Association for Information Systems
AIS Electronic Library (AISeL)

ACIS 2001 Proceedings

Australasian (ACIS)

2001

The Role of Information Systems in Information-Level SecurityManagement

Christopher Lueg
University of Technology Sydney, lueg@it.uts.edu.au

The Role of Information Systems in Information-Level Security Management

Christopher Lueg

Department of Information Systems
University of Technology Sydney, Sydney, Australia
lueg@it.uts.edu.au

Abstract

Proliferation of computers and networks in the age of the Internet has not only enabled novel services, such as email, the web, and electronic commerce, but also new ways to affect companies, their businesses, and their reputations. A look at the relevant literature suggests that so-called information-level threats are not yet sufficiently addressed. In this paper, we provide a summary of the current situation and outline the role of information systems in helping organizations cope with information-level online activities.

Keywords

Online Activities, Information Dissemination, Security Management, Shared Threat Recognition

INTRODUCTION

The importance of the Internet as medium for communication and information dissemination has increased significantly over the past few years. The daily lives of people are more and more affected by information technology and network-related services, and it seems to be appropriate to talk about the rise of the Network Society (Eriksson, 1999). Proliferation of computers and networks has not only enabled novel services, such as email, the web, and electronic commerce, but also new ways to threaten companies. Media coverage is guaranteed if companies such as Microsoft were hacked (e.g., Bridis and Buckman 2000) or if access to the company's web servers was denied while hackers launched a Denial-of-Service (DoS) attack against their domain name servers (e.g., Yasin 2001).

It is now widely acknowledged that computer security is an important topic and the state-of-the-art in computer security provides some protection against threats ranging from hackers trying to break into corporate computer systems to DoS attacks. Companies should be able to reduce vulnerabilities as well as the potential impact of still successful attacks. However, as Bellovin (2001) points out, it is unlikely that there will ever be a "security end state". Accepting that software will be buggy, will have holes, and will be insecure is an important step towards a realistic assessment of computer security and towards a lasting change of attitudes and expectations.

In addition to being prepared for attacks on corporate computer systems and networks, evidence exists that it becomes increasingly important to be aware of potentially threatening activities that are based on the virtually unrestricted dissemination of information. Examples range from the (possibly purposeful) creation of myths and urban legends to setting up web sites that help spread biased information to spamming under the identity of competitors (so-called joe jobs) to harm the competitor's reputation.

So far, threats on the information level-referred to by lawyers as "commercial terrorism through the Internet" (Braun et al., 2001)-have not received much attention in the computer security and security management literature. A look at the relevant literature suggests that these fields tend to focus on making corporate computer systems and networks secure in order to protect them against undesirable activities. The problem is that threats on the information level happen outside such secure corporate environments as they are based on the dissemination of information rather than on direct attacks. In most cases companies will be affected only indirectly which makes prevention, recognition, and reaction difficult.

For companies it is increasingly important to be aware of information-level online threats as more and more people are using the Internet to access information about their (prospective) business partners. In this paper, we argue that information-level security management is needed as response to information-level online threats.

We proceed as follows. First, we provide some examples of recent incidents to illustrate the threat potential of information-level online activities. Then, we provide a working definition for information-level activities that allows to distinguish such threats from lower-level network-based threats and summarize the current situation from an IS perspective. Next, we draw conclusions for IS and outline the role of information systems in helping companies cope with information-level threats. Finally, we summarize our findings and discuss future research directions.

EXAMPLES FOR THREATENING ONLINE ACTIVITIES

Hacking of computer systems and launching of DoS attacks as well as spreading of malicious code, such as viruses, are well-known online threats and are receiving the attention they deserve in the computer security and security management literature. Far less attention receives the fact that the Internet has enabled a range of potentially threatening activities that are based on the active or passive dissemination of certain information. In what follows we list a few examples of such information-based activities.

Myths, Rumors, and Hoaxes

Hoaxes are false email messages with the only purpose to spread to as many people as possible. Along with myths and urban legends they live on the Internet. Such messages may have significant impact on companies, their reputations, and thus their businesses.

