Conceptualizing the Role of IS Security Compliance in Projects of Digital Transformation: Tensions and Shifts Between Prevention and Response Modes

Hassan Raza
University of Warwick, phd16hr@mail.wbs.ac.uk

Joao Baptista
University of Warwick, j.baptista@wbs.ac.uk

Panos Constantinides
University of Warwick, panos.constantinides@wbs.ac.uk

Conceptualizing the Role of IS Security Compliance in Projects of Digital Transformation: Tensions and Shifts Between Prevention and Response Modes

Completed Research Paper

Hassan Raza
Warwick Business School
The University of Warwick
Phd16hr@mail.wbs.ac.uk

Joao Baptista
Warwick Business School
The University of Warwick
J.Baptista@wbs.ac.uk

Panos Constantinides
Alliance Manchester Business School
The University of Manchester
Panos.Constantinides@manchester.ac.uk

Abstract

Research shows that information systems security operates between two main distinct functioning modes, either prevention before a security incident occurs, or response which follows from an incident, usually external to the organisation. In this paper, we argue that this shift between prevention and response modes also happens due to inherent internal tensions created between pressures for digital transformation and the established forces for security compliance. We show how a digital transformation project introduced a security incident and challenged the IS security compliance function, a process that reflected these two approaches to IS security in organizations. We conduct a participatory observation study of the implementation of Robotic Process Automation (RPA) in a financial services organization. We examine the shift from prevention to response in this project and identify generative drivers of digital transformation, and drivers of IS security compliance. Our analysis leads to the development of a process model that explains how organizations move from prevention to response when faced with tensions between IS security compliance and digital transformation.

Keywords: IS Security Compliance, Digital Transformation, Digital Innovation

Introduction

The threat environment to organizations is increasingly dynamic and complex as evident from the Aurora and Stuxnet cyberattacks in 2010 (Carr 2010) and affects a growing number of businesses as suggested by various cyber security breaches surveys (Finnerty et al 2018). This dynamic threat environment has been managed by organization through two main modes of security functioning: prevention and response (Baskerville et al, 2014). The *prevention mode* operates before a security incident occurs and relies on exploitation strategies (March 1991), which capitalize on what organizations have learned to do well in the past. In contrast, the *response mode* operates after a security incident has occurred and relies on exploration strategies (March 1991), which capitalize on the ability of organizations to search for new tactics and approaches for unknown and emergent risks. IS security research has studied and conceptualised the way organizations balance their efforts across these two modes (Baskerville et al 2014). Although this shift between prevention and response is well reported in the literature, our understanding of what triggers this shift has been primarily focused on external security incidents. Much less attention has been placed on internal incidents, especially events that are not considered or perceived to be malicious threats to the organization.

We suggest that one type of these internal non-malicious threats are projects that push the organization towards digital transformation (Kumar and Stylianou, 2014). These projects are often a response to changes in the business and market environment to keep the organization competitive, however they often challenge

established practices and procedures, leading to failure to pass established security compliance frameworks in the organization (Cram et al, 2017). It is therefore worth explore and study the tensions that emerge between these two forces and the role of IS security compliance (Njenga, 2016) in managing emergent risks in digital transformation projects. This is the focus of our research.

To respond to this objective and address this gap in the literature, we formulated the following research question: *what is the role of IS Security compliance in processes of digital transformation?* We answer this question by identifying the underlying phases that are associated with the compliance process and the process organizations go through to modify existing or new security practices as they engage in digital transformation. We conduct an inductive study of Robotic Process Automation (RPA) in a large financial services company (Autofin). Our study explores the journey of an organization as it adopts a new digital technology that uses AI and software robots to replace human activity and automate business processes. Our focus was to examine the emerging tensions when this technology challenges established IS security compliance procedures and frameworks, and to capture the role of the security compliance function while managing the project and inherent tensions between the two forces.

The next section reviews the literature on digital transformation and information systems security compliance. We then describe the inductive case study methods approach used in the study. Following this, we describe our findings and then analyze them to present three compliance phases. We finally end by showing the key contributions and implication for further research in this space.

Literature Review

IS security compliance is a key part of security as it contributes to the enforcing of information security policies, processes and procedures in the organization (Bulgurcu et al, 2010). This represents the formal and mandatory process needed for organizations to demonstrate internal compliance to agreed levels of risk generated by security incidents (Cram et al, 2017; Lee et al, 2016). A common definition of a security incident is *"a change of state in a bounded information system from the desired state to an undesired state, where the state change is caused by the application of a stimulus external to the system"* (Stephenson 2004 p. 18, emphasis added). To this definition, we add, *'a change of state as caused by the application of a stimulus internal to the system'*, and by this we mean internal changes that challenge established ways of working and compliance frameworks. This broadens the scope to include the activities related to risk compliance of internal projects too, which are the focus of this research project.

Below we discuss how the literature on IS security compliance has approached external security incidents by enacting strategies that enable the organization to shift from a prevention to a response mode. We then discuss how we can extend this research by considering digital transformation projects as internal security incidents.

