Human Factors in Cybersecurity, Vol. 91, 2023, 61–71
https://doi.org/10.54941/ahfe1003720

Using Security Metrics to Determine Security Program Effectiveness

Satyam Mishra, Phung Thao Vi, Vu Minh Phuc, Oni Damilola Igbagbo, and Nguyen Van Tanh

International School, Vietnam National University, Hanoi (VNU-IS), Vietnam

ABSTRACT

Security objectives serve as the foundation for security metrics, which are used to guide decisions on how to increase the security of all parts engaged in providing services and processing data. Numerous data breaches are revealed each week, some of which may have affected tens or even hundreds of millions of people. Customers and regulators are both becoming more concerned about firms' information security procedures and their plans for preventing security breaches and protecting sensitive data. As a result, several laws and regulations have been enacted to enhance cybersecurity risk management and to protect personal information that may be held or transmitted among businesses. The majority of these industry-specific and general data protection laws are complex, requiring ongoing oversight to maintain compliance throughout your business and the companies of your vendors. To gauge the effectiveness of and involvement in the usage of security controls, it is crucial to define a set of security metrics. A carefully defined set of metrics will help direct future security decisions and strengthen your organization's security posture. In our study, we proposed to review security metrics to determine security program effectiveness for a company which is fictional for the scope of study. Firstly, we defined security metrics and their key indicators successfully. We discussed different scenarios for Trivest Technologies Limited company, which is fictional, we just used it for our scope of study. We successfully discussed, developed, and used KPIs, KRIs and KGIs; which are security metrics for the Trivest Technologies Limited company, and we found out that these security metrics help us determine the security program effectiveness for a company successfully. By implementation of its successful results, it also aligns with one of the United Nations Sustainable Development Goals i.e., 8th: Decent work and Economic Growth.

Keywords: Metrics, Security, UNSDGS, KPIs, KRIs, KGIs

INTRODUCTION

Through the gathering, analysis, and reporting of pertinent data, security metrics are quantitative benchmarks used to comprehend the status of systems and services. Security objectives serve as the foundation for security metrics, which are used to guide decisions on how to increase the security of all parts engaged in providing services and processing data (*Definition of Security Metrics - Gartner Information Technology Glossary*, n.d.). Numerous data breaches are revealed each week, some of which may have affected tens or even hundreds of millions of people. Customers and regulators are

both becoming more concerned about firms' information security procedures and their plans for preventing security breaches and protecting sensitive data. As a result, several laws and regulations have been enacted to enhance cybersecurity risk management and to protect personal information that may be held or transmitted among businesses. The majority of these industry-specific and general data protection laws are complex, requiring ongoing oversight to maintain compliance throughout your business and the companies of your vendors. To gauge the effectiveness of and involvement in the usage of security controls, it is crucial to define a set of security metrics. A carefully defined set of metrics will help direct future security decisions and strengthen your organization's security posture. Without a quantitative approach to threat intelligence, businesses are more vulnerable to attacks that can harm their reputation and income (*The Most Important Security Metrics to Maintain Compliance | UpGuard*, n.d.). There are some works being done for image processing as well using Canny Edge Detection Algorithm, their security metrics is worth looking into (Mishra & Thanh, 2022). Also, some neural network approach training for object detection etc. for driverless vehicles to take covid patients and their security has been talked about in academia (Mishra et al., 2022). In our study, we express how we can use security metrics to determine the security program effectiveness. It also aligns with one of the United Nations Sustainable Development Goals i.e., 8^{th}: Decent work and Economic Growth (*THE 17 GOALS | Sustainable Development*, n.d.).

Measuring Security

Why would you want to measure security, and how would you do it? We could be interested in knowing how effective our information security program is. People may respond, "Hey, we have an X secure information security program, how do you know?" and we may ask, "How do you know?" But the true way we know is by measuring it. We know using metrics. However, how effectively will your security management program safeguard your assets? Is it worth the time, money, resources, and other resources you are investing in it? Metrics can notify your management how well and how effectively your security program is performing, which is where they come in.