The designer Hilfiger was the victim of a threatening urban legend (Ulfelder, 1997). The legend goes that Hilfiger appeared on the Oprah Winfrey Show and made racist comments about several groups, after which he was tossed off the set by Winfrey. In fact, Hilfiger has never appeared on or taped an episode of Winfrey's show but the legend spread so rapidly and generated so much controversy among customers and potential customers that the company was forced to respond on the net.

More recently, the globally operating mobile phone company Ericsson was the victim of a hoax promising recipients free mobiles if they forward the letter to at least twenty people (Park, 2000). Ericsson received thousands of email from people asking for their free phones. The article quotes an Ericsson Australia spokesman claiming that the company was aware of the email circulating for at least a couple of days and that the way it was sent makes it impossible for them to see where the email originated from.

Fumento (1999) reports the story of a little Canadian manufacturer using its web site to spread information that products of competitors may be horrible dangerous. Moreover, the company's marketing head has been observed to actively support feminists preparing a petition to start a boycott of the company's competitors. According to Fumento (1999), however, scientific investigations suggest that the information is nothing but a myth.

Revenge Web Sites and Fake Web Sites

Setting up a (revenge) web site has shown to be a powerful way to affect opponents or competitors. Ulfelder (1997) describes a web site that supposedly contributed to a car manufacturer's recall of 8.7 million cars and trucks in the US, costing the company approx. US$ 200-300 million.

McSpotlight (URL http://www.mcspotlight.org) is a web site that is dedicated to informing people about the practices of the global fast food company McDonald's. The web site has its origins in McDonald's trying to sue green critics to silence who distributed a leaflet "What's wrong with McDonald's" in back 1996 and provides the information McDonald's tried to suppress. According to Michie (1998), the libel case qualifies as one of the biggest public relations disasters in recent times although McDonald's won in most parts but the company's most embarrassing dirty laundry was aired in the national media. McSpotlight claims that it is virtually impossible to shut down the site as the server is located in a country with fairly liberal laws (as opposed to Britain where the "McLibel" case took place), a number of mirror servers exists all over the world, and last but not least no particular person being responsible for the site in such a way that suing this person would endanger the site.

A different usage of web sites occurred in 1999 when a faked Bloomberg web site announced that a company called ECI Telecom bought a company called PairGain Technologies Inc. (Neue Zürcher Zeitung, 1999). The notice pretended to be an official notice released by Bloomberg which is a well-respected information agency. The fake lead to an increase of the value of PairGain shares. The fake was distributed via a web-based message-board and interested users were guided to a faked web site imitating the design of Bloomberg's original web site.

Chai (1999) describes how search engines can be manipulated to harm companies. A third party web site used information describing a popular web site to fool surfers searching for this particular web site. When using a search engine, surfers were directed to a porn site rather than to the web site they were actually looking for.

Joe Jobs

A more direct method to cause damage is to hire a spammer for a "joe job" which is when somebody spams under the name of another person's domain, or web pages in revenge to get them kicked off the Internet. The effect of the spamming is that lots of people complain to the Internet service provider (ISP) hosting the domain advertised in the spam as they mistakenly assume the domain would be the source of the spam. The global prosperity web site (URL http://www.global-prosperity.com), a site dedicated to collecting information about a particular Get-Rich-Quick scheme aggressively advertised on the Internet, describes how the web site is being attacked by means of "joe jobs". There is some evidence that "joe jobs" are increasingly used to silence opponents as well as competitors on the Internet.

Denning (1999) provides further examples. In addition to incidents reported in the literature it is reasonable to assume the existence of further incidents as companies may not be aware of threatening information circulated online or companies may have chosen to deliberately ignore these information. Ulfelder (1997), for example, reports that the US-based car manufacturer Ford decided not to go online to combat a certain revenge web site as the company was afraid that anything they would do on their own web site would validate what is described on the revenge web site.