IS Security Compliance: Shifting from Prevention to Response Modes

IS Security research is most often approached from a prevention *perspective*. This mode of security is designed around predictable and measurable risks and threats, and is based on the development of predefined security practices to mitigate these risks (Baskerville et al, 2014). However, when organizations are faced with unpredictable threats, a distinct mode of operation is required. A different mode that enables organizations to respond to risks that are non-measurable and transient and therefore allow for more dynamic relationship between the risk and safeguards characterizes a *response* mode (Baskerville et al., 2014). In each mode, organizations need to employ different learning strategies to identifying the risks involved and the possible mitigation approaches by adjusting IS security practices, protocols and structures.

The literature suggests that in the case of operating in a prevention mode, organizations use exploitation strategies to capitalize on past successful practices of IS security compliance. Instead, in a response mode, organizations use exploration strategies to search for new practices and deal with unpredictable and transient risks (cf. March 1991). Further, while the prevention mode places emphasis on persistent controls based on existing IS security compliance practices, the response mode places emphasis on emergent controls to manage risks (Anderson et al 2017; Cram & Brohman, 2016; Siponen & Iivari, 2006; Knapp et al 2009; Cram et al, 2017). We know from recent research that the shift from one mode of security to the other, involves a set of translation mechanisms (Niemimaa & Niemimaa 2017). These include translation from global (i.e. best practices found in the market) to local (i.e. organizational) practices, and the

disruption and reconstruction of local non-canonical practices. In essence, the shift from a prevention to a response mode allows for more dynamic and adaptive responses necessary in uncertain environments (Njenga & Brown, 2012).

In the next section we suggest that the shift from prevention to response, may also be actioned due to internal changes related to processes of organizational transformation, and not only as a response to external security threats as portrayed in extant IS security literature.

Digital Transformation as an Internal Security Incident

Digital transformation is a driver of change in many organizations today (Kumar and Stylianou 2014) and is associated with emergent organizational change (Farjoun, 2010) because it *"changes (…) a company's business model, which result in changed products or organizational structures or in the automation of processes"* (Hess et al 2016, p. 124). These changes are inherently *generative* because of the modular (Yoo, et al 2010) and ambivalent nature of modern digital technologies (Kallinikos et al 2013).

The salient point of generativity in digital transformation is that it creates unpredictable, non-measurable and transient risks (Ransbotham & Fichman, 2016). This therefore means that relying on established rigid patterns and frameworks to assess risk leads to unreliable results. This also means that prevention type of security approaches are inadequate to manage these emergent risks. To better manage the shift between prevention and response, organizations require IS security compliance approaches to match the generative dynamics of digital transformation projects.

We draw on the three phases of digital innovation suggested by Henfridsson & Bygstad (2013) *innovation, adoption and scaling* (Henfridsson & Bygstad, 2013) to help characterize the emergent nature of generativity in the RPA project and juxtaposed these to inductive themes that we found explained the contrarian forces of compliance: *ordering, stabilizing and sustaining*. We explain these attributes and emergent constructs in the findings section.

In the next section we discuss the methods used to operationalize these ideas in a participatory observation study of the implementation of Robotic Process Automation (RPA) in a financial services organization.

Research Methods

We began with a deductive approach and identified key concepts from the literature to start building our theoretical understanding and develop a focus for our case study research (Eisenhardt & Graebner, 2007). We adopted a qualitative research approach to support the theorizing of our findings (Garud et al, 2017) and adopted a diverse criteria to develop a better theoretical perspective (Weick 1989, p.523).

We conducted a longitudinal field study of the implementation of Robotic Process Automation (RPA) in a financial services organization (Autofin). RPA technology represents a new breed of AI using digital automation technologies to replace human activity and transform organizational processes. The robots introduce business efficiencies previously not possible with existing business process automation (Lacity & Wilcocks, 2016). The data collection was done in two phases. In the first phase, the primary source of the data was participant observation (Kemmis & McTaggart, 2005) and project related documents. We used interviews in the second phase to improve our understanding based on the data analysis that was done after the first phase. This approach allowed us to take advantage of the richness in the field data and question our initial assumptions and theories (Walsham, 1995). We used the principles of interpretive field research (Klein and Myers, 1999) to ensure the reliability of our data.

One of the main challenges with information security research in financial services organizations is gaining rich access to vulnerable areas of the organization due to the sensitivity of the information and strict requirements of confidentiality. It is therefore usually difficult for external researchers to access the empirical setting. In this instance one of the researchers is also a member of the organization's information security team so had privileged direct access to the empirical material. The researchers were able to negotiate access with the senior management team of the information security department to gain privileged access and conduct the empirical work necessary for this research project.

Case Description

The empirical setting is Autofin, a financial services organization that provides financing for a large European car manufacturer. Autofin has been operating as a business in the UK for over 50 years and has been through several management changes with the most recent one being in 2017, when they were bought by a consortium of European companies. This required Autofin's management team to create a new IT organization that would service the needs of the business. The challenge was to continue to provide services without affecting the current business operations. This activity started in 2017, with the management team announcing the creation of a strategic 100 days plan that would allow the organization to identify all the main areas of focus for the next few years. Autofin's new management team identified a new set of organizational values to help the organization transition to a new way of working and digital transformation of the organization was part of this overall strategic agenda.

