HE Update

Cyber Security

October 2013

It is now a daily occurrence to hear of another cyber-attack on the news. The probability of an attack is higher than ever, not least with the ever-increasing use of the internet and internet attached devices.

Parallel to this, there is a proliferation of free and "easy to use" software designed to exploit vulnerabilities and "hack" systems. This has made it easier for individuals or groups to hack systems.

It is not about "if" you will suffer from an attack, rather it is a matter of "when". The impact of an attack will depend upon:

- Your governance, risk management and control arrangements for cyber-security. Cyber-security is about mitigating the risks of cyber-attacks to safeguard your intellectual, financial and reputational assets; and.
- The motive and the extent of the attack.

Motives are varied and could include:

- Theft or modification of electronic information assets for financial gain (including personal data; intellectual property)
- Theft of electronic resource, taking control of your IT infrastructure to facilitate further cyber-attacks
- Disruption to online services or institutions' web sites
- Political statements through the defacing of web sites or from claims of successful attacks
- Ego-driven. Some hackers do it, because they can. They enjoy the sense of achievement of breaking in to systems

Cyber Security in the context of Higher Education

It's already happening

Universities are just as likely a target as any other organisation. Well-known attacks have made it to the national press in recent years:

- In 2009, the University of East Anglia suffered an attack on their email system, which saw private and politically sensitive climate research and opinions published online.
- In 2012 hackers targeted the top 100 Universities in an attempt to publish confidential information from breaching any server they could infiltrate. This was politically motivated about education policy worldwide. Some institutions had user name and passwords published.

These are just the reported attacks and there will be a number of attacks that are not publicised as well as undetected attacks that are likely to have taken place.

In our own audits we have witnessed webservers and websites hijacked to host links to disreputable websites, and trade on the good reputation of the University with search engines to boost their own rankings. Within the last month there have been reports of how compromised servers have been used to host illegal material and there are regular press reports of financial fraud, data theft and the use of many compromised servers (often referred to as a botnet) used to attack other networks.

There is enough evidence to show that this is a real risk that needs to be considered.

Security in an Open Environment

Teaching, research and knowledge exchange are the three pillars of the Higher Education Sector. The academics and students, who are the knowledge creators and sharers, need to operate in an environment that is innovative, collaborative and creative. Likewise Information Security also has three pillars, Confidentiality, Integrity and Accessibility will be paramount in supporting the aims of the whole University, and in no way should be considered inhibitors to innovation, collaboration and creativity.

The environment is therefore a lot different from other professional environments such as the financial service sector or defence, and the way in which cyber security is managed has to be proportionate to the activities and risk.

This does not mean that institutions should be more relaxed, they are just as susceptible to cyber attackers as any other organisation operating IT Systems (see Higher Education Attractiveness section below). The key is to protect what needs protecting in a targeted and proportionate manner – simple risk management.

Higher Education Targets

We have listed some areas in the table below which might cause cyber-criminals / attackers to target universities:

Area of potential interest	Who?	Motives
Intellectual Property (research, commercial collaboration, teaching material)	Competitor Foreign State	Financial / Economic Gain
Information relating to sensitive activities (animal testing / sensitive research areas, such as munitions, terrorism etc)	Political activists Terrorists Criminals	Political Malicious intent
Theft of IT Resource (taking control of IT resources as a basis for cyber-attacks elsewhere, or other criminal activities)	Criminals	Financial Gain Malicious intent Political
Student Fees (phishing / pharming to extract fees from students)	Criminals	Financial Gain
Examination Papers / Model Answers	Students Criminals	Academic Gain Financial Gain
Personal Data (identity theft and/or reselling data)	Criminals	Financial Gain

Sector Awareness

Universities UK (UUK) published a Cyber Security policy briefing paper in June 2012 targeted at Vice Chancellors and Registrars (or equivalent). The paper outlines the context of cyber-security, pointing out the UK government recognise it is a tier 1 threat to national security and that "Universities are considered to be part of the UK's critical national infrastructure, and as such are high on the government's list of sectors which are of particular interest".

It urges institutions to undertake three key steps to help reduce the risk of cyber attacks:

1. Ensure that the senior management team and governing body of the university is aware of the risks and vulnerabilities of their own institution as part of the normal routine of corporate governance.

2. Carry out an audit to gain a clearer understanding of the institution's primary intellectual property assets, and take specific measures to protect these assets more effectively.

3. Apply the 20 controls for effective cyber defence as set out on the Centre for the Protection of National Infrastructure (CPNI) website.

