Digital Investigation 12 (2015) S111–S120

Contents lists available at ScienceDirect

Digital Investigation

journal homepage: www.elsevier.com/locate/diin

DFRWS 2015 Europe

Designing robustness and resilience in digital investigation laboratories

Philipp Amann [a, *], Joshua I. James [b]

[a] European Cybercrime Centre (EC3), Europol, P.O. Box 908 50, 2509 LW, The Hague, The Netherlands
[b] Digital Forensic Investigation and Research Laboratory, SoonChunHyang University, Asan, South Korea

Keywords:
Digital investigation capacity
Process robustness and resilience
Laboratory management
Digital forensic standardisation

A B S T R A C T

This work addresses the definition and identification of key elements of robustness and resilience in the context of sustainable digital investigation capacity. After a review of prior work, we describe the results of a structured questionnaire that was sent to 72 law enforcement agencies and subject-matter experts in both online and oral formats (app. response rate 29%). Based on an in-depth analysis of the feedback received, key elements for robustness and resilience of digital investigation capacity are identified and discussed at the strategic and operational levels, including Digital Forensics Strategy, Forensic Discipline, Standardisation, Continuous Education and Training, Research and Development, Co-operation, and Human Resources.

Introduction

In law enforcement organisations the role of robustness and resilience has received little attention in regards to establishing, maintaining and adapting digital forensic capabilities in the face of high staff turnover, complex and changing requirements, and technological advancements. Consequently, and as pointed out in (Braes and Brooks, 2011) for resilience in general, there is no clear definition of the essential concepts. Without a clear understanding of what it is for law enforcement organisations – and digital forensic laboratories in particular – to be robust and resilient, it becomes difficult to plan for and implement an organisation that is effective over the long term.

Conceptually, law enforcement agencies are organisations that can be defined as complex and dynamic systems. It is therefore essential to recognise and understand these dynamics and complexity in the context of organisational resilience and robustness (Burnard and Bhamra, 2011).

(Burnard and Bhamra, 2011) propose a conceptual framework (Fig. 1) that defines the key components of organisational resilience. The framework focuses specifically on detection and activation as a critical component within the response of an organisation to **disruptive events**. Burnard and Bhamra developed the framework from a collection of interrelated propositions, including that:

- resilience is a multidisciplinary and multifaceted concept,
- there is a variety of responses to disruptions and discontinuities,
- it is possible to create bounds for organisational systems i.e. organisational systems can be in a number of different states or (desirable) configurations, and,
- a higher level of thinking is required to develop adaptive systems capable of a resilient response.

In Sutcliffe and Vogus (2003) organisational resilience is based on the processes, resources and structures supporting an organisation's capability to restore efficacy; its ability to effectively process environmental feedback and

* Corresponding author.
E-mail addresses: philipp.amann@europol.europa.eu (P. Amann), Joshua@cybercrimetech.com (J.I. James).

http://dx.doi.org/10.1016/j.diin.2015.01.015

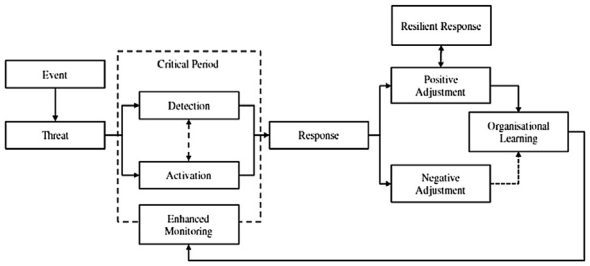

Fig. 1. Resilient Response Framework, K. Burnard and R. Bhamra, "Organisational resilience: development of a conceptual framework for organisational responses", International Journal of Production Research, 2011, vol. 49(18).

flexibly rearrange and transfer knowledge and resources to overcome a given disruptive event. The focus is therefore on resilience as a set of organisational capabilities to mediate and overcome major disruptions. This is similar to (Vogus and Sutcliffe, 2007; Burnard and Bhamra, 2011) who recognise the importance of having a pro-active rather than a reactive approach to organisational resilience. Adaptive capacities through threat analysis, monitoring a system's deviation from the norm and risk management are seen as some of the key concepts for being resilient.

Mafabi et al. (2012) argue that Knowledge Management (KM) leads to innovation and, ultimately, organisational resilience. The study conducted by the authors indeed shows that the relationship between knowledge management and organisational resilience is positive and significant. As knowledge encompasses intangible assets, operational routines, and creative processes that are hard to imitate (Wasko and Faraj, 2005), it is seen as a key resource for organisational growth and sustained competitive advantage, especially for organisations competing in uncertain environments (Gottschalk, 2010). As such, it is also a valuable resource for and an important component of organisational resilience (Mafabi et al., 2012). (Gottschalk, 2007, 2010) submits that KM also plays a key strategic role in international and non-for-profit organisations such as the World Bank or the International Atomic Energy Agency (IAEA) and, increasingly, in the public sector and law enforcement. These roles relate to decision making, enhanced continuity of the organisation, development of core competencies and new business opportunities, reduced risk, and improved responsiveness (Anand and Singh, 2011).

