Traditional KPIs or metrics for evaluating business risks are inefficient for understanding cyber risks

Word Count -1,272

# Introduction

Several sources [1,2,3,12] define KPIs (Key Performance Indicators) as a tool to measure how well an organisation operates to achieve its objectives; for risk management, KPIs are useful in assessing risks within a business [4]. Applied to cyber-attacks, however, scepticism arises over whether these traditional business methods are feasible for monitoring and mitigating threats. This document endeavours to evaluate the proposed statement above. Firstly, to determine a definition on cyber-attacks. Secondly, understand whether KPIs truly are unsuitable for this type of risk. Thirdly, identify various security technologies currently implemented to mitigate cyber-attacks, including issues found in information security.

# Cyber Attacks

A Cyber-attack identifies as a form of cybercrime relating to illegal activity, where attacks target individuals and organisations alike [5, p. 62]. Examples include Malware – malicious software installation systems operating without users’ knowledge or consent [5, p. 62], [6, p. 95]; Phishing - social engineering where an attacker attempts to manipulate a user into providing personal identity information (PII) for immoral purposes [7, p. 22], [8, p. 63], [9, p. 11], or a distributed denial of service (DDos) attack – when resources of a systems are throttled, unable to perform normal activity [10, pp. 5, 42], [11] to name a few. Based on these types of attacks, being able to monitor and mitigate these risks is no small feat, and the very nature of how they operate could help to explain scepticism in why KPIs are a suboptimal approach.

# Examination of KPI use for Cyber Risks

## Key Performance Indicators

In a journal article by Zhou and He [12], they state that KPIs take much time and effort to implement as well as the uncertainty of KPIs capturing all metrics needed; by which point, the state of the cyber risk landscape could have mutated with unknowing all potential cyber risks that are accounted for. Additionally, a journal article back in 2018 [13] participants found it difficult to understand the KPI calculations for assessing vulnerability and impact, and the number of KPIs to determine impact could increase but presents additional challenges. A further study [14] suggests that traditional performance measures are not suitable for IT-focused intangible assets.

## Key Risk Indicators

Conversely to the above, Tammineedi [15] suggests the use of KPIs in tandem with Key Risk Indicators (KRIs) for synergy between business and risk performance; KRI metrics provide insight into weaknesses in monitoring and control tools, allowing for ongoing risk monitoring between risk assessments [16]. This term is further supported by Young [17], though aware that organisations may be unaware of its full use, to exploit the benefits of mitigating cyber risks.

# Various Security Technologies implemented for Cyber Attack Risks

There are various technologies and processes – current and emerging - within organisations which help to avoid, share, mitigate or accept the relevant risks [18, pp. 23–24] a business is willing to face where operating – partially or fully – within a digital environment. Before examining the ways in which these risks get managed, there are issues when dealing with cyber risk in information security itself.

## Issues within Information Security and risks for management

### Compliance

One issue highlighted in terms of Information Security (IS) that remains, is compliance. As Burman suggests [19, pp. 164–165] compliance issues – albeit from a data and internal perspective within an organisation - may appear in IS due to complex standards difficult to interpret, lack of resource in an organisation to enforce, or technology evolves faster than the compliance in place. There is an aspect from Gibson [20, pp. 253–262], that agrees with Burman, where employees need correct training to follow compliance with the prodigious amount of differing legislation, standards, and policies that could prove difficult to always adhere to or learn, even with the best intentions, resulting an in increased exposure to human error. Furthermore, the current compliance measures seen thus far appear to either too complex to construe correctly, or to a high-level to interpret sufficiently. Not only from a user perspective, but ensuring compliance ensues in all aspects that would fall under the information security space - such as equipment, internal networks, system applications, interactions outside this network to name a selection.

