A GUIDE TO CREATE AND USE A TOOL TO MEASURE ADVERSARIAL RISK

THE CAP WAY™

Creating a simple tool that provides a standard outcome

1. WHY DO I NEED A TOOL TO MEASURE ADVESARIAL RISK

It is important that you measure the likelihood and consequence of an adversarial attack in a standard way, so that those assessing the risk adopt one methodology, those responsible for making risk-based decisions use the same criteria each time, and those reading the Risk Register do so from an informed mindset.

1.1. Prior to creating the tool to measure adversarial risk, the following two principles must be understood: 1) the suitably qualified and experienced (SQEP) security specialist is not typically empowered or authorised to create the criteria used to score the adversarial risk on behalf of the organisation, and 2) the Senior Risk Owner (SRO) must be identified to ensure the business needs are truly understood and thus reflected in the risk scoring tool.

1.2. **The Senior Risk Owner.** The SRO is typically an executive level role accountable for providing a safe and secure workplace to ensure the organisation's people, property, information, and organisational reputation are protected. This role would have sufficient decision-making authority to allocate the necessary resources —time, people, and budget— to mitigate the risk. The SRO will be criminally, morally, and ethically responsible to safeguard the mission critical assets (both tangible and intangible) to achieve success and deliver the organisation's business plan. The SRO is the one who goes to jail when things go wrong! The SRO is an influential decision-maker with a budget.

1.3. **The Security Professional.** The SQEP security specialist could be the Security Manager, Head of Security, Security Director employed by the organisation, or a contracted consultant hired to advise the executive level leaders. The SEQP security specialist is an advisor, a practitioner, and the person who created an integrated and/or holistic security programme to protect the organisation's people, property, information, and wider reputation. They do not own adversarial risk; they are not accountable for which risk is mitigated and which risk is accepted, and typically their operational budget is not used to mitigate new or emerging adversarial risk. The SRO and Security SQEP are identified during Stage 1 of ***The CAP Way***™ Security Management Review Process[1]

1.4. This Guide introduces ***The CAP Way***™ Adversarial Risk Assessment Tool (*StoryBoard*® 02) and articulates how it was created and how it can be adapted for use in all organisations. It is simple to use, displayed on one page, and directs the user as to the next course of action (or not).

2. DETERMINING THE LIKELIHOOD THAT AN ATTACK WOULD BE SUCCESSFUL

Its worth noting that ***The CAP Way***™[2] is to assess the likelihood of an adversarial attack being successful and not just that it will occur in the first place. When approaching the assessment from this perspective, it is necessary to consider two factors, 1) the motivation and capability of the attacker, and 2) the efficacy of the defensive measures already in place to reduce the chances that the attack would be successful. Combining the findings of these two assessments will improve the quality of your conclusion when determining the likelihood of an attack succeeding.

2.1. **Capability.** Having identified a threat actor —this is always a person or a group of people[3]— it is necessary to establish if they are motivated to attack your organisation, i.e., do they have a grievance against the organisation's goals, or an individual in the organisation, that would cause them to plan and execute an attack. This may also identify their intent to attack. The second element when assessing a possible adversary is their ability to deliver on their intent; do they have the necessary capabilities, opportunity, time, or physical ability to mount their attack? You can, therefore, start to quantify the adversary's

[1] Reference A

[2] Reference B.

[3] An adversarial [or security] risk assessment should not consider natural disasters, sever weather events, fiscal challenges, or industrial accidents, as this often requires specialist knowledge outside of the security professional's experience and is not always initiated by a person or group of people.

motivation and capability to mount a successful attack and thus start to put a degree of 'science' – or at least, an educated or considered '*guess*'- behind the likelihood that an attack might occur.

