Wireless Networks
https://doi.org/10.1007/s11276-018-01920-5

# Towards a capability maturity model for digital forensic readiness

Ludwig Englbrecht[1] · Stefan Meier[2] · Günther Pernul[1]



**Abstract**
Increasing IT-Security breaches and the extensively growing loss due to fraud related incidents cause the need for being prepared for a digital investigation. A specific capability maturity model can assist organizations to determine their current state according to implement digital forensic readiness measures and get assistance to reach a desired level in having related capabilities implemented. This paper examines how such a model can assist in integrating digital forensic readiness related measures and to reach an appropriate maturity level. Through facilitating core elements of the IT-Governance framework COBIT 5 and the core characteristics of implementing digital forensic readiness a proposal for a specific capability maturity model has been conducted. In five maturity levels (*Initial*, *Managed*, *Defined*, *Quantitatively Managed* and *Optimized*) the different stages of implementing digital forensic readiness measures are represented. It can be shown that with the IT-Governance aligned model the implementation of digital forensic readiness can be assisted.

**Keywords** IT-Security management · Digital forensic readiness · Capability maturity model · IT-Governance

## 1 Introduction

Following the tremendous increased and advanced fraudulent attacks since 2015 even the most security aware executive managers, policy-makers, Chief Executive Officers, or other decision makers were suddenly given a wake-up call. In August 2015, the FBI already warned that losses related to fraudulent email attacks worldwide have been summed up to more than $1.2 billion USD from October 2013 until August 2015 [21].

One of the reasons for such an extensive loss was rooted to attacks on corporate banking accounts caused by the ransomware called *dyre wolf*. This malicious software is a highly effective banking trojan. It is characterized by the fact of being built with feature-rich capabilities and ongoing updates to mitigate its detection. Remarkable is the group behind the malware which enables the unauthorized transaction of large sums of money. A neat combination of knowledge of the banking system, a feasible infrastructure, manpower, social engineering and technical skills demonstrates a new level of quality in malware-caused fraud. A single target could experience losses of $500,000 to more than $1,000,000 USD [20].

Also attacks related to spy and industrial espionage have led to significant losses during the last years. These cyber attacks threat valuable resources, e.g. intellectual property. The high value of intellectual property and its increased interest by attackers had been underestimated for a long time. Nowadays relevance of such risks as well as a proper risk management are also increasingly addresses by policy-makers [10].

Cyber-attacks against IT infrastructures have become more frequent and complex in recent years. The attackers also have become more professional. Cyber-attacks are launched from various places. With the interconnection of various systems and enterprises via the internet it is also possible to conduct hidden attacks. This could be realized by exploiting various vulnerabilities of connected devices and misuse these devices for other attacks. For example, the *mirai* botnet abused weak devices of the Internet-of-things to perform DDoS Attacks [22].

✉ Ludwig Englbrecht
ludwig.englbrecht@ur.de

Stefan Meier
sm@meier-pc.de

Günther Pernul
guenther.pernul@ur.de

[1] Department of Information Systems, University of Regensburg, Regensburg, Germany

[2] Meier Computersysteme GmbH, Deining, Germany

Published online: 01 January 2019

Digital Forensic (DF) is a good approach to unveil fraud. The perspective in digital forensic investigation needs to change from a reactive view towards a pro-active. With the new perspective, various new research questions arise. Given that the forensic analysis task is complex and faces multiple internal and external influences, an interesting question is, how an enterprise can evolve digital forensic capabilities in advance to resist vast changes in its demands. Digital forensic readiness (DFR) is an area that aims to solve this particular problem [34].

Being prepared for a digital forensic investigation in the context of DFR has still not been addressed by many companies or governmental institutes [24]. Mouhtaropoulos et al. [25] have analyzed various governmental and academic initiatives for the establishment of Forensic Readiness. However, due to the broad varying initiatives and an absence of uniformed rules, the authors postulate standardization within the area of DF. They also mention the high amount of accumulated needs in DFR capabilities in organizations. Therefore, implementing DFR within an organization is not a trivial task and there is a need for further assistance through the whole organization. This work provides a capability maturity model (CMM) to assess the current state of initiatives in DFR and shows a guidance to turn efforts into the right direction.

The paper is structured as follows. In the following section we present basics in DF, DFR and CMM. Additionally, an overview of related work in CMM for DFR is presented in Sect. 2. The development approach for a digital forensic capability maturity model is presented in Sect. 3. Section 4 describes the suggested digital forensic readiness capability maturity model in detail. In Sect. 5 an application of the model is presented by a possible implementation and illustrated by a case study. Section 6 provides a summary and an outlook on future work.

## 2 Background and related work

### 2.1 Digital forensics and forensic sciences

The forensic sciences generally deal with the application of scientific methods for investigations in legal cases [18]. In this context, forensic scientists must adapt questions of a legal case into scientific questions and answer these by using appropriate and scientifically validated methods [9, 13]. This requires a well-defined and well-founded knowledge base and a scientific method as well as an experimental base [8, 26]. Following this argumentation, digital forensics is understood as a forensic science that deals with the application of methods from computer science to questions of the legal system [9]. In detail, this means, that digital forensics provides methods to preserve and process digital evidence which guarantee the highest possible objectivity in digital forensic investigations [9].

Nowadays, conducting a digital forensic investigation can be challenging due to the large data sets which need to be stored and analyzed. By facilitating scientifically proven forensic techniques a digital investigation with any data size can be supported. The scientific methods enable the processing, i.e. preservation, analyzation, interpretation and presentation of digital evidence in a proper manner. Also the integrity of possible evidence is protected, which enables that the evidence stands up in a court of law [26].