Security Metrics – Key Indicators

The three most common security metrics will be covered in this section. Key performance indicators, key risk indicators, and key goal indicators are all available. Each of these can also be divided into a number of additional subelements. For instance, we may construct and monitor a list of significant risk indicators. How should metrics be defined now? We start by defining what we hope to learn from the metric, what we hope to measure, and what it should tell us. The second question that we should be asking is, "Is it measurable?" Is there a metric that can provide the information you seek? Is the metric qualitative, which might be subjective depending on the person's point of view, or quantitative, which is normally non-subjective and numerical? Is it possible for someone else to repeat the measurement and get the same results?

It might not be a useful measurement if it can't. Something is wrong with our ruler if I measure something and get 3 inches, and you measure and get 8 inches. As a result, we must ensure that the measurement can be repeated. Therefore, it needs to be repeatable and defined. Does the measure lend itself to computation or aggregation, or, put another way, can you take this metric and translate it into numerical terms? Can it be quantified, concrete, aggregated, or averaged so that we can utilize it to provide metrics on other things when combined with other measurements?

Here are some recommendations on metrics. S.M.A.R.T. is a phrase that is used in the corporate world, the engineering world, and other fields. What does S.M.A.R.T. stand for and why should metrics be S.M.A.R.T. As illustrated in Figure 1: Prior to everything else, Specific should be specific and defined. It is important to specify exactly what we are attempting to gauge. Second, Measurable. The object of our measurement should be measurable. There must be a way to measure it in practice. Things could be measured in terms of price, duration, and other numerical units of time. Alternately, we may quantify it using qualitative units like a scale from very low to very high. Thirdly, the measurement must be achievable, which means that we must be able to perform the measurement rather than merely guess at it. Fourthly, Repeatable (and Relevant). When it comes to R, we can look at it from two distinct angles. First, the metrics should be repeatable because we want others to be able to perform the same measurement and have the same results. This way, we can be sure that the measurement is successful. The measurement in this case should also be pertinent to what we are trying to accomplish or communicate about the security program. To do this, we must define a procedure. The last point is that metrics should be time-bound. We should all concentrate on a particular time frame. How many users, for instance, log out of their accounts per day? (nantham, 2022).

Scenario – Security Metrics at Trivest Technologies Limited

Let's look at our scenario situation, which involves the corporation TTL that is the subject of our study and examine the security metrics that TTL employs. TTL mostly wants to know how effectively they are protecting their assets and how well their security program is working. Additionally, they want to be aware of their hazards. They also want to know if their security systems are operating properly. Finally, they want to know if they are adhering to governance. Now that we have all these inquiries, we can assess the program's

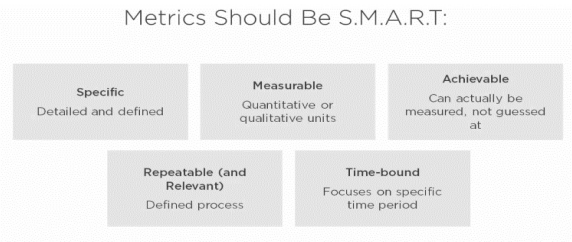

Figure 1: Metrics should be S.M.A.R.T.

effectiveness. Now, however, we are unable to resolve this using a crystal ball. These are questions that we need to be able to measure and collect data to answer.

To resolve these vexing issues, TTL must create metrics! For instance, we can assess how effectively a security program is working if there is a breach. It's difficult to argue that security is doing its job if everything is going smoothly because there may also be other elements at play. TTL must therefore provide some metrics that would enable them to track and provide answers to these difficult questions.

