First Cyber Workgroup Report

Cyber Workgroup:
Paul Schillebeekx, GEBCAI,
Sören Haue, DALAX,
Mark Vos, NIVRE.

Date: December 2016
Version: 18 December 2016

INDEX

Chapter	page:
Introduction	3
Different forms of cyber spying	4
The seven steps	6

Introduction

Cyber spying, or cyber espionage, is the illegal act or practice of obtaining data and or secrets without the permission of the holder of the information (personal, sensitive, proprietary or of classified nature), from individuals, competitors, rivals, groups, governments and enemies for personal, economic, political or military advantage using methods on the Internet, networks or individual computers through the use of cracking techniques and malicious software.

In today's complex environment it is impossible to avoid cyberattacks or prevent infection of computer networks and software within organizations. Computer security threats are relentlessly inventive. Masters of disguise and manipulation, these threats constantly evolve to find new ways to annoy, steal and harm.

It's a dangerous attitude, considering security touches nearly every industry, especially with the advent of the Internet of Things, which aims to connect every device we use.

Arm yourself with information and resources to safeguard against complex and growing computer security threats and stay safe online.

If a cyber incident like a fire occurs in a company, a business interruption will result from it affecting the continuation of the business (BI). A common method for anticipating events that will support a speedy recovery of the production processes of a business, is to create a Business Continuity Plan (BCP) designed to respond to specific incidents. Such BCP is an important building block part of the Business Continuity Management (BCM) of a company.

This document describes the structure which is used for BCM and BCP, and which also is applicable to a cyber incident. This structure consists of seven steps which are explained.

Additionally, you can find a number of questions which ensure your company to be prepared as well as possible in the event of a cyber incident.

Different forms of cyber spying

Malware

Malware is a malicious software or code that typically damages or disables, takes control of, or steals information from a computer system. Malware broadly includes adware, backdoors, bootkits, logic bombs, rootkits, spyware, Trojan horses, viruses, and worms.

A drive by download delivers advanced malware or an exploit in the background, without the user' s knowledge, usually by taking advantage of a vulnerability in an operating system, web browser, or other third party application.

Mobile malware has also become a major threat. As mobile devices grow more powerful, they' ll increasingly be used as replacements for PCs, storing vast amounts of personal — and valuable — data that is largely unprotected.

Spyware threats

Another serious computer security threat is spyware. Spyware is any program that monitors your online activities or installs programs without your consent for profit or to capture personal information.

Hackers and predators

Hackers and predators are programmers who victimize others for their own gain by breaking into computer systems to steal, change or destroy information as a form of cyber-terrorism.

Phishing

Masquerading as a trustworthy person or business, phishers attempt to steal sensitive financial or personal information through fraudulent email or instant messages.

Spear phishing is a targeted phishing campaign that appears more credible to its victims by gathering specific information about the target, and thus has a higher probability of success.

A spear phishing email may spoof an organization (such as a financial institution) or individual that the recipient actually knows and does business with, and may contain very specific information (such as the recipient' s first name, rather than just an email address).

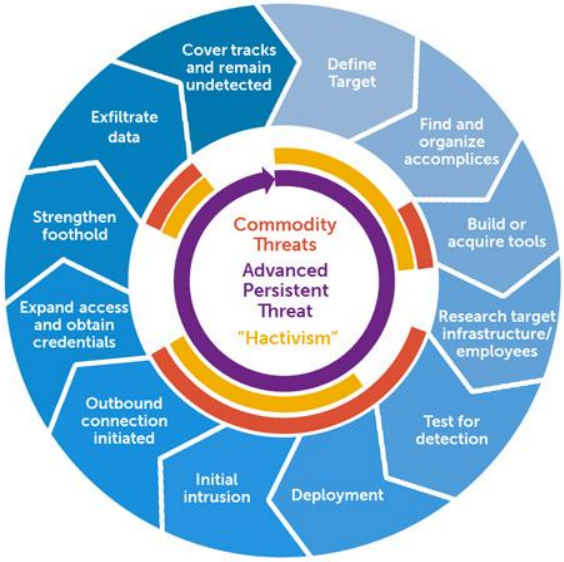
Advanced Persistent Threat

Despite significant investments organizations have made in traditional security solutions, such as anti-virus, intrusion detection and encryption, they still are falling victim to costly security incidents as a result of advanced persistent threat.