### 2.2 Digital forensics readiness

Tan [34] initially mentioned DFR in 2001 and defined it as a mechanism to minimize the costs of digital forensic investigations and to maximize the capability of an organization to collect evidence with a correct legal reliability. Pangalos and Katos [27] extended this definition as "the state of the organization where certain controls are in place in order to facilitate the digital forensic process and to assist in the anticipation of unauthorized actions shown to be disruptive to planned operations". This definition emphasizes the aspect that it is crucial to pursue a proper support of the entire forensic process. The focus is also turned away from just producing credible digital evidence and adds the anticipatory perspective into DFR.

Digital Forensics is a relatively young scientifically discipline. Also the research in DFR has been conducted from many different views and perspectives. For example, Reyes and Wiles [29] analyze the allocation of adequate resources. The selection and usage of adequate technology has been researched by Carrier and Spafford [4]. Training initiatives are discussed in [4, 30]. Also legal investigation, incident response and policies have been analyzed according DFR [1, 5, 31, 34].

Most of these publications just discuss a selected aspect of DFR. The need for whole organizations to be forensically ready by regulations has been increased in the past years. This leads towards a comprehensive view on DFR within an organization. Implementing DFR measures is cost intensive and the desired economical return is lower than in other projects. This puts organizations into the need to balance the costs of being forensically ready and the positive effect of being prepared in case of a digital investigation. The last aspect includes the capability to produce and preserve digital evidences in an efficient way [29, 30].

Carrier and Spafford [4] also distinguish Forensic Readiness between operational readiness and infrastructural readiness. The operational readiness can be determined by adequate provision of training and equipment present for individuals who are involved in digital forensic

activities. Infrastructural readiness can be reached by establishing possibilities to preserve evidences appropriately. Rowlingson [30] covers these elements and proposes a clustering of forensic related activities in planning, policing, training and monitoring. These elements support the achievement of DFR massively [30]. Further important aspects of DFR have been stated by Grobler et al. [12]. There DFR is considered a proactive forensic activity. They also mention that the culture and governance of an organization should be considered in DFR implementation. The tight alignment of implementing DFR measures with the management of an organization can assist to fulfill this aspect [12].

By virtue of the high complexity according to Forensic Readiness initiatives in large scaled companies, Reddy and Venter [28] propose a Forensic Readiness management system. This system supports in managing Forensic Readiness effectively within an organization. Based on the work of Tan [30, 34, 35] the authors define requirements to the Forensic Readiness management system.

Elyas et al. [11] present an expert perspective on their theoretical framework which is a holistic guidance on how an organization can become forensically ready. The framework consists of a set of Forensic Factors within various areas of forensic readiness and a set of Forensic Readiness Capabilities.

Ivtchenko and Sachowski [15] consider the implementation of DFR measures from a business perspective and their work serves as a guideline for establishing the necessary DFR measures in an organization. The areas, *people*, *processes* and *technologies* are considered in a purposeful way. These areas are addressed holistically but without using an IT-Governance framework.

### 2.3 Capability maturity model

Capability maturity models in the area of information technology are generally focused on development-processes and phases within organizations and the involved Information Systems. They build a sound fundamental base for their evaluation according quality assessment. Therefore, the structure of the model is based on a stepwise progress for improvements. Every step acts as an assessment for quantity of processes and methods from enterprises and systems. Based within this assessment approach, corresponding options for improving and options for actions can be derived. Due to the structure of the model the steps are in a chronological order and are built on each other. This sequence shows how an approach for improvement could be designed [7]. By applying this model, a user can determine the current position of an organization according their capabilities and the quality of various services. A capability maturity model also offers assistance for the development of the enterprise or involved elements of an organization [7].

Based on [7] three main goals of a capability maturity model can be noted: (a) A quality assessment of an organization with its processes and information systems. (b) Providing a base for benchmarking with competitors. (c) Show an approach for (quality) improvements.

A CMM is mainly based on a documentation of the processes and systems within an organization and can involve increased bureaucracy which makes an application of CMM complex and expensive [16]. Nevertheless, a CMM can provide a significant benefit to organizations and responsible employees by providing a systematic schema for determining their current positions for a competitive and future oriented development.

The most famous and proven capability maturity models in the area of software development are Capability Maturity Model Integration (CMMI) and Software Process Improvement and Capability Determination (SPICE). In this paper, these models are used as a baseline for developing a capability maturity model for digital forensic readiness.

### 2.4 Related work

Kerrigan [19] performed a study how prepared companies in Ireland are with reference to digital investigations. He provides a CMM including various measures for the implementation of Forensic Readiness. The model provides a possibility to assess the forensic capabilities of an enterprise. In this context, the author emphasizes that the highest goal of the model must not be reached compulsively. This level of the capability maturity model involves significant costs and efforts to be reached. The application of the assessment by facilitating the model has been conducted in ten organizations located in Ireland. Additionally, Kerrigan has proposed a capability maturity model for digital investigations named the Digital Investigation Capability Maturity Model (DI-CMM). This model can be applied as a tool for analyzing the investigation capabilities within an organization. The author defined digital investigation capability maturity levels and enriched these with detailed descriptions. Their work also shows with the application of the objective oriented maturity model in a real-life organization that there is a significant difference to the organizations' subjective assessment according their digital investigation capabilities. As a conclusion a majority of the organizations over-estimated their capabilities according digital investigations [19].

Chryssanthou and Katos [6] present a framework for assessing forensic readiness. The suggested framework is based on the Systems Security Engineering-Capability Maturity Model (SSE-CMM). The purposed maturity

assessment framework has been built up by specifying five different Process Areas (PA). The authors used generic phases of a digital investigation by mapping them to PAs: *Identification*, *Acquisition*, *Examination*, *Analysis* and *Reporting*. The assessment framework for digital forensic has been extended by elements from incident response. The following PAs have been added: *Monitoring*, *Detection*, *Response* and *Restore*.

The forensic readiness levels are used by Chryssanthou and Katos by applying the assessment model in a fictitious scenario with an example company. The assessment is based on linking the PAs to suitable questions. After the fictitious company was questioned, a forensic readiness profile was retrieved. The work shows that the assessment of forensic readiness can be handled with a capability maturity approach. Nevertheless, the development of this capability maturity approach does not follow a comprehensive way and the model cannot be applied to implement DFR holistically.

