Forensics Collaboration with Police

(Digital Forensic Readiness as Business Strategy)

ROGER LARSEN

Term Paper - Fall 2012
IMT4671 Organizational and Human aspects of Information Security

Friday 2nd November, 2012

Master of Science in Media Technology
5 ECTS
Department of Computer Science and Media Technology
Gjøvik University College, 2012

Abstract

Computer crime is an increasing threat, and malware is often strongly involved. Some malware (bots) wait for orders from a remote master (botmaster). This kind of malware can be used in targeted attacks against victims throughout the whole world. This is serious cyber crime. All that it takes to be infected by this kind of malware is; (i) bad luck, (ii) human failure and/or (iii) weak information security level. This can make a rather innocent enterprise partly involved in cyber crime.

In every computerized equipment we use, there will exist several traces as a result of our activity. When serious crimes are committed, these digital traces (or evidences) may be important for police. The search for electronic traces/evidences is often very time consuming. If police confiscate an the office locations and computer equipment in their search for digital evidences, the enterprise may in worst case go bankrupt.

If Small and Medium Enterprises (SMEs) are prepared to collaborate with police - they will most likely be able to reduce the interference of business. In Digital Forensics Investigation (DFI) this preparedness is called *DF Readiness*. In this paper we introduce D-FORCE - a DF Readiness framework that may help SMEs to be more prepared in collaboration with police investigators. D-FORCE focus on humans and organization and is optimized for SMEs.

We describe in this paper cyber crime threats, digital forensics basics and Norwegian police challenges (settlement and organization). We discuss the economic losses regarding computer crime. We describe previous DF Readiness approach and our D-FORCE framework proposal. Finally we suggest further work and summarize our findings.

Keywords: Information security, forensic investigation, digital forensic readiness, cyber crime cost, D-FORCE framework.

Contents

1 Introduction

"The only truly secure system is one that is powered off,
cast in a block of concrete and sealed in a lead-lined
room with armed guards."
– Gene Spafford

The last decades the technological evolution have been enormous in use of online services. We humans have in general embraced every digital equipment both at work and in our homes. We share information all around the world at the speed of light throughout our social networks [5]. For many businesses an Internet access is crucial - they get both their applications and their vital data online in so-called Cloud Services [25]. This is a challenging situation in an information security (IS) context.

1.1 The Threat

We often divide information security threats in two main categories - internal and external threats. In this article we will only mention the internal threat briefly. This is because recent studies & research shows that the external threats are very high. Verizon Business (in cooperation with several other large contributors) show in their report *"2012 DATA BREACH INVESTIGATIONS REPORT"* that external threats is estimated to be 98% in 2012. This is an 6% increase compared to 2011 [40] [9]. Nevertheless, we must never ignore the internal threats.

Internal Threat / Human Factor

Internal threat are most likely an unlucky and/or bad trained employee that makes an error. Employees may also be facing situations like offended/insulted and/or be psychic unstable (traumatized). Other strong motivation can be corruption, extortion, politically/idealistically etc. [18]. We humans may be the biggest threat to information security [30]. Partners/consultants also make an important group of threat to our enterprise. They often get trusted and can easily do a lot of harm.

External Threat

Cyber criminals are most likely well organized professionals that operates in smaller groups in countries with sloppy practice of law and legislation (development countries). They easily pay off police and government to be able to continue their illegal business. Some of these organizations have also web pages where you can order an attack (typical documents from your competitors/enemies). One large and infamous group is the *Russian Business Network*. They was very active from St. Petersburg in 2006-2007 and were most likely a part of Russian mafia. Recent years we have got much criminal activity from China - but this may just be a hide-out. In this professional category we also find government projects intended to e.g knock out an other country's atomic infrastructure (cyber defense as a national military defense strategy). The latter groups may not be a huge threat against general enterprises, but they participate in the development of advanced malware. This kind of malware will soon be available to criminals that develop it further in another form/shape (and signature).

Another threat are politically/idealistically motivated groups. This kind of groups recruits participants that deliberately get their trojan/bot (malware) installed to be a part of the actual campaign. *The Anonymous group* is an example of these attackers. They use the power of Social Networks (SN) in their communications and recruitment for voluntary. Their power have been demonstrated several times last years [26]. One example was triggered when several huge finance companies froze donations to WikiLeaks. This initiated the attack campaign named: "Avenge Assange". Anonymous group manage to knock out the websites and services from e.g. PayPal, Amazon, Visa, and MasterCard in many hours. This only demonstrated how powerful anonymous group is. Anonymous group is claimed to be responsible for over 50% of online data theft in 2011 [2].

Finally we have the individuals; script kiddies/hackers that works for themselves (drive by hacking) just showing off their skills. They can make much trouble, but are not in general so good in hiding their activity - so they are in general easy to track.

It is very easy to commit criminal activity on Internet. This can be don by ordering this service online or performing this yourselves. There are tons of of easily available tools with normal and easy installation

procedures and nice GUIs[1] with all the documentation that is needed. If installing this kind of software, the security software on the actual computer may not even complain (anti virus, firewall, IDS[2] etc.). This is because this kind of software also is used by the "white hat" guys to test their security. You even find frameworks in how to build your own malware. This kind of tools may of-course be used in training and/or penetration testing, but are most likely used as part of many attacks through cyberspace. An good example of this kind of tools are BackTrack

OECD[3] released in 2009 a publication called *"Computer Viruses and Other Malicious Software: A Threat to the Internet Economy"* [12]. This is a very good approach to better understand the threat from malware. Figure 1 illustrates the trends in malware for the last decade.

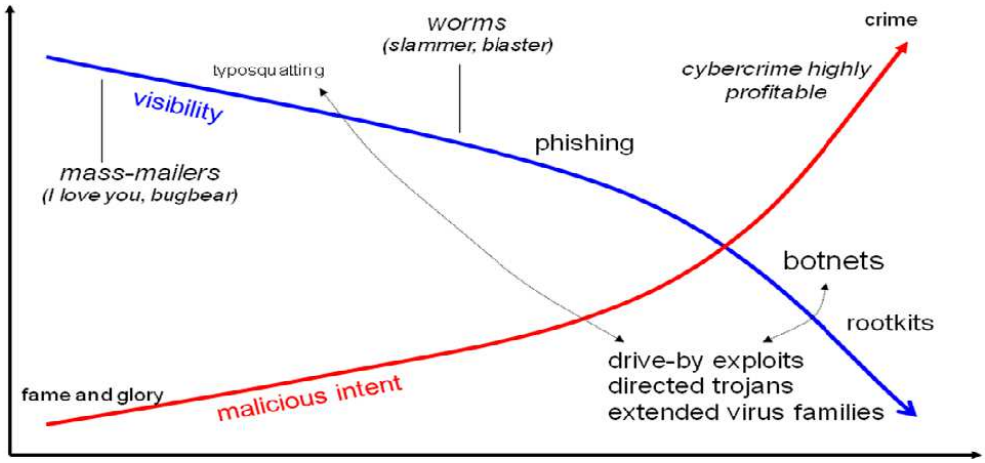

Figure 1: Visibility of malware vs. malicious intent.

The illustration show that malware are in general getting more complex and the malicious intents are increasingly. This is a scary scenario. Source originally from the Dutch government's CERT[4] (`WWW.GOVCERT.NL`).

Malware in general will probably "live on Internet" for a long period of time (years) without any people actively administrate/controls it. This is because there most likely will exist some old and/or weak operating systems that is unpatched and/or without anti virus.

General sources:[10] [40] [34] [14].

Examples of Advanced Malware

- Zeus [11] is a complex malware (botnet). Zeus was huge in 2009 and FBI claims that the criminals behind this malware stole over US $300.000.000 the first year.
- Stuxnet [35] is a large and complex malware that most likely are developed by some government. It was initial built to attack Siemens PLCs[5] and change alter their programming. This may be one of the first government developed malware targeted to use in a national cyber defense. Stuxnet was first detected in July 2010 attacking Iran's atomic industrial plants. The costs this malware have produced is of-course enormous.

1.2 Motivation / Limitation / Outline

In this paper we describe the need for forensic readiness in Small and Medium Enterprises (SME). We hope to motivate the readers to implement forensic readiness in every SME (as part of the emergency plan / business continuity plan). We hope that this paper will help SMEs in their DFI readiness processes.

