In: Proc. 4th European Workshop on Usable Security, EuroUSEC 2019, IEEE 2019. Stockholm, Sweden, June 20, 2019. To appear: IEEE Xplore

2 Fast 2 Secure: A Case Study of Post-Breach Security Changes

Albesë Demjaha, Tristan Caulfield, M. Angela Sasse, David Pym
Dept. of Computer Science
University College London
London, United Kingdom
{albese.demjaha.16, t.caulfield, a.sasse, d.pym}@ucl.ac.uk

***Abstract*—A security breach often makes companies react by changing their attitude and approach to security within the organization. This paper presents an in-depth case study of post-breach security changes made by a company and the consequences of those changes. We employ the principles of participatory action research and humble inquiry to conduct a long-term study with employee interviews while embedded in the organization's security division. Despite an extremely high level of financial investment in security, and consistent attention and involvement from the board, the interviews indicate a significant level of friction between employees and security. In the main themes that emerged from our data analysis, a number of factors shed light on the friction: fear of another breach leading to zero risk appetite, impossible security controls making non-compliance a norm, security theatre undermining the purpose of security policies, employees often trading-off security with productivity, and as such being treated as children in detention rather than employees trying to finish their paid jobs. This paper shows that post-breach security changes can be complex and sometimes risky due to emotions often being involved. Without an approach considerate of how humans and security interact, even with high financial investment, attempts to change an organization's security behaviour may be ineffective.**

***Index Terms*—data breach, post-breach security, participatory action research, humble inquiry, security culture**

I. Introduction

As businesses and organizations become ever more dependent on their information infrastructure and assets, the importance of well-considered and -implemented security likewise increases. Firms that fail to protect their systems and confidential data can suffer severe economic or reputational damage. For organizations that do not have a strong focus on security—along with many that do—suffering a security breach can be the stimulus that causes them to change the way they think and act about security.

This paper presents results from a case study of an organization that suffered a breach after an insider attack and rapidly changed its attitude towards security in order to prevent a future re-occurrence. The case study, conducted through long-term diary studies and interviews with security staff, explores how employees perceive the company's approach to security as directed by its board. Typically, reactions to breaches are only seen in external statements and actions by companies—often to reassure customers and shareholders—so this study offers a unique perspective into the consequences inside an organization of post-breach security changes.

From the study, we see that even though the company is able to devote significant financial and human resources to its security function, there is a great deal of friction between employees' primary tasks and security, which can lead to non-compliance with security policies [4]. This suggests that a rapid, high investment in security without considering how the changes will affect employees or making efforts to shift the security culture of the organization may not be efficient. A more measured effort that accounts for how employees perceive and interact with security policy and controls might be more effective.

In the next section, we give a brief discussion of how other firms have responded to breaches. Following that, in Section III, we describe the organization studied and give details of our methodology. In Section IV we present and discuss the themes around security in the organization that we discovered. Finally, Section V gathers insights from the discussion and concludes the paper.

II. Reactions to Breaches

Literature on post-breach analysis is limited, and the majority is not academic, but rather industrial and regulatory. While there are some papers which discuss log analysis of post-incident data [11], the financial impact of IT security breaches [10], and the economic cost of publicly known data breaches [8], what happens to the security of a company after a breach is not really discussed in the research community.

The number of breaches has drastically increased over the years [9], with 2018 leaving behind at least fifteen severe data breaches in the UK.[1] A previous major data breach which has left its mark in the UK is the TalkTalk breach as the company largely failed at protecting its customers' data. The Information Commissioner's Office was seriously involved and even published a report[2] with the breach analysis and future recommendations. TalkTalk's CEO claimed that the breach was an eye-opener and it strongly impacted the company's security. According to one of the board members, things changed:

[1] https://www.techworld.com/security/uks-most-infamous-data-breaches-3604586/

[2] https://publications.parliament.uk/pa/cm201617/cmselect/cmcumeds/148/148.pdf

> "from cyber security being an item on the board meeting to being a *lens* through which all decisions are viewed." [3]

Although TalkTalk have been encouraged to make substantial changes to their security, they have not excluded the possibility of another breach occurring in the future. In the words of the CEO:

> "You can't say you are 100 percent certain that your measures are going to keep everything secure. Criminals only have to get lucky once." [4]

Target's data breach, on the other hand, was an internationally infamous one. Shu, Tian, Ciambrone, and Yao [22] provide a detailed analysis of how the breach happened and what went wrong. As a result of the breach, Target hired a new CEO and invested 100 million dollars for improving security by deploying chip and pin technology, upgrading insecure point of sale machines, improving network segmentation, etc. [22].

Many companies have suffered great financial losses due to data breaches. In addition, those companies have had to invest a large number of resources for better security. For example, after a horrible breach and an attempt to cover it up, Uber claimed that they added the following resources:

> "Earlier this year we hired our first chief privacy officer, data protection officer, and a new chief trust and security officer. We learn from our mistakes and continue our commitment to earn the trust of our users every day." [5]

Each company reacts and invests differently post-breach. However, there is no silver bullet against data breaches [22]; even high levels of investment cannot guarantee an absence of breaches in the future,

III. Case-Study

This case-study takes an in-depth look at a single company. In this section we give a description of the company and its reactions to a security incident, as well as details about the approach and methodology we used for the study.

