Digital security governance: What can we learn from high reliability organizations?

Stef Schinagl
Vrije Universiteit (VU) Amsterdam
s.schinagl@vu.nl

Abbas Shahim
Vrije Universiteit (VU) Amsterdam
a.shahim@vu.nl

Svetlana Khapova
Vrije Universiteit (VU) Amsterdam
s.n.khapova@vu.nl

Bart van den Hooff
Vrije Universiteit (VU) Amsterdam
b.j.vanden.hooff@vu.nl

Abstract

With the growing digitalization of businesses, digital security governance (DSG) is becoming central to organizational survival strategies. However, many organizations fail to establish successful DSG practices and, consequently, fail to understand how DSG can lower the severity of cybersecurity failures. This paper aims to contribute to filling this gap. By putting the five principles of the High Reliability Organization (HRO) central to the design of our qualitative investigation, we engage in interviewing forty-two chief information security officers (CISOs) and chief information officers (CIOs) of large organizations in the Netherlands about their views on why organizations fail to successfully achieve DSG. Our data show that HRO principles are partly relevant but lacking in DSG approaches, which potentially increases security failure. We conclude this paper by discussing these findings in light of future research and practice.

Keywords: Cybersecurity, IS-security, Digital Security Governance, High Reliability Organizations.

1. Introduction

Digital security governance (DSG) is of strategic importance for contemporary organizations [1, 17, 18, 19]. Hence, today's businesses are exposed to high risk as they digitally transform. Technology, such as the cloud, mobile devices, big data and the Internet of Things, supports companies in the context of digital innovation (speed, agility, and connectivity), but it also substantially increases the attack surface [8, 17, 19, 20]. Cybersecurity attacks now have the potential to cause major disruption to our businesses and society, including damage to assets, people, and the environment [14].

Organizations, therefore, now recognize the importance of fundamentally shifting their security approaches "from the basement to the boardroom", that is, from a narrowly focused isolated IT-technical issue toward a strategic, embedded and institution-wide business issue [1, 6, 13, 17, 18]. Recent literature on strategic considerations of information security in the digital context refers to the concept of DSG [1, 17, 18].

However, the ongoing threat of successful cyberattacks, leading to security failures with large business impacts, shows that many organizations still perform poorly with respect to DSG [1, 9, 11, 18]. In addition, research on DSG is relatively immature, i.e., largely descriptive and provides both limited practical and theoretical guidance [11, 17]. This leads to the situation in which DSG studies do not comprehensively explain, supported by empirical data, the processes of establishing DSG in organizations or provide guidelines for its implementation [1, 11, 17,]. Therefore, a deeper understanding of how organizations and their DSG approaches become effective in the digital era is needed.

This research gap has especially drawn the interest of the authors, since research reveals that there are organizations that properly deal with the challenges of operating in high-risk environments with negligible failure and error rates. These organizations are called high-reliability organizations (HROs) [3, 4, 15, 23, 24]. Typical examples of such organizations are those involving aircraft carriers, air traffic control, submarines, and nuclear plants.

We argue that HRO principles are becoming increasingly relevant for contemporary organizations because today's technology-driven businesses are progressively operating in settings similar to those of HROs, e.g., complex and high-risk environments [16, 17].

Additionally, while traditional HROs remain nearly error free, contemporary organizations cope with security failures (close to) on a daily basis [10, 22]. Hence, HRO research represents a useful field of study where lessons can be learned and applied in the context of DSG. This paper, therefore, addresses the following question:

RQ: What can DSG learn from HRO principles to contribute to lowering security failures?

To answer this research question, we conducted a qualitative study and interviewed 42 chief information security officers (CISOs) and chief information officers (CIOs) of large organizations in the Netherlands.

URI: https://hdl.handle.net/10125/103355
978-0-9981331-6-4

The remainder of this paper is structured as follows. First, the theoretical background is discussed, after which our methods are explained. In the findings section, we provide an in-depth analysis of our empirical findings. The study concludes with a discussion of the research implications.

2. Theoretical Background

2.1 Digital Security Governance

In today's technology-driven environments, organizations are required to consider information security to achieve the sustainability and protection of the organization [1, 17, 18, 25]. In recent literature, the strategic consideration of information security in the digital context is referred to as DSG [1, 13, 17, 18]

DSG can be defined as steering the system (direct, control & monitor, execute) through which security is embedded in the organizational structures and all of the related business dimensions and organizational factors as a whole [18, 21].

By steering the system of components, DSG aims to keep a grip on the organization's strategic objectives and its protection, address required aspects of control and regulation, establish clear roles and responsibilities, ensure compliance with procedures, improve communications and knowledge sharing (about incidents and breaches) and ensure continuous evaluation and improvement [1]. Such security throughout the firm is considered the key to improving security in contemporary organizations [17].

However, as stated in the introduction, the proliferation of cyberattacks and their implications show that many organizations still perform poorly with respect to current DSG approaches [1, 9, 11, 17]. A deeper understanding of how organizations and their DSG approaches become effective in the digital era is needed. We provide a fresh lens by using relevant theories and help provide an in-depth understanding of how DSG lowers the risk of security failures. In this study, we focus on a stream of research that has addressed organizing around high-risk and hazardous technologies within organizations, particularly HROs.

