The ‘Human as a Barrier’ in Cybersecurity Incident Response

Chidera Winifred Amazu\*, Gabriele Baldissone, Micaela Demichela

Politecnico di Torino, Corso Duca degli Abruzzi, 24, 10129, Turin, Italy

\*Corresponding author E-Mail: chidera.amazu@polito.it

1. Introduction

In safety-critical facilities like the process industries, cybersecurity is of grave importance, considering the magnitude of the consequences of a cyberattack, which seems to be somewhat similar to those of physical attacks (Iaiani et al., 2021). In many cases, there are huge losses, environmental, health and economic impacts, for example, due to data theft or loss, plant shutdowns, and so on (Boring et al., 2019; Iaiani et al., 2021). Therefore, it is generally safe to say that prevention of the attack itself is the best line of action.

A systematic review by Iaiani et al. (2021) shows that the attacks in such facilities, which can either be premeditated (internal or external) or accidental (internal attacks), are usually targeted at not only the information technology (IT) system but also the operational technologies from the physical plant systems to higher level management devices. For example, in their review, it was reported that while IT systems were largely infected, the number of operational technology (OT) systems affected was higher. A key OT vulnerability for such attackers involves monitoring and supervision systems, for example, the HMI workstations in control rooms. Out of 23 OT infection attack cases reported, 12 were on the monitoring systems, while those on the control systems and the safety and alarm systems were 8 and 3, respectively.

An attack on important systems as the monitoring and control systems are vulnerabilities as it is possible to infiltrate such OT system making information unavailable as in the case of denial of service (Iaiani et al., 2021) or fills the system with wrong information on process parameter presented to the operators as in the case of man-in-the-middle attacks (Nystad et al., 2020) or where same information is presented over and over like in the replay attacks (Nystad et al., 2021). These have been some of the notable forms of attacks on the monitoring and control systems. In these situations, operators can, through their behaviour and actions, introduce vulnerabilities.

The intention of the attacker, towards operators, is to deceive and ensure poor situational awareness, leading to poor detection and errors in interpretation and response to events. Operators during these times are generally reported to have been observed to assume technical or safety issues in such cases and dire cases resorting to using procedures meant for emergency responses involving eventual plant shutdowns (Nystad et al., 2020). While IT measures are largely introduced to curb such human vulnerabilities, such as the use of passwords, single or two-factor authentication, firewalls, and other company policies etc, certain cognitive, behavioural and correct response targeted measures have been neglected (Boring et al., 2019).

Though the ‘human’ has been cited as a weak link because of the vulnerabilities they introduce and can become a source of premeditated internal attacks (Harper, 2023), their potential to detect, communicate, and perform further roles, as represented in Figure 1, would be advantageous for the industry. However, just like in any human-in-the-loop setup requiring operator involvement, there ought to be a combination of the right set of factors, including dynamic or traditional factors that can make operators’ responses effective. For example, typical factors like the HMI, training, experience, procedures, etc and dynamic ones related to cognition (workload, situational awareness, and so on). Typically, these factors interplay with each other, especially organisational and technical factors on individual factors like behaviour, cognition, etc. There has been a mention of the practical role of factors such as situational awareness, trust in one's capability, communication, training, and procedures in supporting operators and how the combination of these factors can get the operator to be more confident and take ownership (Nystad et al., 2020; Harper, 2023). This is better illustrated in the incidence response chart on Figure 1, where, as shown in the internal illustration, the operator could have a perception of a possible threat, but would need a combination of cognitive activities like recall from memory on training or procedures to be more confident in taking decisions and communicating effectively and would eventually require a experience or some sort of manual to effectively take actions. It is not merely a simple single factor role, but a combination of extrinsic and intrinsic factors, dynamic or static.



Figure 1. Incidence response flow and the role of factors like procedures, etc. Adapted and represented from Cichonski P. et al., 2012 and Harper, 2023.

Despite the need to understand how these factors put together can be of aid to operators for effective intervention and to minimise the vulnerabilities they introduce, there is little out there particularly investigating the aspect of the ‘human’ as a barrier in incidence response during cyber-attacks. This paper briefly discusses two current grey yet important areas in incidence response to understand operator behaviour and factors that shape this and the type of aids that should be included as standard. These areas further form key future exploration topics for exploration, design and eventual testing via an experimental and observatory approach.

