1. Introduction

Recent cyber security breaches, such as those at Ashley Madison, the US Office of Personnel Management and JP Morgan Chase have demonstrated the real and present threat from cyber breaches. Director of the National Security Agency and head of the United States Cyber Command, Admiral Mike Rodgers has been moved to state that ‘It’s not about if you will be penetrated but when’.

In response, there is an urgent need for organizations to truly understand their cyber security status and where necessary take urgent remedial actions to rectify weaknesses. If there isn’t sufficient visibility of cyber security status, organizations won’t be able to manage cyber security risks and they will almost certainly suffer a breach.

By ‘visibility of cyber security status’ we mean having the complete picture, with measurements so that we can answer the following questions:

- What are our current measured levels of cyber security risk across the Enterprise from the multiple threats that we face?
- Are these cyber security risks tolerable?
- If not, what is our justified and prioritized plan for managing these risks down to tolerable levels?
- Who is responsible and by when?

The ability to measure cyber security status is fundamental; if we can’t measure then we can’t manage. Security incident and event management (SIEM) and data analytics solutions can provide valuable indications of actual or potential compromise on the network but these are partial views, indicators of our overall risk status but not measurements of our risk status.

Similarly, threat intelligence services can identify data losses and provide valuable indications of actual or impending attacks but again these are not measurements of our risk status. The same can be said individually about outputs from compliance management, vulnerability management, penetration testing and audits.

Only by pulling together all of the relevant indicators and partial views can we develop overall risk-based measurement and visibility of our cyber security status.
When we have confidence in our cyber security risk measurements we can respond to events and make decisions quickly, for example:

- We can identify risks that we aren’t prepared to tolerate and have a clear and prioritized risk-based action plan for the control improvements necessary to reduce these risks to an acceptable level.
- We will have a better understanding of the implications from threat intelligence or outputs from SIEM and data analytics allowing faster, better targeted responses.
- We can develop risk-based justifications for investment in cyber security solutions and services.

But with the very high level of threat and high rates of change in both the threat and control landscapes we need to be able to refresh our view of our cyber security status on an almost daily basis.

Cyber security risk management which previously might have been an annual process as part of planning and budgeting is now a critical real-time facilitator in the battle against cyber breaches.

This paper describes the required attributes of real-time cyber security risk management, starting with a description of threat and control modelling, going on to discuss risk measurements and concluding with example outputs and benefits.
2. Threat and Control Modelling

Cyber security breaches occur when people, processes, technology or other components of the cyber security risk management system are missing, inadequate or fail in some way. So we need to understand all of the important components and how they inter-relate. This doesn’t mean that your risk management system needs to hold details of (for example) every end point and the status of every vulnerability on the network because there are other tools which will do that but the risk management system does need to know that all end points on the network have been (and are being) identified and that critical vulnerabilities are being addressed quickly.

Figure 1 illustrates key components and relationships related to cyber security:

- Cyber security breaches target **Data**, in most cases confidential data, such as customer records or other valuable information
- **Data** is stored, processed and communicated on, by or to **Assets**, such as software, networks, devices (servers, workstations, smart phones etc.), websites, people and third-parties
- **Threat Actors**, such as organized crime gangs, activists and nation states will deploy **Threats**, usually targeted at or via **Assets** to access **Data**
- **Controls** which defend against **Threats** are mostly applied to **Assets** and occasionally directly to **Data**
- Some **Controls** such as encryption of mobile devices protect against specific **Threats**, such as loss or theft of mobile devices, whereas other **Controls**, such as software patching protect against multiple **Threats**, such as crimeware, web app attacks, cyber espionage etc.
- **Threats** will aim to exploit weaknesses (or **vulnerabilities**) in **Controls** to access **Data**
- If the right **Controls** are applied to the right **Assets** and they are implemented effectively relative to the level of **Threat** then the organization will be able to defend itself against the **Threat**. If this is not the case then a **Data** breach will occur.
2.1 Control Modelling

The ‘Controls’ layer illustrated in Figure 1 can be expanded into three sub-layers as illustrated in Figure 2:

- Control Frameworks
- Control Solutions and Services
- Management Systems.