[1]GUI = Graphical User Interface.
[2]IDS = Intrusion Detection System.
[3]OECD = The Organization for Economic Co-operation and Development.
[4]CERT = Computer Emergency Response Team.
[5]PLC = Programmable Logical Controller (industrial computer unit).

We have in this paper focused on forensic readiness in Digital Forensics Investigation (DFI) in general and especially in SME. When we write the term "police" we refer to "The Norwegian Police" unless otherwise stated. We lack detailed description of the Norwegian police's DFI procedures – this is most likely because of secrecy (database- and web search + several email and telephone calls gave no results).

We initially describe the threats regarding especially cyber crime. We explain the Norwegian settlement and the police organization. We cover typical incidents and the economic loss in cyber crime. We further explain the basics of DF readiness and discuss some previous work including a new standard. We present a framework for better collaboration with SMEs: D-FORCE. We finally suggest further work and summarize our findings.

2 Norwegian Settlement

"There is so much space in Norway".
– Norwegian tourist

Norway is a long country with settlement spread all over. The population in Norway are rather small: we passed 5 million 19 March 2012 [22]. Compared to rest of European and especially Asia we have a lot of space in Norway. The spread settlement in Norway is a challenge for government services (among others). Norway is 1.752 km long in straight line, width varying from 6 to 430 km. The illustration in figure 2 show the population in 2009 [39].

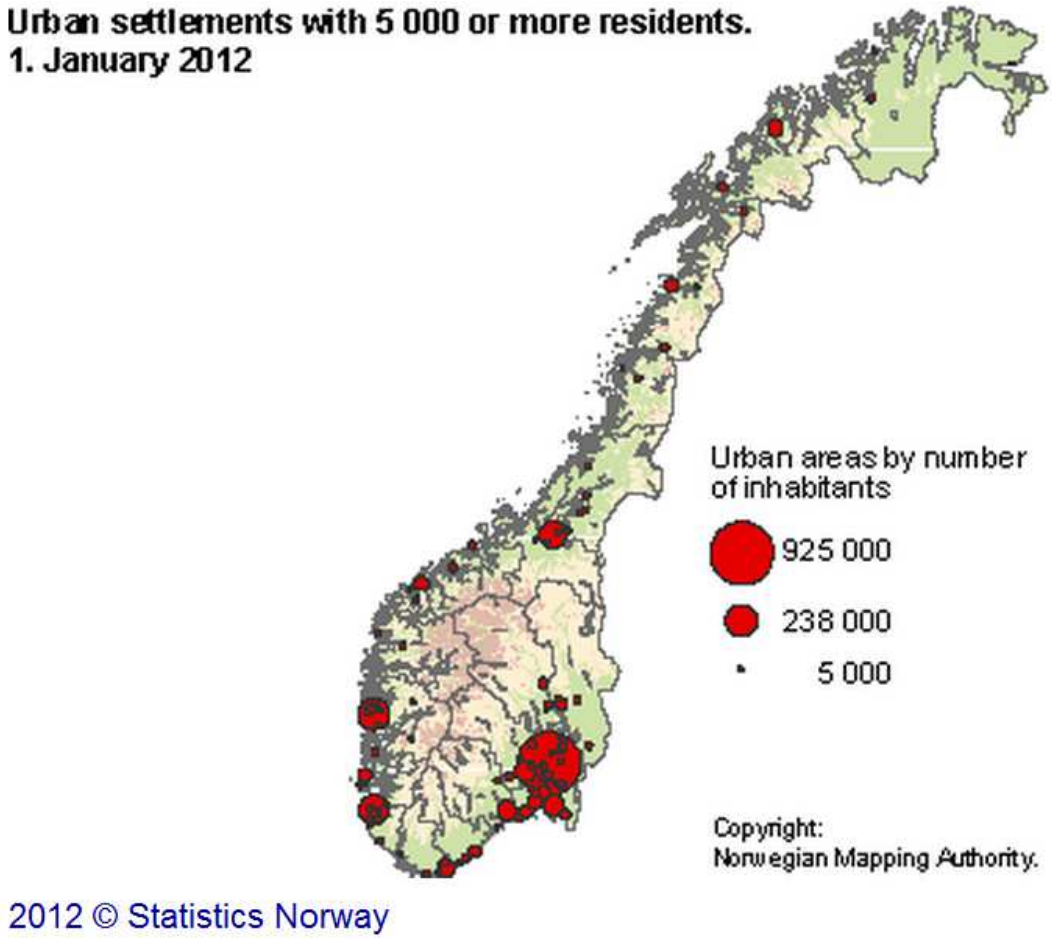

Figure 2: The Norwegian Settlement.

3 Small and medium enterprises - SME

"We have no CEO's or directors,
the owners just discuss and take decisions".
– Unknown, small Norwegian SME

3.1 Definition of SME

Norway is a member of European Free Trade Area (EFTA) and in this context The European Union's definition of SME (EU recommendation 2003/361 [37]) is the current (cited):

> *The category of micro, small and medium-sized enterprises (SMEs) is made up of enterprises which employ fewer than 250 persons and which have an annual turnover not exceeding EUR 50 million, and/or an annual balance sheet total not exceeding EUR 43 million.*

3.2 Norwegian employee distribution in SMEs

Table 1 show the employee distribution for SME in Norway 2009. Please note that over 70 % of all employees in Norway works in SME's. Of this group 24,8% are in the category 10-49 employees [23]. The numbers are closely related to the Norwegian settlement described in section 2.

# employee	Total # employee	%
1-4	327917	18,3
5-9	180136	10,1
10-49	442564	24,8
50-99	144763	8,1
100-249	181561	10,2
>=250	510638	28,6
Total	1787579	100,0

Table 1: The employee distribution in Norwegian SME 2009.

3.3 SME and the usage of ICT

Nowadays, most SMEs make use of information and communication technology (ICT). In 2011, 89-95% of Norwegian SMEs from 10-100 employees had an Internet connection[21]. This tell us that SMEs in Norway are very dependent on Internet in their daily business.

3.4 Small and Medium Enterprises are popular targets

Small and Medium Enterprises (SMEs) are often popular targets in cyber crime. This may be due to several reasons. The smallest SMEs may typically be very focused of their core business production/service and do not focus on computer routines/knowledge and information security. SMEs do in general not consist of large administrations.

4 Norwegian Police

"When we think computers may include important evidences,
we confiscate them and ship them to the experts."
– Per Norstrand, Police Chief Superintendent, Austevoll local police

4.1 Police Organization

The Police are organized under the government's *"Ministry of Justice and the Police"* and *"National Police Directorate"*. In 2010 there where roughly 13.000 employees divided into 27 regions. In every region there are several rural and local police stations. Please find the map of Norwegian Police Organization in appendix B [19].

4.2 General Police Investigation

The police force are in general known to be well trained and prepared for most situations. In a national survey in 2010 focusing on the citizens experience/relation, 86% of the citizens had trust in police [38].

With enough material/information collected they must build up the timeline[6] and document; (i) chain of custody, (ii) evidence integrity, (iii) objectives and (iv) methodology. They finally have to report and document their findings in an easy readable plain English report for the court.

A thorough systematically and efficient work following police procedures are important to build up a strong case without destroying/loosing evidences. In Norway we have a humanistic and highly democratic government that gives every citizen strong rights even under suspicion of having committed a crime. Norwegian law and legislation strive to meet the expression *"innocent until proven guilty"*. If any citizen are found suspicious of committing a crime - s/he will be given a lawyer payed by the government during the case.

4.3 Kripos

In more challenging cases where assistance is needed, the *National Criminal Investigation Service*, Kripos[7] [17], is involved. Kripos is the police's special agency whose task is to combat organized and other serious crime.

Datakrim division (eng. computer crime division) is a separate division in Kripos. Datakrim consists of lawyers, civilian and police trained personnel. People in Datakrim division is involved if any police region need assistance regarding DFI. Datakrim consists of four sections [33]:

- Section for analyses and investigation in malware and hacking.
- Section for electronically evidence: people that performs computer forensic investigation
- Section for communication and data interception
- ICT Management Section: handles and support the large amount of data material in Kripos

4.4 Police Challenges in Forensics Investigation

Centralized expert knowledge

With our widespread settlement and many small municipals (often less than 1000 citizens), police are facing huge challenges if expert knowledge is needed. Kripos may travel many hours (or worst: days) to be physical on the crime scene.

Continuously development of new ICT technology

The Police have also experienced the challenging technological race. Especially the Digital Forensic Team (Datakrim) is criticized in the following references. However, Datakrim can not take the blame alone - the organization may be to small for the amount of work they are ordered.