2. Exploring the role of operators

The areas to be explored by the authors are briefly mapped in Figure 2 and are discussed briefly below. The top left figure shows the research areas of interest, which includes, firstly, comprehensive research on the key factors acting interchangeably and impacting particularly when operators are included as actors and involved in any of the roles mentioned in Figure 1. The idea is to address questions such as the role of such factors in influencing cognition, behaviour and eventually success, which factors stand out in each of the 6-incidence response roles, and so on. Secondly, an exploration of a couple of operator aids augmented on the interface displays, procedures, or independent aids to facilitate support at different stages, as shown in figure 1, but also to support training and learning on cyber-attacks. It seeks to address the questions of the suitability of current displays, display elements and procedures for intervention in cyber events, the type of elements, tools or agents that can facilitate teaming for detection, communication, analysis and so on.



Figure 2. Caption. [Arial 10].

The actors, cybersecurity, have been added because, in some facilities, these persons are present and usually communicate events with the control room operators and vice versa. According to Nystad et al. (2020), in the situation of cyber-attacks, both control room operators and cyber/IT security teams are to maintain communication and possibly have a similar display overview of what is happening, resolution actions, etc. The bottom right loop shows the different stages of the security risk assessment of the API RP 780 methodology. The idea of mapping the two is to show that this research work eventually explores security risk assessment but factors in an important yet unexplored area in security risk assessment of process industries, which is the operator reliability.

2.1 Defining Factors

The need for understanding key behaviour and performance-shaping factors in cyber-attack scenarios has already been established in the introductory section of this paper. Some factors highlighted so far from the reviewed literature to the best of the authors’ knowledge, are quite common in the control room setting, for example, experience, training, procedures, etc. (Nystad et al., 2020; Harper, 2023). There are some others that, though commonly mentioned, are not very much included in many of the pre-defined factors for human reliability assessment, for example, communication, which is very paramount between cyber and control room operators as investigated by (Nystad et al., 2020). In addition, some factors have been identified as peculiar, especially for such scenarios such as Confusion, Trust in the HMI display elements as observed by Nystad et al. (2020), and Trust and Confidence in one's ability to intervene as highlighted by Harper (2023). The inner picture in Figure 1 depicts the role of confidence in launching operators to the point of action, which can be supported by factors like procedures, training, and so on.

A nuclear control room experimental study by Nystad et al. (2020) comes in handy to illustrate further the role of factors and perhaps aids in such settings. It was observed from their study that despite the experience of turbine operators, the operators assumed the events to be due to instrumentation failure until further communication with the cyber-IT team. Feedback from the cyber team, however, made them lose trust in the instrumentation and control (I&C’s) on the HMI. Typically, the attacker took the man-in-the-middle approach in this study. There was no situational awareness, which, according to the authors, would not have been the case with proper training accompanied by response procedures, which should not be used independently of one another. Therefore, the following points and questions should be needfully explored regarding the defining factor in cyber-attack scenarios:

* What factors are defining factors in such human-in-the-loop configurations? The concept of human-in-the-loop in process control rooms has been explained by Amazu et al. (2022).
* How can some of these less commonly mentioned factors be measured and included in the eventual evaluation of operator response capability?
* What role does the interplay between these factors play in shaping behaviour and successful incidence response?
* How can these factors harness or drive the development of operator aids?

2.2 Operator Aids

The most common aids or decision and action support aids in control rooms are the human system interfaces comprising the interface and their display and display elements, procedures and alarm systems (Amazu et al., 2024). However, there are new AI support introductions mentioned or already tested to explore their capabilities in aiding operators at different points of their tasks. For example, use of adaptive interfaces (Hinss et al., 2022), AI recommendation system (Mietkiewicz et al., 2023), virtual reality sets (Roldán et al., 2017), presentation of playbacks or timelines of events with bookmarks (Scott et al., 2006), and temporal image/object presentation and removal (Peysakhovich et al., 2018). The last three have been specifically cited to be effective in increasing situational awareness and interruption recovery.