2.2 Organizations in high-risk environments

The key consideration of scholars who have studied HROs originates from two main questions [15, 23, 24]: Are there high-risk organizations that have operated in a nearly error-free manner over long periods of time? If so, what do these organizations do to reduce the probability of serious error [15]? Within this stream of research, HRO scholars have a optimistic view of organizations in hazardous environments that embrace failure to achieve reliability [23, 24]. While studying HROs, researchers have identified similar characteristics in organizations that appear to operate in an error-free manner despite being very complex and operating under highly error-prone conditions [3]. Together, these characteristics lead to organizational mindfulness and reflect "a way of working characterized by a focus on the present, attention to operational details and an interest in investigating and understanding failures" [2]. The unique cognitive mindset that guides HROs entails five characteristics:

1. **Preoccupation with failure:** The first principle captures the need for continuous attention to be given to anomalies that could be symptoms of larger problems in a system. Therefore, HROs work hard to detect and learn from small, emerging failures because these failures may be indicative of further catastrophic breakdowns [15, 16, 23, 24].
2. **Reluctance to simplify interpretations:** Organizational mindfulness is generated by a reluctance to simplify because simplification obscures unwanted and unanticipated details; in doing so, it increases the likelihood of failure. In this way, HROs sense many details and can develop a richer and more varied picture of potential consequences [15, 23, 24].
3. **Sensitivity to operations:** HROs develop a holistic view of their operations and environments [16]. A sensitivity to operations is about work itself. It is about seeing what 'we' are actually doing regardless of our designs or plans. It is about paying close attention to what is going on right now (in real time), which is also called "having a bubble" [24].
4. **Commitment to resilience:** Effective HROs tend to develop both anticipation and resilience. Anticipation refers to the "prediction and prevention of potential dangers before damage is done," whereas resilience refers to the "capacity to cope with unanticipated dangers after they have become manifest and learning to bounce back" [16, 23]. HROs do not pretend to be error free, but their errors do not disable their operations [3].
5. **Deference to expertise:** HROs have a loose designation of who is the "important" decision-maker to allow decision-making and sensemaking to migrate to the "frontline" along with problems [23, 25]. This means that decisions and sensemaking migrate throughout the organization in search of a person or team who has specific knowledge of a given event. To do this, HROs let go of hierarchies [24]

While there are detailed descriptions and understandings of HRO processes in specific industries such as health care, supply chains, and safety, far less is

known about the extent to which these processes are transferrable to today's "mainstream" digital organizational contexts [3, 16]. In particular, linking HRO concepts to DSG is less documented [17]. The following section explains the potential of applying HRO principles to DSG.

2.3 How HRO principles contribute to DSG

DSG studied via HRO characteristics potentially contributes to achieving effective DSG practices. Hence, HROs establish a way of working that strives to achieve error-free performance while operating in complex and hazardous environments [3, 16, 23, 24]. Today's technology-driven organizations operate in settings similar to those of HROs, e.g., complex and high-risk environments [16, 17]. However, such organizations face cybersecurity failures nearly on a daily basis [10, 22], indicating the poor performance of today's DSG approaches [1, 9, 11, 18].

Against this backdrop, DSG can potentially learn from HRO principles, e.g., how to achieve more error-free performances with regard to cybersecurity. Until now, DSG research has concentrated on common practices (frameworks, standards, models), with a predominant focus on technical and procedural security controls [1, 17, 18]. This is troublesome because past research informs that organizational factors (governance, structures, learning orientation, culture, etc.), rather than technical and procedural controls play a role in almost all security incidents and are a critical part of understanding and preventing them [17]. Thus, applying HRO principles to DSG leads to a more holistic approach toward DSG and, therefore, can significantly contribute to the understanding of how to improve current DSG approaches and reduce security failures.

The HRO principles are further used to structure our findings, as we will explain in the following sections.

3. Methods

To further explore the issue of DSG, this paper reports on an in-depth qualitative study to examine how HRO principles apply to DSG. Our process is in line with the principles of an iterative approach to qualitative research rooted in grounded theory [7]. We explain our methods by discussing the research setting, data collection, research process and data analysis.

3.1 Research Setting

Data were collected from large organizations in the Netherlands. The Dutch National Cyber Security Center (NCSC) shows that the Netherlands is highly dependent on digital services, processes and systems. Additionally, the NCSC concludes that digital threats in such environments are of a permanent nature and cyber incidents can inflict socially disruptive damage and pose serious concerns and failures [12]. Despite these concerns, the NCSC also shows that the basic security measures that have been taken are still insufficient to counter cyberattacks and lower the risk of security failure. In this context, we believe that we find rich data "in what goes on" establishing effective DSG approaches and eventually answer our research question. Additionally, we focus on large organizations (*minimum # of employees >1000, average = 15,000*), as they better fit a high-risk profile due to their processing of large quantities of personal data and large streams of financial data.

3.2 Data Collection

The first author collected qualitative data in three stages between May 2019 and February 2020 (10 months) through 42 semistructured interviews. Twenty percent of the interviewees identified as female. The interviews are conducted at both public (40%) and private organizations (60%), of which 25% are listed. Most of the interviews were conducted face-to-face or by telephone (#3), and they were tape-recorded and fully transcribed. The interviews lasted between 25 and 99 minutes (an average of approximately 60 minutes).

To build trust and increase the probability of uncovering rich data, we ensured the anonymity of all interviewees in the data analysis. Additionally, we strived for transparency, so the transcripts were sent back to the participants for review. If corrections to the transcript were suggested, they were primarily related to the use of informal language concerning the company or the participant's boss or the presence of information concerning sensitive cases. These corrections did not impact the data richness, as we were more interested in understanding DSG in organizations.

3.3 Research process

We increased the analytical rigor of this study by dividing our investigation into three consecutive research phases (see also Table 1).

Phases	CISOs	CIO	Experts	Total
Phase 1	2	2	2	**6**
Phase 2	11	3	3	**16**
Phase 3	20			**20**
Total	**33**	**5**	**5**	**42**

Table 1. Interviews and informants

In the exploratory phase from November to December 2019, six face-to-face semistructured interviews were conducted. We used this first round of interviews to pilot our questionnaire and test the reaction of participants. Reflecting on these initial findings, we refined our research questions and designed our study accordingly to gain a deeper understanding of the research phenomenon.

