more, then here is an outline of some of the analytical tools I have created for clients in the past few years. The first and last in the list, Threat Maps and Incident Profiles, are what I refer to as the 'anchors' of a risk quantification programme. They are the ones your programme should start with. Threat Maps give you a 'heads up' view of the problems you are facing, and Incident Profiles show you how well or how poorly you are dealing with those problems. They set the context and the urgency for the rest of the programme to follow.

Please be aware that, in addition to the tools listed here, I have designed over three dozen security risk metrics for clients. These are metrics that measure the rate of progress of the risk chemistry that is taking place at various places within an IT infrastructure. They quantify how security risk is developing so security managers can deal incisively with the particular risk issues they find lurking there.

Threat Management

Threat Maps

A Threat Map gives you a structured, systematic and transparent way to identify and rank the main security threats you face. It gets your various security teams to agree on one threat list so they can all work together effectively.

A Threat Map is, basically, a list of the main threats within your threat landscape with each one assessed according to its importance to your organisation. It is structured so you can be confident you are covering all the threats that might matter. You can include all types of threat within the one map, including internal threats, external threats, malicious threats and unwilful threats (i.e. acts of God or Mother Nature). You can rank them both overall and by type.

A Threat Map gives you a systematic way to rate each threat, regardless of type, in several dimensions (the two most common dimensions being 'Prevalence' and 'Capability') so you get to see how important each threat is for your organisation. Many of these ratings will start out being subjective. The threat map will encourage you to gather threat data for your top ranked threats so you can confirm or adjust the assessments you have made.

The process of building the Threat Map is transparent so, instead of your different subject matter experts each pulling in different directions based on which threats they personally think are most important, you can get them all to agree on a single set of threat rankings so their teams' efforts become better aligned.

The map shows you what you need to track about each threat from one reporting period to the next. This way you get an early warning whenever a threat evolves and moves into or out of the top rankings. You can track meaningful trends and, on the basis of those, forecast what your security risk might look like in one, two or three quarter's time.

Threat Profiles

A Threat Profile shows you not just how prevalent a threat is (i.e. how often you are seeing relevant attacks) but how capable the threat is at causing you harm. That way you can manage the threat according to the risk it causes you not just according to its level of activity.

The rate at which attacks occur changes all the time, but that doesn't mean your risk changes in the same way. You might see an increase in the overall rate of attacks but that could conceal a decrease in the rate of attacks that matter the most. Your risk could be increasing, decreasing or staying about the same.

A Threat Profile shows you not only the overall rate at which attacks are occurring but, importantly, also how that overall rate is distributed between attacks

you need to know and worry about and those you don't need to worry about because your controls are more than adequate at dealing with them. It is the attacks your controls are less capable of dealing with that create your security risk, so this is the part of the threat profile you will want to keep an eye on and respond to.

A Threat Profile is a dynamic measurement of the current threat and it fluctuates with time. You will be able to distinguish between short-term fluctuations and set trigger levels so you respond tactically when a fluctuation becomes sufficiently significant. For example, you might make a temporary tightening in one or two relevant controls as the threat storm hits you and then relax that tightening once the storm has passed. And you will be able to remove the noise from the signal to see the long-term trends. Those will be the results that drive your security strategies.

Security controls

Controls Maps

A Controls Map gives you a structured and systematic way to assess your security posture and present that posture in a format that is clear and sensible for non-technical management.

A Controls Map is, basically, a highly structured list of controls in which you categorise and rate each control to show in what way and to what extent it contributes to providing you with security protection. These controls could be your baseline controls, i.e. the ones you require all the systems in your IT estate to implement. They could be a standards-based set of controls such as ISO/IEC 27001. Or they could be a more targeted set of controls such as the ones you use to measure your GDPR compliance posture against.