[6] A timeline is a list or illustration of events in a chronological order.
[7] Kripos is an abbreviation for **Kri**minal **Po**liti **S**entralen (Norwegian)

A Police Directorate Report, August 2012

The police directorate published in August 2012 a report written by several internal sources in the police [20]. This report seems very honest/truthful. Here are some of its conclusions:

> *"The fast development in technology is a challenge in the police"*
>
> *"More crimes would have been solved by more use of DFI."*
>
> *"Many crime cases involving ICT equipment are dismissed because of missing DFI expertise and personell"*

Torben Strand's Master thesis, July 2012

Torben Strand's master thesis finalized in July 2012 concludes also on weakness regarding forensics in Norwegian police (cited) [33]:

> *"Both police computer forensic investigators and the organization (leaders/management) lack (enough) knowledge in digital forensics"*

The 22 July 2011 Report

The report after the horrifying incidents 22 July 2011 in Oslo and Utøya, Norway concludes on several critical issues in the police:

> *Missing emergency plans for overlapping major incidents*
>
> *Organizational weakness in collaboration between police regions and stations*
>
> *Much computer and communication equipment are outdated (e.g. emergency radio)*
>
> *Poor qualifications regarding this kind of attack both in command unit and leadership*

Court of justice and new ICT technology

The new technology also gives challenges in the court of justice. It is typical easier to support a new decision based on other previous convicted cases. When new technology is introduced as evidences in a case - it will take more time to conclude on this case. The price (in time and money) for a fully analyzed digital evidence may be difficult to fulfill because the lack of expert knowledge. This time and money obstacle may force the judge(s) to ignore the digital evidence of new technology.

5 Incidents

"There is no such thing as an isolated incident."
– David Lacey

Incidents do happen - whether technical equipment breaks down or human error occur. Unfortunately, most any individual or organization may be a victim of these cyber criminals. All that it takes is; (i) bad luck, (ii) human failure or (iii) weak information security level. Sooner or later at least one of these categories will end with malware installed in a internal/trusted computer. An enterprise with computers infected with evil malware can be very critical to their business services. They may also be seen on as criminals by police and may be directly or indirectly involved in time consuming forensic investigation processes.

5.1 Type of Incidents

The following are examples of serious criminal activities in our SME context:

- Terror
- Murder

- Child pornography
- Theft/Robbery/Burglary
- Economic fraud
- Corruption

The following are examples of ICT related incidents in SMEs context:

- Loss of physical equipment; (i) computers, (ii) servers, (iii) network routers etc. (e.g. theft).
- Loss of services; (i) hardware or software failure on internal equipment, (ii) external services breakdown (e.g. bad maintenance, weak contracts).
- Human error (e.g. stress, lack of knowledge and/or training).
- Malfunction in software (e.g. bugs).
- Internal and/or external access violation (e.g. malware, intrusion).
- Criminal cyber activity (e.g hacking internal and/or external).

The following are examples of cyber crime incidents in SMEs context:

- Online fraud
- Scareware
- Identity theft
- IP Theft
- Espionage
- Customer data loss
- Online Theft
- Extortion

5.2 Time is Money - Cost vs Expenses

The largest category in SME (249 employees) may have time and money to make bulletproof policies, procedures and education plans. Nevertheless, there are still humans involved - and humans do make mistakes [7]. The average enterprise in SME category will most likely not have staff that works 100% with IS - it is more likely that the manager do this himself and/or use external consultants.

A police investigation will in worst case be a very expensive process if the SME have missing business continuation plans. If the police conduct a search for evidences on the SMEs premises this will most likely block the enterprises chances to proceed as normal for many days. This kind of scenario may end up in seizure of several important ICT equipment that takes a lot of time & money to both physically buy and configure, and this is the easiest part of the recover process.

For a SME a restore process after any incident may be "quick and dirty" because of its cost. Time is money and every hour (or minute) without access to Internet and/or file servers may damage an SMEs budget and income in large scale (and in worst case go bankrupt). The nature of DF investigations is that the better prepared an enterprise are - the less interference to core business.

5.3 Incident Lifecycles

Sommer describes the lifecycles of an incident very comprehensive in his guide for forensics readiness (by IAAC[8])"[32]. We have simplified the list in table 2. Please find the illustration in figure 3 which in general show how time consuming an forensic investigation process may be.

[8]The Information Assurance Advisory Council (IAAC) is a private sector led, cross industry forum dedicated to promoting a safe and secure Information Society in UK `http://www.iaac.org.uk/`

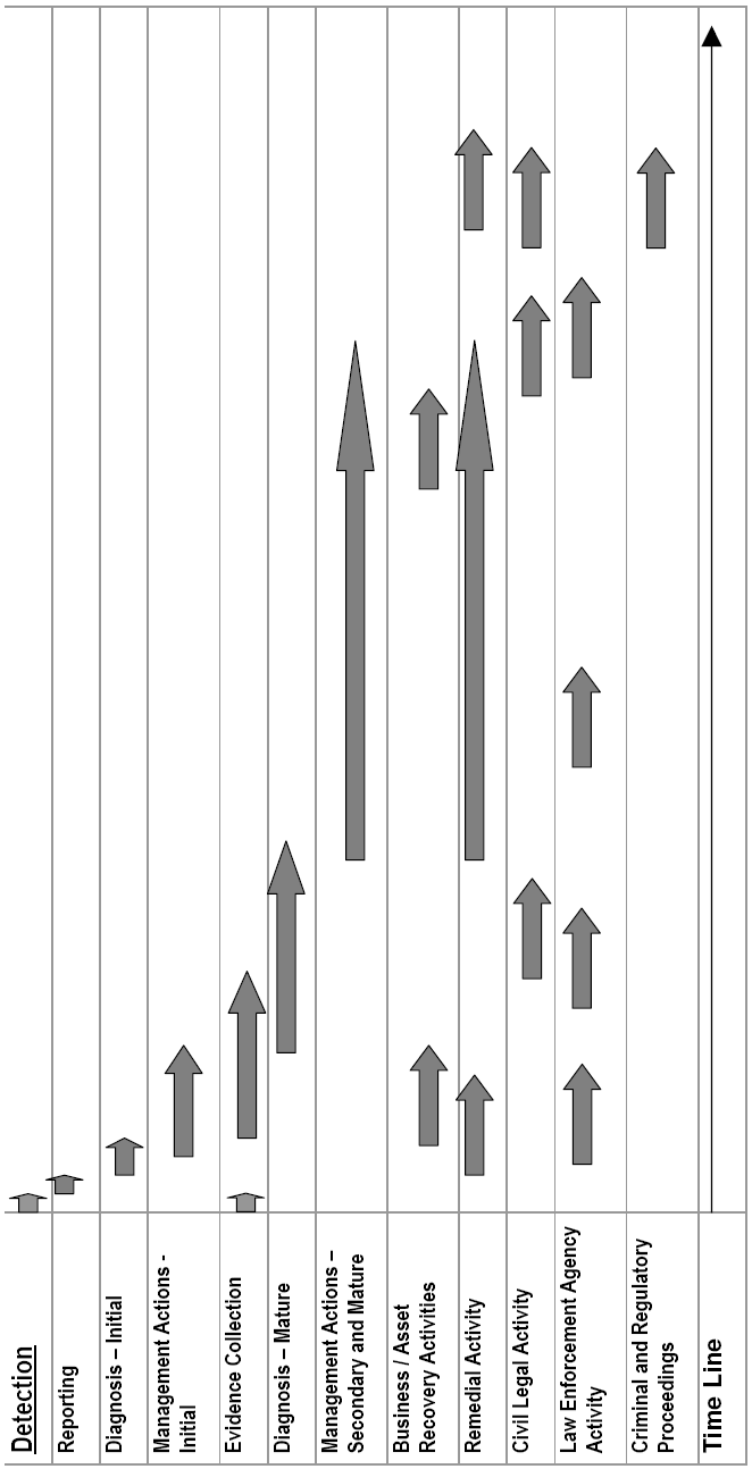

Figure 3: The Life-Cycle of incidents illustrated [32].

5.4 Factors that affects the DFI process

The following factors will directly influence the time and cost of an police DFI process:

- Collaboration with police (will employees in SME resist?)
- Have digital evidences deliberately been tampered with (eager employees in restoring situation?)
- Existing ICT with logs (firewall, IDS, etc.)
- Time from incident to investigation on site starts (how long must the DFI expert travel?)