METHODOLOGY

Developing and Using KPIs

KPIs must function properly because their entire purpose is to establish the beating heart of our performance management process. They inform us of our progress, and eventually, we wish to advance in accordance with our strategy. KPIs are what accomplish that, then. Please make sure they are worthwhile as we will be residing with them. (*How to Develop and Use Key Performance Indicators | OnStrategy Resources*, 2021) KPIs are essentially performance indicators for security mechanisms, procedures, and software. Additionally, performance is the focus. A KPI is used to assess if a measurement is falling short of a predetermined level of desired performance. If we want our servers to be operational 99.99% of the time, for instance, our key performance indicator could be if it drops below that, say if it drops 98% of the time. Higher numbers are typically preferable for KPIs; however, this isn't always the case. If we wanted to gauge the number of security events we experienced, 99.99% of the time that the server is up, and running is certainly better than 98%. In this instance, two security events are preferable to ten. Higher numbers are therefore not always better, just sometimes. (Reciprocity, 2021)

Now that we have established that we are examining performance, let's discuss some examples of key performance indicators. Additionally, although it's possible, performance doesn't always have to be about the technology or security measures. We can measure the performance of firewall interfaces, for instance, by looking at their throughput. The performance is poor if they are being bugged down. Because of this, they run the risk of missing something or limiting incoming traffic. Therefore, we might need to consider that for a particular threshold. As a result, a KPI may be the throughput of fire-wall interfaces. Another KPI example is the accuracy rate of antimalware protection products in identifying malware. For instance, if they have a 99% accuracy rate, we want them to function well. For instance, we don't want them to execute at a 58% accuracy rate. Therefore, if we establish a KPI threshold of, say, 95%, anything below that threshold is below the desired level of performance. Number of employees who reported phishing attempts during a recent phishing exercise is another example of a KPI. For instance, as part of a phishing exercise, we set out phishing attempts for each of 50 people in our organization as our target audience. How many employees reported participating in that exercise? There is certainly a performance issue if just 5 employees reported when we required at least 45 employees to do so. After

that, we can investigate the root of the issue. Therefore, that may be a KPI. Another KPI is the decrease in incident response times during training. That is an instance where a low number is desired. The incident response time should not be prolonged. Ten minutes would be preferable to two hours. These are some important illustrations of key performance indicators.

What other areas can KPIs be applied to generally, then? Performance, throughput, etc. of the equipment have already been covered. We also discussed employee performance, which is crucial to everything because it refers to how well employees are completing their duties. Are they performing up to the bar set for them? Another thing we may gauge using a KPI is compliance. If we don't comply with those rules to a certain extent—say let's 98%—we fall short of that KPI. Reduction of incidents is a good way to gauge how effectively our incident response team is performing, as well as how well we train our staff and how well our network security is. An important performance measure is quicker, more accurate identification and reporting. We can set the level and test it if we have predetermined levels or thresholds that we want to fulfill for incident reporting or event detection. Additionally, we can track more efficient security program management, and once more, KPIs don't exist as a standalone concept. How might you evaluate the administration of a security program that is effective? It can be broken down into various items. It may track budget, timeline, scope, number of occurrences, number of persons trained in a given month, etc (mimecast, n.d., p. 10).

Developing and Using KPIs at Trivest Technologies Limited

Let's talk about Trivest Technologies Limited's performance indicators. They have selected a number of personnel indicators. They have determined that, as an example, how many individuals they train each month is a performance indicator that reveals the effectiveness of our security training program. Infrastructure indicators include throughput, which may be one, the number of dropped bytes and packets, among other concepts. Costs, timeline, scope of work, is work lagging or going over budget, to put it another way, are all performance indicators for program management. We also have signs of compliance. What number of controls do we meet? Do our performance standards meet the majority of our compliance obligations? We also offer security indicators, such as the number of monthly occurrences, identified intrusions, and malformed packets. We also get indicators from third parties, with whom we have agreements, to see if they are performing up to par. Some examples of Personnel KPIs are shown in Figure 2 below.

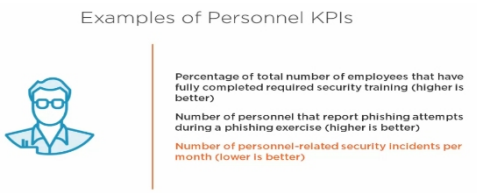

Figure 2: Examples of personnel KPIs.

