NATIONAL CYBER CRIME CENTRE
COMPANY GUIDELINE

Security Precautions

- Breach of IT systems

NC3 POLITI

dansk·it

Contents

01 Introduction

1.01 Preamble

This guide is the result of a cooperation between Danish police and the Danish IT Society. It is intended as a guide for companies to acquire potential evidence for the police in case of an investigation of an IT-related incident.
The Danish National Police, National Cyber Crime Centre (hereinafter NC3), have found, over a longer period of time, that the police often become involved too late in an IT-related incident, i.e. after the evidence has been erased or that it was never acquired in the first place. This is partly due to the lapse of time between the actual crime and the report of the crime to the police. It is also due to the fact that the IT departments of the various companies are focused on damage control rather than gathering digital evidence; therefore they are ill-equipped to assert which evidence to acquire.
Based on these findings, it is the purpose of this guide to:

- Inform companies on what they can do in order to ensure that the necessary information is gathered before a potential breach of IT security.
- Help ensure that, in case of a breach of IT security, potential digital evidence is not destroyed or corrupted.
- Provide directions on how to best secure a company's network in order to give the police the best working conditions.
- Facilitate the gathering of the necessary digital evidence for the police, after the damage is done.

1.02 Structure

This guide consists of an introduction and two separate parts. The introduction describes the basis for this guide as well as why IT security should be regarded as a serious issue.
Part 2 contains examples of precautionary measures you can take in order to provide the police the optimal working conditions.
Part 3 contains examples of how to acquire the evidence after a security breach has taken place, so that it can be used in court.
It is a prerequisite for this guide, that the company manages its own network. If your company has outsourced the management of your network to an external contractor, do make sure that they are able to comply with the precautions described in this guide.
This guide does not concern compliance. Any company that wishes to use this guide must make sure that they do comply with current rules and regulations.

1.03 What is considered evidence in an IT investigation

When it comes to crimes in the physical world, evidence is one or more clues that point to a specific perpetrator. It can be fingerprints, DNA, CCTV recordings, eyewitnesses etc. When it comes to cybercrimes, you rarely have any of the listed types of evidence. It is almost exclusively 'digital fingerprints'.
A digital fingerprint can be an IP address, but it is far from the only thing, that can lead directly to the identification of a perpetrator. The main part of networks is configured with DHCP servers, that assign

available IP addresses to computers connected to that network. The IP address is assigned to a specific computer in a predefined period of time. At the end of the period, the IP address can be assigned to a new computer. Additionally, the IP address can be changed manually to complicate the investigation even further. Therefore, the exact time of the crime is just as important as port numbers, MAC addresses, network names, usernames etc. when it comes to identifying the perpetrator. This is why logs are often the most important source of evidence in an investigation. It is extremely important to retain logs from various sources. You can find examples of these sources in the guide under preventive measures (section 02.06). It also contains a suggestion for facilitating the gathering of information by implementing certain solutions beforehand, such as 'SIEM'.

1.04 The electronic evidence is vital

It is not only in cases where an outsider accesses a company's system, that the electronic evidence is vital to the investigation. It is increasingly important in a number of other cybercrimes that can be committed against a company. It is very important to deal with the – up until now predominant – focus on external threats and rather broaden the focus to include inside threats as well. If you gain access to a network, there very few hindrances to accessing the entire network. The trust placed in employees has been very high – often even too high.
This is why IT security should be equally focused on securing the network from unauthorised access from users within the network, not solely on external users.
The threats in a security incident can more or less be divided into three categories: the inadvertent insider, the malicious insider and the outsider.

