ISSN: 2182-2069 / E-ISSN: 2182-2077

The Smart Approach to Selecting Good Cyber Security Metrics

Emad Sherif[1*], Dr. Iryna Yevseyeva[2], Dr. Vitor Basto-Fernandes[3], and Allan Cook[4]

[1*]Researcher, Faculty of Computing, Engineering and Media, De Montfort University, Leicester, United Kingdom. p2648946@my365.dmu.ac.uk, https://orcid.org/0000-0002-8450-338X

[2]Associate Professor, Faculty of Computing, Engineering and Media, De Montfort University, Leicester, United Kingdom. iryna@dmu.ac.uk, https://orcid.org/0000-0002-1627-7624

[3]Associate Professor, Instituto Universitário De Lisboa (ISCTE-IUL), University Institute of Lisbon, ISTAR-IUL, Lisboa, Portugal. vitor.basto.fernandes@iscte-iul.pt, https://orcid.org/0000-0003-4269-5114

[4]Professor, Faculty of Computing, Engineering and Media, De Montfort University, Leicester, United Kingdom. allan.cook@dmu.ac.uk, https://orcid.org/0000-0002-0041-3724

Received: July 13, 2024; Revised: August 21, 2024; Accepted: September 24, 2024; Published: November 30, 2024

Abstract

When it comes to the need to manage cyber security, identifying and utilizing good cyber security metrics is essential. This allows organizations to manage their cyber risk more effectively. However, the literature lacks consensus on the properties and characteristics of good metrics. Hence, the objectives of this work are to explore and identify relevant technical metrics proposed by researchers in the cyber security domain, and then to assess them against the SMART (Specific, Measurable, Actionable, Relevant, and Timely) criteria to determine their feasibility and improve the quality of the selected security metrics. We identified 105 metrics, of which 23 passed the SMART criteria. The resulting set of metrics can be considered as a feasible set of metrics to implement. Additionally, we identified additional criteria that may be considered when assessing security metrics, most of which can be regarded as variants of the SMART criteria except two, wherein the metrics should be inexpensive to gather and independently verifiable via an outside reference.

Keywords: Cyber Security Metrics, SMART Criteria, Properties, Attributes, Categorization.

1 Introduction

According to (Pendleton et al., 2016), several organizations have described the process of developing cyber security metrics as one of the hardest problems. The authors add that sound security decisions require detailed information about security metrics. Peter Drucker, the often-cited author of business management approaches, once said “if you can’t measure it, you can’t manage it.” Patrinos, (2014). According to (Boyer & McQueen, 2008), to make sound decisions about protecting our infrastructure, we need effective cyber security metrics. Abraham & Nair, (2015) recommend that to gauge the success of a cyber security programme we need to be able to provide shareholders with measurable solutions to facilitate decision-making. According to metrics can facilitate decision-making and improve

Journal of Interner Services and Information Security (JISIS), volume: 14, number: 4 (November), pp. 312-330
DOI: *10.58346/JISIS.2024.I4.019*

*Corresponding author: Researcher, Faculty of Computing, Engineering and Media, De Montfort University, Leicester, United Kingdom.

performance. Similarly, effective decision-making requires some form of cyber security quantification (Xu, 2021). Therefore, we recognize the need to develop effective and suitable cyber security metrics to help with the decision-making process.

Jafari et al., (2010) propose that cyber security metrics provide insight, and they can be utilized to measure the cyber security posture of an organization. Argue that to objectively evaluate the security of systems we need to devise suitable cyber security metrics. On the other hand, "lack of security metrics exacerbates the challenge of measuring risk objectively" (Knowles et al., 2015). Longueira-Romero et al., (2020) discuss that metrics can be used to provide reproducible and repeatable measures that reflect the security protection level. Hence, metrics can be used not just to evaluate the security level, but also for measuring risk.

According to (Kowalski et al., 2011), organizations should assess their cyber risk before they address security measurement. The authors add that cyber security metrics have not been widely integrated in cyber risk assessment (Eko et al., 2024). This clearly calls for the integration of cyber security metrics within cyber risk management programs. However, organizations need to agree to a definition of cyber security metrics that suit their business first and foremost before they begin selecting their cyber security metrics. "Without a restrictive definition, the term metric degenerates to a buzzword, which can be dangerous in terms of suggested comparability" (Hecker, 2008). Jafari et al., (2010) define a security metric as "a collection of several measurements taken at different points in time, compared against baseline and interpreted to reveal an understanding". Thus, we recognize that the process of developing metrics should begin with a suitable definition for the desired metrics, along with specifying the properties that good metrics should possess (Rjaibi et al., 2012).

Moreover, according to (Pendleton et al., 2016), several organizations in the United States recognize that developing effective and suitable cyber security metrics is a hard problem. The authors add that there is a gap between the existing metrics and the suitable metrics. Geleta, (2018) discusses that security metrics pertain to things that can be evaluated and used to measure the security of an information system, which has emerged as an indispensable difficulty in the field of information systems. According to (Zhao et al., 2019), the collection of detailed cyber security metrics is a very difficult task to accomplish. Charlton et al., (2021) argue that despite the enormous efforts, cyber security metrics remains an open problem.

Furthermore, "there are no direct methods of measuring strength of cyber security" (Bhol et al., 2023). Even though, Xu, (2020) argues that solving the problem of quantifying cyber security would contribute to answering decision-making and risk management related questions. The author adds that to solve such a problem, practitioners need to define a set of cyber security metrics that are effective and suitable to achieve quantitative cyber risk management and thus improve the decision-making process. Charlton et al., (2021) suggest that cyber security metrics research can be categorized as follows: firstly, define the metrics, and then design procedures to measure the well-defined metrics.

Therefore, working with cyber security metrics can help to address the challenge of measuring risk objectively, which in turn can be an invaluable tool for decision-makers. The literature suggests that making sound decisions requires some form of quantification in which cyber security metrics can play an important role in closing this gap (Pragadeswaran et al., 2024). However, one of the key challenges to achieving this is the lack of information regarding what constitutes a good metric. To overcome this challenge, several researchers agree that an effective method to assess the metrics should be discussed

first (Pendleton et al., 2016; Boyer & McQueen, 2008; Xu, 2021; Jafari et al., 2010; Longueira-Romero et al., 2020; Kowalski et al., 2011).

Moreover, according to (Charlton et al., 2021), the top two common criteria found in the literature are the SMART and PRAGMATIC, SMART stands for Specific, Measurable, Attainable, Repeatable, Time-dependent, while PRAGMATIC stands for Predictive, Relevant, Actionable, Genuine, Meaningful, Accurate, Timely, Independent, Cheap. Although, the SMART criteria have been widely used. Even though there is not a universal method, the metrics should be assessed in advance to support an effective decision-making process (Longueira-Romero et al., 2020).

Adopting good cyber security metrics can help businesses improve their cyber security risk management by providing a means that will enable them to measure risks effectively (Simon et al., 2022). Conversely, without objective means or measures, businesses will resort to the assessment of subject matter experts. For instance, Ahmed et al., (2019) discussed the challenges that the healthcare industry faced and proposed groups of metrics to improve the protection of their systems, one of which is the risk assessment metrics group, whereby organizations can monitor their risk (Akinsanya et al., 2020). Jafari et al., (2010) proposed a metric that can be used, within the healthcare industry, to assess the security posture of organizations. Although, the metric is domain specific. Knowles et al., (2015) conducted a survey of cyber security management in industrial control systems and concluded that there is a lack of guidance on how to address the area of quantitative and qualitative cyber security metrics which hinders the efforts to implement proper security in the critical infrastructure industry (Mouatassim & Ibenrissoul, 2015).

