Universities and Colleges
Information Systems Association

www.ucisa.ac.uk

Tel: +44 (0)1865 283425 Fax: +44 (0)1865 283426
Email: admin@ucisa.ac.uk

UCISA EVENT REPORT

Cyber security: your survival guide

UCISA Infrastructure Group – Cyber security survival guide event
IET Austin Court, Birmingham
May 2017

On a sunny Friday in May, while all eyes were on the West Midlands mayoral election count, a very different gathering was taking place in IET Austin Court just over the Birmingham canal. Cyber security experts from around the nation were discussing how to protect UK universities and colleges from the ever-growing threat of cyber attacks.

The event was organised by UCISA's Infrastructure Group and is the latest in a long list of their cyber security events and resources for the sector. Over 100 delegates from 51 universities and colleges and 11 suppliers heard 10 presentations covering a wide range of topics from incident management to password policy. For those who couldn't get there in person, the event was streamed live.

Graham Cluley, a security consultant, painted an alarming picture of the scale and nature of the threat, and the implications for the organisations affected. There are 400,000 new malware attacks everyday – one every 0.4 seconds. Being a large, cyber savvy organisation doesn't necessarily protect you – Google and Facebook have both fallen prey to cyber attacks costing them in the region of $100M. Information on the people within organisations, such as contact details for PAs to senior managers or new starters, is readily available in LinkedIn and other social networks. This can be a great help in *social engineering* an attack.

Several common themes emerged from the presentations, and the top one was people. In any organisation, people are the weakest link in the cyber security chain.

Beware of insider attacks – not all staff are well-intentioned. For example, someone leaving an organisation might want to take some information with them, so it is very important to disable accounts as soon as someone leaves the institution.

However the vast majority of people try to be helpful, and this leaves them vulnerable to social engineering attacks and phishing, for example. David Deighton, Chief Enterprise Architect at the University of Birmingham, told the conference that on a recent simulated phishing attack on 1000 users, 28% were tricked and would have compromised their accounts had it been a real attack. Yet only a minority of institutions undertake this type of self-testing. Active testing of your own security is a powerful tool – "Hack yourself before someone else does", say both Deighton and Cluley. Awareness training is a major help, and is widely implemented although not always mandatory. Most institutions use UCISA's free online training resource, and James Smith, Chief Information Security Officer at the University of Oxford, discussed how they had gone beyond this, investing heavily in targeted sessions with key groups and individuals.

Universities and Colleges
Information Systems Association

www.ucisa.ac.uk

Tel: +44 (0)1865 283425 Fax: +44 (0)1865 283426
Email: admin@ucisa.ac.uk

Several speakers pointed out that you can't achieve perfect security, but you can manage the risks effectively. Most security measures have costs in terms of restricting flexibility, hindering collaboration or making access less convenient and these costs need to be carefully weighed against the reduction in cyber risks. Understanding how people make decisions is probably as important as understanding the technological side of cyber security. David Hayling, Head of IT Infrastructure at the University of Kent, illustrated this with a discussion of password policy (see **So safe, it's dangerous**), "You have to base your security on how real people behave, not on how you'd like them to." He also urged organisations to base cyber security decisions on evidence rather than perceived wisdom. One way to guard the crown jewels and still let visitors into the tower is to classify information into high risk (high protection, restricted access) or low risk (lower protection, convenient access). Getting this balance of access and security right needs to involve people from across the institution; it shouldn't be left to the technical experts.

Indeed, institutional ownership of cyber security was another recurring theme. Ted Leath, Information and Assurance Manager at the Ulster University, explained that while IT might set up a framework for managing information security, it is up to the people responsible for the information to do something about it. Robbie Walker, Security Architect at the University of Portsmouth, presented a simple but comprehensive questionnaire to help information owners (in conjunction with suppliers) to assess the risks of cloud based services. Departments and project managers need to build cyber security into their thinking from the beginning, and not leave it to IT to sort it out later. This type of shared responsibility requires trust between the business and the specialists – for example people need to feel that they can report security incidents in a *no blame* environment. This trust building and breaking down of silos takes a lot of engagement and patience, but does bring dividends. Continual engagement in the form of training, support materials and advice needs to be readily available and easy to access.