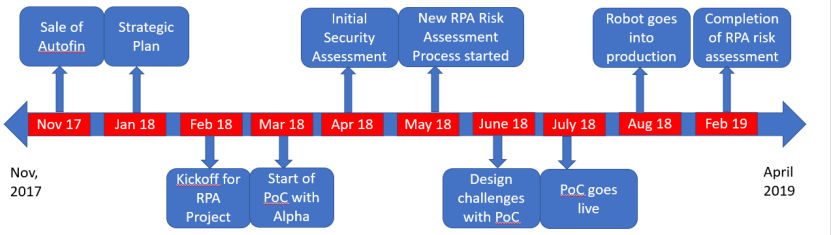
In Feb 2018, the management team of Autofin shared the outcome of the strategic plan and identified the various initiatives that were intended to bring in business efficiency, reduce the IT operational costs and increase profitability for the organization. One of key projects identified as part of this ambitions organizational transformation was the Robotic Process Automation (RPA). The goal of this project was to automate a significant number of business processes to improve efficiency and replace human activity and therefore reduce costs to the organization.

This was a novel project for the organization as it was led by the business side of the company, instead of the traditional approach led by the IT team. Although the budget was approved by the IT executive committee, the digital transformation and delivery of the project was managed by the business team. The project manager played two roles: delivering to timelines set by the business team and acting as a liaison to the wider IT team to ensure the deliverables were met.

The RPA project kicked off in February 2018. We began our research by reviewing the project timelines and identifying critical project related events as shown in figure 1. We were struck by the number of tensions between business and the information security team during the project. Some of the key events included setting up the proof of concept with vendor Alpha and challenges with the information security risk assessment which were first identified in April 2018. This led to the information security team working on a new bespoke and customized risk assessment process for the RPA project which started in May 2018 and ended in February 2019.

The project team faced several challenges with the proof of concept design due to technical and security issues, but these were resolved and the PoC went live in July 2018. Since this was a vendor supported project, Autofin changed vendors from Alpha to Gamma and from August 2018 onwards, the robots were being deployed in the production environment.

Figure 1: Project timeline and critical events



Data Collection

We adopted an iterative two stage data collection strategy. The first stage was from February 2018 to Feb 2019 and it accounted for the bulk of the data collection. We used participant observation (Kemmis & McTaggart, 2005), emails and documents generated during the initial 12 months of the project. As part of the IT governance process, the organization used a checkpoint system and project documents were generated at each stage. For example during checkpoint 1, the documents generated were the business case, technical and information security requirements. In checkpoint 2, the design documents were generated as well as some of the key technical and implementation documents. In checkpoint 3, the testing documents

were generated to show compliance with technical and security requirements. In addition to the governance documents, there were also documents from steering committee meetings, executive communications to the rest of the organization and email exchanges over the course of the project. The list of documents is shown in Table 1 below.

Table 1: Summary of Data Sources

Data Type	Quantity
Semi-structured interviews	5
General project documents	4
Design documents	5
Project governance documents	4
Security documents	3
Recorded meetings	21
Steering committee meetings	6
Emails	92
Executive communications	2
Total number of data sources	142

After conducting the initial data analysis, the next stage was to conduct semi-structured interviews (Myers and Newman, 2007) with key stakeholders from the IT, business and information security teams to investigate the themes that we had identified in our first round of data analysis. This took place between July and August 2018. The interviews provided us further revelatory information about the phenomena we were investigating and allowed us to unpack and explore in greater depth the tensions seen earlier on.

Data Analysis

We relied on qualitative research approaches (Miles and Huberman, 1984) to inductively analyze our data (Garud et al, 2017). We used NVivo to analyze the data at regular intervals during the data collection phase and theoretical sampling helped us identify emerging patterns in the data. Given the privilege to be inside the organization following the project, we kept collecting data until saturation point in our theoretical analysis. Our analysis composed of sequence of phases: collating the case history and identifying key events. We then went through the first round of the coding process to extract key themes, which were further explored in the semi-structured interviews. After the interviews were conducted, we went through a second round of data analysis.

In the first round of the data analysis, we used an inductive approach to code the data (Gioia et al, 2013). We began with the open coding process and using these codes developed first order concepts. In the next stage we inductively developed second order themes and then aggregate dimensions. The data collection and coding process continued until no new significant actions or events were generated. This process of data analysis allowed us to identify critical events which helped guide our data analysis process.

In tables 2 and 3 we show the open codes generated during our analysis and after cycling through the data. In table 2 we show for example codes that link digital transformation with flexible arrangements in the organization. This is also linked to three phases associated with digital transformation namely: innovation, adoption and scaling, which reflected prevention mode of managing risk in the organization. In table 3, we show how the information security compliance process is linked to more rigid organizational arrangements. This is linked to compliance phases: ordering, stabilizing and sustaining, which reflects response modes of managing risk. The two tables illustrate the coding structure that we created using NVivo, and it includes some sample quotes that represent the initial codes. The table explains the process of theorizing from the data to the higher level concepts, which also reflect our review of the themes from the literature. This was therefore both an inductive and deductive approach to systematizing our understanding of the situation. The two tables together illustrate our efforts to abstract theory from the data through the coding process. They are however summaries of much more detailed structures that we have in our NVivo files.

