Security Operating Center: The Solution of the Corporation Level Business

Capstone Project 2

Course: Strategic Information Technology Planning, Organization, and Leadership

Instructor: Dr. Mona Sabuco

Student: Sadegh Bamohabbat Chafjiri

Student ID: 0588462

Date: April 14 2019

Table of Contents page

I. **Executive Summary**

In this capstone project, I recommend a structural solution based on SOC unit to Under Armour company.

A. Brief overview

Firstly, I introduce the data breach exploited on MyFitnessPal, Under Armour's fitness application in 2018. This data breach impacted 150 million customers' account information including usernames and hashed passwords. I present the Security Operating Center (SOC) as the suitable strategy of IT security and compliance for corporation level business. I present Under Armour's current place in the IT security area and compare it with Adidas's situation, and then I compare SOC unit with Supervisory Control and Data Acquisition (SCADA) as an industrial monitoring system. By using SWOT and 5 pillar analysis, I show the SOC unit is a better solution for Under Armour. In addition, I review why building an SOC unit is necessary for an enterprise-level business like Under Armour. Furthermore, I recommend an operating plan which includes marketing, manufacturing, and department. I discuss the value and the risk analysis of the solution. I evaluate how the SOC unit reduces the severity and the frequency of the threats. It enables an admin to improve the functionality of threat detection and remediation. I discuss how the company meets the business requirement in the open-door management style by having an iterative IT governance plan. Finally, I will perform financial analysis to determine Return of Investment and profit and loss statement.

II. **Analysis of the company**

In this section, I introduce Under Armour, an American footwear and sport company. The global headquarter of the company is located in Maryland, and it has subsidiaries in several states and countries.

A. History of the organization

Under Armour can be considered a successful business in the sport industry in recent years. According to Under Armor (2019), its annual revenue was over 5.2 billion dollars in 2018. Its net income experienced a decrease of 46 million dollars and its operating revenue fell nearly 25 million dollars. However, Under Armour experienced a growth in total assets of 4.3 billion dollars. Under Armor can be categorized as a corporation level business because it already has 15,800 employees. According to Dye (2018), Under Armour paid 475 million dollars to own MyFitnessPal application, a nutrition and

sport application, in 2015. The main change in managerial level was that Albert Lee and Mike Lee, the founders of MyFittnessPal left Under Armour in early 2018. This application provides a fitness tracking and nutrition service. It enables the users to check their daily burned calories. Under Armour invested in this application as a strategic marketing plan to increase sales in sneakers and swear-wicking clothes. Kevin Plank, Chief Executive of Under Armour, explained that the MyFitnessPal enabled the company to collect customers' habit information. In addition, to increase the amount of sales, this information helps the company to improve the durability and the efficiency of products and services. However, MyFittnessPal was hacked by a third-party (Lumb, 2018). Regarding available reports, this data breach was caused by a vulnerability in Bcrypt, the hash function deployed in the secure password scheme. Afterwards, the impacted users received a notification to change their passwords (BBB warning, 2018). In terms of financial issues, the data breach negatively impacted Under Armour's revenues. The first day breach was declared, Under Armour's shares fixed on its value up 0.1 percent (Armour Discloses MyFitnessPal Data Breach, 2018) and in the early hours of the next trading day, the value of the shares decreased by 4 percent (Dye, 2018). The scale of attack was so large in other companies that in the first week, the hacker of MyFitnessPal also hacked 750 million users from 24 different sites such as Coffee Meets Bagel and 500px, and after 2 weeks up to 850 million users (Whittaker, 2019). The hacker puts the users' information on the dark web only for 2.6 bitcoins, or $9,350. Ariel Ainhoren, an IT security leader at IntSights located in Israel, said the hacker used the same method of hacking to exploit each website. Therefore, it seems most of the retailers are not aware of the role of IT security in their firms because when Whittaker contacted some of the impacted companies, they were not aware of the data breach at all.

B. Company/Department Strategies, Mission, Vision, Metrics

The mission of MyFitnessPal service is to increase the amount of demands/sales for footwear and sport products. To achieve this goal, MyFitnessPal started a win-win model of business between company and customers. It services the "calorie goals by meal" to provide information such as blood pressure to detect chronic problems and helps customers reach their health goals. It enables users to have food analysis or a standard exercise calorie setting. In addition, this application offers diet settings such as the carbohydrate-loading diet to improve body endurance performance. On the one hand, MyFitnessPal brings a big advantage for users about their health situation and helps athletes achieve their fitness goals. On the other hand, it motivates people to use MyFitnessPal every day, which indirectly increases the number of hits to MyFitnessPal and provides valuable information about sales in the future. Number of hits as a good attribute is correlated with amount of sales for sport product. Therefore, MyFitnessPal

follows an indirect mission in the market strategy. Nutritional goals and exercise plan can be considered as the analytical attribute for the amount of sales. It forecasts the sale behavior and provides a sales trend. MyFitnessPal helps Under Armour's business model to have an iterative value-adding model. Moreover, by analyzing different types of exercise plan, Under Armour has the opportunity to develop or optimize the sport service. As a business vision, MyFitnessPal can be counted as the missing link of the chain of customer-relationship management because it engages customers in the nutrition plan and collects customers' preferences and desired services for statistical analysis purposes. However, collecting the information increases the risk of data breach. If hackers gain access to the collected data, the advantage can cause reversed impact on the market. Therefore, Under Armor should provide the infrastrarctral requirement in IT security and compliance to achieve its market goal.

C. Business Drivers

In this section, I introduce the business drivers of establishing a SOC unit for different services including MyFitnessPal and discuss why Under Armour should consider the SOC unit as a business strategy. Under Armour invested 10 percent of the annual revenue in 2015 in MyFitnessPal so that customers could check their fitness and nutrition plans. Therefore, securing the data in this application can be considered as a necessity of being resilient in the competitive market. However, in March 2018, Under Armour announced that a data breach occurred in MyFitnessPal and affected 150 million customers' account information including email addresses, usernames, and encrypted passwords in late February 2018 (Dye, 2018). Hopefully, the data breach did not include Social Security Numbers and credit-card information because the company had collected the SSN and credit-card information in a separate platform (Under Armour Discloses MyFitnessPal Data Breach, 2018). It seems Under Armour was not aware of the role of Security Operations Center (SOC) in its corporation. Other companies such as Adidas are not aware of the importance of IT security. This lack of awareness is a good driver for Under Armour to run its SOC unit to gain the advantage of better service. Moreover, Under Armor can give the consultancy service about IT security platform to market competitors. It can convert Under Armour's bad reputation from a hacked company to a leader of IT security in the sports and footwear industry. Not only did the SOC unit help this company to meet the requirement of cybersecurity, but it is also the key to open the door toward the other business opportunities in IT security. According to Cybersecurity Industry (2018), there is a large-size market of 113 billion dollars for services and products in cybersecurity area by 2020 because cyber environment experienced a rise in cybercrime and companies are shifting to establish SOC and reliable IT infrastructure in the near future. For example, Target Corp. announced that it would invest 18.5 million dollars on cybersecurity (Germano

& Armental, 2018). Therefore, Under Armour's IT department should be ready for a change in the business platform and strategy.