Situational awareness (SA) can be enhanced through experience or expertise, as this leads to greater activation of long-term memory — particularly procedural and semantic memory. However, for beginners, it is often more effective to provide support for their working memory (Sohn and Doane, 2004). Regular simulation-based training can also play a key role by allowing operators to practice tasks that may not occur frequently but must remain readily accessible in their working memory. A comparable example can be found in aviation, where pilots undergo routine simulations to reinforce emergency procedures and ensure quick, accurate recall when needed. Again, the above examples reinforce training, experience and procedures for situational awareness. How about the capability of these aids or potential aids to minimize confusion or reinforce confidence? Therefore, in developing aids, it is important to understand the defining factors with some of these very common aids already a part of them. It is also vital to propose aids that target experienced versus novice operators. Despite the mention of aids that can come in the form of elements embedded on the HMI, procedures, training tools, etc, there is not a lot out there on the development of such for incidence response with the operators in mind.

The authors, through further research, explore the following points relating to operator aids during cyber attacks

* What type of elements and tools can be adapted on the HSI or asides the HMI to aid operators?
* What should the eventual outlook of training, procedures and other human system interfaces be?
* How do these aids address negative tipping points from the defining factors influencing economy, health, and safety?
* What are the pros and cons of potential teaming agents or other support agents in such scenarios?

2.3 Human Centered Studies

Improving how operators respond during cyber incidents starts with understanding their actual experiences, not just what systems expect of them. The way people act in high-pressure situations, especially when dealing with unfamiliar problems or incomplete information, often depends on more than just training or procedures. The way operators respond often comes down to how tools are laid out, what kind of information is actually visible to them, and whether they feel confident enough to make a quick call under pressure.

Because of that, this study keeps the focus on the people who are using the systems. Instead of assuming what might work in theory, it looks at how operators behave in real situations: what they notice, how they react, and where things get difficult. Their input is not just helpful; it is necessary to build anything that will truly work in practice. Their insights help shape the direction of any improvements, ensuring that solutions are actually practical and not just theoretical.

The goal is to identify which factors really matter when it comes to operator performance during cyber-attacks: things like confidence, trust in displays, or even confusion. It’s one thing to notice when things don’t go as planned, but the harder part is figuring out what helps operators make good decisions under pressure. That is where the real value is — understanding what gets in their way and what genuinely supports them in the moment.

This is not something that can be worked out just by looking at data from a distance. That is why the approach here involves watching people in action: how they respond, what they miss, where they hesitate. What is good or bad behaviour and how can this be guided? It is about learning from the way both new and experienced operators deal with realistic situations, not just ideal ones. It brings in operators with different backgrounds—from those just starting to others with years of experience. Watching how they handle different scenarios gives a clearer picture of what works, what confuses them, and where extra support might be needed.

At the core, it is about designing systems that actually fit the way people think and work. Operators are a critical line of defense. But to do that job well, they need tools and training that make sense in the moment, not just on paper.

2.3.1 Future Experiments

The SERICS project, through a human centred observational and experimental study, aims to investigate operators’ behaviour and decision-support potentials for correct incidence response during cyber-attacks. To address the posed questions in this work, the experimental design will involve different human in the loop configurations that:

* follows a similar process industry case study as previously applied by Amazu et al. (2024). This will comprise scenarios of easy to high complexity levels driven, in this case, by both process and cyber-attack complexity. The varying of task complexity serves two purposes: 1. to evaluate operators’ states: cognition, behaviour, readiness, etc, and tipping points for targeted support, 2. t o evaluates the impact of the type of support during different cyber situations.
* will be shaped by a couple of the identified defining independent factors, especially decision-support factors/aids like training and procedures. Training will be defined at different levels of training aids – videos, manuals, serious games, etc, while procedures will be paper, digital and in different procedure formats – listed or flow charts.

3. Conclusion

The potential of operators as preventive and protective barriers is often overlooked, especially during cyber-attacks. Rather, much attention is placed on technical defences.