When an SME are facing an DFI process they are legally obligated to participate. Police are entitled to confiscate the SMEs locations and/or ICT equipment where a crime has been committed. If an SME refuses to

Phase	Description
Detection	The first signs of the actual incident.
Diagnosis, initial	What happened? Can we reduce the extent of this incident?
Management actions	The management are presented the initial diagnosis and will decide what action to perform.
Evidence collection	Collect traces/evidences if possible.
Diagnosis, mature	Was the initial diagnosis correct? Perhaps change the incidents extent.
Management actions	The management are presented eventually new/mature diagnostics and will decide what action to perform.
Business/asset recovery activity	How can we restore our situation? Execute business continuation plans if possible.
Remedial activity	Document incident to learn and improve.
Civil legal activity	If any crime have been committed - the police will be involved.
Law enforcement agency activity	Depending on the extent of the case - the law enforcement will be engaged.
Criminal and regulatory proceedings	Complex cases will use a lot of time in court.

Table 2: The life-cycle of incidents - different phases explained.

collaboration with police, they will most likely be prosecuted for refuse to work. The latter is never an option unless very good reasons exists.

6 Economic Loss due to Computer Crime

There are three kinds of political accuracy: Lies, estimations and statistics.
– Roger Larsen's rewriting of Mark Twain

There are endless of examples where computer crime incidents are directly the root cause of great economic losses. Some examples are listed below:

- A small New York marketing firm "Little & King LLC" faced bankruptcy after a computer virus infection that cost the company USD 165.000 [16].
- The Dutch bank, Robobank, was knocked offline/unavailable for most of the time during two days in February, 2011 [3]. The attack method was so-called DDoS[9] which is a targeted attack from many different sources. For banks this long time may be crucial for business.
- Sony Portugal was in June 2011 hacked by some Lebanese hackers. They most likely stole internal documents and source code [41]. This kind of incidents may reduce market value for a long time.

6.1 Loss in Several Stages

Economic loss comes typical in several stages. We spend time and money in the following stages regarding computer crime; (i) proactive efforts, (ii) during the incident(s) and (iii) the recovery process(es). We divide the last parts in our paper using the terms direct & indirect losses.

Proactive Efforts In this stage we use a lot of time & money to secure our SMEs assets to be prepared for an incident. We invest in firewalls, intrusion detection systems, antivirus systems and monitoring systems etc. We train our ICT personnel to operate and manage the hardware and applications. If the threat level was not that high as it is today on Internet - we would of-course have used less money in this phase.

[9] DDoS = Distributed Denial of Service

Direct Losses When burglars steal computer equipment the loss is directly; (i) lost physical computer, (ii) lost important documents (stored in the actual computer), (iii) lost money from our accounts, (iv) damaged office doors and/or windows etc.

Indirect Losses The indirect loss may be the biggest part. We need to "clean up"/recover after an incident. This may include a lot of man hours in collaboration with police investigators and several days without being able to use the normal offices. Other indirectly losses are typical; (i) important documents that reveals our business strategy, (ii) identity/privacy information, (iii) source code of closed software application(s), (iv) reduced trust from customers and partners etc. Information and especially identities are the new currency.

There are also a psychic part of every incident. If the burglar incident was a violent/scary situation - we get psychic traumas. This kind of trauma can make employees sick for long term. We may also get a period with "over awareness" in the organization. Both these situations can be very negative to an SME after a major incident. The message here is that the extent of an economic loss may be difficult to conclude on before history reveals it.

The physical objects are most likely the smaller parts of the incident cost.

6.2 Under-reported Incidents

Enterprises are not legally ordered to report incidents involving financial loss (both direct and indirect). Even if they was legally committed - we would probably end up with huge numbers of under-reported incidents. Under-reporting by enterprises are most likely because of the following reasons:

- They will not make to much noise/fuss
- They will not be embarrassed
- They will not publish/report their internal failures
- They see on these incidents as less important
- They may end up keep quiet as a result of a negotiation with the involved (whom they can discharge)
- They lack confidence in police and legislation (investigation takes time!)
- They may be unaware of the actual incidents and economic loss

6.3 Computer Crime in Norway

NSR Survey The Norwegian Industrial Security Council (Næringslivets Sikkerhetsråd,NSR) published in August 2012 a report regarding computer crime in Norway, Mørketallsundersøkelsen 2012 [31]. This report try to estimate the amount of dark figures / unreported computer crime incidents. This work is a comprehensive cooperation with several Government organizations and major enterprises in Norway.

They included 6000 Norwegian organizations in their survey (2011). 4500 private enterprises (both listed on stock exchange and limited) and 1500 government organizations. They got only 886 answers which gives a response on 15% (and then high uncertainty to figures).

The number of officially reported computer crime incidents in 2011 was 361. The NSR report estimates the actual number of incidents to be 44.800. This official reported incidents is below 1% of the estimated. The NSR report have estimated the total loss due to computer crime in Norway to be NOK 20.000.000.000. They have based this assumption on the UK Cabinet Office research [24].

Table 3 show the estimated distribution of computer crime incidents. Table 4 show the percentage of organizations that reported one or more of the actual incident. Figure 4 illustrates the distribution in computer crime; (i) traditional, (ii) common and (iii) cyber crime. Please note that cyber crime makes appr. 40% of all computer crime.

PwC Survey PwC[10] published in November 2011 results from a cyber crime survey in 2011 [27]. 67 enterprises was included in the Norwegian part of the world wide survey. They found that 25% of all enterprises had incidents regarding cyber crime. 55% of them answered that they needed external help to recover from the actual incidents.

[10] PwC is a brand under PricewaterhouseCoopers International Limited. They are a network of firms in 158 countries with close to 169.000 people who delivering quality in assurance, tax and advisory services.

#	Estimated Distribution of Incidents:	%
1	Computer intrusion / hacking	7,1
2	Unauthorized changing/deletion of data	5,1
3	Targeted attacks (denial of service (DoS & DDoS))	2,0
4	Online credit card fraud	66,5
5	Abuse of ICT equipment	5,8
6	Sharing illegal/copyrighted material	13,2
7	Theft of information	0,2
8	**Total**	100,0

Table 3: Estimated distribution of computer crime incidents.

#	Actual Reported Incidents:	%
1	Computer intrusion / hacking	3
2	Theft of information	1
3	Unauthorized changing/deletion of data	3
4	Abuse of ICT equipment (PC/Network/servers)	5
5	Sharing illegal/copyrighted material	4
6	Targeted attacks (denial of service (DoS & DDoS))	2
7	Threats/extortion of attacks to ICT systems	0
8	Online credit card fraud	2
9	Theft of ICT equipment (PC, server, mobile storage, mobiles etc)	13
10	Loss of privacy data	1

Table 4: Computer crime incidents actual reported.

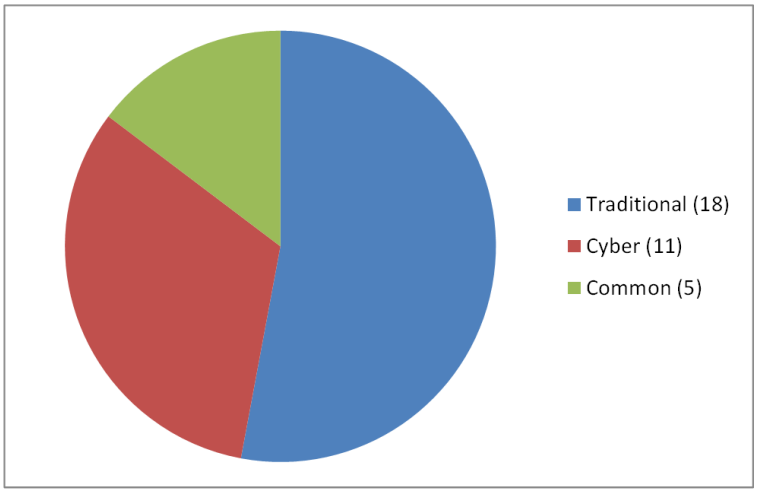

Figure 4: Traditional computer crime vs. Cyber Crime.

6.4 Cyber Crime in UK

UK Cabinet Office & Detica[11] published a report in February 2011: *"The Cost of Cyber Crime"* [24]. This is a very comprehensive work that explains the threats and how the cyber crime economy works. They estimates that cyber crime costs GB £27.000.000.000 in 2010.

[11]Detica is part of BAE Systems, a global defence and security company with over 100,000 employees worldwide.

