Shadow brokers V.s Artificial intelligence

Capstone Project

Course: Strategic Information Technology Planning, Organization, and Leadership

Instructor: Dr. Mona Sabuco

Student: Sadegh Bamohabbat Chafjiri

Student ID: 0588462

Date: Feb 26 2019

Preface

The motivation of this research is to realize role of Artificial Intelligence in future data governance. Human created wheel to run faster, create aircraft to jump higher. Therefore, it makes sense that he made Artificial Intelligence technology to think smarter and more complex. Artificial intelligence technology empowers managers to have a big and comprehensive vision and predict the future. Artificial Intelligence technology enables managers be ready for the nightmare stories before happening and convert them to the pleasant dreams. This power is useful for National Security Agency as a reference of compliance and regulatory as well. National Security Agency can be benefitted from this technology for decision making and updating policies in the smart manner. Artificial Intelligence is a technological opportunity for NSA to control and predict cyber security incidents before happening.

Table of Contents page

I. Executive Summary

This study investigates a serious data breach happened for Equation Group and some partners of National Security Agency rose by shadow brokers between 2015 and 2017. Then, study evaluates available solutions from what NSA did as a short-term or Kaspersky temporarily deployed to help NSA's investigation and then I recommend my solution.

A. Brief overview of the issue

An unknown cyber team called "Shadow broker" caused a serious data breach in NSA's partners in 2015. The breach included exploiting several vulnerabilities in NSA hacking tools. Among stolen data and tools, there was the list below:

1- instruction of NSA operations for hacking tools

2- several real codes to get inside the personal computers

3- expensive tools to control firewall configurations

Stolen data and tools could empower hackers to access several servers of NSA partners all over the words. In 2016, Kaspersky presented a report to NSA that Harold Martin, a contractor of Russian subsidiary of Kaspersky. In this report he was suspected to be in touch with Shadow brokers. NSA arrested him with lots of classified codes. In 2017, Shadow Brokers again exploited a vulnerability in Microsoft Windows and run a malware called "Wannacry" on victim's systems. Wannacry encrypted data on victims' computers and requested for money in bitcoins to give back victims' data.

B. Recommendations

1. Technology Map

There are 3 available recommendations in this study which I list in below:

Temporary solution: temporarily preforming a audit solution and get report from corrupt company to find guilty person

Fast Forward solution: arresting contractor of Kaspersky as a guilty person and banning corrupt company's product

Long term Solution: improving inadequate process, regulations and policies and deploying Artificial Intelligence to estimate probable security incidents in the future.

Kaspersky, partner of NSA, chose temporary solution and reported NSA about details of data breach procedure. It used its control tools to find connection between Martin and Shadow brokers. Then, NSA as an impacted agency, chose fast forward solution and arrested Martin and banned Kaspersky's tools. However, there was no guarantee that Kaspersky's contractor was only guilty person as if Shadow brokers committed another crime by a ransomware called "Wannacry" in 2017. It seems, Both NSA and its partner, Kaspersky, should think about a long term solution. They must remove all ineffective processes, regulations and policies and develop an audit analysis to keep confidentiality of processes. In this study, I developed my solution as a long term strategy by use of Artificial Intelligence technology and a modern audit analysis process. This system empowers auditors to predict probable security incidents in the future. Every solution has its own pros and cons which I presented in Table 1.

Table 1: available recommendations

Technology Map	Idea	Pros	Cons
Temporary solution	Performing audit solutions temporarily	Access to a report about incident to do a fast forward action	Data breach will happen again
Fast Forward Solution	Arresting contractor and banning products of corrupt company	Shaping Public Opinion about data breach	There is no guarantee that all members of Shadow brokers were arrested
Long Term Solution	Improving policies and Deploying Artificial Intelligence technology to predict incidents	predict data breach before happening and make audit system more effective and error-free	Time taking project, it is not good for short-term action

C. Summary of Value Results

1. Tangible factors

Both NSA as an agency and Kaspersky as a partner firm had common Tangible factors threaten and stolen by Shadow brokers. Both lost their confidential instruction data of operations for hacking tools, several codes, expensive embedded control tools in firewall. Moreover, security of servers belonged to worldwide partners of NSA were negatively impacted by Shadow brokers. Moreover, federal government's assets were impacted by this data breach including electronic voting system, governmental tools, applications, codes and infrastructure deployed in senate and federal bureaus which could easily impact private sectors in free market as well (see Table 2).

Table 2: Tangible factors impacted by data breach

Case	type of Asset
Confidential codes, hacking tools and backdoors	Software
control tools in firewalls	Software
NSA partners’ servers	Software and Hardware
players of economy	$/Bitcoins
governmental income	$/Bitcoins
governmental tools and voting system	Software and Hardware

2. Intangible Factors

Shadow brokers damaged credential role of NSA and its reputation in data security which is a vital intangible factor for this agency. Moreover, NSA can not use its previous techniques for penetrating purposes. In addition, Kaspersky lost its global leading position as a trusted consultancy for governmental purposes. Moreover, People can not more trust government about their data and also electronic voting system (see table 3).

