CYBER Security Spring 2022

Case 1 Instructions

Policy

1 Introduction

In order to challenge, exercise, and elaborate on the knowledge that you have obtained during the lectures and literature studies of this course, you are now asked to apply this knowledge in practise by writing a cyber security policy of your own.

The scenario in this assignment is presented in the next chapter. The scenario is fictive, though it is based on events and experience from the industry. The (scientific) base that you are required to have by now is not only based on the lectures and course literature, but also on your own research material and information that you have found on the net (or elsewhere).

During the last couple of lectures, you have learnt about cyber security strategies and policies - both on a national and on an organisational level. You should also have learnt that the purpose of a cyber security policy is to express the goals, objectives, and boundaries for the security management and security solutions of an organisation (or nation if the policy is on that level). A cyber security policy could be a general, high level document that governs cyber security of the organisation in question, but just as important is it to have a more detailed policy of how for example firewalls, severs, routers, employee laptops, even social media applications should be used and handled in the organisation, in order to govern the cyber security of the company on a technical level. Therefore, you will be asked to create one of each type, in this assignment. The work with these cases are structured as follows.

- The case is published in iLearn 08.00 the day before the peer-review.
- The group spends 2 hours working on the case, sometime before Friday 8 April 13.00.
- The group members are not required to meet in person, use some on-line tool for communication.
- On Friday 8 April at 13.00 the group submits its work in iLearn to the fora called Case 1 Hand-ins and it is important that the subject of the message is ‘Case 1 Policy Group X’, where X is replaced by your own group number.
- At 13.00 on Friday the schedule for peer-review is published in iLearn.
- 13.05 the group starts going through the documentation of the group they will peer-review according to the schedule presented in iLearn.
- At 14.45 the group sends their comments and at least four questions to the other group by replying to the original message of their peer-review group, in the fora Case 1 Hand-in in iLearn.
- In this way their documentation, your comments and questions, and then their reply will be in the same message thread in iLearn.
- Now the group reads the answer sent in by the group that has done a peer-review of your group, and this message should be found as a reply to your own original message, with the hand-in of your documentation.
- At 14.45-15.45 the group discuss the feedback from their peer-review group and sends their answers and comments by replying to the correct message in iLearn.
- At 15.45 the group can read the answers of your comments and questions from the group you have peer-reviewed.

- A few days later the teacher will send general comments on the result of the session regarding the questions and the documentation.
- During 13.00-15.45 the groups are expected to have at least a 30 minutes' break.

2 Scenario

Disclaimer: This scenario is meant for educational purposes only. Any resemblance to other names is for realistic and dramatic effect to the task in question only. This scenario is realistic but purely fictive. In the acquisition of a bitcoin service company called Bitflip AB, it has been decided by the board of the acquiring company, Eastchange AB, that the company after the acquisition should enforce a cyber security policy in order to secure the information of both companies. Neither of the companies has ever had a proper cyber security policy, though there has been a contract that the employees of Eastchange would have had to sign before they were handed their company computers, stating that they would not use their company laptops for any personal purposes. Their employees were also required to choose a passphrase of at least 8 characters (lower and uppercase alphanumeric) for the full disk encryption of their company laptops. Bitflip has never had any similar contract or disk encryption policy, though, due to the nature of bitcoins, all employees were eventually made aware of the importance of secure data storage and communications.

2.1 Bitflip AB

Bitflip is a bitcoin service company that buys, sells, mines, and stores bitcoins (bitcoin is a cryptocurrency, based on a decentralised peer-to-peer network: https://bitcoin.org/) for their customers. The company was founded in 2018, and had 17 employees at the time of the acquisition, and 23350 active accounts - estimated to be equivalent to circa 20 000 customers. Bitflip started out as a small company, founded by three students from Stockholm University: two programmers from the department of computer and systems sciences, and one project leader from the bachelor programme in 9IT and strategic marketing. The company grew quickly in 2019, as a result of efficiently mining and selling bitcoins. After the increase in sales and success Bitflip soon started to employ people to manage the finances, accounting, customer service, legal matters, and system administration. After two successful years, Eastchange AB expressed an interest in joining the bitcoin market, and placed a bid of $10 million on Bitflip AB. The bid was accepted and in January 2022, the acquisition was sealed, and Bitflip became Eastchange. Bitflip used to rent spaces at data centres in Boden (primary) and Luleå (secondary) (Data centre backup site: https://en.wikipedia.org/wiki/Backup_site) - communicating over dark fibre. The website and internal systems were run in their office in Sundbyberg (a suburb of Stockholm). Bitflip's backend infrastructure consists of HP ProLiant servers running GNU/Linux Debian (stable), Cisco ASA firewalls, and Cisco Catalyst switches. Only the internal servers were virtualised (using VMWare virtualisation solutions), systems for case management, internal web/DNS/LDAP/FTP/bug tracking/version management/management and more, servers. All of the mining and exchange operations were performed on physical machines in order to decrease latency as much as possible. The software for mining bitcoins was mostly developed "in-house" using the public API of bitcoin.org. The web platform for Bitflip, also developed in-house, was run on physical hardware in the Boden data centre in order to provide co-location for customers who wanted that, and reduce latency in general for all customers.

