PRINCIPLES OF MINIMUM, OPTIMAL AND IMPOSED FINANCIAL CYBER SECURITY

Emil BURTESCU[1]

[1] Faculty of Economics and Law, University of Pitesti, Romania, emil.burtescu@upit.ro

Abstract: *Ensuring cyber security is not an option anymore but has become a responsibility. Implementing security measures meant to diminish risk is done according to the degree of understanding risk and financial availability of the organization. In principle, three approaches can be distinguished: minimal, optimal and financially imposed. Choosing one of these approaches will position the organization on a specific cyber security level - either higher or lower.*

Key words*:* cyber security, risk analaysis, countermeasures, cost.

JEL Classification Codes: D81

1. REALITY

We live in a word in which the Internet is everywhere and nobody questions this anymore. The estimations [1] show that in 2023 almost two thirds of global population – 5.3 bln. people will use an internet connection and the number of connected devices will be more than 29 bln. units. The number if websites has doubled in 10 years reaching over 1.2 bln. and the number of webpages is more than 25 bln. [2].

This is the world in which organizations and people do their activities. These stock and transfer digital data with a volume of approximately 100 Zettabytes (1 Zettabyte = 10^{21} Bytes) in 2022.

In such a non-ideal environment, either slower or faster, threats develop. It is said that we live in a world with a permanent cyber security threat. Any internet connected device (desktop, laptop, tablet, smartphone, gaming console) is a possible threat no matter the operating system that it uses. The security risk is generated by these devices. The risk is represented by the device itself. The risk is part of the huge growth of the Internet in the past thirty years. Risk is everywhere in the digital world [3].

Any organization that does not invest in cyber security is a risk for the other organizations. Any computer must be treated as a threat. Managing cybersecurity within an organization is an option anymore but an obligation.

Understanding the dangers associated to cybersecurity represents the first step that must be done for the organizations to do their specific activities in an optimal manner. If this first step is not done there is a very high risk that the organization might disappear from the market due to security compromise.

A risk analysis within the organization done by cybersecurity experts will reveal the directions and investments that must be done for implementing measures and acquiring controls.

Another step that is as important is represented by fund allocation to implementing cybersecurity investments.

In fact, allocating funds for implementing cybersecurity is maybe the most important and critical decision. Insufficient fund allocation for a detailed risk analysis will generate erroneous data that will lead to erroneous and chaotic cybersecurity measures. Insufficient fund allocation for cybersecurity implementation will lead to the same result – insufficient cybersecurity – even if the risk analysis has been performed by domain experts.

Finally, the implementation of cybersecurity measures will be done according to the degree of understanding of risk and financial allocations.

2. RISK

A threat defined as "Potential cause of an undesired impact over a system or organization" (ISO 13335-1) is in fact an unwanted event (intentional or accidental) that can produce damage to an organization generating financial loses and even more, generate loss of human lives. The threat will generate a risk for the organization. Risk, defined as "Combination between the probability of an event and its consequences" (ISO Guide 73) is in fact a threat that can exploit the potential weaknesses of a system.

Minimising risk is the main objective that must be the focal point of organizations. Risks can be classified in three categories: natural events, business environment and deliberated attacks.

It is highly likely that when people think of cybersecurity they take into account only specific attacks not taking into account the fact that a natural event or business environment can generate risks. A natural event (earthquake, tornado etc.), an uncertain business environment (cooperations and legal and commercial connections, economical circumstances, political circumstances etc) can generate risks that are as high or even higher.

For minimising risk at the level of an organization there are three key aspects that emphasis must be put on: people, processes and technologies. This will assume that for each of the three categories the following must be ensured:

People. Continuous and up to date training. Clearly specified responsibilities. Domain knowledge. Effective organization.

Processes. Clear, actual and viable politics. Tested procedures. Up to date standards.

Technologies. Safe and adequate infrastructure. Safe, adequate, tested and audited applications.

The sole purpose of all these is to reduce threats and diminish risk. For this, the following absolutely necessary stages will be followed – Risk Management Cycle (Microsoft variant) [4] (figure 1).

