Cyber KPI for Return on Security Investment

Cyril Onwubiko
Cyber Security Intelligence, E-Security Group
Research Series Limited
London, UK
cyril@research-series.com

Austine Onwubiko
Information and Network Security
School of Computing, Engineering & Physical Sciences
University of the West of Scotland (UWS)
Scotland, UK

***Abstract*—Cyber security return on investment (RoI) or return on security investment (RoSI) is extremely challenging to measure. This is partly because it is difficult to measure the actual cost of a cyber security incident or cyber security proceeds. This is further complicated by the fact that there are no consensus metrics that every organisation agrees to, and even among cyber subject matter experts, there are no set of agreed parameters or metric upon which cyber security benefits or rewards can be assessed against. One approach to demonstrating return on security investment is by producing cyber security reports of certain key performance indicators (KPI) and metrics, such as number of cyber incidents detected, number of cyber-attacks or terrorist attacks that were foiled, or ongoing monitoring capabilities. These are some of the demonstratable and empirical metrics that could be used to measure RoSI. In this abstract paper, we investigate some of the cyber KPIs and metrics to be considered for cyber dashboard and reporting for RoSI.**

Keywords—Cyber KPI; Return on Security Investment; RoSI; RoI; Return on Investment; Metrics; Cyber-attack; Cyber Security; Cyber Incidents

I. INTRODUCTION

In business, return on investment (RoI) is very well understood, and clearly defined. In simplistic terms, RoI is a measure of the profitability of an investment. For example, the RoI of a stock investment, the RoI on opening a corner shop etc. are all predicated on profit. Generally speaking, if an investment's RoI is net positive, then it is probably worthwhile [1]. With business, RoI is binary, in the sense that it is an agreed measure of net profitability of an investment.

Contrary to Cyber, return on investment of cyber security has no consensus to date. Many people still argue and debate about it. What it means to one organisation may be entirely different to another organisation of the same nature and business [2]. Further, cyber objectives are different among organisations. National cyber programmes have different objectives to organisation-led cyber programmes; hence it will be challenging to have a set of 'one-size-fits-all' cyber key performance indicators (KPIs).

For example, the objectives for national cyber strategies should be geared toward citizen and societal cyber skills improvement, safer society to conduct business, and education, skills and development. Conversely, organisation cyber programmes are likely to focus on their business specific cyber objectives, such as protection of their systems, data and infrastructure and, to a greater extent gain competitive advantage over its competitors. In a sense, organisation cyber programme objectives are bound to be more focused than those of the national cyber security centres. Therefore, cyber KPIs to measure the success or benefits of cyber programmes should, first and foremost, aim to achieve their primary cyber objectives, in addition to other related opportunities it may create.

In this paper, we provide some metrics which can be used to measure organisational and national cyber security RoIs. We hope this research will motivate interest in the research community on Cyber RoI, Cyber KPI, metrics and reporting.

The key contributions of this paper are as follows:

1) We propose Organisation Cyber KPIs to measure cyber with the view that it may offer insight into RoI for cyber.
2) We describe and discuss each of the metrics proposed, and justification to why we have selected them.
3) We provide metrics for assessing return on investment of National Cyber Programmes and Strategies.

The remainder of this paper is organised as follows: Section II outlines some of the motivations of the paper, and discusses related works. In section III our proposed Cyber KPIs are explained in detail, and finally, the paper is concluded including future work in section IV.

II. MOTIVATION

Cyber security investment is an upscale venture. According to the UK Cyber Security Strategy, 2016-2021, £1bn pound has been allocated for enabling, creating and providing a national cyber security capability [3]. This is quite some investment. Similarly, Finland, America, Australia and among other countries have invested hugely in cyber programmes. With such huge investments come return on investment. These stakeholders who have invested hugely in cyber deserves accountability, and they will demand it, too. There has to be some agreed measures to report and demonstrate whether the investments are worthwhile or not.

With most national cyber programmes there are often clearly articulated objectives, such as addressing cyber skills shortage, improving cyber security skills and education for citizens, providing a robust and resilient cyber capability, protection of citizens and businesses etc. These objectives can therefore form the cyber KPIs for national cyber programmes.

The challenge here, is agreeing on general metrics which can be used to describe and demonstrate RoI for all cyber investments.

A. *Related Work*

Return on cyber security investment (RoSI) is a topic of interest for various communities and stakeholders, especially CERTs, Security Departments, Organisation and National Cyber Security Programmes [4, 6, 10] who annually or however often must justify their existence or goal accomplishments for their continued existence or funding support. Such justifications are often presented to their respective agencies or institutions in the form of a *Business Case*.

