Key Performance Indicators and Risk Assessment

Marcelo Fernandes
Wellington, New Zealand
marceelofernandes@gmail.com

I. Definition of Key Performance Indicators (KPI's)

Performance assessment is a concept applied by many organisations to guarantee their businesses are efficiently administered. Although sustainable profit is the major goal for most organisations, performance assessments will not only account for the organisation's financial gain, but will also capture other useful metrics, including delivery reliability, safety of operations, risk aversion, employees and customers satisfaction, manufacturing time, level of social interaction, product volatility, etc.

The metrics mentioned above are known as "Performance Indicators" (PI's). A more formal definition of PI is: “An item of information collected at regular intervals to track the performance of a system” [1]. In other words, PI's are used when evaluating how efficient an organisation is at working towards a certain goal. The addition of the word "key" simply implies emphasis on metrics that are critical for an organisation.

KPI's are usually expressed as quantitative metrics that display a number and its associated activity (e.g 0 minutes of down-time, 2% margin of annual profit), though they can also be expressed as qualitative values (e.g high consumer satisfaction, high employee gratification).

February 15, 2021

II. Can KPI's be applied to support security and risk management?

There are some basic limitations to the extent of valuable information KPI's provide for the analysis of potential risks and security breaches. As discussed, the intention behind KPI's is to provide a measurement of efficiency. From that, some KPI's for security and risk assessment might include:

- Number of leaked private user data per week.
- Weekly down-time (in minutes) due to denial of service attacks.
- Number of instances of business-sensitive information being leaked through phishing attacks per week.

These kinds of KPIs are evidently important in certain cases - they represent a high-level view of how many threats have succeeded in penetrating the organisation's security framework.

However, if these KPI's were to be used as a measure of how risk-resistant an organisation is, they would provide nothing but a logical flaw. As having a boxer on a winning streak of 21 consecutive matches does not imply that he would win the 22nd, the same way having zero data leaks does not imply that the organisation is not susceptible to a first successful penetration.

One could present more examples where KPIs displaying successful security metrics fail to unveil the real risk an organisation currently faces, but without stretching this subject too much, we bring the "cum hoc ergo propter hoc" fallacy, which summarises the idea that having a correlation between two variables does not imply one is the cause of the other. This chain of thought is further explored in [2] and [3] on the account that performance indicators by themselves are incomplete, given that measurements alone are insufficient for guiding an organisation towards improvement of security routines and risk tolerance.

III. From KPI's to Key Risk Indicators (KRI's), Another Strategy for Mitigating Risks

The Key Risk Indicator (KRI) [4] is an alternative solution to avoid deceptive KPIs. Instead of analysing the performance figures, the analysis is shifted towards metrics that best indicate the possibility of future deteriorating impact, such as:

- Number of outdated back-end libraries
- Servers without firewall protection
- Number of exposed private API gateways

The key difference between the KRIs above and the KPIs presented earlier is that the former is a better representation of a cause-and-effect model for understanding potential threats, e.g., If the organisation does not have firewalls installed on a number of servers, then the infrastructure is vulnerable to network attacks.

It is not unreasonable to assume that in most on-line digital environments a hacker attack is a question of "When" not "If". This brings another dimension to KRIs, the one of damage mitigation. Some examples are:

- Number of backup servers
- Number of successful security routines
- Budget for eventual damage repair

From the examples in both this list and the one before, KRI's show more objectiveness when compared to KPI's.

But even though KRI's are an improvement, they still have fragilities. KRI's need to be tailored to specific business cases, and therefore are a matter of expertise and skill. Additionally, organisations may ignore certain risks that don't have a high probability of occurrence or that might not appear sufficiently impactful. These risks would be neglected if they aren't being observed by a KRI.

In summary, both KRI's and KPI's are not sufficient for completely assessing how vulnerable to threats an organisation is. Both indicators shall be treated as complementary tools that need to be used along with robust security and risk management guidelines. These guidelines will be discussed below.

IV. Expanding on Other Relevant Problems and Issues with Information Security and Risks for Management

Organisations assert their commitment to having secure business practices by acquiring certifications and by adhering to protocols that show their compliance to information security and risk assessment guidelines [5].