The importance of KM for law enforcement is discussed in detail in (Gottschalk, 2007; Hinduja, 2007), arguing that the strategic management of organisational knowledge is a crucial element of policing. In (Gottschalk, 2010) special focus is given to KM and combating cybercrime. The author argues that an organisations dynamic or adaptive capabilities relate to dynamic knowledge management and help drive strategy into action. This is achieved through organisational and operational structures, different complementary mechanisms such as leadership fora as well as metrics and performance indicators.

It can thus be argued that organisational resilience and robustness, supported by knowledge management, are key concepts for Law Enforcement in addressing the dynamic nature of cybercrime. However, few works looked at the challenge of long-term robustness and resilience of digital investigation capacity.

While the concept of organisational resilience is linked to a number of different domains, including for instance risk management, quality management or environmental scanning (Braes and Brooks, 2011), (Gottschalk, 2007, 2010; Sambamurthy and Subramani, 2005) contend that the domain of knowledge management is of specific relevance to the work of law enforcement in general, and to the concept of resilience and robustness in digital investigations in particular (Chang and Chung, 2014; Seba and Rowley, 2010).

As such, this work intends to survey and evaluate the current state of digital investigations frameworks among EU law enforcement agencies. A structured questionnaire was developed and sent to 72 law enforcement agencies and subject-matter experts of which 21 responses were received. A description and evaluation of the results will be given.

The second focus is on international environments, using the International Criminal Court (ICC), and more specifically the Office of the Prosecutor (OTP), as a practical example. A slightly modified questionnaire was discussed with key staff at the OTP. Analysis of these results will also be given.

Contribution

This work contributes to the field of digital forensic investigation by identifying and defining key elements of robustness and resilience in the context of sustainable digital investigation capacity. The main focus is on surveying and analysing the current state of robustness and resilience practices that have been implemented in organisations with digital investigation capabilities. The results will be used to extract key elements of robustness and resilience, and describe how to include robustness and resilience when designing digital investigation capabilities in the context of an integrated digital investigations framework.

Robustness and resilience

Generally speaking, digital forensics is about the collection and investigation of electronic evidence stored on digital devices. It is a branch of forensic science that involves a wide range of tools and techniques and requires specialised knowledge and expertise.

(Agarwal et al., 2011) define digital forensics as the use of scientific methods towards the preservation, collection, validation, identification, analysis, interpretation and presentation of digital evidence to investigate and establish facts in criminal or civil courts of law, or to be used in an internal corporate investigation.

Digital forensic examiners are involved in some or all steps of the digital forensics process. They often specialise in one area of digital evidence such as mobile phone forensics, computer forensics, network forensics, or image analysis. Digital forensic examiners may gather or process evidence at crime scenes, including conducting live data forensics.

Digital forensic investigators investigate different types of crimes, including cybercrime. They may handle digital evidence during an investigation but they are investigators rather than digital forensics experts. The main focus of digital forensic investigations is on recovering objective evidence of a criminal activity to be presented in a court of law or to be used in an internal corporate investigation. This involves, among other things, the identification and authentication of documents, sources and suspects. Moreover, it may involve identifying potentially exonerating evidence.

Resilience – and, more specifically, *organisational resilience* – can be defined as the long-term capacity of an organisation to adapt to change and new risk environments, and develop yet remain within certain thresholds. It is seen as a multifaceted and multidisciplinary domain that provides, among other things, a certain level of robustness. It is argued that within organisations, resilience resides in the individual and organisational responses to disrupting events. This involves both the ability to withstand discontinuities as well as the capability to adapt to changing environments (Braes and Brooks, 2011; Burnard and Bhamra, 2011; Burnard et al., 2012).

Following (Vogus and Sutcliffe, 2007), the authors interpret resilience not just as an approach to addressing unexpected events but also as a practice that aims at actively monitoring relevant factors and managing any deviations from norms or a stable state. Therefore, monitoring, situational awareness and forward looking analysis play a vital role in organisational resilience.

While usually covered in the literature as part of organisational resilience, for the purpose of this work *robustness*, or the ability of a system to resist change, is kept as a separate attribute. The idea behind this separation is to highlight the importance for law enforcement in particular to ensure that the basic principles of police work, for instance in the way that electronic evidence is being handled, are maintained while adapting to a changing environment.

It is argued that combining these two characteristics should allow for an integrated digital investigation framework design that can *withstand changes but has the ability to adapt to changing requirements within controlled boundaries*. Current digital investigation frameworks focus on the core processes of digital investigation, offering only limited regard for resilience and robustness.

Digital forensics and relevant frameworks

(James and Gladyshev, 2010) conducted an international survey on digital investigation process and accuracy with a view to determining the state of digital investigations, the process of examination and how those examinations were being verified as accurate. The results showed that nearly 60% percent of the 32 respondents follow Standard Operating Procedures that were developed in-house, indicating that there is a considerable amount of duplicated effort worldwide.

Further, a number of different digital forensic frameworks have been proposed in the literature, for example, (Ieong, 2006) introduces a digital forensics investigation framework – FORZA – that as part of its design includes roles for legal advisors and prosecutors. FORZA outlines eight different roles and their responsibilities during the investigation process, including the case leader, the system/business owner, the legal advisor, security/system architect/auditor, digital forensics specialist, digital forensics investigator/system administrator/operator, digital forensics analyst, and the legal prosecutor.

The final stage of the model involves reviewing all the steps with a view to identifying areas of improvement and further improving existing and establishing new policies and procedures. It can be argued that this is a necessary step to support organisational resilience while offering an appropriate level of robustness.