Table 2: Coding structure that shows the push towards the response mode

Representative Quotes	Initial Open Code	First Order Categories	Second Order Themes
"We have started the route to digital transformation with Robots and Chatbots"	RPA as a source of Innovation	*Innovation Phase*	*Response* mode of managing risk in the organization
"Digital transformation is the key to empower our business for the future"	Focus on digital transformation		
"We can identify the best practices and include it in the runbook"	Moving from PoC to Production	*Adoption phase*	
"We will use UiPath RPA Software with support from Apha and Autofin resources"	Moving from PoC to Production		
"We want the ability to develop a large number of robots in parallel"	Increasing the number of RPA processes	*Scaling phase*	
"We need an RPA standard document that lists all the specific requirements for robots"	Increasing the number of RPA processes		

Table 3: Coding structure that shows the push towards the prevention mode

Representative Quotes	Initial Open Code	First Order Categories	Second Order Themes
"Unauthorized access due to insecure storage of credentials"	Identifying IS Security Gaps with RPA	*Ordering phase*	*Prevention* mode of managing risk in the organization
"We have been through the Autofin security review for VDI and Terminal services option"	Identifying IS Security Gaps with RPA		
"With red team reviews, one person from Gamma is writing code and the other is checking it"	Resolving IS Security gaps with RPA	*Stabilizing phase*	
"There are multiple forms of authentication happening, one for robots and one for system access"	Resolving IS Security gaps with RPA		
"Once we get the RPA vulnerability scan results, we can provide the approvals"	Integrating IS Security changes related to RPA	*Sustaining phase*	
"We need a security lessons learnt process"	Integrating IS Security changes related to RPA		

Findings

We now show empirical data describing shifts between the two modes of managing risk in Autofin. We show the changes to the information security compliance process that signals the shift from the prevention mode to the response mode. Our data shows the existence of different phases in the project that are characterised by distinct dynamics between the forces for digital transformation and forces inherent in information security compliance processes.

As explained in the literature review section we draw on the three phases described by Henfridsson & Bygstad (2013) *innovation, adoption and scaling* to capture the transformation forces and show the emergent generativity of the RPA project, we then juxtaposed these codes to inductive themes representing forces for compliance: *ordering, stabilizing and sustaining*.

Shift from prevention to response

One of the main themes that emerged from our data analysis were struggles between the demands of the project for transformation and demands from established approaches to security compliance. Our data shows that from April 2018, the IS security compliance team emphasized the need to enforce security standards suggesting the need for tighter and perhaps more rigid approaches to the transformation underpinning the RPA project. The quotes below from the Head of Information Security Architecture (HISA) and from the Head of Information Security Governance (HISG) show the frustrations with the rigid nature of the compliance process:

> HISA: "*We also have to remember that we have our own policies and standards you have to be compliant with. Ultimately we need to find the right balance*"
>
> HISG: *"We are focused on compliance checklist oriented security requirements and having that defined across the board".*

In response to this, the project team explored new options and went through a process of learning and development to find ways through, and around, the difficulties with passing the compliance requirements. The quotes below highlight the lack of security knowledge in dealing with the automated robots, and the need to reinvent the role of the compliance team. The second quote follows from this and highlights the need to create a new standard document for RPA:

> HISG: "*As a security person, we have to be willing to be uncomfortable. That does not mean that we don't have a role to play and we don't have an important role*"
>
> HISG: "*For this type of project where we are bringing in a new technology platform, we don't have good references for how to deal with robots in environments*"

What the above represents is a shift in the approach to manage emergent risks and uncertainty in the organization, which also reflect a shift of modes in managing risk from prevention to a response mode. We now describe three phases that represent this process.

Innovation - Ordering phase

In the innovation-ordering phase, the organization introduces the digital technology to drive efficiencies and reduce the staff by replacing human tasks with software robots. The first quote below from the Deputy CIO (DCIO) highlights the importance of the project for the business. While the second quote from the Lead Solutions Architect (LSA) shows the perception from the business that this project should not raise security concerns as they essentially "replace humans with automated robots":

> DCIO: "*It is crucially important that the business can get past the summer peak period in the UK in September, without hiring any additional temps*"
>
> LSA: "*I don't think the robot is a security issue, they are a user issue. In my view, what is different is the scripts that are produced, and the robots execute them*".

However, as the project developed this view from the business became increasingly challenged by the security team, as expressed by the Security Architect (SA) below:

> SA: "*When a human being is carrying out the action, they can identify flaws or potential issues and stop the process. I want to understand how the robot will deal with error conditions and reduce the security risk".*

This innovation-ordering phase is also characterised by checks by the information security team to assess how the project meets the security compliance requirements. The first comment below, by the SA questions the approach that should be taken to conduct the risk assessment, while in the second quote, the HISG identifies that there are no security standards that can be used to evaluate the security requirements.

> SA: "*One of the challenges we have is how do we assess this project. Do we assess it from the perspective of a human or robot*?"
>
> HISG: "*We need an RPA standard document that has all the specific requirements around robots in it*".

