

Exploring Identity Management: The LSE challenge

Isidora Kourti¹ and John Paschoud²

¹Library Research Officer, London School of Economics and Political Science, 10 Portugal Street, London WC2A 2HD, i.kourti@lse.ac.uk.

²Library Projects Manager, London School of Economics and Political Science, 10 Portugal Street, London WC2A 2HD, j.paschoud@lse.ac.uk.

Keywords

Identity Management, Users' Attitudes, Attribute Release Policy (ARP), Delegated Authority Management (DAM), Virtual Organisation Management (VOM).

1. EXECUTIVE SUMMARY

This paper draws on a research project conducted with students and staff at the London School of Economics and Political Science (LSE) looking at how to improve Identity Management in a Higher Education context. The objective of the paper is to make explicit the main themes related to Identity Management as they were expressed by LSE members of staff and students with regard to the dynamics of their institution as well as making recommendations to the wider IT and Higher Education community concerning issues related to Identity Management and users' attitudes, perceptions and requirements.

1.1. Background

The corpus of data on which the analysis is based consisted of questionnaires, interviews, group discussions, internal reports and documents. The data was analyzed qualitatively and quantitatively looking for the key issues underlying LSE users' attitudes to their use of online resources, the release of personal data and the management of their identity. The research team interrelated the themes of Identity Management, ARP and the Users' Attitudes to the use of online services and more specifically with regard to VOM and DAM as they seemed quite relevant and helpful to understand the identity attributes, policies and issues in the Higher Education institution under study.

1.2. Key Findings

Issues raised have been those common in IT and Higher Education community: security risks, absence of privacy, multiple authentication requirements for applications, lack of awareness, release of personal data and use of non-institutional resources to share data. The analysis of the data shows that the main danger to Identity Management is the 'natural consumer behaviour' as the majority of the participants was often more interested in the outputs than the potential risks of using online resources. The data also reveals the need for establishment of institutional applications that will facilitate the collaboration and information sharing between users inside and outside their institutions while providing a space not only for academic purposes but also for personal uses.

1.3. Conclusions

The findings from this study suggest that LSE should review its current policies and practices for the administrative management of identities and seek to streamline them. It should also do more to make students aware of the risks of disclosing their personal data inappropriately and highlight the sensitivity of LSE data. Higher Education's IT community should emphasize the role of institutions' identity credentials, increase institutional users awareness of the risks of 'natural consumer behaviour' and the large scale disclosure of information. As a way forward, universities should create services that provide access to non-institutional users as well, and offer something over and above security of their services to motivate users to use the university's services over the alternatives.

2. INTRODUCTION

Perhaps no other influence has so affected the face of Higher Education than the World Wide Web. With the explosive growth of the Internet over the last few years, researchers have been scrambling to do studies on its effects on education. Probably, the area of education most affected by information technology is that at the university level where staff and students routinely use the internet. It is the preferred technology to raise access, increase productivity, facilitate communication and develop instruction in Higher Education.

According to a recent Info-security Europe poll (Condon 2009), 79% of users and organisations surveyed cited lack of end-user awareness as their greatest information security weakness, with people not knowing about, ignoring or circumventing Identity Management and security processes. As internet crime rises, identity fraud and other identity crimes are daily occurrences and many people in Higher Education worry if their users are aware of the risks and know how to protect their identity. Universities IT departments struggle to find more effective ways to establish, assert, acknowledge and accept identities, and to create, monitor and enforce authorizations. The need for establishment and safeguarding of identity is a priority among the leadership of Higher Education's IT community (Yanosky and Salaway 2006).

This paper draws on a research project conducted with students and staff at the London School of Economics and Political Science (LSE) looking at how to improve Identity Management in a Higher Education context. Founded in 1895, LSE is managing to adapt to the changes and innovate remaining one of the best British universities. Today it has over 9000 students, 1900 members of staff and 80000 alumni.

LSE was selected as a case study because it was presented as an institution highly involved with up-to-date issues in the IT community. Since 2000, the LSE Library's Project Team has investigated the management of access to academic resources, and the middleware that is associated with this. For instance, research has been conducted for the development of access management principles in various e-library projects and the first investigation of Shibboleth and MACE-Dir work at Internet2. Further research has been conducted in order to collect public information about the current use of Shibboleth at LSE to provide simpler and better access control for LSE students, staff and researchers to as many as e-resources and applications they use as possible. Research is also under process to produce an Identity Management Toolkit that fully meets all the requirements for successful Identity Management identified by The Identity Project, a project conducted by the LSE Library's Project Team.