1. *The inadvertent insider* is usually an employee who clicks on a link in a seemingly innocent email or an attached file and unknowingly activates malicious software, e.g. ransomware. It can also be an employee, that - unintentionally - visits an infected website, opens a document with embedded macros or uses an unknown USB stick with malicious software which causes e.g. ransomware to be activated.
2. *The malicious insider* is someone who knowingly downloads child pornography unto the company's system (servers or workstations), abuses email accounts or leaks classified information to the media or competitors. It can also be a former employee who still has access to the systems and uses this for his or her personal gain. It can also be a current or former employee that holds a grudge against the company and wishes to harm their IT systems.
3. *The outsider,* i.e. someone without authorised access to the network, is usually described as a hacker. Their aim is to intentionally exploit a weakness in the network in order to gain unauthorised access. Their motive is often financial gain, but they can also be motivated by political convictions or revenge. This category includes both individuals that target a specific company, as well as those who scan a vast quantity of networks looking for vulnerabilities in order to access any network possible.

Each of the above-mentioned examples can end in prosecution, so it is very important that the electronic evidence is properly preserved. When you increase the quantity and quality of the documentation of your evidence, you vastly increase the chance of an eventual conviction.
Companies have a substantial interest in re-establishing their systems as fast as possible, so they can get back to business. However, it makes it quite difficult in an eventual court case, if the evidence was not properly acquired before the systems were restored. This does not mean that commercial operations should be neglected. On the contrary, it means that companies should have procedures in place beforehand that makes it possible to acquire the right evidence as fast as possible, so that the systems can be restored faster.
If a company only focuses on external threats, it will greatly increase the time from breach to discovery. It generally takes a very long time to discover that a network has been compromised. Globally speaking, the average number of days, from breach to discovery, is 191 days[1]. It is an improvement compared to 2016, where the average was 201 days. There is, however, still room for improvement.

[1] 2017 Cost of Data Breach Study, Global Overview, Benchmark research sponsored by IBM Security, independently conducted by Ponemon Institute LLC, June 2017, © Ponemon Institute Research Report.

The majority of NC3's investigations involve insiders. This is why 'Assume Breach' (i.e. assuming that your network is already compromised) is the best way to structure your network security.

1.05 Data Integrity

Two of the basic principles regarding evidence are that they have to be able to be presented with credibility in an eventual court case and, that they must be indisputable. Naturally, this applies to electronic evidence as well, such as log files etc. That is why it is important to secure the integrity of the electronic evidence. This can be achieved by acquiring data and logs as early as possible in the process, as well as ensuring that they have not been altered.
If you put more effort into securing the electronic evidence, it will carry that much more weight in a court case.
In part 3 of this guide, you can find examples on how to optimise your company's data integrity.

1.06 The cooperation between the police and the companies against cybercrime

NC3Skyt is a cooperation between NC3 and various companies, especially small and medium-sized enterprises (SMEs). The ambition of the cooperation is to achieve better knowledge sharing in order to heighten the general IT security knowledge in the companies. The cooperation was launched in the beginning of 2016 with the primary goals of preventing cybercrimes and to host activities to optimise damage control. The latter can help companies to protect themselves better against an attack. The activities can also increase the companies' capacity to handle the negative effects of an attack on their IT systems.
As a member in NC3Skyt your company will get access to:

- Meetings with other member companies and the police where we exchange knowledge and experiences with cyber attacks in order to strengthen the companies' resistance to cybercrime
- Information from NC3 regarding national and international trends and the like. The materials can include information about different types of malware, ransomware etc. prepared by NC3 and Europol
- The opportunity to ask NC3Skyt-employees questions about IT-related crime.

Membership of NC3Skyt is free of charge.

If your company has the capacity to host meetings or events, you can arrange to do so with the NC3Skyt representative in your police district.

As a member of NC3Skyt you may become privy to your fellow member companies' internal IT security as well as specific events or incidents. This is why we expect you to observe your duty of non-disclosure, even if you eventually resign from NC3Skyt.

Please contact the NC3Skyt secretariat at pol-nc3-skyt@politi.dk, if you wish to join as a representative for your company or have any further questions.