This debate indicates an underlying tension from not having an appropriate way to assess the RPA project, which is captured in the quote from HISG below:

> *HISG:" If you have got 10 controls on your list and you say they are all important, you really have to question if you are understanding the risk at the right level and categorizing the risk correctly"*

Eventually the security team agreed that a new security control framework was needed and accepted that a new security risk assessment framework was also necessary as expressed in the following quote from the HISG:

> HISG: "T*here are some clear actions. The first one is for security to go back and work on the controls based on the RPA risks we have identified. The second part would be to develop an assessment framework around the controls*".

Adoption - Stabilizing phases

In the adoption-stabilizing phase the RPA project is more advanced and the technology more embedded in the organization. It was initially used to automate mundane and resource intensive processes during the new car registration period as part of the PoC phase. Autofin partnered with an external vendor for the technology called "Gamma". Gamma was meant to manage the development and testing of the robots. The first quote from the business lead explains the reasoning for this approach due to the lack of technical capability within Autofin to support digital transformation projects such as the RPA project:

> BL: "*The PDD is the business documentation and SDD is when we start to get into the technical development lifecycle. This will be created by Gamma*."

The involvement of an external company which was led by the business team and not the IT team was unprecedented in the company. The security policies and standards needed to extend to the design and functioning of the robots developed by Gamma. This sparked tensions between the engineering team and Gamma while trying to implement a solution within the constraints of the information security policy. As the quotes below show Gamma identified information security challenges during the adoption phase:

> Gamma: "*Mostly the concerns are about the data security , the access of the users, and if we need to add new processes, how to manage passwords*"

At the same time the LSA identified information security violations, for example in using shared user accounts for robots, as mentioned in the quote:

> LSA: "*When the robots are running multiple processes simultaneously, we run into the security problem of using shared logons, which is against our security policy. The problem is around software management and violating existing IT and security policies*".

Eventually more stable arrangements were reached, following from ongoing conversation between HISA and HISG in response to the tensions associated with identification of new controls and development of a custom risk assessment for the RPA project. The first quote below is from HISA regarding the challenges associated with the existing security control framework and the need to develop a new risk assessment. The second quote from HISG shows the tensions associated with conducting the risk assessment.

> *HISA: "In this case we have two challenges. The first is reviewing the catalogue of controls and identifying which ones we need to apply for the RPA processes. The second challenge is to develop the [security assessment] questions based on those controls. Do you agree?"*
>
> *HISG: "That makes perfect sense. The third thing would be going through the RPA risks that we identified and adding any additional controls that we identified. That's going to be tricky because I am not sure we have the controls yet. All we have are the questions".*

This approach required a new detailed risk analysis framework for the project. The first quote below shows the options that were considered and the second quote covers the final assessment that was created:

> *HISG: "We use the application security questionnaire and modify it. We will add three columns and one for each of the used cases that HISA mentioned and then go through them in a bulk way".*

> *HISA: "We created assessment questions using business friendly language…. We identified some focus areas for this form such as data classification, access control, logging and event management".*

Scaling – Sustaining Phases

The scaling-sustaining phase of the RPA is characterised by Autofin working in the production of more robots, and increased identification of business processes to be automated. For example, the business team managed a lot of passwords and as per the security policy these passwords need to be manually changed every 30 days. This caused a lot of tension with the information security compliance team as the workload had increased significantly to change all the passwords manually and the business team was short on resources. The first quote from the Business Lead (BL) explains the need to expand the RPA project and the challenges with the new access management process:

> *BL: "Every RPA process will have 18 user IDs on average and today we have approximately 120 user IDs that we are maintaining. The challenge we are facing that this will continue to rise exponentially as we continue to bring on board more processes for RPA. The management of these userIDs and passwords is a huge overhead to the RPA team but also it is creating huge business risk".*

The second quote from BL identifies a new approach that they want to consider to simplify the number of userIDs and passwords:

> BL: "*The proposal the RPA team are putting forward is the simplification of the userIDs and limit one userID per robot and one set of user IDs per application*".

We find the tension between scaling and sustaining in the comment from the HISA as he raises a concern with over-simplification and potential risks of this:

> *HISA: "I think we need to avoid a "knee jerk" reaction and avoid over simplification. We always knew that the current system of managing passwords using spreadsheets was not going to be workable when we started scaling and increasing the number of processes".*

During an internal security meeting to discuss the proposal from the business, we find more evidence of the tensions in the discussions between HISA and HISG:

> *HISA: "My main concerns are around the auditability and traceability. If there is a process failure, can they tell us exactly where the problem occurred and provide a step by step forensic analysis of the process".*
>
> *HISG: "It is just that they don't want to create individual applications ids for each robot process and from their perspective, they felt that traceability and the normal approved behaviour will be shown through logging on the client side"*

Through negotiation between the business team and security teams, it was then agreed for the business proposal to be accepted with a condition that a risk exception is raised as per the quote from HISG. The security risk exception is one of the sub processes associated with the main compliance process and is invoked under special circumstances:

> HISG: "We'd like to raise this as a security exception since it may require changing the application security configuration. To do this we need to document the issue in attached risk exception form".

