# Preparing for GDPR: helping EU SMEs to manage data breaches

Keshav Kapoor
Karen Renaud
Jacqueline Archibald



Kapoor, K., Renaud, K. & Archibald, J. 2018. Preparing for GDPR: helping EU SMEs to manage data breaches. In: *AISB 2018: Symposium on Digital Behaviour Interventions for Cyber-Securilty*. AISB, pp.13-20

# Preparing for GDPR: Helping EU SMEs to Manage Data Breaches

Keshav Kapoor
University of Glasgow
Glasgow, Scotland

Karen Renaud & Jacqueline Archibald
School of Design and Informatics, Abertay University,
Dundee, Scotland
k.renaud,j.archibald@abertay.ac.uk

## ABSTRACT

Over the last decade, the number of small and medium (SME) businesses suffering data breaches has risen at an alarming rate. Knowing how to respond to inevitable data breaches is critically important. A number of guidelines exist to advise organisations on the steps necessary to ensure an effective incident response. These guidelines tend to be unsuitable for SMEs, who generally have limited resources to expend on security and incident responses.

Qualitative interviews were conducted with SMEs to probe current data breach response practice and to gather best-practice advice from SMEs themselves. The interviews revealed no widespread *de facto* approach, with a variety of practices being reported. A number of prevalent unhelpful-practice themes emerged from the responses, which we propose specific mitigation techniques to address.

We therefore propose a SME-specific incident response framework that is simple yet powerful enough to inform and guide SME responses to data breach incidents.

**ACM Reference Format:**
Keshav Kapoor and Karen Renaud & Jacqueline Archibald. 2018. Preparing for GDPR: Helping EU SMEs to Manage Data Breaches. In *Proceedings of (AISB'18).* Liverpool, UK, 8 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

## 1 INTRODUCTION

Cyber security has been identified as one of six Tier 1 threats to national security. It is estimated that it will cost the UK up to £27 bn per year [29]. Annually, it is reported by industry white papers [21, 55] that the number of data breaches is rising [23]. Attacks are also becoming increasingly sophisticated.

Small organisations (SMEs) are not immune to being targeted by hackers [20]. SMEs cannot expect to avoid detection or attacks due to their small size. Indeed, Krebs [35] reports that they are increasingly the prime target. It is essential that they plan for, respond to, recover and learn from hacking attacks [48, p. 131].

On the other hand, it is infeasible for SMEs to follow advice given to larger organisations. Incident response advice is rarely tailored to an organisation's needs, nor does it acknowledge organisation size and resources [17, 41]. A number of general standards and guidelines have been published to inform business incident responses [13, 22, 32, 43] but they are extensive and attempt to cover all bases. For example, the Experian guide to dealing with data breaches [22] has 31 pages and makes frequent reference to "upper management". The Data Breach Response Checklist, published by the US government [43], refers to the role of Human Resources and having a 'response team'. Their advice is also extensive and comprehensive, spanning 8 pages. The ICO data security breach management guide [31] also makes reference to Human Resources and IT teams, and having 'technical' and 'non-technical' staff to assist in the development of recovery plans. These data breach response guides, while certainly exemplary and helpful to large organisations, are not practical for SMEs to follow, especially those at the smaller end in terms of numbers of employees.

The situation for SMEs, at present, is that the consequences of a data breach could be bankruptcy [11]. Yet they are simply not in a position to hire and maintain security staff to take care of this the way big organisations can, nor, in many cases, can they afford to outsource their data breach response.

The European Union's GDPR regulation is coming into force in May 2018 and applies to all organisations regardless of size [16]. This is going to force organisations to contemplate their data breach response strategies [10]. SMEs need simple and clear guidelines for responding and meeting the requirements of the new law. Not doing so could make them go out of business or risk breaking the law.

We carried out research to develop an SME-specific incident response framework that was simple enough for SMEs to follow, yet powerful enough to be fit for purpose. The framework we developed is less comprehensive than the general guidelines published by respected bodies, but still covers the legally mandated aspects of a breach response. Moreover, it has been deliberately simplified for use by a non-expert and/or non-technical SME owner. Elements have been incorporated specifically to address typical panicked reactions such as overly technical and unthinking responses, and to encourage the development and maintenance of an organisational memory to ensure that SMEs develop personal best practice in terms of breach responses.

## 2 BEST PRACTICE INCIDENT RESPONSE

We commenced with a literature review in order to inform the formulation of the interview questions we were going to ask our SME respondents.

Academic literature has seen some focus on incident handling within SMEs [26]. Despite this step in the right direction, concrete research has yet to come up with a widely-agreed SME-specific incident response framework.

Several incident response frameworks and guides have emerged from industry [13, 32], government [28, 40] and academia [38, 44]. American standards bodies, such as NIST [13] and CREST [14], also provide helpful guidance. Most demarcate the following distinct incident response stages:



AISB'18, April 4-6, 2018, Liverpool, UK

**Preparation:** the first step and involves organisations readying themselves for an incident through establishment or preparation of an internal information security incident response team (CSIRT).

**Verification:** 'detection or reporting of security incidents within an organisation' [25, p. 32].

**Containment:** this might involve isolating the systems, changing passwords and disabling accounts, depending on the vulnerability that was exploited.

**Eradication:** organisations seek to eliminate the components of an incident with a focus on the restoration of systems [34] through actions including; identification of affected hosts, conducting malware and forensics analysis.

**Recovery:** taking actions such as: continuous testing and verification coupled with using back-ups to restore systems to normal business operations.

**Follow-up:** activity such as holding a post-incident meeting to explore actions that were taken and considering how effective they were. What could be done differently next time? Answers should feed back into organisational practices through the establishment of new controls, procedures and policies [37, 59]. However, as Jaatun *et al.*'s [33] study of the petroleum industry shows, in practice, challenges often arise which makes learning lessons difficult.