In contrast to the approaches described above we present an approach to develop a DFR specific CMM with the intention to cover DFR implementing initiatives holistically within an organization. Karie and Karume [17] state that the implementation of DFR in organizations is still a current challenge due to the fact that decision-makers need to understand and pursue the implementation of proactive measures to respond to an incident and to establish a digital forensic ready environment.

To smoothen the implementation, the approach presented here provides IT-Governance oriented support to reach a desired level in having DFR capabilities present. This approach addresses the government and management as well as decision-makers of an organization as they may already be familiar with elements from the area of IT-Governance.

## 3 Capability model development approach

In recent years, several different applications and variations of maturity models have been developed. They have been implemented across a multitude of domains. The base model was the CMM from the Software Engineering Institute of the Carnegie Mellon University. The increased development of different capability models in various business areas has also shown downsides. Publications of capability maturity models show, that the models or concepts are not scientifically proven according to their development process. A few models seem to be developed as a marketing instrument of a consulting or software development company. The documentation about the development process of a model is also often poorly prepared [2]. To overcome this pitfall, the development of a capability maturity model for DFR in this work underlies a strict and transparent methodology. For this, various concepts for the development of a capability maturity model are described and a specific approach is selected and adopted.

### 3.1 Baseline model

Becker et al. [2] provide a scientifically proven principle for developing a capability maturity model. They define and differ five important phases within the developing process: Definition of the problem, comparison of existing models, defining a development strategy, iterative development of the model and concepts for transfer and evaluation. The intended development of a digital forensic readiness maturity model in this work uses a general development framework provided by De Bruin et al. [3]. The framework presents a guideline to develop a theoretically sound, rigorously tested and widely accepted maturity model. The suggested framework consists of the phases *Scope*, *Design*, *Populate*, *Test*, *Deploy* and *Maintain*.

### 3.2 Definition of the maturity levels for the DFR CMM

The representation of capability profiles is not unrestrictedly applicable for comparing capabilities of an organization with others or companies within the same branch. Due to the fact that the intended capability maturity model is based on the CMMI, essential elements of CMMI can be reused. The CMMI has defined maturity levels to allow an overall assessment of the maturity of an organization. This reorientation of a maturity level aligns to a specific selection of PAs. They should cover the intended assessment holistically. This approach supports the assessment of the whole organization and enables an inter-organizational comparison. To provide this holistic assessment of an organization according DFR including all relevant evaluation domains, five maturity levels have been defined. Based on the core concept of the CMMI [7] and the systematic provided by [19] the following maturity levels are defined. Aspects of [6, 19, 28] also influenced the definition of the levels.

*Level 1* Level 1 represents non-existing measures according DFR. This is general characterized by having no formalization and a digital forensic investigation is performed chaotically and unstructured. There are also no standards or documentations about how a process should be performed. Knowledge about DF and the importance of keeping traces secure and useful for a court of law are not present within the organization.

*Level 2* Level 2 defines basic elements in performing DFR related activities. For example, there is a low or

minimal formalization of procedures in the case of a digital investigation. Also a repeatability in various processes is recognizable. Additionally, a basic documentation is present. In this level, minor DFR aspects are fulfilled and DFR is addressed as a relevant topic inside the organization. It is noticeable that these initiatives are not enough if a real investigation needs to be conducted.

*Level 3* Level 3 provides a solid base in performing DFR activities. At this level an organization has standardized forensic procedures, compressively documented processes and formal trainings. The involved staff has an acceptable understanding of DF and its consequences. This empowers an organization that potential failures in an early stage of a forensic investigation are prevented. According to Tan, the increased usability of evidences is an eminent aspect of DFR [34]. By having measures at this level in place can additionally save costs within a digital investigation.

*Level 4* Level 4 describes an advanced state of having DFR initiatives in place. Beyond the previous levels and aspects, this level focuses on a professional implementation of DFR. For example, DFR is an enterprise-wide and strategic issue. At this level the support of an executive manager is committed and various process improvement measures are in place.

*Level 5* The highest level of the model is represented as level 5. The achievement of this level implies a full implementation of DFR including a continuous improvement of DFR related measures and structures. With the definition of process improvement objectives, implementing formal staff training and a corresponding accreditation this level can be reached.

## 4 The digital forensic capability maturity model

Based on the development approach, suggested in Sect. 3, and the distilled requirement of DFR, presented in Sect. 2.2, the following DFR capability maturity model has been developed by conducting and presenting the various maturity levels of the DFR CMM. For each level the main characteristic processes, people and technology are examined and used in the description. The maturity level of the DFR CMM are described in Table 1.

Besides the first level, each maturity level needs every previous maturity level to be completely fulfilled. A specific maturity level can be seen as accomplished if all included PAs satisfy the highest capability level. In our approach each maturity level is aligned to a set of capability levels across the seven enabler of COBIT 5 [14]. These capability levels are defined in Table 2 and can be measured by querying an organization selected DFR related questions. These questions represent indicators which are present or not. Some measures for implementing DFR need the support by the management or governance of an organization. Due to the fact that the model is built by facilitating IT-Governance principles from COBIT 5, the enabler concept provides a future-orientated guideline for a continuous improvement within the organization. This approach results in an overview of goals the seven enablers need to achieve to successfully implement DFR. With this DFR specific CMM a comprehensive and detailed justification of the intended progress can be reached.

The relation between capability and maturity levels and their possible definitions are presented in Fig. 1. In this figure also a possible linkage between capability levels and the enabler concept of COBIT 5 is illustrated.

The capability level of a specific enabler can be determined by questioning a company or responsible person a set of indicators. Each indicator can be asked and evaluated individually.