A. About the company

The company—hereafter referred to as Company A—is a medium-large company in the financial sector. It is based in the United Kingdom and only operates within the country. The company places great value on its information assets, upon which its business success depends. As such, Company A takes security seriously. The company has significantly grown over the last two decades, with its original start-up mentality slowly shifting to a more corporate one, and is now heading towards a thousand employees.

Company A's serious attitude towards security has not not always been present. In earlier stages of operation and growth, security was largely informal, with very basic security controls. Then, around four years ago, Company A suffered an information security breach in the form of an insider attack. The existing controls were, fortunately, enough to mitigate most financial and reputational damage to the company, but the incident highlighted how the organization's approach to security needed to be taken more seriously.

Following the incident, the company began to invest heavily in security, both in terms of personnel and technology, to ensure that a similar incident could not occur in the future. Now, the increase in security is apparent around the office: physical barriers control entry to and exit from the building, and CCTV cameras are present throughout the office. The number of staff working on security has risen to ten percent of the organization. This includes employees working on security architecture, engineering, incident response, risk, compliance, and physical security.

In addition to this, Company A also made efforts to formalise its security policy. However, this was done in a somewhat ad hoc manner; there is no centralised security policy, but instead a number of policies—sometimes conflicting—in different locations. The policies differ on various terms: technicality, scope, and audience. There are certain policies that are too technical for anyone but the employees required to implement them. Other policies only concern the security of some company assets, while others only adhere to security employees.

The security policies concerning all employees regardless of their job type, can be found in the company's handbook. Although some of the content in these policies is quite useful to read, especially for a new joiner, the majority are too long or over complicated. The rules outlined within this handbook are all contractual, meaning that breaking them can lead to disciplinary action. However, there is no formalised and systematised escalation process for acknowledging necessary disciplinary action. Therefore, some incidents may go without notice, while others may be escalated unexpectedly. Such an approach can raise doubt in the legitimacy of the policies and allow employees to be less cautious about security.

There has been a recent initiative to sort out the security policy issues that are currently present. It has now been decided that a centralised security policy would better fit the new format of Company A. Such a policy will be based on known security frameworks such as NIST and ISO27002. Its main purpose is to achieve consistency among all security policies as well as make security rules more understandable to non-security staff.

B. Methodology

The methods that we used for this case-study were influenced by the context of our engagement with Company A. One of the authors had the opportunity to work in the company's security division for six months. Therefore, it seemed natural to follow a methodology that is based on the

[3] https://www.cbronline.com/business/talktalk-head-of-security-what-we-learned-from-the-cyber-attack-4886225/

[4] https://www.silicon.co.uk/security/cyberwar/talktalk-security-talktalk-dido-harding-182393

[5] https://www.independent.co.uk/news/business/news/uber-fined-information-commissioner-data-protection-failings-a8653631.html

participation and engagement of all stakeholders. Since this study is an exploratory pre-study to a larger follow-up study and focuses on identifying the actual problems, we decided to exclude Yin's case-study methodology [28] in this paper, as the framework is more adequate for a series of studies. Instead, we focus on the principles of participatory action research [13] and humble inquiry [20].

Participatory Action Research: Engaging methods such as action research and participatory action research (PAR) were first introduced to the field of information systems in the 90's [3]. Since then, such creative engagement methods have been applied to security studies [1], [12]. The purpose of these methods is to be playful, participative, open-ended, and democratic [12].

The methodology consists of a self-reflective, iterative process [13] where changes are planned and then consequences are observed and reflected upon—leading to further changes. The process is reflective of the author's activities at Company A as well as the ever changing environment within an organization. It is important to note that the changes occurring at the company were not designed interventions but rather regular changes that happen in organizations.

PAR emphasises the importance of understanding the factors below [13], which were particularly helpful throughout our research—we have added a specific explanation of each in the context of Company A:

- What people do—a clear understanding of what employees do at Company A and what their daily tasks are;
- How people interact with the world and with others—an understanding of how the employees of Company A interact with the colleagues in their division as well as outside of their division;
- What people mean and what they value—a deeper account of the opinions and values that Company A employees hold;
- The discourses in which people understand and interpret their world – a written account of the descriptions Company A employees use to make sense of things.

In addition to these factors, PAR has other key features that have guided our research at Company A. The features are listed below, followed by a description of how these were considered in our research:

Participatory action research is a social process: We deliberately observed the relationship between individuals in the organization and their social environment due to the importance that this interaction plays in the concept of security culture. The above statement implies that *individuation* cannot happen without socialisation and vice-versa; this is reflected in security culture due to necessity of shared assumptions to form a culture, which can only be created as a result of socialization.

Participatory action research is participatory: By examining employees' knowledge, understandings, skills, and values, we gained a better understanding of their actions and how those actions affect the company's security.

Participatory action research is practical and collaborative: Having a member of our team working at Company A enabled us to collaborate with the employees which we were simultaneously observing. Thus, we examined the social interactions that they were taking part in, to explore how that may impact the organization's security and dynamic.

