Towards an enriched language for communicating IT risks for cyber resilience

Fifty shades of orange and beyond.

Keywords: IT risk reporting, cyber resilience, organizational learning, IT governance, behavioral risk, language, metaphors

Information technology (IT) and IT-related risk have become so relevant that it is (or at least should be) a topic of conversation even down to the boardrooms of large corporations and government. This concerns not only the strategic use of IT, but also the extent to which the organization is able to foresee cyber risks in a timely manner to be able to adequately respond. Moreover, while popular emerging digital technologies (e.g., artificial intelligence (AI), Internet of Things (IoT), cloud technologies, and 5G) have the potential to enable impressive business growth, they also have the potential to vastly increase cyber risk.

Even though cyber risk has been promoted as an important focus for corporate governance, that should as such be on the radar of the board of directors (De Haes et al., 2020), many boards are still not well-equipped to perform their strategic roles related to cyber risk (Valentine, 2016). In order to be able to take responsibility for cyber risk in the boardroom and ask the right questions to the expert IT managers within the organization (e.g., CIO, CISO, senior IT management), adequate measures of IT governance should be in place. This involves things like proper information about cyber risks coming from the organization, and board composition and expertise to be able to make an appropriate assessment of cyber risks.

Cyber risks, however, are becoming increasingly complex and dynamic. While most research has focused on the technical aspects of cyber risks and security, a broader approach, including behavioral perspectives, would certainly be beneficial. This is because the course of risks is subject to our own behavior and how we personally assess risk. Risks can be captured less and less in “probability x impact”, but are much more ambiguous (Eling et al., 2021). This raises the question of whether the current dominant way of reporting cyber risks (in the form of traffic light reports) needs improvement.

An experiment by Nuijten et al. (2022) shows that IT experts rate IT-related risks (including cyber risks) higher than non-experts. Non-experts' risk estimates also appear to vary more strongly between individuals depending on their personal risk propensity. These interpersonal differences are more prominent when risks are ambiguous. Like an orange traffic light, these are risks turning orange in heat-map/risk reports. Whereas there is reasonable unanimity on risk assessments and decisions at a red traffic light (almost everyone stops) or green traffic light (almost everyone drives on), it is precisely the ambiguous (i.e., orange group) risks that are multi-interpretable and lead to divergent risk assessments (as a metaphor, some people suddenly brake at orange while other people still accelerate quickly).

Other experimental research shows that IT managers estimate IT-related risks (including cyber risks) lower than IT auditors (Nuijten, Keil, van der Pijl and Commandeur 2018), and more generically: people who are themselves "in charge" (sitting at the steering wheel) estimate cyber risks lower than those not in charge (in the passenger seats). Again, it appears that the differences are greatest for ambiguous risks (i.e., orange group). Also, previous experimental research shows that the relationship between driver and co-driver (as partner or opponent) plays a major role in communication about IT-related risks (including cyber risks) (Nuijten, Keil and Commandeur, 2016). In conclusion, we posit there is potential bias in the way in which various stakeholders communicate and interpret cyber risks, which results in the need for an enriched approach to communicate about cyber risks. More specifically, we pose that a more refined language is needed to communicate and understand the dynamic nature of cyber risks, especially in the context of cyber resilience.

This PhD study has three objectives. Firstly, we examine biases in the use of traffic light reports (green – yellow- red) to communicate cyber risks. Secondly, we probe an enriched and refined language for communicating cyber risks by using metaphors that capture the dynamics of cyber risks and could serve as an instrument for communicating cyber risks between IT experts and C-level executives. Thirdly, we place these insights in the context of a move beyond ‘traditional’ cyber risk management towards cyber resilience to assess their relevance and implications.

PhD-study part 1: Testing biases in the use of traffic-light reporting of IT-risks

The first part of the PhD-study will focus on biases that stem from traffic-light reporting. This could be in the form of an experiment, similar to Nuijten et al., 2016, 2018, 2023 and could specifically focus on the effects of orange traffic-light reporting on risk perceptions and decisions. Next to an experiment, this topic could be examined through vignette-study, focus group or Q-sort to further obtain insights in how relevant stakeholders in practice assign and interpret ‘orange cyber risks’ as a rudimentary form of communicating cyber risks. A third option for this part of the study could be to measure and identify biases in the textual language that people use to describe ‘orange risks’, similar to Benschop et al (2020).

PhD-study part 2: Probing a metaphor to communicate IT-risks.

To facilitate organizational learning, Gareth Morgan (1997) suggest the use of metaphors as a language to interpret and make sense of behavioral patterns within the context of an organization. For the purpose of this study, we adopt the metaphor of an organization as an organism that could suffer from vital risks and how they relate to habits, symptoms, treatments and effects.

Since cyber risks are dynamic, emergent and can be vital to the organization, we were inspired by how patients and doctors communicate about risks, symptoms, pain, and effects that are vital to the patient's health (Nuijten & van Twist, 2019). One of the starting points of the second part of the study could be how such metaphors could provide a more enriched language to communicate risks between IT-experts and non-experts (i.e., C-suite executive level) within the organization. The improvement of using such metaphors could be assessed by how they resolve biases that are found in traffic-light reporting of cyber risks as well as how it changes the organization behavior to be more resilient to cyber risks.