In the context of implementing DFR, two different types of indicators are used. On the one hand, mandatory indicators are used to define measures or structures which are necessary to reach a specific capability level. These indicators need to be fulfilled by an adequate implementation within the organization. On the other hand, optional indicators are defined. These indicators are not compulsory. They can be fulfilled to support a specification or characteristic of DFR capabilities. Such elements are expressly welcomed but not an essential element of having DFR measures in place at the assigned capability level. However, these optional indicators can become mandatory in the future if the requirements in DFR are changing or an implementation of higher DFR capabilities is intended. They can be seen as suggestions for an optimal implementation of the capability level. In "Appendix 1" the Tables 4, 5, 6, 7, 8, 9 and 10 show mandatory and optional indicators for determining the capability level of an enabler. Table 11 provides an overview about the necessary capability levels per enabler for having a specific maturity level.

The minimal necessity to have DFR in place is the maturity *level 3*. As a negative side effect this could mislead managers to think the organization is fully prepared at this level. Even if the minimal level for DFR is reached by an organization, it is necessary to pursue a further development. This guarantees a higher application and faster response to changing circumstances around DFR. The higher levels, *Level 4* and *5*, assist to set up necessary requirements to faster adopt new demands in DFR.

**Table 1** Description of the defined maturity levels

| Level | Description |
|---|---|
| 1—Initial | No documentation is presented |
| | No communication structure is defined |
| | No training is in place |
| | No regulations are defined |
| | DF process is performed ad-hoc and without structure |
| | No DFR structure is in place |
| 2—Managed | Repeatable processes are in place |
| | Informal training is performed |
| | Minimal formalization is present |
| | A basic documentation is present |
| | Low or informal communication structure is defined |
| | DF related measures are informally or ad-hoc performed |
| 3—Defined | Documented processes are present |
| | Documented usage of tools and methods are present |
| | Standardized procedures are in place |
| | Documentation is reviewed and accepted |
| | Formal trainings are offered and conducted |
| | Formal regulations are in place |
| | Communication is defined and new employees are involved |
| 4—Quantitatively Managed | Minimal requirements for DFR are fulfilled |
| | DFR related process improvement measurements are in place |
| | Used documents are checked for alignment with goals & objectives |
| | Frequent communication to all staff is implemented |
| | A formal training and accreditation is in place |
| | Principles are accepted and followed |
| | Monitoring and regulation mechanism are established |
| 5—Optimized | Extended requirements for DFR are fulfilled |
| | DFR related process improvement measurements are in place and objectives are aligned within the organization government |
| | DFR related processes are continuously improved and measured |
| | Changes in the documentation structure are incorporated and clearly communicated |
| | Frequently and timely communication to all staff is implemented |
| | A formal training and accreditation is in place |
| | Legislation and laws are reviewed and DF aspects are integrated into procedures, documents and/or adopted to organizational structure |

**Table 2** Description of the defined capability levels

| Level | Description |
|---|---|
| 0—Incomplete | The DF related objectives are not reached |
| 1—Performed | The intended goals in DF are reached |
| 2—Managed | DF initiatives and activities are managed and not ad-hoc performed |
| 3—Completely defined | A standardized process for DF activities is in place. The procedures underlie a continuous improvement |

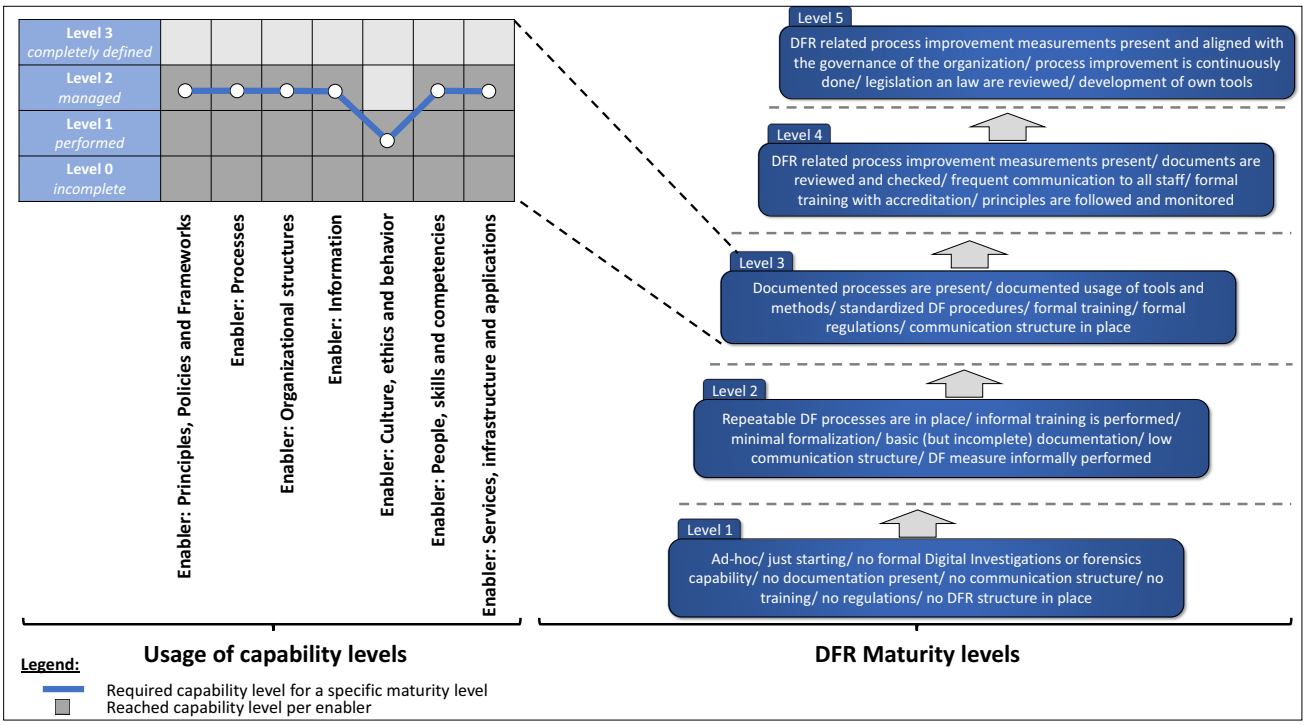


**Fig. 1** Maturity and capability levels of the DFR-CMM

## 5 Application of the model

The following section presents a prototypical implementation of the model to demonstrate the practical usage of the theoretical model. Furthermore, publicly available information about the Target Corp. Data Breach [32] is used for a small case study to determine the maturity level of the organization at the time of the breach.