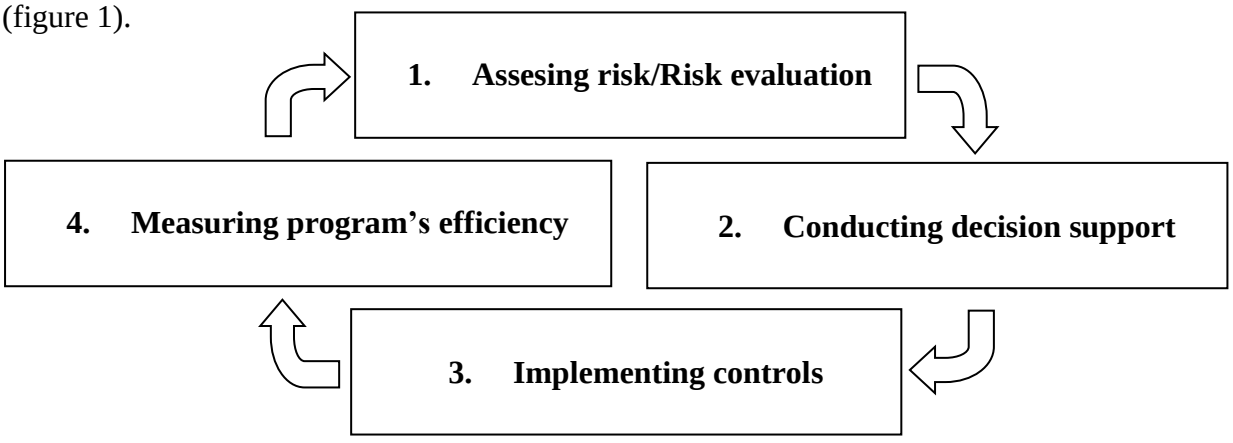

Figure 1. Risk management cycle (Microsoft variant)

In each of these stages, the following will be executed:

1. **Assesing risk/Risk evaluation –** Identifying and classifying the risks that can affect the business.
2. **Conducting decision support –** Identifying and evaluating the control measures and solutions taking into account the cost-benefits report.
3. **Implementing constrols –** Implementing and running control measures meant to reduce or to eliminate the risks.
4. **Measuring the program's efficiency –** Analyzing the efficiency of the adopted control measures and checking if the applied controls ensure the established protection level.

The stage that will be the subject of this study is Implementing controls. Depending on the implemented controls, one will have a risk diminishing (or elimination) level and a level of cybersecurity.

The ideal situation would be represented by a zero risk level. Since this situation is not possible we will have to accept a residual risk which has to be as low as possible (figure 2).

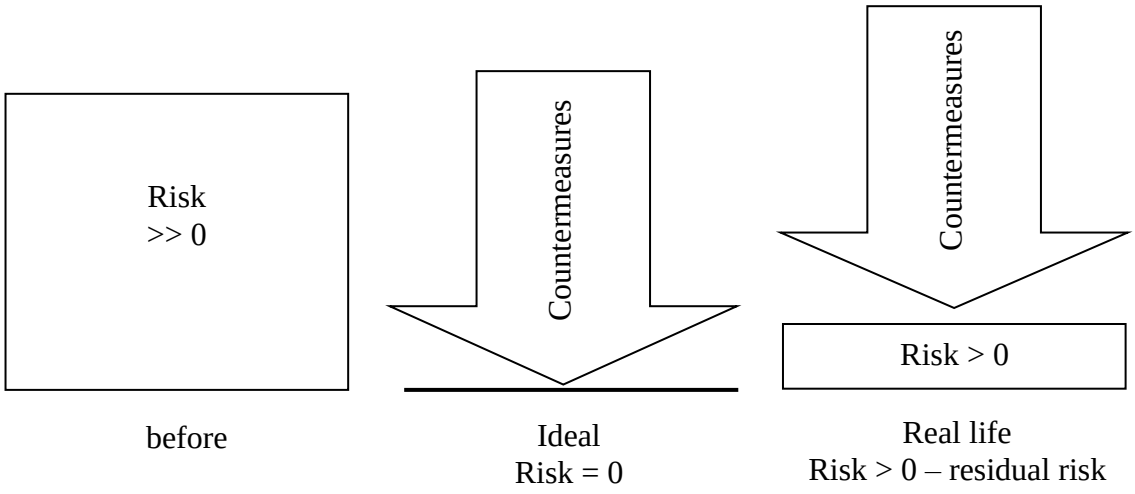

Figure 2. Residual risk

The number and implementation level of the controls meant to diminish risk are directly proportional with the financial resources allocated for this.