This paper outlined key areas where further research is needed: identifying the factors that shape operator behaviour and successful response in high-stress cyber scenarios and developing aids that genuinely support them in making timely, informed decisions and taking correct actions. Aids that are well-designed and based on how people behave can make a meaningful difference in reducing risk.

By taking a human-centred approach and involving operators directly in the development, design and testing of these tools, this work aims to shift the narrative from seeing the human as a weak link to recognising them as an active line of defence.

4. Acknowledgments

This work was partially supported by project SERICS (PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union - NextGenerationEU

References

Amazu, C. W., & Demichela, M., Fissore, D., 2022. Human-in-the-Loop Configurations in Process and Energy Industries; A Systematic Review. 3234-3241. 10.3850/978-981-18-5183-4\_S33-04-572.

Amazu, C. W., Mietkiewicz, J., Abbas, A. N., Briwa, H., Alonso-Perez, A., Baldissone, G., Fissore, D., Demichela, M., Leva, M. C., 2024. Exploring the Influence of Human System Interfaces: Introducing Support Tools and an Experimental Study. International Journal of Human–Computer Interaction, 1–18. https://doi.org/10.1080/10447318.2024.2376354

Boring, R., Ulrich, T., Medema, H., Lew, R., 2019. Operator Resilience to Cyber Interdictions in Nuclear Power Plants. 247-251. 10.1109/RWS47064.2019.8971820.

Cichonski, P., Millar, T., Grance, T., & Scarfone, K., 2012. Computer Security Incident Handling Guide : Recommendations of the National Institute of Standards and Technology. https://doi.org/10.6028/nist.sp.800-61r2

Harper, W., 2023. Cybersecurity: a review of human-based behavior and best practices to mitigate risk. Issues in Information Systems, 24(4), 247–254. <https://doi.org/10.48009/4_iis_2023_119>

Hinss, M. F., Brock, A. M., Roy, R. N., 2022. Cognitive effects of prolonged continuous human-machine interaction: The case for mental state-based adaptive interfaces. Frontiers in neuroergonomics, 3, 935092. https://doi.org/10.3389/fnrgo.2022.935092

Iaiani, M., Tugnoli, A., Bonvicini, S., Cozzani, V., 2021. Analysis of Cybersecurity-related Incidents in the Process Industry. Reliability Engineering & System Safety. 209. 107485. 10.1016/j.ress.2021.107485.

Mietkiewicz, J., Abbas, A. N., Amazu, C. W., Baldissone, G., Madsen, A. L., Demichela, M., & Leva, M. C., 2024. Enhancing Control Room Operator Decision Making. Processes, 12(2), 328. https://doi.org/10.3390/pr12020328

Nystad, E., Katta, V., Simensen, J., 2020. What happens in a control room during a cybersecurity attack?: Preliminary observations from a pilot study. 10.1145/3387940.3391454.

Nystad, E., Simensen, J., Raspotnig, C., 2022. Investigating operative cybersecurity awareness in air traffic control. 10.1109/SIN54109.2021.9699158.

Peysakhovich, V., Lefrançois, O., Dehais, F., and Causse, M., 2018. The neuroergonomics of aircraft cockpits: the four stages of eye-tracking integration to enhance flight safety. Safety 4, 8. doi: 10.3390/safety4010008

Roldán, J. J., Peña-Tapia, E., Martín-Barrio, A., Olivares-Méndez, M. A., Del Cerro, J., and Barrientos, A., 2017. Multi-robot interfaces and operator situational awareness: study of the impact of immersion and prediction. Sensors 17, 1720. doi: 10.3390/s17081720

Scott, S. D., Mercier, S., Cummings, M. L., and Wang, E., 2006. Assisting interruption recovery in supervisory control of multiple uavs. Proc. Hum. Factors Ergon. Soc. Ann. Meet. 50, 699–703. doi: 10.1177/154193120605000518

Sohn, Y. W., Doane, S. M., 2004. Memory Processes of Flight Situation Awareness: Interactive Roles of Working Memory Capacity, Long-Term Working Memory, and Expertise. Human Factors, 46(3), 461-475. https://doi.org/10.1518/hfes.46.3.461.50392