## 3 INTERVIEWING SMES

Ethical approval was sought and granted for interviewing SMEs, see below. We crafted a set of questions to explore SMEs' understanding of data breaches and their extant practice with respect to incident responses. We decided to carry out semi-structured interviews so that we had the flexibility to explore their responses further and elicit valuable insights from them.

We thus commenced with a pre-defined set of questions (see Appendix A) then explored their responses, changing ordering and exploring particular issues they raised [42].

We targeted SMEs, and specifically SME employees who were responsible for Information Security. Participants were recruited via convenience sampling and word-of-mouth. Due to difficulties in recruiting SMEs to participate, we switched to asking them to participate in order to recommend best responses to breaches. This helped us in terms of recruiting, since they were no longer concerned about admitting to being breached themselves.

### 3.1 Carrying out the Interviews

In Summer 2017, we carried out semi-structured interviews with organisations to explore current practice and to gather advice from 11 respondents [30]. We explored three particular topics:

**(1) Understanding:** of what the term "data breach" meant [52, 53],

**(2) Current Practice:** what they currently did with respect to preparing for, and responding to, data breaches [25, 38], and

**(3) Best Practice Advice** what they would advise other organisations like themselves to do with respect to managing data breach incidents (to allow them to feel that they were contributing to compiling 'good practice' for the benefit of other SMEs).

### 3.2 Results

*(1) Data Breach Understanding.* When asked to define the term "data breach", participants used phrases similar to: '*it involves unintended disclosure or access of information*'. Some also highlighted the difference between a security incident and data breach saying '*security incidents are sort of a wider ranging term, for instance you could have an incident with cloud technologies or networks, breaches would kind of be more concerned with data*'.

*(2) Current Practice.*

**Preparation:**

All participants explained that preparation before a data breach was crucial. Only two participants had no formal preparation in place because '*we don't know how and what to plan for.... plus, we have an IT supplier!*' When asked which actions should be prioritised during preparation one explained, '*establishing and preparing; the CISO*' others proposed, '*establishing who to contact*'. Participants who reported to having a CSIRT explained that preparation should focus on '*fully equipping the CSIRT*'.

Participants 11 and 5 outlined the importance of rehearsal stating, '*plans should be war gamed annually*'. Levels of rehearsal varied, with participant 5 explaining that their plan is practiced '*in anger on a daily basis*'. On the other hand, Participant 2 reported '*I don't think the plan is practiced at all!*'. A number of participants reported having plans in place but also admitted that '*we have a plan ... whether we follow that every time (we respond) I am not sure*'.

**Verification:**

All interviewees explained that an immediate first step when responding to breaches is acting on manual and automatic reports. Participant 2 explained '*after the report, the first thing we did was to take steps to verify that it was indeed a data breach*' and Participant 4 said that, they also '*identified [the] nature of the attack by trying to understand the potential impact and damage caused*'.

When asked who should react first to these alerts, those handling externally, such as Participant 3, explained that the external party needs to react first as '*information security incidents are handled, verified and coordinated through an external source*'. Participants handling internally echoed the views of Participant 6 who explained that verification is conducted by '*the person or team most appropriate to respond*'.

Interviewees also explained that during verification, forensic and technical tools were used, with Participant 6 stating '*identify the incident and detect possibly via SIEM tools*'. Some participants explained that once a data breach had been verified, forensic triage was to be completed. At this point Participant 10 added that, '*if you've verified a data breach, identify whether stolen data was encrypted or non-encrypted*'.

**Containment:**

Respondents explained that actions to contain breaches came next, with Participant 9 explaining actions focused on, '*ensuring that the outflow of data has been stemmed*'. Participant 7, further stated '*containment depends on the type of incident that has occurred ... let's say a phishing email came through, you could take some quick steps ... However, with 'WannaCry' we had to take more serious action*'. During containment, common actions included isolation by '*Taking the*

*server offline cut all ties to isolate it from the network.*' '*changing all passwords*'. Participant 10 even mentioned, '*Carry on! Some people will say isolate until you've fixed it — well the answer is, don't*'.

Participants also emphasised the importance of communication which some referred to '*contacting senior management to let them know what had happened … to get their permission to take servers offline.*' and for others referred to getting, '*Legal and PR involved*'. For participant 3, external communication was key as they explained '*we have contractual arrangements with many external suppliers*'. Interviewees also echoed the views of Participant 4 who said, '*dependent on the type of attack, we may have to contact authorities (ICO)*'.

**Recovery:**
Participants described a recovery stage where, similar to Participant 9, actions focused on, '*restoring the integrity of the hacked system*' through the prioritisation of technical actions because as Participant 6 explained, '*technical changes are the quickest to implement for recovery. They may be a blunt instrument to address the problem but may be necessary*'. Participant 5 also suggested if a breach '*results in a loss of system operation, then ideally recovery of systems from a recent backup*'. Meanwhile, Participant 7 pointed out that, '*sometimes recovery from these things can be much bigger*' and others such as Participant 2 even said, '*I have no idea the IT and technical guys took care of the recovery*'.

**Follow-up:**
All interviewees pointed out that learning lessons during the follow up stage and implementing these lessons back into practice after a breach would lead to improvements in the response process and prevent future attacks from happening. Despite this, there was an inconsistent and unreliable execution of lessons learnt in practice. Participant 7, explained that, their organisation prioritised '*continuous application of lessons learnt and proactively apply best practice*'. Others said implementing lessons learnt is difficult because '*events are rapidly forgotten, as business priorities change security concerns drift back towards the bottom of the pile*'.