3. FRAMING IDENTITY MANAGEMENT

In recent years, Identity Management has been researched from a wide range of disciplinary dimensions (i.e. technical, legal, police, social and humanity, security, organisations). Jean-Paul Sartre, Albert Camus, and others were the early introducers of the term Identity Management (Todorov 2007). The leaders and early practitioners of Identity Management presented it as the 'trust fabric' that can be stitched together (Dai and Zhou 2005). Yasin (2002: 1) characterises the 'combination of business process and technology used to manage data on IT systems and applications about users' as Identity Management and explains that the data that can be managed incorporate identity attributes, authentication elements, user aims and security privileges. Burton Group identifies Identity Management as the 'business processes and infrastructure (policies and technologies) that are required to create, maintain, and use digital identities' (Howell and Klein 2006: 1).

Yanosky and Salaway (2006) support that the management of identity consist of authentication, reduced or single sign-on, enterprise directory services, authorisation and access controls, and federated identity. Following their work, we have outlined the main issues related to Identity Management in a Higher Education context. We perceive Identity Management as a tool that tells us whether individuals are who they say they are, if they are affiliated with an institution and what entitlements that affiliation allows. We approach Identity Management as a tool that identifies users' identity, roles and responsibilities in order to allow data organisers and service providers to control access (Berg et al. 2006).

The research team incorporated in the research the themes of users' Attribute Release Policy (ARP: the ability of the institution and each end user to effectively control what personal information about themselves is released to internal and external service providers) and Users' Attitudes towards the use of online services, more specifically with regard to Virtual Organisation Management (VOM: the ability for users to easily provide 'guest' access to colleagues based at other institutions) and Delegated Authority Management (DAM: the ability for users with appropriate authority to define, via a central shared service, the authorisations of other users to access diverse sources of information, online services, and physical spaces (including the power to delegate such powers in controlled ways to other users). These themes seemed quite relevant and helpful to understand the identity attributes, policies and issues in the Higher Education institution under study. As we moved through the different stages of our research, we concluded that these issues (Identity Management, ARP and User's Attributes with regard to VOM and DAM) are interrelated and relevant at any stage of the process of Identity Management, and they should affect the approaches Higher Education institutions take to implementing Identity Management and raise users' awareness of the risks when they access public and non-public online resources.

The research team has used the themes of Identity Management, ARP and User's Attributes with regard to VOM and DAM in order to understand the present LSE project. The research presented in this paper focuses on analysing factors that affect LSE students and staff attitudes to their use of non-public and public online resources, the release of personal data and the management of their identity. The paper aims to make explicit the main themes related to Identity Management as they were expressed by LSE users with regard to the dynamics of their institution. As such, the themes and issues highlighted here are not to be viewed as performance factors, but simply as the aspects of the practice of Identity Management perceived as salient in LSE case study, that needed to be managed. The objective of the paper is therefore not to describe specific factors and issues in Identity Management rather, the themes, as seen by the LSE users, as having relevance in the institution under research as well as making recommendations to the wider IT and Higher Education community concerning issues related to Identity Management and users' attitudes, perceptions and requirements.

4. RESEARCH DESIGN AND METHODOLOGY

The research on which this paper is based was undertaken between November 2007 and March 2009. The research team began with a background literature review to understand the kinds of factors and contexts that relate to the degree of user awareness concerning the use of the vast public medium of the Web, institutional efforts to increase students' awareness and institutions' Identity Management processes (Leeuw et al. 2008). In addition, the relevant literature about research methods was also reviewed to inform the design of the various studies and the establishment of the research questions (Bryman 2008). The data corpus also incorporated documents and internal reports (i.e. on LSE IT infrastructures, LSE IT department, current LSE Identity Management processes etc.) including an earlier pilot study.

