Resources for Chapter 3 – Drivers

RESOURCES

- **Incidental security improvements from sustainability policies – UCL, case study**
- **Information security within the research arena – Loughborough University, case study**

Incidental security improvements from sustainability policies – UCL, case study

UCL Human Factors researchers, led by Prof. Angela Sasse, collaborated with a large telecommunications company and a large utilities company. Researchers interviewed employees across a variety of roles within the companies to understand how security played a role in their working practices: specifically, the interplay between security mechanisms and individual employees' primary (productive) tasks. It was important to understand perceived frictions and benefits of security within the workforce (see Chapter 8, Roles and competencies).

The study found that there was scope for policies and organisation-wide initiatives outside of security to indirectly improve the security posture of an organisation, or otherwise encourage behaviours which were also more secure.

Awareness

Environmentally-sound practices may be promoted side by side with health and safety, or be the focus of specific campaigns such as organisation-wide sustainability drives. In the telecommunications company, employees were encouraged, through training and visible campaigns, to consider the cost of their working behaviours to the environment, and adopt *green* thinking in practice. For some in the organisations, this *thinking green* was more approachable and had a clearer purpose than understanding security and its drivers.

Individuals can be encouraged to adopt visible practices that they can take pride in, and which the organisation can measure against targets. Training relating to sustainability was found to be a channel for recommending behaviours which were incidentally more secure than existing practices.

Paperless approaches

Related policies included the development of a *paperless* office. This encouraged the rationalisation (and ultimately, limiting) of document printing, and - when documents were printed - having printing enabled locally at the printer with existing ID access cards. This then involved users consciously in their own printing of documents and had the potential to create a greater sense of ownership over their personal impact within the organisation, while also recording print rates per employee. This demonstrates change within already existing habits (conscious printing), incidental security (limitation of unattended printouts), as well as a clear measure of performance against company policy (the limitation of printed documents).

Secure disposal

Secure document bins were provided, distributed in such a way as to be within easy access of all employees, further supporting involvement. Crucially this showed consideration of both employee needs (the need to dispose of sensitive documents) and the minimisation of disruption to working habits (limiting the cost to the individual to comply with the policy).

Indirect improvements included a reduced likeliness of documents being left on desks or left overnight in shared office space. There were also less physical copies of confidential documents in circulation, and there was less opportunity for individuals to pick up someone else's printouts from printers (where the action taken with those printouts could otherwise not then be tracked).

Remote working

A paperless office also complemented remote working - individuals would tend towards carrying less print-outs with them when travelling, where otherwise printed documents might have been carried around or left over various locations for any length of time. In the utilities company, there was also a drive toward minimising travel outside of the company where possible as a means to develop sustainable practices (moving instead to (secure) communications applications) - this would incidentally limit exposure of the organisation's assets to risks present in other locations, but would have required investment and guarantees around reliable alternative solutions for communication

Storage benefits

The utilities company also tried to minimise storage costs and adopt just-in-time resourcing practices where appropriate. Sustainable practices such as site management can then be linked to recognised standards, e.g. ISO14001 ("Environmental Management"). This demonstrates clear relation of outcomes to high-level expectations.

Avoiding confusion

There was a need to be mindful of how policies must join up effectively. Both companies provided secure shredders, where shredded documents were then collected by a contracted outside company for disposal. Staff in the telecommunications company were instructed to direct documents either to recycling bins or to confidential document shredders based on their sensitivity classification - this had the potential to confuse employees who wanted to respect both security and the environment. In the utilities company, the policy around disposal of computers (and specifically hard drives) needed to respect data protection concerns raised by employees themselves ("*There's no way you're just taking this away to recycle it, do whatever with it.*") - individuals with knowledge of security will need assurances that other parties are protecting their information.

Key points

- Ensure that there are tangible benefits of following organisation policies.
- Know your suppliers
- Engage with members of the organisation to understand how policies combine in practice within their roles, and where improvements can be made.

Information security within the research arena – Loughborough University, case study

Over the last few years within Loughborough University, there has been an increased requirement for Information Security input to research project proposals, grant applications and contract agreements. Supporting research within the organisation is an important activity; but it is recognised that it is different to supporting the teaching and learning activity.

Awareness

One of the earliest activities required was an awareness campaign within the research community. Colleagues were often in sections of academic schools which did not have the same level of cascaded information about central IT services and support. Providing focused communications explaining what support was available to researchers was greatly beneficial to increase awareness and was welcomed by the recipients.

