A SYSTEM FOR MANAGING RISKS ASSOCIATED WITH EMPLOYEES
INTERACTIONS WITH THE IT INFRASTRUCTURE
NAJIB SAYLANI
HOFSTRA UNIVERSITY
134 HOFSTRA UNIVERSITY HEMPSTEAD NEW YORK 11549
NAJIB.SAYLANI@HOFSTRA.EDU
516-463-4746
KHALID SOLIMAN
HOFSTRA UNIVERSITY
134 HOFSTRA UNIVERSITY HEMPSTEAD NEW YORK 11549
KHALID.SOLIMAN@HOFSTRA.EDU
516-463-1549

ABSTRACT
This paper presents a proposal for a system by which a given organization would manage
human related security breaches as they arise within the IT environment specific to that given
entity.

KEYWORDS
Social engineering, balanced score card, fuzzy system

INTRODUCTION
These days, the risks associated with activities of an employee affecting critical areas of an IT
infrastructure are too high to ignore. These activities are associated with access to sensitive
information and the IT means to access them. The processes that the system will handle in this
new type of risk management are similar to those a security expert would handle. We are not
talking about computer forensics, but forecasting future breaches through real time and
continuous monitoring of all subsets of the IT infrastructure that is directly used by some or all
employees. One of the many risks an organization needs to be aware of is what we will label as
‘internal social engineering’ [7]. The proposal is related to previous work we have done in this
area [9]. In the context of information security and human factors in guarding against attack
against a corporate IT infrastructure, social engineering is the process by which a person
receives confidential information to gain access to restricted areas by acting or posing as
someone else. The social engineer uses deception to reach his/her goal [7]. No matter how
secure a corporate IT infrastructure is, it is still vulnerable to attacks through means that would
overcome even the strongest firewalls and encryption systems [2]. The safest system still has
the human nature as one of the weakest links in its chain of defense. It is well known in the
computer security business that securing an IT domain should take into consideration the
implementation of well defined protocols [1]. Among these protocols are rules by which
employees of a corporation will interact with each other and with persons other than their
colleagues. In many cases, a disgruntled or even careless employee can cause more damage as
his/her actions may go unnoticed for a long time. There is too much managerial focus on external breaches in security caused by non-employees, while many systems’ managers ignore the security threat posed by in-house. The chain in the business of IT security has a more complex structure than what is depicted in most text books. Furthermore, there is evidence that the most volatile and unpredictable links in this chain are actually human and not an encryption program nor an expensive firewall. The human factor is ignored most of the time because of the level of trust in the screening of potential employees during the hiring process and respect for employees’ privacy.

It is time for organization relying on IT for day to day business to start focusing on internal risks associated with their own employees [10]. A new risk management approach in this area must be created. A new system by which a knowledge base is created and populated with historic facts either from external sources or simulated internally. Virtual and transparent ‘E-drills’ in the area of IT security must be conducted to detect risks within the organizations before they arise in reality [5][6].

Further more, any entity should be treated as a heterogeneous dynamical system where human interact with other humans and processes interact and react to other processes.

**PROPOSED SYSTEM**

An initial phase of this project consists of collecting cases that are pertinent to developing such system. Most documented cases are related to past experience of computer forensics dealing with system intrusions and network attacks. A small set of cases deal with acts of deception and social engineering. Some literatures do focus on this side of the problem and the remedies offered are adoption of new protocols and policies dealing with employees’ behavior interacting within an IT infrastructure [1][3][4]. Part of this phase is about discussing the research and hopefully getting good feedback on what constitute good practices in policing employees’ interaction with the local environment and remote systems. We decided to restructure any knowledge equivalent to past experience that necessitated computer forensics. In this case, while computer forensic trace a set of event back to try to find the source of a problem, we need to re-arrange those events to playback different scenarios in relation to there respective environments in order to pinpoint all potential entities involved or may have being involved. Computer forensics is using what was left after an attack to trace a chain of events to the culprit [12]. We are focusing on other hidden variables that can only be inferred with deeper analysis of what could/might have happen. We intend to project some paranoia into the process to exaggerate known consequences to come out with the worst case scenario for each case studied. At this stage, our feeling is that the task is time consuming and difficult at the same time but doable. The analysis process is done without the help of any tool in order to maximize human expertise and extract the necessary and efficient approaches that we can implement later in our proposed system.

The next stage in developing the system is to design an Agent based subsystem that help in collecting information, and mining the knowledge base for patterns that map to a known profile(s) of security breaches. An example of such approach, although in a different context than security, is depicted in [8]. We plan to complement the system by exploring the use of balanced score card by all employees, implementing day-to-day survey to collect information associated with events related to employees interaction with each other, and finally, the use of fuzzy logic. A fuzzy logic subsystem expands the whole system to one that inter-relates experts
and non-expert observations and findings within the organization, and help in generating
decisions that best safeguard the organization against human triggered security breaches.

CONCLUSION

While there are many applications out there used to directly monitor the employee’s interaction
with the IT infrastructure, this paper outlined a proposal for a system that goes one level deeper
to mine for patterns of security breaches as they arise and by detecting dependent and remote
events. The system, unlike traditional monitoring system, can utilize partial information and
correlate it with other newly detected or stored pattern to decide if an ongoing security breach
is developing. The proposed system together with the proactive approach of involving
employees through the adoption of a balanced score card in the area of security is a novel
approach.

REFERENCES

Organizations, Logistics Information Management; Volume 15 No. 5; 2002
Firewalls, Information Management & Computer Security; Volume 10 No. 3; 2002
[4] Harris, Geoffrey, Security and Fraud: Strategies for Prevention and Detection,
Logistics Information Management; Volume 4 No. 3; 1991
[5] Helms, Marilyn M; Ettkin, Lawrence P; Morris, Daniel J, Shielding your company against
information compromise, Information Management and Computer Security; Volume 8 No. 3;
2000
[6] Higgins, Huong Ngo, Corporate system security: towards an integrated management
approach, Information Management and Computer Security; Volume 7 No. 5; 1999
[8] Rus, D., Gray, R., Kotz, D., Autonomous and Adaptive Agents that gather Information,
[9] Saylanì, N., An Automated Approach to Detecting Human Deception for IT Security,
IBIMA, December 2003
[10] Siponen, Mikko, T, Critical analysis of different approaches to minimizing user-related
faults in information systems security: implications for research and practice,
Information Management and Computer Security; Volume 8 No. 5; 2000
Modeling, Kybernetes: The International Journal of Systems & Cybernetics; Volume 32 No. 5;
2003
Wesley 2002
[13] White, Gayle Webb; Pearson, Sheila J, Controlling Corporate E-mail, PC Use and
Computer Security, Information Management & Computer Security; Volume 9 No. 2;