INVESTIGATING COMPUTER CRIMES IN ORGANISATIONS: A QUESTION OF COLLABORATION BETWEEN THE INVESTIGATOR AND THE INFORMATION SYSTEM SECURITY MANAGER

Solange GHERNAOUTI-HÉLIE[1], Bertrand LATHOUD[1], Olivier RIBAUX[2]

[1] *HEC, INFORGE, Université de Lausanne, Lausanne, Switzerland*

[2] *Institut de Police Scientifique et de Criminologie, Université de Lausanne, Lausanne, Switzerland*

ABSTRACT: Computer crime is an epidemic form of crime against which no business, or customer is immune. It can deeply affect each organisation or people who depends on information and communication and the result may be tragic. It is fundamental to be able to: protect computers, networks and information systems resources and data; identify attacker;
prove they fault; pursue them.

The first point is relevant as it covers the ability to define, implement and validate a security policy which must be effective and efficient for an organisation. This is under the responsibility of the security IT manager who has to protect the valuable resources of his enterprise and to prevent it against potential attacks.

The IT manager knows the context of his company and its security's requirements. But, he generally has little knowledge of the criminal context and the investigative methods. On its side, the police officer does not know the environment of the victim. Indeed, the complementarity of both partners is critical to ensure the global effectiveness of the investigative process. This collaboration often works well, but the conditions of success are poorly formalised.

We propose several parameters that influence this co-operation positively, and exploit them under the form of an action plan. This does provide easily applicable guidelines for the IT security manager for an optimal intervention of the crime investigator.

KEY WORDS: Computer-crime; Investigation; Digital traces; Management.

Problems of Forensic Sciences, vol. XLVII, 2001, 43–48
Received 23 February 2001; accepted 15 September 2001

INTRODUCTION

The massive dissemination of the tools for automated information's processing opened new opportunities to the criminals. They have learned how to exploit the knowledge and specialised tools available on the Internet.

The computer crime becomes today commonplace. It takes on various forms and affects the most different organisations. It is consequently important to define right now the procedures to be implemented if one wishes to facilitate the identification's work of the perpetrators by the justice.

Before being able to determine the structure of the procedures which will allow to improve the collaboration among investigators and responsibles for the systems of information, it is indispensable to clarify the outlines of what is commonly called computer crime, and what are its consequences for organisations.

HOW TO PROTECT FROM COMPUTER CRIME

Various forms of computer crime and consecutive needs of protection

It could be possible to consider any intervention in a system of automated data processing as a form of computer crime. This one can take on several aspects: denial of service, sabotage of systems, theft of information or hardware, deception, the destruction of equipments or data, usurpation, to mention only some well known.

Variable consequences on the functioning of organisations, are the result of the realisation of a computer crime. Whatever form it takes, it leads in various degrees to a loss of confidentiality, availability, reliability, integrity, know-how, credibility, etc. which finally, result in economic and even human damages. In a global economic context such as the one that is outlined through the globalisation of economies, it is vital for numerous organisations, to ensure an effective protection of their Information Systems.

How to protect itself

To protect itself correctly, an organisation should know how to set up some structures. At first, it is a question of defining a coherent security policy in relation to the strategy and needs of the organisation. It goes in particular through an evaluation of the risks and threats which can potentially affect the activity of the organisation.

The management of this policy comes essentially within the responsibility of the IT security manager. From an operational point of view it results in

the implementation of procedures, preventive tools; measures of monitoring, control and audit; and directives of reaction and report.

Lastly, the fast evolution of the technologies used as for the attack as for the protection requires the definition of a mission of security watch.

Mission of the IT security manager

Pivot of the management of the Company's Information System's securisation, the IT security manager (ITSM) participates actively in the evaluation of the informative risk, in the definition of the security policy, as well as in the choice of the procedures and tools needed for its realisation. He manages the daily activities, at all levels: strategic, tactical and operational. He ensure the control, validation, and updates of the security means.

He also has a duty of information towards the leaders of the organisation, what brings him regularly to draft synthesis and analysis reports.

As every administrator, he is subjected to constraints of financial, technological, human and temporal order.

DIFFERENCES OF PROFESSIONS, DIFFERENCES OF PERSPECTIVES AND POTENTIAL OBSTACLES

Quality, know-how, different constraints and objectives are at the origin of numerous incomprehensions among an investigator and an IT security manager. The risk is big to see these differences becoming real obstacles to the proper functioning of the investigation.

Whereas the IT security manager tries to recover its systems in the most brief time, to ensure the continuity of the production, the investigator is subjected to the formal constraints of the penal procedure which requires on him to obtain as much traces as possible, and to preserve them in accordance with very precise legal standards.

The concern of reactivity of the IT security manager is going to incite him to concentrate on the means needed to stop the aggression and limit its consequences.

The problem of identification of the author is for him secondary towards the preservation of the activity of the organisation. The recovery of the system represents so for him the end of the incident while it is often situated at the beginning of the investigator's intervention (temporal gap). The procedures of reboot of Information System are often contradictory with the conservation of traces which would allow to prove the reality of the attack, to select a group of suspects, and to obtain possible legally valid evidences.