The Controls Map shows you what proportion of your security effort is aimed at reducing the likelihood of security breaches occurring, and what proportion is aimed at reducing the impact of breaches when they do occur. The balance between reducing likelihood and reducing impact that you should have should reflect the way you use technology. If you provide real-time high-value services online, you will focus heavily on reducing likelihood. If you are a manufacturer of consumer goods, your will want a more even balance. A Controls Map shows you your balance and helps you rebalance your controls if that is needed.

One of the problems with adhering to Best Practices is that it requires you to implement a large number of security controls without any guidance as to which controls are critical to your protection and which are secondary. A Controls Map provides you with that guidance. It shows you which controls are the most effective at providing protection and which are worth having but only just. Instead of following Best Practices blindly, you can focus your security effort and attention where it does you the most good. You can map your controls against your top ranked threats (taken from your Threat Map – see above)

and make sure you have sufficient 'defence in depth' against each top threat, adding additional depth where it is needed.

You can integrate your Controls Map with your security compliance assessment process to go beyond just scoring assessments by compliance percentage to showing a meaningful security posture that can be compared with your organisation's stated risk appetites. Technical and business management can both see which systems are adequately protected and which are the wrong side of permissible risk limits. The security posture results show where your controls shortfalls are so you can build meaningful risk mitigation action plans that will not just get you a tick in the box but will do what is needed most effectively to bring your security risk back to within your organisation's risk appetites.

Control Effectiveness Models

A Control Effectiveness Model is the way to quantify the effectiveness of a chosen security control across the range of different attacks contained within the relevant Threat Profile. It shows you what that control could optimally achieve against that threat, whether your implementation is anywhere near that optimal level, and what you would need to change to achieve that optimal level.

A Control Effectiveness Model is built for each individual control and each specified threat. Here having the right scientific approach is essential, and this is why calculating control effectiveness has proven to be so difficult in the past. You start by working out the right way to define 'effectiveness' given the particular threat / control combination of interest. You determine what effectiveness depends on, and you calculate what it would be (as a % value varying between 0% and 100%) across the full range of attacks covered in your Threat Profile. Effectiveness is calculated both as a function of the characteristics of the threat and as a function of how that control is implemented, configured and operated. This is an enormously powerful result.

You compare the results from your model with the current profile of the threat to get a quantified measure of the overall level of effectiveness that control is achieving. Because the model takes account of the current threat profile, you can calculate how the control's effectiveness would change if the threat were to change. Because the model takes account of the way the control is implemented, you can calculate how your control's effectiveness would vary if you changed any of your control's settings. You can see whether your control is currently stretched to its limits or whether you have spare capability you are not making full use of, and what you would need to do to counter any growth trend in the threat.

Instead of building security metrics that measure only how widely your controls have been implemented you can build risk metrics that show you how effectively your controls have been implemented. You can make control improvements that will make a meaningful difference to your security risk, and you can avoid wasting time and effort on improvements that would bring little risk-reduction return. You can build cost / benefit models to justify further security

investment, and business leaders can decide which security initiatives they want to support and which risks they are prepared to live with.

Vulnerability management

Vulnerability Profiles

A Vulnerability Profile shows you the size and shape of the attack surface your organisation is presenting to a particular threat. By comparing the results from your Vulnerability Profile with the results from your Threat Profile you can see which part of your vulnerability population is responsible for the security breaches you are experiencing, and you can focus your vulnerability management efforts where they will have the most effect.

A Vulnerability Profile shows you the extent to which you are vulnerable to a particular threat, not just as an overall High / Medium / Low figure but as a figure for each section of the profile for the threat you are facing. If your vulnerability peaks around the kinds of attack the current threat is bringing you, then you have a critical problem. If your vulnerability is predominantly to less likely attacks, then maybe you have a little more time to deal with the situation.

Of all the analytical tools I describe in this list, the Vulnerability Profile is usually the most difficult to build. This is because it is typically the composite result from a combination of models. It takes more effort to formulate and requires more data to compile the results. For this reason, Vulnerability Profiles are good to know about but should be put aside until a later phase of your risk quantification programme.