D. Business Model Used

The business model of SOC is determined by several factors such as the size of the company and the IT security strategy of the company. Moreover, according to Gartner (n.d.), the business model of SOC can have a centralized or decentralized architecture. SOC unit has 5 models including Virtual SOC, Multi-function SOC, Co-managed SOC, Dedicated SOC and Command SOC to meet different security requirements. Among the available models, the best architecture for Under Armour is centralized SOC with a dedicated model for 2 reasons: Firstly, Under Armour is a corporation with more than 15 thousand employees and a global platform. Therefore, Under Armour needs to have its own department of IT security. Secondly, as a business strategy, Under Armour can service IT security solutions as the SOC-As-a-Service to other mid-market companies in the sports industry and keep mid-market businesses connected for marketing purposes. Dedicated SOC is the best solution for an enterprise level business. It is based on a dedicated infrastructure with a centralized model and only needs five to eight IT security experts to monitor the business process and operation.

E. Product and Services Delivery Model

The recommended delivery model in this case-study is based on AlienVault USM. In SOC model, service delivery has 6 steps: Analysis, Plan, Design, Build, Test, and Deploy. The senior manager in SOC unit runs discovery analysis, and collects the organizational requirement, and estimates the scope of data breach impact. Senior manager recommends the appropriate solution in the analysis step. In addition, he/she plans the requirement of teaming such as communication, readiness. Then, he/she forms a response team to perform vulnerability assessment and alert analysis (How to build a security operations center, n.d). the response team is responsible to provide data analysis and available forecast about probable risks that threaten the company assets. The senior manager recommends the action plan be moved forward based on available insights of prescriptive analysis. During several technical sessions, the senior manager and the response team improve the plan after testing and reviewing all details so that all team members agree on the final plan. Afterwards, response team implements and operates the plan to meet the company's requirements. The team provides information security and event management. They provide the logical and physical requirements as well. They prepare a pattern for the baseline of normal activities, asset discovery, and behavioral monitoring in the organization and

report their findings to threat intelligence. The report includes domain address, IP address, and other identification of adversary (IOCs). The response team establishes the baseline and log monitoring in order to investigate the incident and to create a story of all abnormal logs and outbound data sharing. Moreover, baseline enables the SOC team to detect and investigate abnormal patterns of activities in the network. Moreover, the SOC team provides signature-oriented intrusion detection to maintain database. In the next step, the SOC team provides the solution and implements the testing plan. If solutions pass all tests, they will be deployed in the network.

F. Tools Used

According to Security Operations Centers (2014), an SOC provides a sort of integrated service, solution, and formal process. It performs the log analysis, Intrusion Detection System (IDS), and Data loss prevention (DLP) to detect anomalies. In addition, SOC has some tools including antivirus, host-oriented and network-oriented malware detection, and firewalls to collect information about and respond to potential risks like Denial of service. Moreover, trend analysis enables the data analyst to study anomalies' behaviors and predict future attacks by correlation, and prescriptive analysis.

1. SWOT Analysis

AlienVault USM as a product and service delivery model has a list of pros and cons which can cause both opportunities and threats listed in table 1. It has a powerful operational platform. It provides the measurable risk posture and safe baseline environment for business core process and objectives. The governance plan is well-designed and covers essential requirement. it benefits from executed processes. Last but not least, senior manager and security team are able to analyze log in/out data in real time manner.

2. IT Business Values – 5 Pillars

In this section, I will evaluate 5 pillars modeled by Murphy to check whether the SOC unit meets its business requirement.

- Strategic Alignment Check: There are 2 checkers showing that SOC adds strategic value to the corporation. Firstly, the SOC unit empowers managers to have better communication with the technical team and provides the statistical report for the budgeting process. Therefore, the SOC unit

enables managers to align the strategic plan based on current and desired situations. Secondly, process safety plays the important role in the corporation strategic plan. The SOC unit brings a process safety which consequently ensures the marketing advantage by protecting the operational process against potential cyber-attacks such as ransomware or virus.

Table 1: SWOT analysis for SOC

Strength	**Weakness**
• Powerful operational platform • Measurable risk posture • Safe baseline environment • Strong core objectives • Well-designed governance plan • Executed process • Empowering managers and security team • Providing log analysis and prescriptive analysis	• Non-integrated solutions and multiple technologies • real-time threat • Limited resources of employees, time and budget
Opportunity	**Threat**
• Increasing the operating security investment by providing an integrated platform • Defining stronger metrics for risk posture • A range of price for different size of business • Designing the continuous progress plan	• Multiple technologies changed model to Multi-function platform • Data breach caused by Non-integrated solutions

- **Business Process Impact:** the SOC process presents a bigger vision of process safety. SOC benefits from powerful operational platform by connecting different units. It has a baseline environment and monitoring system which supervises normal activities and employees' behaviors. It provides a measurable risk posture for process safety. In addition, the SOC unit executes the business process and manages the required course of action to prevent probable damage committed by internal saboteur.

- **Architecture Check:** SOC architecture supports a well-designed architecture including IT governance, organizational chart, and strong core objectives. Moreover, the SOC unit benefits from a good framework to categorize the level of risk. It refers each risk to the certain unit where experts

have the available solutions. In addition, it customizes process safety goals to the metric of data security and determines responsibility of each unit.

- Risk Check: the SOC risk management plan enables Under Armour to analyze the risk assessment in 3 levels: functions, business, and corporation. It ensures that the IT security model decreases the risk of investment by IT-related solution. It empowers managers and the security team to perform log analysis. Moreover, managers can forecast the future of the market by prescriptive analysis and control the risk of investment.

- Direct Payback Check: the SOC financial plan ensures the Return of Investment and the total cost of ownership. The financial analysis in each fiscal year provides the required numerical data to meet financial requirements and limitations. Financial analysis provides a sequential model of budgeting with determined time-slot. The senior manager can manage the financial support to fulfill technical requirement based on the time and the financial requirement.

Therefore, the SOC model meets all 5 pillars which are required to start a business model.