In the second phase, we continued our qualitative study across different sectors and large organizations in the Netherlands. From October to December 2019, CISOs and CIOs across a variety of sectors were interviewed: health care, maritime, financial, technology, e-commerce, education, government and utilities. We also interviewed prominent experts, e.g., journalists, lecturers, researchers and public figures. These interviews helped us collect data and gradually increase our knowledge of the field. During this phase, 16 interviews were conducted, for which we followed a semistructured interview protocol.

In the third phase, between December 2019 and February 2020, we continued the qualitative study but further narrowed it down by interviewing only the CISOs of large organizations in the Netherlands. We focused on CISOs because they best fit the criteria of "knowledgeable agents"; namely, they were individuals in organizations who knew how DSG was implemented and could explain their thoughts, intentions, and actions from strategic to operational levels. During this phase, the semistructured interview protocol moved to the background, as we mainly focused on discussing the primary issues and tensions within DSG found in phase 2. HRO principles were used as a reflection "tool" to help facilitate deep, rich conversations and direct participants to give examples, pros and cons, clear statements, and more information about the research phenomenon.

Importantly, the interviewer always started with open-ended questions (e.g., How is security structured here? What are the main challenges? How does digitalization impact DSG?) instead of directly outlining the HRO concept at the beginning of the interview; this was done to stay close to our qualitative and inductive reasoning approach, which is in line with the Gioia method [7].

3.4 Data analysis

To analyze our data, we applied the structure of the Gioia methodology, which comprises three different levels of abstraction and is designed for inductive inquiry [7].

First, after reading the transcripts many times to gain familiarity with the data, the first author coded, grouped and classified the data. The initial analysis and coding of the interview samples helped identify the first-order concepts. The first level of coding showed the relevance and applicability of HRO principles in the digital security context. For instance, the first-order category "preparing for the unknown" was linked to the HRO principle of preoccupation with failure (Table 2), and that of "knowing your threat landscape to avoid blind spots" was linked to sensitivity to operations (Table 3). Our next step was to perform a second-order analysis by generalizing these categories into broadly conceptual themes. From the data, we identified the themes "security situation" and "problematization" as describing how HRO characteristics appear within the DSG phenomenon (also see Figure 1). Finally, our third-order aggregated dimensions were coded to show what DSG can learn from HRO principles; also see Figure 2.

Tables 2 and 3, and Figures 1 and 2 provide a graphical representation of our qualitative reasoning process and show how we moved from our raw empirical data to more abstract theoretical categories (aggregated dimensions) that reflect the applicability of HROs to the DSG context.

4. Findings

The findings section is structured according to the five principles of HROs. We emphasize the relevance of each principle for DSG. Based on our data, we focus on understanding how these principles are embraced and/or why they are not embedded in today's DSG approaches. Anonymized interview identifiers are used to code direct quotes from the interviews (# of interviews-interview phase). The data structure is visualized in Figure 1.

4.1 Preoccupation with failure

In the context of DSG, a mindset that is preoccupied with failure is relevant in the following ways. First, a preoccupation with failure is essential for security because organizations operate in environments with dynamic threats [2]. Since security failures are currently seen as inevitable, it is not a matter of if a company will be breached but when. This means that security organizations must anticipate failures and understand that 100% security does not exist.

Additionally, a preoccupation with failure is required in DSG implementations due to unknown factors or "black swans" with regard to security breaches, e.g., "zero-day" exploits. A zero-day exploit is an unknown vulnerability of an entity that aims to mitigate its vulnerability. Hackers can exploit such a vulnerability since there are no protective measures. See Table 2 for the data structure regarding "preoccupation with failure" in relation to DSG.

