12-31-2002

Using Information Systems for Enabling Corporate Awareness

Christopher Lueg
University of Technology, Sydney

Using Information Systems for Enabling Corporate Awareness

Christopher Lueg

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

Abstract

The digital economy is hard to imagine without ubiquitous network access. Discussions tend to highlight commercial prospects, such as electronic business, but proliferation of network access has also enabled potentially threatening activities. Threats, such as break-ins and malicious code, are receiving considerable attention. Potential impacts of virtually unrestricted information distribution, however, are just beginning to receive scientific attention. From a corporate perspective, potentially threatening information is not limited to hoaxes, rumours and purposely false information but may also include "true" information potentially having negative impacts on the business situation. Companies need to be aware of such potentially threatening activities. Elsewhere we have discussed what distinguishes these information-level threats from network-level threats, such as break-ins and malicious code, and we have outlined why information-level threats may be hard to detect. We have proposed "corporate awareness" as an approach allowing corporations to prepare for the increasing importance of threatening online activities. In this paper, we focus on practical aspects of corporate awareness and discuss how information systems can be used to enable corporate awareness. In particular, we sketch requirements for online activities information systems and discuss to what extent these requirements are met by collaborative software systems, such as LiveNet.

Keywords

Network age, online activities, information distribution, information-level threats, misinformation, collaboration, groupware, security management, corporate awareness

INTRODUCTION

Proliferation of network access has enabled the digital economy and is continuing to change the way business is conducted. We are particularly interested in the impacts of ubiquitous network access on the informational situation in which companies are operating. Elsewhere (e.g., Lueg, 2001a; 2002a) we have discussed a number of informational incidents described in the literature. The examples suggest that it is not only multi-national corporations but also small and medium enterprises may be affected by informational incidents. Moreover, informational incidents may have impacts on both companies engaged in e-Business activities and "traditional" companies. The latter, in particular, may not be aware of the threat potential of online activities.

The Internet has become a major information source for accessing information about companies and their products. According to Kania (2001) companies are now facing the "super-empowered user" who is able to access vast amounts of information before deciding to purchase a particular product. One of the Internet's most popular services, the World Wide Web, is actually seen as the future of brand marketing. Aaker and Joachimsthaler (2000:233) argue that "[t]o understand the Web, an experienced-based model such as a theme park or retail store is a better metaphor than passively received advertising." Kania (2001:94) maintains, "The web has erased the limits defining how customers can experience brands."

A side effect of customers becoming "super-empowered users" is that customers are much more likely to access potentially threatening information when searching for information about companies and their products. A likely implication is that businesses are easier affected by information circulated online. Such information is not limited to hoaxes, rumours and purposely false information but may also include "true" information potentially having

negative impacts on a company's business situation. Information may be distributed by competitors or disgruntled customers. Often, customers are discussing problems they experienced when using certain products.

As researchers exploring the potential impacts of threatening information we are facing the problem that detailed investigations are difficult to accomplish. Often it is difficult to verify the existence of informational incidents as companies may have chosen to avoid official recognition of threatening information. The motivation behind avoiding recognition is that recognition may be understood as a kind of verification ("company xy was under pressure to respond"). Ulfelder (1997), for example, reports that the US-based car manufacturer Ford decided not to go online to combat a certain revenge website as the company was afraid that anything they would do on their own website would validate what is described on the revenge website.

Incidents reported in the literature are therefore a major source of material investigated in this research. Requiring that informational incidents were actually mentioned in the scientific literature, in traditional media or in corporate statements (rather than in less reliable sources such as Usenet postings or mailing lists) also guarantees a certain level of (potential) impact. Examples of informational incidents acknowledged in traditional media are Jonah Peretti's email exchange with the sports equipment giant Nike and the website of a disgruntled BMW customer. MIT student Jonah Peretti tried to order running shoes customised with the word "sweatshop" (Peretti, 2001). The email exchange was widely circulated on the Internet and made it into a number of traditional media such as MediaGuardian (2001). The website www.nie-wieder-bmw.de ("nie wieder BMW" means "never again a BMW") reported problems a customer experienced with his BMW car and was featured on Spiegel Online (2002) which is a website operated by the renowned German news magazine Spiegel.