Thus, our contributions are as follows:

- We review the literature to identify existing cyber security metrics and their categorizations.
- We provide a tool that can be used to categorize and assess cyber security metrics effectively.

The rest of the paper is organized as follows: in Section two, we highlight the related work on the topic of security metrics. In Section three, we introduce the methodology we used to survey the scholarly knowledge on this topic. This is followed by a discussion where we explain how we identified and assessed the metrics (Panchabhai & Patil, 2012). Finally, in the conclusion section, we summarize the key points of this work, identify limitations, and propose future research directions.

2 Related Work

Definition of Cyber Security Metric

According to (Yevseiev et al., 2022), there is no clear definition for the notion of more secure, and thus cyber security metrics should be leveraged and integrated in the security assessment. Furthermore, according to (Yevseiev et al., 2022), cyber security metrics can be used to provide an up-to-date information regarding the security state of defence and attack sides. The authors add that cyber security metrics allow comparing security systems with each other. Bhol et al., (2023) argue that security metrics can be used to leverage resources and determine whether a security solution has succeeded. The authors add that to respond effectively to the ever-changing cyber threat landscape, the strength of cyber systems needs to be quantified. Moreover, Ahmed et al., (2019) suggest that cyber security metrics can be used to measure the performance of an organization against its peers. However, the authors mention that quantifying the proposed metrics will be addressed in future work. Schneidewind, (2009) developed

risk-based metrics that can detect anomalous behavior to mitigate the effects of attacks on critical infrastructure in the United States. However, developing too many metrics could be expensive to implement and may be too difficult to manage. Additionally, "there are many metrics that may not be directly measurable (e.g., attacker capabilities)" (Xu, 2020). Additionally, Yevseiev et al., (2022) highlight that there is no formal model for metrics, whereby we can conduct a rigorous analysis. Furthermore, Enoch et al., (2018) found that when the number of vulnerabilities become large, the cyber security metrics' values become static. Argue that a static cyber risk management approach may become obsolete very quickly because many parameters used in the analysis constantly change over time.

According to (Pendleton et al., 2016), there is a lack of discussion about how cyber security metrics can be used as parameters in cyber security modelling. Yevseiev et al., (2022) argue that to use cyber security metrics to determine in advance the required preventative measures against cyber threats, organizations need to be able to process and analyze measurements in a way that allow them to extrapolate their values. Furthermore, Xu, (2021) argues that cyber security datasets can be leveraged to define cyber security metrics at the following abstraction levels: data, knowledge, and application. Bhol et al., (2023) point out that cost computation may become too difficult without data driven security metrics and thus decision-making regarding security spending becomes harder. Moreover, Bhol et al., (2023) argue that a metric is usually a product of one or more measures. Hence, Xu, (2021) suggests that a cyber security metric can be a function that maps from a set of objects to a set of values with a scale. Boyer & McQueen, (2008) discuss that a technical security metric is the output of a mathematical model whereby we utilize measurements of a technical object. Moreover, according to (Pfleeger, 2009), measurements have something in common which is an aspect of something that has a descriptor to allow comparison. Similarly, "Metrics are descriptive and measure the current properties and performance of a system" (Scala & Goethals, 2016). Hence, Longueira-Romero et al., (2020) argue that security metrics can be used to compare different evaluations of the same hardware or software over time. The authors add that security metrics can be used to evaluate level of compliance with a standard.

Properties of Good Cyber Security Metrics

Al-Shiha & Alghowinem, (2019) argue that it is important to develop specific cyber security metrics for the purpose of securing systems while conducting penetration testing. Although, the authors have not provided a definition for the desired metrics or what properties such metrics should possess. According to Hecker, (2008), security metrics are classified according to their properties. Thus, choosing the right properties that a metric should possess is as important as developing a definition for the metric. In general, Holstein & Stouffer, (2010) discuss that when it comes to properties of good metrics, we should be able to consistently measure them, collect them by automated means, and express them as percentage or cardinal number. suggest that "values of metrics should be related to the following qualities: efficiency, objectivity, and consistency" (Kowalski et al., 2011).

According to (Geleta, 2018), the attributes of good metrics are as follows: they need to be clear, cheap, and can be collected by automated means, as well as they should be measured objectively. We notice that the authors stress the importance of being able to systematically measure metrics and to not rely on subjective criteria. However, in the context of security metrics, Boyer & McQueen, (2008) discuss that the attributes of technical security metrics are that the number needs to be small so that they can be managed effectively, they need to be easy to understand, and they need to be measured objectively. According to (Abercrombie et al., 2013), good metrics should be able to measure properties for decision-making, be measured in a repeatable manner, and be verifiable independently. Moreover, Pendleton et al., (2016); Boyer & McQueen, (2008); Abercrombie et al., (2013) proposed a set of

common metrics which are easy to understand, measured objectively, and verifiable via an outside reference.

Furthermore, Xu, (2020) calls for establishing a set of criteria that can distinguish between good and poor metrics because "good metrics lead to good decisions and bad metrics lead to bad decisions" (Boyer & McQueen, 2008). Moreover, Longueira-Romero et al., (2020) argue that several security metrics proposed in the literature lack adequate description. Therefore, further research is required to avoid developing poor metrics unnecessarily. Moreover, according to (Boyer & McQueen, 2008), the ultimate goal of utilizing cyber security metrics is to support the quantification of cyber risk. The authors proposed a set of metrics with the aim of providing objective measures of cyber risk that will help decision-makers to make better decisions which will reduce the cyber risk of attacks on control systems. LeMay et al., (2011) proposed a method that can be used to provide model-based security metrics, whereby the steps of an attacker are categorized in an attack execution graph and the attack objectives are captured within an attacker's profile. Chen et al., (2021) proposed a set of metrics for measuring the operational cost of attackers and defenders as part of a framework designed to quantify the effectiveness of network diversity. Hence, security metrics are useful albeit imperfect (Yağdereli et al., 2015; Domínguez-Dorado et al., 2022).

3 Methodology

To survey the scholarly knowledge on the topic of security metrics, we performed a systematic literature review. We conducted the literature search on the following six academic databases: IEEE Xplore, ACM Digital Library, ScienceDirect, Scopus, SpringerLink, and Semantic Scholar. We used the advanced search feature to facilitate the process. We used double quotation marks to search for the exact phrase (search string). Next, after we had applied the inclusion/exclusion criteria, we then examined the results to remove irrelevant and duplicate sources (Sebastian et al., 2019).

With respect to the inclusion and exclusion criteria, we included studies that primarily discuss cyber security metrics, written in English, and whose type are either journal articles or conference proceedings. While the exclusion criteria include studies that do not specifically address cyber security metrics (including definition, properties, etc.), non-peer reviewed sources, and full text is inaccessible. Table 1 highlights the searches conducted at the beginning of this work. We used three different strings to search for relevant sources in each database. The US literature mainly uses 'cybersecurity' keyword, while in the UK it is generally defined as 'cyber security', in addition to 'systems security metrics' that some researchers use to refer to the field of security metrics (Johnson et al., 2020; Rathod & Hämäläinen, 2017). The search string column is followed by the search engine name. This is followed by the date of the search. This is followed by the number of hits. This is followed by the number of eligible sources after applying the inclusion/exclusion criteria (see Table 1). In the first instance, the total number of hits is 873. After applying the inclusion/exclusion criteria and removing duplicates, 38 articles were included.