3. RISK MANAGEMENT

Starting from these ideas and based on the data that will be gathered from within the organization our aim is to determine an approach for cybersecurity.

As a new element we must mention the financial availability for ensuring cybersecurity.

Based on a simple questionnaire with the aim of defining the response to risk level the following questions have been proposed to organizations: Organization type (state/private), Activity domain (administration, education, constructions, commerce, manufacture, automotive etc), Computer number, **Security risk management status** (0 to 5, corresponding to next table – table 1) and **Existence of funds** to ensure cybersecurity (Yes/No).

For defining the security risk management status we will use the Microsoft methodology [4] which defines six levels for security risk management (table 1).

Table 1. The levels of security risk management

Level	Status	Description
0	Non-existent	The organization does not have the security policy well documented.
1	Ad-hoc	The organization is aware of the risk. The risk management efforts are done in a hurry and chaotic. Policies and processes are not well documented. Risk management projects are chaotic and non- coordinated, and the results can not be measured and evaluated.
2	Repeatable	The organization has knowledge about risk management. The risk management process is repeatable but immature. The risk management processes are not sufficiently documented, but the organization is taking actions in this sense. There is no formal training or communication regarding risk management, the responsibility being to the choice of the employee.
3	Defined	The organization adopts a formal decision for implementing the risk management. The objectives and the ways of measuring the results are clearly defined. The employees are formally trained at a base level.
4	Manged	Risk management is well understood in all compartments and levels of the organization. There are well defined procedures of control and risk reduction. Efficiency can be measured. The personnel is trained. The allocated resources are enough. The benefits are visible. The risk management team work to permanently improve the processes and the instruments they use. A great deal of the risk evaluation processes, of control identification, of cost-benefits anlaysis are non-automatic (manual).
5	Optimized	The organization has committed significant resources to security risk management, and staff members are looking toward the future trying to ascertain what the issues and solutions will be in the months and years ahead. The risk management process is well understood and significantly automated through the use of tools (either developed in-house or acquired from independent software vendors).

Source: http://technet.microsoft.com/en-us/library/cc163143.aspx

The subjects that have filled in the questionnaire belong to small organizations (accounting firms, schools, small manufacturing companies etc.) that have a low number of computers and big organizations (state financial control) with a number of over 25000 computers.

The most important role in positioning the organization in a favourable level is represented by the business owner – he/she will define the acceptable risk level and funds approval.

Involving the organization manager / business owner in filling in the questionnaire has led in a few cases to slight modifications of the answer, he/she having the tendency to raise the status and responding with “Yes” to questions referring to fund allocation, this being not in line with the replies of the specialty personnel that is involved in implementing security. The answers of specialty personnel have been taken into consideration.

Overall, from the total number of participants, 77% have responded that there are enough funds while 23% have responded the funds are not enough (figure 3).