As part of this research exploring the impacts of virtually unrestricted information distribution we have reviewed what distinguishes information-level threats from network-level threats, such as break-ins and malicious code, and we have analysed why information-level threats may be hard to detect (Lueg, 2001c). We have proposed "corporate awareness" as an approach allowing corporations to prepare for the increasing importance of threatening online activities (e.g., Lueg, 2001a).

In this paper, we outline the role of information systems in enabling what we call corporate awareness. In particular, we sketch requirements for online activities information systems and discuss how these requirements are met by collaborative software systems, such as LiveNet.

WHY IS RECOGNISING POTENTIALLY THREATENING ONLINE ACTIVITIES SO DIFFICULT?

Businesses need to address two important issues. First, companies need to be aware of what is going on online. Only if they are aware of potentially threatening situations, marketing departments and/ or corporate lawyers can be brought in. Selected aspects of this matter have been discussed elsewhere (e.g., Braun *et al.*, 2001; Ebbinghouse, 2001). The second more fundamental issue is that becoming aware of threatening information circulated online is far from trivial. "Monitoring the Internet" is virtually impossible which means that problems ranging from technical limitations of search tools to organisational and cognitive limitations have to be addressed.

A major problem is that potentially threatening information can be transported in many different forms. In particular, potentially threatening information is not limited to misinformation, such as hoaxes, rumours and purposely false information, but may also include "true" information which is likely to impact a company's business environment. For example, the information that the food company Ferrero launched a legal case against the owners of the Internet domain "kinder.at" (Heise Online, 2000) does not seem to be something to worry about given that "kinder" is a Ferrero brand name. The information becomes more interesting, however, if one considers the fact that "kinder" is the German word for "children" in the first place (the website "kinder.at" published information related to children in Austria). Inaccurate advertising, such as an employee's personal opinion

assumed to be the company's official view (Lichtenstein and Swatman, 2001), is another example of threatening information that does not necessarily qualify as misinformation.

Problems can be mapped according to the following dimensions:

Technical Problems

There are a number of technical reasons why "monitoring the Internet" is virtually impossible. First of all, only a subset of all Internet communication channels can actually be monitored, as monitoring has to be (technically) feasible and (ethically) appropriate. Examples for open communication channels are public mailing lists, Usenet newsgroups and large parts of the World Wide Web. However, email being the most important electronic communication channel is private communication, many mailing lists are only for closed user groups and many websites do not grant unrestricted access to search robots (e.g., password-protected areas, areas that are excluded from third party scanning).

Limitations are such that even in the case of the publicly accessible web it is not feasible to monitor all websites. Reasons are, among others, bandwidth limitations, processing power limitations and storage limitations. In 1998 researchers found that coverage of the web by search engines was severely limited: no single search engine examined indexed more than about one-third of the 'indexable web' (Lawrence and Giles, 1998). The web has expanded enormously since then which means that despite technical progress coverage can be expected to be lower than in 1998.

Another aspect is that the standard monitoring technologies, information filtering and information retrieval, are only good at searching for "known" terms. When people use special nicknames when talking about products or companies it is difficult for search technology to find out what people are actually talking about. An extremely simple version of the problem is a discussion is which the term "Macca" is used instead of the brand name "McDonald's".

Finally, even if search technology detects misinformation, the information is already distributed. Often this means that it is not possible to "remove" the information from the respective Internet source. For example, email cannot be "removed" once delivered and stored in personal mailboxes. Postings to the global conferencing system Usenet news can be deleted to some extent but many news servers do not allow third parties to "cancel" postings; private Usenet archives are typically as inaccessible as email archives. Websites can be shut down but this process may take quite some time. In the meantime, the website may have been scanned by search engines, such as Google, storing images of all pages indexed. This means that such archives may allow users to reproduce information that has been removed from the original website.

Human Resources Problems

Internet surveillance tools are commercially available (e.g., IntelliSeek, CyberAlert) but allocating (human) resources for surveillance activities may be a problem, especially for small and medium enterprises. A related problem is that it may be difficult for companies to find a sufficient number of Internet savvy employees. Especially small and medium enterprises (SME) as well as larger companies having outsourced their IT divisions may not have employees with the expertise that is necessary to use Internet surveillance tools effectively.

Warren and Hutchinson (2000) report that even allocating resources required for undertaking (basic) security reviews may be a problem for small and medium enterprises; monitoring online activities would demand further resources. Batten (2000) expects that outsourcing security to professional businesses will become common. Hiring external specialists for monitoring Internet activities, however, may only be an option for large companies.