A *business case* is a document that explains the need and importance of a project/function, benefit realisations and costs for the implementation, operations and delivery (whole cost) of the project. It should also contain any cost savings that are likely to be gained and of course, value for money propositions.

RoSI has been approached from a number of viewpoints, such as *how much to spend in order to achieve some desired goals*, *what national targets or objectives must the centre accomplish in a specified time period* [10], *what losses must be prevented or the cost of the cyber incident that they must detect or prevent* (ENISA, 2012 [4]) and *what risks will be mitigated or addressed* (D. W. Woods and A.C. Simpson, 2018 [5]).

Unfortunately, deducing or calculating cost of a cyber incident is challenging, and often controversial. This is because there are no empirical methods to calculate exact cost of any particular cyber incident, therefore calculations are often subjective, estimated or projected.

According to (D. W. Woods and A.C. Simpson, 2018 [5]), "making security investment decisions involves giving considerations to a variety of risks". Unfortunately, this task is harder where there are no empirical data to back the decision, and further, where cost of a cyber incident is mostly a guess work, full of subjective hypothesis and estimations.

III. CYBER KPI, METRICS & REPORTING

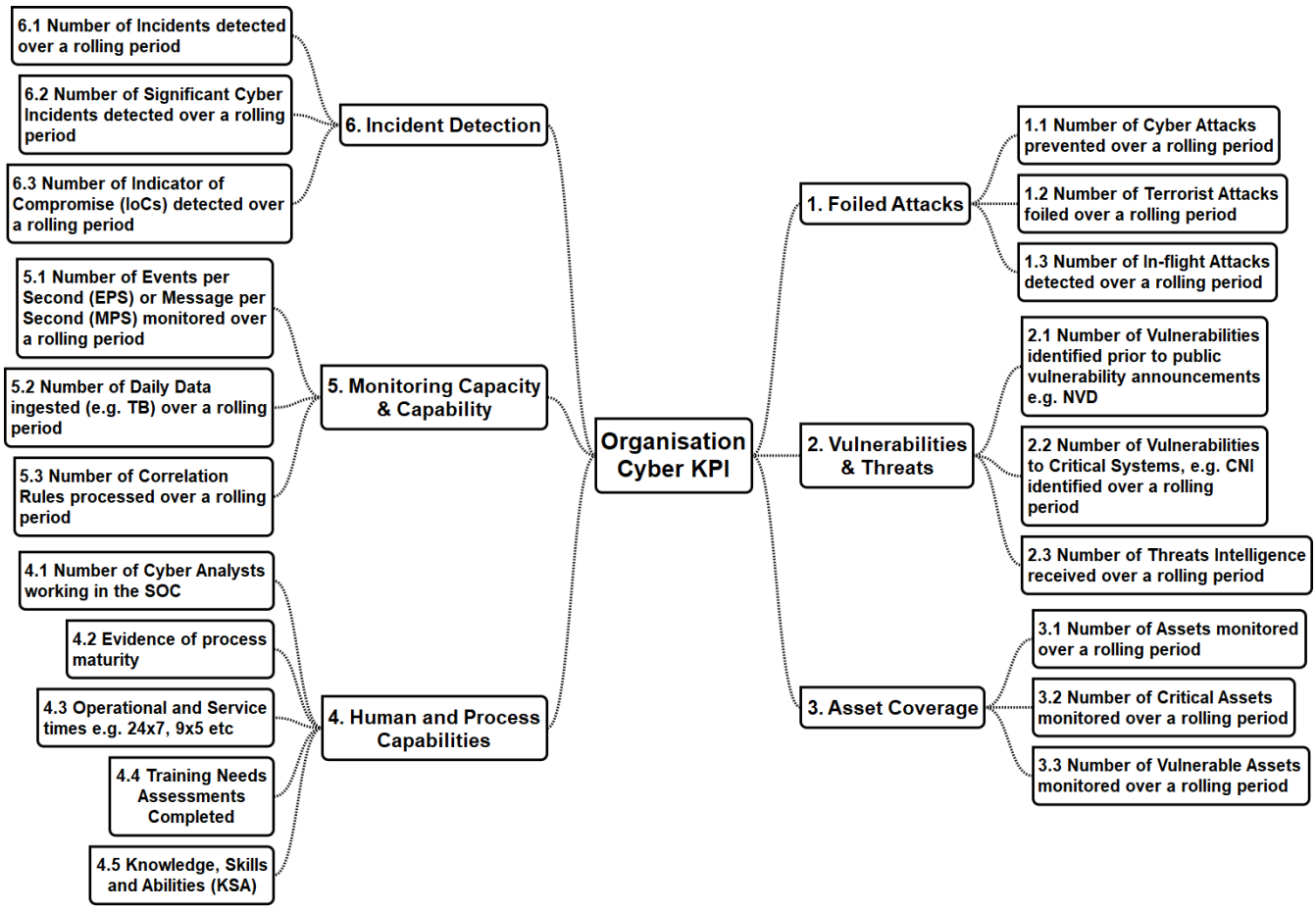

Figure 1: Organisation Cyber KPIs for Assessing Return on Investment

A. Organisation Cyber KPI

In this section, we propose and discuss metrics for reporting organisation cyber KPI and return on investment (see Figure 1). We argue that the metrics used in our proposed model provide useful information about certain aspects of the cyber programme and national cyber strategy that should be used for assessing performance, critical success criteria of cyber programmes to determine how effective and 'profitable' the cyber ventures or investments met the organisational and national overarching objectives.

As shown in figure 1, the cyber KPIs and metrics for assessing organisation cyber programme consists of six (6) measures which can be used to demonstrate cyber RoI, namely: Foiled Attacks, Vulnerabilities & Threats, Asset Coverage, Human and Process Capabilities, Monitoring Capacity & capability, and Incident Detection.

The cyber KPIs and their subcategories their proposed measures and metrics are discussed as follows:

1) Foiled Attacks

These are cyber attacks that the cyber programme through its controls and the SOC are able to prevent, detect and intercept before a security breach or cyber incident is realised. We use this metric to assess the 'benefits realisation of the programe', and also, in meeting its objectives. Three subcategories of metrics include:

1.1 *Number of cyber-attacks prevented over a rolling period*. For example, the report to show RoI may contain the number of cyber attacks that were prevented from being realised on the business in a certain period, say, a 3-month reporting period.

