Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

"Talking a different Language": Anticipating adversary attack cost for cyber risk assessment

*Richard Derbyshire**, *Benjamin Green*, *David Hutchison*

Lancaster University, School of Computing and Communications, InfoLab21, Lancaster, LA1 4WA, United Kingdom

ARTICLE INFO

Article history:
Received 4 June 2020
Revised 21 December 2020
Accepted 22 December 2020
Available online 2 January 2021

Keywords:
Cyber attack
Adversary
Cost
Risk assessment
Threat actor
Threat assessment

ABSTRACT

Typical cyber security risk assessment methods focus on the system under consideration, its vulnerabilities, and the resulting impact in the event of a system compromise. Cyber security, however, increasingly requires anticipating the moves of intelligent adversaries, who make decisions based on a range of factors including the cost of their attacks. A study of current risk assessment literature and industry practice shows that consideration of this cost is a notable gap in the understanding of adversaries. The factors of cost experienced by an adversary are established in this paper as Time, Finance, and Risk, supported by a practical study undertaken with relevant security practitioners. Using these factors as a base, a framework is proposed and developed to support the probabilistic determination of cost incurred by an adversary. This framework is an important extension to existing cyber security risk assessments, and is demonstrated in the paper through the use of a case study.

1. Introduction

For any organisation, the journey to mitigating the risk of a cyber attack begins with a cyber risk assessment. This fundamental starting point is key to understanding the risks posed to an organisation, and the effectiveness of any controls which are currently in place. The significance of cyber risk assessment is evident by its prominence in the UK's National Cyber Security Centre's (NCSC) guidance for achieving compliance with the European Union Directive on the security of Network and Information Systems (NCSC, 2018), the National Institute of Standards and Technology's (NIST) Cybersecurity Framework (NIST, 2018), and ISO/IEC 27001 (BSI, 2015).

As can be seen in Fig. 1, ISO/IEC 27005 (BSI, 2011) describes the risk assessment process, within its wider risk management process, to include three parts: identification, analysis, and evaluation of risk. While the nomenclature and granularity vary throughout academic and industry literature, the objectives are frequently synonymous. A cyber risk assessment must identify, acknowledge, and record risks, noting any controls currently in place and the source of each risk. It must then cultivate an understanding of the recorded risks, further considering the source of each risk, the likelihood that it will be realised, and the possible resulting consequences. Finally, the analysed risks must be evaluated, comparing them to the organisation's risk appetite (the amount of risk it is willing to accept), allowing decisions to be made for risk treatment. Once the risks are assessed, the organisation can then move on to formulate a cyber risk mitigation strategy and select appropriate controls for each assessed risk.

Cyber risk is commonly understood as a product of likelihood and impact, with likelihood being further decomposed into threat and vulnerability (Jones and Ashenden, 2005; NIST, 2013), where

* Corresponding author.
E-mail address: r.derbyshire1@lancaster.ac.uk (R. Derbyshire).
https://doi.org/10.1016/j.cose.2020.102163

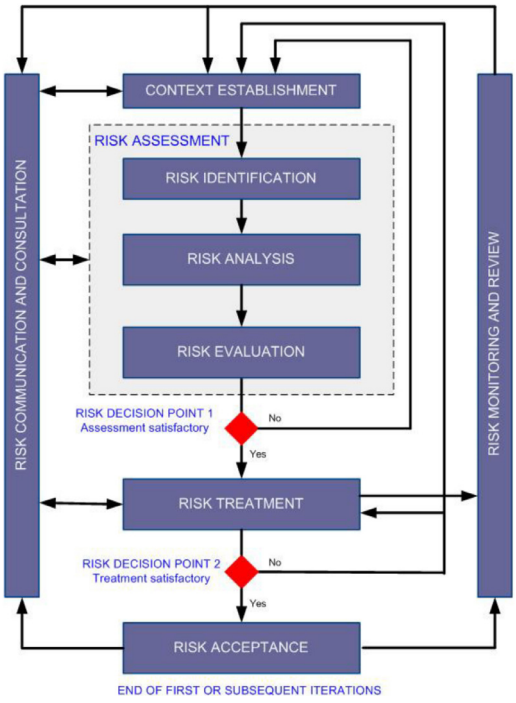

Fig. 1 – Risk management process in ISO/IEC 27005 (BSI, 2011).

- *threat* refers to adversaries intending to attack an organisation;
- *vulnerability* refers to weaknesses within an organisation, such as unpatched software or unaware personnel; and
- *impact* is the consequence of a threat leveraging a vulnerability.

This risk may be derived via the use of various, diverse methodologies, which can be qualitative or quantitative (Hubbard and Seiersen, 2016). The data used to support the components of risk can be captured from multiple sources and in multiple forms across the environment under review (e.g. vulnerability scans and asset registers). When considering threats, however, relevant data may be challenging to identify and acquire, often leading to the use of assumptions (Information Security Forum, 2016). The complexity of understanding threats is further exacerbated when one considers the adaptive, intelligent behaviour displayed by sophisticated adversaries operating in the cyber security domain, and the difficulty of discerning which of these realistically pose a threat to an organisation.

Of the risk assessment methods which do consider threats, there exist two dominant approaches – the primary differentiator being the perspective with which the threat is perceived. One approach involves quantifying threat capability, usually aggregating scores assigned to attributes of potential adversaries and incorporating this into the wider risk assessment process (Information Security Forum, 2016). The other approach focuses on which decisions an adversary will make, commonly based on probabilities inferred from data taken from the system under consideration, and judging how difficult it would for the adversary to perform the attack (Aksu et al., 2017).

Both of these approaches have their advantages in a cyber risk assessment. However, they also have issues, whether that means the data used is limited or based on assumptions, or the output of the threat assessment is disconnected from the rest of the data, thus inhibiting its benefit to the resulting cyber security strategy. In addition to their individual issues, both approaches share weak outputs, which are often qualitative or semi-quantitative, and incongruous with other business outputs such as financial risk, leading to poor decision making or lack of funding (Hubbard and Seiersen, 2016). A common aspect must be found, shared among all adversary types and able to be integrated into the wider cyber risk assessment process as a supplement, and which can be more easily digested by the output recipients.

In performing a cyber attack, one aspect that all adversary types share is cost. Every adversary must exert current, or develop nascent, technical capability. They must also spend time to prepare for and to perform the attack. The notion of adversary cost is seldom addressed in cyber risk assessment methods; when it is, it is often over-simplified or suffers from assumptions as when assessing threats. It does, however, highlight that adversary cost is able to be integrated with the wider process of cyber risk assessment (Roy et al., 2010; Schneier, 1999). Appropriately, the UK government's Home Office recommended in a report (Home Office, 2018) that "Future studies should further investigate the costs and profits to offenders of engaging in cyber crime". Also, if adversary cost can be viably measured, it would provide a clearer output than current cyber risk assessment methodologies, using terms and measurements which typical recipients are more familiar with. This, therefore, represents the core motivation for the remainder of our paper. The key contributions of this work are as follows:

- A review of the inclusion of adversaries within existing cyber risk assessment methods in academic and industry literature.
- A study of how cyber risk assessment is conducted in practice.
- The establishment of Time, Finance, and Risk as the factors of cost experienced by an adversary.
- The development of a framework for anticipating adversary cost.
- A demonstrative application of the adversary cost framework.

The remainder of this paper is structured as follows. Section 2 covers related work. Section 3 reports on interviews with risk assessment practitioners to explore both how they conduct cyber risk assessments in practice and gather their opinions on adversary cost. Section 4 establishes a structure for adversary cost. Section 5 sets out the factors of adversary cost. Section 6 proposes a framework for anticipating adversary cost, followed by a demonstrative application, using data inspired by a cyber risk assessment of a European utility organisation. Section 7 concludes our paper and presents ideas for further work on adversary cost.

2. Related work

Across academic and industry literature, researchers and practitioners alike have made efforts to quantify the efforts of adversaries found in the cyber security domain. These efforts have primarily been focused on providing much needed context to the still-developing area of cyber risk assessment. The following sections provide a brief review of prominent examples of approaches to understanding and measuring adversaries, highlighting the various means by which they are considered in cyber risk assessment.

2.1. *The adversary in cyber risk assessment*

The Information Security Forum's IRAM2 (Information Security Forum, 2016) models an adversary's behaviour with a set of attributes: capability, commitment, competence, culture, history, intent, motivation, origin, predisposition, privilege, and severity. Two numerical risk factors are then generated from this: likelihood of initiation (Loi) and threat strength (TS), which are then aggregated with the other components of the risk assessment. The risk assessment method by Jones and Ashenden (2005) involves a variation of this approach. Rather than using one homogeneous list of attributes assigned to all adversaries, the approach begins by splitting the adversary types into categories such as "nation state sponsored", "terrorism", "pressure group", and "commercial threat agent". Each individual category has a set of attributes which, while not dissimilar to IRAM2, are bespoke for each type, for example, nation state sponsored adversaries have attributes such as "adult population", "level of literacy", and "technological development level". These are assigned scores according to values in tables provided by Jones and Ashenden, then fed into a formula to generate a numerical output, which is finally input into the wider risk assessment. Both of these approaches provide much needed adversarial context to their respective cyber risk assessment methods, particularly because they focus on reducing uncertainty around the potential adversaries. However, they also both require considerable approximation, whereby risk assessors make estimations about entities for which they have no control and limited data.

Not vastly dissimilar to the above two approaches, Freund and Jones (2015) employ threat agent libraries (TALs) to inform their ontological method of risk assessment, namely factor analysis of information risk (FAIR). The TALs give attributes to the adversaries in the form of a threat capability (TCap) percentage and a threat event frequency (TEF) probability or frequency. The attributes require a minimum, most likely, and maximum, which then gives a distribution. This faces similar advantages and disadvantages to the above two approaches. However, FAIR also includes an attack "difficulty" parameter, which is expressed as a distribution. Also, the combination of TCap and "difficulty" do somewhat mitigate the disadvantages seen in the prior approaches by integrating the adversary and the system under consideration. Adversary capability (TCap) is improved when expressed as a distribution, but it still suffers from limited data and no control, and "difficulty" is weakened by being reduced to one distribution for the entire estate in scope of the threat event being analysed.

Insua et al. (2019) emphasise the necessity of intentionality when considering adversaries in a cyber risk assessment. To this end, they use adversarial risk analysis (ARA) (Banks et al., 2015) to "model the intentions and strategic behaviour of adversaries in the cybersecurity domain", further stating that the adversary has its own utility function and "seeks to maximize the effectiveness of his attack". ARA is split into "defender" and "attacker" problems, the latter relying on expert opinion to inform the adversary's beliefs and preferences (Merrick and Parnell, 2011). Insua et al. provide IRAM2 (Information Security Forum, 2016) as a potential source to identify adversaries and their available attack options. The example provided is a distributed denial of service (DDoS) which fits with the rigid nature of such models. However, it is not clear if more complex attacks from advanced adversaries could be so easily modelled, based on the plethora of techniques witnessed to breach and traverse a victim's estate, and negotiate its security controls. Later in the process, interesting aspects of the adversary are considered including earnings, costs of attacking, costs if detected, etc. which are modelled based on real world data. Unfortunately these follow quite a narrow and prescriptive scope. Rajbhandari and Snekkenes (2018) encounter similar issues with their cyber risk assessment method which, instead, uses game theory. Here the issues are exacerbated by the lack of bounds to adversary capability, and only the strategy based on desired outcomes and number of vulnerabilities in scope, loosely relating the threat to the system under consideration.

McQueen et al. (2006) introduce the time-to-compromise model, which estimates how long it would take adversaries to compromise a system. The method uses various sources to define four skill levels and their effectiveness against three states of system vulnerability. The data informing skill level includes estimating "readily available" exploits by consulting Metasploit (Rapid7, 2020), estimating fractions of exploitable vulnerabilities by a team of experts, and constants taken from literature to estimate the average time to discover a 0-day (previously unknown/undisclosed) vulnerability and write an exploit for it. Although quantifying an adversary's capability gives the methodology an edge, an adversary's skill cannot be defined by exploits alone; a wide variety of knowledge is required by cyber adversaries of which exploiting infrastructure is just a fragment. To truly capture the nature of adversary capability, a wider range of quantification would be needed.

Attack trees provide another cyber risk assessment method which inherently must consider the adversary. Pioneered by Schneier (1999), attack trees were introduced as a formal method for describing the security of systems based on the attacks which may be carried out against them. Also in this method, Schneier suggests adding costs to the attack nodes to allow realistic attacks to be discerned, such as all attacks below $100000. Unfortunately no method for establishing the cost is explained, and it must be assumed that for this piece of work the costs were estimated for the purpose of examples. Roy et al. (2010) increment attack trees by the means of attack countermeasures. In their work they mention adversary cost and return on attack as part of their method, including formulae to compute them; however no input data is suggested in the paper, meaning that both of these are open ended. Other than attack cost and the path through a system, no other as-

pects of adversary such as capability, resource, or effort are included in these works.

Similar to attack trees, attack graphs visually represent paths that an adversary may take through a system under consideration. Noel et al. (2010) propose an attack graph used to estimate the aggregate compromise likelihood for paths through a graph. The likelihood in the examples given is as a Monte Carlo simulated distribution generated by a minimum and maximum estimation for each exploit being leveraged. Other suggestions of input are provided including "relative frequencies of events observed on a network over a period of time" and taking values from a threat intelligence product. The overall method produces interesting results for the propagating likelihood that an adversary may breach and laterally move throughout the network. However, there is no further insight into a method to consider the adversary past-estimating likelihood which is based on limited input data.