Table 3: intangible factors impacted by data breach

Case	type of Asset
Insecurity concern of presidential election	Public Opinion/ Mentally
People concerns about their data privacy	Public Opinion/ Trustworthy
method and Data of operations for hacking tool	Public Opinion/ Mentally
Reputation	Public Opinion

3. Risk Analysis

Shadow brokers had a damaging impact on national security and the US business. Some of private sectors had to pay bitcoins to Shadow brokers to get back their own business data. NSA and Kaspersky could identify and control the source of risk. Their reaction was not effective to get back tangible assets. Revealing the method of governmental hacking tools harmfully impacted on gathering information from organized criminal groups. It might make illegal activities more invisible. Our recommended model reduce role of human by Artificial Intelligence system to assess and update inadequate regulations, policies and standards. Artificial Intelligence predict probable risks. Risk of vulnerability will decrease and this model can jail suspicious process in system and servers if they are not based on policies. Artificial Intelligence can decrease risk of aiding and abetting in the auditing system and control sabotage scenarios.

4. Sensitivity Analysis

Arresting Martin might have changed path of investigation process if Martin had some partners in crime as seen that Shadow brokers did another ransomware attack in 2017 called “WannaCry”. Although Kaspersky helped NSA to control uncertainty of output in risk analysis, it might initiate another uncertainty in input of analysis. hard-line decision of NSA about banning Kaspersky product could highly decrease uncertainty in input of model. In our model, Artificial Intelligence technology have 2 sources of input; available policies and the policies which audit managers make by prescriptive analysis on predicted issues. In our model distributed deep learning machine (DL) on Hadoop can learn from incidents and predicted incident. Therefore, there are few unpredictable incidents can impact risk analysis and decision makers can make policies more accurate.

D. Next Actions

In the first stage, NSA should arrange a team of 10 experienced audit managers. The audit team should investigate managerial issues and identify wrong decisions and discuss about probable conflict which can initiate similar issues in the future. NSA should select 3 experts among audit managers who are qualified for reporting purposes preferably the people have Certified Internal Auditor and Certified Information Systems Security Professional Certifications. They should provide a report to clarify model of cooperation which partners can have with NSA. The next action is to create a team of 10 technical experts. They must adjust and develop new codes, programs in a more reliable manner. They must replace infected or incomplete codes by secure codes. Then, This team of developers should configure a customized version of cloud services (Cloudera), operating system and distributed analytical tools on Hadoop. Developers can equip audit analysis tool to Artificial intelligence technology. NSA should arrange monthly sessions with contractors to check project progress and impact of updated regulation on partners and keep its role of problem solving for unpredicted cases. In other side, Kaspersky must follow specific policies, confidentiality and structural requirement in IT security market.

II. Introduction

A. Business Drivers

According to Coldewey (2017), a hacker team called “Shadow brokers” hacked Equation Group and stole classified information. The breach was discovered in 2016. Equation Group is a hacker group linked with different branches of NSA. Equation Group hack different platforms to gather information from specific targets for governmental purposes. Wall Street Journal was claimed that this breach had a foreign source and was lunched by Russian intelligence (Coldewey, 2017). It claimed that it is probable that Russian intelligence had enough time to impact presidential election as well. Wall Street Journal added that Russian intelligence exploited a software released by Russian branch of Kaspersky labs (Coldewey, 2017). This statement was confirmed by Edward Snowden on Twitter. However, NSA got suspicious that an insider had stolen the hacking tools. As a first reaction, Federal Government banned Kaspersky’s product for security concerns which means usage of softwares released by Kaspersky labs was not allowed in congress and federal bureaus more. In 2017, Shadow brokers committed their second crime and exploited a vulnerability in Microsoft Windows and hacked lots of systems in the world by a malware called “Wannacry” (Leonhard, 2017). Wannacry encrypted all information on victims’ systems and then owners of information had to pay money in Bitcoins to get back their information. Shadow brokers had less chance to sell NSA’s codes (Fingas, 2017). However, According to Domonoske (2016), Shadow brokers made a bidding model to sell valuable information of corporations to the highest bidder. In their bidding price model, losers of bid lost both their information and bitcoins. This game model was considered as a big cyber-extortion because only in one case they requested 1/15th of the all available bitcoins in the world which can negatively impacted macroeconomy. Therefore, not only Shadow brokers made one of the widest-ever security issue for NSA but also it was considered as a massive-ever cyber-extortion.

B. Scope of Business Case Analysis

1. Purpose of this Business Case

The purpose of this business case is to find a long-term solution against data breach. According to Rashid (2017), there is a big lesson for professions in this case that how the vulnerabilities in tools can impact whole organizational structure and waste the budget invested on other sectors for years.