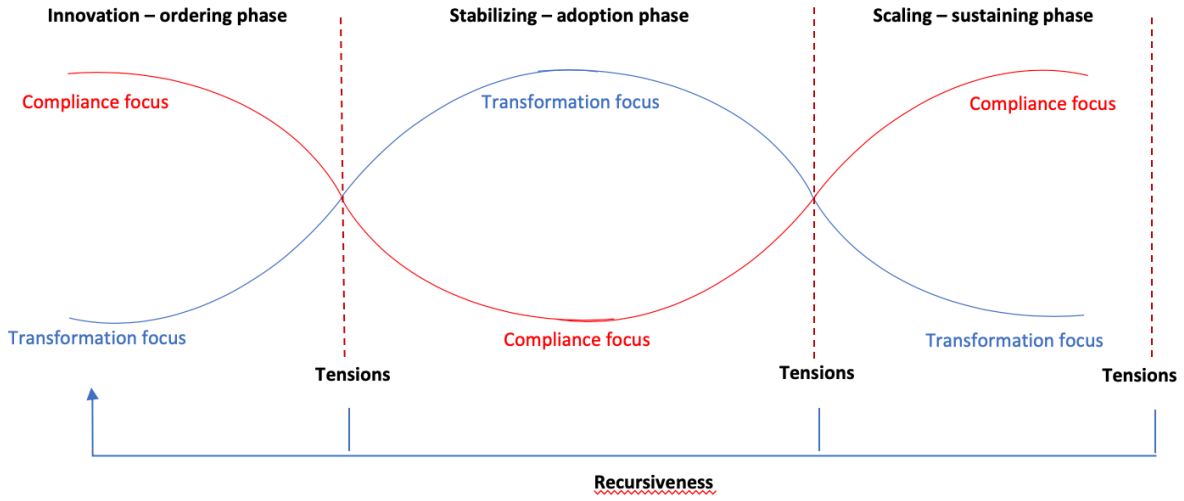
Overall, as seen above one of the prevailing themes emerging from our analysis is the growing realisation that robots require a different risk management approach from humans, as indicated by the following quote from the HISG:

> *HISG: "We have these rigid controls that are not designed for the principle of robots. The real challenge is to think through what is the right way to manage those risks when we are dealing with robots and not people".*

Discussion

In this section we more directly answer the research question "*what is the role of IS Security compliance in processes of digital transformation?*". To answer this question we developed a process model that juxtaposes the compliance process with the digital transformation process undeprining the RPA project. Our theoretical model is summarized in figure 2 and is organized around two aggregate theoretical dimentions that emerged both deductively from literature and inductively from our data.

Figure 2: Theoretical Process model



At the core of the model are the distinct phases that mark the emphasis on either transformation or compliance, it also represents the inflection points that are triggered from tensions when these two dominating forces clash. Our data showed that the activities associated with digital transformation created inherent tensions that challenged established frameworks and models of information security compliance. We chose to investigate the relationship between the constitutive elements of both processes and found a close relationship between innovation-ordering, adoption-stabilizing and scaling-sustaining. The data also showed us that the digital transformation and information security processes are recursive and the shift between the phases can be forwards or backwards as they dependent on how the tensions are managed.

From the literature, we already know that external security incidents pushes organizations from prevention to response mode (Baskerville et al, 2014), and we made the case that digital transformation can act as an internal incident to also push organizations towards the response mode.

Our data shows that a shift between the modes occurs as a result of tensions that emerged from the project. The data also suggests that generative nature of the digital technologies meant that the risks were unknown and emergent so difficult to manage from a prevention perspective. This stimulated a shift towards response to allow for more flexibility in the applicability of the established security frameworks. For example, we found that the methodology associated with management of robot IDs and passwords was based on the view that robots are like humans. However, the generativity of the technology created unexpected outcomes which were only identified after the process was realized in practice. The management of the resulting tensions resulted in the process being pushed backwards from the scaling phase to the innovation phase where robots were designed with a simpler set of robotIDs.

We now take a closer look at the interactions between the different phases associated with the digital transformation process and information security compliance and unpack the tensions that lead to the mode shift. In the case of innovation and ordering, we find that innovation is certainly pushing the organization towards response mode and there is a pull from the security compliance perspective. We see the first

glimpse of the tension when the business team suggest that the robot is not a security issue and more of an access issue and this view was challenged by the security team. We then see a recurrence of the tension when the security team is trying to use the existing risk assessment approach and it is not applicable. The management of the tension results in an initial push towards the response mode where it triggers the need for a new set of security controls and risk assessment process. The expectation is that there will be a shift back to the prevention mode when the organizations starts to use the custom RPA risk assessment process on a regular basis.

In the interaction between the adoption and stabilizing phase, we identify two activities that lead to tensions with information security compliance. The stabilizing phase affects the adoption phase as the project team needs to ensure that the IS security compliance requirements are met, and this has an impact on the configuration and implementation of RPA. The first has to do with the engineering requirements for the final RPA solution and the use of shared logons that violate the information security policy. In this case, we see the push towards the prevention mode and the engineering team have to build the final architecture around this requirement. The second activity is associated with the identification of new security controls and creation of the new risk assessment. We see a push towards the response mode and how the security team manage the tensions to create the new risk assessment form using global control standards to create local standards (Niemimaa & Niemimaa, 2017). The outcome of how the tension is managed leads to the modal shift towards prevention or response.