### 5.1 Implementation

The previously proposed model for determining a company's digital forensic readiness maturity level is based on querying indicators to determine the capability levels. This mechanism was implemented as a web-based application.[1] The indicators shown in the Tables 4, 5, 6, 7, 8, 9 and 10 in Appendix A have been translated into questions and stored in a MySQL database. The logic to determine the capability level and the maturity level was implemented with JavaScript. If a company undergoes such an assessment, a skilled professional can evaluate the indicators, grouped by COBIT 5 enablers, according to the current situation. As soon as sufficient questions for the determination of the maturity level have been answered, the tool presents the result. The result consists of the capability levels of the company per enabler, the level of maturity achieved and a list with the answered indicators. With these results, specific areas of the company can be developed to achieve the DFR objectives.

### 5.2 Evaluation of the model

The applicability of the model is tested by using information about the Target Corp. Data Breach [32] as a baseline for a case study. In November and December 2013, the company suffered a until then unique security breach. Attackers penetrated the company's network via a third party vendor and compromised point of sale devices with malware. This made it possible for the attacker to collect 40 million card numbers and 70 million personal entries. This data was afterwards offered for sale on the black market.

This case was chosen because it occurred despite enormous previously established IT security measures. The case has been under investigation for several years and faces significant barriers to capture the cybercriminals [32].

Subsequently, the seven enablers are examined according to the implemented measures for DFR before the incident. Further the level of capability of the respective enabler is determined and finally the level of maturity is derived.

[1] https://dfr-check.uni-regensburg.de/ (the source code of the assessment tool is available upon request).

**Enabler *principles, policies and frameworks*** The employed Chief Information Officer before the incident had no background in computer science. Management also decided not to follow warnings and advices of a recently installed IT security tool and decided not to re-evaluate the systems. In addition, advices from security experts to the management were ignored. The fact that after the incident the position as Chief Information Officer was filled with a candidate with the appropriate experience also shows that there was no knowledge present about the correct procedure in case of an incident. [33] The analysis of the case shows that the Target Corp. was repeatedly warned about the incident by the protection systems and that the employees did not initiate the correct actions [23].

This analysis allows to conclude that besides the management's lack of understanding of IT security measures, the establishment of suitable principles, policies and frameworks according DF measures was not fully established and therefore no regulations for DFR were implemented.

**Enabler *processes*** It can be assumed that the company has a good understanding of its business processes, since a crucial security function of the point of sale devices had just been deactivated in order to not slow down the check out process of the customer [33]. Target Corp. had implemented good IT security measures, but the handling of messages from the systems was not correct among the employees due to inadequate training [32]. As a result, the knowledge of a correct procedure in case of an incident could not be implemented.

**Enabler *organizational structures*** After the breach a new CIO was announced and a 100 million dollar plan for enhancing their security has been promoted. Therein the enhancement of security of various accounts as well as reviewing and limiting vendor access has been addresses. Especially the insufficient implementation of access control by different groups and third party partners made the attack feasible [32]. This allows the conclusion that central elements of the organizational structure were insufficiently developed.

**Enabler *information*** It is not clear whether sufficient internal information about the handling of digital evidence was available. However, it is well known that major investments were made in IT security tools and measures. These included the network security system named FireEye, which includes a Network Intrusion Detection System (NIDS) [32]. These tools usually also include possibilities to obtain evidence for a forensic investigation. Since different prevention functionalities were deactivated due to lack of knowledge of the administrators [32] it is assumed that further possibilities of the system were also not or insufficiently known among relevant stakeholder.

**Enabler *culture, ethics and behavior*** Little is known about the culture, ethics and behavior before the incident. It is assumed that the data breach was not performed or initiated by an insider [32]. However, employee awareness of IT security incidents was partially suppressed for business-enhancing convenience [23].

Therefore, for the use case presented here, it is assumed that a fraud intolerant culture exists in the company and that the employees do not hinder an investigation. However, in some cases this is overshadowed by measures that threaten IT security for the purpose of promoting direct business goals.

**Enabler *people, skills and competences*** It can be seen that before the attack, management had already been informed about IT security weaknesses but did not follow the recommendations of experts [33].

The lack of knowledge about the consequences of disabling important security warnings in intrusion detection systems combined with the result that employees still do not follow the procedure of the system is critical. This shows that the employees have been insufficiently trained [23]. It is assumed that in this use case not only the teaching of relevant IT security skills and competences but also the DF trainings have failed.

**Enabler *services, infrastructure and applications*** The Target Corp. had extensive ambitions to keep the IT security in the company up-to-date and running. Before the data breach, for example, a malware detection tool was implemented in the company for 1.6 USD. In addition, extensive evaluations of the existing IT security measures were regularly undertaken. [23]

In summary, Target has taken extensive measures to increase IT security and has even deployed a network intrusion system. As mentioned before, these tools also have the ability to acquire usable evidence. For this use case the expected capability level in the area of *services, infrastructure and applications* is therefore defined as *managed*.

The following Table 3 presents the specific levels of capability of the seven enablers and provides the basis for determining the level of maturity of the entire company with regard to DFR.