In this section, I would like to discuss purpose of business case. As a major purpose, I try to integrate 2 non-additive approaches together. The first approach is that a governmental organization requires to update itself by first hand knowledge in cyber security industry while this kind of findings usually grow in a competitive environment of free-market. However, cooperating with private sectors which stay on cutting-edge of knowledge will increase risk of data breach as seen in Kaspersky labs's case. At first glance, this come to mind that it is a contrasting view to expect that NSA should cooperate with private firms to access the first hand knowledge and prevent them from data breach. However, It is not true because NSA can make, upgrade and follow the top organizational standards and policies and deploy high technology of automation to achieve both goals. This study will investigate available option which government has to achieve this purpose

2. Options Evaluated

As the first option, NSA can pick the decision which made in 2016. It banned product of Kaspersky in Government and senate and arrested guilty person. Let explain what was behind this decision. Kaspersky gave some reports of incident in detail to NSA to find source of breach. NSA imposed bans on Kaspersky's products. Kaspersky labs provided some reports in details even after imposed sanctions and empowered NSA by higher technology of monitoring to get a clue about incident. According to Blacklisted Kaspersky tipped NSA (2019) article, subsidiary of Kaspersky in Moscow could find a connection between a twitter message received from a contractor and shadow brokers. It revealed the role of contractor, Harold Martin, in this breach. In August 2016, he was arrested by federal agent with 50 terabytes sensitive data, codes and programs gathered over 20 years which can be considered as the available option for NSA. Kaspersky assistance believed that NSA strategy including investigators and monitoring system were not enough to catch contractor. It means Kaspersky's report was helpful for NSA's investigators (Blacklisted Kaspersky tipped NSA, 2019). Although Kaspersky reached a fast and appropriate audit solution to address the issue temporarily, it had not recommended any preventive action prior to the data breach which means the issue can happen again. Kaspersky did not give any serious reconsideration to modify inadequate internal process and policies which caused this corruption. In other words, lack of policies and compliance was the main problem of Kaspersky labs. This problem enabled Shadow brokers to exploit backdoors in NSA's hacking tools. It seems cooperation between NSA and outsiders needs to be essentially reconsidered by deploying a higher level of standards, policies and technology. Therefore, as a third option, NSA needs to perform fully assessment on its confidentiality requirement in case of outsourcing. It must be legally binding for partners to follow confidentiality policies. Moreover, NSA must put this requirement that its partners perform background check of employees and contractors case-by-case and evaluate risk of data breach for each project. It means Kaspersky must prepare a clearance report as well. This report should determine if company had any limitation in cooperation either technically or politically which forced by foreign governments or not. Clearance report should clearly answer that why this contractor was selected for NSA project. Moreover, Kaspersky must commit to give feedback for future projects constantly and make NSA aware of project procedure. For example, if Kaspersky is going to outsource a specific project with high level of confidentiality, it should first negotiate to NSA and confirm the eligibility of people who will get involved in the project. Then, NSA must perform risk analysis and consider risk of data breach. To achieve this purpose, NSA should use audit analysts to identify if there are potential compliance issues or not. Moreover, NSA should deploy artificial intelligence to perform prescriptive analysis and predict probable incidents occurring in the future. Artificial Intelligence technology can easily determine the probability of each incident and can recommend the best solution. Recommended solution can update previous policies and mitigate risk of data breach. Audit managers can report updated compliance to decision makers to confirm. In this approach, decision makers will be empowered to assess risk of outsourcing for various projects. To be eligible for getting projects, NSA's partners must follow Artificial Intelligence platform and auditing analysis. To achieve this aim, NSA and its partner must agree on a model to do a course of actions in some steps:

1- setting up a seri of sessions
2- analyzing confidentiality, integrity, and progress of projects professionally
3- renewing their methodology of collaboration, standards, policies, and control tools
4-creating a team of audit managers
5- producing audit progress reports
6- reporting faults and invisible issues

7- deploying Artificial Intelligence, distributed deep learning (DL) and Hadoop for monitoring and controlling purposes.
8- having plan B of cooperation to cooperate with other available firms and estimate the cost of technology replacement if Kaspersky continue corruption

3. Business Case Analysis Process and Resources

To achieve aforementioned plan, NSA should do Return on Investment analysis (ROI) to measure value and requirement, manage process and optimize expertise (see Appendix A-2). NSA should prove that in how many fiscal years, investment on Artificial intelligence and audit management will be back. Moreover, NSA should arrange a seri of meeting with Kaspersky's board of directors and let them know that data breach has a serious cost for the corrupt companies and there is a less chance for them to get back, even if they would have accepted a part of cost. NSA should arrange a team composed of audit managers to control both process and confidentiality of projects in partner side. Moreover, NSA should apply Artificial intelligence technology to investigate accuracy of regulations and policies. By deploying Artificial Intelligence, NSA will be analytically empowered to check process, regulations and policies in partner side and makes the optimize decision. In addition, by getting a weekly feedback from audit managers, NSA can confirm that progress in projects meets the compliance and regulations. Moreover, NSA should be in touch with another company for urgent replacement of corrupt company in case.

III.Analysis

In this section, I evaluate key assumption of analysis and then I perform a 5 pillars model suggested by Murphy and finally I present the value analysis. However, before starting, I would like to conduct a survey on case. The hacker team stole NSA classified data, hacking tools and put all of them on internet in 2015 and released a ransomware called "Wannacry" in 2017 which exploited a security hole in Microsoft windows to infect computers. Scale of data breach and the severity of the damage has been so high that NSA banned usage of Kaspersky product in government and arrested Kaspersky's contractor. In this business case, NSA's decision can not be considered as a long term solution because there is no guarantee that the next company providing governmental tools can keep its company away from this kind of issues. To find a way out of this situation, our analysis shows that NSA should be notified of lack of updated policy, regulations and audit control. Moreover, NSA should upgrade its audit system analysis by Artificial Intelligence Technology to predict incidents.