Socio-Cognitive Problems

The impact of information is hard to assess as information may affect companies only indirectly by influencing the environment in which companies operate (e.g., brand reputation, trust, share prices). Accordingly it may be difficult to determine the impact of certain information on a company's business environment. For example, associating Nike with

sweatshops (discussed above) is not necessarily a direct attack but it is also unlikely that this association is supportive in terms of brand reputation.

Another problem is that employees witnessing distribution of certain information may not be capable of assessing the potential impact of the information. Significant domain knowledge may be required to understand the threat potential. For example, recognising misinformation about the development of shares may require detailed knowledge of the past development of those shares.

Finally, it may be difficult to understand information circulated in online communities. For example, persons not familiar with discussions in a particular online community may have problems finding out if the community engages in product discussions or product bashing (e.g., Lueg, 2001b).

THE NEED FOR SHARED THREAT RECOGNITION

In the previous section, we have outlined that any threat recognition approach purely relying on surveillance technology would be inherently limited. Moreover, even specialised surveillance staff are likely to have a specific perspective on the Internet and its information sources which means that their surveillance activities would most likely focus on certain areas while paying less attention to others. A more distributed approach would help circumvent a number of problematic areas:

1. Perspective

   Different employees have different interests; they may be members in different communities; they exchange information with different people; they monitor different online information sources.

2. Sources

   Employees may have access to otherwise inaccessible information resources, such as closed mailing lists; at the same time, they would have an understanding if it were appropriate to forward information retrieved from such sources.

3. Tools

   Different employees may use different tools (e.g., link-rating search engines, such as Google; retrieval-based search engines, such as AltaVista; directories like Yahoo). Research found significant differences between what individual search engines cover (Lawrence and Giles, 1998).

4. Knowledge

   Different employees have a different understanding of what they read. A more technically oriented person may overlook discussions about share prices while an accountant in the same company may recognise that the discussion is flawed (perhaps intentionally “adjusted” in order to produce a certain effect). A product developer may understand that product bashing has its roots in inappropriate usage of the product while a marketing person may not realise this (rather important) matter.

Enabling “corporate awareness” means that a company’s employees act as the company’s (online) eyes and ears. Information systems may provide a suitable environment in which employees from different department can co-operate in recognising information-level online activities. Properly designed information systems may provide the glue connecting the different departments involved. Still, enabling “corporate awareness” requires a sound conceptual perspective as well as practical guidelines to implement the vision (Lueg, 2001a). As conceptual framework we use the theory of distributed cognition and the scaffolding minds perspective.

Distributed cognition (Hutchins, 1995; Hollan *et al.*, 2000) seeks to understand the organisation of cognitive systems and has mainly been used to analyse settings and to design technology, such as computer-supported cooperative work systems, based on the findings. We are using the distributed cognition perspective less to analyse *existing* settings but to justify establishing *new* relationships between actors (which are employees in this

case) by means of technology (in this case online information systems). As a perspective, distributed cognition is extremely helpful to understand an organisation along with its members as a distributed (cognitive) system in which each individual employee contributes his or her capabilities and insights. As mentioned above, different employees may understand information differently based on their varying individual backgrounds.

The concept of "corporate awareness" does not imply that employees are expected to be capable of constructing the "big picture" of a potentially threatening situation. Rather, situation assessment is based on the shared effort to understand the situation. The scaffolding minds perspective (Clark, 1997) helps describe and understand the process of collecting information about online activities. For the sake of this paper's focus, we skip a detailed introduction to the theory (see Clark, 1997 for details) and provide only a practical example that illustrates social scaffolding in an academic research environment. In such an environment, social scaffolding may be implemented such that individual members of a research group forward important scientific information to the head of the group. Researchers focus on their particular research topics (which reduces the complexity of each researcher's "activity") while the scaffolding contributes to the "informating" of the group's head and possibly – in some kind of feedback loop – to the informating of the rest of the group as well.

In the context of shared threat recognition social scaffolding means that for non-expert employees it is sufficient to forward *potentially* relevant information to the "online activities information system" (see below). Employees do not have to fully understand information they forward to this database, as their part is mainly the spotting of the information. 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. Such block effects need to be resolved.

IMPLEMENTING SHARED THREAT RECOGNITION

In the previous section we have illustrated the theory behind shared threat recognition. Being an inherently distributed approach, shared threat recognition is best supported and mediated by shared information systems. Implementing the process involves several important issues. First, a suitable "online activities information system" that supports shared usage by the different parties involved has to be developed. Second, the problem of bootstrapping usage of the system has to be addressed. In the following, we focus on the first issue.