02 Preparing for a security breach

2.01 Computer Incident Response Plan
Have a plan that clearly explains what to do if the damage is done

2.02 Know your network
Draw up a diagram of your computer network

2.03 User administration
Make sure your users only have the access they need

2.04 Network segmentation
Divide your network into segments and establish protocols for user access

2.05 Network Time Protocol Server (NTP)
Make certain that your entire network is synchronised to the same time

2.06 Logs
Make sure you log the correct data and protect your logs

2.07 Backup and encryption
Create a backup policy that enables you to restore your systems without overwriting the evidence

2.08 Configure the digital devices and set up security policies
Configure your company's devices and set up security policies

2.09 Update the systems
Keep your systems updated to avoid security vulnerabilities

2.10 Education and awareness
Educate your employees in IT security

2.01 Computer Incident Response Plan (CIRP)

It is important to have a formalised plan of action in case of a major IT-related incident. It must clearly state what to do and who the incident response team consists of (those responsible for specific parts of the systems or certain actions). Such a plan is called a Computer Incident Response Plan (CIRP).
A CIRP is usually quite extensive with a lot of specific information and explicit step-by-step guides, which is why the CIRP should not be part of the company's general contingency plans (such as system shut-down and the like) but rather a stand-alone plan.
It is impossible to make one generic format for all computer systems each company uses. A CIRP should be made for each system, and it is important to take the time to create one but also maintain it and practice it properly.
A CIRP should contain the following:

- A definition of what qualifies as an IT-related incident
- Contact information for the incident response team
- Information on when to contact the police
- Clear instructions on *who* is allowed to make statements about the incident to the media, *when* they allowed to do so as well as their contact information.
- Information on where to find the network diagram (see section 2.02, 'Know your network') and who to contact.

The list is only meant as an inspiration, as a CIRP needs to contain a lot of other things as well.
It is important to simulate a breach so you can test your CIRP and train your employees (and management, as well). Training will make it easier to remember the plan, when the systems are down and ensure that only the relevant people re-establish the systems. This will limit the harmful effects of a breach such as down time, loss of profit and a decrease in the trust of the shareholders. It also ensures that the evidence is acquired in a more correct manner and becomes more valid in an eventual court case.

2.02 Know your network

Draw up a diagram of your entire network. Spend the necessary time when you are creating it and make sure that you update it, when new systems are added or old ones are discontinued.
If possible, you can boost your security even more by setting up your network to send a notification every time a non-approved device is connected. This can be done automatically with a Nmap script, but there are also numerous commercial products that can give you a comprehensive view of your network and the devices connected to it.
Additionally, you can set up your network and connected devices in a similar manner, so that they can only execute approved programmes (also known as software whitelisting). This serves as prevention against ransomware and hacker tools.
A network diagram is a sensitive document and will not be part of the police's case file. It is solely a working document between the company and the police.
When you know your network, you must monitor it continuously. This can be done by using different security tools such as Intrusion Detection System (IDS), Intrusion Prevention System (IPS) etc., depending on your company's network.
It is important to educate and train your employees in how to use the tools, how to configure them and keep them updated, in order for the tools to work properly. If you do not do this, the worst case scenario is a barrage of false positives that will lead to the opposite of the desired result, i.e. the employees will ignore all warnings.

The company's type, size and network determine what you need to monitor for. However, specific things, such as the use of an encrypted tunnel to send data outside the network, should always result in a warning or notification from the system. There can, however, be legitimate reasons for using encrypted tunnels, but they are the go-to methods for ransomware and hackers to send data outside the network or contacting a server for instructions.
It is worth noting that you can see which countries were contacted afterwards. If the company does not have any activities in e.g. China or Qatar, you can block all data traffic to that country. You could also limit data traffic to areas, where the company does have activities. Naturally, you have to exercise a certain level of caution in doing this. You cannot implement it immediately without testing first as certain programmes might need an active connection to a certain country in order to function.

2.03 User administration

The users on your network should only be given the rights, that they actually need. It is much too common that employees have administrator rights without needing them. It makes a big difference whether or not an employee has administrator rights, when a hacker takes over their user profile. Even the CEO does not need to have access to everything. When an employee leaves a company, his or her profile should be deleted. When new employees are hired, they should have a new profile created specifically for them. Old and unused profiles are rarely deleted, which makes them ideal for a hacker to take over.
A solution to this problem could be to set up the system so that e.g. your Senior Security Officer will get a notification every time somebody is assigned administrator rights, especially if it happens outside your standard working hours.
Furthermore, you should implement two-factor authentication on access to information that you classify as vital for your company.