2.2. **Motivation.** The next assessment is to understand the motivation of the adversary. Why do you think they would attack your organisation? Do you perceive that they would consider you an attractive target? Is it worth them getting caught, have they seen vulnerabilities in your defence, or have they made it public that they intend to disrupt your organisation or others in the industry in which you work? You can obtain a better understanding of your adversary's motivation by conducting in-depth research and learning as much as you can about your 'enemy'. Some would say, you need to '*think like your enemy*' to predict their next action. Much of this background investigation should have already been conducted as part of your adversarial threat assessment (stage 2 of the SMR – Reference A) and thus you have already identified potential adversaries and if they are likely to attack your organisation.

"If you know the enemy and know yourself, you need not fear the result of a hundred battles". Sun Tzu[4]

2.3. ***The CAP Way™*** is to score both the adversary's capability and intent to mount an attack, and you do this by understanding their modus operandi, how they attack, their strengths, have they mounted successful attacks before, what knowledge, skills, or weapons would they need to attack successfully?

2.3.1. It is suggested that you describe the threat by allocating a motivation and capability score between 1 and 5, based on a standard criterion for all to use, such as:

5	Very High	An adversary demonstrates the capability and intent, and similar assets are frequently targeted.
4	High	There is knowledge of an adversary's capability and intent to attack the asset.
3	Medium	An adversary has a desire to attack similar assets.
2	Low	Few known adversaries appear neither motivated nor capable of attacking the asset or similar assets.
1	Very Low	No evidence of capability or intent and no history of planned or successful attacks against the asset.

2.4. **Your Defence.** The second factor that determines the likelihood that an attack would succeed is the quality of your defence; what protective security measures you have in place or what you plan to install if it's a new-build. This requires you to take an honest look at your security arrangements to identify gaps or weaknesses based on your understanding of the adversary's attack methodology and where their strengths lie. Again, this goes back to the quality of your threat assessment so that you design your defence to counter the strengths of your adversary. This process is known as performing a Vulnerability Analysis (Stage 3 of the SMR – Reference A) and ***The CAP Way™*** advocates you complete this after the Threat Assessment but before the Risk Assessment because this has a direct link on determining an accurate level of adversarial risk.

2.4.1. Once again, it's recommended that you describe the vulnerabilities in your current or planned layers of defensive security arrangements by allocating them a score of 1, 3, or 5 based on a standard criterion for all to use, such as:

5	High	Limited protective measures in place to deter, detect, delay, or respond to an attack providing an adversary easy access to the asset.
3	Medium	Protective measures are generally adequate to deter, detect, delay, or respond, but there are some gaps which could be exploited by a determined and capable adversary.
1	Low	Multiple layers of effective protective measures exist to deter, detect, delay, and respond to an attack and the chance is very low that the adversary would be readily able to exploit the asset.

2.5. **Determining the Likelihood Descriptor.** If you multiply the two scores (threat & vulnerability) together, and match it with a predetermined scale, you have identified which of the seven levels is most appropriate on the Likelihood scalar on your typical 7 x 5 risk assessment matrix. More about this later.

2.6. Step 1 of ***The CAP Way™*** Adversarial Risk Assessment Tool proposes a scalar to quantify your threat score with the vulnerability score – see overleaf. This now completes Step 1 of the assessment process – you have determined the likelihood of a successful attack taking place.

[4] Reference C.

Score	Level	Descriptor
25	7	Almost Certain
20	6	Highly Likely
15	5	Likely or Probable
12	4	Realistic Possibility
9	3	Unlikely
3 to 6	2	Highly Unlikely
1 & 2	1	Remote Chance

2.7. **Gut Feel.** The more experienced security professionals may wish to skip Step 1 and, using their intuition or gut feel, jump straight into the Likelihood scalar and select an assessed score by using a prompt or basic definition. Again, ***The CAP Way***™ Adversarial Risk Assessment Tool offers this streamlined approach and proposes the five definitions for a large infrastructure project. These definitions would be adapted to suit the organisation, so they resonate with the user of the tool.