So safe, it's dangerous

At first glance password policy looks like a necessary but not particularly interesting topic, but David Hayling showed that it is a fascinating example of why you need to take account of how people really behave and why you should base cyber security precautions on solid evidence. A University of Kent audit had highlighted the fact that user passwords only needed to be changed every 274 days, and the auditors suggested that changes should be more frequent than that to guard against guessing or cracking.

However, regularly changing a password only guards against a minority of the associated threats, and not very effectively. Furthermore, research showed that the more burdensome a password policy was, the more likely the user would be to circumvent it by, for example, writing the password down, using the same password across multiple systems or not using the service at all (where they have a choice). Tightening policy imposes a cost on users, and we ignore these costs at our peril. If we help users by allowing the same credentials to be used securely across different services, or by removing the requirement for frequent changes, they will be prepared to use more complex passwords in the first place and that will result in improved security.

Usable security means creating something that works, given (or despite) what people do. The University is now working towards an environment where forced periodic password changes are unnecessary, in line with advice from the National Cyber Security Centre.

Universities and Colleges
Information Systems Association

www.ucisa.ac.uk

Tel: +44 (0)1865 283425 Fax: +44 (0)1865 283426
Email: admin@ucisa.ac.uk

Dave Guest, Senior Architect at Oxford Computer Group, made the point that with the growth of cloud computing and remote working, it is no longer enough to use firewalls and routers to protect the internal network, because as often as not the information isn't on the internal network, nor is it accessed from the internal network. The emphasis now needs to be on protecting the information itself, wherever it is, based on who is accessing it, wherever they are. Of course, this depends on the organisation knowing what information it holds in the first place, and Steve Hill, IT Security Coordinator at the University of Wolverhampton, illustrated how challenging it can be to build a comprehensive inventory, given that research shows 40% of all cloud services have been commissioned without the involvement of central IT. Hill said that the key to solving this is to build strong collaboration between central IT and users, and to keep strengthening this so that *shadow IT* doesn't become a threat in the first place. There are ways that technology itself can help to find and safeguard the data, and Guest showed some of the features available in Microsoft's Azure platform. However, as Hill pointed out, spotting data *on the move* isn't good enough, you also need to know who is responsible for it.

Understanding your information holdings will be a crucial element of complying with the General Data Protection Regulation (GDPR) that comes into force in May 2018, explained Craig Clarke, Head of Data Protection and Compliance at the University of East London. These will take over from the Data Protection Act, but go well beyond it in terms of scope, depth and penalties (see **GDPR – What you'll need to know**), and the effort to reach compliance will be massive. One tool that can help right now is the Privacy Impact Assessment, one of the Information Commissioner's Office's best kept secrets and something that will become mandatory under GDPR.

Even with all these safeguards in place, things will occasionally go wrong and it is important to have solid procedures for incident reporting and management. David Deighton presented an approach grounded in the ITIL incident management process. This gives a single point of contact for users and ensures rapid categorisation of incident type and routing to the appropriate team. There are clear targets for resolution based on severity, and escalation where necessary – even as far as the institution's major incident procedure. The system also produces management information on incident trends. The more automated security monitoring and reporting you can do, the better. Awareness and analysis of cyber security incidents is key to knowing what needs improvement.

All these measures need to be underpinned by well thought out policies that clearly set out what the institution is aiming to achieve, and the roles and responsibilities for achieving it. Jerry Niman, an independent consultant to the sector, explained that cyber security policies need to set out clear boundaries for everyone. This gives cyber professionals and information owners the institutional backing they need to navigate their way through the conflicting interests of security versus access. He also gave some tips on how to make policies stable enough to match the pace of typical governance structures yet dynamic enough to keep up with the ever-changing threat landscape.

The increasingly sophisticated ways in which we process information, and growing user expectations of convenient access, just make the task of protecting information more complex. There is no perfect solution, but the conference showed what we can do to change the balance in our favour (see **Top ten tips**).