Participatory action research is reflexive: It is common for companies to initiate change without thoroughly understanding what exactly should change and why. When conducting both the company-specific as well as research tasks, we were always encouraging an investigative approach to a problem. Through an iterative process of critical and self-critical action and reflection, we attempted to help employees make changes where necessary.

Participatory action research aims to transform both theory and practice: PAR does not treat either theory or practice in isolation. This last feature significantly benefits the company implementing the method. Through PAR, we aim to develop both theory and practice in relation to each other in order to create a feedback loop and consequently improve both.

The Study: The study consists of 15 *semi-structured interviews* conducted with members of security management at Company A. The main study objectives are 1) to define and evaluate the daily security processes in Company A, 2) to identify any friction and the reasons behind it, and 3) to identify security behaviours and perceived reasons for them. The study went through our department's ethics review process. Participants were given information sheets and consent forms before the start of the interviews and participated of their own free will.

Diary Entries: Although the key emphasis of the study is on the interviews, it is worth mentioning the diary entries as well. They were written as part of an observational task by the author working at the company. During the first few weeks at the company, the author took the opportunity to become familiar with Company A's security division and how things run at the company in general. Monthly diary entries were produced during the six month period. Although those entries are not included in the paper due to confidentiality reasons, we use them as a research aid in order to further contextualise our findings.

Participants: We interviewed 15 participants in total. In order to best understand the security practices of the company, we focused this first study around the members of the security management at Company A. Security management consists of roles such as senior heads, security managers, deputy managers, and group heads. There were 16 employees at Company A which held such roles at the time. To avoid any selection bias and simultaneously enrich the data set, the entire security management team was asked to be interviewed. 15 out of 16 participants showed up for their interviews. One group head could not make the first interview due to being outside of the country and missed the second interview due to unexpected work obligations. Since the study period had finished, a third interview was not scheduled with the group head.

Interviews and Humble Inquiry: The length of each interview was initially set to 30 minutes due to the hectic

schedules of the participants. However, there were interviews which lasted shorter and longer than 30 minutes, depending on several factors such as the participant arriving late, a mix-up with the interview rooms, having to clarify a question to a participant, etc. The average length of the interviews was approximately 21.8 minutes. We only proceeded with the interview once the participant had read the information sheet and ticked all the boxes on the consent form.

It was crucial to conduct the interviews in a way that reflects the principles of PAR. The interviews were not strictly designed to benefit our research, they were a collaboration between us and the employees of Company A. Therefore, the interview methodology had to mirror this collaboration and treat the participants almost as co-researchers rather than as interviewees. Schein's humble inquiry [20] encourages positive relationships and effective communication.

> "*Humble Inquiry* is the fine art of drawing someone out, of asking questions to which you do not already know the answer, of building a relationship based on curiosity and interest in the other person." [20, p.2]

More specifically, the method relies on the concept of humility and inquiry. The type of humility relevant to this study is the 'here-and-now humility' which Schein describes as a situation in which the researcher, or the person asking questions is inferior to the participant in that the participant has information which would help complete the task of the researcher. The important thing is to acknowledge this dependency and build a relationship with the participant (in this case a Company A security manager) on the basis of curiosity and interest. Inquiry on the other hand, here is described as the type of inquiry that goes beyond overt questioning. It is the type of inquiry that would lead to open communication. When in a situation of here-and-now humility, it is that dependency and temporary 'inferiority' that makes the participant feel more psychologically comfortable and likely to share the information that the researcher needs.

Humble inquiry aims to reduce bias—it does not influence what the participant has to say nor the manner in which it is said. This principle is crucial for attaining data which is not influenced by the researcher. If the content described by the participant is somewhat unclear, instead of leading the content to where the researcher wants, it is better to instead ask for an example. This is a powerful method of showing curiosity and interest and simultaneously clarifying the participant's statements.

IV. Themes

We transcribed the interviews verbatim and used Thematic Analysis [6] for the transcript analysis. Although it stems from psychology, thematic analysis has gone beyond the field and is now a widely used method for analysing qualitative data.

> "Thematic analysis is a method for identifying, analysing, and reporting patterns (themes) within data. It minimally organises and describes your data set in (rich) detail." [6, p.6]

The main coding process using thematic analysis was conducted by the field researcher because of her detailed familiarity with the data. As a sanity-check, this was reviewed by one of the other researchers, who agreed with the codes and themes generated by the process.

A total of 42 codes were produced—some of which were discarded when refining the analysis. Therefore, the final codebook has 38 codes in total. Below are a few example codes with their description and a matching quotation from the interview transcripts.

- ***hierarchical influence***; This code is used whenever a reference is made to top management or board members. They are usually mentioned in the context of having an impact over something which is why the word influence is used.
  - *"I mean you know it's going back down to how do you get people to buy into security. And you either have the champions pushing that out there or you have mandated from the CEO downwards so that people know it's important."*
- ***purpose of having a security policy***; This code questions the purpose of having a security policy. It was generated in reference to employees not taking the policy seriously which makes the existence of a security policy questionable.
  - *"Everybody has to understand that those policies are there for a reason and they must be enforced. If you need an exception to them, fine, go and get an exception through proper channels, don't just ignore them."*
- ***security is security's job***; This code reflects the company's perception about security only being the job of the security division and as a result, the rest of the organization not taking part in the implementation of security or responsibility for it.
  - *"So, if the board is clearly focusing its attention on the security function and saying that 'security is security's job', well it's not surprising that the rest of the organization actually feels that."*

The codes that were related to one another were then grouped together to form themes. Eight themes about Company A's approach to security and its employees' perceptions and attitudes towards security emerged from the thematic analysis of the interview data. These themes are summarised in Table I, which lists them and provides an overview of their meaning. We then discuss each of the themes in more detail.