Developing and Using KRIs

Now let us discuss about key risk indicators. And we will discuss about how to develop and use those in our security metrics. A key risk indicator (KRI) is a metric for estimating how likely it is that the probability of an occurrence and all of its effects will surpass the company's risk tolerance and significantly impair the effectiveness of the business. (*What Is a Key Risk Indicator (KRI) and Why Is It Important?*, n.d.) Key Risk Indicators tells us if specific risk factors are changing and how it changes. If we have pre-established thresholds of risk and the key risk indicator indicates that risk falls below that then that's actually a good thing, risk is lowered. However, if the key risk indicators tell us that risk has exceeded that threshold, then that's not a good thing. So, this is one of those cases where the lower the risk indicator, the better. Figures 3 & 4 below shows the risk factors and indicators we have (OneTrust, n.d.).

So, what are some KRI's we discussed. They are mentioned in the Figure 4 below.

Developing and Using KRIs at Trivest Technologies Limited

Now that we've talked about important risk factors. Let's now talk about how Trivest Technologies Limited develops and employs them. Here's a hypothetical situation. What are some of the major warning signs for Trivest Technologies Limited; Over the previous quarter, TTL noticed a rise

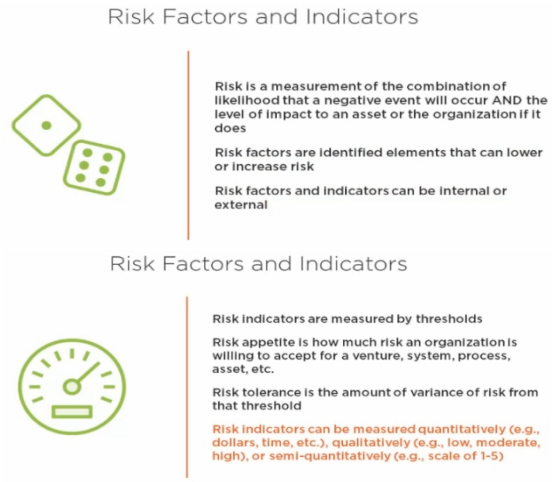

Figure 3: Risk factors and indicators.

Figure 4: KRIs.

in security-related occurrences. Most include occurrences involving people. What risk indicators might be employed to evaluate the efficacy of personnel security? What areas can these measurements indicate as the main problems that need more attention? Therefore, we must create important risk indicators that would inform us of these facts and aid in the solution of these issues. Some incident KRIs at Trivest Technologies Limited are displayed in Figure 5 below.

Developing and Using KGIs

Finally, the third type of metrics we will discuss our key goal indicators. Now, a key goal indicator, basically, measures how effective we are in reaching our security goals. These are kind of top-level numbers and sometimes these are dream numbers. We have goals that we set because management tells us to, but they have to be realistic goals. And our KGIs tell us how good we are at meeting those security goals. First of all, we have to decide what those goals are. So first, we have to have defined measurable goals. They must be defined. They actually must be realistic as well and reachable, and they have to be measurable either quantitatively or qualitatively. They can't be abstract or in the cloud there. These goals should be centered on security Effectiveness. When we look at things like reduction of incidents, reduction of impact if they happen, protection of our assets and so forth. One thing about KGIs is they could be Aggregates of or they could be fed by KPIs and KRIs. For example, if your performance is not up to Snuff or you have a lot of risk do you think you're meeting your goals? Probably not. So, let's look at some key goal indicators. The number of incidents might be an indicator and by itself, that's hard to say whether or not that means the security Effectiveness is where you want it to be. The number of incidents might be that your security program is effective, or it might be because nobody's attacking you lately. How would you know? So, there are other ways you need to measure that to produce that number to be sure, how well are we responding to true incidents. And how are we doing on our incident response exercises? Is our exercise response time increasing or decreasing and what are our goal for that? Our infrastructure up time? Specifically, our security infrastructure up time, are we having failures, is the infrastructure performing the way it's supposed to. What is our goal for performance there? And finally, program management is a key goal indicator. And when we talk about program management, we're talking about things like cost, schedule, scope of work. We're also talking about Personnel training. We're also talking about various things that we do

Figure 5: Some incident KRIs at Trivest Technologies Limited.