Based on the previously determined levels of capability of the seven enablers in Table 3, the maturity level "*1—Initial*" for DFR can be determined for the Target Corp. at the time of the attack in November 2013. This maturity level implies that not all measures to meet the DFR objectives are in place within the organization. The use

**Table 3** Determined capability levels per enabler of the use case

| Enabler | Defined capability level |
|---|---|
| Principles, policies and frameworks | 0—Incomplete |
| Processes | 1—Performed |
| Organizational structures | 0—Incomplete |
| Information | 0—Incomplete |
| Culture, ethics and behavior | 1—Performed |
| People, skills and competences | 0—Incomplete |
| Services, infrastructure and applications | 2—Managed |

case shows that an insufficient understanding of DFR by the management also has a negative impact on all areas throughout the company. The insufficient degree of maturity in the presented case study also supports the thesis that till now the criminals behind the cyber attack could not be prosecuted due to insufficient evidence. In addition, the investigation has already cost an enormous amount of time and money. This could have been mitigated by a company-wide implementation of DFR measures before the incident.

## 6 Conclusion and future work

A significant role of digital forensic activities was endorsed due to the increasing amount of threats to the information systems of organizations. If an incident occurs and all Information Security measures fail, a digital forensic investigation needs to be conducted.

The main goal of this paper is to develop a DFR specific CMM and to show, how its application can assist in implement DFR capability within an organization. Therefore, significant characteristics of being digital forensic ready have been used.

Due to a study of similar capability maturity models it was possible to determine the third level as an acceptable state to consider an organization as digital forensic ready. A concrete suggestion of a DFR specific model has been provided and reflected with the support of IT-Governance aspects and instruments. In addition, the proposed model was applied to an adapted use case and a maturity level of a specific organization was determined.

This work demonstrates the advantage by combining IT-Governance aspects with a capability maturity model. A majority of managers and decision makers know IT-Governance frameworks and may be familiar with their use. A broadly accepted, management oriented framework can be used to implement the necessary measures to reach digital forensic readiness within an organization. Decision makers gain a deeper understanding on what directions the organization needs to focus on. This approach also minimizes the risk of wrong investments and to put efforts into a wrong direction. A capability maturity model assists in this context as a compass navigation to the right direction. It is also a useful tool to determine the current state of ongoing implementation at any time. Due to the fact that some DFR initiatives need further assistance by the higher management, the combination of IT-Governance with the DFR initiatives gains further support. Nevertheless, the application of the DFR specific CMM needs to be evaluated in a real-world scenario with additional expert interviews and is part of future work.

The development and application of a capability maturity model is not a single incentive to assess the maturity level or to improve it. Moreover, the intention of implementing such a model is to establish continuous improvements in specific areas. The use of different types of indicators (mandatory or optional) also shows the temporary character of the capability assessment which is performed on a fixed moment. By rising threats and emerging technologies the measures and structures, previously assigned for the fulfillment of a capability level, could be outdated. This requires a modification and adjustment of the needed measures to reach a specific capability level.

However, assistance is provided by pointing out significant measures, needed to fulfill a desired level. This makes the model useful in practice. Also the continuous assessment and improving by using the capability maturity model can be supported.

**Acknowledgements** This article is an extended version of a paper presented at COMPSE 2018 (held at the Furama Hotel, Bangkok, Thailand, March 2018) which was kindly invited for a consideration in this journal. This work is partly performed under the BMBF-DINGfest project which is supported under contract by the German Federal Ministry of Education and Research (16KIS0501K).

## Appendix 1: Indicators for determining the capability level of an enabler

See Tables 4, 5, 6, 7, 8, 9, 10 and 11.

**Table 4** Indicators for the enabler *principles, policies and frameworks*

| Indicator | Maximum contribution (cap. level) | Type<br>m = mandatory<br>o = optional |
|---|---|---|
| Initiatives to raise awareness for DF activities are in place | 2 | m |
| Initiatives to raise awareness for DF activities are in place and continuously monitored | 3 | m |
| Governance and Management understand DFR initiatives | 1 | m |
| Governance and Management pursue DFR initiatives | 2 | m |
| Governance and Management are completely involved in planning DFR initiatives | 3 | m |
| Governance and Management support DFR related organizational changes | 2 | m |
| A change management is in place | 3 | o |
| Principles and policies according to a DF investigation are present | 2 | m |
| Employees take the principles of DF related actions seriously | 3 | m |
| Principles are clearly formulated | 2 | m |

**Table 5** Indicators for the enabler *processes*

| Indicator | Maximum contribution (cap. level) | Type<br>m = mandatory<br>o = optional |
|---|---|---|
| A basic understanding of the DF investigation process is present | 1 | m |
| A deep understanding of the DF investigation process is present | 2 | m |
| The support for the DF investigation process is continuously improved | 3 | m |
| Related sub-processes to DF are documented | 2 | m |
| Guidelines to prevent business interruption in the case of a DF investigation are defined | 3 | m |
| Process models of business processes are present | 3 | o |
| DF related processes are partially automated | 2 | o |
| DF related processes are partially automated | 3 | m |

**Table 6** Indicators for the enabler *organizational structures*

| Indicator | Maximum contribution (cap. level) | Type<br>m = mandatory<br>o = optional |
|---|---|---|
| Responsibilities for the case of a DF investigation are known | 1 | m |
| Responsibilities for the case of a DF investigation are defined | 2 | m |
| DF related decision-making guidelines are included in job-descriptions or roles | 3 | m |
| Rights within Information Systems are defined | 1 | m |
| Rights within Information Systems are defined and adjusted to prevent potential destroying or tampering of evidences | 2 | m |
| An Identity Management System is in place | 3 | o |
| Escalation rules are defined | 2 | m |
| Escalation rules are defined, reviewed and monitored | 3 | m |