Universities and Colleges
Information Systems Association

www.ucisa.ac.uk

Tel: +44 (0)1865 283425 Fax: +44 (0)1865 283426
Email: admin@ucisa.ac.uk

UCISA EVENT REPORT

Top ten tips

1. Recognise that cyber security is an institutional issue, not an IT one.
2. Protect the information, not the network.
3. Know what information you have and who is responsible for it.
4. Move the role of IT security from locking things down to awareness, support, engagement, and training.
5. Take account of the way the people really behave.
6. Support people in building cyber security into their projects at the outset through dialogue between users, suppliers and security specialists – provide simple checklists and encourage privacy impact assessments.
7. Bring distributed IT, especially cloud based services, out of the shadows by building trust.
8. Implement a good process to report and manage incidents, and learn from them.
9. Hack yourself before someone else does.
10. Ensure your policies are useful and dynamic.

Universities and Colleges
Information Systems Association

www.ucisa.ac.uk

Tel: +44 (0)1865 283425 Fax: +44 (0)1865 283426
Email: admin@ucisa.ac.uk

UCISA EVENT REPORT

GDPR – What you'll need to know

Craig Clarke, Head of Data Protection and Compliance at the University of East London, gave a sobering introduction to GDPR. Many have seen this as an update to the 1998 Data Protection Act (DPA), but it is a much more fundamental change, indeed the DPA would fail to satisfy the GDPR in at least 10 key areas.

To complicate matters, there are more than 50 areas where EU member states can apply derogations. The UK government is unlikely to finalise the detail of these derogations before 2018, but GDPR comes into force in May 2018 and penalties for non-compliance will be effective immediately. Quite apart from not knowing what compliance target to aim for, a *GDPR Lite* outcome could have implications for UK institutions that need to process the personal data of EU citizens. If the EU decided that the resulting regulations did not provide adequate protections, such processing would be subject to much more onerous restrictions than at present.

The Information Commissioners' Offices (ICO in the UK and the Data Protection Commissioner in Ireland) and have produced guidance on GDPR (see **More information**), and this is being updated frequently – make sure you read the latest version! The fines available will be much more than under current legislation (though the maximum permissible fines of €20,000,000 or 4% of global annual turnover are unlikely to apply to institutions, or indeed to be used very often, if at all), and the compliance regime is likely to be more vigorous (the UK ICO has requested an addition 200 staff).

The effort to prepare for compliance with GDPR is going to be significant, and despite what some suppliers are saying, there is no technological quick fix. Clarke recommends running a formal programme as many did for the millennium bug – only this time we know for sure GDPR is going to happen. One of the things that institutions can do to get ahead is to start assembling an inventory of their personal data holdings – this is likely to be no small task. They can also assess existing levels of compliance with the DPA, and the ICO would be willing to do voluntary compliance audits for those with the determination to put right any shortcomings they identify.

The GDPR is coming so act now – this is no time for ostriches.

Universities and Colleges
Information Systems Association

www.ucisa.ac.uk

Tel: +44 (0)1865 283425 Fax: +44 (0)1865 283426
Email: admin@ucisa.ac.uk

UCISA EVENT REPORT

More information

All the slides and videos of the event together with some of the resources mentioned are available on the UCISA website.

Cyber security survival guide event programme
www.ucisa.ac.uk/groups/ig/Events/2017/cyber

Presentations and resources
www.ucisa.ac.uk/groups/ig/Events/2017/cyber/cyber

Videos of the talks
www.ucisa.ac.uk/groups/ig/Events/2017/cyber/streaming

UCISA Information Security Awareness Online training
www.ucisa.ac.uk/infosectraining

UCISA Information Security Management System Toolkit
www.ucisa.ac.uk/ismt

NCSC Password Guidance
www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach

GDPR guidance (UK)
https://ico.org.uk/for-organisations/data-protection-reform/

GDPR guidance (IE)
www.dataprotection.ie/docimages/documents/The%20GDPR%20and%20You.pdf

Authors: Jerry and Corinne Niman