To begin, a questionnaire (face-to-face and online) of attitudes to personal data disclosure was undertaken in October 2008. The online questionnaire included exactly the same questions as the face-to-face questionnaire (Cohen et al. 2000). The Bristol Online Survey (BOS, www.survey.bris.ac.uk), a service that allows developing, deploying, and analysing surveys via the Web, was used for the online version of the questionnaire, and also by the project team to record responses collected from the printed questionnaires. In total, 412 completed questionnaires were collected (351 from LSE students and 61 from LSE staff. The data from the questionnaires were analysed quantitatively using SPSS, a computer program used for the analysis of quantitative data (Brace et al. 2000). Using a multi-level approach, the analysis of the data aimed to elucidate the role of factors such as context, background, public and non-public resources in relation to awareness about the risks when accessing online resources (Crano and Marilyn 2002). This was followed by further analysis of the data focusing on the institution's Identity Management processes and users' Identity Management practices.

Following the questionnaires, group discussions were conducted with LSE students in November 2008 in order to collect data about LSE users' experiences and practices with online services, ARP, VOM and Identity Management (Puchta and Potter 2004). Four focus groups were organised with 18

students (3 research, 5 masters and 10 undergraduate students). The analysis, coding and categorisation of the material were achieved with the aid of Atlas/Ti, a qualitative research software for data analysis and management (Murh 1997).

Finally, 16 face-to-face in-depth interviews were conducted in January 2009 (12 with LSE students and 4 with administrative staff). All the interviews were recorded and they lasted up to one and a half hours (Kvale 2007). The aim was to get the interviewees to talk freely and openly while making sure that we explored in-depth users' attitudes and perceptions to DAM, VOM and ARP in relation to Identity Management (Cohen et al. 2000). Atlas/Ti was used in order to systematically analyse the collected data.

5. RESULTS AND DISCUSSION

From the analysis of the data, it is clear that there are general factors as well as particular institutional factors that affect LSE students and staff attitudes to their use of online resources, the release of personal data and the management of their identity. The different themes emerging from the analysis were categorised in three interrelated stages: the Identity Management, the users' ARP and the Users' Attitudes to the use of online services with regard to VOM and DAM. The findings of the study suggest that the university should take these three themes into account in order to develop their current policies and infrastructures provided to its members, implement Identity Management and deliver business benefits from doing so. Although each factor is separately presented, they should be perceived as interrelated in order to be able to get a holistic picture of the institutions Identity Management processes and users' Identity Management practices.

5.1. Identity Management

5.1.1 Users Perspectives to LSE Identity Management Processes

From the analysis of the data it emerges that LSE members are satisfied with the services their institution provides in terms of Identity Management. Users are aware of the information LSE holds about them the personal information (name, date of birth, address, contact number, nationality, family status), the financial information (bank details, account number, accommodation and school fees, annual income of family, loans), the library information (books issued, fines, internet usage, access to library, journals used) and the study information (exam results, marks, attendance, timetable, courses). Nonetheless, it is apparent that there is little real awareness of why this data is held by LSE. As such, a variety of possible explanations are put forward: communication, registration, enrolment, administration, marketing, operation, reference etc. However, the most common answer is that 'LSE needs to know'.

Moreover, the results show that LSE users are aware of the role of their 'LSE identity' as a credential for accessing services. For instance, the majority of the participants claim that they use LSE credentials to access computers, wireless, email, journal, internet services, library services, career services, Moodle (institutional VLE), LSE for You (the LSE web portal), sign up for classes and print-purchasing. Concerning their LSE ID card, participants support that they use it in order to access the library and other LSE premises, borrow books, enter societies and have discounts.

Apart from the use of their institution's credentials, users recognise the importance of not letting other users use their university's username and password. The same results emerge for the use of a university's ID card, as most of the participants have never lent their LSE ID card to other people. On the other hand, some participants present examples where they lend their LSE account, LSE library card and debit card to their friends verifying that they have less awareness of their responsibility to keep their LSE credentials secure.

As the data show, it is important to acknowledge 'natural consumer behaviour' on the part of the students. They are often more interested in the outputs than the potential risks of visiting sites, they often use the same password for multiple services, take advantage of 'remember me on this computer' options and save passwords in insecure locations. As such, although the majority of LSE members have never been victims of identity fraud, users have not taken any action in order to prevent their LSE credentials from being stolen. For example, most of the participants have never changed their LSE password and some of them do not even know that this is possible. However, users' familiarity with systems that require them to change their passwords regularly and the fact

that LSE does not require this and does not emphasise this practice may well reduce confidence at LSE as a trusted environment for storing personal data.