A. Post-shock security

When responding to questions, almost every single participant refers to an incident that the company was a part of several years ago. Often, this incident is the justification for their answers, as if it changed everything in the company—which it did. The security structure of Company A is completely determined by the aftermath of that security breach. The majority of the security controls were put in place as a

TABLE I
EMERGENT THEMES FROM THEMATIC ANALYSIS

Theme	Brief Description
Post-shock security	The effect of a security breach on the current security structure and practices at Company A
Security theatre undermines policy	The consequences of implementing security controls for the sake of 'security theatre'
Security is like detention	The non-security employees are treated as 'enemies' when it comes to the security of company
Security is a blocker	Employees of other divisions often struggle to be productive because of the blocking nature of the security controls
Lack of effective communication	The importance of security is not effectively communicated across the organization
Zero risk-appetite	The appetite for taking security risks is next to zero in the organization
Sensible security is likely to work	Security managers believe that more sensible security controls are likely to increase compliance
Behaviour change is required	Behaviour change is required across the organization to create better security habits

knee-jerk reaction to the breach itself, and because of the fear of losing everything. For a business that makes profit from generating intellectual property, IP theft is a great concern [17]—and likely to be caused by a disgruntled insider [17].

Such existential threats place cyber security at a level of priority for the board rather than remaining an 'IT concern' [19]. Company boards are increasingly being encouraged to become seriously involved with the security of their organization [25]. However, when it comes to insider attacks, many companies underestimate them and fail to report them when they occur [17]. Company A is on the other side of this spectrum though. The CEO and the board became very much involved after the breach, and if anything, have been overestimating insider threats since.

Therefore, the entire company, and especially the security division, reflect the fear that still lingers on as a consequence of the breach. The controls resemble barriers and it is visually clear that security is present once you enter the company due to the ubiquity cameras in every space. This is intentional, of course, as the board wants to spread the message that the company is secure and it is almost impossible to breach that security. However, even the security managers believe that this post-shock approach is too much. Participant 9 says the following about the visible security measures:

> *"So I think there's something about making it visible and visceral to people, in a way that resonates with them. But there's also something about making whatever security knowledge you've got rational to meet the risk in the first place, because some of them just aren't. The advantage of this culture is that it keeps the board happy. And I don't think it, my experience in security, even in this long time, it's doing security this way, doesn't make you more secure."* - P9

In other words, it is perceived that the security controls are there predominantly to decrease the board's fears of another breach. Although some of those controls might actually be beneficial to the security of the company, the majority of them are there to create a feeling of security rather than practically protect against a threat. Having taken the attack quite personally, the board often takes emotionally-driven decisions that are directly linked to the specifics of the breach. No financial investment appears too big as long as history does not repeat itself. The executives are often caught up in technical reports [19] and spend too much time and money implementing technical controls while losing sight of the importance of people and processes.

B. Security theatre undermines policy

This theme follows the observation that most security controls in Company A are there for show, rather than for actual security. In the words of Schneier, *security theatre* refers to those security measures that are intended to create a feeling of security rather than concretely improve security. [6] Such measures can often unintentionally decrease the level of security because of their undermining nature. Namely, employees (or some of them at least) will realise at some point that certain measures are ineffective, and they will find ways to circumvent them. Once they learn how to do this, they will get in the habit of continuously bypassing certain security mechanisms.

This type of attitude also reflects badly on new joining employees. Once they pick up on these circumventions, that brings along a new generation of non-compliers who are trying to 'fit in' [16]. It is then difficult to convince people to comply with a policy that is unrealistic and clearly being breached by the majority of the company, most likely security employees too. Participant 3 explains this further:

> *"You know if you're not careful, it's the classic thing of you write a policy, it's maybe got ten points, maybe nine of them are actually valid, the tenth one isn't valid at all and isn't enforced because actually it's universally accepted within the organization that you breach that one because it's a real pain. Whenever a new person comes into the organization, they see the ten rules, they say oh everyone routinely breaches this rule, well obviously the policy isn't enforced, we don't really care about policy. Actually, do you know, rule number three is a real pain for me so I'm gonna breach that one. Rule number three might be a really really important one…"* - P3

The reason why this theme holds this title is because employees are usually blamed for undermining security policy, when in fact, the company undermines its own policies

[6] www.schneier.com/essays/archives/2009/11/beyond_security_thea.html

by 1) implementing security theatre, and 2) allowing non-compliance to become prevalent behaviour [16]. Some managers tolerate their trustworthy employees in circumventing the burdensome polices and follow their own *shadow security* to stay secure [15].

Once security violations become a norm [16], it does not take long for employees to see through some of the faux security mechanisms at the company. Once they do, they can challenge the integrity of those security mechanisms and further question the company's seriousness about security. If the company is implementing measures that do not actually improve its security, then employees will feel even less responsible for acting in a secure manner [7].

