Walls of straw – the cyber risks to higher education

Globally, in every facet of life, advances in communications technology and our reliance on computers and the internet allow us to live and work more efficiently than ever before. Higher education relies on the development of knowledge and the need to conduct and communicate research activity. Universities are often bound in research activity to business, government and other organizations whose interests need to be protected and managed. But is there a disparity in approach? Is research activity, security and the protection of privileged, proprietary and classified information appropriately implemented and managed in higher education? In this article the author questions: are there gaps open to cyberattack?

"We fear things in proportion to our ignorance of them."
Christian Nestell Bovee

"To err is human, but to really foul things up you need a computer."
Paul R Ehrlich

PHILLIP WOOD

Head of the Department of Security and Resilience
Buckinghamshire New University

Knowledge is power and universities understand that maxim. Higher education has a role and a duty to develop academic and professional capability, to question, to evaluate and to analyse and, in more recent times, to make graduates more 'employable'. Universities help their students to mature both intellectually and personally in an environment dedicated to the pursuit of excellence. To allow the necessary learning environment (and the students within it) to flourish, knowledge needs to be developed, stored and transferred. Research and associated intellectual property (IP) are essential components of credible academic practice; and the development of new ideas, theories and scientific discoveries is at the core of academic activity. So there is a constant flow of information as facts, ideas and theories are dissected, dismantled, developed, discussed and disseminated; data is sifted, analysed and evaluated for many different reasons. Doctoral and postgraduate research serves individuals, and their research outcomes may contribute to the wider body of knowledge or understanding in a particular field or specialism.

Most universities conduct research with and on behalf of business and industry, governmental and non-governmental organizations. The power of higher education institutions as agents of change and progress has never been underestimated by external organizations who seek either progress or competitive advantage. As a result, universities are funded by multiple interested parties; and it is neither unusual nor undesirable for institutions to work for competing investors concurrently.

"Knowledge is power and universities understand that maxim."

Because academic institutions are a valuable asset, and because the research outputs can have an impact, such as increased profitability, competitive edge or support of national interest, their knowledge assets are immense. Universities are hotbeds of creative thought and innovation. And they have much to protect. Universities UK[1] states that data that has been subject to: ethical approval (and may therefore be especially sensitive), legislative and contractual obligations (and may therefore have economic impacts if lost or accessed) and their own economic or political value will be of particular concern.

With all of this valuable knowledge, and the associated communities of students, academics and researchers who are actively engaging in scholarly work, universities are an attractive target for adversaries. The threat of competitor intelligence gathering is not new, and organizations have been at risk from espionage and the loss of information ever since organizations and competition existed. However, all organizations, large and small, and we as individuals, are now facing an amorphous and unprecedented risk landscape, where the freedoms of information development and transfer of the 'Information Age' bring a concomitant 'cyber' threat.

"… universities are an attractive target for adversaries."

The evidence is beginning to mount that cyber-related problems comprise the main security issues facing organizations currently, and there is no reason to suspect that this will change soon. The UK Government's National Security Strategy[2] categorizes cyberattacks as a Tier One threat to national security, alongside international terrorism. If we consider the comparison between those two threats, terrorism is generally, in risk management terms, low in probability of occurrence and high in impact, while cyberattacks have a high probability of occurrence and have the potential for very high impacts indeed. The UK Government[3] is committed to meeting this challenge and allocated significant resource towards the UK's national cyber security strategy to 2016, which has four objectives:

- to make the UK one of the most secure places in the world to do business in cyberspace
- to make the UK more resilient to cyberattack and better able to protect our interests in cyberspace
- to help shape an open, vibrant and stable cyberspace that supports open societies
- to build the UK's cyber security knowledge, skills and capability.

These objectives are important to current, continued and future ability to face threats, and reflect the general and evident concern of governments, and therefore the organizations that they are required to protect and support. A balance needs to be struck between the use of information and its effective and secure management. However, despite stated threats, the growing allocation of resources and the commitment to protecting organizations, 'cyber' is misunderstood. This is unsurprising given that the threat appears to change, is omnipresent, and that the perpetrators of cyberattacks are faceless. They have multiple motivations including financial gain, competitive advantage, or the exploitation of target information for wider purposes. The investment in cyber protection for businesses is an important component of a wider information management strategy. A particular issue for organizations that employ people (that is, all of them) is that they misunderstand what the threats may be; but, more importantly, they fail to understand that the effect of cyberattacks is multiplied by the targets themselves. Cyberattacks prey upon human inquisitiveness, greed, narcissism and the need to know more, using technology as a conduit. It is not by accident that cyberattacks use fake bank messages, advertisements and offers of some reward or other to lure the unsuspecting and inquisitive mind. (Universities probably have a good share of the former and a necessary core of the latter).

"… the effect of cyberattacks is multiplied by the targets themselves."