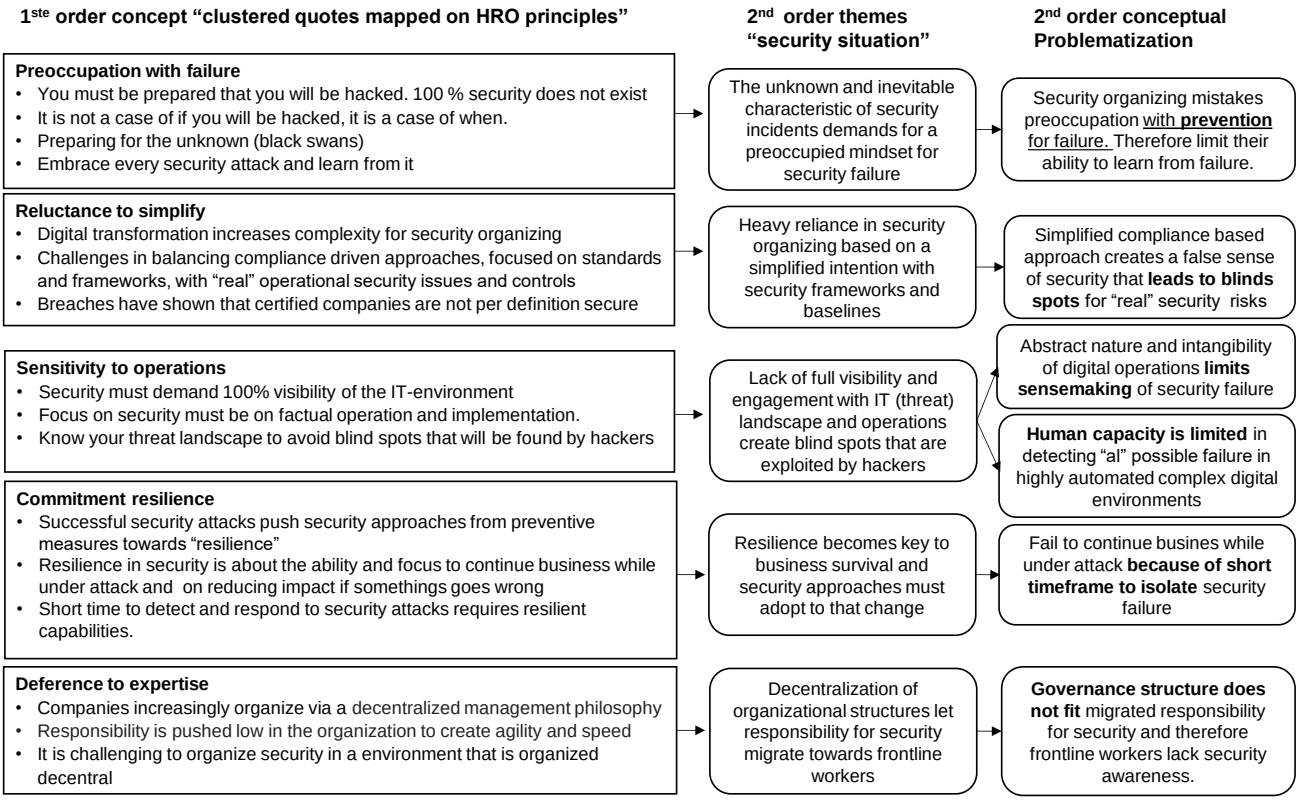

Figure 1. Data structure based on Gioia et al. 2013: HRO principles in DSG.

Mistaking "preoccupation with failure" with "prevention of failure"

As argued above, a preoccupation with failure is relevant in today's DSG approaches. However, in today's security organizational practices, the principle of preoccupation with failure is confused with that of prevention of failure. Organizations predominantly focus on implementing preventive measures with regard to their defense mechanisms. However, contemporary organizations are becoming increasingly connected and therefore are also constantly at risk when operating in a digital context. In such an environment, it is unworkable to hold on to solely preventive measures, which are often referred to as the "Fort Knox" model, e.g., building a protective wall around an organization.

Although the need to shift away from solely preventive measures is clear, our data also show that although there is an understanding of the risk that security issues bring, the way that organizations respond to such a context of continuous failure is not on par with the preoccupation with failure that exists in HROs. Organizations mistake a preoccupied mindset with an excessive focus on preventive measures. An excessive focus on preventing failure in DSG approaches causes

in doing so, increases the likelihood of failure [24]. Today's complex organizations face numerous potential organizations to miss opportunities that HROs take with regard to failure. HROs focus on detecting small, emerging failures because these may be indicative of additional failures [24]. By holding on to a mindset that is focused on prevention, organizations limit their opportunities to learn from security failures.

4.2 Reluctance to simplify

In contemporary firms, the increasing dependency of various systems on information technology (IT) has been fundamental to the management of complex systems and operations [19]. The inherent complexity of digitalization also affects security, e.g., increased threat surfaces, the need for data to be available anytime and anywhere, and the speed and agility necessary to stay ahead of the competition all must be addressed while ensuring security. Understanding how HROs deal with complexity is therefore relevant for DSG approaches.

Reliance on simplified security frameworks and standards

HROs embrace complexity and avoid simplification because simplification obscures unwanted, unanticipated, and unexplainable details and,

sources of failure. However, simplification, particularly in the context of security failure, has taken over. Due to

Theoretical Sample	Sample Activity Code	Theoretical situation
[…] Indeed, you will never be 100% percent secure. The bad guys only have to do it right once to get to us. And we have to keep doing it right in all cases to stop those bad guys. So, we have to get it right a hundred times, and if we fail one time, it's wrong.(40-3.)	Security organizations must anticipate failures and understand that 100% security does not exist.	The unknown and inevitable characteristic of security incidents demands a **preoccupied mindset for security failure**
[…] If it goes wrong--that is not truly a question. When it goes wrong is the question, and what are you going to do when it goes wrong? You have to make clear agreements about this with everyone. (25-3)	It is not a matter of if a company will be breached but when a company will be breached.	
[…] the biggest issue for basically all companies is not so much that the existing security measures are broken… the biggest issue is you have cases that you have not thought of initially. So, you have kind of a breach or you have a validation of a security principle that you have not initially thought of, but you should have considered it initially in your design. So, therefore, this is a kind of unknown domain (1-1)	Preparing for the unknown (black swans).	
[…] there is indeed a turnaround. It [security] used to be very reactive and okay as long as you were sufficiently technically prepared and as long as the castle was strong enough you were doing well. And now you just know that your castle is never strong enough because next week there is something new that you don't know yet. (30-3)		

Table 2: Example data structure based on Gioia (2013): Preoccupation with failure

their desire to implement DSG, organizations rely too heavily on security baselines, standards and frameworks.

Although the benefits of frameworks are clear, e.g., implementing baseline security, HROs shine a light on the limitations of such an approach. As our informants explained, in practice, focusing on security standards and frameworks leads to a simplified compliance-based reality rather than an operational reality.

[…] You can be compliant with a security framework, but that says nothing about security. I always compare it to a motorcyclist. A motorcyclist wearing a helmet is compliant. But if they are wearing shorts and a T-shirt, they are not that secure. And riding a motorcycle in a leather suit with a helmet on is safer than a motorcyclist with shorts, a T-shirt and a helmet. But still, both are compliant. That's the analogy I make for security (33-3)

[…] I am convinced that paper does not protect a company, despite all the certifications that seem to revolve around it. And with every security breach, that becomes poignantly clear, because all large companies that have been hacked--[states examples]--they were all super compliant. (11-2)

Adopting a simplified focus on compliance rather than deeply understanding the underlying causes of operational security issues eventually leads to a false sense of security, as blind spots related to security failures have free play and are not detected.

HROs have learned that the adoption of orderly procedures to reduce errors often propagates them [23]. Thus, they obtain a deep understanding of possible failures in the specific contexts of their operations; therefore, blind spots are avoided. In contrast, the security profession looks for guidance regarding achieving baseline security via occasionally enforced security frameworks and standards. The intention and beliefs of the security profession in terms of the way they maintain and achieve security are grounded in an approach based on simplification that leads to undetected blind spots. In terms of achieving effective DSG, organizations can learn from HROs in the sense that to lower the risk of security failure, an organization should be reluctant to simplify, as this enables organizations to avoid blind spots and gain an improved understanding of complex digital operations.