A. Key Assumptions of Analysis

The key assumption of this study is that hackers' interests changed. They prefer to target corporation rather than ordinary people. According to Study highlights growing criminal interest (2017), although number of attacks decreased from 1.5 million in 2016 to less than 1 million in 2017, cyberattacks became more advanced and complex. Despite the progress which firewalls had in detection in 2017, rate of successful attacks considerably increased. Moreover, hackers prefer to modify existing malware rather than creating a new family of malware. Number of detected ransomware families declined from 62 in 2016 to 38 in 2017 while number of detected modifications in 2017 almost doubled in comparison with 2016. Nearly two thirds of infected business by ransomware lost important or whole data in 2017. Therefore, key assumption of this solution is that cyber security analysts are facing with more professional hackers targeting corporation and stealing strategic data more than hackers infecting personal computers.

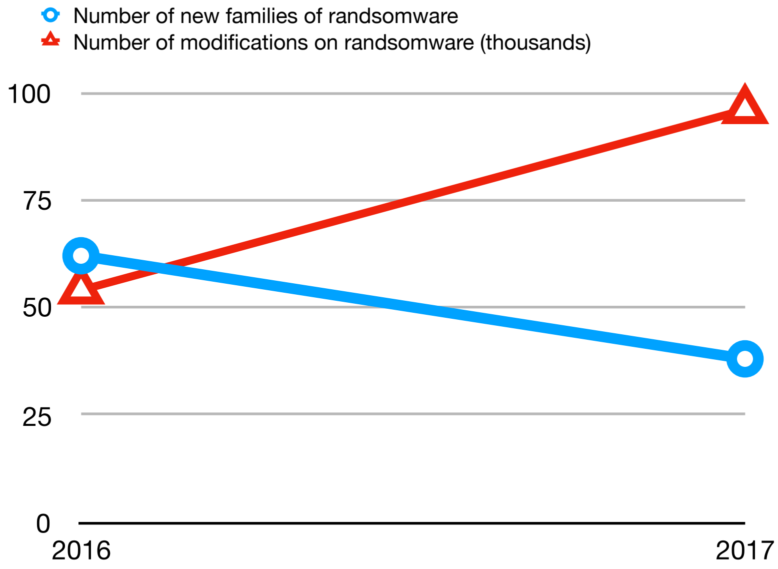


Fig 1. Comparing ransomware vulnerability in 2016 and 2017

B. Analysis of the 5 Pillars

Regarding to Murphy's method, a good model should apply to checkpoints of 5 pillars in below:

1- Strategic Alignment Check: our model try to draw decision makers' attention to develop organizational structure, process and policies and deploy an integrated audit process to confirm confidentiality of project. In this model, Audit managers can ruled NSA's partner to upgrade tools and technology which are used for classifications purposes. To achieve the project confidentiality as a strategic goal, My model benefitted from Artificial Intelligence clustering. Artificial Intelligence makes model mistake-free and upgrade inadequate process, regulations and policies based on prescriptive analysis and classification of information or tools. Moreover, Artificial Intelligence technology decreases risk of informal attack to corporation. These days, informal attacks have complex scenarios against which formal techniques such as firewalls, Anti-malware do not work properly. Therefore, Artificial Intelligence technology adds a considerable strategic value to organizational model.

2- Business Process Impact: The model empowers NSA control system to keep audit analysis available for more process. Different Supervisors or Audit managers can investigate accuracy of security process from different perspectives. Supervisors can add their feedback anonymously and send alarm if something is against protocols and policies. It decreases conflict between NSA policy and internal process of contractors and make contractors aware of risks automatically. Therefore, model has a positive impact on process.

3- Architecture Check: our model recommended four steps. The first step is to identify issue resulted by prescriptive analysis and prediction. In the second step, audit managers investigate predicted issue and report it to board of directors. In the third step, board of director should choose an appropriate response and confirm or reject if update of process, policies or regulations is required and then audit managers should control the incident behavior based on new policy. The input of this model is a security issue and output of model is a solution in a timely manner. The model can suggest a comprehensive architectural solution and upgrade the previous architecture based on requirement of probable incident. In this architecture audit managers have supervisory role to report incident to the decision makers and make contractor aware of corruptions.

4- Risk Check: implementation of artificial intelligence technology is important and the potential risk is that Artificial Intelligence technology could not meet policy requirement specially when there is a limitation on budget. Moreover, there is this risk that hackers want to arrange a social engineering on audit managers to get access to Artificial Intelligence administration. To mitigate this risk the project auditors should be anonymously connected to project tools.

5- Direct Payback Check: This model definitely brings financial benefit by cost saving of the projects by keeping confidentiality of governmental process. Data breach can be considered as the highest cost issue for a security agency. Therefore, investment on the integrated solution will be essential to keep the agency's leadership role. NSA should perform Return on Investment analysis and Earned value management to prove that in how many fiscal years, the amount of investment on Artificial intelligence and audit management will be back.