6.5 Comparison - Norway vs UK

With the use of a CPI[12]= +4% we end up with UK cyber cost GB £ 28.080.000.000 for 2011. Converted to NOK with 2011's average exchange rate GB £1 = NOK 8,9841[13] we end up with **NOK 252.273.528.000**.

Population in UK is calculated (using 2012 figures initial) to be **61.838.395**[14]. Norway had January 2011 the population: **4.985.870**[15]. When the losses are divided with population - we get the figures found in figure 5.

United Kingdom:	**4080 NOK/citizen**
Norway:	**4011 NOK/citizen**

Table 5: Loss divided with citizens.

Description	**UK**	**NOR**
GDP per capita in PPS	108	189
Real GDP growth rate - volume	0,9	1,4
Average Citizen per km^2	254	16

Table 6: National statistics - UK vs Norway.

Comments to comparison

We where a bit surprised by how close Norway and UK ended in figures above. We expected these figures to have more distance. Norway is a very wealthy nation with it's oil income, the GDP[16] is almost double as much as average for Europe. See figure 6. Souurce: European Union's Eurostat.

Norwegians are known to be very interested in new technology.This is much likely because of our high developed nation with high standard of living. This may improve our turnover regarding new computer equipment with improved/more secure operating system.

However, Norwegians may be a bit more naive in our social skills compared to UK. We have this spread settlement and large amount of small cities/villages. On the Norwegian countryside we do not lock either houses or cars. The horrifying terror incidents that happened 22 July 2011 was a serious "wake up call" for Norwegians regarding our low security awareness [13]. This evaluation report showed that the terrible actions was totally unexpected for government and police.

These characteristics of Norway may explain why we ended up so close to UK in the figures.

[12]CPI = Consumer Price Index

[13]Norges Bank exchange rate statistics `http://www.norges-bank.no/no/prisstabilitet/valutakurser/gbp/aar/`

[14]UK Office for National Statistics - Population 2012 `http://www.ons.gov.uk/ons/taxonomy/index.html?nscl=Population`

[15]Statistics Norway - Population 2011 `http://www.ssb.no/minifakta/main_03.html`

[16]GNP - Gross Domestic Product

7 Digital Forensics

"Forensic scientists are not policemen.We are scientists.
We deal with these matters objectively.
We do not [act] on our suspicion."
– Cyril Wecht

Forensic investigation is an ancient science of using expert knowledge for solving crime [29] [8]. In the early days the investigators tried to discover how the victim(s) was killed – by; (i) knife, (ii) scythe or (iii) axe. Today, we may build up the whole detailed scenario regarding most crime cases (depending on time spent).

The term Digital Forensics (DF) is the forensic process where we use basic investigating processes on digital/electronic evidences [1]. With several kind of portable computers and smart phones, in addition to new cloud computing[17], we humans leave a lot of digital traces (evidences) all the time.

In DF investigations we need expert knowledge in computer science to handle several specialized tools in addition to well working methodologies in cases with digital evidences [6].

Examples of places where we may leave traces in business location(s):

- Computers
- Mobile Phone (Smart Phone)
- File-, Database-, Email- and Print Servers etc.
- Telephone System
- Network Equipment (Firewall, WiFi, IDS etc.)
- Internal Alarm-, Access-, Surveillance- and Monitoring Systems

Examples of places where we may leave traces outside business locations(s):

- Telephone Service Provider (Mobile- & Plain Old Telephone System (POTS))
- Application Service Provider (ASP)/Cloud Services
- Internet Service Provider (ISP)'s Network Equipment (Firewall, WiFi, IDS etc.)
- Social Networks Services (Facebook, Twitter, Google+ etc.)
- Email- & Web servers etc.
- Public Alarm-, Access-, Surveillance- and Monitoring Systems

In DF the practical challenge is in general the large amount of data that needs to be handled/processed. This makes this kind of cases complex and comprehensive to investigate.

The typical digital forensics investigation process are shown in figure 5.

Identification We need to identify all ICT equipments and their clock and timezone

Collection We need to collect the desired data evidences in a forensic sound manner

Examination We need to filter out the interesting information in the huge pile of data

Analysis We need to analyze the data collected and build up the chain of custody (at this stage advanced computational and statistical methodology are often used (e.g data mining and machine learning techniques))

Reporting We need to write an easily readable report in plain English with chronological listed events (including e.g timeline)

[17] Cloud computing = the practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer [25].

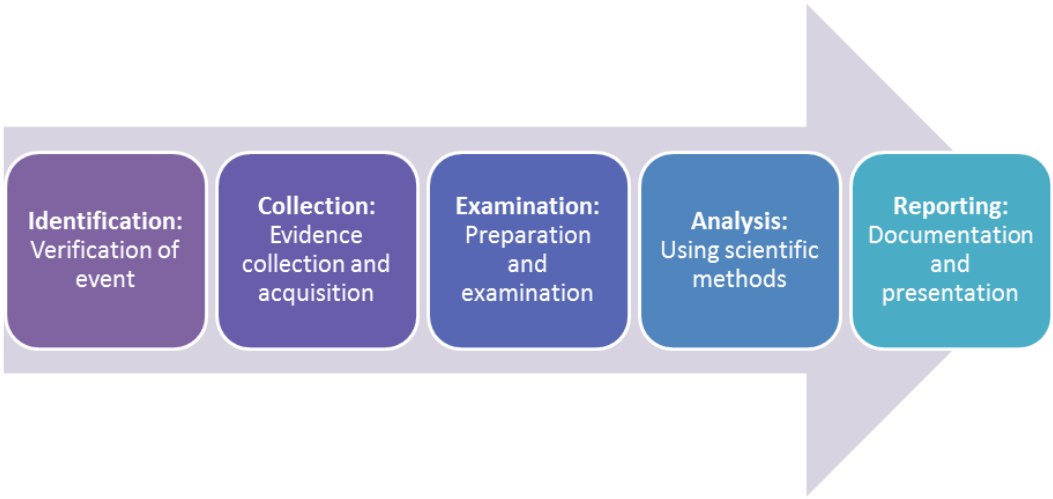

Figure 5: Typical Digital Forensics Investigation Process.

8 Previous Work

"If I have seen further it is by standing on the shoulders of giants."
– Issac Newton

We will mention and describe some previous work regarding DF Readiness in this section. There have been proposed several framework in DF readiness.

8.1 Forensic Readiness: John Tan, 2001

The term "Forensics Readiness" was introduced by Tan in 2001 [36] [4]. Tan described the main goal with forensic readiness; (i) maximize the usage of internal digital traces and (ii) minimize the cost of an forensic investigation. Tan further describes how costly minor incidents can be. The main part of his article describes; (i) how logging is done, (ii) some different popular operating systems properties and (iii) how one can collect evidences in different kind of computerized equipment and systematize them. The last part is how to handle the actual evidences.

The article is written for computer scientists and not for nontechnical management/leaders. It is written in a taxonomy way and makes us focused on how small actions can save enterprises a lot of money.

8.2 A Ten Step Process for Forensic Readiness: Robert R Rowlingson, 2004

Rowlingson published in 2004 an article in *International Journal of Digital Evidences (IJDE)* [28]. This article introduces DF thoroughly with descriptions of previously work. Rowlingson's main part of the article is the following ten steps (quoted):

1. Define the business scenarios that require digital evidence.
2. Identify available sources and different types of potential evidence.
3. Determine the evidence collection requirement.
4. Establish a capability for securely gathering legally admissible evidence to meet the requirement.
5. Establish a policy for secure storage and handling of potential evidence.
6. Ensure monitoring is targeted to detect and deter major incidents.
7. Specify circumstances when escalation to a full formal investigation (which may use the digital evidence) should be launched.
8. Train staff in incident awareness, so that all those involved understand their role in the digital evidence process and the legal sensitivities of evidence.
9. Document an evidence-based case describing the incident and its impact.
10. Ensure legal review to facilitate action in response to the incident.

This article is a well done academic approach to forensic readiness. The previous work are discussed and challenged with listings. The main part is the concluding ten points listed and explained. Rowlingson have done a thorough job and uses business English for his main target: enterprise management/leaders.

8.3 DF Readiness Framework for South African SME, Barske et.al. 2010

Barske et al. wrote in 2010 an article regarding DF readiness targeted to SME [4]. This article is a compressed version of Rowlings's 8.2. Barske et.al. introduces shortly and continue to list DF as Rowlingson described. Barske et.al. further introduce an illustration and describes all the circles (see figure 6). They further describes the challenges in SME and stress the need for optimization in this context.