III. Market and Competitor Analysis:

In this section, first, I evaluate Adidas's fitness application called ALLDAY, and then I evaluate SCADA as the available process monitoring solution used by several industrial companies.

A. Industry Environmental Scan

The IT security environment of industry can be scanned using 3 factors: faith, fears, and facts. In terms of faith, it is clear that SOC unit can be considered Under Armour's technological strategy to integrate the infrastructure of business process and to bring the competitive advantage by protecting customers' data. Moreover, it can open some cooperation or consultancy opportunities for Under Armour. Under Armour can cooperate with well-known companies in the IT industry to build an appropriate platform. Secondly, Adidas and other companies experienced data breach. Under Armour has this chance to lead the IT security solution for nutrition and sport applications. Moreover, a standard infrastructure of business process helps sport industry make its own policies and compliance for healthcare applications. It can make a technological reputation which influences the market environment and increases the intangible asset. Therefore, it is important Under Armour has an open arm strategy to technical

opportunities even though those technical opportunities do not meet the business mission initially. Thirdly, it helps Under Armour recover its cost caused by cybercrimes. The SOC unit deceases the court's penalty cost for data breach (in range of hundred million dollars).

B. Major Competitors and Their Status in the Industry

The competitor which provides a nutrition plan for its users is Adidas. Adidas created ALLDAY application. ALLDAY enables its users to balance their nutrition plan, movement practice, rest schedule, and mindset (ALLDAY, n.d). ALLDAY, as a marketing strategy, has a mission to engage users to maximize their athletic performance by providing information about maintaining a healthy lifestyle. It plans a daily schedule including meditation methods, breathing exercises, game-plan, and method of sleeping at night for its users and displays information about the numbers of steps, miles, and burned-calorie to users. However, Adidas experienced a data breach on its US website in 2018 (Humphries, 2018). A third party informed Adidas about the details of data breach. It seems Adidas has no monitoring system to be aware of IT security incident and struggled with the similar issue in 2018. This shows that well-known brands are not familiar with IT security, which it would be a great opportunity for Under Armour to play the role of the advanced firm in the IT security solution by building a SOC unit. It might make other cooperation opportunities in a coopetition model which leads to an IT security framework for nutrition ad sport applications.

C. Tools Used

Most industrial corporations usually deploy SCADA to monitor the process. This operational technology is based on process controlling principles which does not meet the IT security requirement. The operational monitoring system is equipped by vulnerability scanner which does not professionally focus on IT security requirement in the core business process. Meanwhile, the SOC unit brings more process security and reliability and provides the better platform for IT core process from the security perspective.

1. SWOT Analysis

SCADA is a most popular operational technology used for monitoring purposes in the engineering purposes. It has a self-contained infrastructure and provides open system solutions. Moreover, it increases system robustness. It supports easy operation and maintenance and has this capability to

have a built-in encryption. However, it is not necessarily secure in practice. Lack of authentication is the main problem of the control system like SCADA. An unauthorized-party can access the packet and the control system easily. Moreover, SCADA is vulnerable to buffering overflow which causes the Denial of Service attack.

SCADA would provide more effective IT security platform if it deployed the multi-factor authentication. Moreover, deploying a better controlling processor enables SCADA to check the length of the input data. It will optimize the alert and command line platform. Aforementioned opportunities will be converted to the source of threat if SCADA does not upgrade its platform to meet security requirements. The SWOT analysis is listed in table 2.

Table 2: SWOT analysis for SCADA

Strength	**Weakness**
• self-contained infrastructure • open system solution • System robustness • easy operation and maintenance • Built-in Encryption	• In practice, it is not necessarily secure • Lack of authentication for control system • unauthorized-party can access to the packet and the control system • vulnerable to buffer overflow
Opportunity	**Threat**
• Fixing the security issue and deploying multi-factor authentication to attract industrial market • Fixing the buffering problem by checking the input data	• Harmful data breach • Low performance • Denial of service attack • losing the loyal customers

2. IT Business Values – 5 Pillars

Here is the list of 5 pillar checkers which SCADA must meet to compete with Security Operating Center.

- Strategic Alignment Check: It did not meet the strategic alignment which Under Armor is looking for. The strategic plan is to keep business safety against data breach and deploying a monitoring system for IT security concerns. SCADA is a control process for manufacturing and product-line.

- Business Process Impact: Lack of firewalls and other detectors such as virus and malware detector are another problem of SCADA system. Even though SCADA upgrades its monitoring system, there is no guarantee that it will meet all IT security requirement in the efficient way.

- Architecture Check: SCADA architecture is specified for the process monitoring from engineering perspective. Hierarchy of people is based on their experience in the engineering and not in the IT security area. SCADA has no adequate vision about certified people in IT security, compliance and auditing process.

- Risk Check and Direct Payback Check: SCADA empower the required monitoring equipment from engineering perspective which is not 100% risk assessment for retailers. Moreover, it only guarantees manufacturing monitoring system such as CCTV system, fire detection system and sprinkler in the financial analysis. The financial analysis does not include required tools and softwares preventing data breach.

IV. **Operating Plans**

The model is based on AlienVault USM. It is affordable solution for a corporation (How to Build a Security Operations Center, n.d). Moreover, my operating model meets all general requirement of SOC units. For example, the SOC unit deploys an incident response process to monitor and identify threats. In addition, it includes a threat intelligence unit. Threat intelligence unit has different responsibilities including “open source intelligence” to collect open source information of security incidents from public, "signal intelligence” to empower organization to have an offender-oriented monitoring, “Human Intelligence” to find the qualified people, “employee engagement” to measure the level of commitment that employees should meet in the organization (Security Operations Centers, 2014). It also performs the penetration testing and enables IT department to configure the real-time reporting system of vulnerability. Furthermore, the operating model has a data-leak prevention unit to prevent users of sending confidential data to outsiders. In addition, operating plan of deployed SOC includes a baseline of the core business processes. The baseline can give a good metric to measure the normal network traffic and organizational behavior on network. It

determines the level of access for each employee. Last but not least, SOC unit provides the easier way of IT asset inventory monitoring. Therefore, it is clear that a dedicated SOC will add a technical value to the IT infrastructure of the Under Armour.

In terms of marketing plan, I recommend a coopetition model. This model can bring both advantages of the cooperation and competition for Under Armour because Under Armour can sell its IT security product and services to the competitors such as Adidas. Consequently, Under Armour reduces the cost of malware analysis and digital forensic and returns its investment on SOC unit. In this operating model, Under Armour answers a high-demand IT security market on the healthcare application by building a IT-based risk framework. In this model, Under Armour is responsible to set the IT security standards for nutrition and sport applications and technically leads other companies. Therefore, Under Armour's operating model in IT security is to answer the emerging services by heuristic techniques and self-discovery approaches.