The Common Vulnerability Scoring System (CVSS) (FIRST, 2015) is a method, most often used in industry practices such as vulnerability scanning and penetration testing, to delineate the severity of vulnerabilities. It is also, however, frequently used in cyber risk assessment methods to infer likelihood or required effort to exploit. Gouglidis et al. (2018) and König et al. (2018) both use the "Exploitability" parameter in the Temporal Score Metrics of CVSS v2. Exploitability (or Exploit Code Maturity in CVSS v3) has the possible values: "Unproven", "Proof-of-Concept", "Functional", and "High". On its own, this is not sufficient to denote vulnerability severity, let alone threat and, therefore, likelihood of attack. Gouglidis et al. also include an expert opinion of probability of exploitation as low, medium, or high. However, this is still limited in scope. Alhomidi and Reed (2014) use the entirety of CVSS to derive the probability of attack in their attack graph-based risk assessment method. The severity of vulnerability is a weak identifier of whether there will be an attack; there is no tangible connection to the adversary and so one cannot infer likelihood. Aksu et al. (2017) also use CVSS in their risk assessment method along with a rudimentary consideration of adversaries. They consider all of the parameters of the Temporal Score Metrics and a selection from the Base Score Metrics, along with their own additions - "Threat Motivation" and "Threat Capability" which are scored as low, medium, or high. Including adversary capability is a positive increment; however, CVSS may still be limited when addressing certain techniques and has been known to mis-prioritise vulnerabilities when taken out of context (McAfee Labs, 2017).

Industry standards and guidelines also intend to assist in the cyber risk assessment process. ISO/IEC 27005, the International Standards Organisation's document for Security Techniques in Information Security Risk Management (BSI, 2011), mentions briefly the difference between qualitative and quantitative risk analysis methods along with their advantages and disadvantages. The document also provides examples of risk assessment methods in an annex, all of which are variations of risk matrices using low, medium, high or 1–10 qualitative scales of risk components such as likelihood or threat ranking. The annex also references IEC 31010, Risk Assessment Techniques (BSI, 2010), which is more comprehensive in its discussion of risk assessment methods. However it is not focused on cyber security and therefore has a weak connection to assessing intentional cyber threats. NIST 800-30, the National Institute of Standards and Technology's Guide for Conducting Risk Assessments in Information Security (NIST, 2012), is very similar in nature to ISO/IEC 27005. It discusses quantitative, qualitative, and semi-quantitative risk assessment methods, along with their advantages and disadvantages. In its annexes it provides tables for qualitatively and semi-quantitatively assessing a variety risk components, which can be built up to an adversarial risk table. This table includes columns such as "Threat Event", "Threat Sources", "Capability", "Intent", and "Targeting", all of which are very important to the adversary in risk assessment. The outcome may be likened to a simpler version to that of both Jones and Ashenden (2005), and Information Security Forum (2016); but with the less specific input and the results restricted by a qualitative or semi-quantitative output it suffers all of the same disadvantages but further exacerbated.

There is a limited number of cyber risk assessment methodologies which focus more on the adversary. Intel's Threat Agent Risk Assessment (TARA) method (Rosenquist and Casey, 2009), for example, focuses on which adversaries (threat agents) would be motivated to attack the system under consideration, and what methods they would use. Although this considers threat as the primary component of risk, adversaries are reduced to categories with estimated, generalised attributes. Two papers of note from the TREsPASS (2016) project also approach cyber risk assessment from an adversary focused perspective. Pieters and Davarynejad (2014) consider an adversary's skill and investment against control strength (difficulty to circumvent a cyber security control), resulting in a probability of success for nodes on an attack graph. The variables and examples given are abstract and so it is not clear if the method would be of practical use in a real risk assessment. The method also employs estimations, based on adversary categories, for the static skill parameter, consistent with other methods discussed in this section. While penetration testing is a component of a cyber risk assessment (Such et al., 2016), Arnold et al. (2013) propose a method for quantifying the difficulty of an attack during a penetration test. The method uses item response theory (Klinkenberg et al., 2011; Rasch, 1993) to assess penetration testers' skill levels and then compares that against the time it takes them to execute techniques during an engagement. Arnold et al. (2013) describe the main limitation of the work to be the amount of data necessary to estimate a tester's skill level. This limitation is made worse by the scope-based nature of penetration testing, time constraints in particular, whereby a lower skilled tester will only be able to execute techniques they are familiar with in the allotted time frame (Such et al., 2016); in a real attack, a lower skilled adversary will have more time to learn, and execute, more complex techniques.

2.2. *Summary*

In their work promoting a threat-driven approach to cyber security, Muckin and Fitch (2017) state "The unbalanced focus on controls and vulnerabilities prevents organizations from combating the most critical element in risk management: the

threats". Concluding their survey of information security risk assessments, Shameli-Sendi et al. (2016) state that current methodologies fail to answer the question "How do we calculate the likelihood of a threat?". The review of related work we have presented here reinforces these arguments and extracts two key findings.

1) Adversaries in cyber risk assessments are often considered from two points of view - their capability, or their required effort/skill to carry out an attack. The former is when adversaries are considered as their own independent component, viz. threat (BSI, 2011; Freund and Jones, 2015; Information Security Forum, 2016; Jones and Ashenden, 2005; NIST, 2012). This can be weak because of a lack of real data, a requirement to make difficult estimations, and a disconnect with the rest of the risk assessment. The latter is when adversaries are not considered as independent, but instead their required effort is inferred from the system under consideration (Aksu et al., 2017; Alhomidi and Reed, 2014; Gouglidis et al., 2018; Insua et al., 2019; König et al., 2018; Noel et al., 2010; 2010; Rajbhandari and Snekkenes, 2018; Roy et al., 2010; Schneier, 1999). While the assessor would likely have the required data to work with, it is often too focused on vulnerabilities.

2) There exists a gap for a new assessment method which bridges the disconnected, estimated adversary capability and the vulnerabilities within the system under consideration. This assessment method would ideally use the known data about the system under consideration, along with the estimation of adversary capability, and be relevant to all types of adversary. Finally, it would act as a supplement to existing cyber risk assessment methods, complementing them, and not requiring further data to be captured.

The concept of an adversary's cost stands out as something which has been included as a feature but never a fully explored focus of work (Insua et al., 2019; Pieters and Davarynejad, 2014; Roy et al., 2010; Schneier, 1999); this has even been highlighted by the United Kingdom's Home Office as an area of interest (Home Office, 2018). Regardless of adversary type, their capability – whether they are backed by a nation-state or a novice at home, and no matter their intentions or agenda – all cyber attacks must have a base cost that, in performing it, every adversary must pay. Therefore, if the cost to perform a cyber attack can be derived from the system under consideration, it would bridge the significant gap in the existing approaches to adversary consideration in risk assessment.

3. Cyber risk assessment in practice

The related literature revealed that there is a gap in assessing adversaries within cyber risk, but this may not reflect cyber risk assessment in practice. Moreover, adversary cost may fill the identified gap conceptually, but it may be infeasible or undesirable for practitioners delivering real cyber risk assessments. To resolve this quandary, a qualitative study with current cyber risk assessment practitioners was devised. The primary intention was to discern the required data for cyber risk assessments, any inclusion of adversaries, the resulting cyber risk delivery process and how it is received, and whether adversary cost would provide a suitable supplement for cyber risk assessment.

3.1. *Methodology*

As in our previous work (Green et al., 2017), a combination of semi-structured interviews and template analysis proved to be the most effective way to gather and then analyse the qualitative data.

3.1.1. *Interviews*

Semi-structured interviews allow for a predefined, core question set, with the flexibility to include ad hoc or follow-up questions to gain further insight into topics of interest (Arksey and Knight, 1999).

Sample selection was carefully considered such that cyber risk assessment practitioners from a diverse range of backgrounds were interviewed. This ensured that there were perspectives from assessors of differing experience, who deliver to varying clients, and were from different sized organisations. Although it is noted that eight participants are sufficient for a highly focused study such as this (McCracken, 1988), the sample size for the interviews was ten, ensuring that the data began to saturate and no relevant points were left undiscovered.

Validity of the gathered data is crucial in semi-structured interviews, which means that any threats to it must be considered (Campbell, 1963). This was done first by ensuring the sample was sufficient. Then, interview techniques were employed which would build rapport, trust, and openness. The question set was developed from desired outcomes stemming from a review of the related literature. Finally, the interview protocol/guide was allowed to evolve, adding prompts for future interviews when interesting trends in past interviews emerged (Powney and Watts, 1987).

Reliability of gathered data is of concern in interviews, meaning that some data may not be trusted because of the research instruments, or the way the interviewer generates the data. Some of these concerns may manifest by way of "insider" interviewers; those which share certain traits such as ethnic, linguistic, or national heritage, or part of the same organisation as the interview participant (Ganga and Scott, 2006). While this may prove a valuable feature for gathering interview participants or understanding the subject matter, it may also impact reliability due to the interviewer having biases or making assumptions based on their own experience (Arksey and Knight, 1999). To combat this, neutrality was considered paramount in the design of our interview protocol/guide and during each interview. This means that the positive aspects of past experiences were drawn upon in both of these processes and the negative aspects were accounted for by both the interview protocol/guide and resulting interview transcripts being reviewed by the research team.

Telephone interviewing was the *practical technique* used to perform the interviews due to the geographical limitations of finding a whole sample set of participants. Challenges noted include the difficulty of managing open-ended questions and participant focus during telephone interviews (Frey, 1983). While fixed-response questions may be preferred for telephone interviews, open-ended questions were necessary to gather the desired data. The interview protocol/guide was designed with as little technical depth and as much brevity as possible without compromising on integrity, to manage participant focus.

The *questions* can be seen more at length in the interview protocol/guide (Derbyshire, 2019); however, the main question structure is as follows:

Risk Assessment Data Collection and Processes:

- What do you understand cyber security risk assessment to include?
- What data are you required to collect for use within your existing risk assessment methodology?
- Once you have acquired relevant data, how is it applied within your existing methodology to derive cyber risk?
- How important is it in your risk assessment to consider the adversary and their capability?

Risk Assessment Output and Delivery:

- How is the output of this methodology used to communicate cyber risk?
- With whom do you usually convey the risk assessment results?
- Do there exist any challenges in the conveyance of cyber risk through the use of your existing methodology?

Adversary Cost:

- Do you believe conveyance of cyber risk through "cost" could provide a more effective narrative? More specifically, this is the cost to an attacker seeking to compromise a client's system?

Overall Opinion of Risk Assessment:

- What do you think of the effectiveness of current risk assessment methodologies?

3.1.2. Analysis

Template analysis was selected for its flexibility when analysing qualitative data, such as from semi-structured interviews (King, 1998). Template analysis has fewer specified procedures in contrast to, for example, content analysis (Weber, 1985) or grounded theory (Glaser and Strauss, 1967). However, there are proposed recommendations for use, which were followed within the analysis (King, 1998).

To begin with, the interview protocol/guide was used to create an initial set of data categories, viz. a code set. This code set was hierarchical with a carefully chosen level of abstraction, which allowed for further granularity or abstraction if deemed necessary. Additional codes were added to the set after a brief review of two of the transcripts, and then the set was reviewed by a separate researcher for validation. The code set then evolved throughout the codification process, which included codes being added, deleted, altered, and alterations to the hierarchy of the code set itself.

The resulting coded data was then analysed; this was done by reviewing all transcripts. Code frequency was noted throughout the process, seeking to identify trends in the risk assessment processes of the participants. Where anomalies occurred, such as a small number of participants answering differently to the majority, further reviews of codes and anomalous transcripts were conducted to understand why.

3.2. Results

The following subsections provide a discussion about the analysed data collected during the interviews, presented in the form of major themes discovered throughout, rather than individual questions or a statistical analysis. Each point discussed within the themes is followed by a pertinent statement or assertion made by an interviewee.

3.2.1. Risk assessment data collection and processes

Overall, cyber risk assessment was considered to be both broad and holistic in nature. It was most frequently described as a sum of its granular, practical components, such as threats, assets, and impact. This is synonymous with the formula $Risk = f(Threat, Vulnerability, Impact)$ that is typically found at the centre of risk assessment methodologies. The use of assets – rather than specifically vulnerabilities, combined with concepts more focused around business, including risk appetite, operational/business requirements, and compliance – exposed the perception that it is a function to be considered organisation wide.

"... when I'm doing a cyber security risk assessment, I'm trying to boil the ocean... "

All participants said that they collected asset, or asset value, information as an important part of data gathering, making it the most prominently collected type of data and also consistent with cyber risk assessment being operational/business focused. The collection of asset data was deemed critical in risk assessment because it provides multiple functions; the predominant two are (1) identifying vulnerabilities in, or between, the assets and (2) estimating the potential business impact if the asset is affected by an incident. Example data gathered for the former includes IP addresses, architecture diagrams, and technologies involved; for the latter, the financial value of assets and their required level of confidentiality, availability, and integrity (CIA).

"... you'll kind of leverage those interviews to get the experts to help you understand how the business operates, where the information lives, how it moves around... "

Along with gathering data for assets, threats were also of high priority for the majority of participants. Discussions frequently focused on threat actor, or adversary, categories which infer the level of threat posed in a scenario; these categories included, for example, script kiddie, hacktivist, organised crime, or even nation-state sponsored hackers. For many participants, this would typically not exceed assigning a semi-quantitative number ((1–3), (1–5), etc.) for threat severity in accordance with categories found in various standards and guidelines, dependent on the context of the client's business and particular industry sector. A small number of participants considered threats in more detail in two possible ways: threat intelligence, or breaking the adversary into a sum of components. Threat intelligence will provide more bespoke information about which adversaries will be targeting a specific client; this information is collected via various sources across the participants, ranging from open source intelligence (OSINT) to government reports or even internally operated cyber security operation centres (CSOCs). When an adversary is broken down into a sum of its components, this means participants consider that certain attacks may require a certain amount of

technical capability, any financial costs which may be incurred during an attack, the inherent risk of detection when trying to remain clandestine, and the time it may take to successfully accomplish an attack.