Descriptor	Probability	Yardstick
Event occurs on regular basis on the project	≥ ≈ 95%	7. Almost Certain
Event occurs occasionally on the project	≈ 80% to ≈ 90%	6. Highly Likely
Event can reasonably be expected to occur in the life of the project	≈ 55% to ≈ 75%	5. Likely or Probable
Conditions may allow the event to occur on the project or has occurred in similar projects.	≈ 40% to <50%	4. Realistic Possibility
Exceptional conditions may allow the event to occur on the project. Has occurred in the organisation.	≈ 25% to ≈ 35%	3. Unlikely
Reasonable to expect event will not occur on the project. Has occurred several times in the industry.	≈ 10% to ≈ 20%	2. Highly Unlikely
Has occurred once or twice within industry.	≤ ≈ 5%	1.Remote Chance

2.7.1. Whilst this 'gut feel' process is perfectly OK within some organisations, and probably the chosen path by most security professionals, if however, there is a need to justify or evidence your thought process, it might be necessary to document how the Likelihood score was determined. This is typically the case in a regulated industry or where the cost to mitigate the possible consequences of a successful attack is high. A well-documented adversarial threat assessment and risk assessment is a 'must-have' if you find yourself giving evidence in a coroner's court or public enquiry; even-more-so if you are in a criminal court with the possibility of going to jail.

2.7.2. ***The CAP Way***™ Adversarial Risk Assessment Tool advocates the UK governments Professional Head of Intelligence Assessments (PHIA) Probability Yardstick when measuring the likelihood of an attack occurring. This is further explained in an article available through ***The CAP Way***™ website (Reference D) and explains the preference of a 7 x 5 matrix over the traditional 5 x 5 matrix.

3. IMPACT ASSESSMENT

It's now time to consider how you measure the impact of a successful attack. What are the consequences to your organisation and its ability to meet its legal obligation to keep people safe, protecting its property or information, whilst also delivering against its business model – especially if it's a corporate organisation with commercial needs.

3.1. This is where the Senior Risk Owner's (SRO) direction is needed, and maybe requires input from other members of the organisation's leadership. ***The CAP Way***™ advocates that you identify what the organisation believes is important to them, how would they feel if their people, property, or reputation was negatively impacted by an adversarial attack. Again, much of this is intuitive but maybe the security professional, especially if they are a hired consultant, may not truly understand the organisation's values, culture, or business model and thus misinterpret the importance placed on the intangible assets. It would be typical to see people safety, environment, and cost listed as a Value that might be impacted but, dependent on your organisation, it might also include the project schedule, productivity rates, or the reputation of the organisation. Whatever the

SRO believes is important to the efficient running of their organisation, this should be considered when measuring the impact of an attack.

3.2. The security professional should now sit down with the SRO and agree the top five Values that may be impacted by an attack and then set a measurement against the level of impact for each of those Values. ***The CAP Way***™ suggest this is achieved by creating a table by listing the five Values in the left-hand column. If a 7 x 5 risk matrix is to be used, then set out five further columns to the right of each of the Values and title each of these columns; very low, low, medium, high, and very high (or however your organisation chooses to describe the levels of impact/consequence). In a conversation, the SRO and security professional set a value or description in each of the boxes, starting from very low moving right to very high. This description will guide those conducting future adversarial risk assessments to quantify (score) the forecasted impact of an attack.

3.3. The SRO would then move down the list of impacted Values and agree a description for each. It may be beneficial for the security professional to consult with others in the leadership team and draft recommended descriptors for the SRO to review and agree. For example, the Director responsible for health, safety, and environment (HSE) may already have an impact chart for people safety or the environment, the Chief Finance Officer (CFO) might have the same for financial risk, and the Head of Legal or External Relations might have a method for measuring the impact of reputational or compliance risk. By doing their homework, the security professional not only demonstrates to the SRO that they understand the business, but they also reveal a desire for a consistent and standard approach to measuring the impact of an undesirable event. It helps create a '*one-team'* approach. Here is an example for a large infrastructure project, however; the listed Values that may be impacted and descriptor within the matrix must be bespoke to the organisation to ensure they resonate with the user.