5.1.2. LSE Administrators Practices to Identity Management

As far as LSE administrators are concerned, they create unique naming policies for each of their systems and utilize this naming convention to assign a unique identifier to users of their systems (individual accounts). Their aim is to assign accounts with uniformity across all LSE systems. For systems which cannot use the defined uniform naming convention there arises an opportunity for Identity Management to transcend across the systems and provide a solution.

Although the administration does its job very well, multiple teams are involved in user administration activities, something that looks common in other universities as well. This results in increasing overheads in the administration of identities whilst the teams spend a lot of time performing routine administration tasks that can be automated. For instance, it takes a lot of time to provide access to external users such as visiting students and fellows while their functions or roles may limit their ability to access services available to internal users. Moreover, more confusion takes place when students de-register for one term and later return as it takes time to restore access rights to resources while former staff and students may have restricted access to services as alumni.

Furthermore, issues of Identity Management and security risks related to accounts created with unauthorised system access rights are raised. For example, changes to the staff cause confusion and delays in Identity Management processes whilst security risks occur when frustrated or overburdened administrative staff takes shortcuts. In addition, terminations may not be done as soon as required or permissions granted may be in excess of what is really needed or may limit users' ability to access resources that they need.

Whilst many of the LSE systems use a single LSE username/password to provide access to services, this is not always the case. Some end-user systems (such as Moodle) implement single sign-on in ad-hoc ways (i.e. using direct LDAP connections instead of Federated Access) which reduces the administrative and security benefits of having a single identity and access management infrastructure. Having isolated systems that operate outside of the central system causes potential problems of revoking access controls, having multiple passwords etc.

5.2. Users' Attribute Release Policy to non-LSE resources

Interesting results come from the analysis of the data concerning users' ARP to non-institutional resources. LSE users, like users elsewhere, believe that it is necessary to release personal data in order to get access to online resources. For instance, participants state they are willing to release their name, email address, date of birth, gender, address, university, program of study etc. in order to access those services they wish to use. Moreover, some LSE students claim that they would release any kind of personal data in order to get access to some online resources.

It is quite interesting that users do not wonder why third parties are asking for their personal information. Contrarily, it is presented as a simple fact of their daily life without having any thought about the use of their data by the third parties to whom they have released it. As such, it appears that users do not hesitate to release their real details when they sign up. Therefore, it is apparent that users do not really understand the risks of releasing their personal data and even some times they have a naïve understanding of what personal information is safe to be released and what is not.

Nonetheless, it seems that users are quite careful when they have to release personal data by phone. As such, the majority of the participants claim that they do not release personal information by phone unless they are sure who they are dealing with. It appears that the most common approach to these phone calls is to ask for more information about the person who is calling or call back the organisation that the caller claims to call from. However, there are also users who are happy to provide the information they had been asked to without trying to identify who is calling.

As the data reveal, most of the time users do not look at the terms of the agreement before they agree to sign up for an online service. This shows that the users are not aware of their rights and responsibilities, and the terms and conditions under which they may use the websites they access. Therefore, it appears that the agreement to the terms and the release of personal data are common processes in order to gain access to online resources.

Moreover, when users sign up for an online service, they do not usually read the instructions in order to prevent the release of their personal data. For example, when participants are asked if they have turned on their privacy settings to restrict access to their Facebook account, most of them claim that they have not while some of the participants' admit that do not know that there is this option. Based on these results, it can be argued that LSE users, like users elsewhere, are not aware of the risks related to the release of their personal data and they are not aware of the policies or tips that will help them protect their personal information.

It appears that users put material online for others to share without realising that they put their data at risk. Most of them use Facebook as the main online service to share pictures, videos, notes, personal information (i.e. hobbies, favourite movies) whilst they like to share information without considering too much who has access to that information. A common approach seems to be that since they put their information online they do not mind to share it with those who can get access to their page. This links to the fact that most of the participants do not know about or haven't turned on their privacy settings in Facebook.

Another important issue that emerges from the data is that users do not make any effort to limit the information they put online. The fact that LSE users release their personal information to non-LSE services confirms that participants do trust public online services. Moreover, following students' attitude in other universities, they prefer to share their personal data and material using non-institutional services because they know that their lecturers or colleagues will not have access to this data and they also provide a place to share not only academic material but also personal material.