INFORMATION-LEVEL ONLINE THREATS: THE CURRENT SITUATION

The previous section suggests that for companies it is important to be aware of information-level online threats. In what follows, we summarize the current situation from an IS point of view. We start with a definition of information-level threats and an overview of the coverage of these threats in the literature.

A Working Definition of Information-Level Threats

We define information-level threats (or: information-based threats) as threats that involve the (purposeful) dissemination of information in such a way that companies, their operations, and their reputations may be affected. Dissemination may be active as in the case of sending email or dissemination may be passive as in the case of setting up web sites.

It is important to distinguish information-level threats from network-level threats. By network-based threats we mean that in order to become effective potential threats require network access to corporate computer systems or to networks used by corporate computer systems. Examples for network-based threats (or: threats on the network layer) are the already mentioned hacking of computer systems and launching of DoS attacks as well as spreading malicious code, such as viruses. Other security issues involved when data are transmitted over networks are confidentiality, authentication, integrity, and nonrepudiation (Batten, 2000).

Information-level threats also make heavy use of network but the primary lever is the content of a message rather than its form. Sending faked inquiries to service accounts to eat up resources would qualify as information-based attack as it is the content of the messages that would provide the lever for the attack. Other examples for information-based threats are setting up revenge web sites and disseminating false or biased information as in the case of the false Hilfiger accusation. Dissemination of information that is likely to trigger specific counter reactions as in the case of "joe jobs" also qualifies as information-based threat. To the contrary, a DoS attack that is based on flooding accounts with large quantities of email is a network-based attack as it is the size and the quantity of the email that matters; the content of the email does not matter.

Coverage in the Literature

The computer security related literature does not provide much information on how to address information-level threats. A look at the relevant literature suggests that the focus is on making corporate computer systems and networks secure in order to protect them against direct undesirable activities. Topics discussed at specialized computer security conferences, such as the Australasian Conference on Information Security and Privacy (ACISP), range from authentication and encryption to access control and intrusion detection. Threatening activities that are based on the dissemination of information, however, are happening outside secure environments.

Security management provides some information but does not directly address the problems discussed in this paper. Several related papers were presented at the 1st Australian Information Security Management Workshop (AISM) in November 2000. A paper by Warren and Hutchinson (2000) helps illustrate some of the difficulties of the terrain. The authors discuss a faked web site that has been set up with the intent to capture credit card numbers and other information as example of a spoofing attack. As protection against such bogus web sites they propose to use authentication so that the client can be sure that he or she connects to the right web site. In the context of this paper, the solution is located on the network layer while the problem is mostly located on the information layer: how can a company become aware of a similar attack on its business and what would be an appropriate reaction once the fake has been recognized? Lichtenstein and Swatman (2000) discuss the need for holistic security management but their focus is on organizations and not so much on what is happening in the broader environment. Batten (2000) discusses the need for distributed security and argues that prevention alone is not sufficient. In particular, the author argues that the basic approach to information warfare security is the same as as for general business information security: prevent, detect, respond. Detection involves several components ranging from prior knowledge about potential attackers to appropriate reactions. This is the most relevant paper although its focus is on network-level threats rather than information-level threats.

From a security-oriented point of view, the main problem is that threatening activities typically happen outside secure corporate environment. Moreover, attackers do not have to get into contact with corporate computer systems which means that internal security tools, such as intrusion detectors or usage profilers, provide little help.

The information warfare literature provides some interesting material but it is everything but clear how information warfare relates to the activities discussed in this paper. Some relevance is given as misinformation have long been staples of conventional warfare and in some sense the similarities between the military and the business world grow each day (Cronin and Crawford 1999). Denning (1999) provides detailed information about technical and social aspects of penetration, manipulation, and information systems assurance. Cronin (2000) provides a comprehensive information warfare typology. What we call network-level activities would match levels two and three of his typology and information-level activities would match level five to some extent but it does not really fit. The paper by Hutchinson and Warren (2000) discussing strategies in information warfare mentions, among other things, two specific techniques in information warfare that are related to the activities addressed in this paper: flooding a target organization with information, thereby slowing stopping effective processing or analysis of the incoming information, and exposing confidential or sensitive information, thereby embarrassing or in other ways harming the organization.