"The threat actor needs to be identified and then certainly there needs to be an understanding of their capability... "

A minority of participants did not consider threats at all in their risk assessment, instead opting to focus their efforts entirely on what data they could realistically acquire.

"... it's actually pretty much impossible to say what sort of threat actor is going to be realised on that system."

Participants mentioned additional forms of data that they gather, but these were less frequent than assets and threat information. The impact of an attack is usually predicted either as a combination of asset value and estimated value of it being attacked in money and reputation, or semi-quantitatively on a numeric scale ((1–3), (1–5), etc.) as a representation of CIA impact if attacked. Pure vulnerability data, separate from assets, is usually captured from scanning or penetration testing; this is often first in the form of CVSS and then reduced to (high, medium, low), or (red, amber, green). An organisation's current security controls are gathered to discern its current risk posture and understand which vulnerabilities may already be mitigated, this is usually in the form of documentation and technical configurations. Finally, an organisation's risk appetite is gathered to help assessors understand how much risk the client will accept, along with their willingness to spend or invest to implement necessary changes.

"... if you were going to take a vulnerability assessment as an understanding of vulnerabilities, each of those will have CVSS scores or some kind of risk rating associated with it... "

Processing gathered data to produce a risk output was reportedly less heterogeneous than the data gathered itself, commonly using the various types of data in similar ways. There was a strong emphasis on observing standards and guidelines among participants, including Cyber Essentials, the ISO/IEC 27000 series, and the NIST 800 series. These standards and guidelines prescribe the data gathered, as above, to varying specificity and then offer further methods to process that data. Participants, almost unanimously, combine expert opinion with some form of semi-quantitative risk matrix or spreadsheet, congruent with the review of these, and similar industry methods, in Section 2.1.

"To be honest with you it's all done in the head, when I say "gut feel", it's based upon 20 plus years of experience rather than sort of any actual kind of algorithm per se"

Participants insisted that expert opinion was required to provide much needed context to a variety of aspects of cyber risk assessment. To that end, expert opinion is deemed valuable in cyber risk assessment to ensure that it remains pragmatic and focused on the system under consideration, not limited by processes and procedures.

"I'll use a risk matrix to gain an initial risk score but I'll also allow the context to justify an up/down scoring of where the risk has landed initially if I feel it warrants it"

3.2.2. *Risk assessment output and delivery*

Most participants described the produced risk output as a list of findings uncovered during the risk assessment. All participants who delivered such a list said that it was prioritised in descending order of risk, such that the most critical risk scenarios or vulnerabilities were prominently displayed first. In such lists, risks were characterised as the output of expert opinion and risk matrices in a semi-quantitative or qualitative form, (1–3), (1–5), (red, amber, green), or (high, medium, low). The common opinion among participants was that going into more detail than this for the risk posed to the organisation gave, at best, no improvement but could even confuse the recipient of the report.

"... people understand the difference between a low and high risk, whereas the difference between a six and a five is very difficult for humans to comprehend."

The output varied between participants in that there were different levels of technical detail described, sometimes in the same report in order to provide the most value for both management and technical staff. Headlines and overall risk are presented to executives in a summary, and technical details and remediation advice are reserved for technical staff.

"I always include statements to the various types of people that might read my output... a board is interested in the risk posed whereas the technical person wants to understand what's the risk posed by the individual components"

As has been indicated, the recipients of the risk assessment output were diverse. The three dominant recipient categories were upper management and director level, middle management such as heads of teams, and technical staff. Participants stated they have to report to such a variety of personnel in an organisation due to the holistic nature of cyber security, which affected most aspects of it in some way.

"... there will always be a business owner that's bringing you in to do the test, but what you might be doing is talking to the developers to help them understand the issue."

There exist several challenges when delivering a cyber security risk assessment; however, the most prominent is a lack of awareness on the client's behalf. Participants reported that the middle management and above do not understand the severity of the risk's impact or will not grasp the technical, "cyber" aspect. They, therefore, deem it necessary to deliver separate reports to management, containing simpler terminology.

"We were obviously talking a different language to them... "

At board level, cyber security was said to have been seen as a disabler rather than an enabler because it is so frequently articulated in a way that is unsuitable for many of the board members. This led to another, intertwined challenge of risk assessment delivery, viz. not being able to speak to the right person to make decisions because cyber security becomes less of a priority when the risks are not understood.

"Speaking their language, making sure your risk assessments match the finance people in particular... if you can match the finance director, if he articulates to the CEO, if you don't make that investment this is going to happen, he believes him."

3.2.3. *Adversary cost*

Adversary cost elicited a positive response from the participants. The overall opinion was that delivering cyber risk as, or accompanied by, an anticipated cost for an adversary to realise a scenario or leverage a vulnerability would be an effective narrative to communicate cyber risk, particularly at the executive level. Adversary cost was also described as a poten-

tial solution to improve risk likelihood, which is a perceived weakness in cyber risk assessment.

"... cost on the attacker's side would be a useful thing to the reader, to the non-technical reader, to be provided to maybe convey the difficulty of exploiting the risks that we're presenting."

There were, however, two considerations provided by participants. A number of them, who worked in environments which would potentially attract nation-state activity, stated that there becomes a point where executing an attack provides such a strategic advantage that cost is irrelevant. Once a target is sufficiently mission-critical, a nation-state will clearly be willing to invest a very significant amount of resource to achieve its goal.

"... it makes no odds to them, because if there's something they want they will throw the resources at it."

Participants also noted that in order to understand the cost to an adversary, you first have to understand what security controls are (or could be) in place, and how effective they are. It would therefore be necessary to carefully consider cyber security controls and their effects when assessing adversary cost.

"... I think in order to understand an adversary's cost we have to understand what the efficacy is of a security control in order to prevent that attack, I don't think you can do those two things in isolation; I think they go hand in hand."

3.2.4. *Overall opinion of risk assessment*

Overall, participants had a critical opinion of current cyber risk assessment methods and practices. The criticisms ranged from too much of a focus on compliance and "tick box exercises" to methods which require estimating (abstract) numbers despite a lack of data.

"... adding pretend numbers into an algorithm, and the more numbers you put in and the longer you make that algorithm, the more wild the range of numbers you can get out can be."

3.2.5. *Summary*

Eight out of ten participants considered threats, or the adversary, to be important in their risk assessment. This was typically consistent with one of the approaches in Section 2.1. Adversaries were assessed by their capability, separate from the rest of the risk assessment, then by a notion of likelihood derived from the combination of the two. Although this was the most common way of including the adversary, there were also criticisms that it was a weak link in cyber risk assessment due to poor data availability.

There were reported delivery challenges due to a lack of awareness on the client's behalf. Cyber security risk was said to not have been taken seriously at board level or, in certain circumstances, not reported to the board at all. This was said to be because it does not traditionally conform with similar risk assessment outputs such as that of the financial director or chief financial officer (CFO), something that Hubbard and Seiersen state is due to the qualitative nature in which cyber security risk is delivered (Hubbard and Seiersen, 2016).

Adversary cost received positive feedback as a supplement to cyber risk assessment, postulated to be something which would improve communication to clients and assist in their understanding of the likelihood of a scenario being realised. It was posited that cyber security controls and their efficacy would have to be included in adversary cost for it to be truly effective. Furthermore, relevant considerations for cost could be found in participants' deeper understanding of adversaries, breaking them down into technical capability, time investment into attacks, financial investment into attacks, and the level of risk they are willing to accept.

4. Structuring adversary cost

The gap in assessing threats in cyber risk assessment and the concept of adversary cost filling that gap, highlighted in the literature review, were both confirmed during the interviews with cyber risk assessment practitioners. Moving forward, bringing adversary cost to practical fruition first requires it to have a structure on which to build; therefore, this section provides two functions. First, a foundation of cyber attack techniques is identified, as a basis for establishing structure and a uniform vocabulary for the methods which an adversary would use. Second, and as recommended by the interview participants in Section 3, a uniform and comprehensive set of controls is defined which would allow an end user to make sure no cost-altering controls are missed in an assessment.

4.1. *Identifying an attack framework*

Fig. 2 depicts a high level outline of a cyber attack. However, in between the stages shown here (reconnaissance, exploit, control, or data exfiltration), there exist more nuanced stages such as privilege escalation and lateral movement. Adversaries then have many techniques they may employ for each stage of an attack which, in turn, will vary depending on the environment in which they are performing the attack. The culmination of this points clearly to the complex nature of cyber attacks (Derbyshire et al., 2018).

Our previous work (Derbyshire et al., 2018) analysed cyber attack taxonomies which bring structure to the many techniques and their overarching stages. It found that, among the 7 prominent cyber attack taxonomies under analysis, MITRE's Common Attack Pattern Enumeration and Classification (CAPEC) (Barnum, 2008) achieved all criteria defined in the literature as an adequate taxonomy and could categorise techniques used in all twenty of the historical attacks used as case studies. CAPEC's strength, namely its ability to categorise so many techniques, was also criticized because of the unwieldy nature of its many granular techniques, going as many as seven sub-categories deep for some of them. In our previous work, this criticism stipulated that this granular and detailed nature could be overwhelming for less experienced users of the taxonomy, even with the guidance provided. In the case of deriving an adversary's cost, this intricate granularity would be too cumbersome to provide sufficient detail for each technique described.

The MITRE ATT&CK® (Adversarial Tactics, Techniques, and Common Knowledge) Framework (MITRE, 2019a) is considered the de facto industry standard for profiling tactics, techniques, and procedures of adversaries due to its multi-stakeholder contribution (MITRE, 2019b). It is primarily structured by Tactics that an adversary may perform during an attack to achieve a specific aim, beginning at Initial Access and then moving

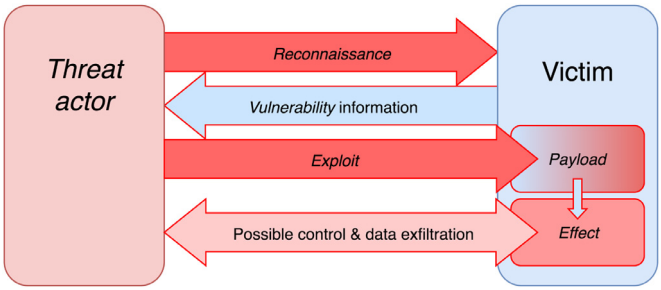

Fig. 2 – High level structure of a cyber attack (Derbyshire et al., 2018).

through all of the high level actions which may be taken such as Privilege Escalation or Lateral Movement, and then concluding with Impact of the attack. Each Tactic is then broken down into individual Techniques; these are more specific ways in which the adversary may achieve the aim of the Tactic. ATT&CK's Techniques are the lowest level of the framework, which remain at a higher level than those in CAPEC and are therefore less cumbersome to convey an adversary's actions costs.

For the purpose of this paper, the lower level Techniques will be taken into consideration throughout, but the predominant focus will be on the higher level Tactics.

4.2. *Cyber security controls*

As the interview participants judiciously noted in Section 3, to truly understand an adversary's attack cost, one must also know the available cyber security controls and be aware of the effect that they have on it. Therefore, a comprehensive set of controls needs to be established at a uniform level of granularity, which would holistically represent an entire Tactic as well as individual Techniques. This would provide end users with a reference of controls which may be in place, to ensure all cost-affecting controls are accounted for during an assessment.

Mechanisms for detection and mitigation are aggregated and described in each Technique of the ATT&CK Framework. To derive an appropriate list of controls, these descriptions were dissected and organised into a list of potential controls for each Technique. This was produced with two particular Tactics of the ATT&CK Framework as a proof of concept - Initial Access and Lateral Movement. The controls derived from ATT&CK's descriptions were compared against three prominent control lists, SANS CIS Critical Security Controls (SANS, 2019), NIST 800-53 (NIST, 2013), and ISO/IEC 27002 (BSI, 2013), for the purpose of ensuring a more authoritative set of controls. The comparison of three control lists allowed the best to be discerned by matching the following criteria:

- Comprehensive coverage of ATT&CK's suggested controls.
- Appropriate granularity of all authoritative controls.
- Uniform granularity across all authoritative controls.

SANS CIS Critical Security Controls was found to have no additional layers of granularity, and while it could arguably cover the controls described by the ATT&CK framework, the single level of granularity could perhaps cause overlap. NIST 800-53 was found to offer multiple layers of granularity for sets of controls, meaning that an appropriate, uniform layer could be used while covering all of those described by the ATT&CK framework. ISO/IEC 27002, like NIST 800-53, has multiple layers of granularity and could cover all of the ATT&CK framework's controls, but the layers are less uniform than found in NIST 800-53 and so would require more in-depth curation. For these reasons NIST 800-53 was chosen to represent the authoritative cyber security controls, creating Table 1 and 2 for the list of controls per Tactic and Technique therein, and a key for those controls in Table 3. The controls were then amalgamated and duplicates removed to represent the holistic controls per Tactic.

4.3. *Cyber security control validation: Methodology*

To ensure the validity of the proposed authoritative cyber security controls, a set of interviews was conducted with offensive cyber security practitioners. This was stage one of a two-stage interview; stage two will be discussed subsequently, in Section 5.