4.3 Sensitivity to operations

Sensitivity to operations refers to an actor's ability to construct and maintain a detailed picture of operations and the related threats in real time [23]. However, this is a true challenge in the context of automated digital environments, especially because traditional HROs achieve sensitivity to operations through collective human cognition [16]. With regard to DSG, our informants emphasized not only the relevance of but also the challenges related to establishing sensitivity to operations and having full visibility of their digital operations; see also Table 3. The informants emphasized the relevance of being sensitive to operations and having full visibility of the environment, as the risks of not having full control increase security failure and can even be catastrophic. However, in a complex digital setting, it seems that organizations lack control and fail to provide the necessary insights into companies' IT environments. Therefore, blind spots that are vulnerable to security attacks remain.

Theoretical Sample	Sample Activity Code	Theoretical situation
[...] You know that something is wrong, but you don't feel it--you don't see it. So, it remains very abstract… No, you literally cannot see or hear it. And you know, when there is war, there is damage and people are dying. This [security] is so abracadabra. Invisible. (32-3)	Abstract nature and intangibility of digital operations **limits sensemaking** of security failure.	Lack of full visibility and engagement with IT (threat) landscape and operations create blind spots that are exploited by hackers.
[…] They don't feel the pain. … So, it [security] is just still elusive. I mean no one really knows, when you are clicking on your laptop, that in the end, ones and zeros eventually cross that line. Who understands that? I mean we from IT do, but who in the business does? (41-3)		
[…] I have walked around in several companies, and the insight in particular is often not complete. They just don't know where the company's information is. And that is an immediate risk. (7-2)	Security demands 100% visibility of the IT-environment.	
[…]You must have visibility. Yes—that is question one, and I always ask the CISOs, how visible is your IT environment? Well, usually 9 times out of 10 it is not. They have blind spots. (33-3)		
[...] And we think in our field [security], okay—we need people, but we can't do it with people because our attackers don't have people either. So, we are forced to take new measures, for example, to do something with machine learning or artificial intelligence. (41-3)	Human capacity is limited in detecting "a" possible failure in highly automated complex digital environments.	
[…] A hacker does not work with random checks. A hacker checks your entire environment, and you only have to get one port wrong—and you are done. We're talking maybe millions of ports; yes, a hacker only needs to find one. We need to get rid of manual checks and we really need to move to automated things (11-2)		

Table 3: Example data structure based on Gioia (2013): Sensitivity to operations

The abstractness of digital operations decreases sensitivity to operations

We argue that contemporary firms, in contrast to HROs, do not naturally engage with risk in their operations. This seems to be even more problematic in digital operations, which are too abstract for people to clearly recognize a possible (security) failure. Thus, implementing DSG while considering sensitivity within the operations of contemporary firms is challenging. Our data provide insights into further understanding the limitations imposed by a lack of sensitivity toward security failures. The informants noticed that the indirect effect of security risk leads to a lack of security awareness and security-related behavior. People do not understand security risks because the "pain" of security failures is not directly heard, seen or felt. Additionally, security risks are experienced as abstract, intangible, elusive and invisible. Due to this abstractness, security risk experiences are placed outside of the "sphere of influence" of employees. In other words, individuals' ability to be sensitive to security failures is limited in the digital context.

Challenge sensitivity to operations with a focus on mindlessness

Additionally, the great complexity of highly automated environments plays a decisive role in why the security profession struggles to implement sensitivity to operations. Highly complex automated environments cannot fully rely on the capacity of humans to lower the risk of security failures. This is because complex environments transcend human capabilities. Therefore, in the context of security implementation, automated (monitoring) tools are necessary to address the inherent limitations of humans' capacity to implement security and reliability in digital operations.

These results challenge the HRO principle and emphasize the importance of including organizational mindlessness, e.g., technology and automation, to achieve fewer security failures.

4.4 Commitment to resilience

In the theoretical section, we clarified that resilience is not only about bouncing back from errors but also about coping with surprises at the moment. HROs retain both connotations of resilience, which refutes the idea that resilience is simply the capability to absorb change and persist. In other words, first, you need something that stretches without breaking; then, if it stretches, it can recover [24].

Coping with "surprises" has become more dominant in the context of DSG because the attack surfaces of digital organizations are vast and constantly growing. Technology-driven operations with high levels of complexity and interconnectedness have the potential for disruption and disaster. In this way, security attacks and failures have become an inevitable feature of operating in digital contexts, and this reality necessitates resilient approaches.

[…] do you know what the impact of a security incident can be on a business? And surviving that? In the end, it really is all about survival (34-3)

[…]You see that cyber issues are really becoming a part of the impact on your business. Operational continuity is under pressure due to what is now possible, and that was actually not the case [previously]. (36-3)

[…] Look, human lives are of course the top priority, but what if the company ceases to exist because all of our data leaks? Is not that important? (28-3)

As digital businesses move further into a world where everything is interconnected, resiliency is becoming an essential business survival skill. Traditional defensive and reactionary security approaches are no longer adequate. Organizations need to revamp their security approaches by adopting a resilience mindset. To this end, organizations should implement security approaches that would ensure the continuous effective functioning of their core operations should a compromise or security breakdown occur [5]. This will help ensure an organization's ability to maintain its business operations despite the effects of a cyber incident.

Short time to detect security failures

The relevance of a commitment to resilience principles in the context of security implementation is understandable. However, the aim of this paper is to understand why organizations still encounter security failures and to understand how HRO principles can apply to or are limited in their application to the DSG context. In our data, we found that integrating resilience into DSG practices entails the specific challenge of anticipating security failures under substantial time pressures.