A more generic solution could be based on groupware products, such as LiveNet or Lotus Notes. The latter has already been used successfully as platform for active collaborative filtering (Maltz and Ehrlich, 1995) that has some similarities to shared threat recognition. The idea behind active collaborative filtering is to "exploit" that members of organisations often search various information sources in order to satisfy their individual information needs. Active collaborative filtering tries to make use of the results of these individual efforts to locate interesting information. In the context of information filtering, such results are especially valuable since the information has been found to meet certain quality criteria. Active collaborative filtering builds on encouraging the members of an organisation to share interesting information with others. The term itself has been introduced to describe a collaborative filtering application at Lotus Corporation (Maltz and Ehrlich, 1995). "Active" as opposed to "passive" stresses that there has to be an intent on the part of the person who located this particular information (or the location) to share with others. The original active collaborative filtering tool was implemented as an augmentation to the commercial groupware application Lotus Notes. The tool added an additional button to the Lotus Notes SmartIcons bar. Clicking the button prepared a "pointer" to the Notes document the user was browsing. The document reference was then automatically augmented with some contextual information, such as the title of the document, its creation date, and the name of the Notes database. Furthermore, the user could add comments to the pointer before he or she would send it off to colleagues (Maltz and Ehrlich, 1995).

The concept of shared threat recognition shares a number of important characteristics with active collaborative filtering. The most important similarities in the context of this paper are

that shared threat recognition also depends on collaboration and active participation of employees. However, there are a number of additional requirements. Any shared threat recognition solution – whether based on Lotus Notes or on a different groupware product – requires support for integrating pointers to a variety of information sources, such as email, Usenet newsgroups, and websites. Often, it may be necessary to copy pieces of information to the information system for analysis purposes or simply for preservation. Information may be coded in different formats, which means that support for different formats is crucial. Furthermore, a shared threat recognition solution needs to provide some support for investigation processes and archive tasks.

To summarise, an online activities information system needs to support at least the following activities:

1. Forwarding information (or pointers to information) to a central repository.
2. Supporting collaborations among specialists from different departments.
3. Reviewing stored information and commenting on findings.
4. Structuring investigations.
5. Monitoring the development of investigations/ incidents.

A non-commercial software system that can be used for supporting these activities is LiveNet (see Figure 1), which is a groupware system developed in the Collaborative Systems Lab at the University of Technology, Sydney. LiveNet has been developed to support workflows within knowledge intensive collaborative processes. Hawryszkiewycz (2000) maintains that collaborative processes are emergent in that the next step is often determined by the outcome of the previous step and may in fact be totally unpredictable. Emergent processes have a number of general characteristics that significantly differentiate them from production workflows. The major differences are that:

1. The objective of the workflow may change and new and unanticipated tasks may need to be created.
2. A “satisfactory conclusion” of a process is not generally known until the process is well advanced.