1.2 *Number of terrorist attacks foiled over a rolling period*. For example, the report to show RoI could include the number of foiled terrorist attacks targeted to the country or nation over a certain period, say in a 12-month period. It is pertinent to note that not many cyber programmes work in the counter-terror unit or space, therefore, this metric would only be used for assessment only for the cyber programme in the counter-terror space.

1.3 *Number of in-flight attacks detected over a rolling period*. For example, the cyber KPI report to show cyber RoI may include the number of in-flight attacks detected in a certain period, say, a 3-month reporting period. An in-flight attack is an attack that is thought to be ongoing attack without a complete mitigation or resolution.

There are other measures which could be used, e.g. threat intelligence analysis, malware analysis, threat hunting etc. – there are threat intelligence subscription services, which the cyber programme could leverage, for instance through threat intelligence sharing partnership e.g. National Cyber Security Centre (NCSC) [6], Cyber Security Information Sharing Partnership (CiSP)[7], Malware Information Sharing Platform (MiSP), and third-party threat intelligence feeds or via open source threat intelligence (OSINT).

2) Vulnerabilities and Threats

These are vulnerabilities in business systems, whether out in the wild or freshly discovered, and also the threat that may intend to exploit the vulnerabilities in order to penetrate business systems and critical infrastructures. We have used three subcategories for this assessment:

2.1 *Number of vulnerabilities identified prior to public vulnerability announcements*. This measure is aimed at the effectiveness of the vulnerability scanning or continuous vulnerability management the organisation operates, and whether they are able to detect the vulnerabilities that may exist in the assets in their environment before the vulnerabilities are discovered by others or before the vulnerabilities are out in the wild.

2.2 *Number of vulnerabilities to critical systems e.g. Critical National Infrastructure (CNI) identified over a rolling period*. This is another useful measure. The reasons for saying 'only to critical systems' is because with some organisations, not all systems are monitored. Therefore, we argue that for the investment in cyber to yield any meaningful benefits, critical assets must be monitored, and this measure is about assessing the effectiveness of the monitoring of the organisation's critical assets.

2.3 *Number of threat intelligence indicators of compromise processed over a rolling period*. Indicators of compromise (IoC) are the parameters used to detect threats targeting systems, for example, malware, command and control bots, ransomware etc. Therefore, any effective cyber should be able to detect IoCs, and hence a report containing the number of such IoCs detected over a certain period could be used as a measure of the return on investment.