### IS governance not keeping at pace with modern technology and threats.

Whilst improvement is apparent in recent times, there seems to be an impression that IS has a fundamental problem which is yet unrectified; the principles of IS not being able to keep the same pace as technology - and new threats – discovered at macro and micro levels. One example is the length of time in which relevant legislation or standards take to become endorsed, by which point, there is a likelihood such laws are already defunct. As quoted by Mallory [21], this creates inconsistencies with between best practice an organisation endorses, and actual operations that need performing. Additionally, this can apply the polices a organisation applies themselves. As stated by Schinagl and Shahim [22] security in organisations is still a concern, only addressed when something goes wrong - such as a cyber-attack or data breach, rather than a continuous resilience to manage it. One vulnerability associated with this could emulate from the adoption of employees having to work from home, where working practices drastically changed due to the COVID-19 pandemic; which as Georgiaadou, Mouzakitis, and Askounis illustrate [23], asserting an introduction of new vulnerabilities and threats, such as a variant of social engineering commenced on employees.

## Current ways of management for risks and threats

There are various methods at present, which are used to handle risk an organisation may experience for ailments found within their digital environment. One approach is for organisations to transfer risk to a third party, to reduce the impacts effect from a threat if also considering the principle of proportionality [24, p. 32]. This method Is known as risk transference [25]. An example of risk transference is when an organisation would purchase insurance, such as Cyber Insurance to cover liability similar to data breaches [26]. Whilst this does not necessarily reduce the risk present, but reduce the impact of loss for the business, such as reduction in financial loss; similar to other insurances a business would obtain to cover elements such as environmental factors like a natural disaster. Another practice of managing risk, is via risk avoidance; whereby entails elimination of risk by withdrawing resources from it [27]. An example of risk avoidance, could be that a business is physically located in an area susceptible to natural disasters such as flooding or hurricanes; which in turn can lead to power failures, business interruption, data loss; therefore an option would be to move the location of the physical office for the business into the area which does not suffer from this difficulty often or never.

# Conclusion

Although it may be obvious that technology will have a large factor to play in terms of the how a business manages risk within a digital environment. Items discussed above are not an exhaustive list of what to consider. People, data, and planning, however, play fundamental roles in contributing towards successful risk management. There is bias on the use of KPIs not being the favoured method, but more the use of both KRIs and KPIs together. Two main issues of compliance and governance keeping pace with new threats and challenges within the cybersecurity space is something that needs to be addressed from a myriad of perspectives. Recommendations would be taken to see if the structure of how legislation and standards are placed in cyber security, that not only keeps up to date and remains applicable for longer, but also try to simplify what is out there so it can be easily digested by the layman.

# References

[1] H. Kerzner, Project Management Metrics, KPIs, and Dashboards A Guide to Measuring and Monitoring Project Performance, Third Edition. Hoboken, Nj, Usa John Wiley & Sons, Inc, 2017, p. 122.

[2] W. W. Eckerson, Performance dashboards : measuring, monitoring, and managing your business. Hoboken, N.J.: J. Wiley, 2006, p. 294.

[3] B. Marr, Key performance indicators for dummies. West Sussex, England: John Wiley & Sons, 2015, p. 18.

[4] Indeed Editorial Team, “7 KPIs You Can Use for Risk Management,” Indeed Career Guide, Sep. 10, 2021. https://www.indeed.com/career-advice/career-development/kpi-for-risk-management (accessed May 12, 2022).

[5] S. El-Bahrawy, GCSE AQA computer science for the grade 9-1 course : the revision guide. Broughton-In-Furness? Cgp Books, 2018, p. 62.

[6] K. D. Mitnick, The art of deception : controlling the human element of security. New York ; Chichester: Wiley, 2003, p. 95.

[7] W. Schmidt, CISSP: A Comprehensive Beginners Guide on the Information Systems Security. Independently Published, 2019, p. 22.

[8] S. El-Bahrawy, GCSE AQA computer science for the grade 9-1 course : the revision guide. Broughton-In-Furness? Cgp Books, 2018, p. 63.