(Kerrigan, 2013) proposes a Digital Investigation Capability Maturity Model that can be used to analyse the digital investigation capabilities of an organisation. As the name suggests, the model is based on the more generic Capability Maturity Model Integration process improvement model.

However, none of these works specifically focused on defining and maintaining robustness and resilience over the life of the digital investigation laboratory. For this reason, we attempted to determine the current status of robustness and resilience as implemented by organisations with digital investigation capacity.

Robustness and resilience in digital investigation capacity

The ubiquitousness of electronic devices and the very nature of cybercrime and its effects require that law enforcement agencies and judicial entities, including international organisations such as the ICC, be able to effectively and efficiently conduct digital investigations with the aim of identifying and capturing relevant electronic evidence.

In order to do so, the authors argue that it is essential to have a robust and resilient integrated digital investigations framework in place that

- follows best-practices and international standards;
- ensures stability to mitigate the impact of change (e.g. staff turnover) and minimise the risk of non-conformity;
- can adapt in a controlled and managed way to current and future trends and developments such as cloud computing, the pervasive use of connected sensors and actuators, the widespread use of encryption and the ever increasing size of storage space;
- ensures that the necessary skills and expertise are available to collect, extract, analyse, present and preserve electronic evidence with a view to allowing for the effective and efficient prosecution of crimes.

Law enforcement agencies and organisations like the ICC face a number of challenges in this respect.

For law enforcement these include the increasing volume, scope and sophistication of cybercrime as well as its trans-national nature. Other challenges are rooted in the speed at which cybercrime develops in terms of new attack vectors, broader attack surface, new techniques, etc., the

difficulties in attributing online crimes to perpetrators, and the legal challenges related to having to work across boundaries. The management of electronic evidence and maintaining the chain of custody, as well as technological and digital advancement and obsolescence deserve to be mentioned as well.

In the case of the Court, additional challenges are linked to the eCourt model, standardising in a multi-lingual environment, and managing the technical complexity of the supporting ICT architecture. Providing adequate support to OTP's Investigation and Prosecution divisions is another area of importance for the Court in this context.

Finally, there are a number of organisational challenges that confront law enforcement and international organisations alike e.g. a frequently changing workforce, hand-over and knowledge transfer issues as well as establishing and maintaining the necessary in-house skills and expertise.

This creates a complex and dynamic environment within which such organisations as equally complex and dynamic systems need to operate. The authors contend that it is therefore essential to appreciate these dynamics and complexity in the context of organisational resilience and robustness.

Existing literature has looked at various aspects of digital investigation frameworks, focussing primarily on the main processes, standardisation, and capturing relevant digital forensic investigation information and knowledge. While some frameworks propose learning and adaptation aspects, this is not looked at from a broader, organisational point of view.

As mentioned before, some research has looked at knowledge management in police work with some authors focussing specifically on digital forensics, which is seen as a knowledge-intensive area for law enforcement.

Apart from capacity planning and building, the authors consider robustness and resilience, supported by knowledge management, as crucial properties for any organisation involved in digital investigations because of ever-changing requirements and scenarios on the one hand and the need to adhere to legal rules and regulations and to follow well-established and approved procedures on the other hand.

This work addresses the problem of identifying and defining key elements of robustness and resilience in the context of sustainable digital investigation capacity and integrated digital investigations frameworks. The main focus is on surveying and analysing the current state of robustness and resilience practices that have been implemented in organisations with digital investigation capabilities.

The results presented in the next section are used to identify the key elements of resilience and robustness, and act as a starting point for considering such elements when designing digital investigation capabilities and for incorporating them into an integrated digital investigation framework.

Research plan

In order to survey and evaluate the current state of digital investigations frameworks among EU law enforcement agencies, looking specifically at robustness and resilience and taking into account knowledge management aspects, the authors conducted a structured online survey consisting of 35 closed and open questions, with several dependent sub-questions.

The questions were designed to elicit relevant elements of resilience and robustness, including aspects of knowledge management, training and education, quality management, standardisation, and research and development.

The survey was sent to EU law enforcement agencies, using the European Cybercrime Training and Education Group's (E.C.T.E.G) mailing list, and subject-matter experts. It was sent to a total of 72 recipients of whom 21 responded resulting in a response rate of approximately 29%.

A slightly modified set of questions was used to elicit the status quo of the digital investigations framework of the ICC's Office of the Prosecutor. This was done through interviews and combined feedback from subject-matter experts at the OTP.

The main purpose of the online questionnaire was to assess and identify areas relevant to organisational robustness and resilience in the area of digital investigations for law enforcement agencies.

Similarly, the main purpose of the questionnaire for the OTP was to assess and identify areas relevant to organisational robustness and resilience in digital investigations in an international environment.

Specifically, the questions of the online questionnaire were centred around digital investigation and digital forensic examination issues with a view to capturing the challenges that law enforcement experiences in these domains (e.g. lack of qualified staff, new types of cybercrimes) and to assessing if and how law enforcement considers resilience and robustness in this area. Moreover, it aimed at evaluating the extent to which law enforcement considers knowledge management measures as a means to achieve resilience and robustness in the area of digital investigations. The evaluation of the responses received was supported by discussions with experts in this area and the authors' experience in this field.