3) Asset coverage

This is related to the coverage of business assets being monitored by the cyber programme or SOC. It does include the quality and capability of the monitoring. Three metrics are used to assess this capability as follows:

3.1 *Number of assets monitored over a rolling period*. These are business assets that are monitored by the security operations centre (SOC), which demonstrates the coverage of the monitoring. SOCs are the custodians for monitoring, detecting and responding to cyber incidents for most organisations, and their core values are in coordinating cyber incidents and ensuring the detection, monitoring and cyber incident response are performed for the organisation, and also for the nation in the case of national SOCs. Asset coverage also asks the question – has the SOC or organisation completed onboarding of all the services that are to be monitored? If the answer is no, then the first priority should be to ensure that all services to be monitored, including systems, networks,

infrastructures and applications are onboarded – that is, that the assets are configured to produce events and logs, which are ingested and analysed in realtime by the SOC using tools and technologies that are appropriate – until then, both the coverage of services onboarded and the number of assets being monitored can be used as metrics for assessing return on investment. Once all onboarding is complete, then there is no business benefit for using asset coverage as a metric to assess RoI because it would have become a 'business as usual' activities with very minimal activities happening since the assets in the entire estate would have been completely monitored. Further, even when some assets are decommissioned or new assets are introduced in the estate, the number is bound to be small in relative terms compared to the number in the estate prior.

3.2 *Number of Critical Assets monitored over a rolling period*. These are business critical assets, such as critical national infrastructure (CNI) type systems that may hold citizens data, intellectual property rights and critical business processes etc. The monitoring of those demonstrates the return on investment of the business for their cyber strategy and cyber investments.

3.3 *Number of vulnerable assets monitored over a rolling period*. These are business systems (e.g. critical business systems and otherwise) that have known exploitable vulnerabilities, e.g. systems running unsupported operating systems (OS) that are either not regularly patched or no longer supported by the vendors e.g. Windows XP. The rational for this metric are as follows: first, it shows that vulnerable systems have been identified in the first instance, and second, while mitigation approaches are being considered, they vulnerable systems are at least being monitored. This can be a very valuable cyber hygiene metric for the business to demonstrate RoSI.

4) Human and Process Capabilities

This relates to human operators and adminstrators of the system capability, experience, skills and abilities. Human operators, in this case, include SOC analysts, incident responders, threat hunters, adminstrators, team supervisors and managers. Process capability relates the maturity, quality and standard of the business and operational processes being used to manage, monitor and respond to cyber incidents.

4.1 *Number of analysts and personnel working in the SOC*. These include all persons working in the SOC, such as those that enable services to be onboarded and monitored, and those that monitor and operate the services, such as analysts, incident responders, threat hunters and supervisors and managers. The knowledge, skills and abilities of these staff or personnel can also be used as a KPI for assessment.

4.2 *Evidence of processes maturity*. Evidence of process maturity relates to the presence and quality of cyber and SOC policies, processes and procedures. The maturity of such collaterals can be used as metrics to evaluate return on investment of the cyber programme or cyber investment of that organisation. Take for example, an immature SOC will undoubtably lack basic policies, processes and procedures for carrying out their duties, and when they exist, may not have appropriate depth and quality. So, we argue that as a metric to assess maturity of the cyber capability or the SOC, we believe it can therefore be used to equally assess the return on investment.

4.3 *Operational and service times.* This relates to the operational hours that the SOC or the cyber programme operates. For example, some businesses operate a 24x7 (24 hours, 7 days per week), 9x5 (9am start and finishes 5pm daily), 9x5 plus on-call services etc. The operational working hours of the SOC, which is a measure of the responsiveness of the SOC, and the coverage of their operational capability. We argue that some businesses require a 24x7x7 (that is 24 hours, 7 days a week and including Saturdays and Sundays), while some don't. Cyber programmes do not necessarily need to operate run the clock because most of the time, it is not an operational function, rather a project-based activity; however, the SOC do because SOCs are operational service monitoring oriented function. How the SOC operates a run the clock service can be executed in a number of different operating service models, such as 24x7xz7, 7x7x7[1] plus On-Call and 9x5 plus On-Call.

4.4 *Training Needs Assessments*. This relates to the training needs required by the SOC to identify which training should be provided to the SOC staff to equip them to become better skilled, experience and capable cyber experts. Every SOC requires training to make the staff relevant, and up to date with the fast-paced cyber world. New skills and capabilities are frequently required in cyber as new technologies and advancements emerge. We argue that keeping the SOC staff skilled is a KPI that should be used to assess the RoI of organisation cyber programme.

4.5 *Knowledge, Skills and Abilities (KSA).* This relates to knowledge, skills, and experience required of the staff that work in the SOC. This assessment can be used to gauge the maturity of the SOC, and fundamentally, a good basis for reporting against the objectives of the cyber programme, and therefore, a key KPI for measuring RoI.