Barke et al. have written a easy readable academic paper that hit their target: the SME's. The illustration and the short size of this article is very good. SME's need quick and effective yet understandable inputs.

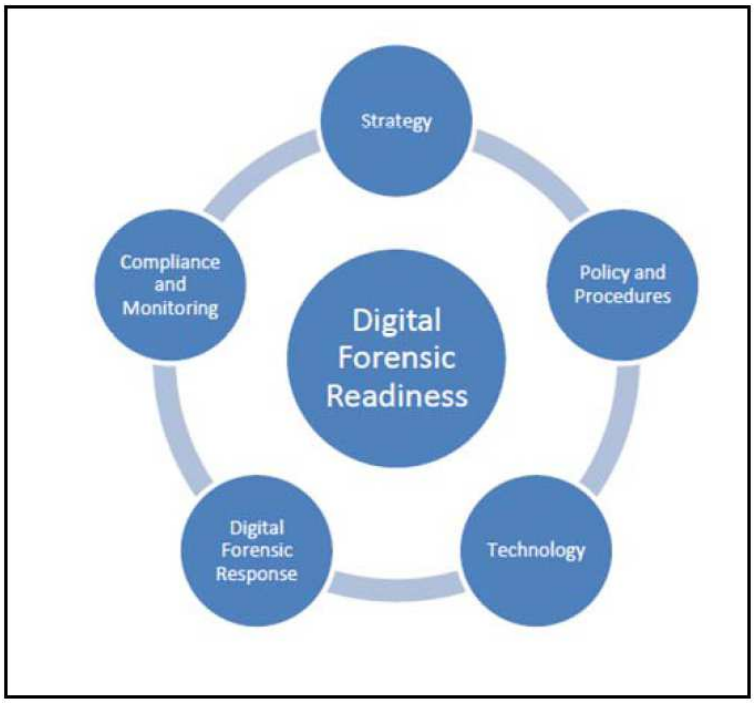

Figure 6: The Digital Forensic Components [4].

9 ISO/IEC 27037 - A Standards for better DFI Readiness?

"The nice thing about standards is that there are so many of them to choose from."
– Andrew S. Tanenbaum

We have great expectation regarding ISO/IEC 27037. The complete name are: *"ISO/IEC FDIS 27037 Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence"* [15]. This ISO standard is a so-called "draft" (FDIS)[18]. This is the last step before a document (under the normal development process) is approved as an International Standard.

As the name reveals - this standard will describe ways of handle digital evidence. Hopefully, this standard will be a large step against a more formalized description of forensic readiness.

[18]FDIS = Final Draft International Standard

10 Our FrameWork proposal: D-FORCE

I cannot think of ANY area in our field
that deserves more attention than security
awareness. Management just doesn't get it!
Pay a penny now or pay many pounds later.
– John C. Glover

We will introduce a new term: **D-FORCE**[19]

10.1 Why a new FrameWork?

We read a lot of framework proposals during our literature study. Our conclusions are that there is a lot of interesting work previously done. However, we struggle finding anyone sufficiently optimized and simplified for general SME usage (which may be a challenging task). Most frameworks are very technical and academic.

The design philosophy with D-FORCE is to develop a understandable framework for DFI readiness in SMEs. We strive for an optimized, simplified and human understandable approach for DFI Readiness. We focus more on the organizational and human aspect and uses plain English.

10.2 Motivation

The following list shows our goals with D-FORCE:

- Minimize the interference to normal business during an investigation
- Make SMEs more prepared/robust in an eventually collaboration with police
- Fulfill the coming standard (ISO/IEC 27037)
- Ensure that evidence are collected and stored in a forensic sound manner
- Quality control and documentation of ICT equipment (bi effect)

10.3 The DF Readiness Project - Will it survive?

Any business continuity project like the DF Readiness project must be thoroughly analyzed before started. The following questions may be a checklist before start:

- How much time will this project demand (make a project plan with slack)?
- Will we manage to do business as usual meanwhile?
- Do we need to hire extra staff and/or consultants?
- Do we have a plan for motivating and including our employees in the processes?
- A risk assessment need to be documented

This kind of questions will CEO and board most likely ask.

10.4 Plan Do Check Act - A Familiar Model

We will in this section define the D-FORCE main phases. We have chosen the PDCA[20] model in our framework. This is a model that is easy to understand and works for its purpose. See figure 7.

[19] This term is derived from the sentence: "**D**igital **FOR**ensi**C**s readiness in SM**E**s".
[20] PCDA = Plan Do Check Act.

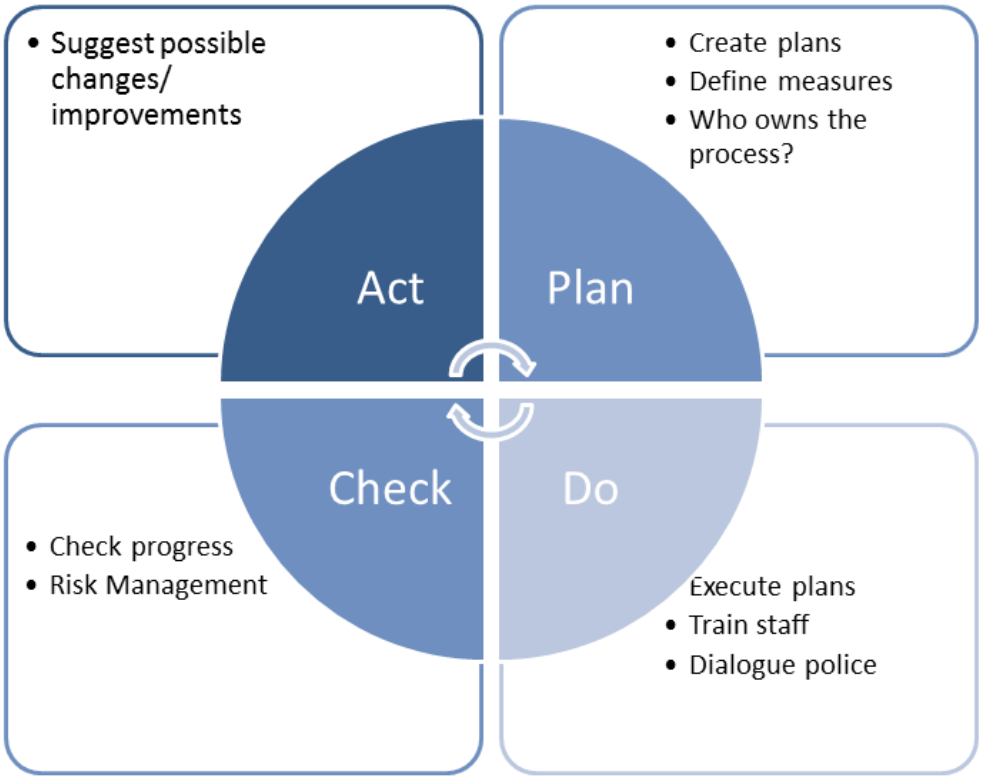

Figure 7: The Plan Do Check Act.

Plan

The "Plan phase" is where we make strategies and plans for D-FORCE.

- Do the necessary organizational changes (does there exist an IS manager/responsible?)
- Updating the organizations policies and procedures
- Create plans for tabletop exercise
- Create plans for evidence logging
- Define ways to measure DF readiness
- Perform cost analysis on the DF readiness job vs. business continuation security advantages

In the plan phase it is crucial to heavily involve the top leaders/management. The DF readiness needs to be sold in to the management in the initial phase - then every employees must be included. The DF readiness process will cost time and effort in the organization. Define measures so the leaders and the process owners can follow the processes.

