VIDZEME UNIVERSITY OF APPLIED SCIENCES

FACULTY OF ENGINEERING

CYBER SECURITY ENGINEERING

INTERVIEW – STRATEGIC ICT MANAGEMENT

VALMIERA, 2020

C O N T E N T S

Document history			
Version	Status / Changes	Date	Author
1.0	The first version	07.10.2020	Mefat Shabani

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

1   Interview

The interview was taken in Albania, I was in contact with the General Manager of Audi company in Albania, Mr. Gentian Bushati. He kindly accepted my interview request and to answer the questions I had for him. I did an online interview with him on zoom, take notes, and proceed with the details as he answers on the video.

1. Please provide characteristics of the company (main industries competing, financial results the company strategic goals for the next 5 years)!

August Horch founded Audi, in Cologne in 1899, and Audi stands for sporty vehicles, high build quality, and progressive design. Our strategy, 'Consistently Audi', which was introduced in May 2019, is changing many things. It has put sustainability at the heart of corporate activity. It is also changing how Audi reports on its activities as part of 'consistently sustainable' – one of the four cornerstones of the strategy. The automotive industry is experiencing radical upheaval. The Audi Group is likewise in the process of redefining itself for the future and playing an instrumental role in shaping the transformation as we head into a new age of mobility. Step by step, we are implementing this strategy. Also, we have a mission that is to act purposefully, systematically, and with our full efforts – in other words, consistently. That is why our mission is also called "Consistently Audi."

Let me give you some of our vision too Mefat:

- In the long term, we will offer CO_2-neutral premium mobility.
- In the medium term, we will offer the strongest range of electric models amongst the premium competitors.
- By the middle of the coming decade, we will sell about a million electrified cars each year.
- By 2025, we will have reduced the CO_2 footprint of the Audi fleet by about 30 percent over the entire lifecycle. In this way, we will improve Audi's environmental impact.

2. What are the generic strategies applied (at functional, business, and corporate levels)?

Each product or strategic business unit needs a business strategy to compete successfully within its industry, Mefat. However, at the corporate level, Audi has to decide on more fundamental questions like: "Are we going to pursue the sport or luxury car at first place?" or "Is it perhaps better to invest more into the high-tech cars or should we focus on the car part instead?" On the functional strategies, we focus more on our customer's requests, feedback, and so on, so we can produce solutions that can improve their daily life. I would like to give more details to you Mefat, for sure I will send you our detailed strategies shortly.

3. Are company strategies well formulated and known by functional units?

Audi as we know is one of the biggest automobile manufacturers in the World, our management and board of directions have perfected the company strategies, would say 3 of them. Currently, we are working at Corporate Level, I am taking personal decisions related to various business areas in which the firm operates and competes in Albania, then also trying to convert those ideas to reality. Currently Audi corporate is to produce a high-quality car, followed by the latest high tech and design.

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

Audi is taking big steps in technology during the last 10 years, and I can say that during those 5 new years we will make huge differences not only for our company but for the entire world. We are planning to launch soon our newest high-tech car that will contain all data and systems in cloud infrastructure. The future is here, stay tuned.

5. Do the executives and board treat security as the basis for long term competitiveness?

I would say we include it, as general managers we mostly discuss ideas, strategies, and how to make the company running smoothly at what we are best car manufacturing. But during COVID-19 and our electrical models, we are focusing seriously on security.

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

Yes, Audi has a clear vision for the future: to reduce CO_2 emissions and become high tech in the balance as a company by 2025 - 2050. To get there, we're letting go of the things holding us back and reimagining how we bring our vehicles to the road—from the supply chain to the emissions at our production plants, to the design of our models' entire life cycle. As we are planning and going to electronic cars, which means that cybersecurity will be important for our company, we have already created our dedicated IT Security teams, followed by Risk Management and other IT professionals that will guarantee to our clients their safety on roads.

7. Does the company have a Cybersecurity capability? If yes, how it was developed?

Yes, the Audi IT Security team has developed and keep maintain the capability following our guidelines that contain 4 steps, Assess, Measure, Analyze and Improve.

8. How often are executives and the board are informed of the organization's cyber capability level and any attacks?

I check the reports would say 1 – 2 twice months, as we have currently CTO that is dealing with that, we have so many international business processes, so we cannot complete and check everything, but can say our offices are very well secured.

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

Over 10% of Audi capital goes for CyberSecurity and Technology fields. We are taking security at a high level of interest as we see our future on major high technology that will change the way we use our cars for entire life.

10. Has the business specifically identified the most important information collected and held by the business and the level of protection expected for that information?