Public relations is an area that is well aware of the potential threat of information-based online activities (e.g., Kalish 1997). Brauer (1998), for example, describes how a company specialized in public relations was hired to stem the damage caused by an Internet fraud. In fact, it is claimed "companies that fail to monitor Internet traffic may be headed for a public-relations disaster" (Ulfelder 1997). Several companies, such as IntelliSeek, CyberAlert, and eWatch are offering tools that are specifically designed to help companies monitor the Internet.

Ebbinghouse (2001) provides a lot of information how to handle threatening situations such as cyber smear and revenge web sites once they have been recognized. Examples discussed range from complaining to the owner to "bringing in the cavalry" which would be the relatively new Internet Fraud Complaint Center (which is located in the US) to launching a law suit. However, the paper is more a collection of hints rather than a systematic approach to addressing the underlying problems.

The Current Situation From an IS Point of View

At its best, the current situation can be characterized as complex:

- Little awareness of the potential threat of information-level online activities.
- Little knowledge about the nature of information-based threats. Some relevant knowledge is available but the knowledge is distributed over different communities ranging from security management to public relations to law.
- Little work has been done on the role of information systems in addressing problems, such as recognition of ongoing online activities.

We see the following main problems. First of all, activities have to be recognized. Tools are available but their strengths and weaknesses and their scope, in particular, are unclear as hardly any technical details are provided. Furthermore, technical approaches to Internet surveillance are always limited due to the Internet's distributed nature and the nature of information. Only a limited number of electronic communication channels can be monitored as monitoring has to be (technically) possible and (ethically) appropriate (Lueg 2001b).

Then, it may be difficult to understand the threat potential of activities on the information layer as the impact of these activities may manifest on a different level. For example, dissemination of information that is detrimental to a company's reputation is located on the network level but the impact of these information does not manifest on this level. Accordingly, tools that monitor network-level activities can hardly be expected to recognize the threat potential. Related is the problem that employees with expertise on the network level may not have the expertise necessary to assess impacts on other levels. An example for such information might be manipulated information about a company's shares.

Another aspect of the problem is that even on the network layer it may be hard to determine whether activities identified as "unexpected" indeed qualify as attacks. Schwartau (1999b), for example, reports that a network administrator on duty at a major Internet service provider (ISP) noticed thousands of connections to his firewall. Such a network scan could be the reconnaissance phase of a planned attack. The reconnaissance phase is the phase in which an attacker gathers information about the target system of network (Boulanger, 1998). The administrator considered this flood an attack and shut down several routers taking down a significant part of the Internet at that time. Investigations revealed that the flood was not meant as attack but the flood was caused when a scanning tool was used during an security assessment conducted by one of the Big Six accounting firms. Similarly, Needham and Dale (2001) report that the web site of the newly launched Australian "reality TV" show "Big Brother" was shut down as security systems mistakenly interpreted four times the expected traffic as attack by a hacker.

Last but not least, situation assessments are difficult as most companies do not have much experience in coping with information-level online threats. Potential impacts of reactions have to be considered carefully as over-reacting may be as fatal as ignoring a potential threat. A recent example for a wrong situation assessment in the context of the Internet is one of the world's largest media corporations, AOL Time Warner, being forced to back pedal when confronted by online communities. AOL Time Warner is the parent company of Warner Bros which is shooting the hyped Harry Potter film. According to Riley (2001), the company tried to shut down Harry Potter fan web sites when launching its own Harry Potter promotional Web site. However, one of the youngsters has teamed with other Harry Potter web site creators in Britain to form the Defense Against the Dark Arts project which is threatening a world-wide merchandise boycott. AOL Time Warner has issued a contrite statement, admitting that it may have been over-zealous with its letters and offered to talk to Harry Potter fans about their sites (Riley 2001).