C. Value Analysis Results

1. Top Benefits

The NSA will get advantage of project confidentiality in a clear process of audit analysis. Artificial intelligence technology supports an anonymous workplace for auditors. It can isolate audit managers and contractors. By artificial intelligence, the model efficiently enable auditors to make a decision about risk level of outsourcing based on different parameters. Artificial Intelligence can provide an audit management service 24/7 and help managers to check the logs every time and everywhere even if they are living in a place with different time zone. Updating the policies will be easier than the past and only by initiating Artificial Intelligence inputs.

2. Risk Analysis:

In section I, I presented tangible and intangible factors. Moreover, this vulnerability had a domino effect on other sectors, market value and domain of marketing. According to Lawrence (2017), Some businesses are negatively impacted by security holes rose by this vulnerability in governmental hacking tools. This vulnerability was “10 times worse” than the previous major vulnerability called “Heartbleed bug”. Heartbleed bug had negatively impacted two IT giant Yahoo and Amazon (Lawrence, 2017). All pieces of evidence showed that Shadow brokers had a harmful impact on national security and market of private sectors. In other words, other players of economy who were less familiar with IT security were surprised by this data breach. Some of them were forced to buy bitcoins and pay to Shadow brokers to get back their own data. Because of classification considerations and worldwide scale, there is already no available data about the dimension of impact and costs in the world. However, by rule of thumb, this vulnerability may have 400,000 victims in the world. Consequently, it adversely impacted governmental income earned from private sectors. Based on story of case-study, NSA and Kaspersky could identify and then control the source of risk because their quick response has no positive impact on tangible factors which both lost (see fig 2).

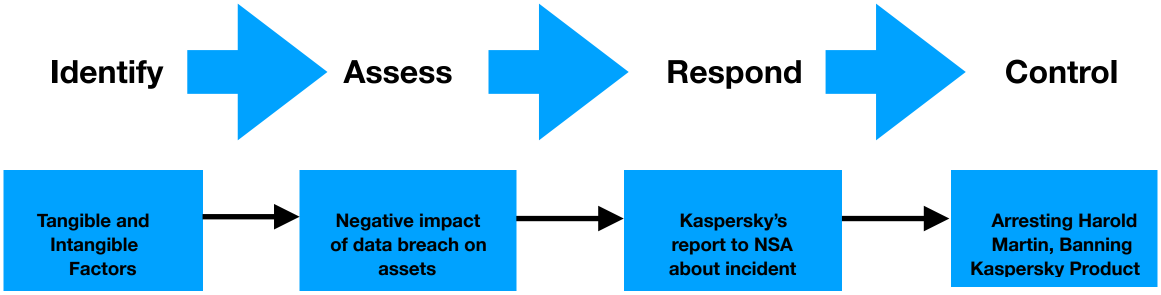

Identify
Assess
Respond
Control
Tangible and Intangible Factors
Negative impact of data breach on assets
Kaspersky's report to NSA about incident
Arresting Harold Martin, Banning Kaspersky Product

Fig. 2: Risk Analysis

Moreover, revealing the method of governmental hacking negatively impacted NSA strategy of gathering information from organized criminal groups. It might empower organized criminal groups to continue their illegal activities more invisible. Instead, our recommended model limits the role of human to only managerial level and suggested an Artificial Intelligence system to assess the regulations, policies and standards (see fig 3). Artificial Intelligence can be loaded more than human to check all issues and think about probable risks. Risk of vulnerability and data breach in this model will be mitigated by jailing the suspicious processes if they are not based on policies. Artificial Intelligence can mitigate risk of aiding and abetting as well and disturb sabotage scenarios.

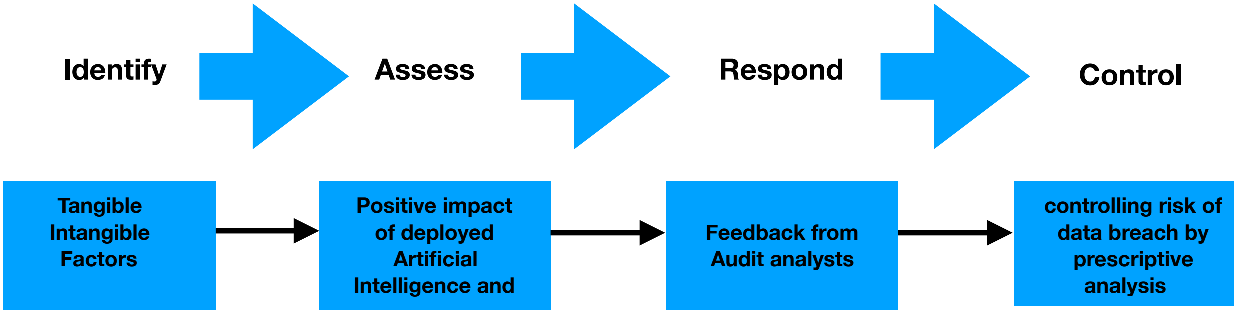

Identify
Assess
Respond
Control
Tangible Intangible Factors
Positive impact of deployed Artificial Intelligence and
Feedback from Audit analysts
controlling risk of data breach by prescriptive analysis

Fig. 3: Risk Analysis of recommended model

3. Sensitivity Analysis

The selected strategy of Kaspersky to use its monitoring tools tended to a fast reaction of federal government. NSA arrested Harold Martin. However, that strategy did not enable NSA to have an accurate vision. In other words, the strategy did not investigate role of invisible factors in that crime. Arresting Martin might disrupt the process of accurate investigation, If Martin had some partners in crime.