Several information security management (ISM) guidelines have been elaborated to supply cyber security and risk assessment best practices to organisations, e.g, GASPP/GAISP, SSE-CMM, ISO/IEC17799: 2000, BS7799, etc. However, one relevant problem amongst these well-known guidelines is that they are either too generic or present an all-embracing scope. A thorough study on the four ISM guidelines above [6], showed that their developers seeked to validate security concepts by "appealing to common practice and authority". This approach brings worrisome weaknesses, and it evidently makes the guideline insufficient for tailoring a successful security framework. Further studies [7-8] showed that implementations of several systems based on ISM guidelines presented vulnerabilities when compared against ISO/IEC 27001. This adds another level of concern, as there are disconnects between system implementations and ISM guidelines.

V. Improving Information Security Management Guidelines

The ISM guidelines mentioned above are regarded with noteworthiness being that they serve as standards for building information security management systems (ISMS)[9] that will later be authoritatively used by businesses.

To begin finding a solution, one postulation is fundamental: 'every guideline needs to be manufactured to the benefit of its user'. Firstly, the guideline developers need to research the current methodologies that are used in practice for avoiding security threats and for minimising risk. These methodologies need to be verified empirically, and, from that, their practice needs to be elaborated upon, and most importantly, their blind spots need to be detailed. Additionally, recommendations for implementing such guidelines should be facilitated to avoid some of the problems mentioned above. As of now, the single guideline that ticks the majority of these requirements is ISO/IEC 27001 [9].

VI. Conclusion

KPI's are practical metrics for summarizing the performance of a business, but they do not provide sufficient information for effectively understanding cyber risks and system vulnerabilities. Alternatively, KRI's present more objectiveness for tracking such vulnerabilities, but express a shared fragility with KPI's, the one of being simple metrics and therefore not being adequate for assessing the full extension of risks organisations face each day. This does not negate the usefulness of such indicators in other contexts, but argues that both indicators are not self-sufficient for being delivered as a cybersecurity framework.

ISM guidelines provide more refined foundations for managing the prevention and response against cyber attacks. One noticeable problem with these guidelines is the often found appeal to authority and the lack of explanation and reasoning behind some recommendations [7-8]. Additionally, some guidelines have a lack of implementation details that affects the ability of ISMS's to put the guideline into effect. All problems considered, one guideline that has been satisfactory and covers most of the issues common to other guidelines is the ISO/IEC 27001 [9].

References

[1] C. Fitz-Gibbon, Performance indicators. Clevedon, Avon, England: Multilingual Matters, 1990.

[2] I. Bakanauskienė and A. Sližytė, "Designing performance measurement system in organization", pp. 135-148, 2007. Available: https://hdl.handle.net/20.500.12259/36744. [Accessed 15 February 2021].

[3] S. Beatham, C. Anumba, T. Thorpe and I. Hedges, "KPIs: a critical appraisal of their use in construction", Benchmarking: An International Journal, vol. 11, no. 1, pp. 93-117, 2004. Available: 10.1108/14635770410520320 [Accessed 15 February 2021].

[4] D. Hoffman, Managing operational risk. New York, NY: Wiley, 2002.

[5] J. Broderick, "ISMS, security standards and security regulations", Information Security Technical Report, vol. 11, no. 1, pp. 26-31, 2006. Available: 10.1016/j.istr.2005.12.001 [Accessed 15 February 2021].

[6] M. Siponen and R. Willison, "Information security management standards: Problems and solutions", Information & Management, vol. 46, no. 5, pp. 267-270, 2009. Available: 10.1016/j.im.2008.12.007 [Accessed 15 February 2021].

[7] W. Park et al., "Analysis of Information Security Management Systems at 5 Domestic Hospitals with More than 500 Beds", Healthcare Informatics Research, vol. 16, no. 2, p. 89, 2010. Available: 10.4258/hir.2010.16.2.89 [Accessed 15 February 2021].

[8] B. Sussy, C. Wilber, L. Milagros and M. Carlos, "ISO/IEC 27001 implementation in public organizations: A case study", 2015 10th Iberian Conference on Information Systems and Technologies (CISTI), 2015. Available: 10.1109/cisti.2015.7170355 [Accessed 15 February 2021].

[9] E. Humphreys, Implementing the ISO/IEC 27001 information security management system standard. Boston: Artech House, 2007.