An advanced persistent threat (APT) is a set of stealthy and continuous computer hacking processes, often orchestrated by human(s) targeting a specific entity. An APT usually targets organizations and/or nations for business or political motives.

Whether through endpoint devices on the desktop, mobile devices or third parties, these sophisticated attacks are succeeding at disrupting organizations and ex-filtrating data.

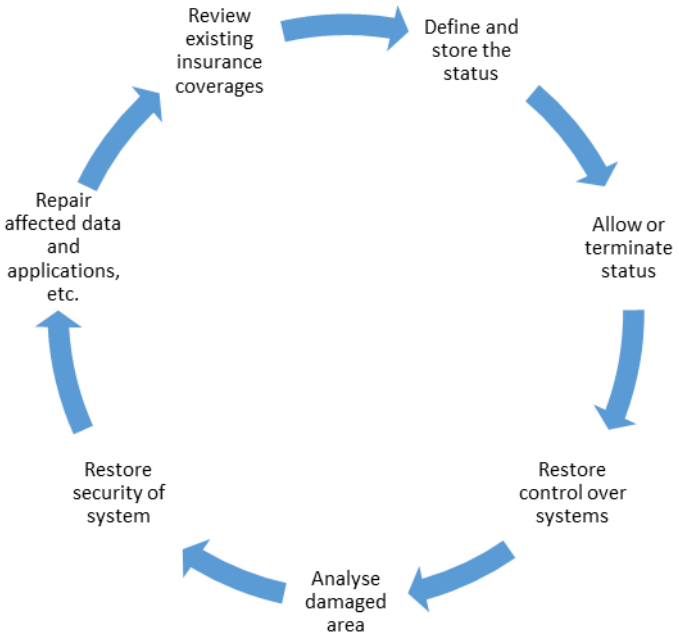
The damage caused by malware and APTs is extensive but even worse, attacks can rage on for weeks and months before being detected.



The seven steps

Business Continuity Plan (BCP) for a cyber-related harm can be based on the existing structure of Business Continuity Management (BCM) model for cyber. This structure consists of seven steps, which must be performed if a cyber emergency occurred:

1. Define and store attack status
2. Allow or terminate attack status
3. Restoring operational control over hardware, software and data
4. Analysis of the damaged area
5. Restoring security of the IT environment
6. Restore and reinstate any changes
7. Review existing insurance coverage.



We Below we further explain the decisions and the actions required.

STEP 1: DEFINE AND STORE ATTACK STATUS

In many cases a cyber-incident will require immediate attention.

Generally the operators want to start solving the incident. However, it is recommended that before any action is taken, the situation at the time of the incident is frozen. In this way a copy of the actual situation is welcomed in both the research phase and later in any legal or technical disagreement of parties, who have contributed to the solution or are held liable for negligence in the quality of services provided prior to the attack.

STEP 2: ALLOW OR TERMINATE ATTACK STATUS

At this step it may be considered not to terminate the "unsafe" situation, but to benefit from a life situation. With the aim of learning more about the cyber situation and the original route from where the impact is initiated. This intelligence can be of assistance for the recovery process, but it may also be that the local Police / Cyber security Authorities insist on continuation of the event to analyze and isolate a wider network of attackers.

This may be in the interests of the national cyber security strategy, but in the same way it will benefit the party involved.
It is evident that this challenge will have an impact in maintaining control over its own business environment, the more as the situation may arise, that as a result of the organization whether Corporate or not the increasing hindrance and loss of system integrity may effect loss of sales.

STEP 3: RESTORING OPERATIONAL CONTROL OVER HARDWARE, SOFTWARE AND DATA.

The operator may require professional support to manage the uncontrolled situation and to restore systems following crypto lockers or other malware.

Moreover where the hacker has created access to the system the hidden exploits need to be found and as full integrity of the system is to be regained.

It is evident that the operator will benefit from a speedy return to a situation, where it has control over its hardware, software and data.

STEP 4: ANALYSIS OF DAMAGED AREA

In laymen terms one can say that the above situations are more or less equal to the discovery of the fire and the quenching of it under step 3.
Where control is brought back to the operator, the next stage is the (forensic) analysis, as it is needed to discover where matters have been copied, added or deleted or values were changed.