Participants expressed 'lessons should be learnt through organisational changes including, '*security policy revision*', '*security culture change*', '*user training*' and, '*changing passwords*'. A large number of interviewees also focused on technical changes such as '*changing firewall rules*', '*deploying canary/honeypot devices*'.

*(3) Best Practice Advice*
**Locate assets:**
Interviewees advised that each individual organisation needed to understand what it's 'crown jewels' are by asking questions such as; 'What issues are created by the compromise of data in an organisation?' so that they can use this information '*to potentially work out plans of what to do when people actually come after them*'. Participant 7 provided an example of this and explained, '*if we lost 50 email addresses and phone numbers it's not ideal but may be catastrophic for others. However, if we lost 2 million customer records —- that's catastrophic for us*'.

**Prioritise security:**
Participant 2 expressed views held by others, stating, '*first things first: you need to establish a mind-set where you expect to be breached*'. Interviewees stated that, by so doing, organisations could prioritise security concerns and '*engender a culture of security within the workforce: both at work and within private lives*'.

**Simplify:**
Participant 9 and others advised organisations to, '*boil security down to the simple things*'. Participant 3 gave examples of simple solutions stating, '*ensure the IT you are using is protected by the latest versions of hardware and software —- saving by using old technology is false economy*'.

**People are important:**
Participants said: '*cyber-threats are often seen too narrowly as a technical issue. In fact cyber-security depends on the right approaches to technology, but also personnel*' .

Participants advised, '*It is essential to establish open and clear communication networks with staff, senior management and third parties*'. Others also advised open and constant communication with '*affected customers*', '*external bodies*' and '*external incident handling parties*'.

**Need for Measured Action:**
Respondents explained that it was essential for organisations to document every action. Participant 2 said this was because '*you need to have evidence of all the actions you've taken*'. Participant 6 advised that, to comply with this, '*organisations should have tools in place to gather information, before the incident takes place*'.

Interviewees encouraged organisations to seek external support before a breach from 'The National Cyber Security Centre' and by '*hiring security professionals*'. Others stated that seeking help during the incident was vital in order to contain the breach, with Participant 10 explaining '*if a breach is verified bring in expertise very quickly to act upon the problem*'.

Interviewees urged organisations to '*report breaches of personal data to the ICO and to become aware of important regulation such as The General Data Protection Regulation (GDPR)*' [31].

## 3.3 Limitations

A limitation of this research is that the sample is not large enough to be fully representative of the views of the general population. This is due to the fact that many organisations do not want to speak about such a sensitive topic. Only eleven of the 100+ organisations we contacted were willing to be interviewed. It was only when we switched the focus, from speaking about their own data breach responses, to eliciting advice for others that we were able speak to eleven SMEs. Still, we have to acknowledge this as a limitation and we hope to be able to find a better way to recruit participants in the future.

# 4 REFLECTION

It is clear that the SMEs we spoke to define and interpret data breaches similarly and are aware of what the data breach meant. As a consequence, they could outline which actions needed to be prioritised during the preparation and follow-up stage. Compared to the unawareness reported by Line *et al.* [53] and Tan *et al.* [52],

these results are somewhat unexpected, but gratifying. It could be a consequence of the intervening years having raised the prominence of data breaches in the media. This is further evidenced by the Marsh Report [36, p. 2] which reports that levels of basic or complete organisational understanding of cyber-risk rose from 60.8% in 2015 to 83.8% in 2016.

A number of insights emerged from our interviews, which we highlight here in order to inform our development of a framework to help SMEs to respond to breaches.

***(1) Over-Emphasis on Technical Measures.*** Results from the interviews show that throughout the breach response process organisations displayed a disposition for implementing technical measures over non-technical ones. Moreover, in scenarios where organisations could not execute the measures themselves, technical expertise and solutions were prioritised. These results are unsurprising as they lend weight to the arguments presented by Shedden *et al.* [48] that organisations prioritise the use of technical measures because they believe data breaches are, by definition, a technical problem which demands a technical solution.

One participant said: '*technical changes are the quickest to implement for recovery. They may be a blunt instrument to address the problem but may be necessary.*' There was little reference to staff training or to the role of the human element in improving resilience to future attacks. Only in the follow-up section was this mentioned but this seemed more of a wish list than something that was actually implemented.

Best practice advice also makes a specific recommendation about technical aspects, but says little about awareness training for staff. They refer to a culture of security but don't say how this ought to be achieved.

This confirms reports from other researchers about incident responses appearing to place an unrealistic 'emphasis on technical competence in responding to incidents' [48, p. 133].

***(2) Unthinking Responses.*** The best practice responses highlight the fact that preparation and a realistic expectation of being breached is important, in terms of knowing where assets are, and prioritising security.

Yet, in the responses about extant practice, there was some evidence that people would respond without really checking that the response would address the source of the breach. For example, requiring all staff to change their passwords before it has been confirmed that the attack vector involved a leaked password imposes significant burdens on staff without necessarily addressing the source of the breach.

The SMEs find it difficult to execute what they propose in theory throughout the entire data breach event. For example, during the preparation and follow up stages, organisations outline the importance of having plans in place and of learning lessons. However, in reality, organisations reported not using or ignoring existing plans during a breach and found learning lessons difficult after because of: a lack of expertise, lack of resources and skills to implement ideas in practice. This resulted in actions being designated to more skilled individuals, and the organisation's failure to prioritise cyber-security.

These results confirm research by Hove *et al.* [30] and Jaatun *et al.* [33] who found that organisations have incident response plans in place but that, in practice, these procedures were not well established. However, whilst current studies outline how organisations experience difficulties implementing theory into practice during each individual step of incident response, this research confirms that these trends are still evident throughout the entire breach response process.