4.3.1. *Interviews*

This first stage of the interviews followed an almost identical methodology to that in Section 3.1. Semi-structured interviews were conducted with a predefined question set; however, the question set was brief, allowing for the discussion to be focused around the participants' thoughts about the authoritative controls.

Sample selection was, again, carefully considered. Experienced, senior offensive cyber security professionals from a diverse range of organisations were chosen as participants. Seniority and experience were critical due to the need to be comprehensive when addressing the authoritative controls. Six participants were interviewed; these were selected from a larger pool of possible participants based on the diversity of skillsets while maintaining the necessary experience and seniority. No further participants were selected due to data saturation in both stages of the interviews.

Validity of data was maintained in much the same way as the prior interviews. In this instance the only difference was the question set, which was derived from the development and nature of the authoritative control set, as seen in Tables 1 and 2, rather than solely the related literature.

Table 1 – Initial Access Techniques and their Controls.

Technique	800-53 Reference
Drive-by Compromise	CM-6, SC-2, SC-7, SI-2, SI-4
Exploit Public-Facing Application	AC-2, AC-6, RA-5, SA-8, SC-2, SC-7, SI-2, SI-4
External Remote Services	IA-2, SC-7, SI-4
Hardware Additions	CM-8, SC-7
Replication Through Removable Media	CM-7, SI-4
Spearphishing Attachment	AT-2, CM-7, SC-44, SI-3, SI-4
Spearphishing Link	AT-2, SC-44, SI-4
Spearphishing via Service	AT-2, CM-7, SI-3, SI-4
Supply Chain Compromise	SA-12, SA-19, SI-2, SI-3, SI-7
Trusted Relationship	AC-2, SA-12, SC-7, SI-4
Valid Accounts	AC-2, IA-5, SI-4

Table 2 – Lateral Movement Techniques and their Controls.

Technique	800-53 Reference
AppleScript	CM-7, SI-4
Application Deployment Software	AC-2, CM-7, CM-9, IA-2, IA-5, SC-7, SI-2, SI-4
Distributed Component Object Model	CM-6, CM-7, SC-7, SI-4
Exploitation of Remote Services	AC-2, CM-7, RA-5, SC-2, SC-7, SI-2, SI-4
Logon Scripts	AC-2, CM-7, SI-4
Pass the Hash	AC-2, CM-6, IA-5, SI-4
Pass the Ticket	AC-2, CM-6, CM-7, IA-5, SI-4
Remote Desktop Protocol	AC-2, CM-6, CM-7, IA-2, SC-7, SI-4
Remote File Copy	SI-4
Remote Services	AC-2, IA-2, SI-4
Replication Through Removable Media	CM-6, SI-4
Shared Webroot	AC-2, CM-6, SI-4
SSH Hijacking	CM-6, IA-5, SI-4
Taint Shared Content	AC-2, CM-6, CM-7, SI-3, SI-4
Third-party Software	AC-2, CM-7, CM-9, IA-2, IA-5, SC-7, SI-2, SI-4
Windows Admin Shares	AC-2, CM-6, CM-7, IA-5, SI-4
Windows Remote Management	CM-6, SC-7, SI-4

Table 3 – NIST 800-53 (NIST, 2013) reference guide.

800-53	Control Title
AC-2	Account Management
AC-6	Least Privilege
AT-2	Security Awareness Training
CM-6	Configuration Settings
CM-7	Least Functionality
CM-8	Information System Component Inventory
CM-9	Configuration Management Plan
IA-2	Identification and Authentication
IA-5	Authentication Management
RA-5	Vulnerability Scanning
SA-12	Supply Chain Protection
SA-19	Component Authenticity
SA-8	Security Engineering Principles
SC-2	Application Partitioning
SC-44	Detonation Chambers
SC-7	Boundary Protection
SI-2	Flaw Remediation
SI-3	Malicious Code Protection
SI-4	Information System Monitoring
SI-7	Software, Firmware, and Information Integrity

Reliability was adhered to in an identical manner to the prior interviews and remained unchanged in methodology.

Individual, face-to-face, interviewing was the *practical technique* used to perform the interviews, and was the major difference between these and the prior interviews. While this was necessary for the second, practical stage of the interview, face-to-face interviewing complemented the semi-structured technique used for this first stage. The protocol/guide was designed with face-to-face interviewing in mind, allowing for a free flow of ideas while maintaining participant focus. Participants were also given ample time to digest the Tactics, with their included Techniques and authoritative controls, before being asked to give opinions on them.

The *questions* asked of the participants, which can be found in the interview protocol/guide (Derbyshire, 2019), focused primarily around the authoritative control sets. For each control set they were asked:

- Do you think this level of abstraction for security controls is appropriate?
  - *Probe: If it is too high/low level, why do you think this?*
- Do you think that the controls listed are comprehensive? That is, in performing the various Techniques in this Tactic,

would you expect to see any other cyber security controls employed to defend against you (the adversary)?

4.3.2. *Analysis*

As with the previous set of interviews, the analysis technique remained the same. Template analysis allowed for flexibility, defining the initial code set from the interview protocol/guide and then allowing it to evolve over the analysis process. Once all the data was coded, this was then analysed, noting code frequency to identify trends and understand the reasoning behind them. Anomalous points were reviewed to ascertain their root cause.

4.4. *Cyber security control validation: Results*

The following subsections are a discussion of the analysed data collected during the interviews. This is presented as the major themes - abstraction, comprehensiveness, and additional considerations. As the process for establishing the authoritative controls was the same for both Techniques, they have been grouped together and are distinguished when necessary by participant comments. Again, each point discussed within the themes is followed by a pertinent statement or assertion made by an interviewee.

4.4.1. *Abstraction*

Overall, participants found that the authoritative controls' level of abstraction was adequate. Most understood the abundance and complexity of controls which had been reduced into categories and thought the abstraction allowed for a flexibility in interpretation.

"I think the level's okay because it gives people freedom, it encapsulates the concept well, but still allows enough agnosticism towards particular setups and technologies and even sub systems... "

Some participants, particularly when considering lateral movement, thought the abstraction level may be too high due to the adversary's wealth of techniques and use of other, complementary Tactics such privilege escalation. This was noted, however, as a weakness of using two isolated Tactics from the ATT&CK framework and that lateral movement was a very hard problem to solve due to it being a fast-paced, moving target.

"Especially in light of the speed at which lateral movement techniques adapt and depend on the elements that are inside the company. There are so many more ways to get access, to escalate my privileges and move around, that is the main battle."

4.4.2. *Comprehensiveness*

The participants found that the authoritative controls were comprehensive in nature, without any notable omissions.

"I am sure that a company implementing all those techniques, will have something that will block that something at some point."

There was a critical comment surrounding the interpretation of the authoritative controls affecting comprehensiveness, where multiple interpretations of one control listed would be needed to defend against multiple Techniques. The underlying issue here was recognised to be abstraction, rather than comprehensiveness, for which a solution was proposed by participants, discussed in Section 4.4.3, Considerations.

"They don't necessarily enumerate what you can do to implement those controls at all... boundary protection, for example, there's different ways of doing that and they are not enumerated... "

4.4.3. *Considerations*

The ability to be comprehensive was seen as compromised with just authoritative controls titles being apparent. Participants were unclear as to what practical controls could be implemented under them, and in some cases thought multiple practical controls could be implemented under one authoritative control for different purposes or to greater effect. Multiple participants stated that the authoritative control list would be considered effective with an explanation of each as supplementary documentation. This can be achieved by using the appropriate text for each control described in NIST 800-53 (NIST, 2013).

"If you give it some bounding and just say that 'By authentication management we mean this sort of scenario or within these areas.' I think that would be really handy."

4.4.4. *Summary*

Participants were presented with two Tactics and their Techniques, together with a list of authoritative controls derived from NIST 800-53 (NIST, 2013). Overall, it was found that the authoritative controls were presented at an appropriate level of abstraction. There were some comments expressing that the Tactic, Lateral Movement, was perhaps too high level. However, it was concluded through discussion that this was a difficulty with the vastness and proliferation of Lateral Movement attack techniques, and also a weakness in the Tactics chosen for this particular interview, due to complementary Tactics which could affect Lateral Movement.

Similarly, the authoritative controls were found to be comprehensive. There was a critical comment during the discussion of comprehensiveness with one participant; it was stated that the authoritative controls could represent multiple practical control implementations, leading to possible ambiguity as to what was covered. This was deemed to be more of an issue with abstraction, rather than not being comprehensive. The suggested solution was for each authoritative control to have a description to indicate what could be included within it.

With the authoritative control set, it is now easier for an end user to consider all of the appropriate controls per Tactic or Technique when assessing cost. This means that during an adversary cost assessment, the end user would be less likely to miss cost-affecting controls, implemented in the system under consideration.

5. The factors of adversary cost

With the offensive and defensive structures established, the next step is to determine the constituent components, or factors, of adversary cost. This section describes two separate approaches which were used.

The first, preliminary, approach used desk based research to extract actions taken by adversaries in historical attacks. The types of cost were then postulated by the research team

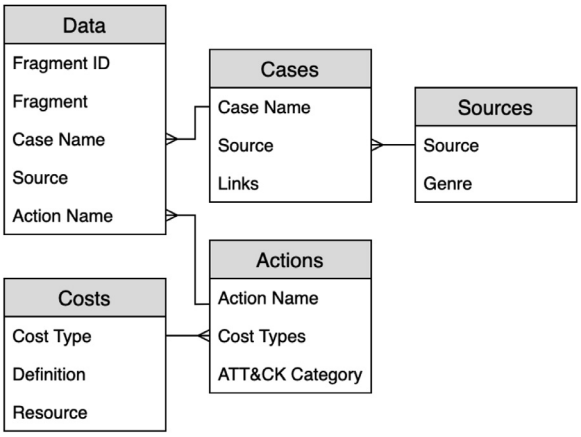

Fig. 3 – Database structure for historical attacks.

for each action, providing a foundation for discussion with experts in the second approach.

The second approach, which was stage two of the previously mentioned two-stage interviews, involved interview participants completing an offensive security scenario based exercise. The participants were asked about the factors of cost they may experience during and surrounding the actions taken in the scenario.

5.1. *Adversary cost factors from historical attacks*

The historical attacks were chosen based on their source material adhering to the following criteria:

- Broad in coverage.
- A reasonable level of detail.
- A reputable source such as an academic artcle or industry whitepaper.

Data fragments were extracted from the historical attacks, each describing an action taken by the adversary. These fragments were then put into a database and aligned to the ATT&CK framework, the relational diagram of which can be seen in Fig. 3. The research team then extracted prospective factors of cost which the adversaries would have experienced in performing the actions. For example, the fragment, "... malicious office documents were delivered via email to individuals in the administrative or IT network of the electricity companies", can be found regarding the Kyivoblenergo attack of 2015 (Lee et al., 2016a). This was identified as a Spearphishing Attachment within the Initial Access Tactic of the ATT&CK Framework. The research team posited that the reconnaissance of targets, crafting of emails and malicious scripts, and setup of the infrastructure would predominantly take time, but the adversary would also have to purchase or rent infrastructure using financial resources. Other attacks reviewed for cost factors were Stuxnet (Farwell and Rohozinski, 2011), Havex (Nelson, 2016), German Steel Mill (Lee et al., 2016b), and the Equifax breach (Luszcz, 2018; Smith and Mulrain, 2017).

This exercise resulted in two factors of cost being extracted from the actions taken by adversaries. It was proposed that adversaries must spend:

- *Time*, including learning the required skills, preparing for, and performing the attack; and
- *Finance*, including purchasing equipment, any server hosting, any tooling, or perhaps 0-days.

5.2. *Validating adversary cost factors: The methodology*

The use of historical attacks proved useful as a preliminary study, to infer what costs an adversary may experience during an attack. There may also be more subtle costs or interdependencies which could not have been extracted. Stage two of the two-stage interview uses an ethnographic approach to further understand adversary cost factors.

5.2.1. *Interviews*

As this was the second stage of the interview process described in Section 4, many aspects remained the same. There were also, however, some significant differences. The primary difference was the use of a practical scenario for participants to complete while asking task-related grand tour questions (Spradley, 2016), an ethnographic approach to semi-structured interviews. This meant that participants were asked about the actions they were performing throughout the scenario as well as questions from a predefined question set.

Sample selection and *reliability* were both related to stage one of the interview process, described in Section 4.

Validity, again, was maintained in a similar way to the prior interview process, the only difference being the derivation of the question set. The majority of the questions were spawned from actions taken by participants during the practical scenario, asking participants to describe the actions, what they meant, and what types of cost would have occurred in a real black-hat (malicious) engagement (Spradley, 2016). Other than these task-related grand tour questions, semi-structured questions were also prepared so they could be asked after individual phases and after completion of the scenario. These were to ensure the data gathered was not just limited to the practical scenario itself and broached other attack vectors and aspects of an attack.

Individual, face-to-face, interviewing was the *practical technique* used to perform the interviews. As discussed in Section 4, in-person interviews were necessary for participants to effectively complete the scenario and discuss their thoughts around it, during this stage of the interview.

The *questions* asked were predominantly driven by the practical scenario, but there were some structured questions asked throughout, all of which can be found in the interview protocol/guides (Derbyshire, 2019).

Prior to the scenario, the participants had the scene set for them, including a scan of the perimeter with nmap (Lyon, 2019). They were then asked:

- For expediency's sake, assume you have completed the nmap scan on the desktop. What types of costs do you think may have occurred up to, and including, that point?