**Control Frameworks** are specifications of controls which are independent of the products and services by which they are implemented.

The SANS Top 20 Critical Security Controls (CSC) for effective Cyber Defense is widely accepted as a valuable Control Framework for cyber security but organizations will deploy the Control Framework that is appropriate for them.

Control Frameworks are implemented by means of **Control Solutions and Services**. These can range from policies and procedures actioned by users and administrators to automated cyber security products and managed security services.

A mapping of Control Solutions and Services from leading vendors to the SANS Top 20 Critical Security Controls Framework is available on the SANS website. [SANS Top 20 Solutions Directory](#).

To have assurance that all controls in the Control Framework are effective, whether implemented by manual or automated Control Solutions and Services, they will need to be deployed within an overall **Management System**, such as the Plan, Do, Check, Act (PDCA) cycle of ISO 27001.

![Figure 2 – Expanded view of the Controls layer](#)
2.2 Threat Modelling

The various threat types and threat actors that have resulted in Cyber breaches are well documented. In its annual Data Breach Investigations report Verizon has for the last 3 years seen the vast majority of incidents fall into 9 incident patterns, as illustrated in Figure 3.

![Figure 3 - Source: Verizon 2015 Data Breach Investigations Report (DBIR) Fig. 24 – Frequency of incident classification patterns across security incidents](image)

Similarly, the Verizon DBIR identifies that the majority of incidents were perpetrated by 4 main threat actors, as shown in Figure 4.

![Figure 4 - Source: Verizon 2015 Data Breach Investigations Report (DBIR) Fig. 28 – Relative frequency of data breaches by incident patterns and threat actor with bar charts showing a 3 year trend](image)

Other sources of information on cyber threats and threat actors include the Information Security Forum, the Symantec Internet Security Threat Report and the UK Government / PWC Information Security Breaches Survey.
2.3 Threat – Control Mappings

We defend against Threats by deploying Controls and we therefore need to understand the Controls which are effective against each Threat. Again, these mappings are quite well defined by various credible sources, including the National Institute of Standards and Technology (NIST) and the Information Security forum. Figure 5 shows a mapping between the SANS Top 20 CSC and the 9 incident patterns.

Some Controls are more effective against Threats than other Controls, for example minimizing administrator privileges is considered to provide higher attack mitigation than, say, document loss prevention although both Controls together will provide the greatest attack mitigation.

So to have visibility of risk we need to understand not only the mappings between Controls and Threats but also the relative potential effectiveness of Controls against Threats. Note the use of ‘potential’ here because Controls will only be effective if they are properly implemented as intended and kept up to date.

The National Security Agency (NSA) has prioritized the SANS Top 20 in terms of their attack mitigation priorities. [Attack Mitigation Priorities for the SANS Top 20 Controls]
3. Risk Measurements

When we understand the components that make up our cyber security risk management system and their inter-relationships we can turn our attention to risk measures – what we can measure or estimate to give us the real-time risk-based visibility that we need.

The National Institute of Standards and Technology (NIST) in publishing its risk-based Framework for Improving Critical Infrastructure Cybersecurity defined risk management as follows:

Risk management is the ongoing process of identifying, assessing, and responding to risk. To manage risk, organizations should understand the likelihood that an event will occur and the resulting impact. With this information, organizations 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, organizations can prioritize cybersecurity activities, enabling organizations to make informed decisions about cybersecurity expenditures. Implementation of risk management programs offers organizations the ability to quantify and communicate adjustments to their cybersecurity programs. Organizations may choose to handle risk in different ways, including mitigating the risk, transferring the risk, avoiding the risk, or accepting the risk, depending on the potential impact to the delivery of critical services.


3.1 Likelihood that an Event will occur

The likelihood that a cyber breach will occur is a function of the level of Threat compared to the ability of Controls to resist the Threat. If there is a high Threat and there are weaknesses or vulnerabilities in Controls which could be exploited by Threats then there will be a high likelihood that an Event will occur.