5.3. Users Attitudes to online services with regard to VOM and DAM

5.3.1. VOM and the need for a new application

The data suggests that the users realise that is hard to control information once it has been released online while some of them admit that they should limit the information they put online more than they do as this is the best way to keep it under control. It emerges from the data that Facebook is the principal space where LSE members, similar to other universities' members, can manage their space and control who has access to their personal files, something that are not able to do with the current LSE services (other popular options are Google and Yahoo).

There seems to be a need for a service that will allow users to share their data and collaborate in a simple and secure way with people inside and outside their university. Nevertheless, it seems that they prefer a non-institutional service instead of a service provided by their institution. For instance, when participants are asked to use and then decide whether they prefer to collaborate with people inside and outside LSE with Google Docs or with FlameSpace (a WIKI-based collaboration and information sharing environment developed by the project's technical team) the majority of the participants chooses Google Docs. It appears that the main reason for their choice is that they find that Google Docs is a more familiar and well established service than FlameSpace. Although they are asked about issues of security, they claim that Google Docs is as safe as an equivalent application provided by their university.

It emerges that LSE users, similar to other institutional users, find the ability to collaborate with LSE and non-LSE users very important. However, the current LSE services do not provide this option and that leads them to use non-LSE services in order to collaborate and share material with people outside LSE (i.e. Facebook, Google, Yahoo and MySpace). As the data reveal, the most important issues of security are related to the use of non-LSE resources in order to facilitate the collaboration between LSE and non-LSE members since these services are not controlled by the LSE and yet students do trust them. As a way forward, universities need to establish institutional applications that will facilitate the collaboration and information sharing between users inside and outside their institutions while providing a space not only for academic purposes but also for personal uses.

5.3.2. DAM and users' need to control access to their space

The findings suggest that users put material online for others to share i.e. pictures, notes, files, documents, videos and personal information, and they regularly use Facebook for this purpose. LSE users choose to give access to their accounts and their material to LSE members, family and friends.

However, since users tend to share a lot of material with people inside and outside their institution, they want to have the ability to give others access to non-public resources, something that are not able to do with the current services provided by LSE. As such, users mostly choose Facebook to share their material. The majority of LSE users chooses to give access to all those who are in 'LSE's' Facebook network without exceptions. It appears that since they put their personal or academic information there, it means that they are actually happy to share it with others.

It appears that LSE members are aware of the risks and the dangers of giving to other users the ability to edit, delete, edit and write effectively the same (at least in an electronic context) or manage 'their' material. As such, users want to be able to share material with viewers who they personally invite. For example, they admit that only in cases where they have to collaborate with others (i.e. for a project or a group exercise) they would give other users the ability to write, edit and delete and even in these cases they would hesitate to share the management role. However, as it appears in most institutional contexts, the use of sites like Facebook, MySpace etc. means that it is normal behaviour to make many different resources available (even with viewer only restrictions) without thinking through the long term implications of this release. As a way forward, it is very important for users to understand the meaning ('power') of each role before they give it to the users of their space while the instructions should be straightforward in order to help them to identify the appropriate access that they wish to give to others.

LSE users, like users in other universities, are not aware of the risks of giving view level access to their material to others, as it seems that users do not hesitate to share pictures, notes, files, documents, videos, personal information and also any kind of material they are able to share with an online service. On the other hand, they do discriminate between users known to them (even if very vaguely, such as other members of the institution) and the public in general. This indicates that the users realise that they should not share their material with anyone apart from people they know.

6. CONCLUSION

The findings from this study suggest that LSE should review its current policies and practices for the administrative management of identities and seek to streamline them. The review process should therefore document/update details of current practices. It should also review all systems and applications which are not integrated with central Identity Management system with a view of achieving full integration. LSE should require users to change passwords regularly and emphasise this practice as well. Moreover, LSE should do more to make students aware of the risks of disclosing their personal data inappropriately and highlight the sensitivity of LSE data. In order to do that, its advice should focus on the act of disclosure and an appreciation of the risks of passing data to different organizations.