This all points to a hasty and unmeasured response to data breaches, which means SMEs run the risk of carrying out the wrong actions and not dealing appropriately with breaches. Ineffective responses can have negative consequences. A prime example is UK telecoms company TalkTalk which lost an estimated 157000 customers' personal data [19]. The BBC reports that breaches at TalkTalk have cost the company up to £35 million in damages [8].

***(3) Lessons are not Learned.*** Our interviews revealed an inconsistent and unreliable execution of lessons learnt. Some participants were indeed aware of the value of such an activity but pointed out the difficulties of doing this in the general melee of business life.

Researchers have highlighted the importance of a follow-up stage where lessons are learned to be commonplace within organisations [37, 59]. However, as Jaatun *et al.*'s [33] study of the petroleum industry shows, and we confirm, in practice challenges often arise that makes learning lessons difficult, and this deters their ability to respond to future incidents more effectively [3, p. 651].

## 5 MITIGATIONS

In proposing the mitigations we were mindful of the fact that SMEs have limited resources. In a more resource-rich organisation, these problems could be solved by hiring extra staff, or by contracting an external company to deal with any breaches that do occur. SMEs often do not have the luxury of these solutions. Hence we proposed mitigations here that would not require major expense and would essentially simplify the process. The main aim was to make it more manageable for solo responders who were not necessarily information security experts.

***(1) Over-Emphasis on Technical Responses.*** Organisations believe that paying more attention to the human element i.e. having the right people in place before the breach, and working with individuals after the breach, is vitally important. These findings are interesting because, in practice, organisations prioritised technical measures, but when giving best practice advice there was an emphasis on prioritising measures addressing users. These findings lend support to research by Adams and Sasse [1] which promoted focus on the increasing importance of human elements within cyber-security research.

Incident response has to be holistic, addressing technical, managerial, legal and human aspects of information security [18]. The emphasis on technical responses is probably due to a measure of panic. Incident response is a stressful experience and Von Lubitz *et al.* [56] explain that, 'stress has a demonstrable negative effect on human information processing and interactions with chaotic environments'.

In helping SMEs to mitigate this tendency we are suggesting the use of checklists, commonly used in the medical field. Checklists providing easy-to-follow instructions to manage complex processes

[24, p. 120]. This technique, we believe, will be useful because the medical environment is also stressful and checklists might well benefit information security as much as it has been shown to benefit medical procedures by preventing omissions and thereby saving lives.

Gawande [24, p. 49] argues that checklists are an effective tool in these kinds of situations because they 'do not try to spell out everything' but instead act as a guide by providing reminders of only 'the most critical and important steps' [24, p. 120].

The Alien Vault's incident response guide [5, p. 21] argues that emergency contact checklists are valuable for maintaining communication with all the relevant stakeholders. Furthermore, checklists can also help maintain a paper trail during the breach because [34].

For SMEs, having checklists that encode essential incident response plans in an easy-to-process format constitutes an inexpensive way to provide valuable, structured and easy-to-understand guidance. This 'can prove highly beneficial as they can help ensure that personnel take prompt, consistent and holistic action under less than ideal conditions' [39]. The core plans that need to be encoded into checklists are [2, 49]: (1) Disaster Recovery Plan, (2) Crisis Communication Plan, and (3) Business Continuity Plan.

***(2) Unthinking Responses.*** When an organisation has been breached, both 'co-ordination and timing' become serious concerns [24, p. 49]. To mitigate this, John Boyd's OODA loop, used extensively in the military, can prove beneficial because it 'provides the essential framework for knowledge-based multidimensional critical thinking and rapid decision-making' [56].

OODA has four stages: *Observe, Orient, Decide, Act*. **Observe** refers to actively absorbing the entire environment and changes that 'identify anomalous behaviour that may require investigation' [5, p. 18]. In the context of data breach response, responders will ask themselves key questions such as; 'What's normal activity on my network?' the better to understand the attack [46].

**Orient** is when information and knowledge gathered during *Observe* is broken down and assessed to introduce 'the first steps needed to re-organise it into the pre-disaster configuration' [56, p. 571].

The third stage is **Decide**, which refers to the responder defining 'the nature and characteristics of the action(s) to be taken' [56, p. 343]. In the context of incident response, responders assess different options obtained during the orientation stage to hypothesise the best course of action which ensures the 'fastest recovery' [5, p. 19].

The fourth stage is **Act** and refers to testing the proposed hypothesis made in the previous stage, to remediate and recover [5, p. 20] back online. The Act section is not the final part of the loop because the feedback from the action taken will form the basis of the next cycle of the loop.

For SMEs, using the OODA loop when responding to data breaches requires them to observe first, then orient and decide before they act. This, together with the checklists, ought to ensure a measured and more effective response to the breach.

***(3) Lessons are not Learned.*** Current incident response frameworks, both in industry and academia [13, 53], perceive incident response cyclically i.e. a feedback-enabled lessons-learned loop feeding into the next incident response in order to improve the effectiveness of the responses.

The best way to do this is firstly to maintain a "lessons learned" database. The *lessons learned, or known errors, database* is a commonly used measure in organisations [54]. Sharif *et al.* [47] argue that it is critical for tacit knowledge be shared within organisations. In the context of incident response, the SME-specific incident response framework needs deliberately to incorporate a feedback loop, as originally proposed by Beer [9], to keep such a database current and helpful.

Other researchers in information security have argued for the need to learn lessons from data breach incident responses [3, 12, 27, 45]. Making such a feedback loop explicit in the framework will help to remind SMEs of the need to examine and learn from incident responses after the event.

This loop, together with the use of checklists to encode essential actions, make it easier to incorporate lessons learned into a simple, usable, and systematic form [24].