3.1.1 Measurement in relation to Assets

Threats are targeted at Data - via Assets - and Controls are applied to Assets. If a Threat Actor wishes to target certain Data it may deploy multiple different Threats against multiple Assets, all with the same aim – usually to steal confidential data. The level of Threat is driven by the motivation, capability and resources of the Threat Actor which may be broadly consistent across the different Assets through which the Threat Actor may launch its attacks - what may differ is the extent to which the Controls are deployed effectively on these various Assets.

So it can be practical to consider levels of Threat in relation to collections of Assets, often referred to as environments, rather than attempting to, say, assess the level of Threat to each individual endpoint. However, one vulnerable endpoint could be all that is needed for a Threat to succeed so
we need to ensure that all endpoints are adequately secured. So while Threats may be assessed in relation to environments, Controls assessment needs to be more focussed and targeted.

We need to be careful about the level of detail that we seek to hold in our risk management system, particularly in relation to the status of Controls. If we try to hold data on every Asset connected to the network then we will be building an asset discovery solution into our risk management system which is impractical and unnecessary because there are other tools that will provide this. Instead, the risk management system needs to know, through measurement, that the Control Framework is being delivered effectively, i.e. that:

- A suitable asset inventory discovery tool is in place and effective
- Appropriate tools, such as automated patching, are in place and that they are properly setup and managed
- We are achieving the desired outcomes which we can measure using suitable metrics, e.g. the percentage of endpoints up to date with the latest available patches.

In all cases weak or deteriorating measurements will indicate high or increasing likelihood that a breach will occur.

3.1.2 Quantifying Likelihood of an Event

To be able to understand cyber security risk in business terms so that we can compare against other business risks and make informed cyber security investment decisions we need to quantify cyber security risk in financial terms and we need to use some form of probabilistic measurement for likelihood of an event. A probability needs to be measured in relation to a time period, i.e. a 10% chance of a breach in the next week is much more serious than a 10% chance in the next year.

In practice, the period we are interested in is our ‘time to the next breach’, i.e. we want to do everything practical and reasonable to avoid a breach today, tomorrow or in the next few days. To avoid a breach today we need to make sure that we have suitable Controls in place, up to date and operating effectively to be able to defend against Threats that we are facing today. So we need to understand the level of Threat and the status of our Controls today. And if we find that our Controls are inadequate then we need to initiate urgent remedial actions.

Our ‘time to the next breach’ will continue to roll forward day by day but as it does so Threat levels and the performance of Controls can change. So we need to know that our assessment of Threat levels and the status of our Controls remain valid.

Threat levels will need to be updated when new information becomes available, e.g. through research, receipt of Threat intelligence or indicators from SIEM and data analytics.

For Controls, the frequency of update required will depend on the nature of the Control and vary from:

- Daily, e.g. patch status
- Event driven, e.g. testing web applications for common security weaknesses following changes
- Monthly or annually, e.g. gap analysis of staff security awareness skills.
The more frequent updates will tend to come via automated updates while less frequent updates can be applied manually.

It is critical that we have a real-time cyber security risk management capability which can react immediately to changes in Threat levels and Control status. However, while our focus is on the ‘here and now’ we also need to be mindful of the longer term and anticipate future Threats to give ourselves time to plan and deploy appropriate Control strategies.

Again, published information on the prevalence of Threats is available, for example Figure 6 shows the relative frequency of data disclosures by incident pattern and victim industry.

![Figure 6](image)

**Figure 6 - Source: Verizon 2015 Data Breach Investigations Report (DBIR) Fig. 28 – Relative frequency of data disclosures by incident patterns and victim industry with bar charts showing a 3 year trend**

### 3.2 Impact from an Event

As we have seen recently, the impact from a cyber breach can be very substantial and can include lost business resulting from reputational damage, loss of goodwill, increased customer acquisition costs and increased turnover of customers. In addition there can be substantial costs in detecting, investigating and responding to a cyber breach.

Significant research has been published on the cost of data breaches, most notably by the Ponemon Institute and IBM. The [2015 Cost of Data Breach Study](#) includes per capita costs by country and industry sector.