The set of questions for ICC's OTP had a similar focus but had to be adapted to the specificities of the Court. Nevertheless, the OTP does face some of the same challenges, which was to be expected. The feedback from the OTP was further enriched by interviews with selected management staff and also combined with one of the author's first-hand experience of having worked with the OTP.

In support of the evaluation step, the data received was split up into separate questions and related sub-questions. Where needed, the data was cleaned by filtering empty or irrelevant fields.

In a next step, the data was analysed and visualised for better understanding. Where useful, links between the various questions were examined with a view to identifying relevant correlations.

Based on the analysis and informed by the literature review and expert input, a set of key design elements for robustness and resilience was extracted. The authors contend that these key elements, which will be discussed in more details in the subsequent sections, are essential for robustness and resilience when designing digital

investigation capabilities in the context of an integrated digital investigations framework.

Survey results

The following section gives a summary quantitative assessment of the survey data. An anonymised version of the raw survey data is publicly available at http://dfire.ucd.ie. A general overview of the results are shown in Table 1

From the survey, it was found that developing and implementing a strategy for digital forensics is considered to be essential for planning, resource allocation, minimisation of duplication of efforts, identification of priorities and key objectives, and for having a streamlined and concerted approach. The responses indicate that the majority of the respondents (app. 76%) have a digital forensics strategy. However, only 24% claim that the strategy has a national/state-wide scope which would suggest that there is room for better co-ordination, synchronisation and standardisation of strategies. It is also worthwhile to note that nearly one quarter of the respondents indicate that they do not have a defined strategy in place. Of the strategies that are implemented, most cover digital investigations and forensic examinations (65%).

Some respondents claimed that digital forensics is considered a discipline of its own as it requires different approaches e.g. in the way the evidence is examined. Others indicate that there is a service-based approach to delivering digital forensics in support of investigations. Based on the responses received, it appears that the majority of the agencies surveyed consider digital forensics a forensic discipline. While there are benefits to be found in treating digital forensics as a separate discipline due to the different methods, tools and techniques used, there is a risk in treating it as a separate discipline as it will still have to follow the basic principles of police investigations and digital forensics. Also, it could lead to siloing of expertise and knowledge, particularly if the interfaces between investigators and digital forensic examiners are not defined or managed well.

Table 1
Generalised overview of key robustness and resilience survey results from 21 Law Enforcement-related respondents.

Question	Yes	No
Have a digital forensic strategy	76%	24%
National strategy scope	24%	76%
Strategy covers digital investigation	65%	35%
DF and DI are separate roles	35%	65%
DF and DI sit in different departments	42%	58%
DF is forensic discipline	65%	35%
Have continuous education plan	68%	32%
Offer computer based training	48%	52%
Have personal development portfolio	52%	48%
Time off for training/research	55%	45%
Have new staff mentoring system	81%	19%
Education considered in evaluations	48%	52%
Have minimum required education standard	48%	52%
Have reporting standards	67%	34%
Have standardised forensic software	61%	39%
Have quality management system	29%	71%
Have knowledge management program	16%	84%
Use open source digital investigation tools	69%	32%
All tools are court approved	35%	65%
Cooperate with academia	76%	24%
Cooperate with private sector	57%	43%
Employ civilian experts	62%	38%
Have competitive pay scheme	47%	53%
Have research and development unit	29%	71%
Have process to manage knowledge hand-over	86%	14%
Offer incentives for LE working as DF	30%	70%
Consider robustness and resilience in hiring	58%	42%

In the context of resilience and robustness, following different concepts may increase additional challenges as it will be harder to streamline planning, risk management, analysis and corrective measures and activities. It may also lead to the creation of a 'group within a group' that is considered to be separate from the rest of the organisation.

Where digital forensic investigators and digital forensic examiners are treated as different roles, nearly 42% percent report that they also sit in different departments. Again, it can be argued that there are advantages in separating these roles to allow for specialisation. However, particularly in cases where examiners are not co-located with investigators, it may be harder to ensure resilience and robustness (e.g. examiners may feel less obliged to adhere to investigative standards) and to manage and transfer knowledge.

Close to 68% of the participants claim to have a continuous education/training plan for digital forensics in place. A number of respondents use a mix of different courses, usually developed in house as well as received from external formal training sources. However, less than 50% of law enforcement agencies claimed to use contemporary learning methods. Despite the existence of training plans, nearly 50% of the responses indicate that there is no development portfolio to keep track of the training courses they have taken, and their specific training needs.

Only 55% of the survey participants claim that digital forensics staff gets time off for training and research. Given that cybercrime is considered to be not only a knowledge-intensive field but also an area where knowledge quickly becomes obsolete, training and research are important for law enforcement to remain relevant and have the knowledge, expertise and skills to investigate cybercrime.

Approximately 50% of the respondents that have a mentoring system in place (81%) follow a formal approach. From a KM perspective it is essential to allow mentoring of staff as much knowledge and expertise cannot be codified in electronic form, making face-to-face interaction and hands-on experience indispensable.

More than 50% of the survey participants claim that education and training is not considered during a staff member's performance evaluation. Further, more than half of the responses indicate that there is no minimum education standard in place during recruiting. Two third of the survey participants claim that their agency offers specialised courses, most of which are not academically accredited. Also, only 40% of the organisations that offer such courses use a modular approach that takes into account the learning needs and level of experience of digital forensics staff.