Table 1: Highlights of the Searches

Search string	Search engine	Date	Hits	Eligible
cybersecurity metrics	IEEE Xplore	15/01/24	22	4
cyber security metrics	IEEE Xplore	15/01/24	7	1
systems security metrics	IEEE Xplore	15/01/24	6	2
cybersecurity metrics	ACM Digital Library	15/01/24	10	2
cyber security metrics	ACM Digital Library	15/01/24	10	1
systems security metrics	ACM Digital Library	15/01/24	3	1
cybersecurity metrics	ScienceDirect	15/01/24	26	2
cyber security metrics	ScienceDirect	15/01/24	13	1
systems security metrics	ScienceDirect	15/01/24	30	1
cybersecurity metrics	Scopus	12/01/24	153	7
cyber security metrics	Scopus	12/01/24	87	1
systems security metrics	Scopus	12/01/24	233	1
cybersecurity metrics	SpringerLink	15/01/24	71	2
cyber security metrics	SpringerLink	15/01/24	38	1
systems security metrics	SpringerLink	15/01/24	30	2
cybersecurity metrics	Semantic Scholar	16/01/24	46	6
cyber security metrics	Semantic Scholar	16/01/24	34	0
systems security metrics	Semantic Scholar	16/01/24	54	3

In the next section, we discuss how we extracted the required information from the identified sources.

4 Discussion

Information Synthesis

Throughout the review process, we maintained our database in the form of a spreadsheet; the *search highlights* sheet that contains the search strings, search engine, date of search, total hits as well as the count after applying the inclusion and exclusion criteria. The *summaries* sheet contains the following headings: title of study, authors, publication date, summary, conclusion, recommendations, properties of cyber security metrics. This is followed by the proposed cyber security metrics. The *cyber security metrics* sheet contains the following headings: study reference number, publication date and type. This is followed by the proposed cyber security metric. This is followed by category and subcategory. The categories and subcategories are adopted from Pendleton et al., (2016) (see Table 2).

Table 2: Summary of the Main Categories and Subcategories (Pendleton et al., 2016)

Category	Subcategories	Remarks
Vulnerability		pertains to measuring the level of system vulnerability
	User	metrics that can be used to measure users' vulnerabilities
	Interface-induced	metrics that can be used to measure the interface to access a system
	Software	metrics that can be used to measure software vulnerabilities
Defence		aims to measure the strength of cyber defence
	Preventive	metrics that can be used to measure the relative effectiveness against preventing unknown as well as known attacks
	Reactive	metrics that can be used to measure the effectiveness of blacklisting
	Proactive	metrics that can be used to measure the power of attack detection
Attack		aims to measure the strength of cyber attacks
	Zero-day	metrics that can be used to measure how many zero-day attacks were performed within a period
	Botnet	metrics that can be used to measure the size of a botnet
	Malware	metrics that can be used to measure the number of computers infected by a malware
	Evasion techniques	metrics that can be used to measure the evasion capability (e.g., false positive/negative)
Situation		reflects the development of attack-defence interaction
	Security state	metrics that can be used to measure the dynamic security state (e.g., the probability of a compromise at a given time)
	Incidents	metrics that can be used to measure the end points that are compromised at least once within a period
	Investment	metrics that can be used to find out whether the investment pays off or not (e.g., security spending)

In addition to these categories, we have included one more category named *Other*, whereby we list any metrics that do not fall under any of the main four categories. Additionally, to enhance the categorization of metrics, we extended the subcategories to include additional ones that were elicited from the literature. They are as follows: configuration management, access control management, backup and restore, security audit, security testing, and security training, in addition to probability-based, time-based, ideal-based, and design-based metrics. Moreover, according to (Longueira-Romero et al., 2020), the SMART (Specific, Measurable, Actionable, Relevant, and Time-dependent) criteria has been used widely for developing good security metrics. Hence, the SMART assessment sheet contains all the identified cyber security metrics in the previous stage in addition to five columns that represent the SMART criteria so that each metric is assessed accordingly (Baybulatov & Promyslov, 2022). For every article, after we gleaned all the required information to fill in the first sheet, such as summary, conclusion, questions/challenges, limitations/future work, we began with identifying the proposed metrics along with their category/subcategory. Once a metric is identified, we would add it to the cyber security metrics sheet whereby we can keep track of the identified metrics, their designated categories and subcategories along with the reference number of the given article. We repeated this process to gather all the proposed metrics. Next, we copied the identified metrics to the SMART assessment sheet where we carried out the assessment of the metrics; we marked the ones that were able to be assessed against each criterion of the SMART criteria, whereby we were able to create the SMART metrics sheet that contains the final set of metrics. This approach allowed us to gather and keep track of all the relevant information in a way that enabled us not just to get insights into the direction and trends of the research in this area, but also to find gaps in the existing metrics, their properties and classification.

Information Analysis of SMART Metrics

In terms of source types, 70 percent of the selected sources are conference proceedings, of which 13 percent used case study as their method, whereas four percent of the journal articles are survey research papers. We analyzed the selected sources by studying their contribution to security metrics research in two key aspects, one of which is proposal of metrics and/or proposal of properties that a good metric should possess. Moreover, whenever gaps and/or unanswered questions are found, we added them under the problems heading of the relevant sheet. In addition to recommendations for future research directions. The three main headings of the *cyber security metrics* sheet are metrics, categories, and subcategories, which are the main elements of this work. Most of the sources proposed security metrics. Nonetheless, the ones that did not propose any metrics explicitly, they either addressed the definition or properties of metrics. We recorded all the proposed metrics accompanied by their proposed description whenever provided, although some sources did not include a description with their proposed metrics and, hence, we noted them with no description. Therefore, the total number of security metrics identified from the selected sources are 105, all of which fall under five categories and 26 subcategories. While the total number of security metrics after applying the SMART criteria is 23, all of which fall under four categories and 11 subcategories. The statistics of security metrics count can be broken down further, to count how many times a metric is identified (i.e., per source) per category/subcategory as outlined in Table 3.

Table 3: Count of Sources from which Security Metrics were Identified per Category/Subcategory

Category	**Subcategory**	**Count**
System Vulnerabilities	Interface-Induced Vulnerabilities	31
System Vulnerabilities	Software Vulnerabilities	22
System Vulnerabilities	Overall Vulnerabilities	10
System Vulnerabilities	User Vulnerabilities	8
Situation	Security Incidents	47
Situation	Security State	16
Situation	Cost	7
Situation	Resilience Metrics	6
Situation	Agility Metrics	2
Other	Configuration Management	10
Other	Probability-Based Metrics	8
Other	Security Training	6
Other	Time-based Metrics	6
Other	Backup and Restore	5
Other	Access Control Management	4
Other	Compliance	2
Other	Design-based Metrics	1
Other	Ideal-based Metrics	1
Other	Security Audit	1
Other	Security Testing	1

From Table 3, we see that the top count is 47, which denotes to the number of metrics identified under *Security Incidents* subcategory which belongs to *Situation* category. On the other hand, at the bottom of the table, we see that there are four metrics with a single count which are identified under *Design-based Metrics*, *Ideal-based Metrics*, *Security Audit*, and *Security Testing* subcategories respectively.