**Table 7** Indicators for the enabler *information*

| Indicator | Maximum contribution (cap. level) | Type m = mandatory o = optional |
|---|---|---|
| Documents about the right handling of digital evidences in general are present | 1 | m |
| Documents about the right handling of digital evidences of all devices and systems within the organization are present | 2 | m |
| Documents about the right handling of digital evidences of all devices and systems within the organization are present and frequently reviewed | 3 | m |
| Information about DF investigations are available and accessible | 2 | m |
| Employee can contribute findings and knowledge regarding DF | 2 | o |
| Employee can contribute findings and knowledge regarding DF | 3 | m |
| The usage of tools for DF is documented | 2 | m |
| The usage of tools for DF is documented and continuously reviewed | 3 | m |
| Information about the usage of digital evidences in a law court is present | 2 | m |
| Information about the usage of digital evidences in a law court is present and frequently updated | 3 | m |
| Employees get frequent updates according DF related topics (e.g.: e-Mail, letter) | 2 | o |
| Employees get timely updates according DF related topics (e.g.: e-Mail, letter) | 3 | m |

**Table 8** Indicators for the enabler *culture, ethics and behavior*

| Indicator | Maximum contribution (cap. level) | Type m = mandatory o = optional |
|---|---|---|
| A fraud intolerant culture is present | 2 | o |
| A fraud intolerant culture is pursued | 3 | m |
| Open handling of mistakes and issues is present | 2 | o |
| Open handling of mistakes and issues is present | 3 | m |
| Anti-fraud ethics are established | 3 | m |
| A willingness to unveil fraud/crime is present | 1 | m |
| DF related activities are accepted within employees | 2 | m |
| Specific guidelines for potential fraud related situations are present | 2 | o |
| Specific guidelines for potential fraud related situations are present and reviewed | 3 | m |
| Employees do not hinder a DF investigation | 1 | m |

**Table 9** Indicators for the enabler *people, skills and competences*

| Indicator | Maximum contribution (cap. level) | Type m = mandatory o = optional |
|---|---|---|
| Employees understand the importance of digital evidences | 2 | m |
| Employees get informal DFR related training | 1 | m |
| Employees get formal DFR related training | 2 | m |
| The proper application of the knowledge is assessed regularly | 3 | m |
| Human resource division ensures the right amount of DF skilled employees | 2 | o |
| Human resource division ensures the right amount of DF skilled employees | 3 | m |

**Table 10** Indicators for the enabler *services, infrastructure and applications*

| Indicator | Maximum contribution (cap. level) | Type m = mandatory o = optional |
|---|---|---|
| Services, infrastructure and applications are documented | 2 | m |
| Services, infrastructure and applications are documented and continuously updated | 3 | m |
| Possibilities to retrieve log-files are known | 1 | m |
| Possibilities to retrieve log-files are known and the configuration is reviewed | 2 | o |
| Possibilities to retrieve log-files are known and the configuration is reviewed | 3 | m |
| An internal laboratory is present | 3 | m |
| A possibility to store and protect digital evidences is present | 2 | m |
| Tools and methods to produce forensically sound copies of hard drives and memory are present | 2 | o |
| Tools and methods to produce forensically sound copies of hard drives and memory are present and reviewed frequently | 3 | m |
| Own tools for DF related tasks are developed in a forensically sound manner | 3 | m |
| Methods to adjust infrastructure and applications are present | 3 | m |

**Table 11** Required capability levels per enabler for a specific maturity level

| Maturity level | Required capability levels per enabler | | | | | | |
|---|---|---|---|---|---|---|---|
| | Principles, policies and frameworks | Processes | Organizational structures | Information | Culture, ethics and behavior | People, skills and competencies | Services, infrastructure and applications |
| 5 | 3 | 3 | 3 | 3 | 3 | 3 | 3 |
| 4 | 2 | 3 | 3 | 3 | 3 | 3 | 2 |
| 3 | 2 | 2 | 2 | 2 | 1 | 2 | 2 |
| 2 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

## References


1. Ahmad, A., Hadgkiss, J., & Ruighaver, A. B. (2012). Incident response teams—Challenges in supporting the organisational security function. *Computers & Security, 31*(5), 643–652.
2. Becker, J., Knackstedt, R., & Pöppelbuß, J. (2009). Entwicklung von Reifegradmodellen für das IT-Management. *Wirtschaftsinformatik, 51*(3), 249–260. https://doi.org/10.1007/s11576-009-0167-9.
3. de Bruin, T., Freeze, R., Kaulkarni, U., & Rosemann, M. (2005). *Understanding the main phases of developing a maturity assessment model*.
4. Carrier, B., & Spafford, E. H. (2003). Getting physical with the digital investigation process. *International Journal of Digital Evidence (IJDE), 2,* 1–20.
5. Casey, E. (2005). Case study: Network intrusion investigation—Lessons in forensic preparation. *Digital Investigation, 2*(4), 254–260.
6. Chryssanthou, A., & Katos, V. (2012). Assessing forensic readiness. In *Proceedings of the seventh international workshop on digital forensics & incident analysis (WDFIA 2012)*.
7. CMMI Product Team. (2010). *CMMI® for Development, Version 1.3, Improving processes for developing better products and services*. no. CMU/SEI-2010-TR-033. Software Engineering Institute.
8. Cohen, F. (2010). Toward a science of digital forensic evidence examination. In K. P. Chow & S. Shenoi (Eds.), *Advances in Digital Forensics VI. IFIP Advances in Information and Communication Technology* (pp. 17–35). Berlin: Springer.
9. Dewald, A. (2012). *Formalisierung digitaler Spuren und ihre Einbettung in die Forensische Informatik*. Erlangen: Universität Erlangen-Nürnberg.
10. Dowdy, J. (2012). The cyber security threat to US growth and prosperity. In N. Burns & J. Price (Eds.), *Securing cyberspace: A new domain for national security*. Washington, DC: Aspen Strategy Group.
11. Elyas, M., Ahmad, A., Maynard, S. B., & Lonie, A. (2015). Digital forensic readiness. Expert perspectives on a theoretical framework. *Computers & Security, 52,* 70–89. https://doi.org/10.1016/j.cose.2015.04.003.
12. Grobler, T., Louwrens, C. P., & von Solms, S. H. (2010). A framework to guide the implementation of proactive digital forensics in organisations. In *ARES 2010, Fifth international conference on availability, reliability and security, 15–18 February 2010, Krakow, Poland* (pp. 677–682). IEEE Computer Society.
13. Inman, K., & Rudin, N. (2000). *Principles and practice of criminalistics: The profession of forensic science. Protocols in forensic science*. Boca Raton: CRC Press.