2.04 Network segmentation

Divide your network into segments and establish protocols for user access. Traditionally, network security has been focused on outside threats. This problem is very much exposed, when companies are attacked, e.g. by ransomware. The ransomware can freely encrypt the entire network, once an approved user of the network clicks on a link, visits an infected website or opens an infected attachment. Occasionally, the ransomware can even reach backup drives in this manner. This can be avoided by segmenting your network and only allowing access to certain segments, if necessary. Bear in mind that a ransomware can only encrypt the segments that the infected user has access to.
Access to sensitive information, such as backups and retained data, should be protected by two-factor authentication. The best course of action is to assume that your network has already been compromised, in order to ensure that your company is prepared if a breach does occur.

2.05 Network Time Protocol-Server (NTP-server)

A NTP-server is a central server on the network that is used to synchronise the computers of the network to exactly the same time reference. It is very important to synchronise all the devices to exactly the same time reference, since even a slight time difference can obstruct the investigation severely. A mere 1/100 of a second can have a tremendous negative impact on the investigation.
Once you have set up your NTP-server, you will need to implement procedures to ensure that both existing devices as well as new ones have the correct time reference.

2.06 Logs

It is a fact that lack of logs and system surveillance often obstructs or even terminates investigations. This is why you should consider increasing your company's logging capabilities and system surveillance. It will also optimise the possibility of finding the electronic traces, once the damage is done.
In regards to logs, it is very advantageous if this is done separately from the rest of your network – preferably on a designated server. Hackers are usually very careful to erase all traces of themselves, which becomes much easier to do, if the log collection process is using the standard set up. Ready-made 'hacker tools', which are readily available online, are often constructed to erase traces in log files or event logs. You must consider that it is in the retained data that we find the electronic evidence, which makes it essential to decide exactly which data your company should retain. Source IP, date/time, source port, target IP and target port are all important, but it is also important to be able to see what has happened, e.g. in a web server log, which commands were executed, which operating system and browser was used etc. Additionally, you should set up each computer so that it retains any commands executed in the command prompt. Exactly which logs to collect varies from system to system. The main objective is that you log adequate data to prove the act. There is a tendency to only monitor and react to errors in the system, but it can be just as important to monitor the successful actions. Many companies only monitor the obvious areas such as firewalls, while DHCP-log files are forgotten or only preserved for a brief period of time, which means that they have been overwritten by the time the police get involved. Make sure you keep track of your logs and set up your logging policy in a manner that ensures that the files are not overwritten prematurely. It must be stressed that preparatory acts could have been committed long before the actual breach occurs.

It is entirely up to each company to choose which systems to collect logs from. However, it is important to stress that there might be certain legal requirements to meet in regards to national law and/or international law, such as the EU's 'General Data Protection Regulation' (also simply known as: 'GDPR').

The following list has been compiled by Danish police. Experience shows that the below mentioned data is either rarely acquired, does not exist, or have been overwritten by the time the police get involved. In many of those cases, the logs could have solved the case, had they been available. The list is not exhaustive, but merely meant as an inspiration:

- Firewall
- Router
- IDS systems
- IPS systems
- DMZ
- Proxy
- DHCP
- Guest network
- Active Directory
- Physical access logs (key cards and the like)
- Logs containing executed terminal commands
- Surveillance (both physical and of the network)
- Antivirus
- Event logs

The police are very much aware of the fact that you cannot retain every bit of data forever. However, you should make an informed decision on which logs to collect and for how long you will retain the collected logs. The list contains a lot of different logs in a lot of different formats. Luckily, there are specific types of programmes such as Security Information and Event Management (SIEM), which can be set up to gather all the logs in one joint format for you to monitor. You can even set up rules for what should be defined as abnormal, i.e. generate a notification to e.g. your Senior Security Officer. You should draw up a procedure for these notifications that clearly shows, who should receive them and how to respond when they are received. It must be stressed that a weekly check of the systems is nowhere near sufficient. The systems should be monitored constantly. Hackers rarely work during standard working hours which your contingency plan must take into account.