During this integrity analyzing step, forensic research is required of the modus operandi of the attack , the assumed objective, and the discovery of traces left behind in the system. This forensic investigation will also drive to the discovery of the root cause of the cyber incident, where and how the incident could have occurred.

The response time in such an event is very much dependent on the risk considerations prior to such an event.

Where the loss of data or the copying of data refers to data falling within the definition of the Personal Data Protection Regulation , the situation arises of the fact of a breach of the regulation around the Personal Data Privacy.

This will require a prompt reaction and notification of the countries in which the private persons reside.

Non conformity to national and European regulation of Data Privacy breach expose the operator to serious fines potentially reaching up to 4% of the global revenue.
It may be interesting to note that there is no penalty for loss of encrypted personal data.

EU Data Protection Directive (also known as Directive 95/46/EC) is a directive adopted by the European Union designed to protect the privacy and protection of all personal data collected for or about citizens of the EU, especially as it relates to processing, using, or exchanging such data. Directive 95/46/EC encompasses all key elements from article 8 of the European Convention on Human Rights, which states its intention to respect the rights of privacy in personal and family life, as well as in the home and in personal correspondence.

The Directive is based on the 1980 OECD "Recommendations of the Council Concerning guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data."
These recommendations are founded on seven principles, since enshrined in EU Directive 94/46/EC:

- Notice: subjects whose data is being collected should be given notice of such collection.
- Purpose: data collected should be used only for stated purpose(s) and for no other purposes.
- Consent: personal data should not be disclosed or shared with third parties without consent from its subject(s).

- Security: once collected, personal data should be kept safe and secure from potential abuse, theft, or loss.
- Disclosure: subjects whose personal data is being collected should be informed as to the party or parties collecting such data.
- Access: subjects should granted access to their personal data and allowed to correct any inaccuracies.
- Accountability: subjects should be able to hold personal data collectors accountable for adhering to all seven of these principles.

In the context of the Directive, personal data means "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity" (Article 2a).
Data is considered personal when it enables anyone to link information to a specific person, even if the person or entity holding that data cannot make that link. Examples of such data include address, bank statements, credit card numbers, and so forth.

Processing is also broadly defined and involves any manual or automatic operation on personal data, including its collection, recording, organization, storage, modification, retrieval, use, transmission, dissemination or publication, and even blocking, erasure or destruction (paraphrased from Article 2b).

These data protection rules apply not only when responsible parties (called the controller in this EU directive) is established or operates within the EU, but whenever the controller uses equipment located inside the EU to process personal data. Thus, controllers from outside the EU who process personal data inside the EU must nevertheless comply with this directive. EU member states set up supervisory authorities whose job is to monitor data protection levels in that state, and to advise the government about related rules and regulations, and to initiate legal proceedings when data protection regulations are broken.

All controllers must notify their governing authority before commencing any processing of personal information, and such notification prescribes in detail what kinds of notice is expected, including name and address of the controller or representative, purpose(s) of the processing, descriptions of the categories of data subjects and the data or

categories of data to be collected, recipients to whom such data might be disclosed, any proposed transfers of data to third countries, and general description of protective measures taken to ensure safety and security of processing and related data

STEP 5: RESTORING SECURITY IT AROUND

When step 4 is completed, better understanding is made of the vulnerabilities of the IT environment.

Subsequently a review of existing and required security standards and implementations are a priority, and where needed an investment is to be made to meet up-to-date standards and a security infrastructure in line with the vulnerability of the organization in question.

A new strategy may be required at a logic and hardware level, but also human behavior and IT access authorities require to be re-visited and stress tested.

The response time in such an event is very much dependent on the risk considerations prior to such an event.
It is therefore required to maintain proper security strategies as well as pre-agreed service providers of companies like forensic investigators etc.

In the approach to review the IT security environment the following questions are to be answered.

- Were all releases of the system patches, firewall, virus software up to date,
- What extra security ID / password procedures were not adequate,
- Was encryption in place or should it be considered as part of the environment,
- What failing applications need to be upgraded or migrate to new levels,

- Pending the nature of the business even the need to introduce a more comprehensive monitoring of all traffic; called SIEM environment (Security Information and Event Management) may be required. The latest security is moving in a dynamic watch over all traffic to predict or detect unexpected traffic as a pre-alert.

Any kind of increased integrity of the security environment should be considered separately, but the interconnectivity of systems and traffic brings the need for IT specialists in the fields of hardware, infrastructure, device communication, data and data privacy breach.