Do

In this phase we execute the strategies and plans given in "Plan phase". Examples of tasks:

- Train employees (both in technical and organizational/legal matters)
- Document every ICT equipment used in the organization
- Set up server(s) to collect digital traces (logs) from all ICT equipments
- Synchronize clocks and timezone
- Ensure that our important data are safely backed up and able to be restored
- Ensure that our basic ICT security mechanisms works (firewalls, anti virus etc.)
- To collect and secure digital traces for potential crimes and disputes
- To ensure that evidence are collected and stored in a forensic sound manner
- Define easily measures (both easy to measure and administrate)
- Document and store configuration and user names/passwords in a safe place

- Establish contact with external consultants and/or police/law-enforcement to ensure the quality of DF readiness work
- Perform tabletop exercises: "a crime has been committed"

Check

In this phase we evaluate the results from the Do phase vs. what we planned. Examples of tasks:

- Do all necessary in the organization understand the need for DF readiness?
- Are the business more robust and ready to collaborate with a police forensic investigation?
- Evaluate the DF readiness process/project plan vs. execution
- Are we familiar with proper evidences handling?
- Results of our tabletop exercise - did we help/improve the law-enforcement process?
- Collect and report the results/answers from this section

Act

In this phase we evaluate the results given in the "Check phase". Examples of tasks:

- Why did we not got the results as expected in our plans?
- Why are people resisting our plans?
- Why do we failed in handling evidences?
- How can we change our plans to get our initial goals?

10.5 Selling the DF Readiness Project

Management and Board must be Positive and Involved

The DF readiness project must be "sold" to the management and board as a part of the business contingency plan. We have to communicate clearly regarding costs, benefits and risks. We may manage to align DF readiness with the IT strategy. The following bi-effects are important; (i) better control of ICT equipment, (ii) increased trust and compliance and (iii) reduced internal threats. Leaders do not like technical terms in general. They are busy people striving for doing the right decisions. Give them scenarios and alternatives. Get to know leaders and people in board to build your support group. This sales job may be in large degree a political job so you better prioritize your effort where it is most effective.

Be prepared for a resisting organization

The DF readiness may not be positively welcomed by the organization. Organization culture is often very difference inside an enterprise. We need to sell our project with a thoroughly prepared plan. Every counter scenario attack must be prepared and handled positively and correct. Organizational changes takes time and a lot of effort. Let the supporting colleagues sell the message through the organization.

Selling our project to Employees

People are often difficult to change. We can teach them new knowledge and make them willing to change (attitude), but to change behavior is much more difficult. Do not be impatient! Think as a salesman and communicate where you meet the most of them (social network, posters, games, free-bees etc). Be patient - every stakeholder is important. The chain is only as strong as the weakest link!

10.6 Critical Success Factors

We have listed critical factors to manage success in using our D-FORCE framework. Please note that they are not ranked/ordered.

Management and Board

The management and board must be strongly involved in the DF readiness project. Without them the project is most likely doomed to failure.

Basic DFI knowledge

The DF Readiness project manager need some level of knowledge to DFI - especially regarding evidence handling. Police are most likely positive to have a dialogue and perhaps course SMEs in how they work.

Measures for DF Rediness

The DF readiness is a continuous process and need to have some measurable metrics. If we measure before, during and after the our DF implementing process we can easily evaluate our work. The typical are number of; (i) near miss events, (ii) minor incidents, (iii) major incident and (iv) critical incidents in the SMEs.

Event Reporting

Employees must be positively motivated to report all level of events (included all near miss events). Reporting must be an popular, common and easy task. Anonymously reporting may also be an option. Any reporting that produces negative feedback will directly reduce the employees will to report. The SME need every employees to practice security awareness, but overreacting to incidents is not the best approach. The level of reporting will variate - be patient.

All employees must be included

The employees are in general the most important assets in any SME. Be sure to include every stakeholder in the organization. An internal investigation process can be a tough situation. Personnel need training and exercise to be positively motivated to collaborate with police.

Learning by doing

It is crucial to understand why events happens. Collect and document all possible knowledge in the organization of events and learn! Especially the one that escalated to major or critical level of severity. This is a boring and often time consuming job, but nevertheless important.

Courses and Training is important

External training can have an initial high cost - but is most efficient in long term. People get to broaden their networks and exchange knowledge.

Triggers for DFI process?

When do we start an internal investigation? Overreacting to incidents is not the best approach. The levels will most likely be in lost money and/or man hours, and must be evaluated frequently to fit the organization (typical yearly).

11 Further work

We would like to create some nice templates for the D-FORCE framework. This would help an SME to get started.

We would like to test out our D-FORCE framework proposal in several SME categories and most likely get valuable experiences.

Can an IDS work as an log collector? Perhaps also with enciphered archive in cloud services? Can these ideas be an easily D-FORCE approach for SMEs?

12 Summary

We have in this paper explained cyber crime threats and given examples in how business can be harmed. We have described the challenges in Norway regarding settlement and police organization. We have further explained incidents and the basics of DF. There exists several good articles regarding DF readiness and we have discussed the most important one plus a coming ISO standard covering the same matter. Finally we introduced the D-FORCE framework which is an DFI readiness framework that are optimized for SMEs.

We have used a lot of effort hunting for good statistical figures from Norway. The best (and mostly referred to) was the Mørketallsundersøkelsen 2012 by NSR. Norwegian Statistics blamed Norwegian Police for odd ways of calculate economic loss regarding computer crime. Hopefully this will soon be history and we may get better statistical data to work with.

Police have huge challenges with Norwegian settlement and the way police are organized with DF expert knowledge located in Oslo. It is most likely that SMEs will start their incident recover process rather than wait for police to arrive. Our conclusions is that by introducing DF readiness approach SMEs are prepared and more robust facing police investigation processes. They can recover from incidents and in the same time have digital traces/evidences for police when they arrive. The D-FORCE framework will contribute positively helping SMEs in the DF readiness process.

13 Acknowledge

Thanks to Prof. Dr. Bernhard M. Hämmerli (Gjøvik University College (`www.hig.no`) & Acris GmbH (`www.acris.ch`)) for his patience, supervising and feedback's. Thanks to fellow student Ernst Kristian Henningsen and Aud Gran for good feedback's.

References

[1] Andre Aarnes. Digital forensics I. Lecture Notes. Gjøvik University College, October 2010.

[2] Charles Arthur. Activists commit more data breaches than cybercriminals. URL, March 2012. Accessed: 2012-09-25.

[3] Jasper Bakker. Ddos attack forces dutch bank offline. URL, February 2011. Accessed: 2012-10-27.

[4] D. Barske, A. Stander, and J. Jordaan. A digital forensic readiness framework for south african sme's. In *Information Security for South Africa (ISSA), 2010*, pages 1 –6, aug. 2010.

[5] Danah M. Boyd and Nicole B. Ellison. Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication*, 13(1):210–230, 2007.

[6] Peter Cooper, Gail T. Finley, and Petteri Kaskenpalo. Towards standards in digital forensics education. In *Proceedings of the 2010 ITiCSE working group reports*, ITiCSE-WGR '10, pages 87–95, New York, NY, USA, 2010. ACM.

[7] T. Cox and A. Griffiths. Work-related stress: nature and assessment. In *Stress and Mistake-Making in the Operational Workplace, IEE Colloquium on*, pages 1/1 –1/4, oct 1995.

[8] Crime Circle Inc. Forensics science timeline. URL, November 2010. Accessed 2012-09-13.

[9] P.A. Diaz-Gomez, G. ValleCarcamo, and D. Jones. Internal vs. external penetrations: A computer security dilemma. In *Proceedings of the 2010 International Conference on Security & Management*, 2010.

[10] Tom Espiner. British stuxnet could have unintended fallout, government admits. URL, July 2012. Accessed: 2012-09-25.

[11] Federal Bureau of Investigation, U.S. Cyber banking fraud. URL, 10 2010. http://www.fbi.gov/news/stories/2010/october/cyber-banking-fraud.

[12] Organisation for Economic Co-operation and Development. *Computer viruses and other malicious software : a threat to the internet economy*. OECD, Paris, 2009.

[13] Norwegian Government and the Office of the Prime Minister. *Rapport fra 22. juli-kommisjonen : Oppnevnt ved kongelig resolusjon 12. august 2011 for å gjennomgå og trekke lærdom fra angrepene på regjeringskvartalet og Utøya 22. juli 2011 : Avgitt til statsministeren 13. august 2012*. Norwegian Ministry Service Center, Oslo, 2012.

[14] Selina Harrison. Cyber crime: A global threat. URL, September 2012.

[15] ISO/IEC and ISO. ISO/IEC FDIS 27037 Information technology – security techniques – guidelines for identification, collection, acquisition and preservation of digital evidence, September 2012. Accessed: 2012-09-22.

[16] Brian Krebs. N.y. firm faces bankruptcy from $164,000 e-banking loss. URL, February 2010.

[17] Kripos. Om Kripos (norwegian). URL, July 2012. Accessed 2012-09-14.

[18] David Lacey. *Managing the Human Factor in Information Security: How to win over staff and influence business managers*. John Wiley & Sons, Inc., 2009.