	1	2	3	4	5
	Very Low	**Low**	**Medium**	**High**	**Very High**
Schedule	No schedule impacts.	Up to 1 month.	1 to 2 months.	2 to 3 months.	More than 3 months.
Environment	No environmental impacts.	Offsite Reportable Event.	Regulatory investigation; minor offsite impact.	Prosecution by regulator; large offsite impact.	Government intervention.
Cost (£)	up to £10,000	Between £10,000 to £1000,000	Between £1000,000 to £10,000,000	Between £10,000,000 - £25,000,000	Over £25,000,000
Casualty	Minor injury onsite. No injuries offsite.	RIDDOR injury onsite. No injuries offsite.	Potential for widespread onsite serious injuries.	Potential for onsite fatalities; Possible offsite fatalities.	Possible for on and offsite fatalities from large-scale toxic release or explosion.
Reputation	No impact or loss of reputation.	Informal query by regulator; local press coverage. Local MP or council concern.	Formal notification to the regulator; national press coverage. Issue raised in Parliament.	Prosecution by regulator; extensive national press coverage. National NGO Campaign.	Government intervention; international press coverage.

3.4. This process serves to document the SRO's appetite or tolerance to adversarial risk. Arguably, if consistently used by those across the organisation, it creates a common or standard understanding of the impact for all risk, not just adversarial risk. Irrespective of the cause, if an unwanted event creates a 96-day delay in the project schedule, it will always be perceived as a 'very-high' impact (using the above example as it causes a delay above 3-months). The cause of the delay could have been a safety incident, an environmental spill, a loss of funding, or – in our case- a terrorist attack. Either way, the impact should be measured in a standard way so the leadership can place the adversarial risk in context with other risks.

4. Calculating the Adversarial Risk Score. The next step is easy, simply multiply the likelihood score with the impact score having added a descriptor next to each of the five Value, e.g., very low = 1, low = 2, etc. etc. This means that an '*almost certain'* likelihood event (scoring 7) that has a '*very high'* impact (scoring 5) would attract an overall adversarial risk score of 35. So, what does this mean? This is where you pick up the conversation with the SRO once again. It is necessary to determine what action, if any, does the SRO direct – remembering that, to do nothing is, in itself, an executive level decision. It may also be decided that work might stop —or approval to continue work is automatically denied without prior consultation with the senior leadership— if the adversarial risk is so high that it would place the person, property, or reputation at an unacceptable level of risk.

4.1. When multiplying seven levels of likelihood with five levels of impact, there are multiple answers, so ***The CAP Way***™ recommends you group these results into five categories of adversarial risk and then provide explanatory text to direct the next course of action.

CATASTROPHIC	>21	Immediate risk reduction necessary. Executive level approval to proceed required.
CRITICAL	18-21	Short-term, interim risk reduction required. Long term risk reduction plan must be developed and implemented.
HIGH	10-16	Additional long-term risk reduction required. If no further action can be reasonably taken, senior management approval required to continue activity.
MEDIUM	5-9	Risk is tolerable if reasonable safeguards are confirmed to be in place and proportionate to the relevant organisational Security Response Level.
LOW	1-4	No further risk reduction required.

4.2. ***The CAP Way***™ Adversarial Risk Assessment Tool provides the above guidance on a single side of A3 paper to allow the user to follow a cognitive methodology to achieve a standard outcome that is understood by all. It is acknowledged that this may appear complex, but once practiced, it will prove to be a logical and repeatable process that will withstand external scrutiny, because it is based on robust scientific research. There is, however; a couple of important considerations to ensure the outcome has value.