THE ROLE OF INFORMATION SYSTEMS

Information systems (IS) can hardly answer the question whether an online activity observed qualifies as a threat or attack but information systems can support companies in recognizing information-level online activities and in organizing an appropriate reaction. In particular, IS can support the following phases:

(i) Recognize potentially threatening activities
(ii) Assess the relevance and the threat potential of activities identified
(iii) React (or ignore)

The recognition phase (i) is the phase in which information systems research can be expected to contribute most by providing advanced search technologies and visualization tools. In addition, IS can contribute to a better understanding of information-level activities and, in particular, to an understanding that is shared across the different levels and hierarchies in an organization.

Early recognition of potentially threatening online activities requires the monitoring of online activities. Tools supporting the monitoring of Internet activities are commercially available but their strengths and weaknesses is largely unknown. For example, a brand name could be mentioned in a discussion (which means that a search tool would indicate a "hit") without being the topic of the discussion. However, a discussion could also focus on a particular brand without ever mentioning the brand name. Apart from these technical issues, using such tools may require significant expertise as the context of online utterances may be important. Lueg (2001a) describes online discussions about the ignoring of quality standards in restaurants of a particular fast food company (which could produce lots of search engine hits on the company's name and brands) and reports that those sharing their bad experiences are nevertheless fans of the products offered by that particular fast food company. Therefore, considering the discussions as attack would certainly be a wrong situation assessment.

A related problem is that only large companies may have financial and other resources that are required to set up specialized teams. Warren and Hutchinson (2000) report that even allocating resources required for undertaking (basic) security reviews may be a problem for small and medium enterprises and monitoring online activities would require further resources. Similarly, hiring external specialists for monitoring Internet activities will only be an option for large companies. Batten (2000) expects that outsourcing security to professional businesses will become common.

In the case of companies who cannot afford outsourcing security or setting up specialized teams, it is the net savvy staff who are most likely to detect threatening online activities. Net savvy staff are typically technical specialists and other staff who are using the Internet for their regular work. It is important that knowledge concerning online activities detected is not kept but shared with others. As Lichtenstein and Swatman (2000) report, knowledge of Internet security matters is often available on lower levels in a company but effectively blocked at this point of the managerial chain to the top. It is reasonable to assume that similar block effects may occur in the context of threatening online activities.

A recent investigation by Pawlowski et al. (2000) describes that information technology (IT) professionals supporting shared information systems learned about their stakeholder communities and their specific characteristics. A shared (information) system is an information system that is used by multiple communities of practice. Maintaining shared systems is challenging as system changes may be triggered in any of the stakeholder areas while effecting other areas. Pawlowski et al. (2000) argue that the IT group observed has acquired an amazingly broad view, spanning both the informal boundaries of communities and the formal organizational boundaries. In particular, the authors argue that the professionals are put in brokering roles (brokering in the sense of Wenger 1998) and discuss how they could be used to enable knowledge transfer among communities. Lueg and Riedl (2001) have outlined how similar approaches could be used to enable effective socially-shared information management.

When assessing the relevance and the threat potential of activities identified (2), the IS task is to span levels and hierarchies in order to bring together different forms of expertise and different perspectives. For example, the above mentioned discussions of ignoring quality standards in fast food restaurants may be understood quite differently depending on an observer's background and expertise. An employee in the company's marketing department may understand these discussions as threat to the company's caring image in the public while an employee who enjoyed similar experiences may understand the discussions as opportunity to improve the company's business.

Assessing a threatening situation may lead to the conclusion that the situation is in fact a chance. As discussed by Ebbinghouse (2001), it is possible that those considered as threats were previously harmed by misinformation. If so, it would be best to compensate them, to make sure that the company's problem never happens again, and to spread the word. The same holds in the case of the newsgroup described in Lueg (2001a). Rather than considering such discussions as threats, it might be more appropriate to understand the online discussions as chance and use the information to actually improve services and to enhance the own reputation.