Table 4 shows the counts of sources accompanied by references per category after applying the criteria.

Table 4: Count of Sources (with references) from which the SMART Security Metrics were Identified

Category	Subcategory	Count	References
System Vulnerabilities	Software Vulnerabilities	7	[3, 5, 7, 13, 25, 32, 39]
System Vulnerabilities	Overall Vulnerabilities	7	[2, 6, 9, 16, 17, 31, 37]
System Vulnerabilities	Interface-Induced Vulnerabilities	6	[7, 11, 16, 32 (x2)]
System Vulnerabilities	User Vulnerabilities	5	[7, 12, 13 (x2), 25]
Defence Power	Intrusion Detection	6	[7, 20, 27, 29, 31, 39]
Defence Power	Proactive Defences Strength	3	[4, 7, 8]
Defence Power	Preventative Defences Strength	1	[39]
Defence Power	Reactive Defences Strength	1	[39]
Situation	Security Incidents	9	[3 (x2), 5, 13, 15, 16, 24, 28, 40]
Other	Configuration Management	6	[7, 13, 17, 22, 24, 27]
Other	Security Training	5	[12, 16, 17, 31, 33]

From Table 4, we see that there are two metrics with a count of 10, which are identified under *Security Incident*s and *Intrusion Detection* which belong to *Situation* and *Defence Power* respectively.

Moreover, to present the data visually, we first imported the two datasets (total cyber security metrics and the SMART security metrics) to Elasticsearch - "the world's leading free and open search and analytics solution" (Elasticsearch, n.d.), and then we used Kibana to create various visualizations, such as data table, tag cloud, pie chart, etc. For instance, we created visualizations for the first dataset to show statistics in relation to the percentage of metrics that fall under each category and subcategory so that we can gain insight into how the metrics are categorized. Additionally, we created multiple visualizations to show security metrics per category. This is useful when we look at the metrics from the categorization perspective. Therefore, we began by creating a tag cloud visualization to show all the metrics (see Figure 1). We see that the largest tag is *vulnerability count* metric which reflects the occurrences. The second largest tags are *attack surface* and *detection performance*, while *mean time between incidents* comes third. Hence, we can see that the other tags look smaller, their size is relative to their count (i.e., how many times a metric is identified).

Figure 1: Summary of the Identified Security Metrics Depicted in a Tag Cloud Visualization

Moreover, we created a visualization for each category that shows all the security metrics and subcategories within each category and then add it to the main dashboard. However, this was not necessary for the *attack/threat severity* category because there is a total of three security metrics identified, all of which did not satisfy the SMART criteria. Hence, since the focus of this work is on the assessed security metrics, we present the visualizations that address the SMART security metrics as outlined below. We begin with the category named '*Other*'. Figure 2 shows a pie chart of the assessed metrics (i.e., assessed against SMART) that fall under this category accompanied by the percentage of how many times a metric was identified out of the total number of the identified metrics within the category. To do this, under slice by, we add the category field first, and then add the subcategory field as a second slice, aggregated by the security metric field. Hence, the inner circle represents the category, the middle circle shows the subcategories, and the outer circle shows the cyber security metrics.

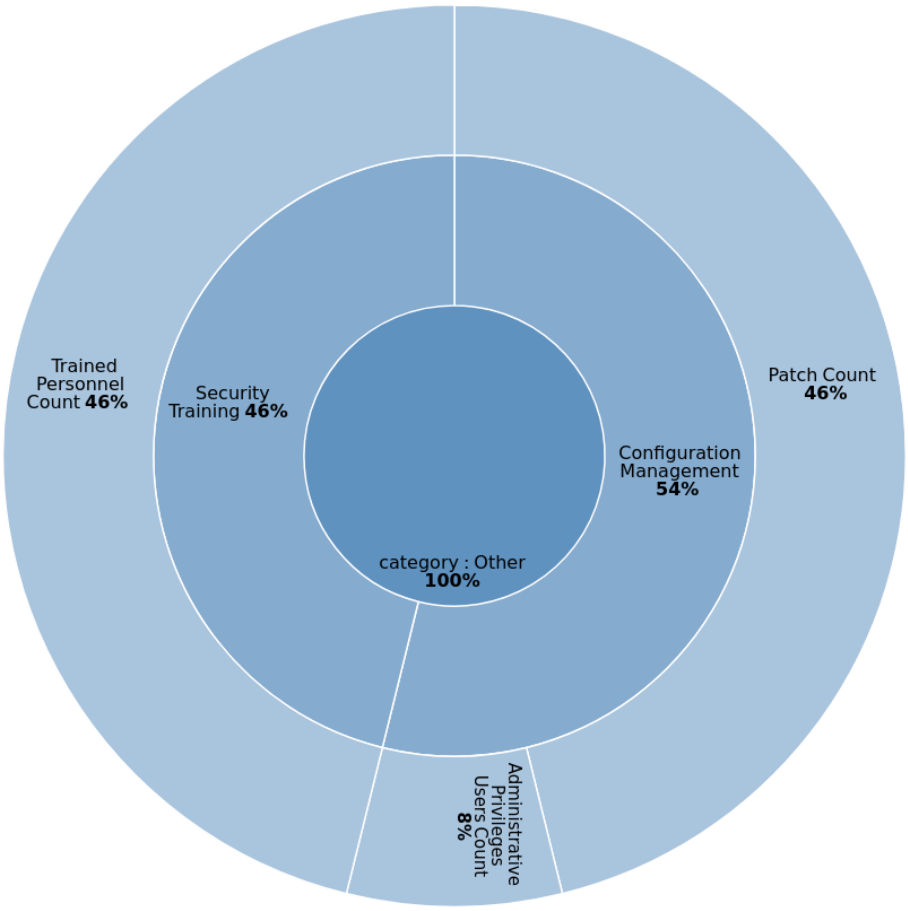

Figure 2: Summary of the SMART Security Metrics within the 'Other' Category

This shows the ranking from the most used to the least used metric within each category. We see that the top security metric in this category is the *trained personnel count*, identified in six sources. Jafari et al., (2010) describe this metric as percentage of IT security staff who have received training.

In Figure 3, we present the SMART metrics that fall under the *Situation* category.

