UNIVERSITY CHALLENGE:
Protecting research in higher education

A report by VMware and Dell EMC on the current landscape of cyber security at UK universities, the impact this could have on the country’s national security, and how these institutions can best safeguard against an increasingly sophisticated threat landscape.
TABLE OF CONTENTS

Foreword 2
About this research 3
UK universities in the digital era 4
A threat to national security 7
What is the cost? 8
Advice from experts 9
Five things universities need to do now 10
Conclusion 12
National secrets are always prone to attack. That is why they are guarded by the appropriate security mechanisms when part of a government organisation. What happens, however, when they exist outside of traditional structures and defences? What if, for example, they take place in universities?

Why would anyone want to target a university? They are academic institutions of learning, not security organisations. How often do they even house national secrets?

As it happens, more and more UK universities are embarking on highly sensitive, government-backed research programmes, which are putting institutions at the cutting edge of innovation in a variety of fields. This is vital, not only to further national interests, but for the institutions to be able to differentiate themselves in an increasingly crowded marketplace.

They are undergoing their own digital transformations as they establish what their mission is and how they fund it. Driven by tech-savvy students and teaching staff, combined with the revenue potential of remote learning and research projects often totalling millions of pounds, UK universities are rapidly expanding their digital footprints.

With such evolution comes increased profile, which institutions are using to establish themselves as both education and innovation hubs. The research programmes being carried out are putting institutions at the cutting edge of innovation in a variety of fields. However, the very nature of these programmes means they attract unwanted attention from hackers. Whether state-sponsored or financially motivated, the cybercriminals targeting UK universities have access to an increasingly sophisticated arsenal of digital weaponry.

In 2016, VMware examined the threats UK universities face and how they can guard against cyber-attacks to protect intellectual property. The study concluded that in majority of cases, these world-leading institutions were experiencing successful cyberattacks every hour. Today, with Dell EMC, that study has evolved into examining the impact of a successful attack in today’s environment and considers whether weak security practices at academic institutions pose an unwitting risk to national security.
VMware and Dell EMC commissioned research to explore how universities that conduct research programmes currently combat cyberthreats, the impact of successful attacks on highly sensitive data, and the financial, reputational and human costs incurred.

On the companies' behalf, an independent research organisation questioned 75 senior IT leaders at 68 universities in the UK between November and December 2018.
Thanks to digital technologies, places of higher learning are increasingly able to offer learning and research opportunities to students across the world, without requiring them to physically be on campus. This is demonstrated in the 20 per cent growth from 2012/13 to 2016/17 in students based outside the UK studying for awards with UK higher education providers.

What this means is a much larger marketplace with new potential sources of revenue. Exactly what universities need at a point when traditional sources of income are increasing strained.

Research, in particular, is an important stream of finance. The institutions we surveyed generate an average of £22m income each through research. A significant proportion of that funding comes from the UK government, with 93 per cent of programmes receiving some form of public sector money.

As with any organisation, becoming more connected means creating a larger digital footprint. This in turn increases the chances of operations being exposed to potential cyber-attacks. Forty-nine per cent of universities surveyed said that a cyber-attack is attempted on their institution daily or more than once a week. Of equal concern is that the same number strongly agreed that attacks were growing in sophistication as well as frequency.

What are hackers after?

- 54% Scientific research
- 33% Security and defence research
- 50% Medical research
- 37% Economic research
While this is certainly cause for concern, universities that have robust security practices, regularly updated, can reduce the likelihood of cybersecurity events happening and reduce the impact of those that do; thereby enhancing the protection of their operations, teaching and student populations, and intellectual property.

Unfortunately, few universities have complete confidence in their security infrastructure and approach – often due to insufficient budget allocation to secure environments and protect information. For example, based on the responses to our survey, UK universities have, on average, a £7m IT budget, but only commit eight per cent of this budget towards cyber security. This equates to a £5m drop in budget from 2016.

Could the shortfall be made up via increased revenue? In theory, but if that’s to happen universities need to either increase their research income or review their spending priorities: of the average £22m they earned through research, only seven per cent of that goes towards data protection.

A lack of IT investment means that institutions cannot simply throw more money at the problem; processes and procedures need to change. Many recognise this, with 49 per cent stating that their overall security practices need to be more robust to compensate.