Researchers have found a strong correlation between the cost of a cyber breach and the number of records lost. Figure 7 shows the range of expected loss by number of records.
3.3 Level of Risk

By combining our understanding of the likelihood of an event and the resulting impact we can form a view on the level of risk that we face.

At the very simplest level if we think that the likelihood of a cyber breach, say, from an Activist WebApp attack on our on-line store in the next week is 10% and the resulting impact would be $10m then we are facing a $1m risk and we can decide whether or (most probably) not to tolerate the risk in which case we must take action to reduce the risk until it becomes tolerable.

Assuming that our on-line store is critical to our business model then we may not have the option to avoid the risk. We may be able to transfer some of the financial impact through insurance but we will still face potential reputational impacts so we will need to mitigate the risk by seeking to reduce likelihood, impact or both. We have little control over the level of Threat that we face but we can reduce the likelihood of an event by adding further Controls or improving the performance of existing Controls.

In some circumstances we may also be able to take action to reduce the impact of a breach, e.g. in the health sector by partitioning personally identifiable data and clinical data with separate access policies and Controls.

Most organizations will be subject to multiple Threats from multiple Threat Actors and therefore to multiple individual risks, each of which we need to make sure that we can tolerate. However, in aggregate, these individual risks could represent a substantial total risk to the organization and we therefore need to make sure that our total cyber risk also falls within our overall appetite for risk.

A comment about uncertainty. Figure 7 illustrates a range of expected losses by number or records. The centre column shows an ‘expected loss’ but the Average columns show the mean loss at a 95% confidence level from multiple incidents while the outer Prediction columns shows a very large estimated range from single events.

Similarly there is uncertainty in the likelihood of an event. We can’t say with certainty, as in our simple example above, that there is a 10% chance of a $10m breach in the next week.

In practice there will be both an impact range and a likelihood range with a corresponding level of risk range.
When faced with uncertainty, statistical analysis techniques can sometimes be used to estimate ranges of risk but these techniques are not particularly well suited to real-time cyber security risk management due to the lack of comparable data on the status of the Control environments under which measured breaches have occurred.

However, since we know that the cyber Threat is very high then as the status of Controls deteriorates we do approach certainty that we will suffer a breach. At the extreme where we have completely inadequate Controls then it is reasonable to assume that there is (a very close to) 100% chance of a breach sometime soon. We don’t quite know when, but it could be within hours or a few days.

We also have information on the relative frequency of breaches. For example, Figure 6 shows that in 2015, 36% of the cyber breaches in Financial Services were from Crimeware, 31% were from WebApp attacks and so on. These figures can be adjusted for Threat Actors (ref. Figure 4) and local variations, e.g. from threat intelligence and experience of incidents and near-misses.

We can use this information to make statements along the lines of: “in a very high Threat situation, as the status of our Controls deteriorates we approach a 100% probability of a breach - most likely a Crimeware breach or a WebApp breach etc. sometime soon”. We don’t know when ‘sometime soon’ actually is but it doesn’t really matter whether this is today, tomorrow or in a few days or weeks since none of these outcomes will be tolerable.

This type of analysis gives us a starting point from which we can start our risk management by making sure that the Controls defending against our highest risks are fully and effectively deployed such that the likelihood of a breach is reduced to an acceptable lower level.

As we have seen from Figure 5, some Controls defend against multiple Threats and we will probably want to prioritize our attention on Controls that defend against multiple high risks.

By estimating and comparing the risk reduction that will be achieved from deploying new Controls or improving existing Controls we will develop a valuable insight into the relative risk-based merits of various Control strategies. However, as we develop cyber security investment appraisals, we should remain aware of potential uncertainty in our estimates of risk.
4. Outputs from a real-time Cyber Security Risk Management System

4.1 Example Outputs

A real-time cyber security risk management system will provide a clear, risk-based picture of cyber security status by bringing together the various components and measures of cyber security into a consistent, coherent view.

Figure 8 shows an example dashboard for an on-line payments environment showing tolerable (green) risks, intolerable (red) risks and an overall aggregate position against risk appetite (shown on the middle gauge at the top right of the image).