Perceived consequences have a significant impact on employees' decision about complying with security [7]. They must be shown that policies are there for a sensible reason and purpose and that they must be enforced—by everyone. However, Company A seems to be in the habit of acknowledging and identifying breaches but not systematically following up on them. Participant 2 confirms this:

> *"I think it's probably that nothing is happening to the members of staff. There's no consequences. A hundred percent. So, yeah, if there was something where if they have done it multiple of times and something happened then I think we will have a much lower... much lower* [non-compliance]. *So I think, for us personally, I think we should have some escalation or something."* - P2

When employees see that non-compliance is going unpunished, that encourages them to continue bypassing policy. The real danger happens when policy rules that are genuinely important start being breached as a result of other 'less important' rules being circumvented. It is therefore more effective to have fewer rules in the policy that actually must be complied with, rather than adding a larger set of rules, some of which are inevitably going to be broken [15], [16], [24].

C. Security is like detention

Regardless of the obvious security theatre in the company, non-security employees are still treated like bad students in detention, having to re-read the same policy multiple times until they decide to stop breaking the rules. Some of these employees might not have broken the rules thus far, but are implicitly expected to do so in the future. Such a severe attitude towards the employees' security behaviour may have an undesired, opposite effect. Employees respond better to intrinsic motivation-based approaches than to sanction-based approaches [23]. That level of distrust in people is risky, in that it could build resentment. According to participant 9:

> *"Because we apply such a low level of trust to individuals, that can feel insulting at times. So I think you almost get the reverse of what you'd expect."*

Furthermore, in relation to the overplayed monitoring:

> *"We've talked about it very much in the terms of I don't trust you, so I'm watching you. That's what my department was when I started—I'm watching you."*

This approach does not seem to be working though, as non-compliance has increased in the last few months. The majority of employees in organizations tend to be trustworthy [16]—treating them as untrustworthy components is counterproductive [14] and merely leaves employees feeling untrusted [16]. It is likely that even employees who are willing to make the effort and invest a portion of their time into security, are deterred by this almost patronising approach. It is not beneficial for either party to continue working with fear as their primary driver [23]. Without trust and collaboration, it is difficult to achieve effective and inclusive security [2].

D. Security is a blocker

Employees in an organization have primary (production) and secondary (enabling) tasks [18]. As an example in this particular context, an employee's production task would be to produce intellectual property, whereas their enabling task would be securing that intellectual property. The completion of a secondary task is not necessary for the completion of their primary task. Rather, in this case, a secondary task is an investment to protect the assets of the individual and of the organization. But, employees have a limited budget for spending time and effort on secondary tasks [4], especially since they were hired for their primary one. When a secondary task, in this case security, prevents one from completing their primary task, it is natural for that individual to view security as a blocker rather than as an enabler. In Company A, even the security managers agree with this:

- *"I think actually it is quite common, quite common thought in this business that security is a blocker to progress in this company."* - P3
- *"You know the disadvantages of [the security approach] are obviously people see that as a roadblock to being able to do your job. If you can't trust people, you're not necessarily using people as effectively as they can. You're paying a lot of smart people to do a lot of smart things and basically you're handcuffing them and not allowing them to do those things, if you do that."* - P7

When faced with a secondary (security) task, employees have to make a choice between complying with that task or bypassing it [26]. This decision-making process will usually include some low-level cost-benefit analysis from the employee's perspective to determine the amount of effort they are willing to sacrifice for security compliance. Due to the lack of any personal gain coming from this compliance, employees exceed their compliance threshold soon enough and refuse to comply any further. Thus, in an attempt to increase their work productivity, they put the organization's security at risk. However, they are not to blame—such situations occur when business and security goals are misaligned and friction is introduced as a result [4]. Employees should not have to break security rules for productivity reasons [16].

In addition to blocking employees' production tasks, security can also affect other parts of the organization. For example, many managers mention that security restrictions such as 'no homeworking' and 'no personal devices in the

work space' have made some employees leave the company while preventing others from joining it:

> *"I think no home working is too restrictive. We can deliver that in a safe and secure way."* - P11
> *"I'm sure there's been one or two people or ten or twenty or thirty people who have decided to resign or don't work here just because they can't have their smartphone or whatever."* - P1
> *"And one thing that changed for us fairly fast after our data breach was that homeworking was disabled and that's turned out to have quite an impact on the hiring. It doesn't actually bother me but for a lot of people it does."* - P15

E. Lack of effective communication

The participants mention lack of proper communication as one of the factors that negatively affects the organization in general, and security in particular. This may involve different types of communication lines, such as communication between different security teams, different members within a security team, security division and other divisions, and the board and the rest of the organization. A lack of communication further instils a lack of trust within the organization and creates an environment of uncertainty.

One reason why there is a lack of effective communication in Company A is the fast growth of the company. Employees used to know each other by name and walk across the room to talk to the person they needed whereas now it is physically difficult to reach people from other teams due to several new floors being added. Effective communication was simpler when Company A was small [27] and the communication process has suffered from this across the organization.