There is a parallel theme of changing culture and improving training, which is focused across the organisation. The research community within Loughborough have welcomed these initiatives with open arms as they can sometimes feel isolated or unsure how to get the IT support required by their research. Opening a dialogue in the information security area has brought about a change in provision in other areas to the benefit of the wider organisation.

Third party requirements

Auditing

As part of a pre-existing research contract, the University received a request from the commercial company supporting the research to allow a security audit of the information systems used to facilitate the research activities.

The commercial company audit team spent two days on site reviewing the written policies, technical controls and undertaking testing of the systems concerned. Whilst the activity took several days to prepare for (as the information security controls were not as mature as required), the exercise was greatly beneficial, as the University received an external and commercial perspective on the security controls required. With a small number of recommendations for improvement being received, it was a positive activity and something which has been repeated, in subsequent years, by the commercial company.

Depending on the nature of the research, organisations will engage with different companies, research organisations and other academic institutions. Based on the number of information security surveys, questionnaires, forms and interviews completed over the last ten years, there is an increasing similarity of questions being posed. From the straight forward such as “Do you have a firewall?” to providing copies of patching policies. In order to improve responsiveness to these requests for additional information, colleagues in the information security function were quick to produce a number of stock responses in a default proforma.

Data disposal

One of the interesting requests received was that of assurance of data disposal following previous research activities. One of the research grants required assurance that previous research information assets from a previous grant were passed to the funder to be centralised with confirmation that the data has been securely destroyed from site. This can be a challenge with modern file space provision with: volume shadow copies, tiered storage and backup robots. In the case of Loughborough University, it took a three month period for this data to be removed through a cycle of standard process activity.

Secure communications

The use of secure electronic mail technology has been raised a couple of times by funders; the preferred access mechanism for government related research grants appears to be the Criminal Justice Secure Email. This provides a secure webmail facility to interact with the police, government and solicitors. There is an option to integrate this into the standard desktop email client in some scenarios, depending on the Business Impact Level (BIL).

Information leakage

A large part of supporting research at Loughborough University has focused on a risk assessment of information leakage and what controls are required to mitigate this risk. The government Business Impact Level assessment process continues to be used, despite the new Government Security classifications introduced on 2 April 2014. The Business Impact Level provides guidance on the risk assessment process; the new classifications are not used to label the information. However, researchers do not fully understand what this means, and what systems can meet this level of data. Funding applications are starting to request a Risk Management and Accreditation Documentation Set (RMADS), which describes the Business Impact Level of the information being held/processed.

Managing costs

If there are any costs associated with providing information security support to a research project, it is important to investigate the funding schedule available as this tends to differ depending on the research funding partner. Based upon experience, information security costs are often overlooked when putting the research grant together. At Loughborough University this was introduced as part of the central advice provided by the research and enterprise offices. Areas which may need to be included in funding include

penetration testing, managed hosting services and a secure coding audit for middleware.

Within Loughborough, a pragmatic approach has been made to address the areas described in this case study, initially utilising the resource which is available for information security, there was no additional funding or posts provided.

Maintenance of "orphaned" information systems developed for research.

At the end of a research project, there is the requirement to make the research data, methodology and reports available. However, researchers' effort is being moved onto the next project and next grant. This leaves the previously created systems unsupported.

> Based on experience in the sector, non-maintained and development systems pose a credible risk and easy attack vector.

One of the first steps to addressing this issue at Loughborough has been to require these systems to be installed on virtual machines within the infrastructure managed environment. This provides a regular three monthly vulnerability assessment of the virtual machine with exception reporting. It is important to recognise this is the first step to try and address this problem and it is not the panacea to solving the issue. Within Loughborough University, we also provide a central hosting solution for blogs based upon WordPress, to manage the security aspects of the software.

Research data management

Research data management is a hot topic among many organisations. Loughborough is no different in this- we are investigating how to make research data available to the public in a secure and sustainable manner.

Learning Points

- Researchers may not be aware of the Information Security support offered by your organisations, so run a campaign to make them aware.
- Some research grants or contracts may require your organisation to undertake a formal security assessment as part of the agreed terms.
- The questions which form part of research, grant or contract applications are broadly similar. Consider creating a bank of stock responses which will make the completion of these documents easier.
- Funding for research tends to be made available up front as part of the grant or contract; introduce any associated costs, for example an external penetration test, upfront.
- At the end of a research project, some information systems will become orphaned. Consider research data management and how the organisation will manage information at the end of a project to avoid information systems being left unmanaged.