The participants were then asked to begin compromising systems. During each action or technique performed throughout the scenario, participants were asked task-related grand tour questions such as the following:

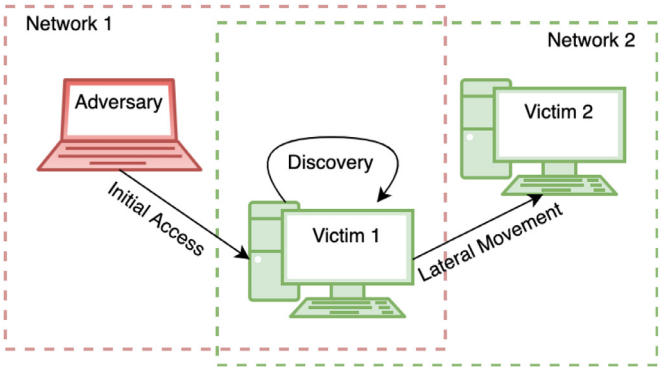

Fig. 4 – Diagram of the practical scenario.

- What particular techniques are you using?
- Why are you using these techniques?
- What tools are you using?
- What costs are there in acquiring and learning these tools/techniques?
- What processes would be involved for learning these tools/techniques?
  - *Probe: If courses are mentioned, what kind of financial/time investments would be expected in order to complete?*

As Initial Access and Lateral Movement were the prominent Tactics demonstrated during the scenario, on completion of these, participants were asked:

- Do you think there would be any different types of costs incurred if you used a different {Tactic} Technique such as {alternative Technique options}?

Finally, after the scenario was completed, the following questions were asked in order to ensure no other cost factors would arise outside of the scenario:

- Do you think you would incur any different or extra costs for carrying out additional tactics?
- Do you think these costs are affected by the target implementing cyber security controls? If yes, how are they affected?

5.2.2. *Practical scenario*

The scenario was designed to elicit the maximum information about adversary cost factors from the participants while not posing too much of a challenge or taking too much time, to maintain concentration. Another design choice was to represent multiple Tactics of the ATT&CK framework. It was decided that two of these would be Initial Access and Lateral Movement, in congruence with the authoritative control selection in Section 4.2. In addition to these, the Discovery Tactic was chosen so that it could facilitate Lateral Movement.

Fig. 4 depicts a high level overview of the scenario and how the machines were connected; the suggested commands to completion can be found within the interview protocol/guide (Derbyshire, 2019). The 'adversary' machine had access to a network interface of the first victim as it would across the Internet, allowing for *Initial Access* techniques to be used against it. The participants would find an nmap (Lyon, 2019) scan of Victim 1 on the desktop of the adversary machine they were given access to, which was running Kali Linux (Offensive Security, 2019); this was to expedite the potentially long scanning process. Within the nmap scan's output, participants would find that the target machine was vulnerable to the EternalBlue exploit, chosen for its infamy and stability (Dillon et al., 2019; Nakashima and Timberg, 2017), to ensure participants knew exactly what choice to make and that failed attempts were kept to a minimum.

Once the participants had access to the Victim 1 machine, they would use *Discovery* techniques to discern that, on it, there was a second network interface and a text file on the desktop containing remote desktop protocol (RDP) credentials with an IP address. It was then up to the participants to use *Lateral Movement* techniques to pivot to Victim 2. To do this they would need to route their traffic through Victim 1 and use the RDP credentials to log in. After they were logged in, the scenario would be signalled as over by the participants finding a text file on the desktop of Victim 2, thanking them for completing it.

While participants were completing the scenario, the desktop of Kali Linux was recorded, to ensure that if any particular actions of interest were performed during the interview it would be possible to review them during analysis.

5.2.3. *Analysis*

Although the interviews used a different technique based on ethnography, viz. task-related grand tour questions, the data was not considerably different. This allowed for the use of template analysis again, which was achieved in the same way as discussed in Sections 3.1 and 4.3.

5.3. *Validating adversary cost factors: Results*

The following subsections present a discussion of the analysed data extracted from the practical interviews. This discussion is separated into the Tactics as they occurred in the scenario, including both the task-related grand tour questions and all other Tactic-related questions asked of the participants. After this, all post-scenario questions are discussed.

5.3.1. *Pre-scenario*

Prior to performing any actions, participants were presented with the output of an nmap scan and asked what factors of cost they may have experienced up to that point. The most prominent factor identified by participants before the attack was time. Reconnaissance and enumeration, phases preceding Initial Access for gathering and contextualising information, were highlighted as extremely important. It was noted that, for an attack to be truly successful, these phases must be conducted in a thorough and rigorous manner, meaning they can be time consuming. The output of the nmap scan was said to be indicative of the final stages of reconnaissance and enumeration, where prior actions would have been taken such as open source intelligence (OSINT) to gather precursory information.

"... you have to take the time to work recon properly, and while nmap is a stage of that, it's the later stages of recon. What you might do first is OSINT... There's a lot of prologue, if you will, so even nmap scanning you will need to find that information... "

Active techniques such as nmap, where the adversary interacts with the target infrastructure, produce well known signatures due to a relatively large amount of identifiable traffic, which the participants called 'noisy'. The majority of participants stated that this highly detectable traffic created a factor of cost in perceived risk, meaning there was a risk of being detected by the target. When mentioning this, participants also said that this would induce more time cost, due to the need to slow the techniques down and reduce the likelihood of detection.

"... it's also very noisy, so even if you get half open ports, SYN scans and stuff are likely to trigger some kind of defensive mechanisms that log attacks or identify potential attacks and port scanning... "

While often described as time by participants, it was posited that there was an experience or capability cost prior to the attack. In every aspect of the reconnaissance and enumeration phases described, prerequisite knowledge was said to have been necessary. This ranged in technical depth, from generally how to find out information about a target using OSINT to interpreting scan data, or even setting up infrastructure to obfuscate the origin of the attack.

"The cost might be knowledge and the cost might be experience and it might be technical skill, and that translates to time... "

Certain actions, such as setting up infrastructure, may cost money, which leads to a Finance cost factor for adversaries. It was mentioned that an adversary may pay for this infrastructure, on a cloud hosting provider, that may provide some anonymity or make the traffic look more genuine. This complements the previously mentioned Risk cost factor, in that a financial cost would be willingly incurred to reduce it.

"Say this is a customer that has a virtual desktop on Azure and I know this server is accessed during the day in Australia. I will rent a box on Azure in Australia, log on in Australian daytime and do the activities so they cannot run into the whole day activity."

5.3.2. *Initial access*

During the Initial Access stage, participants were all expressing concern about the Risk cost factor. While the scenario had no security controls or detection capability, the possibility of these being there (had it been a real black-hat engagement) was noted as pivotal in all decision-making processes. Participants frequently mentioned that, rather than use Metasploit (Rapid7, 2020), which would produce well known signatures to all security monitoring controls, they would exploit through a manual script and use a custom payload to reduce likelihood of detection.

Furthermore, despite the nmap scan's output being verbose about the vulnerability, participants would double check they had the correct exploit and payload for the target machine. This would be done using the exploit module's check functionality within Metasploit or the dedicated auxiliary module (Dillon et al., 2019; Dillon and Jennings, 2019).

"Sometimes the exploits have a check function... So, if it's possible, I normally do, just to reduce the risk - because some of these exploits, if they don't work, they do a denial service and you don't need that in your life"

Experience and time were two cost factors which were used almost entirely in a synonymous way by this stage of the interview, with time being the overarching factor. The time in gaining the knowledge and experience was said to have constituted the main cost in all of the participants' opinions. Whether through previous time spent in information technology roles, completing training courses, experimenting with private testbeds, or just in-depth reading about the technologies used, investing time into being able to perform the attack was deemed absolutely necessary.

"... the cost of going from that to that is just about time, effort, and perseverance really. It's not a dark art, it's just that you just have to dedicate the time."

The Initial Access phase also highlighted a Finance cost factor. The most prominent one mentioned was the possibility of purchasing, legitimately or otherwise, a server for launching the attacks. While cloud hosting services were one avenue suggested by the ethical participants, it was suggested that black-hat adversaries might purchase access to a pre-compromised machine from other black-hats to reduce any links back to themselves.

Another financial cost mentioned was paying for courses to gain the required knowledge and experience. Building a testbed to learn or practise was also given as an alternative or extension to paying for courses, which would also involve a financial cost.

Finally, adversaries may purchase licenses for legitimate, commercial tooling or less-than-legitimate, black-hat tooling. One, extreme, suggestion was that if no other method of access was available, purchasing an exploit to a 0-day vulnerability would be possible. However, this was mooted as an option likely to only be available to well resourced adversaries.

"... you may rent access to somebody else's attack machines. I don't go shopping for botnets but I believe that botnets are very easily bought and I would imagine that staging servers would also be very easily bought... "

No additional factors of cost were offered by participants when asked about using alternative Techniques to complete the Initial Access Tactic. It was suggested, however, that using alternative Techniques would incur varying quantities of cost. For example, phishing may incur more financial cost for the infrastructure, time cost to collate email addresses and understand how to set up the infrastructure, and carry an element of risk if the phishing emails get reported.

"You need to understand who your victims are... to spin up your infrastructure to send those emails... All of this information is leaving a trail. Did I use my credit card to buy the domain?"

5.3.3. *Discovery*

Once Initial Access was completed, participants were then tasked with finding the second network interface and RDP credentials on the first victim machine.

Familiarity, and therefore time spent gaining experience, with the compromised machine was deemed a critical factor in completing the Discovery Tactic. When discovering information about a compromised machine, participants mentioned that their familiarity with an operating system, such as how the networking, file system, or user structure works, is what they primarily rely on. This is typically learned through time spent using the operating systems and an understanding of how users may use the file system, and where they would store their files which may contain data of interest.

Another aspect of the Time cost factor is to find useful information within an operating system, whether manually or programatically searching for credentials, or cracking password hashes taken from software or the operating system itself. Discovery can be a time intensive Tactic.

"First of all, familiarity with the base operating systems, like functionality... The other thing is just general awareness of people's behaviour, really... "

There were two elements of the Risk cost factor discussed during this stage in the scenario; the risk of being detected and the risk of losing access to the compromised machine. Both of these risks being realised would significantly hinder the adversary's operation.

"An experienced attacker will know that it is likely to be a short connection that they have got for various reasons, particularly if they are attacking us over the internet."

5.3.4. *Lateral movement*

The cost factors identified by participants for Lateral Movement coincided with both Initial Access and Discovery.

Risk was identified as a cost factor while moving laterally within the scenario network. Participants would scan the internal machine's RDP port to check that it was open as it would generate less traffic than if they incorrectly assumed it was open and tried to connect. It was highlighted that any anomalous activity generated from offensive techniques, while on the target network, heightened the chance of discovery and so every precaution should be taken to reduce that risk.

"... the big cost is that every time you are doing something you are potentially drawing attention to yourself and you are increasing the risk of discovery."

Participants suggested that increased time in extra steps was also due to increased time needed to understand the risk of discovery; therefore Time was a cost factor of note. One participant mentioned that a less mature adversary, with less time invested in experience, would be less cautious and could be discovered on the network.

In addition to reducing risk, it was said that there was a further time investment in experience to understand the necessary routing techniques to pivot onto the internal network from the compromised perimeter machine.

"With routing traffic through that second interface, I think that as soon as you add that step in, there is a greatly increased cost in terms of experience and knowledge to be able to pull the attack off... "

When asked about the possibility of using other Techniques within the Lateral Movement Tactic, only financial cost was offered as an alternative, although other costs may be altered in value if alternative Techniques were used. This Finance cost factor would be incurred in the event an adversary decided to extract password hashes from the machine they had compromised and were attempting to crack these offline. This example would require the adversary to either rent relatively powerful server space, or buy their own and pay for the electricity to run it.

"... if you have obtained hashes and are then trying to crack the hashes, potentially there are some significant costs there in terms of computing recourses... if they are using a kind of cloud based solution to do it then it could be monetary costs."

5.3.5. *Post-scenario questions*

When asked about performing alternative or additional Tactics from the ATT&CK framework, no novel cost factors were provided by participants. As with the answers given regarding alternative Techniques during each Tactic, differing amounts of cost would be incurred to undertake additional Tactics, but no new cost factors. For example, it was suggested that the natural next step after Initial Access would be persistence. This additional Tactic would require more time invested in gaining experience to complete the Tactic, financial cost for infrastructure to be in place, and an increased risk as additional actions were taken. Out of these increased costs, the primary concern to participants was risk.

"The cost of persistence is the increased cost of being detected over time. As in, if you persist, the scope for detection is lengthening and therefore the chances of detection will increase over time."

Other than alternative Tactics or Techniques, context also contributes to varying or increased cost. During the post-scenario questions, one participant said that different contexts, such as industrial control systems (ICS) would increase time and financial costs. This ties to our earlier work on the fundamental challenge of process comprehension when targeting such infrastructure (Green et al., 2017). The increased cost would be due to first acquiring the necessary, physical hardware, and second spending the time to practise or even develop exploits for it.

"If you talk about things like Stuxnet, then unless you have details on the centrifuges, you've got no chance. You need to somehow acquire that. And the acquisition of that might be that the cost is too high."

When asked whether cyber security controls would increase an adversary's cost, participants unanimously answered yes. Dependent on the Tactic and underlying Technique being perpetrated, and the controls in place against them, various cost factors would be increased and in varying amounts. A common reason for increasing costs was that, as more controls are put in place, the risk of being detected also increases, therefore participants would spend more time and finance costs to mitigate that risk.