React (or ignore) (3) appears to be a "pure" action phase but IS are again involved as mediators and as monitors providing feedback. In fact, In fact, the three-step sequence should be considered as a loop as complex issues may not be handled straight away. For example, a threatening myth listed on a web site might have been deleted on that site but may re-appear on a different web site.

In the case of the Electronic Disturbance Theater's (Wray 1998) DoS attack on servers operated by the US Department of Defense (DoD) (Schwartau 1999a), possible reactions could have ranged from re-routing identified Floodnet requests to other servers to shutting down the corresponding servers for a limited time (contrary to certain e-business companies, the DoD does not crucially depend on the running of these servers) to counter strikes. The US Department of Defense-knowing about the DoS attack planned by the Electronic Disturbance Theater-decided not to ignore the attack but to launch a kind of counter-attack. Request from browsers supporting the Electronic Disturbance Theater were re-directed in such a way that the browsers were crashed by Java applets. The DoD's offensive reaction stimulated a discussion whether this reaction qualifies as launching a (cyber) attack against people within the US which would be illegal.

SUMMARY AND FUTURE RESEARCH

In this paper, we have outlined that information-level online activities may qualify as serious threats and we have provided a way to distinguish these threats from network-level threats, such as break-ins and Denial-of-Service attacks. A look at the relevant literature has suggested that information-level threats are not yet adequately addressed. Apart from a summary of the current situation, the main IS contribution of this paper is that we have outlined the role of information systems in enabling shared threat recognition in companies.

We are continuing this research in a variety of directions. First, we are investigating the strengths and the limitations of search tools that are specialized on monitoring online activities. Second, we are working framework for analyzing information-level online activities that allows to assess such activities in terms of their nature and their main levers. Classification schemes exist for network-level threats (e.g., Howard 1997; Moore et al. 2001) but information-level activities have not yet been addressed. Related to this research is work on ways to quantify impacts on companies, their businesses, and their reputations. Finally, we are investigating how our work on information-level activities can be combined with existing work on security management and work on security policies.

REFERENCES

Batten, L. M. (2000). Security for future computing environments. In *Proceedings of the 1st Australian Information Security Management Workshop*.

Bellovin, S. (2001). Computer security - an end state? *Communications of the ACM*, 44(3):131-132.

Boulanger, A. (1998). Catapults and grappling hooks: The tools and techniques of information warfare. *IBM Systems Journal*, 37(1):106-114.

Brauer, M. (1998). Net spreads lies far and wide. *Detroit Free Press*. Article available at URL http://www.freep.com/tech/qblarn30.htm (last visit 15/10/2001).

Braun, B., Drobny, D., and Gessner, D. C. (2001). Model statute: www.commercial terrorism: a proposed federal crime statute addressing the solicitation of commercial terrorism through the Internet. *Harvard Journal on Legislation.*

Bridis, T. and Buckman, R. (2000). Microsoft hacked! Code stolen? *Wall Street Journal Interactive Edition*. Article available at URL http://www.zdnet.com/zdnn/stories/news/0,4586,2645850,00.html (last visit 15/10/2001).

Chai, J. (1999). Search engines point to porn. *ZDNet*. Article available at URL http://www.zdnet.com/zdnn/stories/news/0,4586,2317225,00.html (last visit 15/10/2001).

Cronin, B. (2000). Strategic intelligence and networked business. *Journal of Information Science,* 26(4):131-136.

Cronin, B. and Crawford, H. (1999). Information warfare: Its application in military and civilian contexts. *The Information Society,* 15:257-263.

Denning, D. (1999). *Information warfare and security.* ACM Press. 4th printing January 2000.

Ebbinghouse, C. (2001). You have been misinformed - now what?: attacking dangerous data. *Searcher,* 9(4).

Eriksson, E. A. (1999). Information warfare: hype or reality? *The Nonproliferation Review,* SpringSummer:57-64.

Fumento, M. (1999). Tampon terrorism. *Forbes Global.* Article available at URL http://www.forbes.com/global/1999/0517/0210033a.html (last visit 15/10/2001).