14. ISACA. (2012). *COBIT 5. A business framework for the governance and management of enterprise IT*. Rolling Meadows, IL: ISACA.
15. Ivtchenko, D., & Sachowski, J. (Eds.). (2016). *Implementing digital forensic readiness. From reactive to proactive process*. Cambridge, MA: Syngress.
16. Jacobs, S. (2017). *Reifegradmodelle* (August 2017). Retrieved August 21, 2017 from http://www.enzyklopaedie-der-wirtschaftsinformatik.de/lexikon/is-management/Systementwicklung/reifegradmodelle.
17. Karie, N., & Karume, S. (2017). Digital forensic readiness in organizations: Issues and challenges. *JDFSL*. https://doi.org/10.15394/jdfsl.2017.1436.
18. Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). *Guide to integrating forensic techniques into incident response*. NIST SP 800-86.
19. Kerrigan, M. (2013). A capability maturity model for digital investigations. *Digital Investigation, 10*(1), 19–33. https://doi.org/10.1016/j.diin.2013.02.005.
20. Kessem, L., Kuhn, J., & Mueller, L. (2015). *The Dyre Wolf Attacks on Corporate Banking Accounts*. Retrieved August 7, 2017, from https://portal.sec.ibm.com/mss/html/en_US/support_resources/pdf/Dyre_Wolf_MSS_Threat_Report.pdf.
21. Kitten, T. (2015). *FBI alert: Business Email Scam Losses Exceed 1.2 Billion*. Retrieved August 7, 2017, from http://www.bankinfosecurity.com/fbi-alert-business-email-scam-losses-exceed-12-billion-a-8506.
22. Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. (2017). DDoS in the IoT. Mirai and other botnets. *Computer, 50*(7), 80–84. https://doi.org/10.1109/MC.2017.201.
23. Manworren, N., Letwat, J., & Daily, O. (2016). Why you should care about the Target data breach. *Business Horizons, 59*(3), 257–266.
24. Meier, S., & Pernul, G. (2014). Einsatz von digitaler Forensik in Unternehmen und Organisationen. In *Sicherheit 2014: Sicherheit, Schutz und Zuverlässigkeit, Beiträge der 7. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V. (GI), 19.-21. März 2014, Wien, Österreich* (pp. 103–114). LNI, 228. GI.
25. Mouhtaropoulos, A., Grobler, M., & Li, C.-T. (2011). Digital forensic readiness: An insight into governmental and academic initiatives. In *Proceedings of the 2011 European intelligence and security informatics conference. EISIC'11* (pp. 191–196). IEEE Computer Society.
26. Palmer, G. (2001). A road map for digital forensic research. In *First digital forensic research workshop (DFRWS)*.
27. Pangalos, G., & Katos, V. (2010). Information assurance and forensic readiness. In A. B. Sideridis & C. Z. Patrikakis (Eds.), *Next generation society: Technological and legal issues. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering* (pp. 181–188). Berlin: Springer.
28. Reddy, K., & Venter, H. S. (2013). The architecture of a digital forensic readiness management system. *Computers & Security, 32,* 73–89. https://doi.org/10.1016/j.cose.2012.09.008.
29. Reyes, A., & Wiles, J. (2007). Developing an enterprise digital investigative/electronic discovery capability. In *The Best Damn Cybercrime (2007)* (pp. 83–114).
30. Rowlingson, R. (2004). A ten step process for forensic readiness. *International Journal of Digital Evidence (IJDE), 2,* 3.
31. Shedden, P., Ahmad, A., & Ruighaver, A. B. (2010). *Organisational learning and incident response: Promoting effective learning through the incident response process*.
32. Shu, X., Tian, K., Ciambrone, A. et al. (2017). *Breaking the target: An analysis of target data breach and lessons learned*. arXiv preprint arXiv:1701.04940.
33. Stanwick, P. A., & Stanwick, S. D. (2014). A security breach at target: A different type of bulls eye. *International Journal of Business and Social Science, 5,* 12.
34. Tan, J. (2001). *Forensic readiness*.
35. Yasinsac, A., & Manzano, Y. (2001). Policies to enhance computer and network forensics. In *Proceedings of the 2001 IEEE workshop on information assurance and security*.


**Ludwig Englbrecht** studied Business Information Systems at the University of Regensburg, Germany and at the Queensland University of Technology, Australia. His major field of study was IT-Security during his master studies. Currently he is a research assistant of Prof. Dr. Günther Pernul and Ph.D. student at the University of Regensburg. His research focus is on new approaches in IT-Forensics (Digital Forensics).

**Stefan Meier** received both the Bachelor of Science and Master of Science degree from the University of Regensburg, Germany. Prior to his current position as CEO at Meier Computersysteme GmbH he was a research assistant at the Department of Information Systems at the University of Regensburg, Germany. During this time his research was in the field of digital forensics, forensic readiness and enterprise forensics and thereby he received his doctoral degree.

**Günther Pernul** received both the diploma degree and the doctorate degree (with honors) from the University of Vienna, Austria. Currently he is full professor at the Department of Information Systems at the University of Regensburg, Germany. Prior he held positions with the University of Duisburg-Essen, Germany and with University of Vienna, Austria, and visiting positions the University of Florida and the College of Computing at the Georgia Institute of Technology, Atlanta. His research interests are manifold, covering data and information security aspects, data protection and privacy, data analytics, and advanced data centric applications.