PhD-study part 3: Moving beyond 'traditional' cyber risk management, towards cyber resilience.

Due to the complex and adaptive nature of cyber risk, interactions between risks need to be considered, and effective cyber risk governance needs to be developed that promotes resilience and adaptation in response to a volatile, uncertain, complex, and ambiguous threat environment (Scala et al., 2019). Based on Starr et al. (2003), *cyber resilience* could be defined as "the ability and capacity to withstand systemic discontinuities and adapt to new [cyber] risk environment." Resilience is useful for risks that are unexpected (i.e., impossible to identify in advance) and for which risk analysis as part of 'traditional' risk management is less (or not) effective (Linkov et al., 2014). In line with Gisladottir et al. (2017), we probe that a cyber resilience approach requires an inter-disciplinary move, to include behavioral perspectives.

This third part of the study aims to investigate the implications of cyber risk assessment and communication tools on cyber resilience. Particularly, we augment cyber risk assessment with organizational learning research to investigate how cyber risk assessment might contribute to cyber resilience at multiple (interacting) learning levels (i.e., individual, team, and organizational) (for instance based on Crossan et al. (1999)), in line with De Maere et al. (2022). Moreover, this study may explicate what aspects of (organizational) learning are particularly useful in the context of cyber security and dealing with cyber risks. For instance, learning from failure is a well-elaborated stream and can be translated to anticipated resilience (Argote et al., 2021), and arguably fits well to the context of cyber security. Yet, it is unclear how and under which conditions learning from failure is more effective for resilience in general, and cyber resilience in specific. An unbiased risk assessment or a well-developed risk communication tool might illuminate and inform this unclarity.

Note

Depending on the PhD-candidate, any of the three parts discussed above could receive more weight in the PhD-project. While the formal station for this PhD project is the OU's headquarters in Heerlen, the supervisory team is not opposed to hybrid forms of working. Moreover, the supervisory team is geographically dispersed, and has links to other universities and business schools in the Netherlands and Belgium, as well as to several national and international practitioner organizations that could prove useful for the research activities and the candidate's network.

References

Argote, L., Lee, S., & Park, J. (2021). Organizational learning processes and outcomes: Major findings and future research directions. *Management science*, *67*(9), 5399-5429.

Benschop, N., Hilhorst, C., Nuijten, A. & Keil, M. (2020). Detection of early warning signals for overruns in IS projects: Linguistic analysis of business case language. *European Journal of Information Systems,* Vol. 29, No. 2**,** pp. 190-202.

Crossan, M. M., Lane, H. W., & White, R. E. (1999). An organizational learning framework: From intuition to institution. *Academy of management review*, *24*(3), 522-537.

De Haes, S., Van Grembergen, W., Joshi, A., & Huygh, T. (2020). *Enterprise Governance of Information Technology, Third Edition*. Cham: Springer.

De Maere, K., De Haes, S., von Kutzchenbach, M., & Huygh, T. (2022). Identifying the Enablers and Inhibitors of Organizational Learning in the Context of IT Governance: An Exploratory Delphi Study. *Information Systems Management*, *39*(3), 241-268.

Eling, M., McShane, M., & Nguyen, T. (2021). Cyber risk management: History and future research directions. *Risk Management and Insurance Review*, *24*(1), 93-125.

Gisladottir, V., Ganin, A. A., Keisler, J. M., Kepner, J., & Linkov, I. (2017). Resilience of cyber systems with over-and underregulation. *Risk Analysis*, *37*(9), 1644-1651.

Linkov, I., Bridges, T., Creutzig, F., Decker, J., Fox-Lent, C., Kröger, W., ... & Thiel-Clemen, T. (2014). Changing the resilience paradigm. *Nature Climate Change*, *4*(6), 407-409.

Nuijten, A., Keil, M. & Commandeur, H. (2016). Collaborative partner or opponent: How the messenger influences the deaf effect in IT projects. *European Journal of Information Systems,* Vol. 25, No. 6**,** pp. 534-552.

Nuijten, A., Keil, M., Pijl, G.v.d. & Commandeur, H. (2018). IT managers' vs. IT auditors' perceptions of risks: An actor–observer asymmetry perspective. *Information & Management,* Vol. 55, No. 1**,** pp. 80-93.

Nuijten, A., Keil, M. & Zwiers, B. (2022). Internal Auditors' perceptions of IT related risks: A comparison between IT experts and non IT experts. *Journal of Information Systems,* Vol. preprint.

Nuijten, A. & Twist, M.v. (2019). Capturing temporal risks in metaphors. *Audit Magazine,* Vol. 4**,** pp. 22-25.

Scala, N. M., Reilly, A. C., Goethals, P. L., & Cukier, M. (2019). Risk and the five hard problems of cybersecurity. *Risk Analysis*, *39*(10), 2119-2126.

Starr, R., Newfrock, J., & Delurey, M. (2003). Enterprise resilience: managing risk in the networked economy. *Strategy and business*, *30*, 70-79.

Valentine, E. L. (2016). Enterprise technology governance: New information and technology core competencies for boards of directors. *Queensland University of Technology*.