## 6 AN SME-SPECIFIC INCIDENT RESPONSE FRAMEWORK

SMEs need to develop a mind-set whereby a breach is expected at any time, and plan accordingly. The framework we suggest here incorporates the essential requirements of the GDPR, incorporated into checklists, and moderated by applying OODA instead of leaping in, in a panic.

Those actions that are required by **GDPR** are marked as such. The other items have been added specifically to help SMEs, mitigating their resource limitations. Although they have been marked as **SME-Specific** they would be helpful for large organisations too, but might not be necessary

### Before the Breach

- *GDPR — Identify Business-Critical Resources and Sensitive Information:* Identify the 'crown jewels' (business-critical systems and personal customer information) to establish which areas need focused attention.
- *GDPR — Be Aware of Regulations:* The new GDPR regulations have to be complied with. Organisations have to ensure that they are aware of their responsibilities before any incident occurs. SMEs must familiarise themselves with the relevant notification regulations.
- ***SME-Specific** — Seek External Advice & Support:* Seek external support and knowledge from government initiatives and freely available advice guides. Boil security down to the simplest things. For example, implement the H.M Government 'Cyber Essentials' as a starting point [15].
- *GDPR — Assign Response Roles:* Decide if it is beneficial for cyber-security matters to be handled in-house or externally. By doing this, roles and responsibilities are clearly defined.
- ***SME-Specific** — Develop Checklists to guide Incident Response:* Compile checklists to help responders recall essential information regarding organisational processes. It is vital that three plans are encoded into checklists [2, 49]: (1) Disaster Recovery Plan, (2) Crisis Communication Plan, and (3) Business Continuity Plan.
- *GDPR — Carry out Security Awareness Training:* The employees of an organisation are an essential link in the information

security chain. Conducting regular awareness training is the only way to increase their resilience.

### During the Breach Response

- ***SME-Specific*** *— (OODA) Observe, Orient, Decide, then Act:* ***First***, *Observe:* Responders gather information from the incident environment. ***Second***, *Orient:* Responders use information gathered to prioritise response actions. ***Third***, *Decide:* Responders use knowledge to hypothesise the best course of action to effectively respond to a breach. ***Finally***, *Follow the Disaster Recovery Plan:* Now, follow the checklist developed during the preparation phase.
- *GDPR — Document all Actions, with Timeline:* Checklists should be used to prompt responders regarding key processes and also to document every action taken. A paper trail is crucial.
- *GDPR — Report the Breach to the Supervisory Authority:* This must be done within 72 hours.
- *GDPR — Follow the Crisis Communication Plan:* Maintain communication with important internal stakeholders, regardless of whether the breach is being handled internally or externally. Employees are also stakeholders [7].
- ***SME-Specific*** *— Summon External Incident Response Support if Required:* If a breach is being handled internally and overwhelms resources use emergency external professional support.

### After the Breach Response

- *GDPR — Reflect on Lessons Learned:* Irrespective of internal or external handling of breaches, evaluate the experience and ask questions such as: "What could be done better?"
- *GDPR — Feed Lessons back into Checklists:* Transform the main takeaways from the evaluation to refine the: (1) Disaster Recovery Plan, (2) Crisis Communication Plan, and (3) Business Continuity Plan.
- *GDPR — Boost Security Awareness:* Use the breach to boost security awareness and encourage individuals to learn lessons proactively through open forums.
- ***SME-Specific*** *— Do not Neglect the Humans:* Security is not just about technical measures. Work with and educate employees across the organisation regarding security using free advice e.g. H.M Government 'Cyber Essentials'.

## 6.1 Expert Review Feedback

Following ethical approval, see below, we sent the previous list of recommendations to four security experts. We asked them for feedback so that we could refine the recommendations

(1) '*I love where you are going with this. You need to get organisations into a state of preparedness by asking: Is it important to your business if someone can get into your computer and steal your customer information?*

(2) *'These are implementable, and scalable, you could strengthen them further by encouraging organisations to devote some effort to situational awareness – Is somebody responsible for understanding what sorts of threats are out there? The recent NHS malware incident is, a good example. Did the average organisation cotton on to that, and take precautionary steps?'*

(3) *'There is very little improvement, just more expansion is needed. The term 'crown jewels' refers to any business-critical systems the organisation relies on that would have a significant detrimental impact should they be unavailable. Look at other regulation such as: The NIS Directive and PECR.* Organisations should seek to incorporate lessons learnt into the organisation's security awareness programmes, for key incidents such as WannaCry, conduct 'ask me anything' type awareness-raising sessions allowing employees to understand more about these types of incident.

(4) *'It looks good, you could put a bit about policies and feeding lessons learned back into policy'*

Based on this feedback, the final incident response framework is presented in Figure 1, and Figure 2.

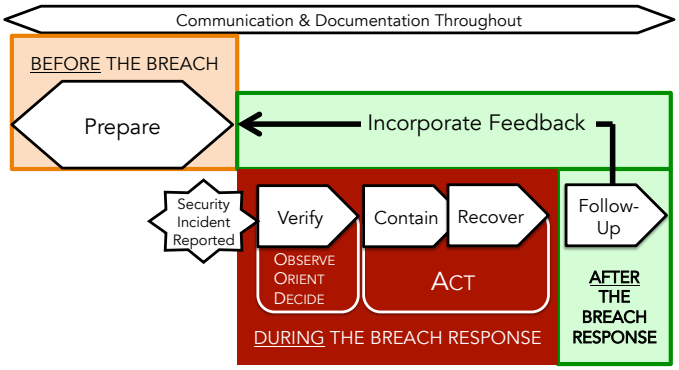


**Figure 1: Final Incident Response Plan**

## 7 DISCUSSION

The SMEs who participated in our study were well aware of data breaches, an improvement since 2003 [52]. Many were also aware of the fact that they ought to have some kind of plan in place to deal with any data breaches that did occur.