Only approximately 29% of the respondent claim to have a quality management system in place, of which only one organisation is certified; this should be considered an area of potential action for law enforcement. As established

before, there are close links between organisational resilience and robustness and KM. However, only about 16% or three respondents indicate that they have a KM program in place.

The majority of organisations claim to use a standard set of digital investigation tools. According to the data received, close to 70% claim to used open-source tools. Six respondents indicate that the digital forensics tools they use are court-approved. One respondent claims that the approval process is ongoing. A large percentage (65%) claims that the tools that are being used are not court-approved. This does not have to be a problem per se but may impact on the investigation and presentation of cases in court.

The need to co-operate with academia is reflected in the high percentage of respondents (app. 76%) that claim to do so. On the co-operation with the private sector, the responses received suggest that co-operation is more diverse as it also encompasses areas such as the development of tools and the exchange of information. However, co-operation with the private sector is only happening for approx. 57% of the respondents.

Only about 29% of respondents claim to have research and development capabilities. Of the survey participants that claim to have a research and development unit, the number of staff is between two and six. One respondent claimed to employ 100 research and development staff. The main areas of research and development cover current fields of digital forensic investigation and examination. A number of activities seem to be more future oriented e.g. vehicle forensics and trend analysis.

According to the feedback received, nearly half of the digital forensics examiners leave within the first 5 years. About 56% stay for at least 6 years. Of those who leave within the first five years, the majority leaves after two to three years. When looking at digital forensic investigators, a similar picture can be drawn. The number of investigators leaving within the first five years is even slightly higher than for examiners. About 50% stay for at least more than 6 years. Of those who leave within the first five years, the majority leaves after four to five years. After 6 years, it appears that there is a slightly higher turnover in digital forensic examiners. Comparing the numbers per respondent, there is a tendency for investigators to stay longer than forensics examiners.

Only a small percentage of the participants in the survey indicate that they have a formal knowledge hand-over process in place. The large majority does not manage the hand-over between outgoing and incoming digital forensics staff.

When asked what the definition of resilience is, responses covered a number of relevant aspects of resilience in digital forensic investigation:

- Education and skills, including the systematic increase of knowledge
- Adaptiveness, including awareness of new technologies and adapting the investigation process
- Capability to consistently produce forensically sound results, based on skills, tools and standard operating procedures
- Speed and quality in conducting digital forensic investigations, specifically in terms of the no. of cases and the volume of data
- Business continuity plan
- Budget

The responses in relation to robustness in digital forensic investigation largely corresponds to the input to the previous question:

- Enough time, right tools and adequate skills and expertise
- Education and training courses
- Quality control and validation of findings by subject-matter experts

One of the key questions of the survey aimed to elicit the (subjective) rating of law enforcement in terms of resilience and robustness. It allows putting some of the previous responses in perspective and, more importantly, provides an indication of how law enforcement rate the level of robustness and resilience of the agency for which they work.

None of the participants in the survey considers their organisation to be robust and resilient enough to deserve the highest rating. Most respondents give a robustness and resilience rating of three or four. A comparably large percentage (19%) gives the lowest rating which is certainly an area of concern.

Nearly 58% of the participants state that they look for elements of robustness and resilience during the hiring process. Consequently, about 42% do not consider these elements as part of the hiring process.

Survey assessment

This section provides a summary of the feedback received from EU law enforcement and a comparison to input by ICC's OTP. This includes a description of the similarities and the differences.

Commonalities with the ICC's OTP

As there is a general increasing tendency of cybercrime, with trends suggesting considerable increases in scope, sophistication, number and types of attacks, number of victims and economic damage, the need for law enforcement to have the digital forensics capabilities to effectively and efficiently address the problem of cybercrime is undisputed. It is of interest to note, however, that an organisation such as the ICC, which deals with large investigations involving war crimes and other forms of atrocities, also estimates that 80% of the current investigations require digital forensics, a percentage which the OTP expects to go up to 100% in the future. As a consequence, the need to develop and maintain digital forensics capabilities is of equal importance to the OTP as it is to law enforcement. This is also reflected in the OTP's responses.

The OTP and 76% of the participants in the EU law enforcement survey indicate that they have a digital

forensics strategy. 39% of law enforcement respondents state that the strategy has only been implemented partially. This is also true for the OTP. Therefore, similar arguments for the full implementation of the strategy apply to the Court as well.

Similar to EU law enforcement, the OTP uses a mix of industry standards and best practices including NIST, ACPO and Council of Europe as well as guidelines that were developed in-house. As previously mentioned, this is an area of potential redundancy and duplication of effort. In this context, cooperation and coordination among the relevant agencies and organisations, including for instance Europol, should be considered with a view to avoiding possibly conflicting or incomplete guidelines and standards. It can be argued that this is an important element of organisational resilience and robustness, but also knowledge management, as it is about capturing and codifying relevant information and knowledge.

Benefiting from its overall investigation strategy and the organisational setup, where the digital forensics function is part of a broader set of forensic activities, the OTP considers digital forensics a forensic discipline conducted under the same conditions as other forensic examinations. This is also the case for approximately 65% of EU law enforcement agencies. It can be argued that this is another contributing element to resilience and robustness as it allows for improved streamlining of planning, risk management, analysis and corrective measures.