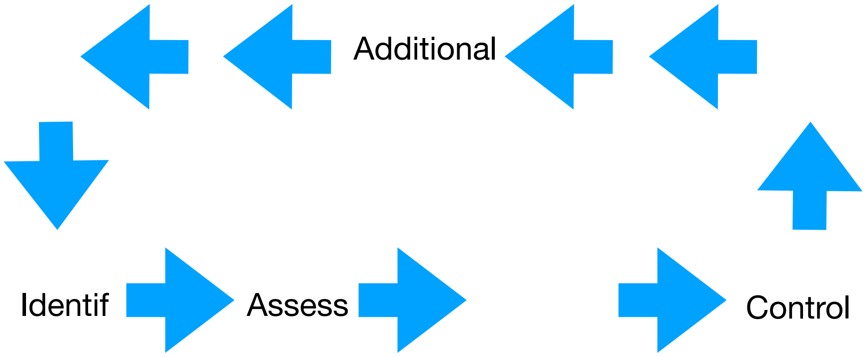


Fig 4: Sensitivity Analysis

According to Lawler (2017), Shadow brokers did another ransomware attack in 2017 called "WannaCry". This ransomware used a vulnerability in Microsoft Windows operating system and encrypted data. It means more crime partners were involved in Shadow brokers project. Although Kaspersky strategy was considerably helpful to control uncertainty in output of risk analysis, there was this potential that its strategy initiated another uncertainty in input of incident (see Fig 4).

Hopefully, hard-line decision which NSA made about banning Kaspersky product could highly reduce dependency of input to output of model in Fig 4, specially, when NSA found the second vulnerability. As a result, the best strategy in sensitivity analysis of hard-line reaction was what NSA did and banned all risky tools in senate and federal bureau.

In my recommended model, the solution is based on prevention before incident. In our model Artificial Intelligence technology can feed from 2 sources of policies for auditing analysis; available policies derived from previous issues and also new policies derived from audit managers views on estimated issues predicted by Artificial Intelligence process. Artificial intelligence can learn current policies and predict future incidents. If there is any conflict between current and updating policies, Artificial Intelligence can inform audit managers. In recommended model, every change in output has no direct impact on input and can be memorized and analyzed by distributed deep learning machine (DL) on Hadoop. So, system is not seriously impacted by unpredicted issue. In other words, there are few unpredicted incidents which Artificial Intelligence needs to experience in practice and decision makers can make policies for probable incidents and let Artificial intelligence learn them based on knowledge produced by prescriptive analysis and big data analysis. By distributed deep learning (DL) on Hadoop, technology empower decision makers to be smarter and give the comprehensive solutions for incidents (See Fig 5).

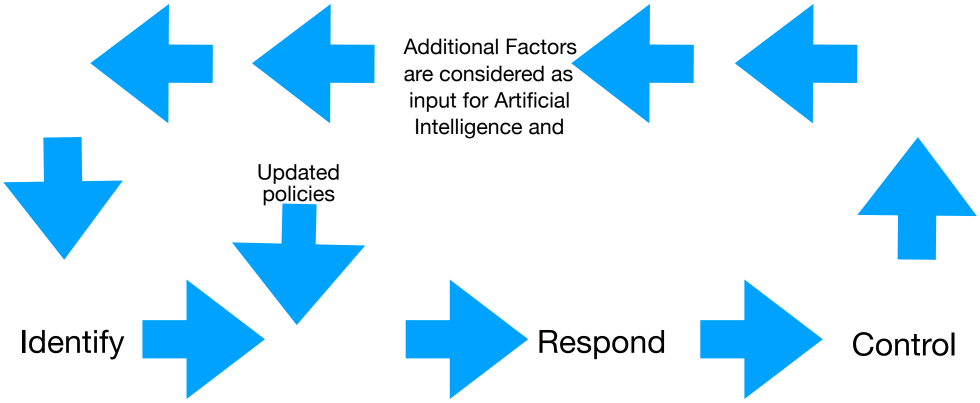

Additional Factors are considered as input for Artificial Intelligence and
Updated policies
Identify
Respond
Control

Fig 5: sensivity Analysis of recommended model

D. Financial Analysis

Financial analysis can estimate required budget which model needs initially (see Table 4). Moreover, It can determine what type of Capex and Opex are required. This analysis is a good metric to compare initial cost which NSA should pay to make the new platform and can give a good measure that how much cost saving this model will bring for NSA. It can guarantee stability of system and can warrant investment. By financial analysis, government can estimate by how many fiscal years they can get back amount of investment.