5) Monitoring Capacity & Capability

This relates to the size, quality and maturity of both the operational and technical monitoring aspects of the cyber

[1] 7x7x7 – means 7am start, 7pm finish, and 7 days a week, including Saturday and Sunday.

programme and the SOC. If the technology used for security monitoring is immature and if the processes are not robust or the people are not trained, then one would argue that the outcome of such as investment is likely to be of lower quality. To assess this attribute, we have used three metrics such as:

5.1 *Number of Events per Second (EPS) or Message per Second (MPS) monitored over a rolling period*. EPS is a useful metric to assess the capability of the cyber programme or SOC monitoring tool/technology, and this invariably is equally a useful barometer to measure the return on investment of the cyber programme. We argue that EPS or its equivalence, such as MPS or size of data being processed by the SOC tooling offer useful metric to assess their capacity. For example, small to medium size SOC tools are limited to the amount of EPS it can handle, while large enterprise security information and event management (SIEM) tools can hande an order of magnitude more EPS compared to lower-end tools.

5.2 *Number of daily data ingested over a rolling period*. Similar to #5.1 above, daily data ignested, which is measured in bytes (e.g. terabytes, gigabytes, patrebytes etc) gives an indication of the capacity of the tool and the volume of data it can handle, process and store. Handling relates to the volume of data ingest, 'processing' relates to the concurrency, user activities, correlation and cross-correlation of data. This type of activites requires both the processor (CPU power), swap memory, and also the graphics. Store relates to the storage capacity that allows for persistent storage and archive of data for long term usage. The number of dialy data ingest metric is a useful indicator to measure RoI of the organisation cyber programme, as it gives an indication of their capacity, and capability, too.

5.3 *The number of correlation rules processed over a rolling period*. This relates to the capability of the monitoring tools, especially the SIEM. Correlation is the ability to analyse events from dissparate sources and of different formats to detect threats that could exploit or breach security. Most of the known SIEMs tools do come with 'out of the box' correlation engine and rules; which are a set of well-defined codes to detect certain trait of malware, policy violation, misuse or abuse, and often referred to as use cases. To assess the capability of the SOC, one parameter is to evaluate the capability of their monitoring tools, and these could be, for instance, an assessment of the correlation rules, and ability of the correlation engine and the capacity, too. We believe that since this is a known feature of all SIEMs, we could use this feature to assess the capability of the SIEM, and consequently use it to measure RoI.

6) Incident Detection

This relates to the detection capabilities that the cyber programme or SOC possess. It assess whether the programme is able to detect simple, advanced, or sophisticated attacks, and also an understanding of the mean time to respond (MTTR) of the SOC.

We have used three metrics to assess this feature for the cyber programme, as follows:

6.1 *Number of incidents detected over a rolling period*. This relates to the cyber incidents that the cyber investment is able to detect. It could be that the cyber investment is able to detect basic, advanced or very sophisticated attacks, hence this measure can then be used to assess the capability of the cyber programme or the SOC.

6.2 *Number of significant cyber incidents detected over a rolling period*. This relates to the ability to detect significant cyber incidents. Significant cyber incidents as defined in [8], means very advanced cyber incidents that could lead to major incidents when occurred. The reason for considering significant cyber incidents is that not all monitoring capabilities have the ability to detect advanced and sophisticated complex attacks, therefore monitoring system that are able to do so must be recognised, and hence, a good metric to assess for detection capability, and consequently a metric to record in the cyber KPI for reporting RoI.

6.3 *Number of indicators of compromise (IoCs) detected over a rolling period*. This relates to IoCs detected by the monitoring system over a rolling period, say, daily, weekly or monthly. IoCs are identifiers for threats, such as malware, botnets, ransomware, command and control (C2) etc. When using IoCs as an indicator to assess the capability of the monitoring system, emphasise should be on the capability of the monitoring system to detect IoCs in various formats and nature. For example, IoCs can appear as MD5 or SHA Filehashes, Domain names, Hostnames, Fully qualified domain names (FQDN), IP address, uniform resource indicator (URI), Domain Name system (DNS), Domain, Uniform Resource Locator (URL), Email, Mutual Exclusion Objects (Mutex) and Common Vulnerability Exploit (CVE). We argue that the capability of the monitoring system can be deduced by its ability to detect IoCs of different types and nature. We believe this metric is a useful indicator in measuring return on investment for cyber security.