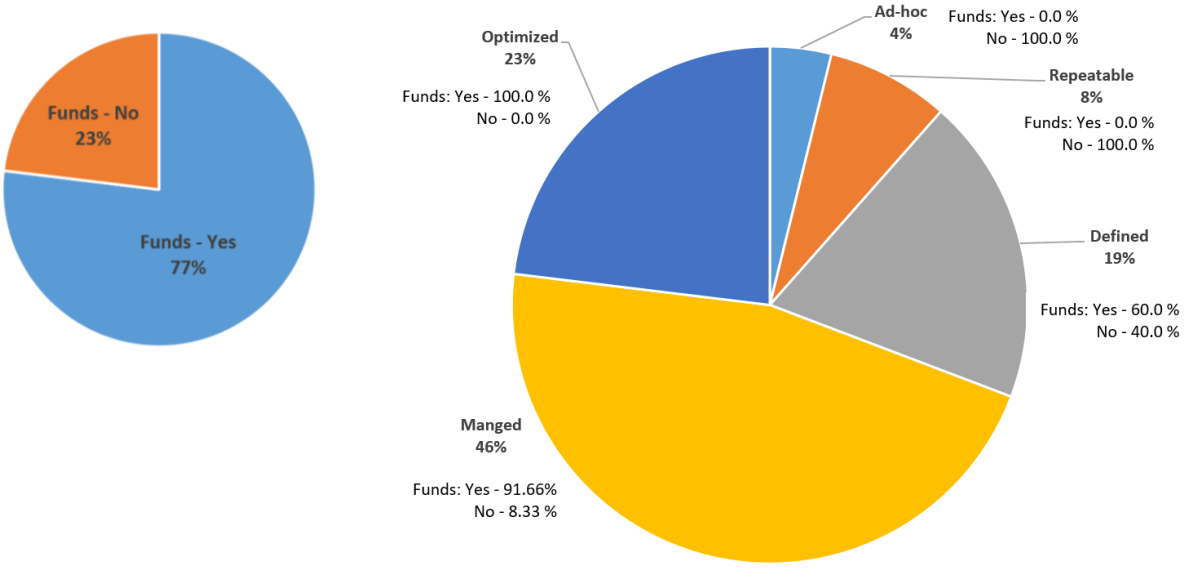

Figure 3. The levels of security risk management si suficienta fondurilor

From figure 3 we can easily notice that the organization that have achieved an optimized security risk management level (23.0%) have enough funds available – 100.0%. In this category we include very large organizations (state financial control, automotive, software product, aerospace, railway etc).

The organizations that have indicated a managed security risk (46.00%) tend to high values when answering the questionnaire questions related to the existence of funds – 91.66% declare there are enough funds while 8.33% declare the funds are not enough. In this category we find organizations from state administration, companies from industrial production, trading companies etc.

Organizations that have indicated a defined risk management level (19.00%) declare they have sufficient funds – 60.00% while 40.00% declare the funds are not sufficient. This category is represented by companies in industrial construction, trading companies and educational institutions – schools, highschool and even regional universities.

Organizations that have a repeatable risk management level (8.0%) or ad-hoc (4.0%) declare the funds are not enough to ensure cybersecurity. This category is represented by small and medium sized companies from industrial constructions, consultancy, accounting, schools in suburban areas.

It is worth mentioning that corrections have been made in what existing funds are concerned due to the different responses that have been received from the organization manager / business owner and the personnel responsible with ensuring cybersecurity.

To sum up, we can distinguish three approaches in ensuring cybersecurity: minimal security, optimal security and imposed security.

4. MINIMUM SECURITY

This risk analysis is done especially within large companies and eventually within medium companies. Small companies have no specialised personnel and no money to pay for such evaluation. Nevertheless a minimum of security measures must be taken.

A minimum security level is represented by level 0, 1 and 2 from the above table (table 1). A hard to manage situation is the one in which the business owner is not aware of the cybersecurity risks. We could say that we have a special risk – the risk of not understanding risk. Based on the principle that something cannot happen in a certain organization no or very little investments are done.

It is obvious that some organizations – startups – will not have sufficient funds to allocate to security. These prefer to invest in the production area and postpone the security specific investments. Security investments are limited to purchasing from a security vendor antivirus applications (sometimes without internet security components) or take specific freeware applications.

In the case in which an insufficient amount of funds is allocated to tackling potential threats, the feeling of at least something was done' arises and it is enough.

Only when a loss causing event occurs the need for cybersecurity will be taken into account and level 3 in the table is achieved – Defined. A minimum level of security will not generate adequate security.

5. OPTIMAL SECURITY

If in order to obtain an optimal level of security one must financially invest in controls, the following question arises: How much shall be invested in security?

Following the completion of the second stage in Risk management cycle – Conducting decision support, an amount of funds that needs to be invested in controls will be obtained.

In specialty literature [6] a cost/benefit analysis of 20/80 (figure 4) is specified.