If your company does implement a programme like SIEM, you will need to spend a substantial amount of time on training your employees in how to use the programme as well as setting up the programme and fine tuning the settings of the notifications. If you do not spend sufficient time on setting up the notifications to an appropriate level for your company initially, it may create too many false positives, which will drown out a real incident.
You should implement e.g. two-factor authentication to access the retained data and make sure only selected employees have access in the first place.

2.07 Backup and encryption

Your company's backup policy should be constructed in a way that enables you to restore the system without overwriting the evidence. You should take into account that your system backup ought to be separate from your general network. If a ransomware strikes your general network, a backup will be of little use, if it is encrypted by the ransomware.

Sensitive data at rest should be stored in an encrypted form. Naturally, this includes any backups, but also any in-house procedures, network diagrams and any passwords you might have. Remember to monitor for access to the encrypted data, set up notifications and log any attempt of unauthorised access.

2.08 Configure your digital devices and set up security policies

There are numerous commercial products as well as built-in programmes available to configure your company's digital devices and set up security policies.

If you use Windows-based workstations, you can implement The Enhanced Mitigation Experience Toolkit (EMET). EMET is a build-in part of Windows 10, but you will have to configure it specifically for your system in order for the programme to work optimally. If your company uses Windows 7, you can download the programme free of charge at Microsoft's website. There are similar programmes available for the Mac and Linux operating systems. This is not the only thing you should do in regards to configuring your devices, but it is a big step in the right direction.

You might want to create a 'secure image' of a computer you can deploy on all new computers. Again, the 'secure image' must be kept separate from the rest of your company's network.
You should consider which employees have to be able to execute which programmes. An employee, who only needs access to emails, a browser and be able to open attached files, has no need for rights to execute, say, a PowerShell script.

If your company does have a SIEM, you should set it up so that it collects event logs and other logs from the local computers.

2.09 Update the systems

Make certain that all systems are updated at all times. Even a network printer that has not been properly updated can be used to access critical network areas. Usually, it does not take long from a vulnerability has been identified and published before hacker tools to exploit it has been developed. Keeping all your systems updated is a safeguard to protect your company against hackers.

Sometimes an update can disrupt your set up so you should test updates on a test network beforehand. If the update disrupts anything, you should take other security measures to prevent that the vulnerability is exploited.
Your update-policy should take into account that some updates do not follow the usual update cycles, which means your policy should include emergency updates.

2.10 Education and awareness

Besides the continuous education of the IT security staff, it is also important to educate *all* staff in proper IT security behaviour.
Your IT security staff should be continuously trained in acquiring data in the best possible way in order to facilitate optimal working conditions for the police. The evidence that the police receive is far too often either corrupted or tainted due to mishandling. An incident can result in a court case, in which case the evidence must be indisputable.
In regards to all other staff your network might be safe from outside intruders but still open to employees' inexpedient behaviour. An employee might be exposed to e.g. a spearphishing scam and lured into executing a malicious file that circumvents your internal network security. There have been several examples of hackers that have used months building the trust of an employee (i.e. 'social engineering') only to get them to execute a malicious file on the company's network. Hence, it is important that the education of your staff is very broad and not solely focused on complex IT technical subjects.
When an employee is tricked into transferring large amounts of money into accounts (typically in foreign countries), it is called CEO or BEC (Business Email Compromise) fraud. This type of fraud can be countered by continuously educating your employees in order to heighten their IT security awareness. As part of the education you might consider hiring a company to carry out an ongoing campaign that exposes your employees to different types of fake attempted fraud. Even reputable IT security companies run this type of campaigns to train their own employees. Even the most alert employee might be fooled, if they receive an email from the CEO's own email account requesting an action, transferral of money or the like. Take the time to develop a protocol for your company that clearly states what the employee should do in situations of this nature. The protocol can contain e.g. which precautions to take when transferring money over a certain amount. It could be that a request must be made both via email and verified by a phone call as well. You must remember to practice these protocols. IT security is not just for IT security staff. Even if your company has outsourced your IT operations, you must train the awareness of everyone who has access to your network, from the CEO to the part time student assistant. This does not mean that every employee must know the IT security policy for every single aspect of the company. It merely means that your IT security policy should take every type of employee into account. It is advantageous to create e.g. a leaflet to specify