Table 4: Financial Analysis

Total cost of software and R&D			
Deployed Technology	**Cost per unit (USD) or Year**	**Number of units/ members**	**Total cost (USD)**
Research and Develop team	100,000	10	1,000,000
Customized cloud services	25,000	1	25,000
Prototype Implementation of Artificial intelligence	25,000	1	25,000
Product Release	1,00,000	1	100,000
Customized operating system	5000	10	50,000
Customized analysis tools and Hadoop	5000	10	50,000
Total			1,250,000 USD

Total cost of Hardware and Certificate			
Deployed Technology	**Cost per unit (USD) or Year**	**Number of units/ members**	**Total cost (USD)**
Certified Internal Auditor Certification	500	10	5,000
cloud servers	3,000	500	1,500,000
OTP based dongle flash drive	1,000	10	10,000
Customized secure Cell-phone	10,000	10	100,000
Total			1,615,000 USD

E. IT Governance Plan

In terms of IT governance plan, NSA as a reference of compliance and regulations should be aware of its leadership role in IT security in the world. NSA should proactively get consultation from private sectors. It enables NSA to be aware of new findings in cyber security area and gives more metrics to update inadequate and outdated frameworks. The main outcome of IT-governance plan in this model would be to integrate all security solutions in Artificial Intelligence technology and give an easier vision to audit analysts. NSA should identify opportunities and threats of deploying Artificial Intelligence in a security system and regulate Artificial Intelligence solutions.

IV. Next Actions

In the first stage, NSA should arrange a team of 10 experienced audit managers in its agency. Audit managers should have multi-factor problem solving skills. This team should be selected from trustworthy managers who have done higher sensitive and classified projects before. The audit team should investigate managerial issues and identify wrong decisions and discuss about probable conflict which can initiate similar issues in the future. In other words, they should first correct the mistakes in structural and managerial level and then focus on technical side. NSA should select 3 experts among audit managers who are qualified for reporting purposes preferably the people have Certified Internal Auditor and Certified Information Systems Security Professional Certifications. They should provide what model of policies and organizational structure partners and contractors must follow to cooperate with NSA.

The next action is to create a team of 10 technical experts from other departments which were not involved in this case. They must adjust and develop new codes, programs in a more reliable manner. They must replace infected or incomplete codes by secure codes and patches to protect governmental system against next cyber attacks. Then, This team of developers should configure a customized version of cloud services (Cloudera) and Hadoop, operating system and distributed analytical tools for agency purposes. Developers should equip audit analysis tools to Artificial intelligence technology. Artificial Intelligence technology can learn policies, roles and regulations and should have this capability to give root access to 10 audit managers to control project process anonymously. Deployed Artificial intelligence should update policies by audit managers' confirmations. Artificial Intelligence should get feedback from output of each project to update policies. Artificial Intelligence should learn from predicted incidents which prescriptive analysis estimated. NSA should arrange monthly sessions with contractors to check project progress and impact of updated regulation on partners and keep its role of problem solving for unpredicted cases.

On the other side, Kaspersky should think more about multi-variant characteristic of IT security market. It should be notified of IT security market which is not based on supply and demand structure. This business follows specific policies, confidentiality and structural requirement to be successful. In this case, Kaspersky should provide requirements of confidentiality based on Client's sensitivity analysis, not only its own profit. Kaspersky by Changing the approach may again open more opportunities toward itself.

A. Your conclusion

In this project we introduced a data breach known as "Shadow brokers" impacted Equation Group and NSA's partners between 2015 and 2017. We investigated the short-term decisions which NSA made to address the issue. We analyzed their solution was not effective in risk analysis methodology. Then we recommended our solution by employing audit analysts and deploying artificial intelligence to predict and regulate incidents before happening.

B. Next steps

NSA should continue its research on Artificial intelligence technology and sponsor more Research and develop (R&D) projects to reduce role of human where machine can do better and make organizational process mistake-free. The main part of this project would be related to functions of ETL and prescriptive analysis on big data. The best start point to approach the best function would be sponsoring world-wide think tanks. Think tanks can think and recommend efficient functions and models. Moreover they can study method of cooperation between different sectors of government and private sectors. Research institutes can generate academic results to answer serious questions about confidentiality and of course is not enough. Moreover, It is vital to think what is a security agency's threshold to identify a high risk out-sourcing and low risk out-sourcing and what issue can be predicted if NSA cooperate with private cybersecurity firms. However, it is clear that some experts basically disagree with the idea of outsourcing which I disagree on their opinion. I have a doubt here if internal standards could negatively impact effectiveness of organizational standards or not. I guess they should answer to this challenge if demanding internal effort with policy might not increase risk of vulnerabilities as well? because reaching to fewer experts' views in IT security department means making fewer modifications and making fewer modification causes having more vulnerabilities.

Bibliography

Leonhard, W. (2017). Shadow brokers threaten to release even more NSA-sourced malware. *InfoWorld.Com,*Retrieved from

https://0-search.proquest.com.library.ggu.edu/docview/1899382066?accountid=25283

Lawrence, D. (2017). Seriously, beware the 'shadow brokers'. *Business Week*, 34. Retrieved from

https://blendle.com/i/bloomberg-businessweek/seriously-beware-the-shadow-brokers/bnl-bloombergbw-20170508-751d553cb7b?sharer=eyJ2ZXJzaW9uIjoiMSIsInVpZCI6Im15N21laHIiLCJpdGVtX2lkIjoiYm5sLWJsb29tYmVyZ2J3LTIwMTcwNTA4LTc1MWQ1NTNjYjdiIn0%3D

Lawler, R. (2017). 'Shadow brokers' threaten to release more hacking tools in June. Retrieved from

https://www.engadget.com/2017/05/16/shadow-brokers-nsa-june/

Rashid, F. Y. (2017). Shadow brokers lessons: First, don’t panic. *InfoWorld. Com,* Retrieved from

https://0-search.proquest.com.library.ggu.edu/docview/1889708556?accountid=25283

Fingas, J. (2017). 'Shadow brokers' give away more NSA hacking tools.