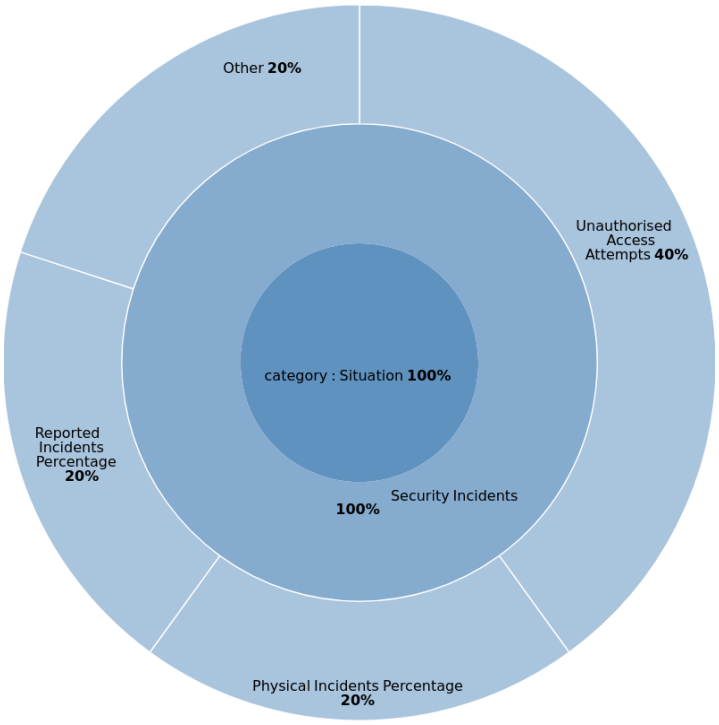

Figure 3: Summary of the SMART Security Metrics within the Situation Category

The top security metric in this category is the *unauthorized access attempts*, identified in four sources. Ahmed et al., (2019) describe this metric as number of failed authentication attempts.

In Figure 4, we present the SMART metrics that fall under the *Defence Power* category.

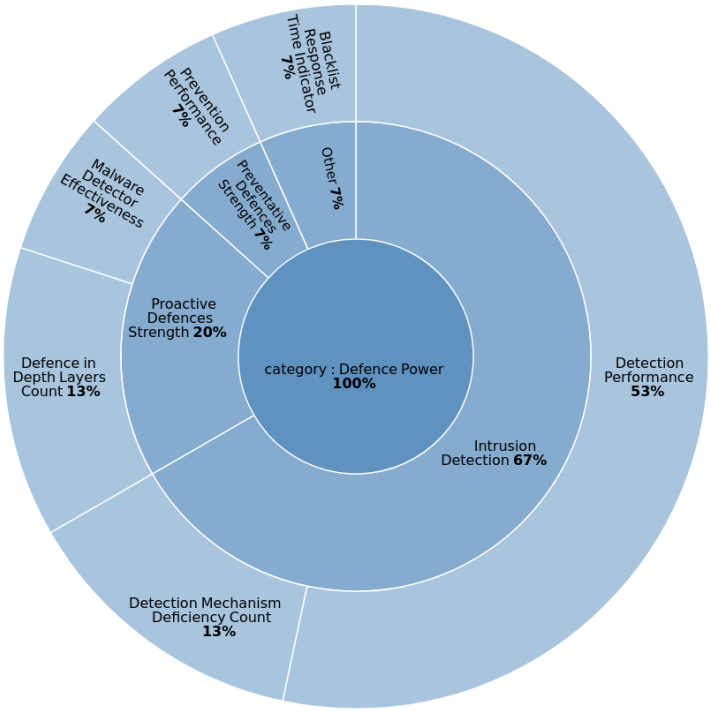

Figure 4: Summary of the SMART Security Metrics within the Defence Power Category

The top security metric in this category is the *detection performance*, identified in eight sources. Boyer & McQueen, (2008) describe this metric as a measure of the effectiveness of the detection systems (intrusion detection system, anti-virus software, etc.).

In Figure 5, we present the SMART metrics under the *System Vulnerabilities* category.

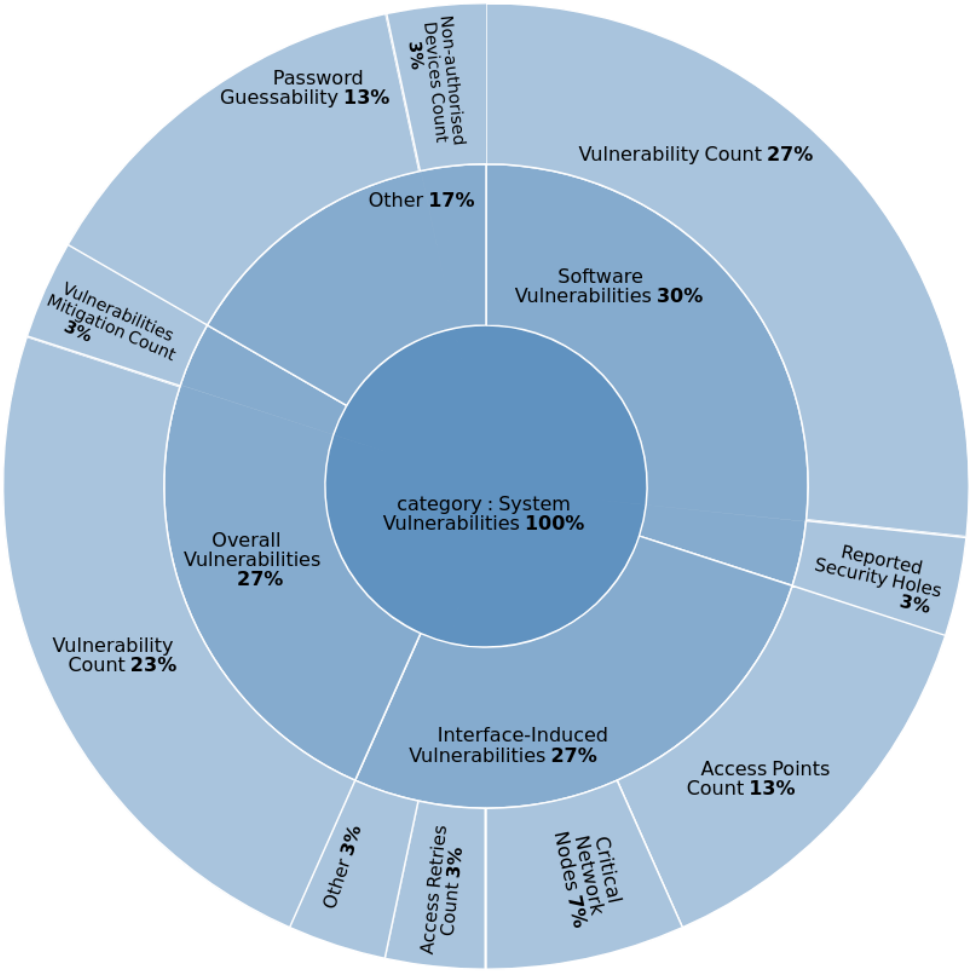

Figure 5: Summary of the SMART Security Metrics within the System Vulnerabilities Category

The top security metric in this category is the *vulnerability count*, identified in 15 sources. Pendleton et al., (2016) describe this metric as the number of systems that haven't been patched yet. The authors add that it normally takes a while for all the required patches to be applied successfully.

Additionally, we created one more visualization, whereby the SMART security metrics can be depicted in one pie chart as shown in Figure 6. The pie chart shows the four categories in the center, subcategories in the middle ring, and the security metrics in the outer ring.

Figure 6: Count of the SMART Security Metrics per Category/Subcategory

In Figure 6, we can see that majority of the identified metrics fall under *system vulnerability* category with 44 percent, 13 percent of which fall under *software vulnerability* subcategory, while 12 percent fall under *interface-induced vulnerability* and *overall vulnerability*, and 7 percent fall under *user vulnerabilities* subcategory. Hence, the top security metric is the *vulnerability count* with 10 percent. Similarly, the second top category is *defence power* with 22 percent that comprises four subcategories *intrusion detection* 15 percent, *proactive defences strength* four percent, and *preventative* and *reactive defences strength* 2 percent each. Hence, the top metric is *detection performance* with 12 percent.