An additional reason as to why having effective communication in an organization is important is due to the circulation of information. As mentioned before, some employees may not follow security policy because they do not understand its purpose, or what may happen if they do not comply with such a policy. It is difficult to have the motivation to invest in a secondary task, without properly understanding why you are being asked to do so.

> *"I think sometimes the understanding of why things are being done the way they're done hasn't always been communicated."* - P13

If the board believes that security is important and an integral part of the company, it must ensure that this message is communicated throughout the organization. The communication should specify that security protects the business and is integral to the entire organization [16]. In other words, the risk aversion and the strict controls should come directly from the people driving them, in order for people to understand their true importance. Otherwise, the non-security employees will be convinced that 'security is security's job' and rely heavily on their expertise whilst taking no responsibility themselves [5]. It is natural for such an opinion to be formed if everything about security comes from security rather than its original source—the board. Participant 8 summarises this argument very well:

> *"[The board] put a lot of the security responsibility on the security division and they don't talk about it as much to other divisions, the message that other divisions hear coming from the board is all about "deliver us these functional requirements, deliver us these new capabilities" but they don't hear the board saying "deliver it securely" or "make sure you are thinking about security". So then the security divisions come along, I will come along, or the CISO will come along and say to those divisions "well we need to actually do that securely". But they're hearing that requirement second hand. And I don't think the board get that, they need to be saying to those divisions, even at the moment "security is tremendously important, you need to work with the security division to make sure that your services are secure" ... even just saying that message I think would go a long way even at the moment with a centralised security model."* - P8

F. Zero risk appetite

The most unanimously-mentioned term amongst the participants is *risk appetite*. It is always mentioned in the context of the company having very little to almost none of it. After the breach, one of the board's knee-jerk reactions was to severely reduce appetite for security risk. By trying to almost completely eliminate security risks, and overplaying the security controls, the board is convinced that such an incident will not occur again. Once again, the emotional reasoning takes over the rational one and even extremely low risks remain untaken due to the incredibly low probability of there being an identical attack again.

All necessary measures have been put in place to carefully asses security risks, on several levels, by several people. Very rarely is any risk accepted; big risks are never accepted even if their likelihood is extremely low. Participants 3, 9 and 12 disagree with this approach:

> *"If the risk to the business is very very low, don't put the security in place. If the cost to security is going to be higher than the risk of loss, risk of a breach, or risk of whatever it might be, then just accept it, that's the cost of doing business, try and reduce it... obviously but don't hurt the business because of it."* - P3
> *"I think we overplayed some of the threat, so we've kind of said we've got to do security here cause this could happen. But actually when you think about it, it could happen, but it's really really unlikely"* - P9
> *"I think historically the company has been very reluctant to accept risk and it's still on a place that certain risks are not even considered to be accepted although the benefit would hugely overtake the actual risk. And I think that part of the problem is the understanding of the risk is not as well*

understood as it should be and that kind of comes in the way." - P12

Having a non-existent risk appetite frustrates the majority of the security managers. They believe that such an approach hinders the business from thriving. When asked what they would like to change in the company's security, more than one manager made reference to the company's lack of risk appetite. Participant 3 continues to talk about the issue:

"Because I think at the moment our… the risk function doesn't actually understand the business drivers and so their risk appetite is prohibitively low. As in, it stops the business from progressing." - P3

Having a low risk appetite does not only impact the security division—it impacts the employees who are trying to do their jobs. The security managers are aware of the frustration that a low risk appetite causes to non-security employees, but it is out of their hands to change this reality:

"I think most of the divisions still see that our risk appetite is too low—and they'd want us to take more risk rather than the level it is at now which is extremely low from a security point of view. So I guess it would be a frustration with a lot of people that they can't just get on and do what they do." - P9

"Would a non-security person look for something different? I think non-security people would just want less security and more risk appetite." - P15

The two main issues that arise from such a risk-averse approach to security are that employees lack the proper understanding of why the company's risk aversion is at this level and are left frustrated, and, employees believe that this approach is driven by security and ultimately blame them for always saying 'no'.

This relates to the previous theme—lack of effective communication. The reasons for having such a low risk appetite have not been properly communicated throughout the company and employees are often left confused. They do not comprehend the importance of rejecting certain security risks and how accepting those risks could *potentially* lead to a second breach. Severity of threat often impacts employees' non-compliance [24]. Thus, it is important to educate employees on the potential security consequences their non-compliance can lead to [24].

G. Sensible security is likely to work

Generally, in security, it is the security professionals that insist on heavy and technical security controls. However, in Company A, this is not necessarily the case. The interviewed participants are almost unanimous in the opinion that the current controls are overplayed and thus, they are not particularly shocked that non-security employees are not happy to comply with them. On the contrary, while the board are demanding extreme measures, the security professionals are trying to to shift towards more sensible security. They believe that if security controls are sensible, employees are more likely to comply with them.