A. **In General – Operating Plan:**

1.**Value Analysis of the Plan**

The recommended SOC unit provides a powerful tool for data governance. It empowers people to experience an excellent functioning to confront with security incidents. It can simplify the process execution and keep the IT team knowledgeable against the new techniques of exploiting. It ensures the business safety by integrating control tools in incident response process such as Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) and anti-malware and anti-virus. It provides a core center which improves effectiveness and efficiency of the business objectives. Moreover, it reduces the risk of investment by adding a security vision to the all process and cooperation protocols. By following the strategic guidelines, SOC plays an important role to meet the quality of service and attract more investment. Therefore, deployed operating plan of recommended SOC adds the considerable value to efficiency, security, consistency, cooperation and quality of service.

2. **Risk Analysis**

There are 4 steps to meet the requirement of risk analysis which is presented in fig 1. Firstly, Under Armour's SOC unit should identify the critical tangible and intangible assets that can be impacted by security breaches such as financial process or reputation. There is a list of tangible and intangible factors in table 3 and 4. Then, each asset has its own profile for stored data. Each profile includes

some information such as the type of criticality, managerial details and also the technical characteristic of the data transmission deployed in each asset. Secondly, risk analysis assesses the potential cost of each security incident and measures the likelihood of each risk and creates a profile for each risk including impacted assets and the potential amount of cost for each specific asset. Thirdly, Under Armour's response team (combination of the IDS team and the decision makers of the IT issues) should provide the solution plan to mitigate the risk. Response team should deliver the solution plan to IPS team and IPS team is responsible to run the solution plan to prevent and minimize the impact of incidents on the core business process.

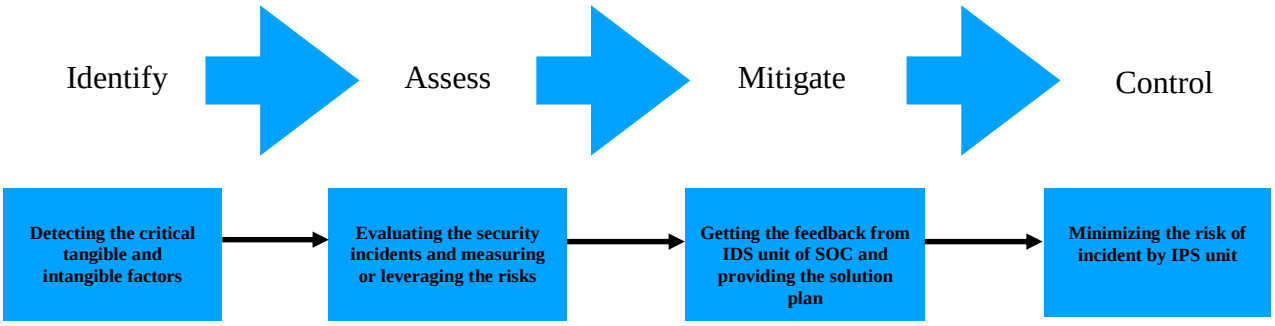


Fig 1: risk analysis process

Table 3: Tangible factors impacted by data breach

Issue	type of Asset
Transaction systems/Financial process	Income in $/Bitcoins
Investment	Shares in $/Bitcoins
power of processors on servers	Giga byte per seconds
Market secrets and Confidential information about business	Intellectual property

Table 4: intangible factors impacted by data breach

Issue	type of Asset
Customers' trust	Public view
Reputation	Public view
Credit in the banking system	Organizational credit/ Trustworthy

3. **Process Value Analysis**

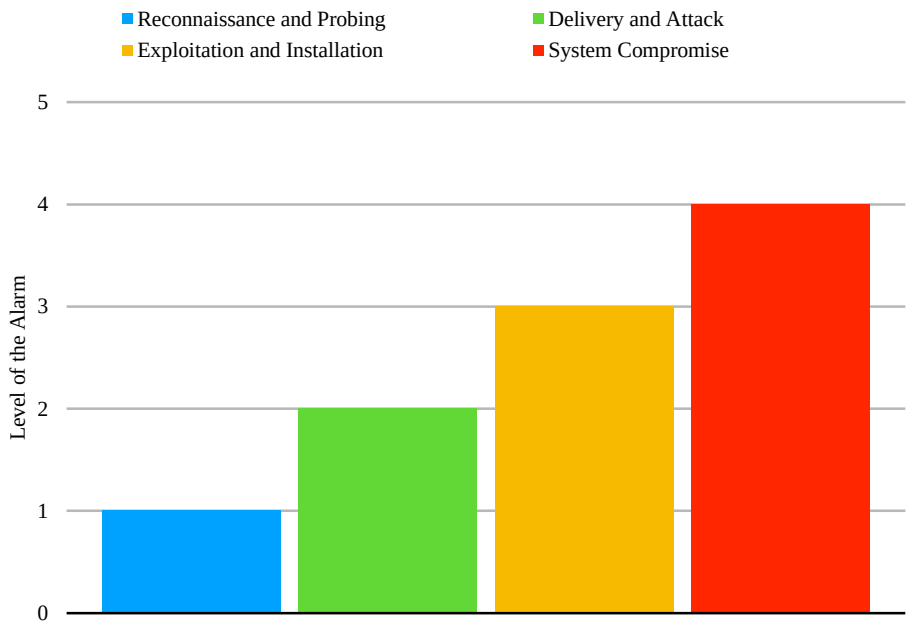
In SOC there are 3 levels of intelligence: tactical, operational and strategic (How to Build a Security Operations Center, n.d). The process value analysis is belonged to the second level of intelligence called operational intelligence. By providing the portfolio for each security incident, SOC is able to prioritize the events based on business requirements and then analyze the high-priority incident. The prioritization brings the operational value to the corporation. By detecting signal activities, SOC can collect data about potential adversary to map the competitors' operational values. It can find the correlation between different incidents and can detect the similar scenario. It helps Under Armour provide the fast-forward solution and remediation plan in the effective manner. This step includes reproducing the system back up, updating the operations systems, reinstalling the network configuration, modernizing the system by stronger scanning metrics and deploying a powerful vulnerability monitoring system. It empowers the SOC to have smarter metrics for the event-story classifications. For example, if the third-party tries to collect information about company, SOC system will alarm in "Reconnaissance and Probing" class which has the lowest level of the risk. However, it has this potential to convert to the second level of risk. The second level of alarm called "Delivery and Attack" which is associated with the misuse of a low cost vulnerability. The Third level of alarm is called "Exploitation and Installation." This level of the issue needs to be investigated seriously. This level is associated with a real vulnerability exploited by hacker. The forth level which needs investigation and auditing process called "System Compromise" which shows that the hacker compromised the system. I show the all classes of alarm in fig 2.