In the sustainability phase we see the translation of disrupting and reconstructing local practices (Niemimaa & Niemimaa, 2017). The result is formalizing security controls identified during the creation of a new RPA security policy or standard, which did not exist previously. In the data, we see a clash with the scaling phase. The business team realized that the use of multiple userids for each robot and process being automated led to a userid and password management issue during the scaling phase of the digital transformation process. We see a shift to the prevention mode as the business team had to comply with the rigid security standard of not using shared logons and password resets every 30 days. However, the business team challenged this view and provided a proposal to simply the process. This led to tensions with the security team and initially they challenged this view but then accepted the change under specific conditions. This is an example of a shift from prevention to response and back to prevention.

We found an emergent theme in our data where the organization makes the transition from prevention to response and then reverts back to prevention. The transition from prevention to response is driven by uncertainty and using an incident-centric approach taken by Baskerville et al (2014), we find some common traits. The security team is challenged with a set of unpredictable and unmeasurable threats that cannot be mitigated with existing controls. The fact that they could no longer exploit existing controls led to the exploration process to identify a new set of controls that would align with the dynamic nature of RPA.

Conclusions and Implications

The role of the information systems security compliance function in organizations has been described to be centered on managing known risks by adopting a *prevention* approach, or on managing emergent risks through a *response* approaches instead (Baskerville et al., 2014). Previous research has considered the role of security compliance in managing mostly external threats to the organization. However we find that these two security modes are salient in internal processes of digital transformation, which trigger similar modes of functioning by the security compliance function in organizations. Although the threat is not-malicious, digital transformation can be seem to create emergent risks and therefore requiring a response mode to managing risks associated with the project. Our study captures the inherent tensions between the transformative effects of the RPA project in Autofin and the way the compliance team responded by adopting postures that are similar to response mode as described in the study by Baskerville et al (2014).

The analysis of our data allowed us to identify distinct periods or phases when either the transformation or compliance forces dominated the project development, we represented these phases in Figure 2 above. Each phase is marked by an inflexion point, which represents a tension between the two dominating forces. In the findings we describe some of these tensions and resolutions, including the tension that emerged when the teams realized that the existing compliance frameworks were inadequate to assess the risks inherent in

the RPA project. The negotiations led to adjustments to the framework and the progressing of the project forward, although then with an emphasis on transformation rather than compliance.

These tensions resulting from the juxtaposition of forces for digital transformation and forces for information security compliance reflect a process of organizational learning (Smith & Lewis, 2011), which allows organizations to move from a mode of enforcing established frameworks for known risks – *security prevention mode*, towards a mode of that allows for new frameworks to capture emergent risks – *security response mode*. We can therefore indicate that organizing tensions inherent in the RPA (Tilson et al, 2010) play a pivotal role in shifting the emphasis of the project from transformation to compliance, which also represent swings in IS security compliance function from prevention to response. We believe that is a useful and valuable contribution to this field of research.

Another key learning from this research is that the inherent generativity of digital technologies creates emergent unknown risks which requires a response mode approach to security compliance. Our study therefore makes a contribution to information systems security research by showing how the security compliance in organizations copes with pressures from projects of digital transformation. We conceptualize the pressures for compliance as they react against pressures for digital transformation in Autofin, and identify and describe inflection points that shift the dominant mode of compliance from prevention to response and the reverse. This extends the work by Baskerville et al (2014) on internal security threats to review the significance of their ideas in the context of internal pressures for digital transformation.

References

Anderson, C., Baskerville, R. L., Kaul, M., Anderson, C., Baskerville, R. L., Information, M. K.,Kaul, M. 2017. "Information Security Control Theory: Achieving a Sustainable Reconciliation Between Sharing and Protecting the Privacy of Information Information Security Control Theory", *Journal of Management Information Systems* (34:4), pp. 1082–1112.

Baskerville, R., Spagnoletti, P., & Kim, J. 2014."Incident-centered information security: Managing a strategic balance between prevention and response",*Information and Management* (51:1), pp. 138–151.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. 2010. "Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness", *MIS Quarterly* (34:3), pp 523–548.

Carr, J. 2010. "The Four Minute Malware: Aurora, Stuxnet, and Beyond", *Retrieved on August, 2019 from Forbes, http://www.forbes.com/sites/firewall/ 2010/12/27/the-four-minute-malware-aurora-stuxnet-and-beyond/*.

Cram, W. A., & Brohman, K. 2016. "Information Systems Control: A Review and Framework for Emerging Information Systems Processes", *Journal of AIS (17:4),* pp. 216–266.

Cram, W. A., Proudfoot, J. G., & D'Arcy, J. 2017. "Organizational information security policies: A review and research framework", *European Journal of Information Systems* (26:6), pp. 605–641.