The results of the research also allow us to make some recommendations to the wider IT and Higher Education community. Institutional users should be made aware of the risks of 'natural consumer behaviour' and given specific advice about password security, whilst encouraging them to change their passwords on a more frequent basis. In addition, universities should do more to explain what data is held about students and why it is held whilst should use this as an opportunity to review the data that is collected and held about students with a view to assessing whether it is really needed. In order to increase awareness of the risks of large scale disclosure of information, the institutions should emphasize the role of institutions' identity credentials and that access to academic resources is one of the privileges of student status. They should also review the use of 'remember my settings on this computer' and consider disabling them by default where the consequences are potentially risky.

The results from the use of DAM/VOM highlight the importance of sharing materials beyond the institution (i.e. family and friends) and this is a necessary feature of any DAM/VOM alternative proposed. If universities decide to go forward with the creation of such services, those must provide access to non-institutional users as well. They should offer something over and above security of their services in order to motivate students to use the university's services over the alternatives. Otherwise, if institutions are not going to provide their own DAM/VOM services, they should provide lists of available services highlighting those that require the minimal disclosure of personal data. However, if universities are going to recommend commercial DAM/VOM services, they might focus on those that provide limited viewer rights for other users rather than full scale levels of access.

Institutions should also clearly state the implications of students signing up to these services using their personal details and which personal details are particularly sensitive.

The aim of the paper was to examine factors that affect LSE students and staff attitudes to their use of non-public and public online resources, the release of personal data and the management of their identity. In order to do that, we interrelated the themes of Identity Management, ARP and the Users' Attitudes to the use of online services and more specifically with regard to VOM and DAM. The research team aimed at presenting the themes, as seen by the LSE users, as having relevance in the institution under research as well as making recommendations to the wider IT and Higher Education community related to issues of user's attitudes and Identity Management. Certainly, the fact that our study occurred within a single Higher Education context suggests that these findings should be generalized to other contexts with caution. Future research that investigates issues of security related to the use of non-institutional resources and examines the detailed rationale behind users' decisions about the level of access that they provide to their material seems a useful step.

7. REFERENCES

- Berg, J. E., Kraemer, R., & Raatz, C. (2006). *Identity Management (IdM): A case study in building an IdM governance process*. Madison: University of Wisconsin.
- Brace, N., Kemp, R., & Snelgar, R. (2000). *SPSS for psychologists: A guide to data analysis using SPSS for Windows*. Basingstoke: Macmillan.
- Bryman, A. (2008). *Social research methods*. New York: Oxford University Press.
- Cohen, L., Manion, L., & Morrison, K. (2000). *Research methods in education*. New York: RoutledgeFalmer.
- Condon, R. (2009). Infosecurity Europe bucks economic recession, as does cybercrime. *Information Security Magazine*. Retrieved March 25, 2009, from: http://searchsecurity.techtarget.co.uk/news/article/0,289142,sid180_gci1355457,00.html.
- Crano, W. D., & Marilynn, B. B. (2002). *Principles and methods of social research*. Mahwah, N.J.: Lawrence Erlbaum Associates.
- Dai, Z., & Zhou, W. (2005). *The Federated Identity and Access Management Architectures: A Literature Survey*. Deakin: Deakin University, School of Information Technology.
- Howell, L., & Klein, S. W. (2006). *Identity Management at NC state university*. New Bern, NC: UNC CAUSE.
- Kvale, S. (2007). *Doing interviews*. London: SAGE Publications.
- Leeuw, E., Fiscber- Hubner, S., Tseng, J., & Borking, J. (2008). *Policies and Research in Identity Management*. Boston: Springer.
- Murh, T. (1997). *ATLAS.ti: The knowledge workbench. User's manual*. Berlin: Scientific software development.
- Puchta, C., & Potter, J. (2004). *Focus group practice*. London: SAGE Publications.
- Todorov, D. (2007). *Mechanics of user identification and Authentication: Fundamentals of Identity Management*. Auerbach Publications.
- Yanosky, R., & Salaway, G. (2006). Identity Management in Higher Education: A baseline Study. *EDUCAUSE Center for Applied Research*. Retrieved April 24, 2009, from: www.educause.edu/ecar.
- Yasin, R. (2002). What is Identity Management? *Information Security Magazine*. Retrieved April 12, 2009, from: http://www.inforsecuritymag.com/2002/apr/cover_casestudy.shtml.