In terms of the way that they are structured and run, most universities do not differ significantly from any other business organization that has a concentration of data in one place, alongside the significant concentration of knowledge that is linked to external partners. If we compare with 'for profit' organizations that depend upon their trade secrets, recipes, plans and market knowledge for their survival, we can begin to identify some potential disparities. We can select any number of industry sectors to make the comparison; but if we consider the financial services sector and banking in particular, or the energy or pharmaceutical sectors; the main and high profile companies invest much time, effort and money in their information management and protection. Governance and protection of research and development will ensure that the information security management requirements will be expected to be met; and that the orientation towards,

and understanding of, the vulnerabilities related to cyber security should be part of the organizational DNA. Although, as a general rule, the application of effective cyber security management may be considered to be patchy, for those organizations who are serious about their competitive edge and financial viability, there is good reason to expect that there is awareness and resource allocated to protection.

On the flip side, the DNA of universities is different. Higher education needs thinkers, talkers and disseminators of ideas who are open and free with thought and ideas. Academics publish; and that is the core of high-level academic work: to constantly seek to challenge and add to existing bodies of knowledge, demonstrating excellence in thought and learning, and giving wide access to its outcomes, successes and failures. However, this is at odds with what Edward Wilding[4] noted, as an 'enduring issue':

'Knowledge and information are amongst the most valuable assets that an organization owns. These assets, referred to as intellectual property, are vital to the wellbeing of commercial operations but are often poorly protected.'

The consequences of lack of protection can be catastrophic to an organization; successful exploitation by adversaries can be more damaging than direct financial theft and can lead to significant consequential effects including loss of reputation and market share and the need to devote excessive effort to recovering operational effectiveness. In addition to the fact that information is often an intangible asset, which can mask the routes by which it is lost, the perpetrators of any crime can be difficult to categorize because of their varied origins and motivations..

Who 'they' are and what 'they' want covers a range of threats. The risks to information integrity can come from either inside or outside the organization; insider employees will steal for financial gain, a desire to damage the organization, personal use or gain, or they may retain or release information inadvertently. Outsiders may retrieve information for competitive advantage in the marketplace, or aim to damage the organization; there is also a considerable and enduring risk of economic or government-sponsored industrial espionage, the activities of the media and protest and activist groups. I outlined this in a cyber-related blog post[5] last year: 'out there in the new threat environment, the adversaries operate and wait for the opportunities; they already have the motive and the means.' Threats to information are not confined to a single level of the organization and for universities the range of activities serves to compound vulnerabilities. Moreover, because universities are often linked to the organizations that may suffer business 'fatality' due to information loss – the compounded vulnerabilities and their potential impacts make them part of their own partners' cyber risk problem!

The dilemma of information protection is a challenge in universities, where restricting access can inhibit information flow and the development of ideas. Information needs to be used and manipulated to be effective, and there is therefore a requirement to ensure that a degree of risk management should be applied to ascertain what is used, and when, and take into account the impact of misuse and loss. This need to balance *'need to know'* with *'need to flow'* can mean that levels of protection need to be compromised so that information routes and the freedom to work within them can be maintained. This compromise is essential, and perhaps is the normal requirement in education, but in turn it gives an opportunity to adversaries. The access routes for cyber loss are opened and maintained by the very openness and information sharing needs of the organizations that they target.

"… for universities the range of activities serves to compound vulnerabilities."

After reading this article, it is a worthwhile exercise to conduct an internet search for guidance on cyber security in organizations. You will find commonalities; there will be recommendations to implement processes and governance, invest in technology and develop monitoring and reporting structures. These measures make sense for protecting against all security and continuity risks and threats to organizational resilience and will be incorporated into any effective and sensible set of security measures. The other 'pillar' of all security

functions is that of instilling a culture and awareness related to the understanding and protection of information. You will find recommendations related to this in most guidance; UUK's example[6] states that:

'Effective institutional assessment of risks and implementation of secure practices rely on a shared understanding of the threats and challenges facing the institutions. All networks should have use policies that should be understood and implemented by all users.'

There is nothing wrong with this advice; however, the reality is that the issue of 'understood and implemented' is the most challenging element of the complete cyber security requirement. While all institutions are relatively adept at producing policies, how do they instil understanding and implementation in a fluid, thinking, innovative and interconnected workforce, whose intellectual approach will naturally push the boundaries of information management requirements?

"… the strictest of protection measures are being bypassed daily by the rapid growth of availability of information loss facilitators …"

The prime and truly confounding area of cyber security management is not that of the technology. Cyberattacks need not be aimed at targets within a university's four walls. Firewalls, network protection, passwords and access levels all reduce the risk. However, the strictest of protection measures are being bypassed daily by the rapid growth in availability of information loss facilitators which can be brought into the workplace. Mobile telephones, flash drives, mp3 players and cameras, all of which can be used for information theft, are now in one device. Home working and the use of mobile computing to process organizational data on the move also facilitate the leakage of information. We take our information (and that of our partners and stakeholders) and process it in coffee shops and our spare bedroom 'offices' at home. We take our mobile computing systems on holiday and on business to and via global locations and use wireless and state communication networks to process our trade secrets and personnel information. None of these environments can be guaranteed to be secure at all; and in many cases can be 'hostile'. (If you want to scoop up information, always look to hotels, airports and coffee shops first). Effectively, the protection of documentary and electronic information being carried by communicative and networked remote workers and travellers is more difficult and requires an organization to educate and train its people in the many routes of information loss through such facilitators. However, thinking about what universities do, and how they need to operate: is that realistic?