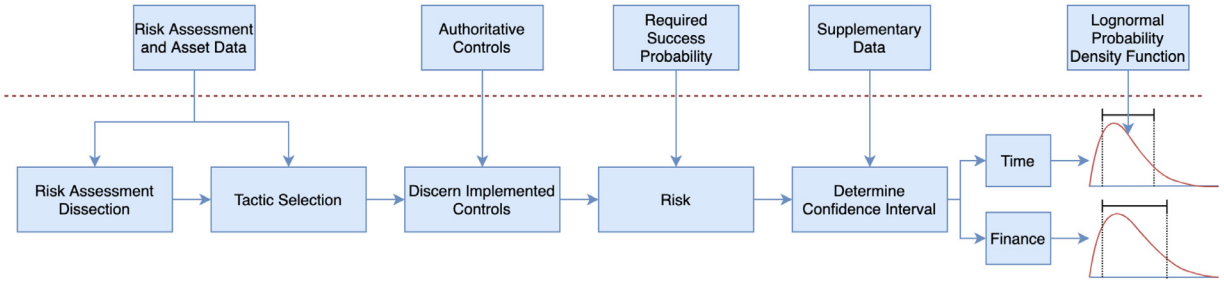

Fig. 5 – Proposed framework of adversary cost

"This really is where defence and depth comes into play. It requires more of me as an attacker in my knowledge but also increases the amount of time that it takes me to do what I need to do. Therefore does that time also equate to the ability for me to be discovered?"

5.3.6. *Summary*

The purpose of this study was to ascertain what experienced, senior offensive cyber security professionals thought their factors of cost would be, should they perform an attack as a legitimate, black-hat adversary. From this, three factors were established, as in Section 5.1, namely *Time, Finance*, and *Risk*.

The primary cost factor identified by the participants was Time, of which the first component is time spent preparing for, and performing, the attack. The other, much more substantial component, is the adversary's time spent gaining the necessary knowledge and experience, in a multitude of areas, to successfully complete the attack. All participants acknowledged the time cost in gaining prerequisite experience, meaning that adversary cost was regarded as threat actor agnostic, rather than being defined by adversaries that would already have gained the experience in advance.

Finance was less prominent than Time as a cost factor. However, certain Tactics and Techniques required money to be spent to be conducted effectively. Moreover, participants suggested that some methods which an adversary would use could demand financial investment, such as the purchase or rental of infrastructure.

While the Risk of failure when performing an attack was considered a cost factor, it serves as a function to manipulate the Time and Finance cost factors, rather than being a tangible metric itself. Every Tactic or Technique performed carries its own inherent risk of negative consequences such as failure or detection, as perceived by the adversary. Therefore, the participants felt that their risk aversion would be the prime delineator of time and financial investment, or whether they even conducted the attack. If a particular Tactic or Technique carried a large amount of risk, participants said they would either find an alternative method, or spend more time or money to reduce their risk exposure.

With the offensive and defensive structures of adversary cost established in Section 4, and the adversary cost factors in the present section, a framework to anticipate it can now be built.

6. A framework for adversary cost

This section introduces the framework proposed to anticipate an adversary's cost, as illustrated in Fig. 5. Each step, and its constituent inputs, is first described in terms of motivation and mechanics. After this, an example application of the framework is proposed using data inspired by a cyber risk assessment of a European utility company during our previous work (Busby et al., 2017). It is important to note that the adversary cost framework is supplementary to a cyber risk assessment, meaning it is conducted as a proactive component of a cyber security strategy, and not conducted mid-incident.

6.1. *The proposed framework for adversary cost*

It is necessary to understand each step of the framework in order, and what input data is required. The descriptions here are in the order in which the steps would be carried out, therefore traversing left to right of the framework's depiction in Fig. 5.

6.1.1. *Risk assessment dissection*

The adversary cost framework is intended to be supplementary to existing cyber risk assessment methods, rather than competing with them. Therefore, it commences subsequent to an existing cyber risk assessment, using all the data to deduce risks and the results from it where possible. Asset and correlating vulnerability information is the predominant requirement, which is used to build up attack narratives that adversaries would likely carry out. Further information on the security posture of the organisation under consideration is necessary, such as any security policy information, patching regimes, and personnel security awareness training. This is used as an evidence base to more accurately determine the upper and lower bounds of cost.

6.1.2. *Tactic selection*

Once the prerequisite information has been gathered, the attack narrative is then broken down into individual Tactics, as described in the ATT&CK framework (see Section 4.1). This could be displayed as an attack graph or perhaps labelled actions on a network graph. From here the adversary cost is split into each individual Tactic and worked out separately.

6.1.3. *Discern implemented controls*

The controls implemented by the organisation under consideration are established for the current Tactic. These are then

categorised within the authoritative controls provided as per Section 4.2. This includes active measures such as a firewall, and endpoint detection and response, as well as more passive measures such as employee awareness training. Consulting with the authoritative controls ensures that no implemented controls are overlooked.

6.1.4. *Risk*

As discovered in the practical interviews in Section 5.3, perceived risk during the attack was established as a key adversary cost factor. In the framework, the Risk cost factor is delineated as the adversary's risk aversion, meaning their unwillingness to accept perceived risk of potential negative outcomes such as the attack failing or being detected, being caught, and the potential negative impacts subsequent to being caught. Rather than a direct cost, Risk is used as a modifier, by leveraging any prior threat intelligence to estimate the minimum accepted chance of successfully executing the tactic without being detected, for the adversary. If an adversary is known to be particularly risk hungry, they would spend less of their resources navigating the cyber security controls implemented within the system under consideration. However, because adversary risk aversion is not a factor which the end user of the framework may have capability to establish, it is optional.

6.1.5. *Determine confidence interval*

Once all of the information has been gathered regarding the Tactic, the cyber risk assessor should determine with what confidence level they can reliably estimate upper and lower bounds of costs. It is recommended the confidence interval is allocated in multiples of 10% (e.g. 10%, 20%,... 90%). If the they believe they can estimate the costs to a reasonable accuracy, for example, they might decide that their upper and lower bounds are to a 90% confidence interval. However, if they deem that some of the data gathered from the prior risk assessment is weak, or there are unusual technologies in place, they may decide to determine their confidence interval is only 50%.

6.1.6. *Time and finance*

The confidence interval determined in the prior step now needs an upper and lower bound of costs for both Time and Finance. The framework is intended to be adversary agnostic for time and financial costs, meaning it is recommended that any prerequisite experience or equipment should be accounted for. If the end users have their own threat intelligence capability or are working with threat actor categories, these can be used to substitute estimated prior experience and financial spending, contributing to the upper and lower bounds.

Time and Finance costs are derived by decomposing what the adversary may be required to spend to complete the Tactic. Each decomposed item should also be provided with a likely upper and lower bound. If the adversary's risk aversion has been defined, as in Section 6.1.4, this should be taken into consideration. Incorporating the adversary's risk aversion would typically reduce the upper and lower bounds as, by default, the framework assumes they would accept no less than their perceived 100% chance of not being detected.

When considering time, end users should be mindful of:

- General information technology (IT) knowledge and experience
- Offensive security knowledge and experience
- Time to gather relevant information using reconnaissance and enumeration techniques
- Time to complete the Tactic

Once decomposed into its constituent parts, time is more tangible for an expert end user to provide figures for. If there is any doubt with regard to the time spent to gain knowledge and experience, consulting trajectories through white-hat (ethical hacker) certification schemes (e.g. OSCP (Offensive Security, 2020)) and their likely required investment is a suitable solution.

When considering finance, end users should consider:

- Hardware necessary to complete the attack
- Any hosting for Tactics/Techniques such as command and control (C2), procured legitimately or otherwise
- Tools, n-day (novel proof of concept for known vulnerability), or 0-day exploit code

It is important to note that an adversary may choose to spend more time on an attack in exchange for a lower financial cost, or vice versa. As an example, an adversary may decide to spend time developing a proof of concept exploit, or they may instead decide to externally source it and incur financial cost. It is up to the end user's discretion as to whether they think the adversary would be more likely to invest Time or Finance in performing an attack.

Once all of the decomposed items for time and finance have been given upper and lower bounds they are then aggregated, such that Time and Finance both have an overall upper and lower bound.

6.1.7. *Lognormal distributions*

The framework uses lognormal distributions to depict adversary cost. This acts as both a visual aid and a guide to probable Time and Finance costs experienced by the adversary, given the bounds and confidence interval. The decision for this was based on the following factors. The distributions allow an end user to input an upper and lower bound based on their expert opinion, something deemed valuable by participants in Section 5.3, and define how confident they are in their inputs. The end user bases their expert opinion on known data, derived from a prior cyber risk assessment method, which supplements existing approaches rather than requiring a new approach or additional data, and minimises estimations found commonly throughout Section 2. The outputs of the distributions provide visual representations of adversary cost which are simplistic in nature and easy to understand, consistent with findings in Section 3.2. Finally, the distributions are lognormal, which prevent any negative values and taper off towards higher values, something to be expected with the cost of cyber attacks due to always costing positive values and possible extensive, high-expense engagements.

To plot the lognormal distributions, the upper and lower bounds for Time and Finance, and the confidence interval are

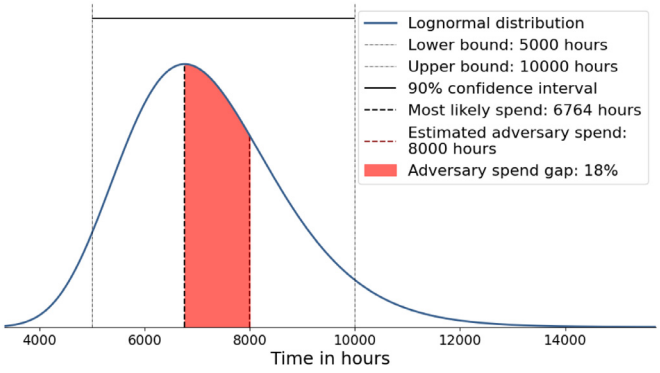

Fig. 6 – Example of lognormal distribution curve with estimated adversary spend.

applied to the lognormal probability density function:

$$f(x) = \frac{1}{\sigma\sqrt{2\pi}} \exp\left[-\frac{(\ln x - \mu)^2}{2\sigma^2}\right], \quad x > 0$$

where:

- x = values of Time or Finance above 0
- μ = the mean of the natural logarithms of the upper and lower bounds
- σ = the standard deviation of the natural logarithms of the upper and lower bounds

The lognormal distribution curve provides a visual prompt for the risk recipients, and the mode of the distribution ($e^{\mu-\sigma^2}$) can be derived as the adversary's most likely spend for the tactic, symbolised by the curve's peak. This can be seen, depicted with an example curve for the Time factor, in Fig. 6, which uses the upper and lower bounds of 10000 and 5000 respectively, and a confidence interval of 90%. The most likely spend is identified as 6764 hours, within the confidence interval.

The lognormal distribution curves and most likely spends generated by the adversary cost framework are not to be interpreted as exact, but as a representation of adversary cost as anticipated by the framework user, in order to reduce uncertainty. Similar approaches have been used in other quantitative risk assessment methodologies such as the one described by Hubbard and Seiersen (2016).

6.1.8. *Optional: Use of prior adversary data*

If the end user has prior threat intelligence capability, and can estimate what costs an adversary accepted for a previous attack, this can be used to extract further value from the framework. The adversary's estimated previous spend can be compared against the most likely spend on the distribution to easily depict whether this Tactic is within their known limits. An example of this can also be seen in Fig. 6 with the estimated adversary spend of 8000 hours, depicted by the area under the curve highlighted in red. This shows that the estimated adversary spend is 18% higher than (or 118% of) the most likely spend, indicating the adversary would be willing to spend more than the most likely Time required to complete the Tactic. If the estimated adversary spend is lower than the most likely spend, the area under the curve would be highlighted in green. The red and green highlights further reinforce the visual representation which was said to be effective for risk recipients, particularly at a management level, in Section 3.2.

Including adversary spend can be used to compare current controls against the adversary, but perhaps more crucially, it can be used to project whether implementing further controls would encourage the most likely required spend to exceed prior adversary spend.

6.2. *Example application of the framework*

It is imperative that the proposed framework performs effectively when provided with real world cyber risk assessment data. The example given is a vulnerability, inspired by our previous work (Busby et al., 2017), during a cyber risk assessment of a small European utility provider. Due to its sensitive nature, detailed information of the provider, its infrastructure, and vulnerabilities involved, is obfuscated. For brevity's sake, the example considers just one Tactic from the ATT&CK framework, which will be Initial Access as it has been covered in Sections 4 and 5.

6.2.1. *Risk assessment dissection*

During the cyber risk assessment, an unpatched Internet-facing service was discovered in which, for the version running at the time, a vulnerability could allow a malicious actor to bypass its authentication. There was no public proof of concept code to exploit the vulnerability. However, if an adversary were to exploit it, they would gain remote code execution within the provider's network.

6.2.2. *Tactic selection*

An adversary exploiting this vulnerability would be breaching the perimeter of the utility provider, therefore it would be considered as Exploit Public-Facing Application within the Initial Access Tactic in the ATT&CK framework.

6.2.3. *Discern implemented controls*

Using the authoritative controls list from Section 4.2, the controls to be mindful of fall under the categories: AC-2 Account Management, AC-6 Least Privilege, RA-5 Vulnerability Scanning, SA-8 Security Engineering Principles, SC-2 Application

Partitioning, SC-7 Boundary Protection, SI-2 Flaw Remediation, and SI-4 Information System Monitoring. However, there were no controls put in place by the utility provider for this vulnerable service, which means the attack could go ahead without too much concern about detective or preventive measures.

6.2.4. *Risk*

With the system under consideration belonging to a utility provider, and including some reasonable assumptions regarding threat intelligence, it was decided that nation-state actors would be a likely adversary encountered in this attack narrative. For this reason, we decided to assume that the adversary's minimum accepted chance of successfully carrying out the tactic and navigating the security controls was 90%. This would not affect the cost very much as, assuming the adversary had done prior reconnaissance, they would know that it was unlikely any detective or mitigation controls were in place. However, with the necessity to write proof of concept exploit code to leverage this vulnerability, there is an element of risk as to whether the service could crash on launching the exploit.