Our research found that people are one of the weakest links

Half of respondents believe professors / teaching staff and students are most likely to be the causes of data breaches

Nearly 1 in 6 respondents consider researchers to be the biggest contributors to shadow IT
Delegated acquisition and implementation of technology rapidly is not, in itself, a negative. Properly managed and governed it can be a major factor in any organisation being able to act quickly. However, when done so without the oversight of central IT, therefore outside of defined security practices, it presents a major risk. It’s consequently not a surprise to find shadow IT as one of the three internal challenges that universities are having to overcome to improve cybersecurity. The others were a lack of control over IT architecture and silos between departments.

So, what happens if security practices are not improved?

97% of respondents felt that a successful cyber-attack could damage their reputation

93% thought it might make third parties reconsider working with them

While this might seem like broad assumptions, those that have been victim of a successful cyber-attack know for certain the impact it can have. Over a quarter (28 per cent) had seen it reduce their credibility, while 61% said it has forced a research project to stop. This has increased significantly since 2016 when only 22% said attacks had led to a halt in research projects.

Even not being able to demonstrate cyber security competency can have an effect – one in four said they have lost potential research partners due to not attaining or maintaining certain cyber security certifications.

Reduced credibility not only threatens research revenue; for example, since 2016, there has been a 30 per cent increase in the impact of cyber-attacks on reducing researcher talent wishing to work with universities.

In short, a damaged reputation can have long-term detrimental effects to a university’s ability to attract research support and talent. However, as we’ll discover, this is not the only impact nor the most severe.
As well as providing UK and international citizens with high quality education, universities are also vital research houses into breakthrough medical treatments, environmental management, new manufacturing materials, technological advances and many other innovations.

Because of this, it’s heavily supported by the UK government and public sector.

- 93% of research programme funding comes from the UK government
- 36% of UK universities believe a successful cyber-attack on their research data would pose a risk to national security

As well as risking national security, 1 in 10 strongly agree that a successful attack on research could have a harmful impact on the lives of UK citizens. This may seem farfetched; but consider this – over half of respondents say a successful cyber-attack has resulted in research ending up in hands outside the UK. While much overseas interest is likely to be linked to industrial or economic interests, research linked to national utilities, defence, food security or healthcare infrastructure could pose a serious threat to life if it fell into the wrong hands.

“The higher education sector in the UK has long been a target for cyber criminals, tempted by the world-leading academic research that universities produce in sensitive areas such as medical and defence research. As the cyber threat evolves, and attacks become more sophisticated, it is imperative that universities invest heavily in their cyber defences and protect the professional and personal data of the 2.5 million students and staff learning and working in universities across the UK.”

Talal Rajab,
Head of Programme, Cyber and National Security, techUK
Despite recent increases in income, universities’ finances remain precarious. Even for the most prestigious of institutions, there are no guarantees of future revenues.

Damaged reputations from successful cyber-attacks lead to loss of income; those research partners scared off by porous security represent sources of funding. Breaches also carry a cost directly as well.

Almost all (92%) of UK universities say that a successful cyber-attack on their research data could result in serious financial loss for their institution = an average of £300,000 per successful attack on research data in the last 12 months alone.

These are major causes for concern, and alone would represent motivation to ensure cybersecurity is a high priority for universities. Ultimately however, they are individual organisational concerns – if an institution in London, for example, suffers a breach, it doesn’t necessarily affect those in Birmingham, Manchester or Edinburgh (unless they were working in partnership on the affected project).

There is, however, another issue that has ramifications not just for specific universities, or even higher education as a sector, but the entire country.

“UK universities have a huge opportunity to offer a higher level of educational experience with digital technologies. The revenue implications of this, at a time of uncertain income, are immense. Yet the race to differentiate themselves in an increasingly crowded market must not come at the expense of security. Increased connectivity renders traditional security practices redundant, which means universities must assign cyber defence as much priority, if not more, as acquiring and integrating new digital tools.”

Louise Fellows,
Director, Public Sector UK&I at VMware
The findings of this survey therefore paint a worrying picture. Despite a clear understanding amongst practitioners of the financial consequences of a successful breach, investment levels remain relatively low. This must change. Universities must invest in defensive measures, adapt to the ever-changing cyber threat and ensure that the profitability of their academic research remains protected.

Talal Rajab,
Head of Programme, Cyber and National Security, techUK

It is certainly true that as an institution we are spending more time and resource focussing on the security of our systems, sensitive data and take that responsibility seriously. We practice what we teach and seek to prevent, detect and be proactive with the use of technology to help look after the data we hold.