Figure 6: TTL security KGIs.

Figure 7: Relevant KGIs at TTL.

when we run a security program when we manage it. ("Key Goal Indicator (KGI), Key Performance Indicator (KPI), Key Risk Indicator (KRI)," 2020)

Developing and Using KGIs at Trivest Technologies Limited

Now that we've covered Key goal indicators. Let's see how we might use those at TTL. So here are some security KGIs for TTL. TTL is reviewing its information security KGIs for the previous quarter. Other KGIs are mentioned in Figure 6 below and also in Figure 7 are mentioned some relevant KGIs at TTL.

RESULTS AND DISCUSSION

Since we've covered KPIs, KRIs and KGIs. Now, how do we use security metrics?

Security Metrics

One thing that we need to point out is that we can use the security metrics in conjunction with each other. We want to gain a larger holistic view of the

Security Programs Effectiveness, we can use them individually of course and they tell us individual data points, but we can also combine them in a way that it tells us simply how well we're doing. So, using these metrics together, we can provide a comprehensive view of the organization. These metrics can answer for us, how well we're performing using the KPIs of course, how much risk do we actually have using KRIs and how will we meeting all of our overall goals the KGIs. We can use those individually or in aggregate, of course. Now, one thing we noticed is that there are relationships between these three types of metrics between KPIs, KRIs and KGIs. KGIs are overall goals, KRIs subtract from those goals and also subtract from performance and KPIs actually help us to meet our goals. So, what kind of relationships are there here?

In Figure 8, we can see that if we reduce risk, then we can increase performance and maintain our achieve goals. And what does risk do, risk reduces our performance, and it makes achieving our goals more difficult. We measure those with our KRIs. Now, if performance increases which are measured by KPIs, we reduce risk and we make our goals achievable and if we maintain our achieved goals, of course it demands increase performance and it's an incentive to reduce risk if we set a goal. That means when we achieve that goal, we have actually reduced risk. We've also increased our performance, otherwise we wouldn't have met that goal. Reducing risk is a good thing, but if we maintain risk, then we impact performance and goals, and the better our performances, and the more we achieve our goals, obviously, the more we're going to reduce risk, so those are the relationships between those three types of metrics.

KPIs, KRIs, KGIs vs State-of-the-Art Methods

KPIs, KRIs, and KGIs are metrics used to measure various aspects of a security program, while state-of-the-art methods refer to advanced techniques and technologies used to enhance the effectiveness of security programs.

KPIs, KRIs, and KGIs provide a quantitative measure of security program performance, risk, and value generation, respectively. On the other hand, state-of-the-art methods such as data analytics, machine learning, and artificial intelligence can be used to analyze large amounts of data and identify patterns, trends, and potential risks that may not be visible through traditional methods.

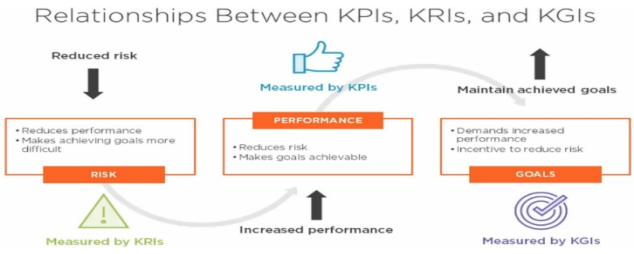

Figure 8: Relationships between KPIs, KRIs and KGIs.

By combining KPIs, KRIs, and KGIs with state-of-the-art methods, organizations can have a more comprehensive view of their security program performance, risk, and value generation. This can help organizations make data-driven decisions to improve the effectiveness of their security programs.

Some examples of the integration of KPIs, KRIs, KGIs and state-of-the-art methods include:

- Using machine learning algorithms to analyze log data and identify potential security incidents based on KRIs
- Using data analytics to track the trend of KPIs over time and identify areas for improvement
- Using artificial intelligence to identify and prioritize security risks based on their potential impact on the organization.