[19] National Police Directorate. *The Police in Norway*. Number 2010/07 E. POD Publication, June 2010.

[20] National Police Directorate. Politiet i det digitale samfunnet (norwegian). URL, August 2012. Accessed 2012-09-13.

[21] Statistics Norway. Enterprises with internet broadband in 2011. URL, 2011. Accessed 2012-09-18.

[22] Statistics Norway. Population in norway. URL, March 2012. Accessed 2012-09-13.

[23] Norwegian Ministry of Trade and Industry. Små bedrifter, store verdier. regjeringens strategi for små og mellomstore bedrifter. URL, March 2021.

[24] UK Cabinet Office, editor. *The Cost of Cyber Crime [electronic Resource]: A Detica Report in Partnership with the Office of Cyber Security and Information Assurance*. Cabinet Office, February 2011. Accessed: 2012-10-29.

[25] Oxford University Press. Definition of cloud computing. URL. Accessed 2012-09-17.

[26] Aiko Pras, Anna Sperotto, Giovane C.M. Moura, Idilio Drago, Rafael Barbosa, Ramin Sadre, Ricardo Schmidt, and Rick Hofstede. Attacks by "anonymous" wikileaks proponents not anonymous, December 2010.

[27] PwC. Cybercrime: protecting against the growing threat. URL, November 2011. Accessed: 2012-10-30.

[28] Robert R. Rowlingson. A ten step process for forensic readiness. Technical Report 3, QinetiQ Group plc, 2004.

[29] Norah Rudin and Keith Inman. Forensic science timeline. URL, 2002. Accessed 2012-09-13.

[30] Bruce Schneier. *Liars and Outliers: Enabling the Trust that Society Needs to Thrive*. Wiley, 1 edition, February 2012.

[31] Næringslivets sikkerhetsråd. Mørketallsundersøkelsen om datakriminalitet 2012 (in Norwegian). Technical report, Næringslivets sikkerhetsråd, August 2012.

[32] Peter Sommer. Digital evidence, digital investigations and e-disclosure: A guide to forensic readiness for organisations, security advisers and lawyers. URL, March 2012. Information Assurance Advisory Council (IAAC).

[33] Torben Strand. Are we doing a proper job? (an analysis of the computer forensic investigation in scandinavia). Master's thesis, School of Computer Science and Informatics, University College Dublin, July 2012.

[34] Symantec. Internet Security Threat Report, Vol. 17, Published April 2012. Technical report, Symantec Corp., April 2012. Accessed: 2012-09-25.

[35] Symantec Corp. W32.stuxnet dossier. URL, 11 2010. Accessed: 2012-10-31.

[36] John Tan. Forensic readiness. URL, July 2001. Accessed 2012-09-19.

[37] The European Union. Commission recommendation of 6 may 2003 concerning the definition of micro, small and medium-sized enterprises. *The European Union*, Official Journal(C(2003) 1422):6, September 2012.

[38] TNS Gallup. Politiets nasjonale innbyggerundersøkelse (norwegian). URL, November 2010. Accessed 2012-09-15.

[39] The European Union. European polulation density. URl, 2010. Accessed: 2012-10-09.

[40] Verizon Business. Data breach investigation report. URL, March 2012. Accessed: 2012-09-25.

[41] Chester Wisniewski. Sony portugal latest to fall to hackers. URL, June 2011. Accessed: 2012-10-27.

Appendix A — Acronyms and abbreviations

ASP	Application Service Provider
Bot	A bot is malware that can be controlled by the botmaster (short for "software robot")
Botmaster	A botmaster is the master of a botnet. S/he controls a botnet
Botnet	Botnet are a network or networks of many bots
CERT	Computer Emergency Response Team
CPI	Consumer Price Index
DF	Digital Forensics
DFI	Digital Forensics Investigation
EFTA	European Free Trade Area
FDIS	Final Draft International Standard
GNP	Gross Domestic Product
GUI	Graphical User Interface
ICT	Information and Communication Technology
IDS	Intrusion Detection Systems
IS	Information Security
IPR	Intellectual Property Rights
ISP	Internet Service Provider
NIDS	Network Intrusion Detection Systems
NOK	Norwegian Kroner
OECD	The Organization for Economic Co-operation and Development
PCDA	Plan Do Check Act
PLC	Programmable Logical Controller (industrial computer unit)
POTS	Plain Old Telephone System
PPS	Purcasing Power Standards
SME	Small and Medium Enterprises
USD	US Dollar

Table 7: Acronyms and abbreviations

Appendix B — The Norwegian Police Organization Chart

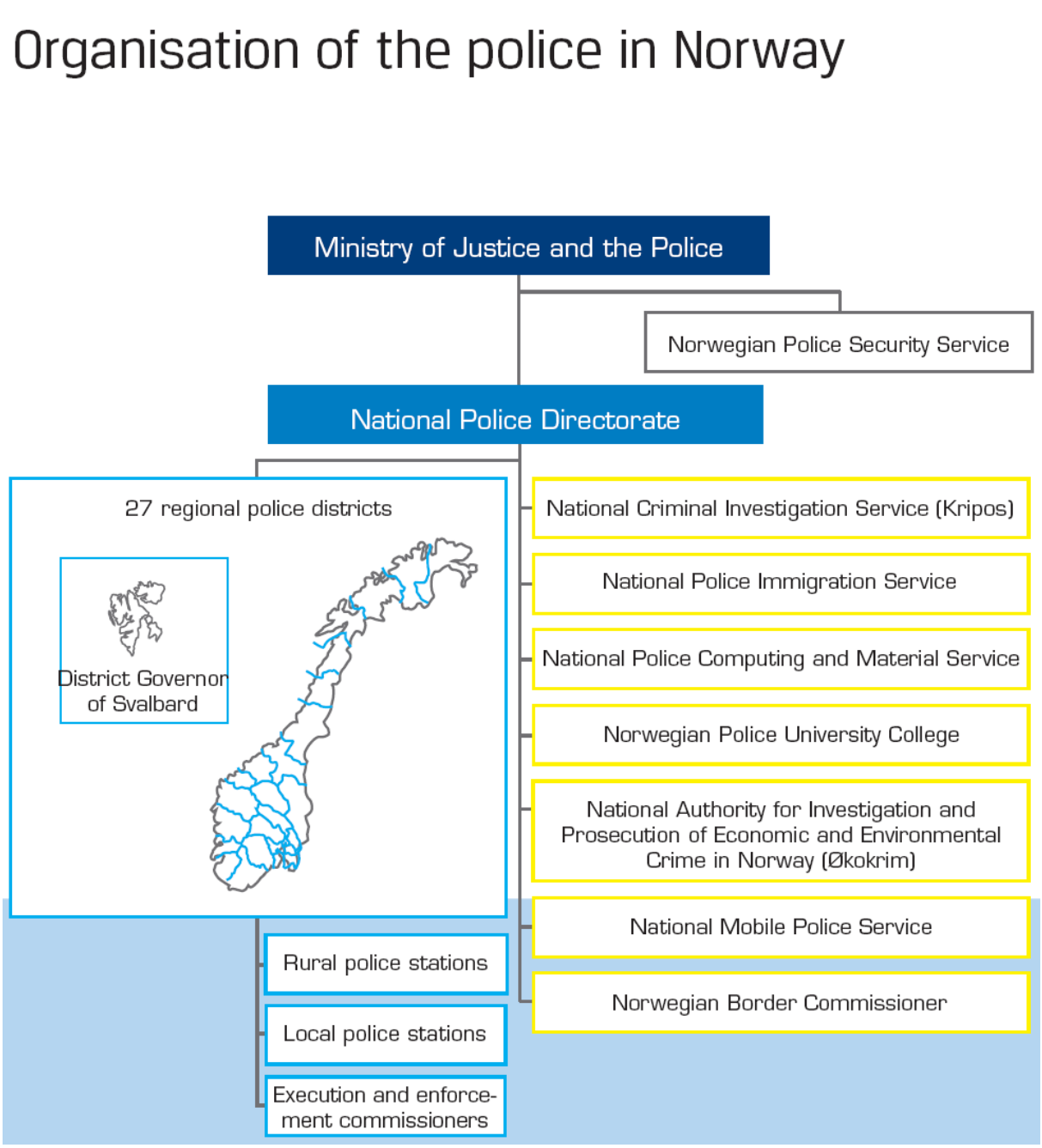

Figure 8: The Norwegian Police Organization Chart.