2.2 Eastchange AB

Eastchange new player in the money exchange business that started up in Sweden in 2013. Eastchange was founded by two students from Stockholm School of Economics, and they quickly settled in the market thanks to the bankruptcy of an unsuccessful money exchange company Swedex AB, from which Eastchange recruited a lot of their current staff. Eastchange sells and buys currency of the most common currencies in Sweden. They have 20 exchange offices in Sweden, one at every major airport in Sweden, and in the biggest cities, but mostly they sell and buy currency online via their website and smartphone applications. Eastchange currently has 100 employees, and has a typical small/medium enterprise IT infrastructure with an internal network for internal economy systems, human resources systems, DNS services, FTP services, internal web services. Externally, Eastchange has their website (including database and backend calculation engine servers), an API server for clients developing external applications, an FTP server for fetching documents and other files. In August 2019, the board decided to expand their currency selection to also include virtual currencies like bitcoin. In January 2022 Eastchange bought Bitflip, which at the time was the leading bitcoin service company in Sweden. With the currency trade and exchange knowledge that Eastchange possessed, the board saw an opportunity to use the same knowledge to sell, and buy bitcoins. After an initial meeting with Bitflip, the board of Eastchange was soon informed about the fact that a digital currency like bitcoin needs very safe and secure environments, hence, the CIO of Eastchange proposed a cyber security policy to be written and applied at the company. Eastchange's head quarters are located in Hornstull in Stockholm, with their data centres close by - at Renstiernas gata. Eastchange kept the data centres in Boden and Luleå for bitcoin mining, trading and bitcoin storage that Bitflip AB possessed, though they moved the data centre in Sundbyberg to the one at Renstiernas gata - though, the infrastructure remained the same as described above.

3 Your Task

As the new manager of the cyber security team at Eastchange, your task is to propose a cyber security policy to the CIO of Eastchange, that they can later present to the board and apply on the whole company. The security policy should preferably be based on an industry standard (ISO 27002/27001, COBIT5, NIST SP-800, or similar - that you were introduced to in the course SECORG). You should also motivate to the CIO why you chose the policy points that you chose. You are expected to use all knowledge you have gained from previous courses here at DSV to come up with a solution to this task. The scenario descriptions are rich in detail - you do not have to take all these details into consideration when creating the policies - though you have to motivate during your presentation which details you included and which ones you did not. You are required to create two policies:

- One overarching cyber security policy that concerns the aspects that you find the most important to include in the policy in the scenarios described above.
- One detailed, technical cyber security policy, i.e. a policy that concerns the technical aspects that you find most important to include in the scenario described above.

Please note that you should identify the needs of the company as a starting point - do not use a template or example policies as your starting point. Each policy is expected to be 1-3 A4 pages.

Examples of technical cyber security policies are:

- Backup and restore policy
- Internet usage policy
- Redundancy policy

- Encryption policy
- Logging policy
- Access control policy
- Firewall policy
- Patch management policy
- Network security policy

3.1 Requirements

You are not expected to come up with a complete cyber security policy for the whole company described above - the idea of this exercise is to get you thinking in terms of policies and be able to identify the most important aspects of a security policy from a given description. The following requirements must be fulfilled in order to pass:

- Group size should be 3-4 people
- Groups must be registered in iLearn
- Files should be submitted as pdf to iLearn before the deadline on Friday 8 April 13.00.
- All group members should be active in the group work

If you have any questions regarding the case, you can post your question in Supervision in iLearn. Since the groups can work with the case any time between Wednesday and Thursday the teachers may not read the Supervision fora immediately after you have sent the question, so there could be some time before you get the answer. Remember: Internet search engines could provide you with the most detailed and adequate answers for some of the questions that you may have.

4 Extended Reading

In order to provide you with more information about what bitcoins are and how they work, here is a short description of everything you need to know for completing this assignment.

Bitcoin is a virtual currency - a so called crypto currency. A bitcoin is basically a file that you can store on your own computer, in a so called "wallet". This can also be at hosted by a third party provider (like Bitflip in the example in section 2.1). The bitcoin wallet is simply a file that contains all bitcoin transactions that have ever been made - hence, it requires a lot of disk space. The bitcoin transactions are made using asymmetric cryptography, a receiver of bitcoin transaction must provide their public key in order to be able to receive the transaction. For sending and managing transactions, a bitcoin wallet holder must unlock it with their private key - just like sending asymmetrically encrypted emails using PGP/GPG as you learned during Introsec. If a user would lose or in some way damage their private key, the bitcoins in their wallet are lost as well. This is an important aspect to keep in mind for the above mentioned specific scenario. Bitcoins can be created by "mining" them. Mining bitcoins means that you use computational power to calculate hash sums that will eventually be turned into bitcoins. This is computationally heavy, and in order to be effective, it nowadays requires specialized hardware – which of course was included in the acquisition of Bitflip in 2020. Bitcoin trading, like all trading, is highly affected by latency; be it latency in network communication, hardware, or software. Therefore, the in-house developed software needs to constantly be reviewed for potential optimisation possibilities - the same goes for the hardware, operating systems, and network equipment. To conclude: Bitcoins are highly valuable digital files that are dependent on swift and secure communication, backed up by robust hard- and software.

5 Resources

The following is a collection of links that might be useful. You are of course free to search for, and use, any relevant resources you might find as well, but these might get you on the right track.

- https://www.sans.org/information-security-policy/
- https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt957812312514f63a/5e9df9554c47dc64d2a649d0/remote_access_policy.pdf - A more technical example policy by SANS
- http://fcc.gov/cyber/cyberplanner.pdf - Federal Communications Commision's guide to cyber security