Both law enforcement and the OTP rely on co-operation. The Court's underlying legal framework - the Rome Stature - includes a provision on requests for cooperation. This means there is a formal framework within which the OTP can ask States Parties for assistance; in addition it has established Memoranda of Understanding with partner organisations. In both domains co-operation with academia appears to be more common (76%) than working with the private sector (57%). Considering the important role the private sector plays in terms of the intelligence, expertise, knowledge and tools it can offer, possibilities to improve public-private-partnerships should be elaborated.

Given the comparably small size of OTP's Forensics Unit, digital forensic investigation and examination are not separate roles. The total number of digital forensics staff is currently four. For the forensic staff employed by the Court minimum education standards apply, including relevant university degrees and a certain number of years of experience depending on the level of the position. This is linked to the UN common system of which the Court like many other international organisations is a member.

The OTP has implemented a number measures supporting resilience and robustness as well as KM, as shown, for instance, by the fact that it has a continuous digital forensics education and training program in place. However, other relevant measures such as a reporting standard, a handover process or mentoring have not been considered yet. While mentoring seems to be in place for around 81% of the participants in the law enforcement survey, more than 33% do not have a reporting standard either and only around 14% of the law enforcement respondents claim to have a handover process in place. As these are considered important for achieving and maintaining/transferring digital forensics skills and expertise, this should be considered an area of improvement for both law enforcement and the Court.

As mentioned before, research and development is crucial for a robust and resilient digital investigation framework as it supports a pro-active and forward-looking approach and drives innovation. It is essential in examining new types of crimes and informing about emerging and future trends. The OTP and more than 71% of law enforcement do not have dedicated research and development capabilities, making this another potential priority area.

Only about 29% of the survey participants claim to have research and development capabilities. Considering the importance of this area, the authors argue that this would establish an essential element of a robust and resilient integrated digital forensics framework.

Although the definitions of robustness and resilience provided by the OTP and the law enforcement respondents differ, there are a number of similarities such as the soundness of investigations, quality, repeatability as well as speed and the need to be able to handle large volumes of data efficiently.

The challenges in conducting digital investigations identified by the OTP, including budget and operational costs, training and education and maintaining staff expertise, which could be translated to the number of qualified staff, match the three top challenges identified by law enforcement, which are:

- Number of qualified staff
- Training and education
- Budget

This supports the fact that despite the organisational dissimilarities and difference in terms of mandate and scope, law enforcement organisations and international organisations such as the ICC face similar challenges in the area of digital forensics.

Differences from the ICC's OTP

There are some notable differences too. For instance, the ICC and the OTP are governed by the Rome Statute as the main legal framework and, in the case of the OTP, instruments of implementation such as the Rules of Procedure and Evidence, and the Regulations of the Office of the Prosecutor. As a consequence, national legislation or EU legislation is not applicable to the Court. This means, for instance, that national rulings e.g. on the admissibility of certain digital forensics tools or methods have limited relevance for the ICC and the OTP. The ICC along with 65% of the law enforcement respondents should consider the endorsement of digital forensics tools as a means to increase the robustness and resilience of the digital investigation process.

Another interesting difference is the OTP's need to conduct digital forensic examinations on technology that is no longer a priority for EU law enforcement. The example given in the corresponding response are floppy disks. The cases that the ICC currently investigates are often in geographical areas where such technology is still in use.

This may pose challenges for digital investigators and digital examiners. A lack of adequate training courses and practical experience due of the comparably low frequency of digital forensics examinations further exacerbate this issue.

With regard to staff motivation and providing incentives for digital forensics staff, the ICC is limited by its staff rules and regulations, which are based on the UN common system. As a consequence, certain options such as offering free education or considering additional training and education during performance evaluation are difficult to implement. There are also minimum education and work experience requirements that come with the classification of a particular job. In some instances this may create challenges as relevant work experience may not be accepted in lieu of a lack of formal education, thereby eliminating potential candidates on formal grounds. Finally, international organisations such as the ICC usually do not have career development plans. In fact, a number of such organisations have a tenure system in place that requires staff to leave after a certain number of years.

Finally, OTP's multi-national and multi-lingual environment creates additional challenges in establishing standards for digital forensic investigations and examinations, and in ensuring resilience and robustness. These include different education standards, potential language barriers and varying levels of experience.

Proposed features for robustness and resilience

Considering the results of the literature review and informed by the analysis of the survey responses received, there are a number of key design elements for organisational resilience and robustness that can be identified.

Recalling also that there are strong links between organisational resilience and robustness and KM, the following key elements are proposed in the context of sustainable digital investigation capacity and designing integrated digital investigations frameworks. They have been grouped into strategic and operational elements.

It is important to note that not all of these elements should be seen as equally important. Furthermore, there are certain dependencies between these elements – for instance, not having a digital forensics strategy will most likely have a negative impact on any dependent elements such as education and training. It is also not suggested to consider all of these key elements at the same time or that all of them have to be fully considered in order to achieve robustness and resilience in the context of sustainable digital investigation capacity and integrated digital investigations frameworks. Rather, this should be interpreted as a gradual process using a weighted mix of the key elements identified, taking into account the strategic and operational objectives of an organisation and its risk posture.

Strategic level

The strategic level focuses on short and long term goals relating to identified key factors of resilience and robustness.