Retrieved from

https://www.engadget.com/2017/04/08/shadow-brokers-give-away-more-nsa-hacking-tools/

Domonoske, C. (2016). *'Shadow brokers' claim to have hacked the NSA's hackers*. Washington: NPR. Retrieved from

https://0-search.proquest.com.library.ggu.edu/docview/1812040612?accountid=25283

Coldewey, D. (2017). Russian intelligence reportedly breached the NSA in 2015, stealing cybersecurity strategy. Retrieved from

https://techcrunch.com/2017/10/05/russian-intelligence-reportedly-breached-the-nsa-in-2015-stealing-cybersecurity-strategy/

Blacklisted Kaspersky tipped NSA on security breach: media (2019) Retrieved from

https://phys.org/news/2019-01-blacklisted-kaspersky-nsa-breach-media.html

Security Breach and Spilled Secrets Have Shaken the N.S.A. to Its Core, Retrieved from

https://www.nytimes.com/2017/11/12/us/nsa-shadow-brokers.html

Study highlights growing criminal interest in corporate targets. (2017). *Networks Asia,* Retrieved from

https://0-search.proquest.com.library.ggu.edu/docview/1974851775?accountid=25283

Appendices

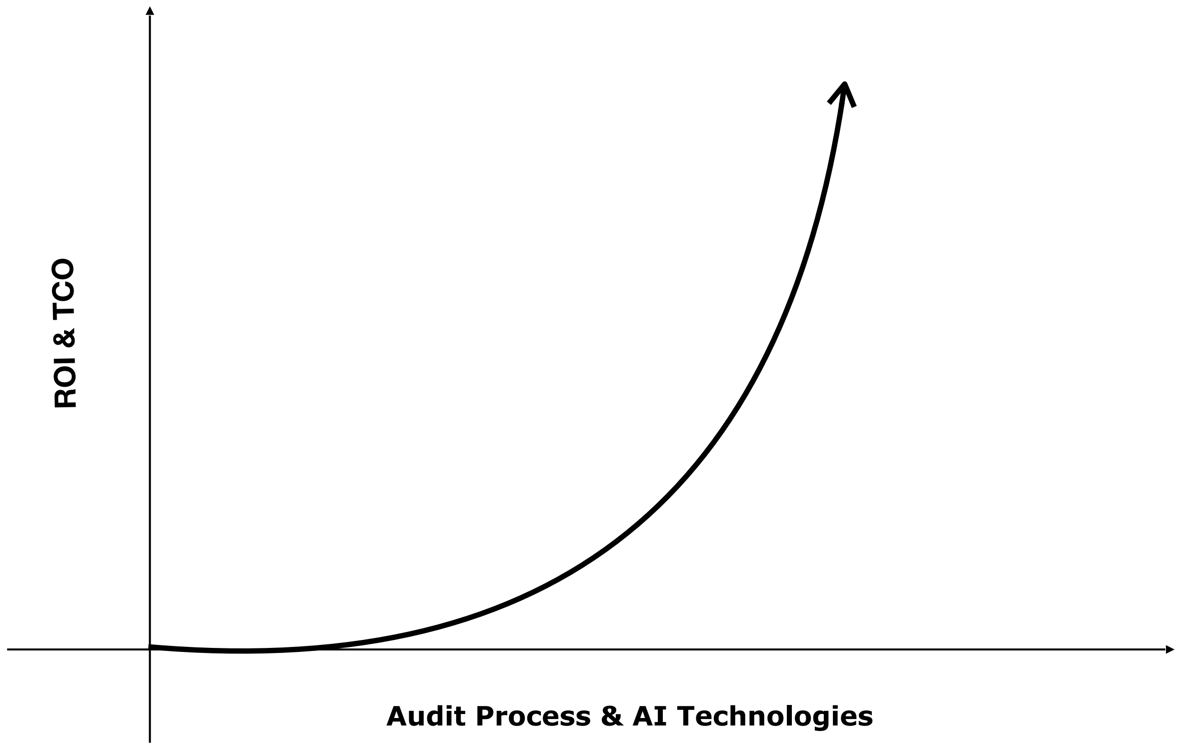
Appendix A-1: For more research, read Haas' Laws of Operation Security

Fist Law: if you don't know the threat, how do you know what to protect

Second Law: if you don't know what to protect, how do you know you are protecting it?

Third Law: If you are not protecting it (the information), the Dragon wins!

Appendix A-2: ROI (Return on Investment) and TCO (total cost of ownership) are considered as value which grows with progress of audit process and AI technology exponentially because AI technology reduced time of process logarithmic.


ROI & TCO
Audit Process & AI Technologies