"But also, sensible reality. A lot of people, if they think something is sensible, won't need educating. I'm trying to give a security example—most people, most people don't pile up rubbish in front of fire escapes because you understand why you shouldn't do that, because you're going to burn to death. And even if there isn't a big sign on the door saying do not pile rubbish here, there's a very good chance if there is somebody who does, somebody else will move it because it's sensible and everybody can understand it." - P9

In other words, if the security controls put in place actually make sense, and they are properly explained to employees, it should come more naturally for them to comply. When security is sensible and designed with the purpose of assisting people rather blocking them, they are more likely to make sensible decisions [16]. Rules that keep being broken are likely unfit to support the company and should be re-designed to fit employees' primary tasks [15], [16]. Participant 12 states:

"You want people to take sensible, common sense decisions in their every day work. So you don't want to have a very deterrent security culture that makes them always want to bypass every little thing, you want something that helps them do what they need to do but also supports them in doing that in the right way." - P12

In order to introduce sensible security into the organization, the people running security must also join this approach. An important part of it is communicating the reason why security is doing something and why not doing it may risk the company. Ideally, employees should have the freedom to make suggestions to security about a control that affects their work. In relation to this, participant 6 states the following:

"So it just makes easier working life for everyone, if you raise awareness, push awareness about why we're doing things, invite people to look at what we're working on and the reasons behind that not just 'you can't do this thing… there's actually a reason behind why you can't do this thing. Here's the reason, here's the main reason, here's the way it may leave us vulnerable'. Once they kind of understand that, they're kind of 'okay, that kind of makes sense'. Or let's work out how to achieve still the same level of security but maybe in a better working way for the person or the customer or whoever's trying to get work done. - P6

H. Behaviour change is required

This is not the last theme by coincidence – the rest of the above themes are an indication that Company A requires behaviour change, both of the board, and its employees. In order to leave behind the current security culture and move on to a more preferable one, a period of behaviour change is necessary. Such change can take a lot of effort and time [21]. Participant 9 states that somebody has to be told the same

thing seven times before they actually listen to it. Participant 10, on the other hand, comments on how long cultural change takes:

> *"To change the culture it takes between, around 2 years or more, on average 2 years. To change the culture, the way people think."* - P10

Before any change can be truly initiated, there's the challenging bit of *unlearning* people's behaviours and discarding their old habits. According to Schein, a cultural transformation primarily requires the unlearning of current behaviours in order to move on to new ones [21]. A few participants shed light on the difficulty of changing security behaviours:

> *"I think it's harder for people that used to work in a certain way to change. I'm guessing if you come from a company that's a lot more open and a lot more flexible in the working approach because of the nature of the business or what they're working on, I can understand that but I think also for people that have been here a long time and going through change I think can be a challenge for some as well."* - P6
>
> *"I think the sense of a shared... some level of a shared responsibility for security was there [in participant's previous company] from the start. So, I think the potential damage that's being done here by pushing a heavily centralised security model had never happened there."* - P8

The statements above point out that change is difficult and it takes time. People have their habits and those cannot be broken over night [24]. There are certain security behaviours at Company A which need to be changed, but because they were encouraged from the very beginning, that change will require timely persistence. A crucial step in this change process is to let employees know exactly what the company is tending to change, which specific behaviours, and why. Once that has been clearly communicated, employees will need assistance and constant reminders to achieve that change. A systemised transformational process is required to accomplish desired cultural results, as well as sufficient time [21]. The majority of participants suggest training and education efforts to achieve behavioural change. Although those measures will be necessary, they are not sufficient in isolation. Employees must be given the adequate understanding and skills to be able to change their behaviour.

V. Conclusion

This study is limited in that it looks only at a single company, but we feel it nevertheless provides some interesting insight into the problems that can be encountered when rapidly adjusting an organization's attitude and approach to security after a breach. Company A's board responded to its breach with a determination to prevent another. Security became a high priority, and investment increased accordingly. However, even with an giant security budget and large team, our study found that security was perceived as a barrier to work by employees, some of whom also felt that they were being treated as the enemy, under constant surveillance.

One of the main causes of friction appears to be the lack of effective communication around security. The board sees security as a high priority, but communicates this mainly to the security team and not other employees, who then become frustrated when their primary tasks—their jobs—are interrupted or blocked by the need for security. Better communication would create a better understanding and help harmonise the relationships between the board, who are setting the security policy, the security team, who must implement it, and the other employees, who must follow it while performing their primary tasks. Improved communication might also help with some of the other perceived problems. The low risk appetite in the organization leads to barriers to employees' primary tasks and ubiquitous surveillance. But if the reasons behind these security decisions were better explained, employees might be happier to comply.

There is an awareness among the employees interviewed of a need for more sensible security policies and behaviour change to remedy the perceived problems. These are things that should have been considered all along. A large budget and a refusal to accept risk is not guaranteed to create a good security environment. Post-breach changes in security should not just aim to rapidly 'increase security', but be made with knowledge of the company's security culture and how that will interact with any proposed policies in order to be effective. A traditional sanction-based approach treats employees as untrustworthy [16], whilst the only way forward is to nourish a security culture through trust and collaboration [2].

This work is part of a longer-term project that aims to study how an organization's culture, employees, and security interact. Future work will be to look at how to plan migrations of policy and culture to achieve the organization's desired security objectives, the importance of which is shown by this study—without an approach considerate of how humans and security interact, even with high investment, attempts to change an organization's security behaviour may be ineffective.

References

[1] D. Ashenden and D. Lawrence, "Security dialogues: Building better relationships between security and business," *IEEE Security & Privacy*, vol. 14, no. 3, pp. 82–87, 2016.