Figure 8 - Source: Acuity STREAM – Example dashboard showing Threat / Threat Actors for an On-line Payments Environment with individual risk statuses against tolerance and overall status against appetite

The data sources contributing to the summary view shown on the example dashboard in Figure 8 are:

- Threat Actor / Threat lists for the financial services sector, in this case drawn from the Verizon 2015 Data Breach Investigations Report
- Threat levels from research, threat intelligence and organizational experience of previous incidents and near-misses
- The potential impacts from breaches of confidential data, e.g. customer records, payments records etc.
- Controls mapped to Threat Actor / Threat, in this case the SANS Top 20 CSC with associated metrics and relative importance using the NSA attack mitigation priorities
- The deployment status of the mapped Controls.

Figure 8 shows an intolerable high (Red) risk: Organized Crime - Crimeware to the On-line Payments Environment. The status of the Controls mapped to this risk is shown below in Figure 9.
Figure 9 - Source: Acuity STREAM – Example dashboard showing the status of SANS Top 20 Controls which are mapped to the risk of Organized Crime – Crimeware to the On-line Payments Environment

Figure 9 indicates 5 relatively weak (Amber) controls and a very weak (Red) control ref. SANS 13.07 (Require remote login access to use two factor authentication). These weak controls are contributing to the high (intolerable) level of risk and by addressing the weak controls we can reduce risk down, hopefully to a tolerable level.

Some controls mitigate multiple risks and Figure 10 shows 7 risks that two factor authentication for remote login access helps to mitigate. The 3 columns to the right show estimates of risk with the control at its current level of deployment (50%), if the control was at fully deployed (100%) and the difference (Risk Delta) which is a measure of potential risk improvement.

Figure 10 - Source: Acuity STREAM – Example risk-based view of a Control showing the estimated risk improvement (Risk Delta) which could be achieved by full deployment of the Control
Figure 11 below shows all Controls which are mitigating risks to the On-line Payments Environment ranked by Risk Delta, i.e. showing risk-based priorities for Control improvement.

Figure 12 - Source: Acuity STREAM – Top 10 Risks to UK Payments

Further example management information is illustrated in the two images below, Figure 12 (Top 10 Risks) and Figure 13 (Summary Status of SANS Top 20 Critical Security Controls).
4.2 Level of Detail

These examples have shown information at a fairly high level of abstraction and analysis can go down to as low a level of detail as required. For example Threats could be deconstructed to a lower level as illustrated in Figure 14 from the Verizon 2015 DBIR which summarises the variety of hacking actions within the Web App Incident pattern.

Figure 14 - Source: Verizon 2015 Data Breach Investigations Report (DBIR) Figure 35 – Variety of hacking actions within Web App Attacks pattern
Similarly the target of our risk assessments could be deconstructed into components of the on-line payments environment. The level of detail will be that which management feels comfortable in working with and taking decisions on.

### 4.3 Reacting to Change

It is particularly important that management information of the type shown above can be updated instantaneously whenever relevant changes occur to continue to provide a real-time view of cyber security risk status. Table 1 below summarises the initiators of change, the components and risk factors involved and how the changes will manifest in the risk management system.