5. MAKING A RISK-BASED DECISION

At the outset, this Guide stated that "*They [the security practitioner] do not own adversarial risk; they are not accountable for which risk is mitigated and which risk is accepted, and typically their operational budget is not used to mitigate new or emerging adversarial risk*". It is, therefore, necessary to further consult the SRO once the adversarial risk has been determined to allow them to direct which risks must be addressed and those that are within their tolerance levels. Remember, "*the SRO is the one who goes to jail when things go wrong*!".

5.1. **Recording the Adversarial Risk**. It is important that all stakeholders have a shared understanding of the adversarial risk to the organisation. This helps those responsible for mitigating the risk to focus on the risks that will impact their organisation the most and thus allow them to allocate their finite resources for the maximum effect. ***The CAP Way***™ advocates that the adversarial risk is recorded by creating a three-part structured 'risk statement' as follows:

Part 1: define the cause — Part 2: document the risk — Part 3: describe the effect on the asset

5.1.1. **Part 1** of the risk statement is identified during the vulnerability analysis of the existing defensive security arrangements that may provide an opportunity for the adversary to exploit, and thus, increasing the likelihood that the attack would succeed.
5.1.2. **Part 2** documents the behaviour or attack methodology used by the adversary during the attack.
5.1.3. **Part 3** lists the probable outcome, impact, or consequence if an attack were to succeed.

5.2. Here is an example of an adversarial risk statement for a large construction project:

Risk #	Risk Statement	Likelihood	Impact	Risk Score
1	Due to the lack of control at the entrance of the work area[5] there is an increased risk that unknown person(s) can sabotage[6] installed equipment rendering it unusable. This could impact commissioning, increase cost, or delay production and lead to reputational damage.	5	3 Cost	15-High

[5] This should be better defined, where possible, i.e., "*Main Building*" to provide clarity and avoid misunderstanding.

[6] Avoid listing multiple behaviours, actions, or attack methodologies in the same risk statement as this includes unnecessary complexity when designing proportionate mitigation, i.e., don't make statement like this: "*…can sabotage, steal, maliciously damage or substitute critical equipment, instruments, or plant with inferior products …*".

5.3. The “*lack of control at the entrance*” was noted when reviewing the security arrangements during the vulnerability assessment, the “*sabotage* [of] *installed equipment*” was established as a known attack methodology of the adversary during the threat assessment, and the impact on the “*commissioning* [phase], *increase* [in the project] *cost, or delay* [to the date of the building under construction] *production*” was established from speaking to those who understand the purpose for which the building was being constructed.

5.4. Moreover, a successful attack may impact the organisation in more than one area, so it is advisable to list the area that is impacted the most, in the above example the *Cost* impact is scored at Medium (3) because the cost of the attack was estimated between £1,000,000 to £10,000,000.

5.5. **Residual Risk**. It is unlikely that where a motivated and capable adversary has been identified, the associated risk of them mounting a successful attack can be completely eliminated and thus, —once protective security measures are designed to address the vulnerability (gap/weakness)— it is necessary to document and notify the SRO of the residual risk. This shall allow them to accept this residual risk and approve the proposed defensive upgrades knowing that the risk still exists, albeit at a much-reduced level.

5.6. **Adversarial Risk Register**. An experienced security professional will always maintain an adversarial risk register and an ability to demonstrate regular conversations with the SRO during which the content of the risk register is discussed. ***The CAP Way***™ recommends that a PDF copy of the Adversarial Risk Register —displaying the date and version number— is produced for each of these periodic meetings between the SRO and their security advisor. For completeness, and to demonstrate executive commitment and help focus the mind, these copies could be signed by both parties. These documents will prove useful to the security professional during a post-incident investigation and probable appearance at court.

6. THE BIGGER PICTURE: SECURITY MANAGEMENT REVIEW (SMR)

6.1. ***The CAP Way***™ Adversarial Risk Assessment Tool is just one tool in the ***Cannon Asset Protection (CAP) Limited*** protective armoury and is specifically designed to help structure one of the six elements —the risk assessment— of the CAP Security Management Review (SMR) Methodology – Reference A. Other tools exist to help characterise the asset to be protected, support the threat assessment, explain the vulnerability analysis, steer the design process to create a layered defence, and to suggest what would trigger a review of the security arrangements. Annex A to this document lists the available ***StoryBoards***® within ***The CAP Way***™ Governance Pack.