Therefore, by leveraging alarms, SOC unit will add value to the both protection and recovery process.

4. **Key Assumptions and Options Analysis**

In terms of the key assumption, I would like to add this fact that hackers' preference changed and they focused on exploiting the corporation-level of vulnerabilities (Bamohabbat, 2019). Among the available solutions between SOC and SCADA, I chose dedicated SOC for several reasons. Firstly, Under Armour is a large-scale market with a net-revenue range of 5 billion dollars. Under Armour has a world-wide platform of transactions which needs to come to the agreement on the fair-competition or GDPR protocols in the host country. A dedicated SOC platform enables Under Armour to achieve a higher transparency of the e-commerce security.

Fig 2: different operating alarms in the SOC unit



5. **Leadership and Management Styles**

SOC determines an associated role for each level of the alarm. For the "Reconnaissance and Probing" level, Under Armour's SOC has a team combined from two security analysts with administrator skills. Both are specialist in programming languages such as PHP, Ruby, R or Python, Java and got the professional certifications such as GCIA, GCIH, GCFA, GCFE and CISSP. They

are in charge of monitoring the status of urgent alarms. They produce alarm tickets to determine the required course of action which incident response unit should take. Available tool for this level include IDS, net flow and the correlation-analysis tools. There are two data analysts in the next level i.e "Delivery and Attack". They should be more skillful about cybersecurity stuff. They should have a deeper knowledge about the mission of cybersecurity and have a background in ethical hacking as well. They are responsible to check the tickets issued by first team. They classify the scope of cyber incident by threat-intelligence tools such as Indicator of Compromise (IOC). They are responsible to identify impacted tangible and intangible factors and to respond the threat by the adequate remediation plan. In the third level, a senior IT security specialist assess the vulnerabilities caused by "Exploitation and Installation". He/she is skillful to defend the system against the attacks. He/she is expert to discover attack scenarios. He/she develops or updates the threat identifiers and deploys the optimized controlling system based on the sensitive requirement and updates the rules, policies and configurations. The forth level of management called "IT security officer". An IT security officer plays the leadership role in the IT security operation and compliance. He/she supervises the SOC unit and he checks the incident story. his seniority and experience enables him to perform the auditing process. He/she is mentally ready to lead the unpredictable situation. He/she is very skillful in communication. It runs different metrics in auditing process to discover the source of vulnerability and threat.

6. **Organizational Chart**

The line-chart presented in fig 3 shows the hierarchy of SOC unit. This unit is following the standards and compliance requirement which Chief Operating Officer and Compliance unit determined due to the NIST standard and compliance. The highest position in SOC unit is Certified Information Systems Security officer (CISSO). CISSO should have a background in auditing process or should in cooperation with an internal senior auditor. The second level of the organizational chart is Incident Response unit which monitors the baseline of the security policies and also manages both IDS unit and the Threat Intelligence unit. IDS unit has 3 sections including software, network and hardware security which protect the application, the infrastructure, and the website against threats such as malware, virus and physical disasters. Threat Intelligence have 4 sections including Human Intelligence, Signal Intelligence, employee engagement, Open Source Intelligence Unit. IDS and Threat Intelligence units are both connected to the Incident prevention units such as data-leak prevention unit, Indicator of Compromise (IOC) which do course of action

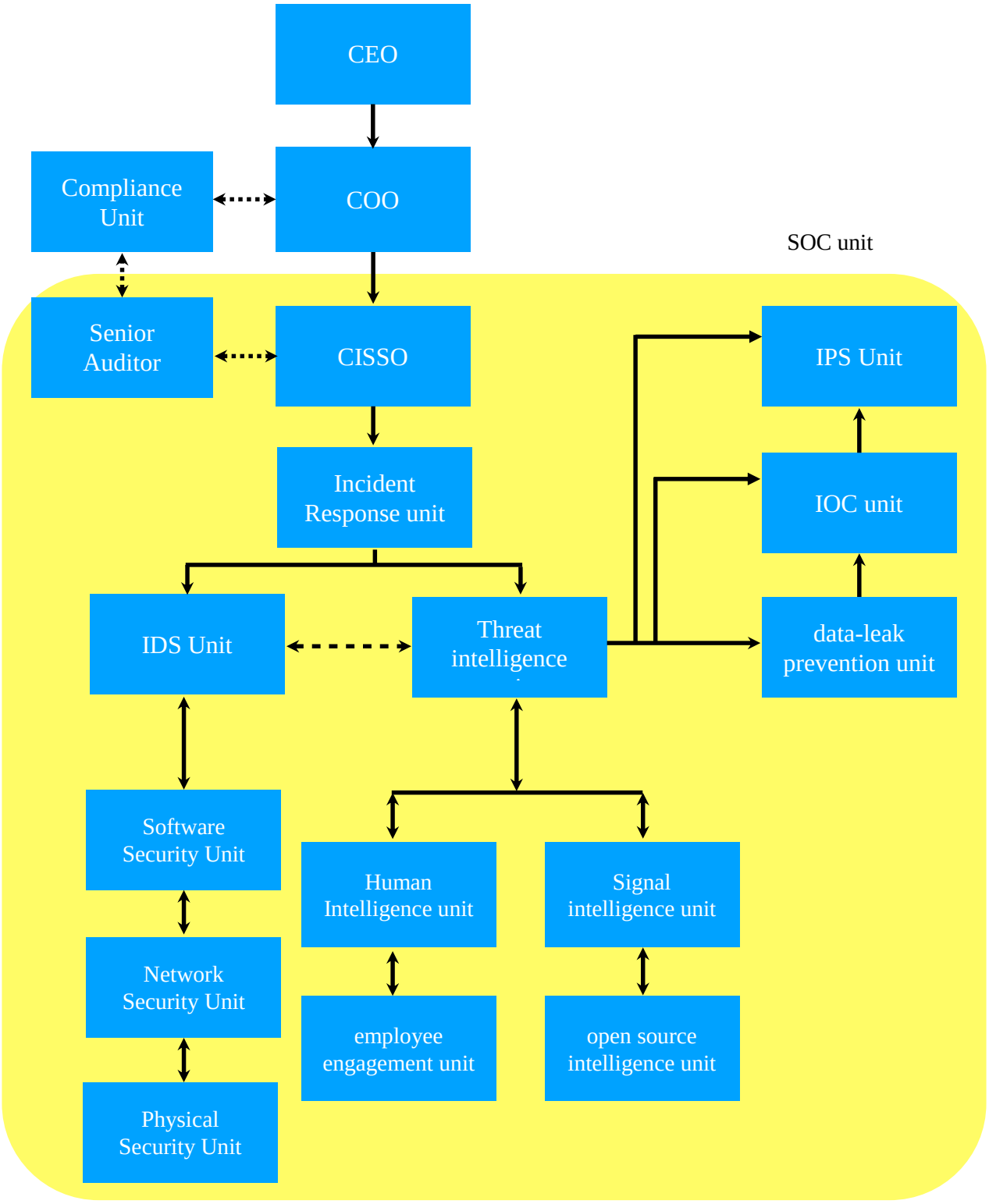


Fig 3: organizational chart of the SOC unit

against exploiting vulnerabilities. The IOC unit collects the forensics for Incident Prevention System unit and also lawsuit purposes.