6.2.5. *Determine confidence interval*

The cyber risk assessment performed was particularly thorough, meaning that the data gathered is most likely to be comprehensive without any asset data or security controls missing. Moreover, the service in question is not unusual, and the vulnerability in it is also particularly common and not likely to require an abstract or particularly expert skillset. Because of the above two points and our confidence in understanding the processes of performing the attack, we can anticipate the upper and lower bounds of time and finance with a 90% confidence interval.

6.2.6. *Time and finance*

The assumption is made that a nation-state adversary would use their experience and spend time to develop the proof of concept exploit internally, rather than spend finance, sourcing exploit code from an external party and risk revealing any intentions. Therefore, the decompositions of Time and Finance consist of:

Time:

- Gaining general IT experience (ITE)
- Gaining general offensive security experience (OSE)
- Conducting necessary reconnaissance and enumeration for the Tactic (RaE)
- Gaining specific exploit development experience (ExE)
- Writing and testing the exploit (ExW)
- Setting up and configuring C2 infrastructure (C2T)

Finance:

- Purchasing necessary local infrastructure (LI)
- Purchasing tool and vulnerable service licenses (TL)
- Purchasing or renting equipment for C2 infrastructure (C2F)

Each of the individual items in the decomposition is given an upper and lower bound, which are then amalgamated to provide a total upper and lower bound for the Time and Finance cost factors. This can be seen in Tables 4 and 5.

Table 4 – Time (hours).

Cost	Lower	Upper
ITE	1000	2000
OSE	500	1000
RaE	8	40
ExE	500	1000
ExW	486	1350
C2T	80	400
Total	2574	5790

Table 5 – Finance values (in GBP (£)).

Cost	Lower	Upper
LI	990	2960
TL	450	2100
C2F	200	4000
Total	1640	9060

It is important to reiterate that these values are not just those that the adversary would be spending directly on the attack, but also include prior experience and acquired hardware/software. The prior experience chosen in this example is on top of an assumed knowledge and experience acquired during a typical, 3-year computer science bachelor's degree.

Table 4 shows the upper and lower bounds for the Time factor's decomposition, in hours. The values are based on there being approximately 40 hours in a work-week, and therefore 2000 hours in a work-year. ITE, OSE, and ExE are the three experience-based elements. Through their own experience and qualifications relevant to the required skillsets, the authors anticipate it would take a combined 1–2 years' experience to successfully complete the Tactic described. The qualifications, which the decisions were based on, include those such as Offensive Security (2020) Certified Professional, Certified Expert, and Exploitation Expert (OSCP, OSCE, OSEE), in addition to all of the prerequisite experience. RaE assumed the adversary would already have a reasonable idea of their target and its infrastructure meaning it would take as little as a day and as much as a week to complete, given the designated experience. ExW would be expected to take between 3 and 8 months of work, which is due to the necessity of identifying the known vulnerability's entry point for the exploit, and then bringing it to fruition with practicable stability. C2T can be a time consuming process to establish, including the creation of multiple instances of active and failover (backup) C2, their set up, testing, and running them for a period to ensure the domains are indexed. The values of ExW have also been reduced by 10%, signifying the impact of our adversary accepting a 10% chance of unsuccessfully completing the attack and being detected, the Risk factor's value designated in Section 6.2.4. ITE, OSE, and ExE describe the necessary experience to complete the attack; therefore it is unlikely the adversary would require less and they cannot retroactively spend less time gaining it.

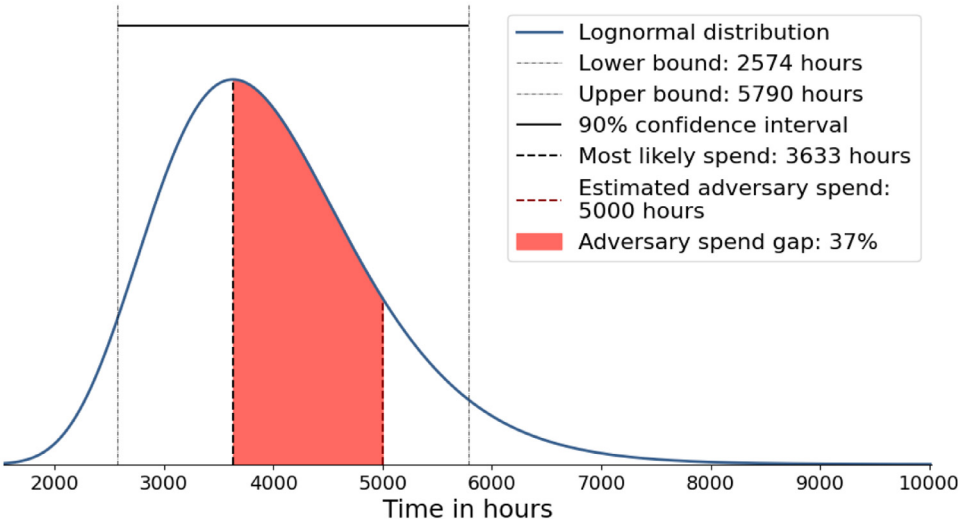

Fig. 7 – Lognormal probability distribution of Time cost factor.

RaE and C2T are standard procedures and would likely be unaffected by the Risk factor.

Table 5 shows the upper and lower bounds for the Finance factor's decomposition, in GBP (£). LI is comprised of two elements, a computer/laptop and an internet connection, with the former being between £600 and £2000 and the latter relating to estimated monthly costs of £30 based on the total estimate of the Time factor (15 to 32 months). TL also has multiple components as the adversary may purchase varied licenses such as operating systems, virtualisation software, disassembling and debugging software, and C2 software. It is expected that the various components for TL would sum between £400 and £2000. C2F's variation between upper and lower bound is due to the fact an adversary may use a cheap and temporary, cloud-hosted solution for their C2, or they may opt to pay for their own, on-premises, server which also would then include more noticeable electricity costs. These two variations reflect the lower bound of £200 and upper bound of £4000.

6.2.7. *Lognormal distributions*

The upper and lower bounds of the Time and Finance cost factors can then be applied to the lognormal probability density function. The resulting probability distributions can be seen in Figs. 7 and 8. The modes of these distributions, or the most likely spend, are calculated as 3633 hours (approximately 22 months) and £2942 for the Time and Finance factors, respectively. This is calculated based on the upper and lower bounds, and confidence interval as described in the formula in Section 6.1.7.

The cyber risk assessment and the data being used did not require a significant threat intelligence component, and therefore the data to anticipate a likely adversary spend is weak. However, estimates are made for the purpose of demonstrating the framework.

Fig. 7 contains an estimated likely adversary spend of 5000 hours, or 2.5 years. This likely adversary spend is based on the fact that the utility provider is a small organisation. Because of this, any impact of an attack would be comparatively small in relation to a large nationwide utility provider, thus the strategic importance would also be low. Therefore, the estimated adversary spend accounts for a junior operative's experience and 6 months worth of work on writing and deploying the exploit. It can be seen, from the red highlighted area under the curve, that this is greater than the most likely spend by 37%, meaning it is estimated that the adversary would be prepared to spend 37% more time on this Tactic than is most likely required.

Similarly, Fig. 8 contains an estimated likely adversary spend of £6300. This accounts for a laptop and other hardware costing £1200, an Internet connection across the 2.5 years of experience and execution of the Tactic costing £900, tools and licenses costing £1200, and a small server and electricity for C2 infrastructure costing £3000. Again, the red highlighted area under the curve shows the estimated likely adversary spend as higher than the most likely spend. More specifically, it shows that the adversary would be prepared to spend 114% more than is required by the most likely spend, in order to achieve the designated 90% perceived chance of remaining undetected while the Tactic is carried out.

Both of the Time and Finance factors show that the adversary would be prepared to spend more than is required, from the estimations made. This would be considered a negative outcome, and therefore there is a risk of attack from the adversary in question. However, if the utility provider were to put a control in place to mitigate the vulnerability within the Internet facing service, the cost to the adversary could be increased past the estimated adversary spend. The intention would be to increase the attack cost to the adversary such that it would outweigh the strategic value in carrying it out. For example, if the utility provider implemented a regular patching regime (SI-2: Flaw Remediation in the authoritative controls) and therefore patched the Internet facing service such that no vulnerability were present, the Time and Finance costs would be greatly exacerbated for this Tactic, due to the necessity of finding a new, 0-day vulnerability within the service. The additional costs would be accrued due to further necessary experience in vulnerability discovery, time spent identifying the

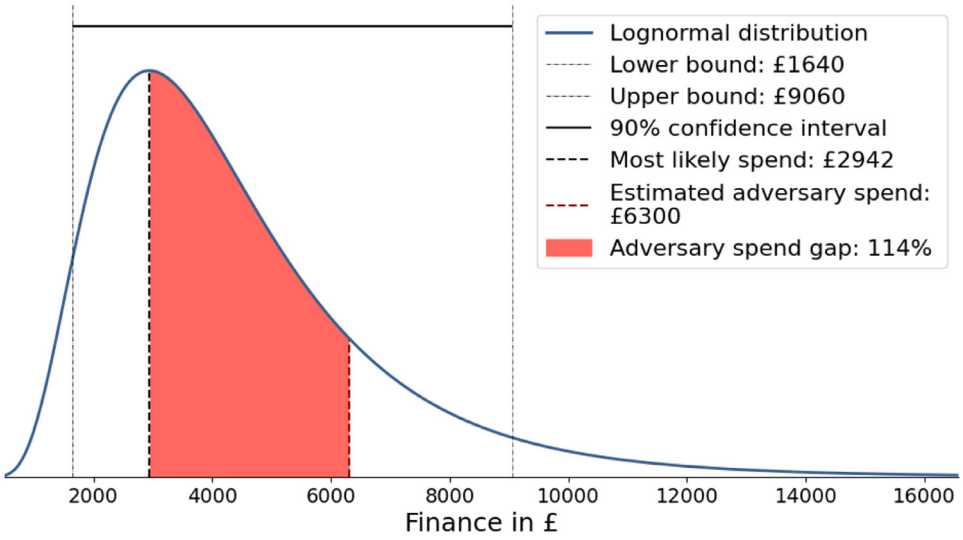

Fig. 8 – Lognormal probability distribution of Finance cost factor.

vulnerability, and purchasing expensive vulnerability discovery tools such as fuzzers.

7. Conclusion and further work

We have identified a gap in the academic and industry literature whereby, in the traditional risk function, $Risk = f(Threat, Vulnerability, Impact)$, the threat was often considered in isolation and with weak data. A possible bridge across the gap, viz. adversary cost, was also identified; however, it had seldom been explored and reported in the literature. Adversary cost was therefore investigated through interviews with cyber risk assessment practitioners, as we have reported in this paper. We aimed to understand areas of a cyber risk assessment including data collection, processing the data, method and challenges of delivery, and whether the notion of adversary cost would be an effective narrative. The gap identified in the literature was clearly present in current practice, and adversary cost was evidently of interest to all interview participants.

The MITRE ATT&CK framework was established as the best foundation on which to build a framework for adversary cost, due to its two appropriate layers of granularity - Tactics and their underlying Techniques. A list of authoritative controls was developed from the detective and mitigation measures discussed within the ATT&CK framework, and aligned with NIST 800-53, also chosen for its appropriate granularity and uniform abstraction. These controls were evaluated in the first stage of a two-stage interview with senior offensive cyber security professionals, to discover whether they were appropriately granular, abstract, and comprehensive. These authoritative controls allow end users to refer back and ensure that they are mindful of all possible cyber security controls implemented in the system under consideration.

The factors of adversary cost were established as *Time*, *Finance*, and *Risk*. Time and Finance were first determined by creating a database of historical attacks and extracting each action taken by the adversary as a fragment aligned to the ATT&CK framework. These were then given their own expected factors of cost by the research team. To further solidify these factors, the second stage of the two-stage interviews involved an ethnographic approach which entailed the participants completing a practical scenario exercise, demonstrating offensive security techniques. While completing the scenario, participants were asked to describe what costs they may experience should they be a real black-hat adversary in a live environment. The participants unanimously concluded that the adversary cost factors were indeed Time, Finance, and Risk. However, the Risk element, which was identified in the interview stage, was seen as a function to modulate the Time and Finance cost factors rather than being a cost in itself. This means a risk-averse adversary would spend more Time and Finance in performing the attack to lower their risk, or may actually be deterred if they cannot afford to lower their risk appropriately, or if the risk element cannot be reduced.

Finally, a framework for anticipating an adversary's cost was proposed; this takes data from existing cyber risk assessments and complements their results, rather than competing with them as another risk assessment methodology. The framework follows attack narratives through the system under consideration, breaking them into Tactics aligned to the ATT&CK framework, and considering the currently implemented cyber security controls for each Tactic. Threat intelligence sources can be used to estimate the adversary's risk aversion, the maximum accepted risk of negative consequences such as being detected, or failing the attack, which functions as the Risk cost factor. The end users can then define their confidence level in anticipating any costs using the data with which they have been presented. The two other cost factors, Time and Finance, are then decomposed, the individual components of which are given an upper and lower bound based on the end users' confidence interval and the estimated Risk cost factor. Once all cost components have been given an upper and lower bound, both factors are aggregated such that each has its own total upper and lower bound. The Time and

Finance cost factors' total upper and lower bounds are applied to the lognormal probability density function to provide each factor with a lognormal probability distribution. The peak of each distribution, its mode, is determined as the adversary's most likely spend to complete the Tactic. Any threat intelligence may be used to determine the adversary's likely willingness to spend on the Tactic, which can then be compared visibly on the probability distribution, against the most likely spend.