how the different staff groups should react in certain situations. The leaflet should be exact and to the point, so keep it as short as possible.

03 Precautionary measures regarding a potentially compromised network

3.01 Appoint someone competent to handle the incident

3.02 Gain perspective
Find out what has happened and when. Initiate the pre-defined procedures

3.03 Is the system currently compromised?
Find out if the incident is still ongoing and initiate relevant procedures

3.04 Decide whether or not to report to the police

3.05 Start collecting data
Gather the relevant data as soon as possible in order to avoid contamination and/or loss of data

3.01 Other types of documentation for the police
Supply the police with the correct documentation straight away in order to speed up the process

3.01 Appoint someone competent to handle the incident

Appoint someone competent as a contact person to handle the incident inhouse and potentially be the liaison between your company and NC3, if you choose to involve the police. Preferably, you should appoint an alternative contact person as well, if the designated contact person is unavailable. Both contact persons should be educated and trained in handling IT security crises.

3.02 Gain perspective

Follow your CIRP as described in the guide's section 2.01.
As a minimum, you should certify the following:

- Is the incident isolated?
- Is your network diagram still valid? Find your network diagram, assess if it is still valid in the current situation.
- Can the systems be restored? If they can, will that destroy evidence that should be acquired beforehand?
- Is it necessary to shut out possible intruders from the system or can it wait until you have established what their intentions are and perhaps their identities as well?
- What actions has the company taken so far in regards to restoring systems or shutting out the intruders?
- Which parts of the system are affected and which are not?
- What does the incident entail for your system?
- Time frame? Remember, there might have been preparatory acts long before you discovered the breach.
- Do you suspect any individuals or perhaps staff groups?

Chain of custody should be observed. The person responsible for handling the situation should start to document as early as possible what has been done and when it happened.
This is of great value to the police, but even if the police do not get involved it will help your company tremendously in regards to gaining a subsequent perspective.
If it is an actual intrusion into your network, you should avoid using email as much as possible, because the hackers might be monitoring them. It is an easy way for them to find out whether or not they have been discovered.

3.03 Is the system currently compromised?

It is important to distinguish between a system that is currently compromised (i.e. the perpetrator might presently be connected to the system) and a system that is probably compromised (i.e. without current malicious activity). The optimal chance of securing evidence is with a currently compromised network, because hackers put much effort into covering their tracks once they do exit the systems. You should contact the police immediately if you have a network that is currently compromised – preferably through an informal enquiry, see the next section 'Decide whether or not report the incident to the police'.

3.04 Decide whether or not to report the breach to the police

Decide as fast as possible whether or not you want to involve the police.
The crime should be reported to the local police who are able to get assistance from NC3. If you are unsure whether you should report or not, NC3 will be happy to help by having an informal conversation about your breach and guide you. Please note that you should only contact NC3, if your systems are currently breached or have just been breached. A call to NC3 does not equal reporting the crime to the police. Depending on the urgency, you can choose to report the crime either to your local police, who can assess if NC3 should be contacted, or on our website: https://www.politi.dk/da/borgerservice/anmeldelser/hacking/. During standard opening hours you can reach NC3 via phone on +45 2283 4439. It must be stressed that you can only report a crime at your local police station or via our website. The hotline is solely to be used as an informal way of guiding you during an ongoing breach, when everything is very chaotic.