[…]. So, with Maersk, it took the ransomware seconds—and the whole operation was down. That's seconds. …. This means that you must be able to detect and isolate that very quickly. (19-2)

[...] [That is] my job, and that's why you have resilience—that's why the detect and response time is getting shorter--because then we can survive. Do you understand? (41-3)

These quotes draw attention to the significance of time in detecting security failures and their impacts on business survival. In line with the limitations of sensitivity to operations principles, a commitment to resilience in the digital era is problematic, as it relies heavily on the collective mind of people to achieve resilience through mindfulness.

4.5 Deference to Expertise

To maintain their performance and survive in the face of changes related to the pace of demand, organizations striving for a high level of reliability shift their decision dynamics, authority structures and functional patterns to create the potential for flexible responses to changing circumstances [15, 24]. Because of high demand in terms of performance, a trend within contemporary organizations is that "self-organizations", decentralized structures, and hierarchies are established permanently [26]. The main argument for this approach is that decisions to enable the speed and agility that are required in the digital era can best be made by people on the frontline (business).

[…] "Security is just another business risk. And just as you are responsible for other risks that affect business operations, this [security] is also a risk" (42-3).

Digital frontline workers lack security awareness

[…] The biggest challenge for security is: in such an environment that works in a decentralized way, how do you do security there? (3-1)

However, according to our data, deference to expertise in the context of DSG is challenging. The key point of deference to expertise is that decisions should be made based on the accurate knowledge of frontline workers. In the context of security, this principle requires that security expertise and the ability to understand security failures should also be present on the frontline, e.g., within business operations and agile teams. However, our informants saw the following issues.

[…] So, what you see is that Agile teams themselves are in such a sprint that they themselves will not bring up security. It's just not in their system. (5-1)

[…] Our business is partly DevOps and partly Agile. I see that this is reflected in the quality of security, which I think is deteriorating. (8-2)

The above quotes illustrate that decentralized organizing strategies, e.g., agile and DevOps approaches, migrate responsibility for security towards the frontline and "self-organizing" teams. However, there is still a lack of awareness with regard to security risks on the frontline.

Culture does not change along with migrated security responsibilities

A possible explanation that arose from our data is that although some companies become more IT-centered over time, the surrounding culture fails to change along with them [15]. This means that the people on the frontline of such companies remain knowledgeable in terms of performing their traditional tasks but struggle to adopt the skills required within digital IT-(security) environments.

[…] IT was introduced, let's say, in the 1980s and it increased. What you see now is that you can almost say that all companies [listing former organizations] are IT companies

….the core business is IT. Only the culture of that company and the people who work there do not have that in their genes. (32-3)

This is challenging for DSG as well. For example, the informants emphasized their experiences of conflicting employee goals involving their traditional tasks and their responsibilities related to security. Such a situation leads to employees who fail to understand the security risk that goes hand in hand with the digitalization of their work.

[…] Traditionally, that is really a culture that still exists here--to be helpful to people and to be transparent. Yes, that is sometimes at odds with negative thinking—that people can commit fraud, perform social engineering or that kind of business. (16-2)

[...]Our concern is, of course, what people do in practice. That is quite difficult sometimes, especially when you are talking about an infrastructure company. Those people want stability. And now comes cyber awareness. And now I say to them: yes, but you know, maybe I would rather be safe than always be stable. That is a mindset change and that is really culture and you do not change that from one day to the next. (9-2)

An entire organization must be security savvy to encounter security failure. However, in HROs, failures are directly related to the core of the "business process", while security in digital organizations is thought to be secondary or nonfunctional. As our quotes above show, in digital organizations, people do not have experiences that show them that they are actually working in very high-risk environments and that their actions can cause major damage.

5. Discussion and conclusion

The aim of this paper was to understand what DSG can learn from HROs to counter ever-increasing cyberattacks and lower the risk of security failures. In particular, we used the lens of HROs to structure our findings and answer our research question. Hence, we analyzed the five core HRO principles and revealed their relevance and applicability in the context of DSG. Based on our data, we first presented the "situation of security" to inform our readers about the status quo and what and how principles are practiced in the DSG context. Next, by discussing a "problematization", we identify three main implications that affect security failure.

5.1 Implications

Understanding the relation between DSG mechanisms and the effect on security failure is central to (IT) security governance studies [6, 17, 18]. To this end, the implications found in this study make an important contribution to DSG research. We visualized the implications in Figure 2. These are as follows:

First, DSG can learn from HROs in the way they treat and learn from (near) failures. HROs are preoccupied with and learn from small, emerging failures to avoid potentially catastrophic impacts. Current DSG implementations rely heavily on prevention and therefore miss the opportunity to learn from failure. Additionally, DSG implementations rely heavily on a simplified compliance-based reality (frameworks, standards, and guidelines) rather than an operational reality. This type of simplification distracts individuals from understanding and learning about real operational risks, creates blind spots and eventually increases the likelihood of failure. Furthermore, the abstract nature of digital operations limits the understandability of security failures. In HROs, failures are related to operations and are embedded in the culture and DNA of the entire workforce. Digital operations, however, are too abstract for people to actually make sense of possible (security) failures [16, 18]

Second, our findings show that in the increasing digital context of contemporary organizations, the abilities necessary to achieve a lower rate of security failure might exceed human capabilities. To date, research fundamentally relies on human factors or cognitive ability to achieve less security failure; in other words, it relies on "mindful organizing" [23, 24]. Our findings provide evidence to question whether this central human-based assumption is effective in today's DSG approaches. Hence, excessively relying on human capacities in digital operations arguably increases the risk of detecting and responding to security failure [16]. The speed, volume and complexity of security attacks demand increasingly "mindless" methods, e.g., automation, tools, and algorithms, to lower the risk of security failure and become resilient.