Howard, J. D. (1997). An analysis of security incidents on the Internet 1989-1995. PhD thesis, Department of Engineering and Public Policy, Carnegie Mellon University, Pittsburgh, USA.

Hutchinson, W. and Warren, M. (2000). Concepts in information warfare. In *Proceedings of the First Conference on Challenges in the New E-conomy.*

Kalish, J. (1997). P.R. firms surf the net. Article available at URL http://www.mcspotlight.org/media/press/reuters_14feb97.html (last visit 15/10/2001).

Lichtenstein, S. and Swatman, P. M. C. (2000). Issues in e-business security management and policy. In *Proceedings of the 1st Australian Information Security Management Workshop.*

Lueg, C. (2001a). Virtual communities as challenges to real companies. In *Proceedings of the Pacific Asia Conference on Information Systems (PACIS 2001),* Seoul, Korea.

Lueg, C. (2001b). Towards a framework for analyzing information-level online activities. *Proceedings of the 2nd Australian Information Warfare and Security Conference,* Perth, WA, Australia.

Lueg, C. and Riedl, R. (2001). Information systems, information sharing, and communities of practice. In *Proceedings of the Pacific Asia Conference on Information Systems (PACIS 2001),* Seoul, Korea.

Michie, D. (1998). *The invisible persuaders.* Bantam Press, London, UK.

Moore, D., Voelker, G. M., and Savage, S. (2001). Inferring Internet Denial-of-Service activity. In *Proceedings of the 2001 USENIX Security Symposium,* Washington, D.C., USA.

Needham, K. and Dale, D. (2001). Bare buttocks a turn-on but Big Brother can't hack it. *Sydney Morning Herald*, April 26, 2001, page 2.

Neue Zürcher Zeitung (1999). Internet-Missbrauch für Kursmanipulationen. Falschmeldung über eine Fusion. Nr. 81. April 9, p. 33.

Park, B. (2000). Free mobile phones offer a hoax, says Ericsson. *IT News from The Age and the Sydney Morning Herald*. Article available at URL http://it.mycareer.com.au/breaking/20000407/A54797-2000Apr7.html (last visit 15/10/2001).

Pawlowski, S. D., Robey, D., and Raven, A. (2000). Supporting shared information systems: boundary objects, communities, and brokering. In *Proceedings of the International Conference on Information Systems (ICIS 2000).*

Riley, M. (2001). Harry Potter magics a fortune from the marketing wizards. *Sydney Morning Herald*. 24 February 2001, page 3.

Schwartau, W. (1999a). Cyber-civil disobedience. Inside the Electronic Disturbance Theater's battle with the Pentagon. *Network World*. Article available at URL http://www.nwfusion.com/news/0111vigcyber.html (last visit 15/10/2001).

Schwartau, W. (1999b). Guidelines for would-be corporate vigilantes. *Network World*. Article available at URL http://www.nwfusion.com/news/0111vigitips.html (last visit 15/10/2001).

Ulfelder, S. (1997). Lies, damn lies and the Internet. *Computerworld*. Article available at http://www.computerworld.com/cwi/story/0,1199,NAV47_STO6800,00.html (last visit 15/10/2001).

Warren, M. and Hutchinson, W. (2000). On-line attacks against small and medium sized enterprises. In *Proceedings of the 1st Australian Information Security Management Workshop*.

Wenger, E. (1998). *Communities of practice: learning, meaning, and identity*. Cambridge University Press, Cambridge, UK. First Paperback Edition 1999.

Wray, S. (1998). The Electronic Disturbance Theater and electronic civil disobedience. June. Article available at URL http://www.thing.net/~rdom/ecd/EDTECD.html (last visit 15/10/2001).

Yasin, R. (2001). Tools stunt DoS attacks. Monitors dam packet floods at ISP routers. *Internet Week*. Article available at URL http://www.internetweek.com/newslead01/lead020501.htm (last visit 15/10/2001).

COPYRIGHT