[2] D. M. Ashenden, L. Coles-Kemp, and K. O'Hara, "Why should i?: Cybersecurity, the security of the state and the insecurity of the citizen," *Politics & Governance*, vol. 6, no. 2, pp. 41–48, 2018.

[3] R. L. Baskerville, "Investigating information systems with action research," *Communications of the association for information systems*, vol. 2, no. 1, p. 19, 1999.

[4] A. Beautement, M. A. Sasse, and M. Wonham, "The compliance budget: Managing security behaviour in organisations," in *Proceedings of the 2008 New Security Paradigms Workshop*, ACM, 2009, pp. 47–58.

[5] J. M. Blythe, L. Coventry, and L. Little, "Unpacking security policy compliance: The motivators and barriers of employees security behaviors," in *Eleventh Symposium On Usable Privacy and Security ({SOUPS} 2015)*, 2015, pp. 103–122.

[6] V. Braun and V. Clarke, "Using thematic analysis in psychology," *Qualitative research in psychology*, vol. 3, no. 2, pp. 77–101, 2006.

[7] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, "Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness," *MIS quarterly*, vol. 34, no. 3, pp. 523–548, 2010.

[8] K. Campbell, L. A. Gordon, M. P. Loeb, and L. Zhou, "The economic cost of publicly announced information security breaches: Empirical evidence from the stock market," *Journal of Computer Security*, vol. 11, no. 3, pp. 431–448, 2003.

[9] K. Finnerty, H. Motha, J. Shah, Y. White, M. Button, and V. Wang, "Cyber security breaches survey 2018: Statistical release," 2018.

[10] A. Garg, J. Curtis, and H. Halper, "Quantifying the financial impact of it security breaches," *Information Management & Computer Security*, vol. 11, no. 2, pp. 74–83, 2003.

[11] J. Haggerty and T. Hughes-Roberts, "Visualization of system log files for post-incident analysis and response," in *International Conference on Human Aspects of Information Security, Privacy, and Trust*, Springer, 2014, pp. 23–32.

[12] C. P. Heath, P. A. Hall, and L. Coles-Kemp, "Holding on to dissensus: Participatory interactions in security design," *Strategic Design Research Journal*, vol. 11, no. 2, pp. 65–78, 2018.

[13] S. Kemmis and R. McTaggart, *Participatory action research: Communicative action and the public sphere.* Sage Publications Ltd, 2005.

[14] I. Kirlappos, A. Beautement, and M. A. Sasse, "comply or diei is dead: Long live security-aware principal agents," in *International Conference on Financial Cryptography and Data Security*, Springer, 2013, pp. 70–82.

[15] I. Kirlappos, S. Parkin, and M. A. Sasse, "Learning from shadow securityi: Why understanding non-compliance provides the basis for effective security," 2014.

[16] I. Kirlappos and M. A. Sasse, "What usable security really means: Trusting and engaging users," in *International Conference on Human Aspects of Information Security, Privacy, and Trust*, Springer, 2014, pp. 69–78.

[17] J. R. Nurse, P. A. Legg, O. Buckley, I. Agrafiotis, G. Wright, M. Whitty, D. Upton, M. Goldsmith, and S. Creese, "A critical reflection on the threat from human insiders–its nature, industry perceptions, and detection approaches," in *International Conference on Human Aspects of Information Security, Privacy, and Trust*, Springer, 2014, pp. 270–281.

[18] S. L. Pfleeger, M. A. Sasse, and A. Furnham, "From weakest link to security hero: Transforming staff security behavior," *Journal of Homeland Security and Emergency Management*, vol. 11, no. 4, pp. 489–510, 2014.

[19] R. A. Rothrock, J. Kaplan, and F. Van Der Oord, "The board's role in managing cybersecurity risks," *MIT Sloan Management Review*, vol. 59, no. 2, pp. 12–15, 2018.

[20] E. H. Schein, *Humble inquiry: The gentle art of asking instead of telling*. Berrett-Koehler Publishers, 2013.

[21] ——, *Organizational culture and leadership*. John Wiley & and Sons, 2010, vol. 2.

[22] X. Shu, K. Tian, A. Ciambrone, *et al.*, "Breaking the target: An analysis of target data breach and lessons learned," *arXiv preprint arXiv:1701.04940*, 2017.

[23] J.-Y. Son, "Out of fear or desire? toward a better understanding of employees motivation to follow is security policies," *Information & Management*, vol. 48, no. 7, pp. 296–302, 2011.

[24] A. Vance, M. Siponen, and S. Pahnila, "Motivating is security compliance: Insights from habit and protection motivation theory," *Information & Management*, vol. 49, no. 3-4, pp. 190–198, 2012.

[25] B. Von Solms and R. Von Solms, "From information security to business security?" *Computers & Security*, vol. 24, no. 4, pp. 271–273, 2005.

[26] D. Weirich and M. A. Sasse, "Pretty good persuasion: A first step towards effective password security in the real world," in *Proceedings of the 2001 workshop on New security paradigms*, ACM, 2001, pp. 137–143.

[27] P. A. Williams, "What does security culture look like for small organizations?," 2009.

[28] R. K. Yin, "Case study research: Design and methods (applied social research methods)," *London and Singapore: Sage*, 2009.