The framework uses data and experience which is known to the end user, removing the required speculation of threats common with current cyber risk assessment methodologies. This effectively bridges the gap between the isolated *threat*, with weak data, and the *vulnerability* and *impact*, with good data. Furthermore, the identified difficulty of communicating cyber risk to senior management is mitigated by changing the form of language from cyber security outputs, such as risk matrices, to time and finance.

7.1. *Further work*

While the framework functions appropriately for the intended goals, it is not without its limitations while in its current, developing, state. There are two prominent aspects which would be of benefit in further work.

First, in its present state, the framework is reliant on end user experience. End users may use this flexibility to their advantage and be pragmatic in their assessments, basing their costs on known data from the system under consideration, which is favourable to the more speculative approach of current threat assessment methods. However, this can also lead to the fluctuation of results, depending on who is performing the adversary cost assessment. To mitigate this problem, further work should develop supplementary data for the assessor, informing them of likely costs and the effects of controls; the latter would complement and extend the authoritative controls that we established in Section 4.2. Additionally, to assist in estimating upper and lower bounds, a calibration method needs to be created, inspired by Hubbard and Seiersen (2016).

Second, Tactics are considered as separate compartments within the attack narrative, with their own most likely cost per Time and Finance. Further work should create an encompassing step in the framework, to amalgamate all costs accurately, providing full Time and Finance costs for the overall attack narrative.

Once the adversary cost framework is equipped with sufficient guidance to be easily adopted and used, it needs to be thoroughly evaluated by industry practitioners – first within a strictly controlled environment (Green et al., 2020) and then against real-world cyber risk assessment data.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

CRediT authorship contribution statement

Richard Derbyshire: Conceptualization, Methodology, Software, Investigation, Data curation, Writing - original draft, Writing - review & editing, Visualization. **Benjamin Green:** Conceptualization, Methodology, Writing - review & editing, Supervision. **David Hutchison:** Writing - review & editing, Supervision, Funding acquisition.

Acknowlgedgments

The research conducted in this paper is part of an industrial CASE PhD studentship provided by the UK Engineering and Physical Sciences Research Council (EPSRC) and by Airbus; we thank both for their ongoing support.

REFERENCES

Aksu MU, Dilek MH, Tatli EI, Bicakci K, Dirik HI, Demirezen MU, Aykir T. A quantitative CVSS-based cyber security risk assessment methodology for IT systems. Proceedings - International Carnahan Conference on Security Technology 2017;2017-Octob:1–8. doi:10.1109/CCST.2017.8167819.

Alhomidi M, Reed M. Attack graph-Based risk assessment and optimisation approach. International Journal of Network Security & Its Applications 2014;6(3):31–43. doi:10.5121/ijnsa.2014.6303.

Arksey H, Knight PT. Interviewing for social scientists: An introductory resource with examples. Sage; 1999.

Arnold F, Pieters W, Stoelinga M. Quantitative Penetration Testing with Item Response Theory. In: 2013 9th International Conference on Information Assurance and Security (IAS). IEEE; 2013. p. 49–54.

Banks DL, Rios J, Insua DR. Adversarial risk analysis; 2015. doi:10.1201/b18653.

Barnum S. Common attack pattern enumeration and classification (CAPEC) schema description; 2008. p. 1–20. http://capec.mitre.org/documents

BSI. Risk Management - Risk Assessment Techniques; 2010.

BSI. Information Technology ' Security Techniques ' Information Security Risk Management; 2011.

BSI. BSI Standards Publication Information Technology ' Security Techniques Code of Practice for Personally Identifiable Information Protection; 2013.

BSI. Information Technology - Security Techniques - Information Security Management Systems; 2015.

Busby J S, Green B, Hutchison D. Analysis of Affordance, Time, and Adaptation in the Assessment of Industrial Control System Cybersecurity Risk. Risk Analysis 2017.

Campbell DT. Experimental and quasi-experimental designs for research on teaching. Handbook of research on teaching 1963;5:171–246.

Derbyshire R, Green B, Prince D, Mauthe A, Hutchison D. An Analysis of Cyber Security Attack Taxonomies, 2018.

Dillon S, Davis D, Group E, Brokers S, thelightcosine. MS17-101 EternalBlue SMB Remote Windows Kernel Pool Corruption; 2019. https://www.rapid7.com/db/modules/exploit/windows/smb/ms17_010_eternalblue. Accessed: 2020-05-29

Dillon S, Jennings L. MS17-101 SMB RCE Detection; 2019. https://www.rapid7.com/db/modules/auxiliary/scanner/smb/smb_ms17_010. Accessed: 2020-05-29

Farwell JP, Rohozinski R. Stuxnet and the future of cyber war. Survival (Lond) 2011;53(1):23–40.

FIRST. Common Vulnerability Scoring System v3.0: Specification Document. Forum of Incident Response and Security Teams (FIRST) 2015:1–21. Accessed: 2020-05-29
Freund J, Jones J. Measuring and managing information risk: A FAIR approach; 2015.
Frey JH. Survey research by telephone. SAGE Publications; 1983.
Ganga D, Scott S. Cultural "Insiders" and the Issue of Positionality in Qualitative Migration Research: Moving "Across" and Moving "Along" Researcher-Participant Divides, 7; 2006.
Glaser B, Strauss A. Grounded theory: the discovery of grounded theory. Sociology the journal of the British sociological association 1967;12(1):27–49.
Gouglidis A, König S, Green B, Rossegger K, Hutchison D. Protecting Water Utility Networks from Advanced Persistent Threats: A Case Study. Springer International Publishing; 2018. p. 313–33.
Green B, Derbyshire R, Knowles W, Boorman J, Ciholas P, Prince D, Hutchison D. ICS Testbed Tetris: Practical Building Blocks Towards a Cyber Security Resource. 13th USENIX Workshop on Cyber Security Experimentation and Test (CSET 20) 2020.
Green B, Krotofil M, Abbasi A. On the Significance of Process Comprehension for Conducting Targeted ICS Attacks. Proceedings of the 2017 Workshop on Cyber-Physical Systems Security and PrivaCy 2017:57–67.
Green B, Prince D, Busby J S, Hutchison D. "How Long is a Piece of String": Defining Key Phases and Observed Challenges within ICS Risk Assessment. Proceedings of the 2017 Workshop on Cyber-Physical Systems Security and PrivaCy - CPS '17 2017. doi:10.1145/3140241.3140251.
Home Office. In: Technical Report. Understanding the costs of cyber crime: A report of key findings from the Costs of Cyber Crime Working Group; 2018. Accessed: 2020-05-29
Hubbard DW, Seiersen R. How to measure anything in cybersecurity risk. John Wiley & Sons; 2016.
Information Security Forum. Information risk assessment methodology 2; 2016. Accessed: 2020-05-29
Insua DR, Vieira AC, Rubio JA, Pieters W, Labunets K, Rasines DG. An Adversarial Risk Analysis Framework for Cybersecurity; 2019. doi:10.1111/risa.13331.
Jones A, Ashenden D. Risk management and computer security. Butterworth-Heinemann; 2005.
King N. Template Analysis.; 1998.
Klinkenberg S, Straatemeier M, van der Maas HL. Computer adaptive practice of maths ability using a new item response model for on the fly ability and difficulty estimation. Computers & Education 2011;57(2):1813–24.
König S, Gouglidis A, Green B, Solar A. Assessing the Impact of Malware Attacks in Utility Networks; 2018. p. 335–51.
Lee RM, Assante JM, Conway T. Analysis of the Cyber Attack on the Ukrainian Power Grid; 2016. https://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf
Lee RM, Assante JM, Conway T. German Steel Mill Cyber Attack; 2016. https://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf
Luszcz J. Apache struts 2: how technical and development gaps caused the equifax breach. Network Security 2018;2018(1):5–8.
Lyon G. Nmap: the Network Mapper; 2019. https://nmap.org/. Accessed: 2020-05-29
McAfee Labs. Don't substitute cvss for risk: Scoring system inflates importance of cve-2017-3735; 2017. https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/dont-substitute-cvss-for-risk-scoring-system-inflates-importance-of-cve-2017-3735/. Accessed: 2020-05-29
McCracken G. The long interview. SAGE Publications; 1988.
McQueen MA, Boyer WF, Flynn MA, Beitel GA. Time-to-Compromise Model for Cyber Risk Reduction Estimation. In: Quality of Protection; 2006. p. 49–64. doi:10.1007/978-0-387-36584-8_5.
Merrick J, Parnell GS. A comparative analysis of PRA and intelligent adversary methods for counterterrorism risk management. Risk Anal. 2011;31(9):1488–510. doi:10.1111/j.1539-6924.2011.01590.x.
MITRE. MITRE ATT&CK deltextsuperscript deltextregistered; 2019. https://attack.mitre.org/. Accessed: 2020-05-29
MITRE. MITRE ATT&CK deltextsuperscript deltextregistered contributions; 2019. https://attack.mitre.org/resources/contribute/. Accessed: 2020-05-29
Muckin M, Fitch SC. A threat-Driven approach to cyber security methodologies, practices and tools to enable a functionally integrated cyber security organization. Lockheed Martin 2017:1–45.
Nakashima E, Timberg C. Nsa officials worried about the day its potent hacking tool would get loose. then it did. Washington Post 2017.
NCSC. Network and information systems directive - objective a; 2018. https://www.ncsc.gov.uk/collection/nis-directive/nis-objective-a. Accessed: 2020-05-29
Nelson N. The Impact of Dragonfly Malware on Industrial Control Systems. SANS Institute InfoSec Reading Room 2016:1–25. Accessed: 2020-05-29
NIST. Guide for conducting risk assessments. NIST Special Publication 2012(September):95. doi:10.6028/NIST.SP.800-30r1.
NIST. In: Technical Report. Security and Privacy Controls for Federal Information Systems and Organizations; 2013. doi:10.6028/NIST.SP.800-53r4.
NIST. Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1; 2018. doi:10.6028/NIST.CSWP.04162018.
Noel S, Jajodia S, Wang L, Singhal A. Measuring security risk of networks using attack graphs. International Journal of Next Generation Computing 2010;1(1):135–47.
Offensive Security. Kali Linux | Penetration Testing and Ethical Hacking Linux Distribution; 2019. https://www.kali.org/. Accessed: 2020-05-29
Offensive Security. Cybersecurity Courses and Certifications | Offensive Security; 2020. https://www.offensive-security.com/courses-and-certifications/. Accessed: 2020-05-29
Pieters W, Davarynejad M. Calculating Adversarial Risk from Attack Trees: Control Strength and Probabilistic Attackers. In: Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance. Springer; 2014. p. 201–215.
Powney J, Watts M. Interviewing in educational research. Routledge; 1987.
Rajbhandari L, Snekkenes E. Utilizing Game Theory for Security Risk Assessment; 2018. p. 3–19.
Rapid7. Metasploit; 2020. https://www.metasploit.com. Accessed: 2020-05-29
Rasch G. Probabilistic models for some intelligence and attainment tests.. ERIC; 1993.
Rosenquist M, Casey T. Prioritizing information security risk with threat agent risk assessment. IT@Intel White Paper 2009(September 2019):8.
Roy A, Kim DS, Trivedi KS. Cyber security analysis using attack countermeasure trees. ACM International Conference Proceeding Series 2010. doi:10.1145/1852666.1852698.
SANS. CIS critical security controls; 2019. https://www.sans.org/critical-security-controls/. Accessed: 2020-05-29
Schneier B. Attack trees. Dr. Dobb's Journal of Software Tools 1999.
Shameli-Sendi A, Aghababaei-Barzegar R, Cheriet M. Taxonomy of information security risk assessment (ISRA). Computers & Security 2016;57:14–30. doi:10.1016/j.cose.2015.11.001.

Smith M, Mulrain G. Equi-Failure: the national security implications of the equifax hack and a critical proposal for reform. J. Nat'l Sec. L. & Pol'y 2017;9:549.
Spradley JP. The ethnographic interview. Waveland Press; 2016.
Such JM, Gouglidis A, Knowles W, Misra G, Rashid A. Information assurance techniques: perceived cost effectiveness. Computers & Security 2016;60:117–33.
TREsPASS. Technology-supported Risk Estimation by Predictive Assessment of Socio-technical Security; 2016. http://www.trespass-project.eu/. Accessed: 2020-07-31
Weber RP. Basic content analyis (first ed.). SAGE Publications; 1985.
Derbyshire, R., 2019. Interview Protocol/Guide. GitHub https://bit.ly/2IIfOEK.

Richard Derbyshire is a PhD student in the School of Computing and Communications at Lancaster University, UK. His research involves both offensive and defensive elements cyber security, with a focus on penetration testing and risk assessment. He is involved in the research project Cyber Security Competence for Research and Innovation (CONCORDIAIA).

Benjamin Green is an Academic Fellow in the School of Computing and Communications at Lancaster University, UK. His research involves both offensive and defensive elements of Industrial Control System security. He is involved in several related research projects, including Operational Technology Management after Cyber Incident (OT-MCI), and Cyber Security Competence for Research and Innovation (CONCORDIA).

David Hutchison is Distinguished Professor of Computing at Lancaster University, UK, and the Founding Director of InfoLab21. His work is well known internationally for contributions in a range of areas including Quality of Service, active and programmable networking, content distribution networks, and testbed activities. His current research focuses on the resilience of networked computer systems, and the protection of critical infrastructures and services.