B. National Cyber KPI

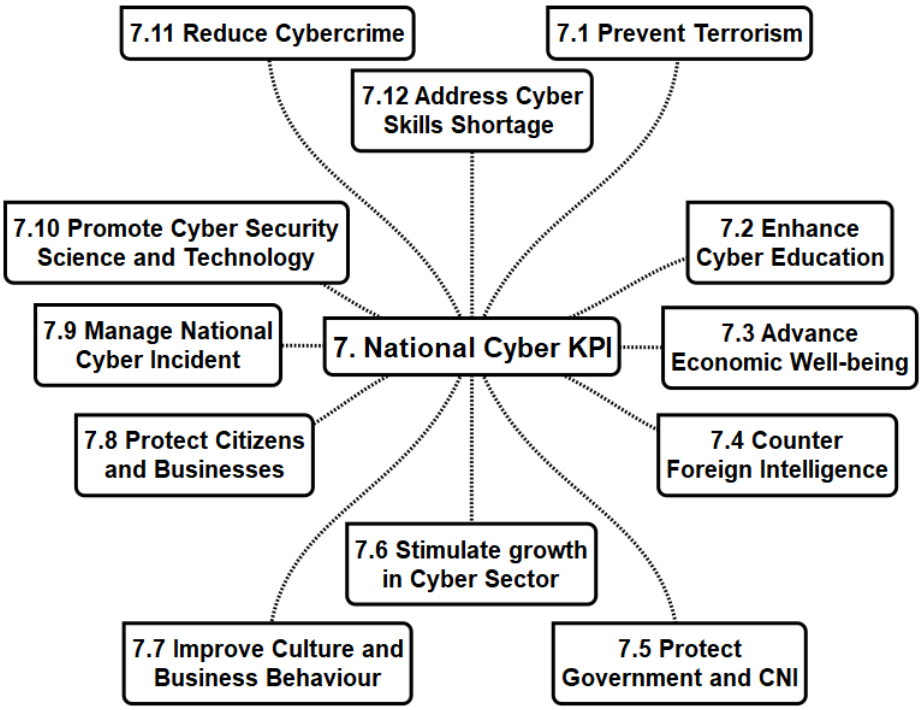

Figure 2: National Cyber KPIs for Return on Investment Reporting

In section, we propose and discuss cyber metrics and cyber KPIs we consider important when assessing RoIs of reporting national cyber security programmes or centres. These metrics stem from reviewing the overarching goals and visions stated in known national cyber security strategies [2, 9, 10].

National Cyber Security Programmes are shaped by the country's cyber security strategy. For example, the UK National Cyber Security Strategy [3], its overarching vision is to ensure economic wellbeing of the country and to make "Britain confident, capable and resilient in a fast-moving digital world". Similarly, the vision of the Finnish Cyber Security Strategy [9], is to provide a safe cyber domain that citizens, the authorities and businesses can effectively utilise, with a target to make Finland a global forerunner in preparedness and resilience to cyber threats. The vision for the Australian Cyber Security Strategy [10] is to "protect their Australia from cyber-attacks and to ensure that they can defend their interests in cyberspace". Based on a review of these cyber security strategies and other notable materials we have extracted common notable themes, goals and objectives and crystallised those into the key metrics shown in our proposed National Cyber KPI model (see Figure 2), which we explain as follows.

7.1 *Prevent Terrorism* – This is one of the prime objectives for establishing national cyber programmes in modern times to foil terrorist attacks in order to keep citizens secure and protected. According to GCHQ Chief, Jeremy Fleming [11], GCHQ continues to play critical role in stopping European terror plots. As one of the objectives for creating national cyber programmes, we argue that to measure RoI and to report cyber KPI, the ability to prevent terror attacks should be one of such KPIs to be reported against. This should include but not limited to foiling of terror attacks, awareness of terror groups, deterrence and monitoring capabilities required by the national cyber security centres and other agencies in executing this role.

7.2 *Enhance Cyber Education* – Cyber security education is an important aspect of growing the cyber skills workforce, and also developing people with appropriate cyber skills. Cyber security education, training and skills capability building either through apprenticeships or In-House training programmes should be high on the agendas of most national cyber security strategies. Without a great plan on how to enhance cyber security skills of citizens through diligent and well developed programmes then it will be challenging to address the current cyber security skills gap. Universities, colleges and secondary schools should prioritise cyber security education in their curricular. On the job training programmes should also become a defacto standard for industry employees, especially those who do not have information technology skills to learn on the job. Student apprenticeships and work placements should focus on enhancing cyber security skills in the offer.

7.3 *Advance Economic Well-being* – Advancing economic outlook and wellbeing of the society is a prime national cyber programme objective. All of the national cyber security strategies reviewed in this paper [3, 9, 10], all had the tangible objective of the national cyber security programme primarily for the development, advancement and enhancement of economic opportunities through cyber. Economic growth may be measured in terms of job creation opportunities, partnerships among government, industry and academia to create open, free and secure cyberspace that encourages both national and international investments thereby bolstering economic wellbeing for citizens and the countries alike.