ACKNOWLEDGMENT

Foremost, we would like to express our sincere gratitude to our advisor Dr. Nguyen Van Tanh for the continuous support for our group's study and research, for his patience, motivation, enthusiasm, and immense knowledge. His guidance helped us in all the time of research and writing of this research. We could not have imagined having a better advisor and mentor for our work.

CONCLUSION

To conclude all, we proposed to use security metrics to determine security program effectiveness for a company which is fictional for the scope of study. Firstly, we defined security metrics and their key indicators successfully. We discussed different scenarios for Trivest Technologies Limited company, which is fictional, we just used it for our scope of study. We successfully discussed, developed, and used KPIs, KRIs and KGIs; which are security metrics for the Trivest Technologies Limited company, and we found out that these security metrics help us determine the security program effectiveness for a company successfully. By implementation of its successful results, it also aligns with one of the United Nations Sustainable Development Goals i.e., 8th: Decent work and Economic Growth i.e., promote sustained, inclusive, and sustainable economic growth, full and productive employment, and decent work for all.

REFERENCES

Definition of Security Metrics—Gartner Information Technology Glossary. (n.d.). Gartner. Retrieved December 10, 2022, from https://www.gartner.com/en/information-technology/glossary/security-metrics.

How to Develop and Use Key Performance Indicators | OnStrategy Resources. (2021, May 17). https://onstrategyhq.com/resources/how-to-develop-and-use-key-performance-indicators-kpis-4-mins/

Key Goal Indicator (KGI), Key Performance Indicator (KPI), Key Risk Indicator (KRI). (2020, October 9). *ZAQINFOSEC*. https://zaqinfosec.com/2020/10/10/key-goal-indicator-kgi-key-performance-indicator-kpi-key-risk-indicator-kri/

mimecast. (n.d.). *Top 10 Cybersecurity Metrics and KPIs*. Mimecast. Retrieved December 10, 2022, from https://www.mimecast.com/blog/top-10-cybersecurity-metrics-and-kpis/.

Mishra, S., Minh, C. S., Thi Chuc, H., Long, T. V., & Nguyen, T. T. (2022). Automated Robot (Car) using Artificial Intelligence. *2021 International Seminar on Machine Learning, Optimization, and Data Science (ISMODE)*, 319–324. https://doi.org/10.1109/ISMODE53584.2022.9743130

Mishra, S., & Thanh, L. T. (2022). SATMeas - Object Detection and Measurement: Canny Edge Detection Algorithm. In X. Pan, T. Jin, & L.-J. Zhang (Eds.), *Artificial Intelligence and Mobile Services – AIMS 2022* (pp. 91–101). Springer International Publishing. https://doi.org/10.1007/978-3-031-23504-7_7

Nantham, S. (2022, August 29). *What are Smart Metrics and why are they Important?* Best OKR Software by Profit. Co. https://www.profit.co/blog/kpis-library/what-are-smart-metrics-why-are-they-important/.

OneTrust. (n.d.). *How are You Measuring InfoSec KRIs and Cybersecurity Metrics?* OneTrust. Retrieved December 10, 2022, from https://www.onetrust.com/blog/how-are-you-measuring-infosec-kris-and-cybersecurity-metrics/.

Reciprocity. (2021, April 14). *Cybersecurity KPIs to Track + Examples*. Reciprocity. https://reciprocity.com/cybersecurity-kpis-to-track-examples/.

THE 17 GOALS | Sustainable Development. (n.d.). Retrieved December 10, 2022, from https://sdgs.un.org/goals.

The Most Important Security Metrics to Maintain Compliance | UpGuard. (n.d.). Retrieved December 10, 2022, from https://www.upguard.com/blog/security-metrics.

What is a Key Risk Indicator (KRI) and Why is it Important? (n.d.). CIO. Retrieved December 10, 2022, from https://www.techtarget.com/searchcio/definition/key-risk-indicator-KRI.