There was no broad agreement with respect to what the response to incidents ought to be. For example, during Containment, organisations discussed a variety of different actions with some suggesting isolating systems and others disagreeing with this approach. This confirms Grispos [25] assertions about the variability of incident responses. Morever, despite a general awareness that something ought to be done, and plans to lay down what the reaction should be, it did not seem that they tested or followed their plans when the need arose. This disconnect between awareness and action has already been commented on by other researchers [4].

We identified three particular themes that seemed to be getting in the way of SMEs responding as effectively as possible to data breaches, quite apart from their size and limited resources.

The *first*, an over-emphasis on technical security measures, was raised by Von Solms and Von Solms [57] in 2004, more than a decade ago and confirmed by [3]. It is disappointing to find that this kind of myopic focus is still prevalent in industry in 2017, when an increasing focus on the human's role in information security is becoming accepted by industry [1, 6, 51].

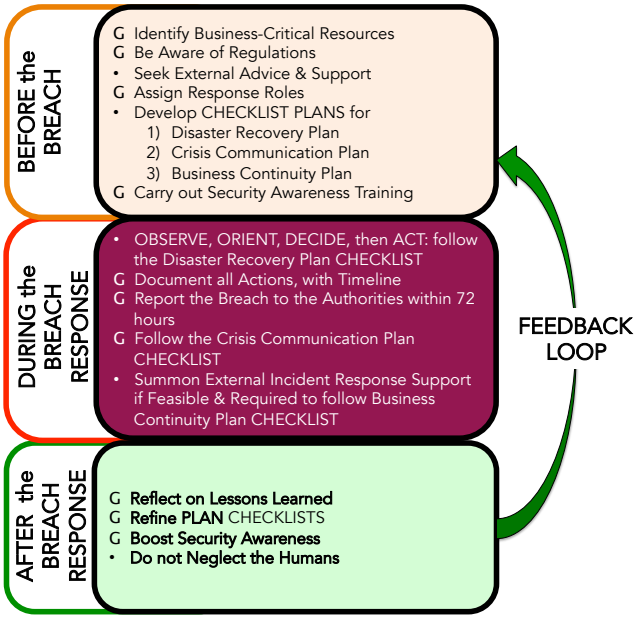


**Figure 2: SME-Specific Incident Response Framework (G=GDPR-Required Response)**

The *second* problem is that organizations struggle to respond in a measured way. In our discussions with participants about containment it was obvious that they did not really respond in a consistent way. This is understandable because people are going to be stressed by the event [50, 58].

The *third* problem is that SMEs did not seem to have a mechanism for learning lessons from previous data breach events and responses.

The framework we propose specifically addresses each of these problems, using techniques that have proven successful in other disciplines: checklists (medicine) [24], OODA (the USA Military) [56] and an institutional lessons-learned archive resource (business knowledge management) [47, 54].

## 8 CONCLUSION

This paper set out to propose a feasible yet helpful framework to inform SME incident responses to data breach responses. We carried out a series of semi-structured interviews in order to inform the development of this data breach response framework. This SME-specific framework is different from others because it incorporates successful techniques from medicine (checklists) and the military (OODA), and explicitly incorporates a feedback loop to ensure that lessons are learned over the lifetime of an organisation. It is also relatively simple and not as heavy-weight as other best practice recommendations aimed at more resource-rich organisations.

This framework is not intended to be the final version. It clearly needs to be used "in anger" by SMEs and refined and improved based on their experiences. We present it here in order to gain feedback from other researchers. We hope to find SMEs who are willing to trial the framework and we hope thereby to refine it until it starts becoming a helpful resource. We believe that our deployment of proven techniques from other disciplines will prove helpful in incident responses too.

Our long-term aim is to support SMEs more effectively in coping with data breaches in the face of the coming GDPR legislation.

## ETHICS

Ethical concerns centred on the need to maintain the anonymity of interviewees and the confidentiality of information they revealed. To address this plain language statements and consent forms were given to participants and offered participants anonymity and confidentiality. The ethics form was reviewed on 20 June 2017 (Application number: SP S/2017 SOCIAL SCIENCE/859) and approved subject to minor amendments which were adhered to.