The experience of a challenge of company sustainability and associated job losses bring a good learning curve, but like with fires it is better to without them.

STEP 6: RECOVERY OF DAMAGE CAUSED OR CHANGES

On the basis of the analysis step 4, one must have gained insight where data integrity was challenged or information is copied. In step 5 security is analyzed and generally improved. What remains is step 6 the recovery of the damage caused and the changed made.

One will require to restore data and software over and one must consider that the backups are also infected, as hacks and virus attacks etc. are often be detected a few months later.

It is evident that proper back-up security management is a strategic element for a speedy disaster recovery. Do we have the adequate back-ups in house , external or do we need to download high volumes of GB from the Cloud, which may need to be managed by contract.

STEP 7: ANALYSIS OF COVER DAMAGES UNDER EXISTING POLICIES

An organization being an SME, Industry or Corporate that has been exposed to cybercrime will be faced with costs.

Given the impact of legal advice and IT forensics and possibly other investment like a.o. consumer relation management and marketing responses lead to amounts, which may be undesirably high.

Existing insurance policies or service contracts will need to be scrutinized for financial contribution.

Perhaps not all repairs and financial losses are covered under existing insurance policies.

The closing of a (cyber) insurance or improve the safety and internal procedures can both be considered together. The first bring protection against financial instability of the company, whilst the second bring sustainability and operational stability of the day to day operation.

To manage the unexpected it can be recommended to consider Business Continuity Management as a training and process platform, which should lead to a Business Continuity Plan viz. a Disaster Recovery plan covering the above steps.

The discussion about insurability or too high premiums or deductibles may generate support and can be off set against the need to invest in a security management to the BCM and BCP project and the vision of the fulfillment of the responsibilities of the company and its employees.

HOW DO WE REVIEW A BUSINESS CONTINUITY PLAN

A good methodology is the work along the line of a Triage model, where questions need to considered and answers require decisions. Moreover answers may need to be provided by owners of the subject matter.

Triage
In this triage the below mentioned seven steps need to be weighed.

T1: Does the organization , when legally exposed to regulatory matters, require legal assistance to control the potential breach and or any possible penalties in its own or other countries

T2: Is the organization adequately equipped to deal with complex IT hack and what IT security standards do we require to defend our interests

T3: Is the organization exposed to mandatory publication of the incident, and how does it manage a loss on a public relation platform

T4: Is personal data of consumers at risk. As of what level of breach do we need to warn the consumer

T5: Is the occurrence of such a nature that various government agencies like the police must be informed and within what timeframe should it then be done

T6: Who is coordinating internally all these actions now and in the future

It is clear that if the triage is completed and sufficient attention has been given to all subjects, which gives a great advantage in preparation Disaster Recovery or Business Continuity Plan.

How to protect yourself …
Security best practices dictate that mission critical applications and data be separated in secure segments on the network, based on Zero Trust principles ("never trust, always verify").

On a physical network, Zero Trust is relatively straightforward, using firewalls and policies based on application and user identity.

In a cloud environment, direct communication between virtual machines within a server host occurs constantly, in some cases across varied levels of trust, making segmentation a real challenge.

Mixed levels of trust, when combined with a lack of intra host traffic visibility by virtualized port based security offerings may weaken your security posture.

Governance and management work best if they' re based on a set of smart policies, processes, and training, developed by the four major stakeholders in the organization' s network landscape: IT, HR, executive management, and the users.

Clearly IT has a role to play, but it can' t be the strictly defined role that it often plays.
Neither can IT be lax about its role as the enabler and governor of applications and technology.
Even if IT leads the efforts to create and promote secure procedures and practices, the other three stakeholders should play a part in training employees to be aware of risks and vigilant about potential attacks.

Insurance matters
The above already gives a good insight in to the risk elements an underwriter is facing, and these elements are therefore also the basis of the loss adjusting aspects to consider.

The Cyber policy market is presently providing two models, which either provide hands-on support – a kind of repair in kind cover – or a specific cyber cover , where the policy needs to be triggered.
The latter a generally either existing polices extended with cyber clauses or specific cyber risk policies.

The extended version may challenge the conventional considerations as the situation of risk may be the virtual systems operating outside the confinement of a site , data in the cloud or at a datacenter and therefore not necessarily the situation of risk as defined in the policy.