VIDZEME UNIVERSITY OF APPLIED SCIENCES

VIDZEME UNIVERSITY OF APPLIED SCIENCES

FACULTY OF ENGINEERING

CYBER SECURITY ENGINEERING

INTERVIEW – STRATEGIC ICT MANAGEMENT

VALMIERA, 2022

VIDZEME UNIVERSITY
OF APPLIED SCIENCES

C O N T E N T S

Document history			
Version	Status / Changes	Date	Author
1.0	The first version	16.12.2022	Denys Shabelnyk

Contacts and responsible person (s)			
Name, Surname	Department	Role	Contact information (e-mail)
Denys Shabelnyk	IT	Individual Work	Denys.Shabelnyk@va.lv

1 Interview

The interview was taken in Ukraine**,** I was in contact with the CEO of UPC company in Ukraine, Mr. Anton Romanchuk. We had interesting conversation. The full interview text below:

1. *Is the business embarking on any major digital, big data, cloud, mobility, outsourcing or third-party ventures in the next 3-5 years?*

Answer: Yes, we have the development plan to build our server infrastructure during next 3-5 years. We want to open new business direction in cloud computing. We have already had many partners who have interest with cooperation with us on this business direction. We have budgeted enough money for server infrastructure, support teams, network equipment and development teams.
We hope our new business direction will bring us significant profit in the next 3 - 5 years.

2. Is security treated in the company as the basis for long-term competitiveness?

Answer: Cybersecurity is one of the important part in our business. We have the deep internal integrated cybersecurity policy that is closely linked to all business units. All cloud providers have a cybersecurity focus in its business, but we will have focus on properties for our clients. We guarantee high level of cybersecurity defence as basic property.

3. How cyber security is treated as a business or IT responsibility?

Answer: In our company we have the separated security department which work closely with IT team. They have responsibility to create cybersecurity policy for all departments and teams and check how another departments follow policies. Of course in our company cybersecurity is treated as a business, but team work closely with IT in questions about equipment and digital forensics.

4. Are security goals aligned with business development priorities?

Answer: Yes, of course, because cloud service provides not only IaaS and also data storage, must be protected from tampering and damage. The goal of new business direction is provide IaaS and data storage with high level of cybersecurity in the box. We keep in touch with cybersecurity community and cybersecurity best practices every day.

5. Are generic strategies well formulated and known by functional units?

Answer: Since foundation we have developed the main stategie about our company. How it will grew up ? What our responsibility and how we will develop our business ?
We build our plan for next 5 years with small tasks for every department. These tasks help to achieve the main business goal of our company. As usually, these small tasks don't reconsider but the live is being made changes and we think how to change particular task rapidly. Also, we have a reserve budget for these changes.

6. Are the cyber activities for the next 3-5 years aligned with the business long-term goals and generic strategies?

Answer: as I have said before, every department follow the main business strategy and solve only their local problems. Each department contributes to the achievement of the common goal.

7. Does the company have a Cybersecurity capability? If yes, please provide its characteristics and how it was developed.

Answer: as I have said before, our security department has developed policy for every department. Those policy describe step-by-step algorithm how to do in case a common accident which may happened in their business. The important focus has the policy for IT department. They describe steps for access granted, for laptop/desktop install, hard drive replacement and etc. It was a long process to create full document about general cybersecurity policy. We had many meetings with boards, head of departments. I don't count how many internal meetings were conducted.

8. Are executives and board members well informed of the organization's cyber capability level?

Answer: Yes, enough. They took part in all boards meetings where were discussed about cybersecurity in general and where was created the main directions of development general cybersecurity policy. They didn't consider questions deeply but know about cybersecurity in general and its impact for business. We monitoring meetings monthly that boards listening reports from all departments about cybersecurity accidents if they were happened.

9. What level of interest do the executives take in setting the level of cyber capability and cyber security budget to ensure business viability in a long term?

Answer: we have enough budget for support our cybersecurity environment and build new cybersecurity infrastructure for new business direction. Our boards know and support new ideas which generate every department to improve their work related with security. Boards invited cybersecurity mentors to conduct trainings and train employees in the basics of cybersecurity, create learning materials and learn HR department how to provide periodical checks employee knowledge.

10. Does organizational culture support a secure cyber environment?

Answer: Yes, we are IT company and we provide IT services for our customers and I won't afraid the phrase: "CyberSecurity is our mother and source code is our father". Cybersecurity culture has already implemented into heads and hurts of our employee and they follow it every day. Our culture is use only the last version of coding libraries and follow only last version of security standards. That is the highest level of security in all ages.

11. Is company certain that the third-party partners are securing the most valuable information?

Answer: we don't consider customer's products and we don't know how they protect them but in our side we try following only last cybersecurity policy for each level. I mean infrastructure level, software code level, network level. Our goal is provide IaaS and secure data storage.
We take care about our customers data every day.

12. Does company regularly evaluate the effectiveness of our Cyber security? Are there any goals set for the CS?

Answer: Yes, cybersecurity department has annual report which built within pattern and present every and of year on special event. Also, on this event evaluate status of annual cybersecurity goals.

13. Is company well-resourced and insured against cybersecurity risks?

Answer: we have qualified person and spend enough money to improve employee knowledge and upgrade our infrastructure. Also, we have risk budget to overcome the consequences of incidents and improve infrastructure after.
We also take part as member in cloud-service company community and share experience between each other.

2 Conclusion

A strategic approach in a global perspective helps to plan better and helps to achieve business goals more effective than without it. This solution provides effective budgeting and more precisely improve cybersecurity in long perspective.