Thoughts about cybersecurity and workplace innovation

Introduction

Security and safety are important fundamental needs in every human. Without it is easy to argue that creativity and innovation will suffer. The last decade has seen an increase in cyber threats. Organizations have experienced a 435% increase in ransomware[i] in 2022 (WEF, 2022a). In addition, the World Economic Forum's cybersecurity report states that 95% of cyber incidents can be traced back to human errors (WEF, 2022b). These numbers tell that cyber security is first and foremost an organizational issue and not a technical issue. Organizations should prepare how they deal with attacks, not thinking that they will not be attached, due to small size, good internal competence, having a service provider for it, etc. The threats have grown in the wake of the ongoing digitalization of processes and activities. However, the long-term influence of a cyber incident is purely understood.

SFI NORCICS

Centers for Research-driven Innovation (SFI for short in Norwegian) is a Norwegian tool to enhance the continuous innovation in Norwegian companies helped by universities and research institutes. One such center is NORCICS (Norwegian Center for Cybersecurity in Critical Sectors). Since Norway is among the most digitalized countries in the world, the center's vision is to contribute to making Norway the most securely digitalized country in the world by improving the cybersecurity and resilience of critical sectors, through research-based innovation. One focus area is the human and organizational impact of cyber-attacks and how to learn from them to become more resilient. A story can illustrate such impacts.

Big company case

Early one morning: 35.000 employees in 40 different countries got the message to not log on to any computer or any device. The company was under a sophisticated cyber-attack. During the night, the top managers tried to figure out how to communicate this without any functional communication platform. Soon, it was obvious to them the only way was to choose an extremely open policy for communication. Putting out information on Facebook and WhatsApp as basic tools, and within a week establishing a new website, in addition to daily press conferences. The policy included a focus on the people behind solving the problems, the cyber heroes, as the company called them. They invited journalists to visit these heroes and even opened the control room for such visits. The media praised the openness and received a prize for openness in crisis.

Seemingly, they did everything right, and the stock market responded with a raised stock price during the crisis. The employees at the production plants felt it differently. An interview with the person in charge of ICT at one of the production plants in Norway told an interesting story. The plant was in a small community where everyone either worked at it or the plant was the reason for their existence. Coming to work that morning, a handwritten note met the workers telling them not to log on or start their PCs, a frightening message. Everybody felt an existential threat, especially from the ICT person in charge. He felt that the entire future of the small community lay on his shoulders. If he doesn't fix this and get the production started, the plant will be closed for good. An enormous responsibility that was not part of his job description. However, the main office flew in experts with a helicopter to help this poor man. The other employees saw this unusual helicopter with experts, and it

contributed to more uncertainty. In this situation, Facebook, WhatsApp, and the press briefings were vital to getting reassuring information to all employees.

Eventually, the attack is estimated to cost 800 mill. NOK.

Short about the theoretical lens

Employee-driven innovation (EDI) is a concept that has gained interest in the last decades. It tries to answer the fundamental question "How do employees who are learning in the work-place produce innovation?" (Høyrup, 2012). It aims to tap into the ordinary employee, that does not have innovation in their job description, effort to learn and innovate for increasing productivity. Høyrup (2012) argues that it has three strategic dimensions, bottom-up, mixed, and top-down pointing to where the initiative originates from. Opland (Opland et al., 2022) argue for the concept of employee-driven digital innovation, where the digital tools for creating innovation are central. However, in the employee-driven digital innovation framework the cyber security issues are missing. Illustrated by the case, several burning issues emerge.

Why is this story important?

First, it shows that it is not a question about how to prevent a cyber-attack, but what do you do when attacked? Even big companies with lots of resources for preventing cyber-attacks do not go untouched. Training and planning for such an event must be high on the agenda in every company or organization.

Secondly, a cyber-attack will have a tremendous influence on any organization. It can be an existential frightening experience and therefore needs special attention. Little research has been done to understand how it affects innovation efforts and continuous improvement.

Thirdly, we are slowly realizing that learning through "pointing the finger – do not do this", is not the best learning tool. What types of training and knowledge are needed at the operator level to have better resilience for such events?

Fourthly, the person(s) that has unwillingly done something to expose the company for attack, should be taken care of. They will feel a big responsibility and be put under tremendous stress, just as much as the "heroes" in the story. How does the organization care for the personnel involved?

Conclusion

Workplace innovation needs to address cyber-attacks as a research field. The importance is just growing, and the impact will hamper the overall innovation efforts of any organization. Digital tools are essential for almost every work and innovation. Since the spread of cyber-attacks has accelerated and now is one of the major threats to the organization, we need to include aspects of it into our theories, EDI and workplace innovation. Perhaps, it would be fruitful to divide the efforts into how to build a robust organization, the notion of robustness, and how to deal with the attack and the aftermath of it, resilience. Robustness will include learning about cyber attacks and what to do, while resilience deals with training for such event, for example serious gaming.

References

World Economic Forum, 2022a, The Global Risks Report 2022, 17th edition.

World Economic Forum, 2022b, Global Cybersecurity Outlook 2022, insight report, January 2022.

Høyrup, S. (2012). Employee-Driven Innvation: A New Phenomenon, Concept and Mode of Innovation. In S. Høyrup, M. Bonnafous-Boucher, C. Hasse, M. Lotz, & K. Møller (Eds.), *Employee-Driven Innvation - A New Approach*. Palgrave Macmillan.

Opland, L. E., Pappas, I. O., Engesmo, J., & Jaccheri, L. (2022). Employee-driven digital innovation: A systematic review and a research agenda. *Journal of Business Research*, *143*, 255-271. https://doi.org/https://doi.org/10.1016/j.jbusres.2022.01.038

[i] Ransomware is a type of attack where the data of the organization is permanently blocked unless a ransom is paid.