In Table 5, we summarize the security metrics that satisfied the SMART criteria. The first heading contains the metric. This is followed by the category the security metric falls under. In turn, this is followed by the count that contains the number of times a metric was identified from the selected sources. The last column contains the sources from which the metrics were identified.

Table 5: Highlights of the SMART Security Metrics

Metric	Category	Count	References
Vulnerability Count	System Vulnerabilities	12	[2, 3, 5, 6, 7, 9, 13, 17, 25, 31, 37, 39]
Detection Performance	Defence Power	6	[7, 20, 27, 29, 31, 39]
Patch Count	Other	5	[13, 17, 22, 24, 27]
Trained Personnel Count	Other	5	[12, 16, 17, 31, 33]
Password Guessability	System Vulnerabilities	4	[7, 12, 13, 25]
Unauthorised Access Attempts	Situation	4	[3, 5, 13, 28]
Access Points Count	System Vulnerabilities	3	[7, 16, 32]
Defence in Depth Layers Count	Defence Power	2	[4, 7]
Detection Mechanism Deficiency Count	Defence Power	2	[7, 31]
Physical Incidents Percentage	Situation	2	[16, 40]
Reported Incidents Percentage	Situation	2	[16, 24]
Access Retries Count	System Vulnerabilities	1	[15]
Critical Network Nodes	System Vulnerabilities	1	[32]
Administrative Privileges Users Count	Other	1	[7]
Blacklist Response Time Indicator	Defence Power	1	[39]
Events Assignment Delay	Situation	1	[15]
Malware Detector Effectiveness	Defence Power	1	[8]
Non-authorised Devices Count	System Vulnerabilities	1	[13]
Percentage of Severe Systems	System Vulnerabilities	1	[11]
Prevention Performance	Defence Power	1	[39]
Reported Security Holes	System Vulnerabilities	1	[31]
Simultaneous Logins Count	Situation	1	[3]
Vulnerabilities Mitigation Count	System Vulnerabilities	1	[16]

We note that *vulnerability count* metric is categorized under two subcategories *software* and *overall* respectively. This is due to the different description given by the authors from which we identified the metrics. For instance, Boyer & McQueen, (2008) describe vulnerability count as the number of unpatched vulnerabilities, multiplied by their exposure time, which falls under software vulnerability subcategory. While Yağdereli et al., (2015) describe vulnerability count as the number of vulnerabilities present in a system, which falls under *overall vulnerability* subcategory. That is why it is important to develop an appropriate definition or description for the desired metrics right from the start.

To this end, the breakdown of the metrics can be found in (Sherif, 2024). Whereby, the spreadsheet can be used as a tool to categorize and assess metrics effectively. The tool allows organizations to categorize their metrics systematically, and then assess them according to the organization's preferences. For instance, to only list the metrics that are categorized under system vulnerabilities category, click on the arrow next to the category heading. Next, from the drop-down list, untick the box next to select all. Next, tick the box next to system vulnerabilities, and then click on apply button. This will show all the metrics that are categories under the selected category. Similarly, we could follow the same steps to select a subcategory. Moreover, this tool is also useful for those who are just starting to look at their cyber security metrics and do not know yet where to begin. For instance, a practitioner in a small organization may select a small subset of metrics to begin with, and then extend when appropriate.

Additional Attributes of Good Metrics

As discussed, using the SMART criteria should be sufficient for a wide range of uses, shouldn't this be the case, there are additional criteria that can be considered alongside the SMART approach. In this subsection, we discuss a few further characteristics that a good metric should possess.

According to (Hecker, 2008), security metrics are classified according to their properties. The author discusses that security metrics need to be objective and verifiable. Pfleeger, (2009) argues that top level security metrics should be dynamic. Abercrombie et al., (2013) recommend that a good metric should be repeatable and verifiable. Scala & Goethals, (2016) discuss that in addition to repeatable, metrics should be feasible, quantifiable, and objective.

Moreover, Pendleton et al., (2016) agree that metrics should be quantifiable, and they add that metrics should also be easy to understand. Knowles et al., (2015) argue that a good metric needs to be efficient and cost effective. However, Jafari et al., (2010) argue that cost effectiveness is difficult to achieve. According to (Geleta, 2018), in addition to meaningfulness, objectiveness and cost effectiveness, it is important that we should be able to collect metrics by automatic means. Longueira-Romero et al., (2020) recommend that metrics should be comparable and reproducible. Yevseiev et al., (2022) suggest that metrics should be time-bound.

According to (Longueira-Romero et al., 2020), without an assessment method, it is hard to know whether the selected metric is useful or not. The authors argue that since the SMART criteria has been widely used, it can be used to assess good metrics. Holstein & Stouffer, (2010) argue that quantitative metrics should satisfy some criteria that yield in a set of good metrics; some of the elements that can be considered are quantifiable, meaningful, consistent, and collectable by automated means. Savola, (2009) discusses the importance of looking at the feasibility of metrics, in which the SMART criteria can play an important role in assessing good metrics.

Thus, we identified all the relevant properties from the selected sources and then compared them to each element of the SMART criteria (Specific, Measurable, Actionable, Relevant, and Timely). In this way, on one hand, we would verify the elements of the SMART criteria, and on the other hand the criteria can be enhanced by extending it to include properties identified in the literature that might be useful for small organizations when they are looking to assess their metrics (Zieger et al., 2018).

Table 6 summarizes the identified properties, followed by the element of the SMART criteria that can be matched with or equivalent to such a property, followed by some remarks to denote whether a property matches, equivalent to, or can be considered as a variant of one of the five elements of the criteria.

Table 6: Summary of the Properties that a Good Security Metric should Possess

Property	**SMART**	**References**	**Remarks**
Objective	S	[7, 12, 14, 16, 19, 31, 38]	equivalent to *Specific*
Quantifiable	M	[7, 15, 21, 25, 31]	equivalent to *Measurable*
Cost effective	No match	[12, 16, 18, 21]	inexpensive to gather
Repeatable	~M	[1, 21, 31]	considered as a variant of *Measurable*
Reproducible	~M	[16, 21, 38]	considered as a variant of *Measurable*
Verifiable	No match	[1, 14, 16]	independently verifiable via an outside reference
Meaningful	R	[12, 15, 16]	equivalent to *Relevant*
Auto collected	A	[12, 15]	i.e., it can be collected by automated means
Consistent	~T	[15, 19]	considered as a variant of *Timely*
Easy to understand	~S	[7, 25]	considered as a variant of *Specific*
Efficient	~R	[18, 19]	considered as a variant of *Relevant*
Comparable	~S	[21]	considered as a variant of *Specific*
Feasible	A	[23, 31]	equivalent to *Actionable*

Moreover, we see that most of the identified properties are equivalent to an element of the SMART criteria, some of which can be considered as variants. The two unique attributes are *cost effective* and *verifiable*. Thus, the SMART criteria could be extended to include these two attributes, which can be beneficial. For instance, a metric being inexpensive is important for small organizations with limited resources. Conversely, metrics that are expensive or involve a lot of computation or data collection may not be sustainable. Therefore, the final 23 metrics can be assessed against these two additional criteria without loss of the initial selection result as there is no interdependence between the five elements of the SMART criteria as well as between them, and the two additional criteria; cost effective and verifiable.