7. **IT Governance Plan**

In the IT governance plan, I govern the organizational workflow by COBIT 5. It is a standard framework proposed by ISACA society for the enterprise. COBIT 5 can be considered as a well-organized IT security plan in the SOC unit. It is a reliable and well-developed framework to align the organizational priorities and values (A Business Framework for the Governance, 2012). It meets the requirement of business owners and stakeholders by providing the privacy and confidentiality of information which is vital for the business. According to Suer and Nolan (n.d.), information lifecycle of COBIT 5 includes 5 blocks. The first block is business IT processes. Business IT process is responsible to collect and extract data for the next block called data block. Data block transforms data into the information and then information generates knowledge and then knowledge will be loaded for decision makers to create the business value. The business value as a driver develops the business model and expand the market vision (see fig. 4). In the enterprise level, COBIT 5 is a good framework to categorize and control the risk against tangible and intangible assets and presents the available resource to protect the confidential and intellectual asset. It enables Under Armour to decrease the level of risk and increase the benefit by providing the IT-related solution. It provides a model of risk reduction and profit maximization for decision makers by converting the business goals to the measurable factors. In terms of service delivery, COBIT increases the coordination between different departments and keeps consistency, efficiency, integrity and effectivity of them. This model is compatible with other frameworks in the enterprise level such as ISO/IEC 3100, COSO and IT-related level such as ITIL or TOGAF. COBIT 5 employs 7 enablers to run Governance of Enterprise IT (GEIT) which I present in the appendix A. Based on a game theory principle, firms are looking for the competitors' strength; knowing complete information of competitor's strategy adds value to the firm and increases profits. COBIT 5 recommends a reliable governance plan which structurally prevents competitors to get the firm's information.

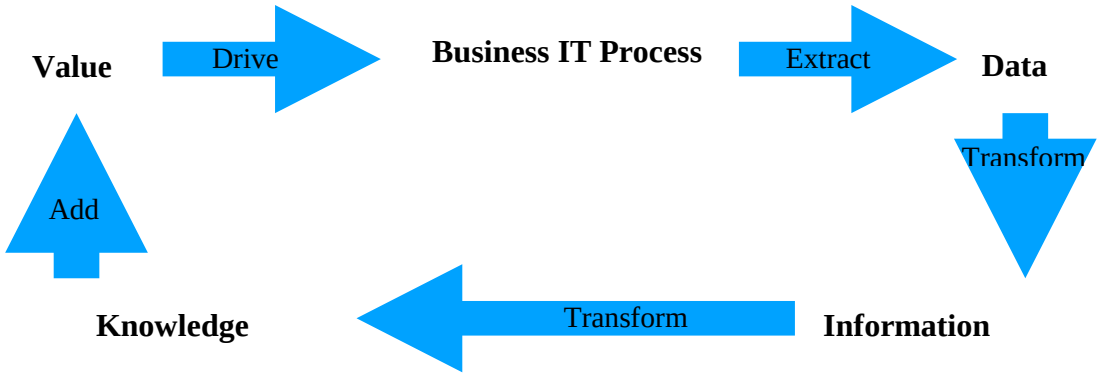


Fig 4: Iterative IT Governance Plan

Moreover, it determines the company's point of view about legislation associated with IT security policies such as employee complaint (lawsuit made by the employees) or the wrongful dismissal. Furthermore, this model uses General Data Protection Regulation (GDPR) for data sovereignty purposes. In terms of training plan, SOC team's members are trained by the principles and advanced topics of IT security, compliance and auditing process. Moreover, they will be trained for working with the valid protocols of lawsuit in IOC process. In terms of technical skills, COBIT 5 forces SOC unit members to get required certifications such as CISSP, GCIA, GCIH, GCFA, GCFE. COBIT 5 plans to update knowledge of SOC unit members in several areas such as data analytics, programming and management and leadership.

B. **Marketing and Manufacturing Plans**

According to the Business Framework for the Governance (2012), COBIT 5 has seventeen generic goals in the different balanced scorecard (BSC) dimensions (See table 5). COBIT 5 classified the benefit in 4 plans: customer, financial, intra-organization and Training & progress. COBIT 5 meets the marketing and manufacturing goals which Under Armour is looking for.

V. Financial Analysis

The financial plan provides the financial transparency into the financial goals and ensures the business sustainability. It models the required financial stages and resources. Moreover, it works to determine the share of each stakeholder or investor. In addition, it adds the investment value to the business model. Furthermore, it gives a financial metric to assess the business risk. Last but not least, it can make the model

profitable financially. Financial analysis as a good metric initially measures the total cost. It calculates cost saving and determines what type of investment are required (Capex or Opex).

Table 5: generic goals of COBIT 5

Balanced Scorecard Dimension	Enterprise aims	correspondence with Governance priorities		
		Benefits Realization	Risk Optimization	Resource Optimization
Consumer/Customer plan	Considering the culture of host-country in the service providing process	Primary		Secondary
	Maintaining the sustainability (availability and continuity) of the service		Primary	
	Keeping the business framework (Agile) flexible with market changes	Primary		Secondary
	Making strategic decisions based on evidence and information	Primary	Primary	Primary
	Optimizing the cost of service delivery	Primary		Primary
Investment and Financial plan	Adding the investment value to the business model	Primary		Secondary
	Gaining the competitive advantages in products and services	Primary	Primary	Secondary
	Assessing and managing the business risk		Primary	Secondary
	Adapting the internal compliance with external regulations and laws		Primary	
	Providing the financial transparency	Primary	Secondary	Secondary
intra-organizational plan	Optimizing the functionality of business process	Primary		Primary
	Optimizing the costs of business process	Primary		Primary
	proposing the clear plan for the business-change management	Primary	Primary	Secondary
	Increasing the operational and staff productivity	Primary		Primary
	Adapting Compliance with intra-organizational policies		Primary	
Training & progress plan	Developing the staff skills and motivations	Secondary	Primary	Primary
	strengthening the business, innovation and Product culture	Primary		

A. Operating Expense Proposed Budget

In table 6, I list the estimated cost of operating process (OPEX). The table includes the start date and end date of equipment installation and configuration and period of employment for the first year. As you see in the fiscal year, the operating expense of the SOC unit costs 55,739,000 dollars.