Eisenhardt, K.M. and Graebner, M.E., 2007. "Theory building from cases: Opportunities and challenges", *Academy of management journal (50:1),* pp.25-32.

Farjoun, M., 2010. "Beyond dualism: Stability and change as a duality", *Academy of Management Review* (35:2), pp.202-225.

Finnerty, K., Motha, H., Shah, J., White, Y., Button, M. and Wang, V. 2018. "Cyber Security Breaches Survey 2018: Statistical Release",*Retrieved on August, 2019 from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/702074/Cyber_Security_Breaches_Survey_2018_-_Main_Report.pdf*

Garud, R., Berends, H. and Tuertscher, P., 2017. " Qualitative approaches for studying innovation as process". In *The Routledge companion to qualitative research in organization studies,* pp. 226-247, Routledge.

Gioia, D.A., Corley, K.G. and Hamilton, A.L 2013. "Seeking qualitative rigor in inductive research: Notes on the Gioia methodology", *Organizational research methods* (16:1), pp.15-31.

Henfridsson, O. and Bygstad, B., 2013, "The generative mechanisms of digital infrastructure evolution", *MIS quarterly*, pp.907-931.

Herath, T., & Rao, H. R. 2009. "Protection motivation and deterrence: A framework for security policy compliance in organisations", *European Journal of Information Systems* (18:2), pp. 106–125.

Hess, T., Matt, C., Benlian, A. and Wiesböck, F., 2016. "Options for formulating a digital transformation strategy", *MIS Quarterly Executive*, *15*(2), pp. 123-139

Kallinikos, J., Aaltonen, A. and Marton, A., 2013. "The ambivalent ontology of digital artifacts",*MIS Quarterly*, pp.357-370.

Kemmis, S. and McTaggart, R., 2005. "Communicative action and the public sphere", *The Sage handbook of qualitative research*, pp.559-603.

Klein, H.K. and Myers, M.D., 1999. "A set of principles for conducting and evaluating interpretive field studies in information systems", *MIS quarterly*, *23*(1), pp.67-94.

Knapp, K. J., Morris, R. F., Marshall, T. E., & Anthony, T. 2009. "Information security policy : An organizational-level process model", *Computers & Security* (28:7), pp. 493–508.

Kumar, R.L. and Stylianou, A.C. 2014. "A process model for analyzing and managing flexibility in information systems", *European Journal of Information Systems* (23:2), pp.151-184.

Lacity, Mary and Willcocks, Leslie 2016. "Robotic Process Automation at Telefonica O2," *MIS Quarterly Executive*: Vol. 15 : Iss. 1 , Article 4.

Lee, C. H., Geng, X., & Raghunathan, S. 2016. "Mandatory standards and organizational information security", *Information Systems Research* (27:1), pp. 70–86.

March, J.G., 1991. "Exploration and exploitation in organizational learning", *Organization science*, *2*(1), pp.71-87.

Miles, M.B. and Huberman, A.M.,1984. *Qualitative data analysis,* Beverly Hills.

Myers, M.D. and Newman, M., 2007. The qualitative interview in IS research: Examining the craft. *Information and organization*, *17*(1), pp.2-26.

Niemimaa, E., & Niemimaa, M. 2017. "Information systems security policy implementation in practice: From best practices to situated practices", *European Journal of Information Systems* (26:1), pp. 1–20.

Njenga, K. 2016. "Information Systems Security Policy Violation : Systematic Literature Review on Behavior Threats by Internal Agents" in *CONF-IRM 2016 Proceedings (38)*, May 1–13.

Njenga, K., & Brown, I. 2012. "Conceptualising improvisation in information systems security", *European Journal of Information Systems* (21:6), pp. 592–607.

Ransbotham, S., Fichman, R.G., Gopal, R. and Gupta, A. 2016. "Special section introduction—ubiquitous IT and digital vulnerabilities", *Information Systems Research* (27:4), pp.834-847.

Siponen, M., & Iivari, J. 2006. "Six Design Theories for IS Security", *Journal of Association for Information Systems (7:7)*, pp. 445–472.

Smith, W. K., & Lewis, M. W. 2011. "Toward a theory of paradox: A dynamic equilibrium model of organzining", *Academy of Management Review* (36:2), pp. 381–403.

Stephenson, P. 2004. "Managing digital incidents – a background", *Computer Fraud & Security* (12), pp. 17–19.

Tilson, D., Lyytinen, K., & Sørensen, C. 2010. "Digital infrastructures: The missing IS research agenda", *Information Systems Research* (21:4), pp. 748–759.

Walsham, G., 1995. "Interpretive case studies in IS research: nature and method", *European Journal of*

information systems, *4*(2), pp.74-81.

Weick, K.E., 1989. "Theory construction as disciplined imagination", *Academy of management review*, *14*(4), pp.516-531.

Yoo, Y., Boland, R. J., Lyytinen, K., & Majchrzak, A. 2012. "Organizing for Innovation in the Digitized World", *Organization Science* (23:5), pp. 1398–1408.

Yoo, Y., Henfridsson, O., & Lyytinen, K. 2010. "The new organizing logic of digital innovation: An agenda for information systems research", *Information Systems Research* (21:4), pp. 724–735.