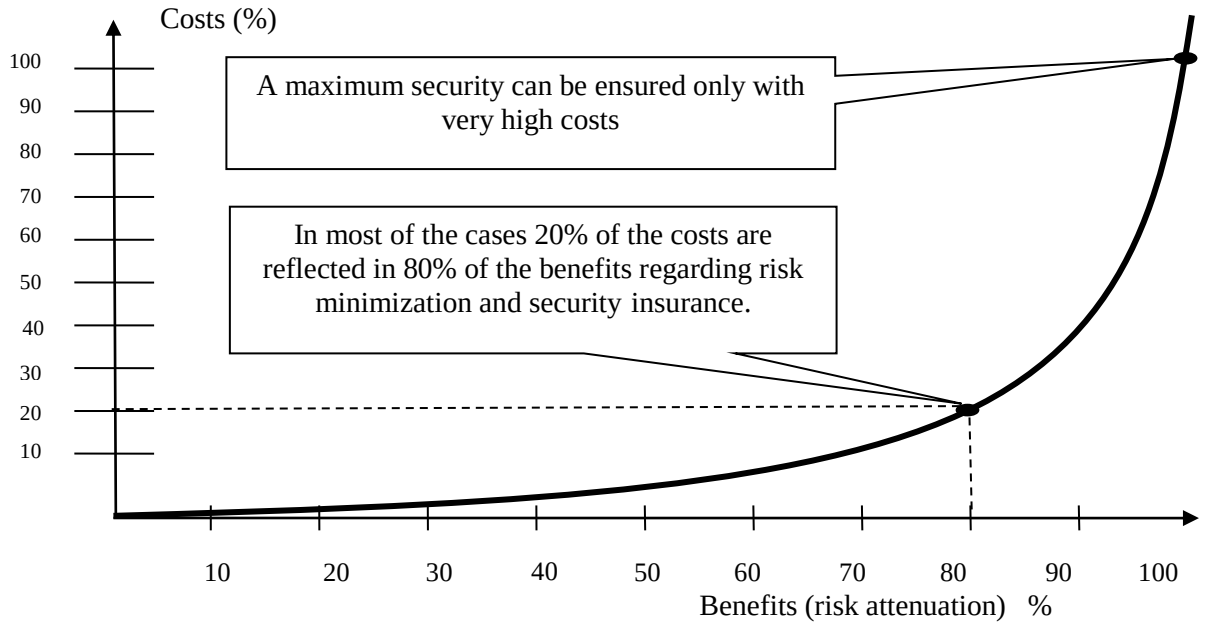

Figure 4. Cost/benefit of security

In other words if from the total of the amount resulted in the stage of Conducting decision support one will invest only 20%, the organization will have a coverage of 80% in risk diminishing.

This situation is common in medium and large organizations that are placed on levels 3 to 5 from table 1 – The levels of security risk management.

6. IMPOSED SECURITY

Even if an organization is ensured by the security buffer offered by the cost/benefit analysis (figure 3), Allocated sum (As) is less than Calculated sum (Cs) for implementing controls. In this situation we need to take into consideration and discuss about a financially imposed security – lack of funds for covering implementation costs.

There are two possible ways to overcome this (figure 5):