7.4 *Counter Foreign Intelligence* – With the increasing number of reported nation-sponsored cyber-attacks, espionage, terrorism, therefore, one of the core objectives of nation cyber security strategies is to counter foreign intelligence activities thereby reducing or preventing foreign intelligence actors and their agents from unleashing attacks in the country. Foreign intelligence may be interested in disrupting critical national infrastructures, cause national unrest, disrupt national elections or our ways of life etc. It is important that our national cyber security programmes are capable of countering foreign intelligence actions, hence a core goal of national cyber security programmes.

7.5 *Protect Government and CNI* – Government and critical national infrastructures are the bedrock of modern society. For example, CNI systems such as power grid, water, national health service (NHS) etc. if disrupted, could cause distress to many citizens' lives, lead to instability in our society, and could lead to loss of lives. This is why it is important that our government and CNIs are adequately protected, hence one of the primary duties of national cyber security programmes must be to protect our governments and their critical national infrastructures.

7.6 *Stimulate Growth in Cyber Sector* – Cyber security is now likened to critical national infrastructures such as water, gas, electricity or national health service because cyber is pervasive and foundational to the appropriate operation of these traditionally known CNIs systems. Without cyber security, these CNI systems may be compromised, and used to impact or disrupt other critical services, which then have consequential impact on citizens. Growth in cyber security will drive research and innovation, competition, creation of jobs and other opportunities and a brighter outlook. Investment in research and development, academia, research institutes and encouraging local establishments to target solving local problems through products and services offerings, and institutionalizing agencies/bodies that sponsor high-tech innovation through facilitation and grants will help stimulate growth in the cyber security sector.

7.7 *Improve Culture and Business Behaviour* – National cyber security programmes should drive improvements in culture and business behaviours. There should be guides and schemes use to offer security awareness, and drive improvements in culture and business behaviour. For example, the ten steps to cyber security, guides to cyber security guidance for business [12] developed by the UK NCSC [13], and the Cyber Essentials Scheme [14], are some of examples of broader initiatives to improve culture and business behave. These schemes offer free online training materials, and guides to encourage good cyber behaviour and awareness.

7.8 *Protect Citizens and Businesses* – Protection of citizens and businesses are extremely important for any government, and hence a prime objective of national cyber security programmes. For any society to thrive, it must protect its citizens and the economy, and businesses are fundamental to this. The same way that government and CNIs must be protected, too. Citizens make government while CNIs support both citizens and businesses. Without critical national infrastructures such as electricity and gas, most businesses will go out of operation, likewise, there would not be a government without citizens. We argue that national cyber security programmes must be obliged to protect, government, citizens, CNIs and businesses, and hence these are key cyber KPIs that should be reported to guide business realisation of national cyber security centres or programmes.

7.9 *Manage National Cyber Incidents* – As we know, cyber incidents cannot be completely avoided or provided. They do happen from time to time, and hence national cyber programmes must have mechanisms to manage largescale national incidents, whether they are critical cyber incidents, significant cyber incidents or widespread cyber incidents. Managing national cyber incidents require the cooperation and collaboration of many stakeholders ranging from government, academia and industry, and partnerships are required to coordinate national cyber incidents. Incident management playbooks and protocol must be developed well in advance on how to coordinate and manage national cyber security incidents [8].

7.10 *Promote Cyber Security Science and Technology* – Science, technology, mathematics and engineering (STEM) are important aspects of society. The drive business process change, culture change, and enable growth. It is pertinent that national cyber security programmes or centre invest on science and technology capabilities that is future proof, allowing the country to stay ahead of risks posed by cyber-attacks, encourage the next generation of cyber security tools and techniques that will drive our digital economy and enable government to make better policy decisions [15].

7.11 *Reduce Cybercrime* – Cybercrime is on the rise. This should not surprise anyone. With high-value bearing government service (e.g. benefit systems) going online, financial services operating digitally, e.g. online backing, electronic commerce etc., there will be motivated hackers and organized criminals who will be driven to penetrate these systems for financial gains, and in some occasion by foreign

intelligence services or nation-sponsored actors. The new frontier for attack is not shifting to cyber, and less of land, sea or air. National cyber security centres or programmes should be capable of preventing and detecting cybercrimes, especially those realised on national and government systems. While national cyber security programmes are not instituted to monitor individual citizens traffic or cybercrimes on end user devices (EUD), however, they should be capable of advising, understanding and knowing cybercrimes on the wild.

7.12 *Address Cyber Skills Shortage* - Cyber skills workforce is one of the core objectives of most national cyber security programmes. According to the Australian Cyber Security Strategy [10], one of the actions stemming from its national cyber strategy is to ensure Australia has appropriately trained cyber skills workforce. According to Dr Tobias Feakin, Director of the International Cyber Policy Centre at the Australian Strategic Policy Institute [10], "the current shortfall in the workforce – and the research and development base which complements it – can only be addressed through investment in sound policy and a long-term education plan that targets high schools and universities to promote careers in the cyber security profession". Therefore, we argue that to measure or assess the benefit realisation of national cyber programmes, a valid KPI would be to consider reporting cyber education and cyber skills workforce as a cyber KPI for return on security investments for the programme.