Digital forensics strategy

The groups that claimed to have implemented a digital forensics strategy were also more likely to rank their agency as more robust and resilient. We contend that having a strategy for digital forensics is essential for providing the necessary strategic, legal and operational framework. As such, it also establishes a reference point for organisational resilience and robustness as it should define the main scope and boundaries for digital forensic investigations and examinations. Moreover, it should establish the basis for high-level performance indicators and capacity objectives. Given the trans-national nature of cybercrime and the need for a co-ordinated multi-stakeholder response, the scope of such a strategy should go beyond the individual department or organisation.

Standardisation

Following industry standards and best practices is considered critical for digital investigations and examinations. It helps ensure a high level of quality and facilitates cross-organisational and cross-border co-operation and exchange of information as well as multi-national investigations. Standardisation also helps avoid duplication of efforts and supports a more efficient management of resources e.g. through re-use, transfer and pooling of resources. It is therefore considered an essential design element for an integrated digital investigations framework that is resilient and robust. Given that the majority of respondents do not use quality or knowledge management systems, the use of industry-level best practices can serve as a starting point for in-house knowledge management.

Forensic discipline

Linked to the elements of Digital Forensics Strategy and Standardisation, following the relevant principles and processes established in the field of forensics provides a way to better streamline digital forensics with other forensic disciplines, thereby supporting organisational resilience and robustness by allowing for a more holistic and integrated approach to digital forensics. It also helps prevent siloing of information and knowledge, and helps avoid a fragmented approach to digital investigations and examinations which could be especially common in the organisations where digital examination and investigation are separated.

Continuous education and training

Presently, some organisations are providing training opportunities as a benefit of digital forensic examination, but in general there appears to be little incentive or support for continued education of investigators.

Continuous education and training is essential to establishing and maintaining the necessary digital investigation and examination knowledge, expertise and skills. Thus, it is also crucial for organisational resilience and robustness as it provides individuals and the organisation with relevant and up-to-date training to help respond to a changing environment, potentially in a pro-active manner.

Including all levels in an organisation also helps create a baseline awareness of digital investigation and examination issues which can help justify resources, including

support from other business areas and help inform policy makers and other senior decision makers.

Research and development

Research and development is also shown to not be a priority area for most organisations. As mentioned previously, innovation is an important aspect of organisational resilience and robustness as well as knowledge management. Thus, research and development is considered essential in providing a forward-looking function and in strengthening an organisation's adaptive capacities. This allows for a pro-active approach to developing sustainable digital investigation capacity in the context of an integrated digital investigations framework, for instance by informing decision makers about relevant trends or new types of cybercrime.

Co-operation

The complex and dynamic nature of cybercrime requires an equally diverse and dynamic response by law enforcement. Among other things, this involves adapting existing and developing new methods and techniques of digital forensic investigation and examination, while ensuring that they are sound and lawful. Supporting also the previous key element, co-operation with academia is considered an essential aspect in supporting research and development; especially since organisations often do not have the required resources themselves.

The survey results suggest that co-operation with the private sector seems to be less common. However, taking into account the important role that the private sector plays in terms of the intelligence, expertise, knowledge and tools it can offer, the area of public-private-partnerships should be given a special focus.

Operational level

The operational level focuses on practical implementation relating to identified key factors of resilience and robustness.

Standardisation

At the operational level, working to approved, documented and standardised procedures is seen as a central requirement for digital forensic examinations and investigation, and also for achieving resilience and robustness. This is shown by the majority of organisations at least attempting to implement standardised processes and tools. Thus, it should be an important element to design for sustainable digital investigation capacity in the context of an integrated digital investigations framework. Ideally, this should be integrated with an organisation-wide quality management system, which would require having all business processes be documented and reviewed on a regular basis.

Continuous education and training

As shown, much training is happening in-house, and is developed in a relatively piecemeal fashion that is largely unsustainable. At the operational level, continuous education and training needs to be translated into education and training programs that have well established interfaces with the digital investigations framework and all other relevant stakeholders to ensure that all relevant requirements are captured and considered in the planning, design and delivery education and training programs.

Where possible this should be combined with knowledge management measures to capture any lessons learned, which then support planning of training and education activities. The use of e-learning should be considered as an efficient and effective use of resources in this context.

Research and development

At the operational level, research and development would ideally require dedicated resources e.g. in the form of an organisational entity dedicated to research and development. As this is often not feasible, co-operation with academia and the private sector should be strengthened in this context as well.

Co-operation

Co-operation is considered a key design element in the context of sustainable digital investigation capacity and integrated digital investigations frameworks. At the operational level this could include entering operational agreements with academia and the private sector and may require developing the necessary protocols and trust relationships.

Human Resources

There are a number of enabling design aspects that fall into the realm of Human Resources. This includes, for instance, giving staff time off to conduct research and development.

As reflected in the feedback received, there is a mix of Human Resources measure that are considered critical in establishing and maintaining robustness and resilience. These include developing processes for mentoring and managing the hand-over process between incoming and outgoing staff, creating incentives and benefits for sharing knowledge and expertise and for keeping it up-to-date and relevant, and, last not least, providing training and education opportunities.

Conclusions

The trans-national, dynamic and evolving nature of cybercrime requires that law enforcement agencies and judicial entities, including international organisations such as the ICC, be in a position to effectively and efficiently conduct digital investigations and examinations while being able to adapt to a constantly changing environment in a controlled manner. In order to achieve this, the authors argued for a focus on robustness and resilience when developing digital forensics capabilities.