5 Conclusion

We have identified 105 technical security metrics, 23 of which satisfied the SMART criteria. The final set of metrics can be regarded as feasible to implement and organizations should select the ones that would best suit their requirements and preferences. To this end, we have developed a tool that can be used to categorize and assess metrics effectively. Furthermore, we have identified the properties that a good metric should possess, most of which can be considered as variants of the SMART criteria except two, cost efficiency and verifiability. Hence, the SMART criteria should be extended to include these two elements. Thus, this is particularly useful to facilitate the assessment of metrics.

The limitation of this work is the need to consider the context of metrics selection in practice, e.g., objectives of the company and business goals, which require a considerable amount of time and effort. Thus, in our future work, we will look in depth at the cyber security frameworks proposed in the literature and thoroughly explore the gaps in the existing works. Additionally, we will investigate different scenarios of metrics selection, e.g., a set of metrics selection for a Security Operation Centre (SOC) of a Small and Medium-sized Enterprises (SMEs). Additionally, we aim to look at the linkage between effective security metrics and risk informative measures. We envisage that metrics will be selected depending on the organization's requirements and preferences, whereby the organization could measure cyber risk in a reliable manner.

References

[1] Abercrombie, R. K., Sheldon, F. T., Hauser, K. R., Lantz, M. W., & Mili, A. (2013, January). Risk assessment methodology based on the NISTIR 7628 guidelines. In *2013 46th Hawaii International Conference on System Sciences* (pp. 1802-1811). IEEE. https://doi.org/10.1109/HICSS.2013.466

[2] Abraham, S., & Nair, S. (2015, June). Exploitability analysis using predictive cybersecurity framework. In *2015 IEEE 2nd International Conference on Cybernetics (CYBCONF)* (pp. 317-323). IEEE. https://doi.org/10.1109/CYBConf.2015.7175953

[3] Ahmed, Y., Naqvi, S., & Josephs, M. (2019, May). Cybersecurity metrics for enhanced protection of healthcare IT systems. In *2019 13th International Symposium on Medical Information and Communication Technology (ISMICT)* (pp. 1-9). IEEE. https://doi.org/10.1109/ISMICT.2019.8744003

[4] Akinsanya, O. O., Papadaki, M., & Sun, L. (2020). Towards a maturity model for health-care cloud security (M2HCS). *Information and Computer Security*, *28*(3), 321–345. https://doi.org/10.1108/ICS-05-2019-0060

[5] Al-Shiha, R., & Alghowinem, S. (2019). Security metrics for ethical hacking. In *Intelligent Computing: Proceedings of the 2018 Computing Conference, Volume 2* (pp. 1154-1165). Springer International Publishing. https://doi.org/10.1007/978-3-030-01177-2_83

[6] Baybulatov, A. A., & Promyslov, V. G. (2022, September). A Metric for the IACS Availability Risk Assessment. In *2022 International Russian Automation Conference (RusAutoCon)* (pp. 750-754). IEEE. https://doi.org/10.1109/RusAutoCon54946.2022.9896250

[7] Bhol, S. G., Mohanty, J. R., & Pattnaik, P. K. (2023). Taxonomy of cyber security metrics to measure strength of cyber security. *Materials Today: Proceedings*, *80*, 2274-2279. https://doi.org/10.1016/j.matpr.2021.06.228

[8] Boyer, W., & McQueen, M. (2008). Ideal based cyber security technical metrics for control systems. In *Critical Information Infrastructures Security: Second International Workshop, CRITIS 2007, Málaga, Spain, October 3-5, 2007. Revised Papers 2* (pp. 246-260). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-540-89173-4_21

[9] Charlton, J., Du, P., & Xu, S. (2021). A new method for inferring ground-truth labels and malware detector effectiveness metrics. In *Science of Cyber Security: Third International Conference, SciSec 2021, Virtual Event, August 13–15, 2021, Revised Selected Papers 4* (pp. 77-92). Springer International Publishing. https://doi.org/10.1007/978-3-030-89137-4_6

[10] Chen, H., Cam, H., & Xu, S. (2021). Quantifying cybersecurity effectiveness of dynamic network diversity. *IEEE Transactions on Dependable and Secure Computing*, *19*(6), 3804-3821. https://doi.org/10.1109/TDSC.2021.3107514

[11] Domínguez-Dorado, M., Carmona-Murillo, J., Cortés-Polo, D., & Rodríguez-Pérez, F. J. (2022). CyberTOMP: A novel systematic framework to manage asset-focused cybersecurity from tactical and operational levels. *IEEE Access*, *10*, 122454-122485. https://doi.org/10.1109/ACCESS.2022.3223440

[12] Elasticsearch. (n.d.). Available at https://www.elastic.co/. Accessed 15 June 2024.

[13] Enoch, S. Y., Ge, M., Hong, J. B., Alzaid, H., & Kim, D. S. (2018). A systematic evaluation of cybersecurity metrics for dynamic networks. *Computer Networks*, *144*, 216-229. https://doi.org/10.1016/j.comnet.2018.07.028

[14] Geleta, R. (2018, December). Cyber security metrics for performance measurement in E-business. In *2018 International Conference on Smart Systems and Inventive Technology (ICSSIT)* (pp. 220-222). IEEE. https://doi.org/10.1109/ICSSIT.2018.8748525

[15] Handri, E. Y., Sensuse, D. I., & Lusa, S. (2024). Examining Cybersecurity Culture: Trends and Success Factors. *Journal of Internet Services and Information Security*, *14*(3), 330-352. https://doi.org/10.58346/JISIS.2024.I3.020

[16] Hecker, A. (2008, August). On system security metrics and the definition approaches. In *2008 Second International Conference on Emerging Security Information, Systems and Technologies* (pp. 412-419). IEEE. https://doi.org/10.1109/SECURWARE.2008.37

[17] Holstein, D. K., & Stouffer, K. (2010, January). Trust but verify critical infrastructure cyber security solutions. In *2010 43rd Hawaii International Conference on System Sciences* (pp. 1-8). IEEE. https://doi.org/10.1109/HICSS.2010.410

[18] Jafari, S., Mtenzi, F., Fitzpatrick, R., & O'shea, B. (2010). Security metrics for e-healthcare information systems: a domain specific metrics approach. *Int. Journal of Digital Society*, *1*(4), 238-245. https://doi.org/10.20533/ijds.2040.2570.2010.0029

[19] Johnson, J., Onunkwo, I., Cordeiro, P., Wright, B. J., Jacobs, N., & Lai, C. (2020). Assessing DER network cybersecurity defences in a power-communication co-simulation environment. *IET Cyber-Physical Systems: Theory & Applications*, *5*(3), 274-282. https://doi.org/10.1049/iet-cps.2019.0084

[20] Knowles, W., Prince, D., Hutchison, D., Disso, J. F. P., & Jones, K. (2015). A survey of cyber security management in industrial control systems. *International journal of critical infrastructure protection*, *9*, 52-80. https://doi.org/10.1016/j.ijcip.2015.02.002

[21] Kowalski, S., Barabanov, R., & Hoffmann, R. (2011, September). Cyber security alert warning system: A socio-techinal coordinate system proposal. In *2011 Third International Workshop on Security Measurements and Metrics* (pp. 21-24). IEEE. https://doi.org/10.1109/Metrisec.2011.15