Matthew Storey
Head of Storage and Virtualisation, Lancaster University
Universities need to improve their approach to cyber defence, without hampering long-term innovation or the digital experience of their users. To do that, they need to approach how they combat digital threats differently.

**Enforce good rather than chasing bad:**

Rather than trying to keep up to date with the different techniques cyber criminals will use to launch a hack and escape detection, and chasing bad threats after they have hit the network and already caused havoc, universities should look to adopt a more “knowing good” approach to security. That means focusing on approved behaviour for applications and services rather than trying to block all unknown activity or potential threats. Understanding these good behaviours makes it much easier to enforce known good.

**Unlock IT:**

IT is a key enabler of innovation and positive change, and it must be seen as just that. IT needs to act just like a business, positioning themselves as the best, most attractive option otherwise staff or students will be tempted to look elsewhere for their needs, leading to Shadow IT. By providing a creative, agile platform that can deliver support quickly, the security implications of Shadow IT can be avoided.

**Educate, educate, educate:**

Balancing a culture of openness, access and seamless experience whilst ensuring security is a tough challenge for any organisation. Often staff or students, uneducated in the role that they play in security, may unintentionally ‘open the door’ to hackers. User education is critical and the only way to maintain balance is to educate everyone on their collective responsibility when it comes to security, to keep the university and the information it holds safe from potential breaches.
Securing the user:

With data constantly on the move, and digital footprints expanding rapidly, traditional firewalls are no longer sufficient on their own to protect against today's threat landscape. Staff and students are accessing information from many different places on many different devices, and that needs to be done in a secure way. Universities should take a more user-centric approach to security, in which they secure the user and their interaction with data first, building policies around students and faculty and the way they work before working backwards to the portals and channels that the IP is delivered over, and before focusing on on-premise and legacy infrastructure.

21st century security for 21st century education – University of Central Lancashire delivers secure yet seamless student experiences

The University of Central Lancashire (UCLAN), based in North West England, is one of the UK's largest universities with a student and staff community approaching 38,000. The institution is dedicated to creating real-world learning experiences for its students and embracing a broad pool of academic talent.

In order to deliver that objective, UCLAN has transformed its approach to security, with the IT team adding layers of security, right down to the network level. This means that all systems and web servers will be kept secure and compliant at the heart of the infrastructure, no matter where students need to browse. With increased agility and flexibility in its approach to technology, students will be able to interact with the university IT services in the way that suits them best – anytime, anywhere and with any device of their choosing.
CONCLUSION

Digital technologies offer huge opportunities for universities at a time when they need to be expanding their reputations, driving new sources of revenue and increasing existing income streams. Yet if universities are unable to properly secure their systems, users and intellectual property, investors may reconsider whether the return is worth the potential risk.

Universities need to improve their cyber security practices if they are to protect their reputations and most importantly, national security. Failure to do so could compromise the UK’s defences – too high a price for the result of reduced IT budgets. It’s not a simple fix, but by looking at security as an intrinsic element of IT infrastructure, educating users in their collective responsibilities, and positioning IT as an innovation enabler to avoid risky work-arounds, universities in the UK will stand a far better chance of holding strong against increasingly complex threats.

“

In conducting research that will shape the future of the nation and its citizens, universities are putting themselves under the microscope of some of the world’s most well-resourced and potent cyber attackers. We hope that this study will encourage them to look critically at their cyber security investment by highlighting that, right now, their security systems simply aren’t holding up to the challenge. Universities must do more to protect the sensitive information they hold and invest in systems which can dynamically manage the range of threats faced by each institution, to ensure research delivers on its promise and is not compromised.

John Chapman,
Chief Information Security Officer, UK Public Sector, Dell EMC

"
About VMware

VMware software powers the world’s complex digital infrastructure. The company’s compute, cloud, mobility, networking and security offerings provide a dynamic and efficient digital foundation to over 500,000 customers globally, aided by an ecosystem of 75,000 partners. Headquartered in Palo Alto, California, this year VMware celebrates twenty years of breakthrough innovation benefiting business and society.

For more information, please visit https://www.vmware.com/company.html

About Dell EMC

Dell EMC, a part of Dell Technologies, enables organizations to modernize, automate and transform their data center using industry-leading converged infrastructure, servers, storage and data protection technologies. This provides a trusted foundation for businesses to transform IT, through the creation of a hybrid cloud, and transform their business through the creation of cloud-native applications and big data solutions. Dell EMC services customers across 180 countries – including 99 percent of the Fortune 500 – with the industry’s most comprehensive and innovative portfolio from edge to core to cloud.