It has been shown that the role of robustness and resilience in the area of digital investigations and examinations has received little attention in the literature. However, it can be expected that organisational resilience, and related concepts such as KM and quality management, will play in increasingly important role for law enforcement and organisations like the ICC in creating and maintaining the resources required to effectively and efficiently

prevent, protect, disrupt and investigate cybercrime in the face of high staff turnover, complex and changing requirements, and technological advancements.

The proposed approach offers a more holistic view on digital investigations and examinations and, as such, presents an expansion to existing digital forensics investigation frameworks discussed in the literature.

Specifically, this paper aimed to address the problem of identifying and defining key elements of robustness and resilience in the context of sustainable digital investigation capacity and designing integrated digital investigations frameworks.

Future work

Future research will focus on how to extract some additional key performance indicators such as the backlog of cases to provide a deeper understanding of the impact of resilience and robustness on digital investigations and examinations. Such key indicators may also be combined with other work, such as the Capability Maturity Model (Kerrigan, 2013), to assess digital investigation capability of an organisation and perform a gap analysis to identify the most critical areas for development. Further, more analysis of the survey data will be conducted to determine further significant factors in relation to the perceived robustness and resilience of an organisation.

Disclaimer

The views expressed by the author in this publication do not necessarily reflect the views of Europol's EC3.

References

Agarwal A, Gupta M, Gupta S, Gupta SC. Systematic digital forensic investigation model. Int J Comp Sci Secur 2011;5(1):118–31.

Anand A, Singh MD. Understanding knowledge management: a literature review. Int J Eng Sci Technol 2011;3(2):926–39.

Braes BM, Brooks DJ. Organisational resilience: understanding and identifying the essential concepts. In: Guarascio M, Reniers G, Brebbia CA, Garzia F, editors. Safety and security engineering, Vol. IV. WIT Press; 2011.

Burnard K, Bhamra R. Organisational resilience: development of a conceptual framework for organisational responses. Int J Prod Res 2011;49(18):5581–99. http://dx.doi.org/10.1080/00207543.2011.563827. http://www.tandfonline.com/doi/abs/10.1080/00207543.2011.563827.

Burnard K, Bhamra R, Young RI. Critical factors of organisational resilience. In: Proceedings of the 19th International EurOMA Conference; 2012.

Chang W, Chung P. Knowledge management in cybercrime investigation A case study of identifying cybercrime investigation Knowledge in Taiwan. Of lecture notes in computer science, Vol. 8440. Cham: Springer International Publishing; 2014. http://dx.doi.org/10.1007/978-3-319-06677-6. http://link.springer.com/10.1007/978-3-319-06677-6.

Gottschalk P. Knowledge management systems in law enforcement: technologies and techniques. IGI Global; 2007.

Gottschalk P. Policing cyber crime, bookboon. 2010.

Hinduja S. Computer crime investigations in the United States: leveraging knowledge from the past to address the future. Int J Cyber Criminol 2007;1(1):1–26.

Ieong RS. FORZA digital forensics investigation framework that incorporate legal issues. Digit Investig 2006;3:29–36. http://dx.doi.org/10.1016/j.diin.2006.06.004. http://www.sciencedirect.com/science/article/pii/S1742287606000661, http://www.sciencedirect.com/science/article/pii/S1742287606000661/pdfft?md5=1e4d5926b123af6d64fa5ee3e50f82c1&pid=1-s2.0-S1742287606000661-main.pdf, http://linkinghub.elsevier.com/retrieve/pii/S1742287606000661.

James JI, Gladyshev P. 2010 report of digital forensic standards, processes and accuracy measurement. 2010.. In: http://www.forensicfocus.com/2010-digital-forensics-standards-processes-accuracy.

Kerrigan M. A capability maturity model for digital investigations. Digit Investig 2013;10(1):19–33. http://dx.doi.org/10.1016/j.diin.2013.02.005. http://linkinghub.elsevier.com/retrieve/pii/S1742287613000133.

Mafabi S, Munene J, Ntayi J. Knowledge management and organisational resilience: organisational innovation as a mediator in Uganda parastatals. J Strategy and Manag 2012;5(1):57–80. http://dx.doi.org/10.1108/17554251211200455. http://www.emeraldinsight.com/10.1108/17554251211200455.

Sambamurthy V, Subramani M. Special issue on information technologies and knowledge management. Manag Inf Sys Quart 2005;29(1):1–7.

Seba I, Rowley J. Knowledge management in UK police forces. J Knowl Manag 2010;14(4):611–26.

Sutcliffe K, Vogus T. Organizing for resilience, positive organizational scholarship: foundations of a new discipline. In: Cameron K, Dutton J, Quinn R, editors. Positive organizational scholarship: foundations of a new discipline. Berrett-Koehler; 2003.

Vogus TJ, Sutcliffe KM. Organizational resilience: towards a theory and research agenda. In: 2007 IEEE International Conference on Systems, Man and Cybernetics. IEEE; 2007. p. 3418–22. http://dx.doi.org/10.1109/ICSMC.2007.4414160. http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4414160.

Wasko MM, Faraj S. Why should I share? Examining social capital and knowledge contribution in electronic networks of practice. MIS Quart 2005;29(1):35–57.