Business risk

Value-at-Risk (VaR) Calculators

A VaR Calculator is a structured way to identify in financial terms how much harm a realistically possible major security incident could cause you. It gives everyone at Board level a realistic understanding of what the organisation could lose so security provision gets the priority and attention it deserves at the top table.

A VaR Calculator covers all your major asset types and each of the different types of business harm a serious security incident could cause (direct financial, brand, regulatory, etc.). It provides a structured way for you to estimate the magnitude of the harm you could be caused. Instead of just having a vague sense that a major security incident could cause the business a lot of harm, the VaR Calculator shows you which incidents could cause you most harm, how much harm they could cause in financial terms, and what types of harm are

most likely to arise. It helps you prioritise where you need to provide the most security protection and what type of security protection you most need, and it shows you the depth of reserves and resource capabilities you would need to enable you to survive and recover from each type of eventuality.

A VaR Calculator can be used on its own as a way to engage Board members in the need for appropriately structured security provision, and it can be used with a Business Risk Map (see below) to determine, to the next level of detail, what types of security provision you need to prioritise.

Business Risk Maps

A Business Risk Map gives you a structured and systematic way to identify and rank the main pathways by which security incidents can cause you operational and business harm. It helps business leaders articulate the business' susceptibility to major security incidents, and it tells the security function what type of security protection it needs to provide.

A Business Risk Map is, basically, a list of your mission-critical activities with each one mapped to each of the different types of significant security incident your organisation could experience (data theft, data loss, systems outage, etc.). It brings into view all the major pathways by which security incidents could cause you significant business impact, and gives you a way to rate each pathway in several dimensions so you can see how susceptible your business is to being harmed by each type of incident.

The mapping reflects the nature of your business operations and the way the fulfilment of your mission relies on your use of technology. It steps through each type of major security incident and gives you insights into not only which areas of business activity are most likely to be affected by security incidents but also which areas would suffer the greatest disruption if they were affected. It brings to the fore the less likely pathways that could result in critical impacts and balances them against the more likely pathways that typically would cause less harm. It helps business leaders articulate their concerns and needs, and it helps the security function provide the balance of protection the business requires. Security gets better aligned with business need, and business leaders get more assurance for the money and effort they put in.

Incident Profiles

Incident Profiles show you not just how much harm each type of threat has caused you over the past reporting period but how that harm has been distributed across the larger number of small incidents and the smaller number of large incidents. It helps you decide on both the overall amount and the right mix of security protection you need for each threat.

Some organisations (but surprisingly few) gather data about the incidents they suffer. For those that don't, their approach is sometimes to blame the victim rather than try to learn from the incidents that occur. Of those that do gather

data, the two main challenges they face are to gather data consistently across the full range of their operations, and to extract meaningful and actionable insights from the data they collect. Both challenges can be addressed by incident profiling.

Incident profiling involves building a structured scheme for the data you capture about each incident so the data can be aggregated to provide meaningful headline results. Its emphasis is on getting a full understanding of business impact. It is the guidance system for security planning: without it security plans are flying blind. Incident profiling enables you to attribute incidents to threats, it gives operations teams a meaningful and consistent way to report the effects incidents have on their activities, and it gives both business management and security management the data they need to identify the level of security protection needed and the aspects that need strengthening.

The main consumers of the results are the business areas themselves. They get to see the full magnitude of the impact security incidents have on their business activities, not just the occasional headline incidents but also the smaller more frequent disruptions. Smaller disruptions often get overshadowed by larger incidents and don't get recognised for the aggregate impact they have. This encourages reporting teams to gather the data consistently and continuously across their operations and leads to action plans that address the breadth of security incidents not just the headline events. And, because the resultant profiles are dynamic, you will be able to distinguish between short-term variations that can be ignored and long-term trends that indicate meaningful variations in the threat and call for the corresponding strengthening of controls.