IV. Conclusions and Future Work

In this paper, we have discussed metrics and key performance indicators that could be used when reporting organisational and national cyber security return on investments.

We argue that while return on security investment have been calculated using the known formula, that is:

RoSI = (Benefits of Investment – Cost of Investment) / Cost of Investment

It is unclear how *benefits of a cyber security investment* can be obtained, especially, since empirical data on this seldom exist, and values are subjective and estimations. Many contributors have used the 'cost of cybercrime' [4] as a way to deducing the *benefit of investment*, while other parameters have been used. Unfortunately, calculating the cost of cybercrime or cyber incident is challenging, and equally nondeterministic at present.

Therefore, in this paper, we have provided 20 metrics or KPIs that can be used to assess the benefits of cyber security investments. These metrics provide a rich set of values that organisations can use to measure benefit realisations for their cyber security investments without being overly hung-up on fictious estimated values, most importantly, these parameters are key performance indicators that we believe offer useful measures for cyber security programme assessments.

Similarly, we have also provided 12 metrics or KPIs which can be used to assess national cyber security programmes or centres. These 12 metrics are deduced by reviewing some of the known national and sovereign cyber security strategies, such as the United Kingdom Cyber Security Strategy, Finnish and Australian Cyber Security Strategies.

We believe that the KPIs proposed in this study are not complete or conclusive, so future research should focus on conducting a much extensive study on other metrics that could argument the set provided in this paper.

V. Reference

[1] Investopedia (2019), "Return on Investment". Accessed 2nd Feb 2019. https://www.investopedia.com/terms/r/returnoninvestment.asp

[2] CSEurope (2019), "Feature: Cyber Security Return on Investment". Accessed 2nd Feb 2019. https://www.cseurope.info/cyber-security-roi/

[3] UK Government (2016), "UK National Cyber Security Strategy". Accessed 2nd Feb 2019. https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021

[4] European Network and Information Security Agency (ENISA), 2012, "Introduction to Return on Security Investment", Helping CERTs assessing the cost of (lack of) security, Dec. 2012

[5] D. W. Woods and A.C. Simpson, (2018), "Towards Integrating Insurance Data into Information Security Investment Decision Making, published in 2018 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (Cyber SA), 2018

[6] NCSC (2019), "National Cyber Security Centre". Accessed 2nd Feb 2019. https://www.gov.uk/government/organisations/national-cyber-security-centre

[7] CiSP (2019), "Cyber Security Information Sharing Partnership". Accessed 2nd Feb 2019. https://www.gov.uk/government/news/government-launches-information-sharing-partnership-on-cyber-security

[8] C. Onwubiko and K. Ouazzane (2019), "SOTER: A Playbook for Cyber Security Incident Management", to appear in the IEEE Transactions on Engineering Management, Special Section: Cyber-attacks, Strategic Cyber-foresight and Security, 2019

[9] Finnish Cyber Security Strategy (2013), "The Finland's Cyber Security Strategy, Government Resolution 24.1.2013", ISBN: 978-951-25-2438-9 PDF, 2013. Accessed 10th Feb 2019. https://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf

[10] Australia Cyber Security Strategy (2016), "The Australia's Cyber Security Strategy, Enabling innovation, growth & prosperity", ISBN 978-1-925238-62-4 PDF, 2016. Accessed 10th Feb 2019. https://www.pmc.gov.au/sites/default/files/publications/australias-cyber-security-strategy.pdf

[11] GCHQ (2018), "UK plays critical role in stopping European terror plots", Independent, Wednesday 20 June 2018. Accessed 23 Feb 2019. https://www.independent.co.uk/news/uk/crime/gchq-foiled-terror-attacks-europe-brexit-eu-jeremy-fleming-a8407196.html

[12] NCSC (2016), "Cyber Security Guidance for Business", Department for Digital, Culture, Media & Sports, 2016. Accessed 24th Feb 2019. https://www.gov.uk/government/collections/cyber-security-guidance-for-business

[13] NCSC (2016), "10 Steps to Cyber Security", 09 Aug. 2016

[14] NCSC (2017), "Cyber Essentials Scheme", 27 November 2017. Accessed 24th February 2019. https://www.cyberessentials.ncsc.gov.uk/

[15] Cabinet Office (2017), "Interim Cyber Security Science and Technology Strategy", 30 November 2017.