[9] K. D. Mitnick and W. L. Simon, The Art of Deception : Controlling the Human Element of Security. Hoboken; Indianapolis, Indiana: Wiley, 2002, p. 11.

[10] Darril Gibson, Managing Risk In Information Systems. S.L.: Jones & Bartlett Learning, 2020, pp. 5, 42.

[11] NCSC, “How Cyber Attacks Work,” Ncsc.gov.uk, 2019. https://www.ncsc.gov.uk/information/how-cyber-attacks-work (accessed May 12, 2022).

[12] H. ZHOU and Y.-L. HE, “Comparative Study of OKR and KPI,” DEStech Transactions on Economics, Business and Management, vol. 1, no. eced, pp. 319–323, Jul. 2018, doi: 10.12783/dtem/eced2018/23986.

[13] H. Kure, S. Islam, and M. Razzaque, “An Integrated Cyber Security Risk Management Approach for a Cyber-Physical System,” Applied Sciences, vol. 8, no. 6, p. 898, May 2018, doi: 10.3390/app8060898.

[14] S. Huang, C. Lee, and A. Kao, “Balancing performance measures for information security management,” Industrial Management & Data Systems, vol. 106, no. 2, pp. 242–255, Feb. 2006, doi: 10.1108/02635570610649880.

[16] P. Kervan, “What is a Key Risk Indicator (KRI) and Why is it Important?,” SearchCIO, Oct. 2021. https://www.techtarget.com/searchcio/definition/key-risk-indicator-KRI (accessed May 12, 2022).

[17] J. Young, “THE USE OF KEY RISK INDICATORS BY BANKS AS AN OPERATIONAL RISK MANAGEMENT TOOL: A SOUTH AFRICAN PERSPECTIVE,” Corporate Ownership and Control, vol. 9, no. 3, 2012, doi: 10.22495/cocv9i3c1art2.

[18] Darril Gibson, Managing Risk In Information Systems. S.L.: Jones & Bartlett Learning, 2020, pp. 23–24.

[19] J. J. Berman, Principles and practice of big data preparing, sharing, and analyzing complex information. London Cambridge, Ma Academic Press, An Imprint Of Elsevier, 2018, pp. 164–165.

[20] Darril Gibson, Managing Risk In Information Systems. S.L.: Jones & Bartlett Learning, 2020, pp. 253–262.

[21] P. Mallory, “Time to update your cybersecurity policy?,” Infosec Resources, Sep. 15, 2020. https://resources.infosecinstitute.com/topic/time-to-update-your-cybersecurity-policy/ (accessed May 12, 2022).

[22] S. Schinagl and A. Shahim, “What do we know about information security governance?,” Information & Computer Security, vol. 28, no. 2, pp. 261–292, Jan. 2020, doi: 10.1108/ics-02-2019-0033.

[23] A. Georgiadou, S. Mouzakitis, and D. Askounis, “Working from home during COVID-19 crisis: a cyber security culture assessment survey,” Security Journal, Feb. 2021, doi: 10.1057/s41284-021-00286-2.

[24] Darril Gibson, Managing Risk In Information Systems. S.L.: Jones & Bartlett Learning, 2020, p. 32.

[25] S. Snedaker and C. Rima, “Risk Transference - an overview | ScienceDirect Topics,” www.sciencedirect.com, 2014. https://www.sciencedirect.com/topics/computer-science/risk-transference (accessed May 12, 2022).

[26] Nationwide, “What Is Cyber Insurance? – Nationwide,” Nationwide.com, 2019. https://www.nationwide.com/lc/resources/small-business/articles/what-is-cyber-insurance (accessed May 12, 2022).

[27] S. Hajmohammad and S. Vachon, “Mitigation, Avoidance, or Acceptance? Managing Supplier Sustainability Risk,” Journal of Supply Chain Management, vol. 52, no. 2, pp. 48–65, Dec. 2015, doi: 10.1111/jscm.12099.