Table 6: Financial Analysis (OPEX)

Operating Expenses					
List of Equipment	**Start date of configuration/employment**	**End date of configuration/employment**	**Annual price per unit/person $**	**Quantity/number of customers**	**cost per year**
AlienVault USM	January 1 2020	April 1 2020	0.133	150,000,000.00	20,000,000
Cisco Umbrella	January 1 2020	April 1 2020	0.026	150,000,000.00	35,000,000
OKTA	March 1 2020	April 1 2020	0.0006	150,000,000.00	90,000
Carbon Black	March 1 2020	April 1 2020	0.0006	150,000,000.00	90,000
Kali Linux	January 1 2020	April 1 2020	0.0006	150,000,000	90,000
VMware	January 1 2020	April 1 2020	5,000	1	5,000
CISSO's annual salary	January 1 2020	January 1 2021	144,000	1	144,000
Senior data analyst's annual salary	January 1 2020	January 1 2021	90,000	2	180,000
Junior Data analyst's annual salary	January 1 2020	January 1 2021	65,000	2	130,000
Training	January 1 2020	January 1 2021	2,000	5	10,000
Total					55,739,000.00 USD

B. Capital Expense Proposed Budget

In table 7, I list the cost of CAPEX including department office, furniture and technical requirement such as personal computer and video projector. It totally cost 331,300 USD.

Table 7 : Financial Analysis (CAPEX)

Capital Expenses		
List of capital	**Cost per unit/person**	**costs**
SOC department unit	1	300,000.00
Personal computers	5	10,000.00
Furniture	1	10,000.00
Desks	5	10,000.00
Video projector	2	800.00
coffee maker	5	500.00
Total		331,300.00 USD

C. ROI, Profit and Loss Statement

In fig 5, I present a Sankey diagram for profit and loss statement. All numbers are in million dollars. I suppose an interest rate of 25 million USD and 500 million dollars (ten percent of annual revenue) for Research and development purposes in all departments. Total available budget is equal to 525 million USD. Total cost for SOC unit is about 55.8 million dollars. It means company has a good investment margin to establish a secure infrastructure for 150 million people by SOC unit. It can consequently increase the reliability and decrease number of lawsuits which consumers can file for data breach. It is estimated that Under Armour has to pay the fine around 200 million USD to the federal government for 150 million people impacted from data breach. If I consider the cost saving amount as profit, ROI is equal to 25%.

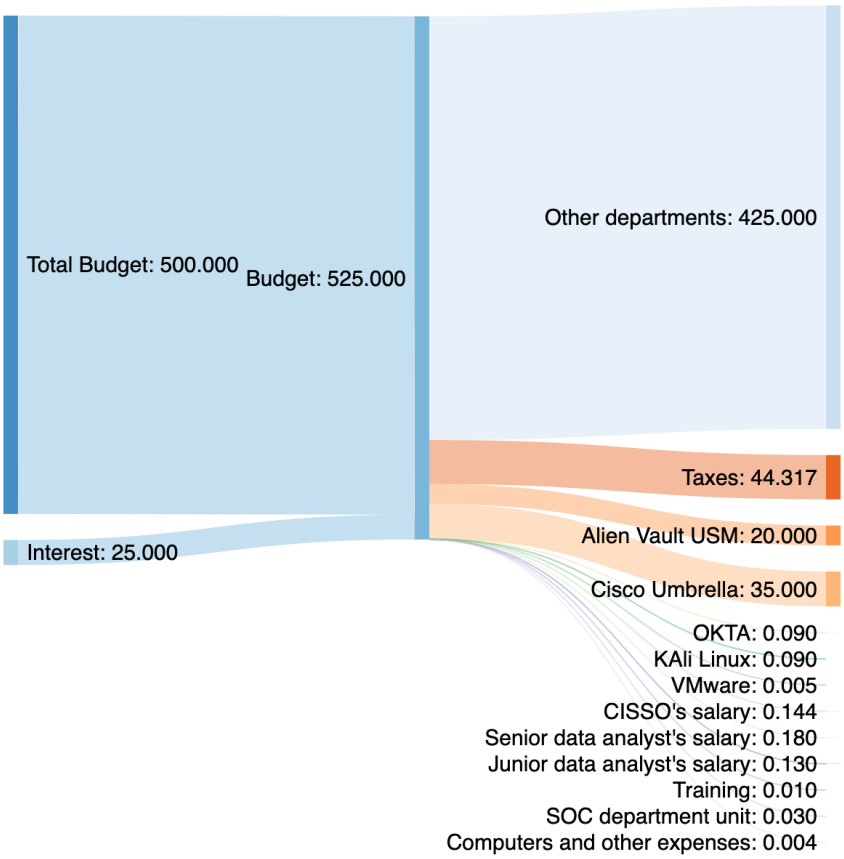


Fig 5: Sankey diagram for profit and loss statement

VI. **Conclusion**

In this case-study, I introduced the data breach exploited on MyFitnessPal, the Under Armour's fitness application. This data breach impacted customers' account information including usernames and hashed passwords. I realized that Under Armour suffers from lack of Security Operating Center (SOC). I recommended a centralized Security Operating Center (SOC) with a dedicated model to meet the IT security requirement.

A. Plan Recap

I recommended a security operating center which monitor threats by 3 units: incident response unit, threat Intelligence and Intrusion Detection System and provide course of action by 3 units: IPS unit, IOC Unit and data-leak prevention unit. The SOC has 4 levels of alarms:

- "Reconnaissance and Probing" is for collecting information about company by unauthorized party. It has the lowest level of the risk,
- "Delivery and Attack" is for misusing a low cost vulnerability.
- "Exploitation and Installation" is for a serious exploitation of the breach
- "System Compromise" is for the case in which hacker compromised the system

The hierarchy of SOC unit has 3 levels of position: CISSO, Senior IT security analyst and Junior IT security analyst. I compared Under Armour's fitness application with Adidas's application, and I compared the advantages of SOC unit versus SCADA by using SWOT and 5 pillar analysis. I showed the SOC unit is a better solution for Under Armour. Furthermore, I recommended an operating plan and core business process for SOC unit and discussed the value and the risk analysis of the solution. I evaluated that how the SOC unit decreases the impact of unknown threats and provides forensics for legal purposes. I recommended the open-door management style and iterative IT governance plan for SOC platform. Finally, I performed the financial analysis and determined a rate of 25% for ROI.