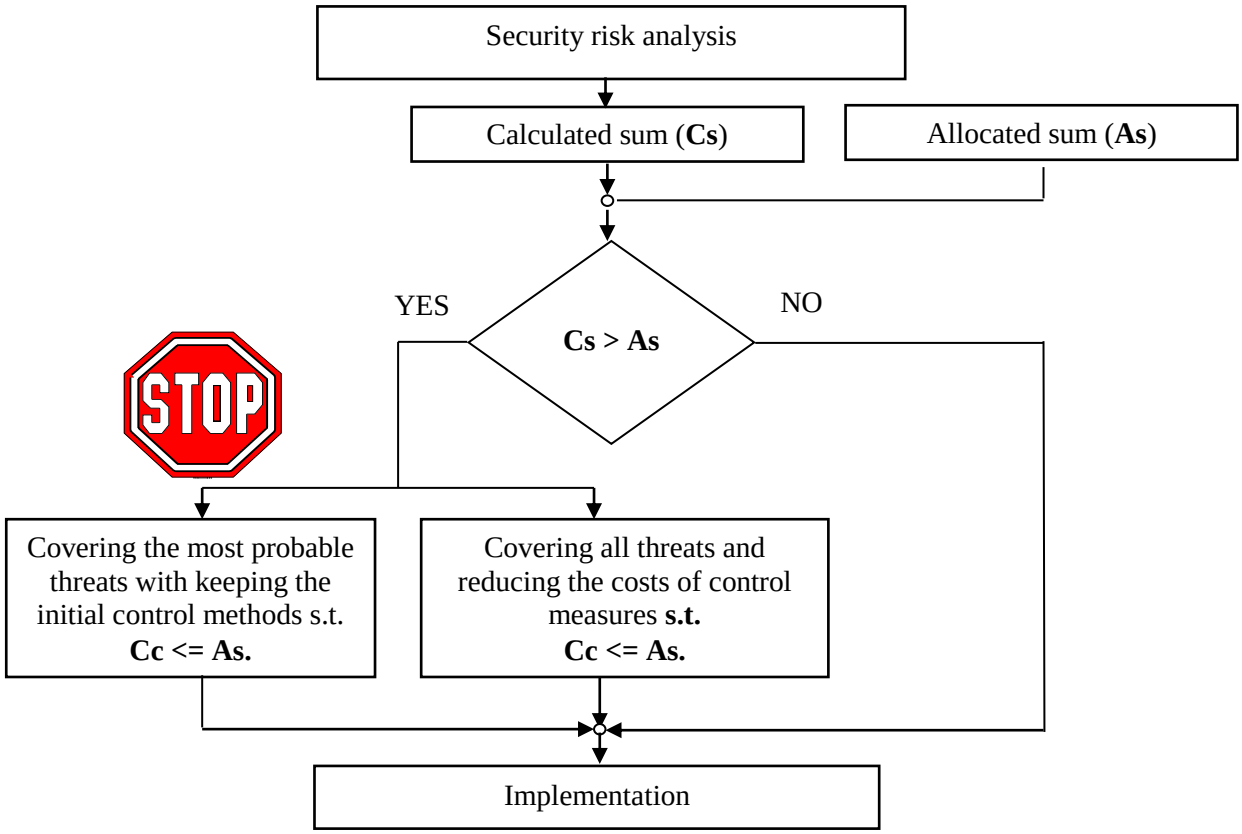

Figure 5. Imposed security (financial)

The fact that company managers are hard to be convinced to invest in something that doesn;t bring immediate profit is very well known. And when they are convinced about the necessity of the sums for ensuring security, the alloted sums are under the imposed ones. In these conditions a security whose expenses should not exceed a certain limit must be ensured. We can talk about a financial imposed security. The alternatives of solving this situation are two:

- covering the most probable threats by keeping the initial control methods;
- covering all threats and reducing the costs for control measures.

The first measure will allow a maximum of security for certain threats but will leave partially or totally uncovered other threats.

The second measure will impose reducing the expenses necessary for ensuring controls in order to cover all the possible threats. This could reflect in the modification and configuration of the control measures.

For example, two uninterruptible sources APC UPS of 350VA will not be bought for the price of 95 a piece for two computers, but a single APC UPS source of 650 VA at 140 a piece.

The saving is of 50 (95 x 2 – 140 = 50). In this case though, the two computers will have to be powered from the same uninterruptible source by extending the power cables or by placing them very close, with the acceptable reduction of the initial maintenance time for both computers.

7. CONCLUSIONS

For ensuring cybersecurity the organizations must prevent, detect and respond to threats. That means:

For prevention – Correct and optimize the selection of controls, update hardware and software, quickly adapting to changes.

For detection - Control of information from the organization, traffic filtering, analysis of alert messages.

For responding - Adoption of appropriate measures for events, adequate personnel training and communication of changes.

Prevention, detection and response to malicious events will be more effective if they focus on people, processes and technologies.

For financial reasons, the adoption of security measures will be difficult. Large firms have sufficient funds, while small firms do not have sufficient funds. Sufficient funds will allow covering all risks and the continuous development of the business. Insufficient funds will leave uncovered risks and the existence of the danger of business discontinuity or its closure.

Cybersecurity is difficult to quantify. One will never be able to say - now I am insured.

Do not overdo the security measures. Taking excessive measures will be annoying for employees and will have unwanted side effects for the business.

Minimal security is preferred instead of its absence.

The cybersecurity approach must be based on the following conduct: cybersecurity is a state that must be permanently maintained.

REFERENCES

1. https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html
2. https://siteefy.com/how-many-websites-are-there/
3. P. Day, CyberAttack, Carlton Book, 2014, pp. X.
4. http://technet.microsoft.com/en-us/library/cc163143.aspx
5. http://www.microsoft.com/technet/security/topics/policiesandprocedures/secrisk/default.mspx
6. P. E. Proctor, F. C. Byrnes, The Secured Enterpise. Protect Your Information Assets, Prentice Hall PTR, 2012, pp. 11.
7. https://www.nasdaq.com/articles/investing-in-cybersecurity
8. https://allcode.com/why-cybersecurity/