## REFERENCES

[1] Anne Adams and Martina Angela Sasse. 1999. Users are not the enemy. *Commun. ACM* 42, 12 (1999), 40–46.
[2] Steve Adubato. 2008. *What were they thinking?: Crisis communication: the good, the bad, and the totally clueless.* Rutgers University Press.
[3] Atif Ahmad, Justin Hadgkiss, and Anthonie B Ruighaver. 2012. Incident response teams–Challenges in supporting the organisational security function. *Computers & Security* 31, 5 (2012), 643–652.
[4] Eirik Albrechtsen. 2007. A qualitative study of users' view on information security. *Computers & Security* 26, 4 (2007), 276–289.
[5] Alien Vault. 2017. Insider's Guide to Incident Response – Expert Tips. (2017). https://www.alienvault.com/resource-center/ebook/insider-guide-to-incident-response (Accessed on: 18/05/2017).
[6] Debi Ashenden. 2008. Information security management: A human challenge? *Information Security Technical Report* 13, 4 (2008), 195–201.
[7] Debi Ashenden and Angela Sasse. 2013. CISOs and organisational culture: Their own worst enemy? *Computers & Security* 39 (2013), 396–405.
[8] BBC. 2015. TalkTalk hack to cost up to £35m. (2015). http://www.bbc.co.uk/news/uk-34784980 (Accessed on: 14/07/2017).
[9] Randall D Beer. 2000. Dynamical approaches to cognitive science. *Trends in Cognitive Sciences* 4, 3 (2000), 91–99.
[10] C Rustici. 2016. Don't think that Brexit will save you from the EU data protection rules. (2016). http://www.computerweekly.com/opinion/Dont-think-that-Brexit-will-save-you-from-the-EU-data-protection-rules (Accessed on: 23/08/2017).
[11] Cabinet Office. 2015. Cyber security 'myths' putting a third of SME revenue at risk. (2015). https://www.gov.uk/government/news/cyber-security-myths-putting-a-third-of-sme-revenue-at-risk (Accessed on: 15/07/2017).
[12] Julia S Cheney. 2010. Heartland Payment Systems: lessons learned from a data breach. (2010). FRB of Philadelphia - Payment Cards Center Discussion Paper No. 10-1 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1540143.
[13] Paul Cichonski, Tom Millar, Tim Grance, and Karen Scarfone. 2012. Computer security incident handling guide. *NIST Special Publication* 800 (2012), 61.
[14] CREST. 2017. Cyber Security Incident Response Guide. (2017). https://www.crest-approved.org/wp-content/uploads/2014/11/CSIR-Procurement-Guide.pdf (Accessed on 26/05/2017).
[15] Cyber Essentials. 2018. (2018). https://www.cyberessentials.ncsc.gov.uk/ Accessed 20 February 2018.
[16] Deloitte. 2016. Incident Response: We've had a privacy breach – now what? (2016). https://www2.deloitte.com/content/dam/Deloitte/za/Documents/risk/ZA_CIC_Incident_Response_09062016.pdf (Accessed on: 23/08/2017).
[17] Department for Digital, Culture, Media and Sport. 2016. Cyber Security breaches survey. (2016). Available at: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2017 (Accessed on: 06/05/2017).
[18] Sneza Dojkovski, Sharman Lichtenstein, and Matthew Warren. 2006. Challenges in fostering an information security culture in Australian small and medium sized enterprises. In *ECIW2006: proceedings of the 5th European conference on Information Warfare and Security.* Academic Conferences Limited, 31–40.
[19] Experian. 2015. Nearly 157,000 had data breached in TalkTalk cyber-attack. (2015). https://www.theguardian.com/business/2015/nov/06/nearly-157000-had-data-breached-in-talktalk-cyber-attack (Accessed on: 14/07/2017).
[20] Experian. 2016. SMEs under threat - The crippling consequences for unprepared small to medium sized businesses. (2016). http://www.experian.co.uk/assets/identity-and-fraud/smes-under-threat.pdf (Accessed on: 26/06/2017).
[21] Experian. 2017. Fourth annual 2017 Data Breach Industry Forecast. (2017). http://www.experian.com/assets/data-breach/white-papers/2017-experian-data-breach-industry-forecast.pdf (Accessed on: 16/07/2017).