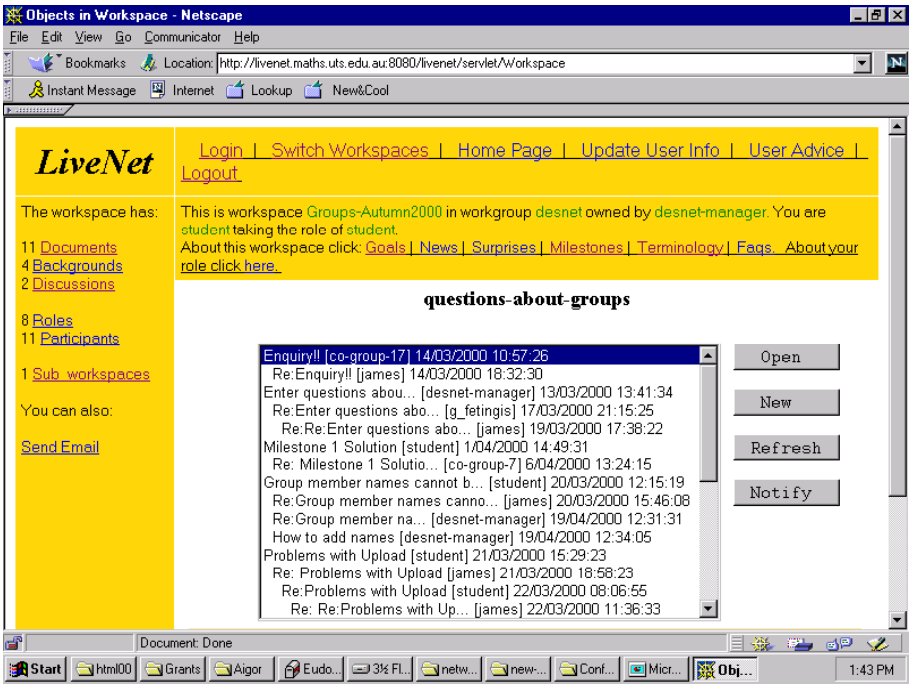

Figure 1: A workspace in LiveNet III (used by permission)

Examples given by Hawryszkiewycz (2000) are activities where innovation is important. These activities usually develop new ideas, propose solutions, evaluate them and then look at implementation. New ideas may identify totally unanticipated possibilities, which will need

to be investigated. The tasks to investigate these possibilities will have to be created and the goal of the tasks will need to be defined and redefined.

LiveNet provides ways of creating workgroups, giving them places to carry out their tasks and allowing them to create a process as their work emerges. A workgroup is a collection of people and activities and can operate independently of other workgroups. People however can participate in more than one workgroup. Workgroups have been included in LiveNet to supports scalability in the sense that independent workgroups can be created in the same system but gradually merge or intersect if needed. The work of each workgroup is organised into a number of activities. Typically, the activities are knowledge intensive concerned with developing and exchanging artifacts. They are also coordinated towards an enterprise goal. Each activity itself is defined in more detail. Broadly it is made up of a number of roles each authorised to access particular artifacts and participate in different actions. Activities are carried out in workspaces. Workspaces can be used to create and access sub-workspaces.

In the context of this paper the concept of workspace cascades (top level workspaces and sub workspaces within workspaces) and the support for work process coordination are particularly interesting. Requirement (1) [support for forwarding information (or pointers to information) to the central repository] is directly supported by LiveNet's workspaces. Information can be referred to by posting links or by creating new information artifacts. If necessary, access to information in the workspace may be regulated by using different roles (e.g., employee, investigator, lawyer, public relations) and by setting access rights accordingly. Requirement (2) [Allowing specialists from different departments to collaborate] is also supported. It should be noted however that this is more an organisational than a technical issue.

If specific information is considered particularly interesting in terms of its threat potential a sub workspace may be created for closer inspection without interfering with other activities going on in the main observation workspace. Re-locating activities to sub workspaces (instead of further toplevel workspaces) avoids that these activities disappear completely. LiveNet's support for merging workspaces is particularly helpful as it may turn out that under investigation, the same person initiated different threats; merging workspaces investigating different parts of the same problem (or re-instantiating them as sub-workspaces of the main activity) may be helpful to focus resources. LiveNet also provides support for attaching discussions to workspaces that resemble anchored conversations (Churchill *et al.*, 2000) despite the fact that LiveNet does not yet support real-time chatting. To sum up, requirement (3) [Reviewing stored information and commenting on findings] is fully supported.

The structure of investigation processes (e.g., initial posting, investigation, resolution or further activities) could be modeled in LiveNet but it is our understanding that coordination of such processes should be left to those involved. If necessary, LiveNet provides appropriate resources to dynamically create workspaces, roles, and artifacts as required. Accordingly, requirement (4) is addressed as well.

Requirement (5) [Monitoring the development of ongoing investigations/ incidents] means for example that information about websites is automatically updated when the website under investigation changes. Such services are not yet supported by LiveNet and need to be addressed.

Other limitations include the lack of a real-time chat facility (under development) and the limitation to certain datatypes that limits the system's support for requirement (1) [support for forwarding information (or pointers to information) to the central repository]. These additional requirements can integrate into LiveNet's development cycle. This means that a platform such as LiveNet can be set up to meet specific corporate requirements towards an "online activities information system" (e.g., interfaces to legacy systems).

LiveNet currently does not provide professional document management functionalities, which means that its application is restricted to scenarios in which the amount of information is limited. Most likely LiveNet could be used to support shared threat recognition in smaller companies while shared threat recognition in medium to large companies would require implementing interfaces to professional document management systems.