Bibliography:

Under Armor (2019), Retrieved from https://en.wikipedia.org/wiki/Under_Armour

Under armour discloses MyFitnessPal data breach -- MarketWatch. (2018). *Dow Jones Institutional News* Retrieved from https://0-search.proquest.com.library.ggu.edu/docview/2019724512?accountid=25283

Dye, J. (2018). Under armour discloses data breach affecting 150m user accounts.*FT.Com,* Retrieved from https://0-search.proquest.com.library.ggu.edu/docview/2122766257?accountid=25283

BBB warning: The latest data breach is under armours MyFitnessPal. (2018). *Financial Services Monitor Worldwide* Retrieved from https://0-search.proquest.com.library.ggu.edu/docview/2019988722?accountid=25283

Lumb, D. (2018). Fitness app PumpUp left users' personal data exposed on server. Retrived from https://www.engadget.com/2018/06/01/fitness-app-pumpup-left-users-personal-data-exposed-on-server/?ncid=txtlnkusaolp00000616

Whittaker, Z. (2019). ClassPass, gfycat, StreetEasy hit in latest round of mass site hacks. Retrived from https://techcrunch.com/2019/02/16/classpass-gfycat-streeteasy-hacks/?ncid=txtlnkusaolp00000616

Cybersecurity Industry. (2018). Yass: Acquisdata Pty Ltd. Retrieved from ABI/INFORM Collection Retrieved from https://0-search.proquest.com.library.ggu.edu/docview/2162339489?accountid=25283

Germano, S., & Armental, M. (2018). Under Armour discloses breach affecting 150 million MyFitnessPal app users; athletic-wear company's investigation hasn't found evidence that unauthorized people have used the exposed data. *Wall Street Journal (Online)* Retrieved from https://0-search.proquest.com.library.ggu.edu/docview/2019655157?accountid=25283

Gartner. (n.d.). Brief-Top 5 SOC Models by Gartner. Retrieved from https://arcticwolf.com/resources/security_operation_center_models/

Bamohabbat Chafjiri, S. (2019) Shadow brokers Vs. Artificial intelligence. Retrieved from https://www.slideshare.net/secret/lBa0eWltw1GqI

Suer & Nolan, (n.d.). Using COBIT 5 to Deliver Information and Data Governance. Retrieved from http://www.isaca.org/COBIT/focus/Pages/Using-COBIT-5-to-Deliver-Information-and-Data-Governance.aspx

A Business Framework for the Governance (2012). Retrieved from https://static1.squarespace.com/static/.../t/.../COBIT-5_res_eng_1012.pdf

Security Operations Centers (2014). Retrieved from https://www.ey.com/Publication/vwLUAssets/EY-security-operations-centers-helping-you-get-ahead-of-cybercrime/$FILE/EY-security-operations-centers-helping-you-get-ahead-of-cybercrime.pdf

How to build a security operations center (n.d). Retrieved from https://www.alienvault.com/resource-center/ebook/how-to-build-a-security-operations-center

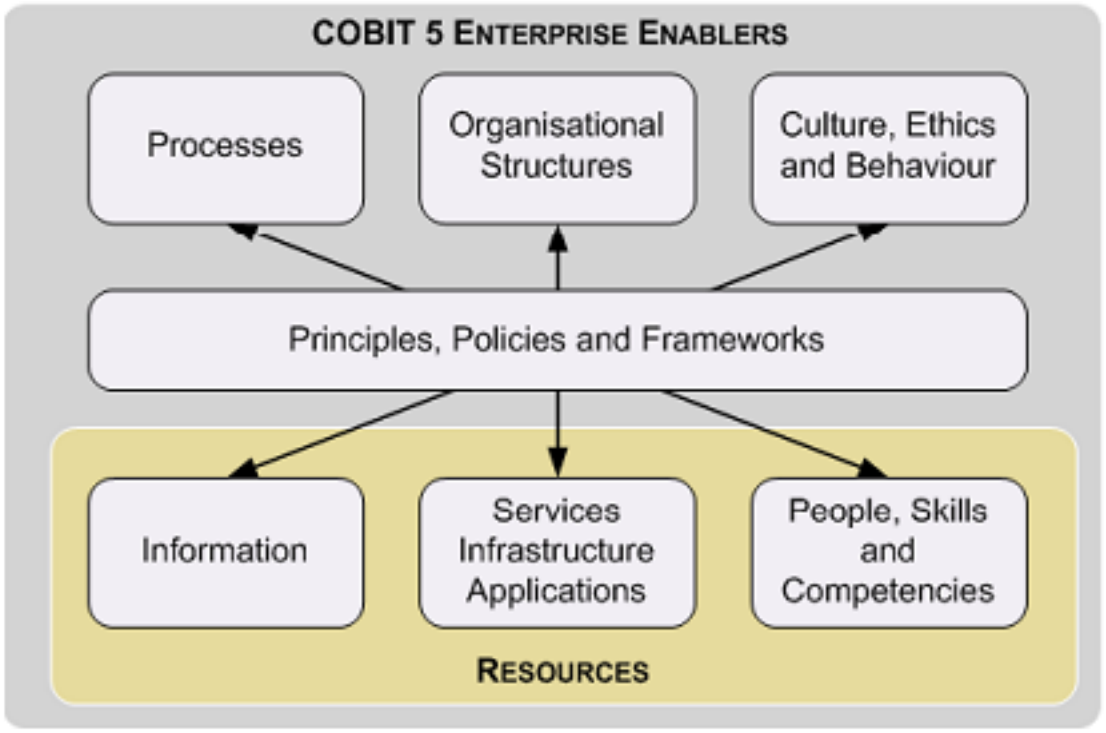
Humphries, M. (2018). Adidas Website Hacked, Millions of US Customer Details Stolen. Retrieved from https://www.pcmag.com/news/362173/adidas-website-hacked-millions-of-us-customer-details-stole

ALLDAY (n.d) Retrieved from https://www.adidas.com/allday/blog/new-adidas-day-app/

Appendices

Appendix A: The figure shows the interaction of units: roles, activities and relationships (Retrieved from COBIT® 5, figure 8 and figure 9. © 2012 ISACA® All rights reserved.)

- Enablers



- Interaction of units