Sensitive information of Audi are well protected and secured in Germany, our main headquarters there have 4 to 5 levels of security, where mostly specific teams and board members can access them. Our data slowly are passing everything online, the risk that we will face will be high, but our expert team is taking good care of it.

11. How to treat cybersecurity as a business or IT responsibility?

Audi treats cybersecurity as a part of the business and we mainly train our employees to know our Cybersecurity Policy, and make monthly training for them with the latest update regarding security.

12. How to align security goals with business priorities?

Aligning IT with business objectives requires a commitment and a roadmap is a critically important topic in academic and industry. It is the key to success for modern organizations that are needed to survive and compete. It refers to the degree of congruence between business and IT strategies.

13. How to identify and protect the most valuable business processes and information?

Protecting confidential information assets throughout an enterprise is a journey rather than a one-time event. It fundamentally requires a systematic way to identify sensitive data; understand current business processes; craft appropriate access, usage, and distribution policies; and monitor outgoing and internal communications. Ultimately, what is most important to understand are the potential costs and ramifications of not establishing a system to secure nonpublic information from the inside out. From my knowledge as the General Manager of Audi in Albania, I can say that our security team follows a small 5 step procedure like:

- Identify and prioritize confidential information
- Study current information flows and perform a risk assessment
- Determine appropriate access, usage, and information-distribution policies
- Implement a monitoring and enforcement system
- Review progress periodically

14. How to ensure that the organizational culture supports a secure cyber environment?

At Audi, we have the opinion that the security department is responsible for security. Sustainable security culture requires that everyone in the organization is all in. Everyone must feel like a security person. This is a security culture for everyone. Security belongs to everyone, from the executive staff to the lobby ambassadors. Everyone owns a piece of the company's security solution and security culture. When someone goes through the mandatory security awareness program and completes it successfully, give them a high-five or something more substantial. A simple cash reward of $100 is a huge motivator for people and will cause them to remember the security lesson that provided the money. They also will be quick to tell five co-workers they received cash for learning, and those five will jump into the training quickly. If you are shuddering at the idea of giving away $100 per employee, stop being so cheap and count the cost. The return on investment on preventing just a single data breach greatly outweighs the $100 spent.

15. Are the basics rights in place in a company?
    (For example, access rights, software patching, vulnerability management, and data leakage prevention.)

Yes, as I understood from your question you wanted to know about software and cyber threats that might happen at Audi. We daily update our software as we are using dedicated solutions for our car repair, modifications, and so on. All our employees have a clean desk policy that follows daily to guarantee confidentiality, integrity, and availability. In general, all policies are strictly followed to guarantee safety in our workplaces.

16. Does the company focus on security compliance or security capability? Does the company have a cybersecurity capability?

I can say as General Manager, that Audi might be one of the first companies in Albania that had even a Cybersecurity Policy. We do have a dedicated team that focuses on security compliance and capability, but our main company focus is not security, and yes I confirm that Audi has an international cybersecurity policy and capability, mostly by ISO standards.

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

No, everything is located in our offices, we protect our information, Audi since start never had any agreement with any third-party for securing any of our information.

18. Does the company regularly evaluate the effectiveness of our security? How it is measured?

Audi has an analyst team for evaluating the effectiveness of security. This team measures it by tracking the False Positive Reporting Rate. Analysts are tasked with sifting out false positives from indicators of compromise before they escalate to others in the response team. Despite the implementation of automated filtering, the SOC team must make the final determination as to whether the events they are alerted to are real threats. The reporting of false positives to incident handlers and higher-level management increases their already heavy workload and, if excessive, can de-motivate and cause decreased vigilance. A high FPRR will generally indicate the need for more accurate detection technology and better tuning of analytics tools. This team also perform regular security audits.

19. Does the company monitor CS systems, and can the company prevent breaches?

Yes, we daily monitor the CS systems, our Cybersecurity testes do their best to find and avoid data breaches on Audi servers, and data centers. I cannot say they did not have any data branch during those 5 years, but finally, we manage to keep everything backed and safe. How we take actions to prevent this to happen is by limiting access to our most valuable data, updating our software regularly, conducting employee security awareness training, and developing our cyber breach response plan.

20. Is there an organized plan for responding to a security breach?

Yes, Audi has a very detailed plan to respond to the security breach, but for security reasons, I am not allowed to share it, but I will tell the main key parts we follow.

- Identification
- Containment
- Eradication
- Restoration

21. Is the company resourced and insured against cybersecurity risks?

Audi is well resourced and insured about cyberattacks and risks, we have very well structured teams who perform daily penetration hacking of our systems,

I must thank Mr. Gentian Bushati for the full 2 hours he was sharing his ideas and accepted the interview with me, I specify him that the interview was for study purpose, and he gladly helps.