SUMMARY AND FUTURE RESEARCH

In this paper, we have outlined how information systems can be used to enable shared threat recognition in companies. A well-designed system can provide the glue that is required to bring together experts from different departments. Focussing on more practical issues, we have discussed the suitability of groupware systems and the collaborative system LiveNet in particular as an implementation platform for an online activities information system.

Future research includes modelling informational incidents in LiveNet and exploring news ways to raise awareness of this increasingly important domain. We are also investigating ways to support deployment of online activities information systems in companies. Experiences with problems to field 'regular' groupware applications (e.g., Grudin, 1988) suggest that bootstrapping usage of such a system would a non-trivial endeavour.

REFERENCES

Aaker, D. and Joachimsthaler, E. (2000). Brand leadership. The Free Press. New York, NY, USA.

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

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.

Churchill, E.; Trevor, J.; Bly, S.; Nelson, L.; and Cubranic, D. (2000). Anchored conversations. Chatting in the context of a document. Proceedings of the ACM SIGCHI Conference on Human Factors in Computing Systems, pages 454-461. ACM Press.

Clark, A. (1997). Being there. MIT Press, Cambridge, MA, USA. A Bradford Book.

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

Grudin, J. (1988). Why CSCW applications fail: problems in the design and evaluation of organizational interfaces. Proceedings of the International Conference on Computer Supported Collaborative Work (CSCW'88), pages 85-93.

Hawryszkiewycz, I.T. (2000). Describing work processes in collaborative work. Proceedings of the Fifth International Conference on Computer Supported Cooperative Work in Design, pp. 264-268. IEEE Computer Society.

Heise Online (2000). Süßwarenkonzern will "Kinder"-Domain freiklagen. Article available at URL http://www.heise.de/newsticker/data/psz-22.12.00-000/ (last visit 1 October 2002).

Hollan, J., Hutchins, E. and Kirsh, D. (2000). Distributed cognition: toward a new foundation for human-computer interaction research. ACM Transactions on Computer-Human Interaction, Vol. 7, No. 2, June 2000, pages 174-196.

Hutchins, E. (1995). Cognition in the wild. MIT Press, Cambridge, MA, USA.

Kania, D. (2001). BRANDING.COM - Online branding for marketing success. NTC Business Books (In conjunction with the American Marketing Association). Lincolnwood (Chicago), IL, USA.

Lawrence, S. and Giles, C. L. (1998). Searching the world wide web. Science (280), pages 98-100.

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

Lichtenstein, S. and Swatman, P. (2001). Effective Management and Policy in E-business Security. Proceedings of the 14th Bled Electronic Commerce Conference. Bled, Slovenia, June 25-26, 2001.

Lueg, C. (2001a). A distributed cognition approach to integrate security management and business processes. Proceedings of the 2nd International Conference on Working for e-Business, 29-30 November 2001, Perth, WA, Australia.

Lueg, C. (2001b). Knowledge dissemination in virtual communities as challenge to real world companies. Proceedings of the First IFIP Conference on E-Commerce, E-Business , and E-Government. 3-5 October 2001, Zurich, Switzerland. Elsevier.

Lueg, C. (2001c). Towards a framework for analyzing information-level online activities. Proceedings of the 2nd Australian Information Warfare & Security Conference, 29-30 November 2001, Perth, WA, Australia.

Lueg, C. (2002a). Knowledge sharing in online communities and its relevance to knowledge management in the e-business era. International Journal of Electronic Business, in print.

Maltz, D. and Ehrlich, K. (1995). Pointing the way: active collaborative filtering. In Proceedings of the Annual ACM SIGCHI Conference on Human Factors in Computing Systems, pages 202-209. ACM Press.

MediaGuardian (2001). Jonah Peretti and Nike. Article available at URL http://www.mediaguardian.co.uk/news/story/0,7541,440022,00.html (last visit 31 August 2001).

Peretti, J. (2001). URL http://www.media.mit.edu/~peretti/nike/ (last visit 31 May 2002).

Spiegel Online (2002). www.nie-wieder-bmw.de: Frust auf der Überholspur. Article available at URL http://www.spiegel.de/auto/werkstatt/0,1518,versand-197022,00.html (last visit 28 May 2002).

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.

ACKNOWLEDGMENTS

The author is grateful to Igor Hawryszkiewycz for the permission to use the LiveNet illustration and to the anonymous reviewers for insightful comments on the draft version of this paper.

COPYRIGHT