Third, we found that contemporary organizations face the problem of how to align changing organizational structures and corresponding responsibilities related to security failure. Our data show that security responsibilities do not change along with decentralizing structures. "Frontline" workers in agile/DevOps teams lack a direct understanding of security failure since failure is not directly related to their daily operations, e.g., it is not "visible and tangible". This means that the people on the frontline of an organization remain knowledgeable in terms of performing their tasks but struggle to adopt the skills required within digital IT (security) environments. The lack of security responsibility in the operations does not contribute to lowering the risk of security failures.

The implications above provide further insights into how DSG approaches can achieve more error-free

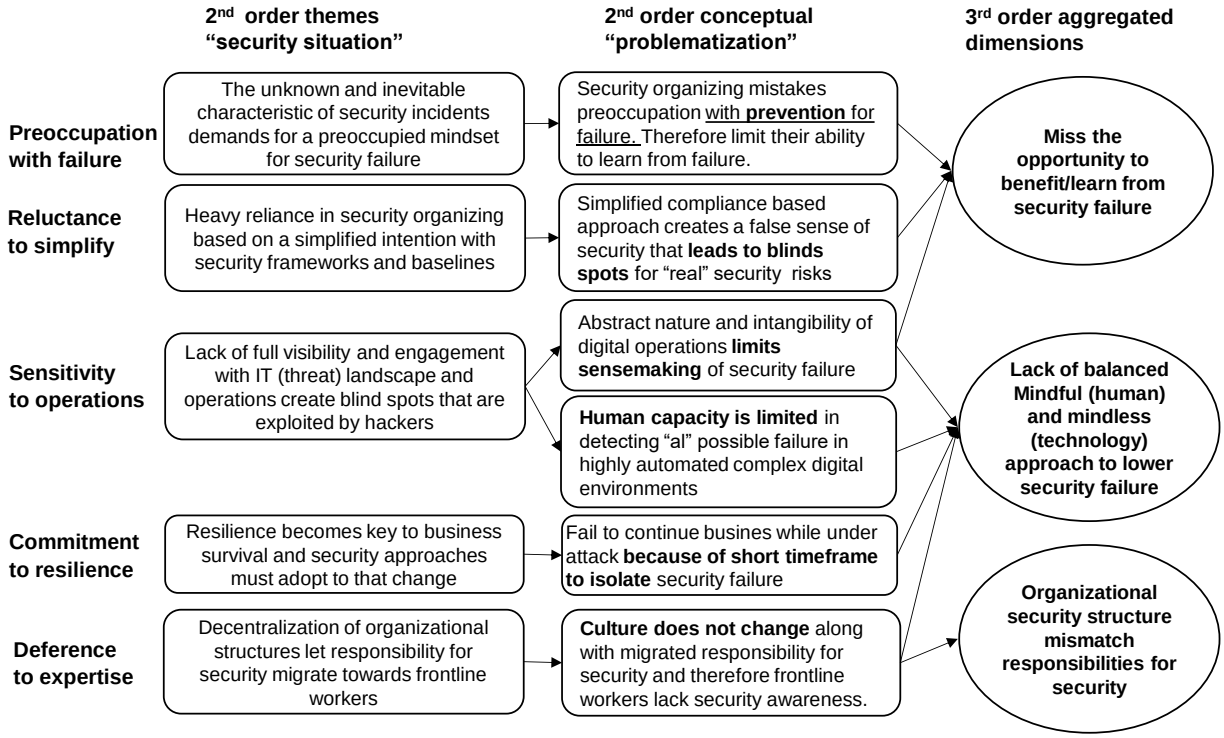

Figure 2: Three aggregated dimensions of HRO principles in security organizing

performances. To date, DSG research remains descriptive and provides both limited practical and theoretical guidance on how to establish effective DSG in organizations [1, 11, 17,]. By providing an HRO perspective, we indicate why current DSG approaches are unsuccessful in decreasing security failures and what DSG approaches can potentially learn from HRO principles to become more effective.

5.2 Limitations and further research

The main limitations of the study lie in the nature of qualitative research and in the interviews of this particular study. The interview data could be criticized in terms of reliability since the first author, who conducted the interviews, may have intentionally or unintentionally influenced the data because of his professional background and experience in the field of information security. To demonstrate to our readers that our findings are plausible and defensible, we applied systematic conceptual and analytical approaches following the Gioia method [7]. This study also faces limitations since the empirical data mainly report findings from the Netherlands. Cultural differences are known to influence governance, and therefore, the level of generalizability regarding the paper's findings outside this geographical area is limited. In addition, the study is designed to collect data across a large variety of organizations and sectors, limiting the empirical richness to some extent. With the current understanding of our findings, e.g., the implications of DSG in relation to HRO principles, researchers can be more specific in their sampling techniques. For example, future studies could focus on organizations where it is more expected to have a DSG approach grounded in HRO principles, e.g., digitally born companies or companies that suffered severe cyber damage.

Our suggestions for further research are twofold. First, the relevance of HRO research for today's digital "mainstream" organizational contexts should be further explored [3, 4, 16]. The established HRO theories have been used on a limited basis to respond to the recent surge in digital operations [16]. Further research can concentrate on the relevance of HRO in the context of digital environments and how to achieve secure digital operations. Second, researchers can continue to answer a long-standing call in DSG research, e.g., to move away from descriptive research and reliance on practical security frameworks to a focus on empirical and theoretical insights [17, 18]. Theoretically and empirically grounding DSG will provide opportunities for deeper understanding and fresh insights into the relation between DSG and security failure reduction.