Reference:

A. ***The CAP Way***™ Security Management Review Guide & ***StoryBoard***® # 02.
B. ***The CAP Way***™: https://thecapway.com/
C. The Art of War: Sun Tzu. Translated by Thomas Cleary. Shambhala, London. 2005.
D. 230412-articles-yardstick-frank-CAP10: https://thecapway.com/articles.

ANNEX A: **FURTHER READING AVAILABLE** ON ***THE CAP WAY***™ Website: https://thecapway.com/.

Each ***StoryBoard***® (SB) consists of a two-sided piece of A3 paper (a communication tool) used by a security practitioner to engage their stakeholders during a one-to-one or small group conversation. It is not a poster or slide, but more an *aide memoir* to help facilitate a conversation using the images, graphics, and bullet points to deliver a consistent message in a standard way. SBs can be designed, adapted, or branded to suit the organisation; ***Cannon Asset Protection Ltd*** can help the security practitioner develop their own SBs for use within their organisation.

As Frank Cannon develops his learning he will update each SB from time-to-time and upload the revised version to ***The CAP Way***™ website. The SBs, that make up revision 3 of ***The CAP Way***™ Governance Pack, are:

SB1: Security Management Review Methodology
SB2: Adversarial Threat, Risk, & Vulnerability
SB3: Adversarial Threat Assessment Methodology
SB4: Managing Security Vulnerabilities: Defence-in-Depth and Layered Security
SB5: Building a Security Strategic House
SB6: Organisation's Security Team Key Job Responsibilities
SB7: Developing a Security Culture
SB8: Security Awareness Programme: Four Campaigns
*SB9: Security Campaign Cards: Creating Key Messages**
*SB10: Creating Security Campaign Pamphlets: The 7Qs**
SB11: Security Community of Practice (SyCoP) – Collaboration Will Always Win
SB12: Roles of A Security Responsible Person – Guide to Identifying Levels of Security Competency
*SB13: Stakeholder Management: Identifying Key Groups**
*SB14: Security Documents: A Hierarchical Approach**
SB15: Writing a Security Plan: A Plan-on-a-Page.*
*SB16: Writing a Security Contingency & Response Plan**
*SB17: Developing a Security Competency Matrix**
*SB18: Writing a Security Training Plan, SOPs, & Exercises**
*SB19: Security Investigations & Incident Reporting**
*SB20: Security Assurance Methodology**
SB21: Developing a Suitably Qualified and Experienced Person – Counter Terrorist Security Specialist (CTSS)
SB22: Creating a Security Partnership: We are Always Stronger Working Together
SB23: Engaging the Next Generation: Protective Security Industry
SB24: Collaborative Protection: Working With Others (Cheese & Onion Flavour Security)
SB25: Close Protection: Developing a Protective Entourage
SB26: The Value of a Community Guardian: 1 Role with 5 Deliverables
Note: ** SB under construction – not yet available.*

Why Use **Cannon Asset Protection Limited?**
Managing Director & Principal Consultant:
Frank Cannon

THE CAP WAY™
CANNON ASSET PROTECTION

FSM AWARDS
Winner!
2023
Security Manager of the Year

THE SECURITY INSTITUTE

ROYAL MILITARY POLICE

Special INFLUENCERS Edition
SJUK
I'M AN SJUK INFLUENCER 2023
Frank Cannon
Founding Director, Cannon Asset Protection and Fellow of The Security Institute
SJUK ISSUE 36 | JANUARY 2024

CPP® Certified Protection Professional
Board Certified in Security Management

SUPPORTS ASIS INTERNATIONAL UNITED KINGDOM

ASSOCIATION OF SECURITY CONSULTANTS ASC