[22] Experian Data Breach Resolution. 2014. Data Breach Response Guide. (2014). http://www.verizonenterprise.com/products/security/incident-response/ Accessed 27/12/2017.
[23] Kevvie Fowler. 2016. *Data Breach Preparation and Response: Breaches are Certain, Impact is Not.* Syngress, Cambridge, MA.
[24] Atul Gawande. 2011. *The Checklist Maniufesto.* Profile, London.
[25] George Grispos. 2016. *On the enhancement of data quality in security incident response investigations.* Ph.D. Dissertation. University of Glasgow.
[26] Alexander Harsch, Steffen Idler, and Simon Thurner. 2014. Assuming a state of compromise: A best practise approach for SMEs on incident response management. In *IT Security Incident Management & IT Forensics (IMF), 2014 Eighth International Conference on.* IEEE, 76–84.
[27] Ying He, Chris Johnson, Karen Renaud, Yu Lu, and Salem Jebriel. 2014. An empirical study on the use of the generic security template for structuring the lessons from information security incidents. In *Computer Science and Information Technology (CSIT), 2014 6th International Conference on.* IEEE, 178–188.
[28] H.M. Government. 2015. Cyber security: advice for small businesses. (2015). https://www.gov.uk/government/publications/cyber-security-what-small-businesses-need-to-know Accessed 3/1/2018.
[29] Houses of Parliament. 2017. Cyber Security of UK Infrastructure. (2017). Number 554, May. http://researchbriefings.files.parliament.uk/documents/POST-PN-0554/POST-PN-0554.pdf.
[30] Cathrine Hove, Marte Tarnes, Maria B Line, and Karin Bernsmed. 2014. Information security incident management: identified practice in large organizations. In *IT Security Incident Management & IT Forensics (IMF), 2014 Eighth International Conference on.* IEEE, 27–46.
[31] Information Commissioner's Office. 2017. Data security incident trends. (2017). https://ico.org.uk/action-weve-taken/data-security-incident-trends/ (Accessed on: 16/07/2017).
[32] International Standards Organisations. 2011. ISO/ IEC 27035, Information technology – Security techniques – Information security incident management. (2011). https://www.iso.org/standard/44379.html (Accessed on: 05/07/2017).
[33] Martin Gilje Jaatun, Eirik Albrechtsen, Maria B Line, Inger Anne Tøndel, and Odd Helge Longva. 2009. A framework for incident response management in the petroleum industry. *International Journal of Critical Infrastructure Protection* 2, 1 (2009), 26–37.
[34] Patrick Kral. 2011. SANS Institute The Incident Handlers Handbook. (2011). https://uk.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901 (Accessed on: 05/07/2017).
[35] Brian Krebs. 2017. 4 Years After Target, the Little Guy is the Target. (2017). 17 Dec https://krebsonsecurity.com/2017/12/4-years-after-target-the-little-guy-is-the-target/.
[36] Marsh. 2017. UK Cyber Risk Survey Report: 2016. (2017). https://www.marsh.com/content/dam/marsh/Documents/PDF/UK-en/UK%20Cyber%20Risk%20Survey%20Report%202016.pdf (Accessed on: 04/09/2017).
[37] Stefan Metzger, Wolfgang Hommel, and Helmut Reiser. 2011. Integrated Security Incident Management–Concepts and Real-World Experiences. In *IT Security Incident Management and IT Forensics (IMF), 2011 Sixth International Conference On.* IEEE, 107–121.
[38] Sarandis Mitropoulos, Dimitrios Patsos, and Christos Douligeris. 2006. On Incident Handling and Response: A state-of-the-art approach. *Computers & Security* 25, 5 (2006), 351–370.
[39] Emilio F Moran. 2016. *People and Nature: An Introduction to Human Ecological Relations.* Vol. 1. John Wiley & Sons.
[40] NCSC. 2017. Cyber Security: Small Business Guide. (2017). https://www.ncsc.gov.uk/smallbusiness Accessed 3/1/2018.
[41] NCSC. 2017. Professional service scheme Cyber Incidents. (2017). https://www.ncsc.gov.uk/scheme/cyber-incidents Accessed 3/1/2018.
[42] Briony J Oates. 2005. *Researching Information Systems and Computing.* Sage, London.
[43] Privacy Technical Assistance Centre. 2012. Data Breach Response Checklist. (2012). http://ptac.ed.gov/sites/default/files/checklist_data_breach_response_092012.pdf Accessed 17/12/2017.
[44] Chris Prosise, Kevin Mandia, and Matt Pepe. 2003. *Incident Response & Computer Forensics.* McGraw-Hill/Osborne New York.
[45] Karen Scarfone, Tim Grance, and Kelly Masone. 2008. Computer security incident handling guide. *NIST Special Publication* 800, 61 (2008), 38.
[46] Bruce Schneier. 2014. The future of incident response. *IEEE Security & Privacy* 12, 5 (2014), 96–96.
[47] Mohammad Nazir Ahmad Sharif, Nor Hidayati Zakaria, Lim Shu Ching, and Low Soh Fung. 2005. Facilitating knowledge sharing through lessons learned system. *Journal of Knowledge Management Practice* 12 (2005), 117–124.
[48] Piya Shedden, Atif Ahmad, and AB Ruighaver. 2010. *Organisational learning and incident response: promoting effective learning through the incident response process.* School of Computer and Information Science, Edith Cowan University, Perth, Western Australia.
[49] Susan Snedaker. 2013. *Business Continuity and Disaster Recovery Planning for IT Professionals.* Newnes, Amsterdam.
[50] Daniel J Solove and Danielle Citron. 2017. Risk and Anxiety: A Theory of Data Breach Harms. (2017). https://scholarship.law.gwu.edu/faculty_publications/1244/.
[51] Zahoor Ahmed Soomro, Mahmood Hussain Shah, and Javed Ahmed. 2016. Information security management needs more holistic approach: A literature review. *International Journal of Information Management* 36, 2 (2016), 215–225.
[52] Terence Tan, AB Ruighaver, and Atif Ahmad. 2003. Incident Handling: Where the need for planning is often not recognised. In *1st Australian Computer, Network & Information Forensics Conference.*
[53] Inger Anne Tøndel, Maria B Line, and Martin Gilje Jaatun. 2014. Information security incident management: Current practice as reported in the literature. *Computers & Security* 45 (2014), 42–57.
[54] Gertjan Van Heijst, Rob van der Spek, and Eelco Kruizinga. 1998. The lessons learned cycle. In *Information Technology for Knowledge Management.* Springer, 17–34.
[55] Verizon. 2017. Data Breach Digest. (2017). http://www.verizonenterprise.com/resources/reports/rp_data-breach-digest-2017-perspective-is-reality_xg_en.pdf (Accessed on: 16/07/2017).
[56] Dag Von Lubitz and Nilmini Wickramasinghe. 2006. Dynamic leadership in unstable and unpredictable environments. *International Journal of Management and Enterprise Development* 3, 4 (2006), 339–350.
[57] Basie Von Solms and Rossouw Von Solms. 2004. The 10 deadly sins of information security management. *Computers & Security* 23, 5 (2004), 371–376.
[58] Bryan Watkins. 2014. The impact of cyber attacks on the private sector. *Briefing Paper, Association for International Affair* (2014), 12.
[59] Rodrigo Werlinger, Kasia Muldner, Kirstie Hawkey, and Konstantin Beznosov. 2010. Preparation, detection, and analysis: the diagnostic work of IT security incident response. *Information Management & Computer Security* 18, 1 (2010), 26–42.

# 9 APPENDIX A

1. What company do you work for? (if you prefer not to be identified then anonymity will be respected)
2. What is your role in the company?
3. What does the term data breach mean to you?
4. Have you had any security breaches within your organisation? (if you prefer not answer then skip to question 6)
a. If yes, can you describe the breach? (i.e. DDOS) ….
b. How did you detect the breach? – what methods were used? (automatic or manual?)
c. How did you follow up the event, was the breach investigated? If so
d. Does your organisation have an incident response plan to use in case you get hacked?
If you have a plan –is it rehearsed,
If yes, how often, and what sort of vulnerabilities does it cover?)

5. Do you have a CSIRT team –
If yes, how does the team prepare?
if no team or plan – then why not?
6. Say you experience a hacking event. Could you say how you think you should respond?
7. Who should react first?
8. What actions should be taken to recover from the breach?
9. What actions should be prioritised?

**What General Advice would you give to other companies?**

1. What would be your top three incident response tips for an organisation that has suffered a breach?
2. How would you simplify the process of incident response?
3. How should lessons be learnt?
4. How could we ensure that companies can learn from attacks?
5. How do you think events could change security attitudes within your organisation?
6. How important do you think preparation and having a pre-determined plan is in terms of being able to deal with a breach?