Security professionals and researchers can use these findings to shift their current DSG approaches and be more effective, e.g., make the most of security failures, challenge the assumption that humans are the weakest link and start institutionalizing security responsibilities across organizations as a whole. Practitioners who play

active roles in establishing "digital strategies" must understand from these findings that DSG is a key concern in the context of adopting sustainable and resilient approaches. Additionally, a broad group of practitioners can learn that today's technology-driven operations show characteristics that are similar to those of HROs. Thus, these practitioners can learn from HRO principles to create resilient organizations and understand that in digital operations, a focus on DSG might be the key to successful business survival in the long run.

Our findings come at a time of intensive media coverage regarding security incidents, breaches and failures, which have become routine daily news rather than the exception. We believe that we have conveyed the need to further study the phenomena of DSG in relation to a security failure, and we encourage other researchers to join us in our research endeavor.

6. References

1. AlGhamdi, S., Win, K. T., & Vlahu-Gjorgievska, E. (2020). Information security governance challenges and critical success factors: Systematic review. Computers & Security, 99, 102030.
2. Burns, A. J. (2019). Security organizing: A framework for organizational information security mindfulness. ACM SIGMIS Database: the DATABASE for Advances in Information Systems, 50(4), 14-27.
3. Cantu, J., Gharehyakheh, A., Fritts, S., & Tolk, J. (2021a). Assessing the HRO: Tools and techniques to determine the high-reliability state of an organization. Safety Science, 134, 105082.
4. Cantu, J., Tolk, J., Fritts, S., & Gharehyakheh, A. (2021b). Interventions and measurements of highly reliable/resilient organization implementations: a literature review. Applied Ergonomics, 90, 103241.
5. Conklin, W. A., & Shoemaker, D. (2017). Cyber-resilience: Seven steps for institutional survival. EDPACS, 55(2), 14-22.
6. Dhillon, G., Smith, K., & Dissanayaka, I. (2021). Information systems security research agenda: Exploring the gap between research and practice. The Journal of Strategic Information Systems, 30(4), 101693.
7. Gioia, D. A., Corley, K. G., & Hamilton, A. L. (2013). Seeking Qualitative Rigor in Inductive Research: Notes on the Gioia Methodology. Organizational Research Methods, 16(1), 15–31.
8. Heierhoff, S., Hoffmann, N. (2022). Cyber Security vs. Digital Innovation: A Trade-off for Logistics Companies?. In Proceedings of the 55th Hawaii International Conference on System Sciences.
9. Jalali, M. S., Siegel, M., & Madnick, S. (2019). Decision-making and biases in cybersecurity capability development: Evidence from a simulation game experiment. The Journal of Strategic Information Systems, 28(1), 66-82.
10. Li, L., Shen, Y., & Han, M. (2021, January). Perceptions of Information Systems Security Compliance: An Empirical Study in Higher Education Setting. In Proceedings of the 54th Hawaii International Conference on System Sciences (p. 6226).
11. Lidster, W. W., & Rahman, S. S. (2018, August). Obstacles to Implementation of Information Security Governance. In 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE) (pp. 1826-1831).
12. Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). (2020). Cybersecuritybeeld Nederland (CSBN). Postbus 20301, 2500 EH Den Haag.
13. Nicho, M. (2018). A process model for implementing information systems security governance. Information & Computer Security, Vol. 26, Issue 1, pp. 10-38.
14. Plachkinova, M., Steiner, S., Leon, D.C., Shepherd., M. (2021). Introduction to the Minitrack on Organizational Cybersecurity: Advanced Cyber Defense, Cyber Analytics, and Security. In Proceedings of the 54th Hawaii International Conference on System Sciences
15. Roberts, K. H. (1989). New challenges in organizational research: high reliability organizations. Industrial crisis quarterly, 3(2), 111-125.
16. Salovaara, A., Lyytinen, K., & Penttinen, E. (2019). High reliability in digital organizing: Mind-lessness, the frame problem, and digital operations. MIS Quarterly.
17. Schinagl, S. and Shahim, A. (2020), "What do we know about information security governance? "From the basement to the boardroom": towards digital security governance", Information and Computer Security, Vol. 28 No. 2, pp. 261-292.
18. Schinagl, S., Khapova, S. N., Shahim, S., (2021). Tensions that hinder the implementation of digital security governance. In proceedings of 36th IFIP TC-11 International Information Security and Privacy Conference (SEC 2021), June 22-24
19. Sepúlveda-Estay, D. A., Sahay, R., Barfod, M. B., & Jensen, C. D. (2020). A systematic review of cyber-resilience assessment frameworks. Computers & Security, 101996.
20. Spremić, M., & Šimunic, A. (2018). Cyber security challenges in digital economy. In Proceedings of the World Congress on Engineering (Vol. 1, pp. 341-346).
21. Von Solms, R., & von Solms, S. B. (2006). Information Security Governance: a model based on the direct–control cycle. Computers & Security, 25(6), 408-412.
22. Wang, Y., Muthusamy Ragothaman, K. N., & Shakya, B. (2021, January). Towards Trusted Data Processing for Information and Intelligence Systems. In Proceedings of the 54th Hawaii International Conference on System Sciences (p. 6242).
23. Weick, K. E., & Sutcliffe, K. M. (2015). Managing the unexpected: Sustained performance in a complex world. John Wiley & Sons.
24. Weick, K. E., Sutcliffe, K. M., and Obstfeld, D. 1999. "Organizing for High Reliability: Processes of Collective Mindfulness," in Research in Organizational Behavior (Volume 1), R. S. Sutton and B. M. Staw (eds.), Stanford, CT: JAI Press, pp. 81-123;
25. Wong, C. K., Maynard, S. B., Ahmad, A., & Naseer, H. (2020). Information Security Governance: A Process Model and Pilot Case Study. Forty-First International Conference on Information Systems, India
26. Zhang, J. J., Lichtenstein, Y., & Gander, J. (2015). Designing Scalable Digital Business Models", Business Models and Modelling (Advances in Strategic Management, Vol. 33), Emerald Group Publishing Limited, pp. 241-277.