We fully agree with all of these suggested steps, but all three are not going to be straightforward to implement particularly the 3rd component, where careful risk assessment, segregation of activities and a heightened sense of IT Security awareness across the whole organisation, not just IT are essential.

Awareness and training is another essential ingredient. Often hackers will try and exploit human beings (known as social engineering) to harness information (sending fake emails requesting security details etc) to allow them to perform an attack. Using our sector and IT Security experience we can facilitate IT security awareness sessions for staff across the University.

Managing cyber-security is complex and requires considerable assessment of risk, control and cost. This is where our experience can help you.

How Uniac can help

We can help you in a number of ways through assurance or consultancy.

- If you have well developed cyber risk management framework we will validate your risk assessment and responses to risk.

- If you are starting from a low base we will work with you to identify and prioritise the necessary controls that are proportionate to your institutional risk profile and risk appetite.

Specialist Team

We are an experienced IT Audit team – team members have an average of seven years of Higher Education experience. We are all qualified Information Security Auditors (Certified Information Systems Auditors) and between us we hold the Certified Ethical Hacker and Certified Information Systems Security Professional accreditations. Most importantly, we understand the sector and the challenges you face, particularly in the area or information technology and systems.

Appropriate and Flexible Approach

We have delivered Cyber Security reviews at a number of our institutions. We have taken several approaches, adapted to the institution's needs, for reviewing cyber security:

- Facilitated workshops with IT staff to benchmark existing technical controls against the Centre for Protection of National Infrastructure Critical Security Controls for Cyber-Defence (UUK recognised framework for managing cyber threats at a technical level).
- Reviewed institutions own self-assessments against the Centre for Protection of National Infrastructure controls to validate.
- Undertaken focused and in-depth reviews of specific areas that contribute towards cyber-defences, for example network perimeter security review (entailing vulnerability assessment).
- Worked with institutions to assess electronic information assets by meeting and understanding how researchers; academics and administrative staff manage electronic information.

We will work with your institution to develop the most appropriate approach. We have included two case studies of work undertaken to give you some more detail on what we have done. See Appendix A.

Working with UNIAC you will be given the assurances and advice required for managing the ever-increasing risk of cyber threats. **To find out more, please contact us:**

Peter Follett

t: 0161 247 2861

e: pfollett@uniac.co.uk

David Tomlinson

t: 0161 247 2846

e: dtomlinson@uniac.co.uk

Appendix A – Case Studies

Perimeter Network Security Audit

An external cyber-attack can cause financial and reputational damage by disrupting IT services, risking personal or commercially sensitive data or exposing systems to criminal activity. Strong network perimeter defences are vital to counter these threats.

Scope

The audit assessed:

- Design of the network perimeter
- Internal network design, including network segmentation and DMZ (or De-Militarised Zone – a restricted area of the network which houses servers involved in riskier activities such as hosting websites
- Firewall position and firewall rules management (including change control)
- Incident response procedures for external based attacks

Key Observations

- Servers on the network with significant vulnerabilities;
- Network switches using weak authentication and visible from the internet; and
- Webservers running in a corporate database VLAN (segmented area of the network) the network.

Value

The vulnerability assessment tool provides a thorough level of testing and allows us give an increased level of assurance.

The tool picked up issues that would have been difficult to identify on a sample basis, some of these were unknown to IT Services. A full report generated from the tool was provided as an appendix to the report, at no extra cost. The Director of IT Services valued the output.

Cyber Security

This audit followed the guidance of the UUK Briefing Paper and assessed the University against the CPNI 20 controls and also evaluated how the institution understands and manages the value of electronic information assets.

Scope

Phase 1 assessed:

- the existing governance and policy framework for managing cyber-security risks.
- the organisation's understanding of its research and intellectual property information assets by meeting a number of academics across the organisation.

Phase 2 assessed:

- the organisation's IT provision against the CPNI recommended 20 technical controls for managing cyber threats.

Key Observations

- Handling of data and information at the behest of staff, including the lack of research data management plans
- Absence of information security policies, particularly around emerging issues such as using cloud services and mobile devices
- Weaknesses in network perimeter
- Limited training and awareness of information security and cyber threats (i.e. phishing)

Value

The Director of IT Services welcomed the output of the audit and used this as a catalyst for transformation in the approach and design of IT security.

A pragmatic assessment against the recommended 20 CPNI controls to manage cyber threats, recognising the sector and institutional context.