Back now to considering our *people*: employees and students, academics and administrators, who make our universities successful centres of knowledge and growth. In effect, as inquisitive and connected people, who need to access information and carry their information with them, and who *need* to be networked, it is important to understand that those who are employed in higher education will mutate the risk through bypassing systems and may be non-responsive to deterrence and defence measures. Moreover, because of their need to access and ensure that information flows, they may well take random or imprecisely targeted attacks and direct them to where they may cause more damage. This is now common human behaviour that is not necessarily malicious – but can be highly damaging in effect. Importantly, and as a major enabler of cyberattacks, our behaviours do not require financial investment by adversaries, as all universities have invested in structures and networks to process, store and manage information. All that the enemy needs to do is find the way in and our people can do the rest.

"If you want to scoop up information, always look to hotels, airports and coffee shops first."

If we cannot manage our people, we are handing over the access control 'keys' and offering free facilitation for cyber adversaries. So, we need rules. But these will only be effective if employees are willing and able to comply. Our growing connectivity and the embedding of social networking into our lives (the new and enduring cultural change of the 21st century) has changed all that. Controlling the new normality of disinhibited networked behaviour requires a strict covenant between employer and employee, clear disciplinary processes,

training, and awareness of risk and consequence. Importantly, we need to understand 'ownership' of the risk, which is a wide organizational challenge, as Harvard Business Review[7] mentions in its report:

'There appears to be a disconnect … between organizations' confidence in their efforts to instil a cyber risk culture and its actual implementation. Chief executives all seem to think they're doing a great job, and maybe it's because they're talking about it and their budgets indicate it.'

"… we need to protect our information assets as the consequences of not doing so are potentially severe."

Our universities are part of a wider society that faces immense challenges in dealing with the risks of cyber activity. We are no different than any other organization; we need to protect our information assets as the consequences of not doing so are potentially severe. As targets, with research and innovation at our centre and with unique and compounded access to business and information of strategic value, we must recognize and manage our vulnerabilities. Despite the technology risks, the emergent cyber vulnerability comes from human re-adaptation and psychological and social evolutions: we have a need to communicate and share constantly. The next time you sit on a train, or even walk down a busy street, *look at the scale of information movement that is happening*. This is a social and behavioural phenomenon, enabled by technology that makes it easy for humans to do what they need to; be recognized, stimulated, share, store and access information and communicate – exactly the business of education and research. We can consider the imposition of systems, processes and frameworks to manage our intellectual activity and the information that we own and share. In higher education, we have access to information that we do not necessarily own, but must protect. But we need to use that information constantly, we need to share it, and the new normalities of social networking provide an additional layer of shifting and accessible vulnerability gaps. And as a final thought, sometimes, educators can assume that those around them may be less intelligent or capable than themselves. Sometimes that may be true. However, to make that assumption in the cyber context, where adversaries are highly skilled and in many cases backed by huge resource, is dangerous. The academic mind is a marvellous and inventive thing to be valued and nurtured; the mind of a high-risk cyber adversary is equally marvellous – and is outwitting any number of professors every hour of every day. And cyber adversaries don't take long vacations!

"… the mind of a high-risk cyber adversary … is outwitting any number of professors every hour of every day."

References

1. Universities UK, *Cyber Security and Universities; Managing the Risk*. Industry Report, 2013 London, Universities UK.
2. HM Government, *A Strong Britain in an Age of Uncertainty; The National Security Strategy*, Policy Report, 2010, London, Cabinet Office.
3. HM Government, *The UK Cyber Security Strategy; Protecting and Promoting the UK in a Digital World*, 2011, London, Cabinet Office.
4. Wilding, E, *Information Risk and Security*, 2006, London, Gower.
5. Wood, P, 1 August 2013, Cyber Cyber Burning Bright, Bucks New University Security blog: http://buckssecurity.wordpress.com/2013/08/01/cyber-cyber-burning-bright/ (accessed 12 April 2014).
6. Universities UK, ref. 1.
7. Harvard Business Review *Meeting the Cyber Risk Challenge.* Report by Harvard Business Review Analytic Services, 2013, Watertown, Harvard Business Review.

Phillip Wood
Head of the Department of Security and Resilience
Buckinghamshire New University, High Wycombe Campus, Queen Alexandra Road, High Wycombe, Buckinghamshire HP11 2JZ, UK
Tel: +44 (0)1494 522 141 | E-mail: Phillip.Wood@bucks.ac.uk

To cite this article:

Wood, P, Walls of straw – the cyber risks to higher education, *Insights*, 2014, 27(2), 192–197; DOI: http://dx.doi.org/10.1629/2048-7754.160