3.05 Start collecting data

You should start collecting data as soon as possible regardless of whether or not you report the crime to the police. This must be done in order to avoid losing data and/or contamination of available data. In order to keep the data integrity intact, you must also write down exactly which actions have been carried out. Every action must be recorded including who executed the action, the exact time/date of the action and how it was executed. Your written record should also include a 'chain of custody', i.e. who have had access to which logs and how were these logs handled as well as which actions were executed.
You should collect logs from all accessible sources. Even sources that might seem irrelevant at the given moment can become pertinent as the incident – and perhaps also the police's investigation – progresses. Bear in mind that not all retained data is saved for the same length of time, so some of it might be overwritten if you wait too long before collecting it. This process of collecting data from various sources should be written down in your CIRP.
Please see section 2.06, if you need inspiration for which kind of log-sources you should focus on.

The implicated workstation/devices should also be acquired as soon as possible. You should also consider acquiring RAM, depending on the character of the incident. Acquiring workstations and RAM can be a complicated process so you should make sure that the person doing the actual data acquisition has the necessary training and knows the process. If not, you should ask NC3 for guidance to make sure that it is done correctly.
If you do acquire data from devices, be sure to collect the data in a way that allows you to continuously control the data integrity.

The proper order of acquiring various logs, RAM etc. is:

1: Acquiring volatile data (primary storage, e. g. RAM)
This may cause the device to crash so you must weigh that possibility against the importance of the system. Whether or not the system is encrypted also a factor. It might be advantageous to talk to NC3 about the need for acquiring volatile data.

2: Acquiring offline data (secondary storage, e.g. hard disk)
Once you have identified the devices that are to be acquired, it is important to specify how you conduct your data acquisition, including who performed it and the time/date. The time should be logged as specifically – and correctly – as possible. There might be situations where the systems can be shut down, which means you can perform the data acquisition afterwards, and there can be situations where you have to perform the data acquisition, while the system has to remain active.
There might even be situations that do not fall directly into those two categories, where you simply have to acquire as much data as possible.
You may want to contact NC3 for guidance on this matter.

3: Acquiring other types of information
A complete mirror of a machine does not always yield all the information you need. You can be fortunate enough to find certain things in RAM, but it is far from certain that you will find everything so you should always execute some commands in the terminal/command prompt to make sure you get everything. Do contact NC3, who has scripts for this very purpose, that you can go through before executing them. Because this too can lead to a system crash, you may want to contact NC3 and get the scripts beforehand in order to avoid being forced to test them during a live situation.

You should create a standard for how to name the acquired items. When you have multiple parties involved a name like "Mr. Smith's laptop" is not desirable. You may consider naming them 'device 1', 'device 2' and so forth, while keeping a written record that clearly lists the devices and which types of data acquisition have been performed on them. If NC3 is already part of the case, you should coordinate the naming convention with them.

Do NOT decrypt a device before performing data acquisition, if the device was encrypted during the incident. You should contact NC3 if this specific situation arises because decrypting can potentially destroy evidence. Immediately after performing data acquisition, you should hash the acquired data including logs for each device you have acquired. This must be done to avoid working on corrupted/altered evidence.

This may all sound very tedious, but NC3 has seen examples of data being so damaged by the time it was finally collected that it was practically useless.

3.06 Other types of documentation for the police

Other types of documentation that will help the police solve the incident might be:

- Procedures that were followed during the security breach (e.g. Incident Response Plan)
- A network diagram
- List of which systems are affected including operating systems and installed third-party software
- Information on patch level
- Guidelines for use of the system
- A list of users/administrators of the system
- A list of people responsible for the applications on the network
- A list of IP ranges in the system
- A list of former employees that have recently been dismissed (if relevant).

04 Concluding remarks

IT security is a necessity and should be very high on your company's agenda. You are not expected to implement everything in this guide, and some of the sections might even be irrelevant for your company. You are, however, expected as a bare minimum to come to a decision on each of the sections (e.g. an informed decision on whether or not you will you not create an Incident Response Plan).
It is much easier and cheaper in the long run, if you have been thorough with your IT security. Once your network has been compromised and operations have been interrupted, it will be too late and your company will have suffered irreversible damage.