<table>
<thead>
<tr>
<th>Change</th>
<th>Components / Risk Levels</th>
<th>Effects of change / Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat intelligence received relating to certain Data or Assets that may be targeted by specific Threat Actors / Threats</td>
<td>Threat Levels for targeted Assets will increase</td>
<td>The measured Risk level increases and may exceed tolerance. Identify Assets that may be affected and review the status of Controls for those Assets. If necessary, initiate improvements and additional Controls. Identify and notify Business Units that may be affected.</td>
</tr>
<tr>
<td>Incident research received, e.g. new Verizon Data Breach Investigations Report published</td>
<td>Existing Threat Levels and mappings may change. New Threats may be identified and included</td>
<td>Risk levels may change. Review Risks and see whether measured changes to Risk levels are tolerable individually and are within overall appetite. Review Control improvement priorities in light of any new Threat levels.</td>
</tr>
<tr>
<td>Performance of key controls deteriorates, e.g. patch status on certain Assets</td>
<td>Metrics measuring patch status on affected Assets will indicate weak performance</td>
<td>Measured Risk levels will increase and may exceed tolerance. Initiate actions to restore the performance of the Controls.</td>
</tr>
<tr>
<td>SIEM or data analytics solutions identify suspicious activity or events affecting certain Assets</td>
<td>May affect Threat Levels or indicate weaknesses in Controls which were previously considered to be well deployed</td>
<td>Measured Risk levels may increase and exceed tolerance. Initiate actions to improve the performance of Controls or consider additional Controls.</td>
</tr>
<tr>
<td>Vulnerability scanners identify vulnerabilities on certain Assets</td>
<td>May indicate weaknesses in Controls which were previously considered to be well deployed</td>
<td>Measured Risk levels may increase and exceed tolerance. Initiate actions to improve the performance of Controls.</td>
</tr>
<tr>
<td>Control non-compliances raised from self-assessments or audit reports</td>
<td>Indicates weaknesses in Controls which may previously have been considered to be well deployed</td>
<td>Measured Risk levels may increase and exceed tolerance. Initiate actions to improve the performance of Controls.</td>
</tr>
<tr>
<td>Proposal to delay a cyber security project, perhaps due to lack of resources or budget restrictions</td>
<td>Data and Assets which are known to require additional protection will remain at risk for longer</td>
<td>Anticipated reductions in measured Risk will be delayed and potentially leave the Organization exposed to intolerable levels of Risk for longer than would otherwise have been the case. This ‘risk from delay’ can be quantified and used to inform debate on the proposal.</td>
</tr>
</tbody>
</table>

Table 1 – Acuity Risk Management – Summary of changes that may affect cyber security risk status
5. Benefits of a real-time Cyber Security Risk Management System

A real-time cyber security risk management system will provide the timely, measurable cyber security risk status information for senior management that they need to perform their Governance responsibilities. Only by understanding and measuring our status can we manage our cyber risks and given the very high Threat, if we don’t have effective real-time cyber security risk management we will suffer damaging cyber security breaches.

Specifically, effective real-time cyber security risk management will:

- Reduce the likelihood of a damaging cyber security breach
- Allow us to control our costs by targeting resources at intolerable risks and avoiding over-control of tolerable risks
- Help us to prioritize and justify cyber security investments by focusing on those cyber security solutions which will provide the greatest risk-based return on investment
- Demonstrate to shareholders, customers, regulators and other stakeholders that we have our cyber security under control.

By measuring cyber security risk in financial terms we will also be able to align cyber security risk management with Enterprise Risk Management.
6. Summary

Cyber security breaches pose a serious and growing Threat and cyber security risk management is a critical management tool for understanding cyber risk status and making important investment decisions on cyber security.

With the recent escalation of the Threat to a ‘not if but when’ scenario comes a need for cyber security risk management to provide the visibility and decision support through which management can exercise its Governance responsibilities. The real-time nature of Threats and the need to keep cyber security Controls performing effectively imposes the need for real-time cyber security risk management.

For effective real-time cyber security risk management we need to:

- Model (at the appropriate level of detail) the key components of cyber risk, including Data, Assets, Controls, Threats and Threat Actors and their inter-relationships
- Implement a suitable Control Framework, e.g. the SANS Top 20 CSC using automated solutions where appropriate within a suitable information security management system, such as ISO 27001
- Map Threats to Controls using best available guidance, e.g. by reference to Verizon DBIR, other research and cyber security experts
- Measure cyber risk in financial terms, assessing and updating the likelihood of a cyber breach in probabilistic terms by reference to best available guidance, e.g. incident data (such as Verizon DBIR), threat intelligence, other research, SIEM, data analytics and cyber security experts
- Measure the performance of Controls at a frequency appropriate to the nature of the Control and rate of change - using metrics with automated daily updates for critical controls, such as patch status
- Continually review cyber security risk status and take action to manage risks down to within management’s tolerance and overall appetite for risk.

Such real-time cyber security risk management can only be delivered with an integrated risk management software solution which can model all of the key components, consolidate all relevant data from multiple sources and present managers with credible measurements on which they can monitor status and take decisions.