Furthermore, this gap can be also widened by some behaviours of an IT security manager or a system administrator, if these try to resolve the crime

by themselves. They possess generally a partial knowledge of the legal constraints consecutive to the conducting of a penal investigation. They usually are not experienced in a correct management of the existing traces. Besides, their different attempts will also have the effect of delaying the implication of the police forces, and in many cases, awakening the attention of the offender. Furthermore, they can be actively involved in the criminal process.

All this will generally have the effect of slowing down, and even hindering, the progress of the investigation.

On his side, the investigator has an insufficient vision of the technological, organisational and human context of the concerned entity.

A certain number of obstacles to the smoothly functioning of the investigation are added to these causes of incomprehension. Such a new form of crime leads also, besides the damages provoked directly by its commission, to an erosion of the image of the attacked organisation, what has for consequence a low level of denunciation of the computer offences. Furthermore, the negative image often associated to the supposed weakness of the investigator's technical knowledges, strengthens this hesitation to report officially the undergoing attacks. This perception of a relative incompetence is strengthened by the lack of real of communications strategy on these subjects, on behalf of the police forces. Insufficiently proactive, they do not succeed in using the cases brought to their knowledge to draw a more general frame of a public policy turned to fight against cybercrime. It is why it is urgent to rethink relationship between police and Information System's managers, in order to succeed in fighting effectively against these emergent forms of crime.

A MANDATORY COLLABORATION

To be effective, the collaboration between the investigators and the IT Security Manager, will have to be based on a certain number of points that can't be ignored. The various involved parties have to respect the basic principles of an effective collaboration in this particular sector.

Principles for an effective collaboration

It is not possible to envisage the reduction of the cultural and technological gap separating policemen and system without underlining the mandatory, inevitable character, of their collaboration in case of investigation. It should go through the understanding of the each one's objectives, and the recognition of the importance of the temporal constraint in the management of their collaboration. It means in particular that the human dimension of this interaction should be privileged. The technological aspect should re-

main a support for the action It's why the translation of the ideal principles, in a reality not always controllable, is going to imply a process of planning and preparation of the conducting to be followed which should notably determine each one's area of action. So, the investigator will know where to conduct the investigation according to the information obtained at once from the Security Manager of the targeted system.

This one has a great interest to follow a predefined frame if he wants to accelerate the progress of the investigation and then to get back the control of his system as soon as possible.

What responsibility for the IT security manager?

In order to make their possible collaboration the most effective, the ITSM should be able to supply the elements which will help the investigator in his work. It consist for the main part in the definition of the monitoring policy of the system, through specialised tools like intrusion detection systems, as much as through of the implementation of active audit procedures. It is also necessary to take care of the specifications of the backup and filing in order to increase the conservation of good quality electronic traces. This is particularly appreciable when the investigation is followed by a lawsuit. A judge will be all the more inclined to accept an electronic trace as valid element in the preparation of the case for an eventual judgement, that this digital trace will have been collected within the framework of the daily management of the system.

These elements are defined during the conception and implementation of the Information System. The coming of an investigator is then an eventuality that one wishes the least likely. However, when an incident has occurred, it can be useful to have additional information which could accelerate the work of the investigator. First of all, it is about the complete inventory of the human, software and hardware resources which make up the information system of the organisation. In particular, the configuration and location of the computer systems and the networks should be available, as well as a logical map of the information system. Secondly, it is convenient to operate specific tools of collection, memorisation, and analysis of electronic traces, which respect the constraints in which is subdued the procedure of investigation. It concerns the operational management tools of the network, the analysis means of the traffic, the audit methods, the intrusion detection systems, the firewalls, and the log files. The common use of rigorous procedures of authentification of the data produced by all these means, in particular through the integrity control and the time stamping of the corresponding files, should strengthen the value of the electronic traces which they can supply. Eventually, an additional guarantee is brought by the regular conservation of the most important data (logs of logins and errors) on supports

such as CD-ROM and DVD-ROM. It is necessary to underline that these various means will see their "judicial" value increasing by the yardstick of the regularity with which they are operated.

CONCLUSION

One can not keep any more, today, to a security policy based essentially on prevention and detection. Such a point of view would mean that criminals, in this domain, are not as good as their homologues of the "real" world...

It is mandatory to include, as soon as the conception phase of a security strategy, the elements needed by an effective collaboration between IT security managers, and investigators in charge of tracking possible traces after the commission of an offence. To make it possible, it seems that two ways have to be preferred. It is first of all necessary to create the conditions of a real dialogue between representatives of two professional worlds who misunderstand each other. It is then unavoidable to alter the methods of conception of Information Systems, in order to allow, as soon as they are used in production processes, the protection of the information generated by the management of the system, in order to use it during the judicial proceedings of possible delinquents. The tools helpful to make the most of these "deposits" of daily data, remain to invent, or at least to be improved for those of them who already exist.

PRACTICAL MEASURES

- Logs should be protected and authenticated.
- Backup supports for log files should not be rewritable.
- The format of these files should be as universal as possible (text?)
- The place where backups are stored should be protected.
- The duration for backup storage should be long enough.
- The risk analysis performed during the elaboration phase of the security policy should lead to the definition of quantitative parameters allowing to measure how critical are the different log files.
- Security policy should be implemented and managed by skilled professionals.
- These practical measures should be integral part of the specifications of the security policy.