[22] LeMay, E., Ford, M. D., Keefe, K., Sanders, W. H., & Muehrcke, C. (2011, September). Model-based security metrics using adversary view security evaluation (advise). In *2011 Eighth International Conference on Quantitative Evaluation of SysTems* (pp. 191-200). IEEE. https://doi.org/10.1109/QEST.2011.34

[23] Longueira-Romero, Á., Iglesias, R., Gonzalez, D., & Garitano, I. (2020, July). How to quantify the security level of embedded systems? a taxonomy of security metrics. In *2020 IEEE 18th International Conference on Industrial Informatics (INDIN)* (Vol. 1, pp. 153-158). IEEE. https://doi.org/10.1109/INDIN45582.2020.9442219

[24] Mouatassim, H., & Ibenrissoul, A. (2015). Proposal for an implementation methodology of key risk indicators system: Case of investment management process in Moroccan asset management company. *Journal of Financial Risk Management*, *4*(3), 187-205. https://doi.org/10.4236/jfrm.2015.43015

[25] Panchabhai, B. S., & Patil, A. N. (2012). Enterprise Software Management Systems by Using Security Metrics. *International Journal of Science and Research*, 1536-1540.

[26] Patrinos, H. (2014). You Can't Manage What You Don't Measure. Available at https://blogs.worldbank.org/education/you-can-t-manage-what-you-don-t-measure.

[27] Pendleton, M., Garcia-Lebron, R., Cho, J. H., & Xu, S. (2016). A survey on systems security metrics. *ACM Computing Surveys (CSUR)*, *49*(4), 1-35. https://doi.org/10.1145/3005714

[28] Pfleeger, S. L. (2009). Useful cybersecurity metrics. *IT Professional Magazine*, *11*(3), 38-45. https://doi.org/10.1109/MITP.2009.63

[29] Pragadeswaran, S., Subha, N., Varunika, S., Moulishwar, P., Sanjay, R., Karthikeyan, P., Aakash, R., & Vaasavathathaii, E. (2024). Energy Efficient Routing Protocol for Security Analysis Scheme Using Homomorphic Encryption. *Archives for Technical Sciences, 2*(31), 148–158. https://doi.org/10.70102/afts.2024.1631.148

[30] Rathod, P., & Hämäläinen, T. (2017, August). A novel model for cybersecurity economics and analysis. In *2017 IEEE International Conference on Computer and Information Technology (CIT)* (pp. 274-279). IEEE. https://doi.org/10.1109/CIT.2017.65

[31] Rjaibi, N., Rabai, L. B. A., Aissa, A. B., & Louadi, M. (2012). Cyber security measurement in depth for e-learning systems. *International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE)*, *2*(11), 1-15.

[32] Savola, R. M. (2009, July). Development of Security Metrics-Based on Decomposition of Security Requirements and Ontologies. In *International Conference on Software and Data Technologies* (Vol. 1, pp. 171-174). Scitepress. https://doi.org/10.5220/0002243501710174

[33] Scala, N. M., & Goethals, P. L. (2016). A review of and agenda for cybersecurity policy models. In *Proceedings of the 2016 Industrial and Systems Engineering Research Conference. http://www. tinyurl. com/PolicyModels. Accessed* (Vol. 2, p. 2019).

[34] Schneidewind, N. (2009). Metrics for mitigating cybersecurity threats to networks. *IEEE Internet Computing*, *14*(1), 64-71. https://doi.org/10.1109/MIC.2010.14

[35] Sebastian, D. J., Agrawal, U., Tamimi, A., & Hahn, A. (2019). DER-TEE: Secure distributed energy resource operations through trusted execution environments. *IEEE Internet of Things Journal*, *6*(4), 6476-6486. https://doi.org/10.1109/JIOT.2019.2909768

[36] Sherif, E. (2024). A data set from a survey investigating the smart approach to selecting good cyber security metrics [Data set]. Zenodo. https://zenodo.org/records/11943816

[37] Simon, V., Bela, G., & Martin, G. J. (2022). Guest Editorial: Special Issue on Interdisciplinary Cybersecurity. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 13*(3), 1-3. https://dx.doi.org/10.22667/JOWUA.2022.09.30.001

[38] Xu, S. (2020, November). The cybersecurity dynamics way of thinking and landscape. In *Proceedings of the 7th ACM Workshop on Moving Target Defense* (pp. 69-80). https://doi.org/10.1145/3411496.3421225

[39] Xu, S. (2021). SARR: a cybersecurity metrics and quantification framework (keynote). In *Science of Cyber Security: Third International Conference, SciSec 2021, Virtual Event,*

August 13–15, 2021, Revised Selected Papers 4 (pp. 3-17). Springer International Publishing. https://doi.org/10.1007/978-3-030-89137-4_1

[40] Yağdereli, E., Gemci, C., & Aktaş, A. Z. (2015). A study on cyber-security of autonomous and unmanned vehicles. *The Journal of Defense Modeling and Simulation*, *12*(4), 369-381. https://doi.org/10.1177/1548512915575803

[41] Yevseiev, S., Milov, O., Opirskyy, I., Dunaievska, O., Huk, O., Pogorelov, V., ... & Tomashevsky, B. (2022). Development of a Concept for Cybersecurity Metrics Classification. *Eastern-European Journal of Enterprise Technologies*, *118*(4), 6-18. 10.15587/1729-4061.2022.263416

[42] Zhao, X., Zhao, J., Jiang, X., Zhang, X., & Zhang, W. (2019, August). Construction and Security Measurement of Cybersecurity Metrics Framework Based on Network Behavior. In *Journal of Physics: Conference Series* (Vol. 1302, No. 2, p. 022069). IOP Publishing. https://doi.org/10.1088/1742-6596/1302/2/022069

[43] Zieger, A., Freiling, F., & Kossakowski, K. P. (2018, May). The β-time-to-compromise metric for practical cyber security risk estimation. In *2018 11th International Conference on IT Security Incident Management & IT Forensics (IMF)* (pp. 115-133). IEEE. https://doi.org/10.1109/IMF.2018.00017

Authors Biography

Emad Sherif, is a Cyber Systems Engineer, and a PhD student at De Montfort University, UK. He obtained his Master of Science in Information Management and Security from Bedfordshire University, UK. Emad worked as an IT Security Team Lead for a Bank. His research interests focus on the use of data science to improve cyber security risk management.

Dr. Iryna Yevseyeva, is an Associate Professor at De Montfort University, UK. She is Subject Group Leader for Cyber Security and Deputy Director for Cyber Technology Institute. Her main research interests are operational research and cyber security. In particular she uses multi-criteria decision analysis and multiobjective optimization for cyber security risk assessment and investments, cyber threat intelligence and cyber security decision making.

Dr. Vitor Basto-Fernandes, is an Associate Professor with habilitation at the University Institute of Lisbon. He was head of the Research Center in Computer Science and Communications at Polytechnic Institute of Leiria, and a researcher in several international projects in the areas of information systems integration, anti-spam filtering and multiobjective optimization.

Prof. Allan Cook, holds a Master of Science and PhD from the Faculty of Computing, Engineering and Media, School of Computer Science and Informatics, De Montfort University, UK. He helps to integrate cyber security into all areas of the curricula. Allan's first-hand experience and expertise have given staff, researchers and students unrivalled insight into the cyber security industry.