vmware®

University Challenge: Cyber Attacks in Higher Education

A report by VMware exploring the evolving threat for UK universities and how they can guard against cyber attacks to preserve their intellectual property

Contents

Foreword

Tim Hearn, Director, UK Government and Public Services, VMware

Today data is widely regarded as one of the most valuable assets any business can have; most understand it has to be fiercely guarded from competitors and other parties unauthorised to access it. Yet with recent high profile data breaches highlighting how frequent and damaging a cyber attack can be, it shouldn't be a surprise that cyber crime is now the fastest growing economic offence.[1]

The range of incentives for hacking into an organisation and stealing its data is becoming increasingly diverse and reflects the growing economic and social power of data. As ambition increases among hackers, so do the risks and the sophistication of attacks.

With attention frequently focused on the threats faced by commercial businesses, it is important to remember that public sector organisations in the UK such as universities are also increasingly at risk from cyber crime. Their status as world-leading research institutions also makes them a prime target. If their information falls into the wrong hands, the consequences can be serious, from anti-competitive commercial practices, to threats to national security, as well as the usual risks of identity fraud and financial crime.

Protecting our higher education institutions from cyber crime is vital if the UK is to remain as one of the world's top research and innovation destinations; it has to be a board level issue both in the commercial and public sector world. If UK universities are to continue attracting the best students from both home and abroad, damage to reputation through cyber attacks and associated data breaches can create a serious threat to their ability to compete for applications and associated funding.

To discover more about the scale of this issue, we recently questioned senior IT figures at UK universities about the scale and nature of the cyber attacks they had experienced. Our findings revealed that the situation is increasingly prevalent, with the majority reporting that they experience successful cyber attacks every hour.

This report explores the steps universities can take to protect against today's increasingly sophisticated threat landscape and to ensure that their intellectual property (IP) remains in safe hands.

Tim Hearn, Director, UK Government and Public Services, VMware

[1] PWC Economic Crime Survey 2016

About this research

VMware commissioned research to explore the extent of cyber attacks and the standard of IT security within UK higher education institutions. On VMware's behalf, independent research house Vanson Bourne questioned 75 IT decision makers[2] in approximately 50 universities across the UK about their experiences of cyber attacks and their approach to dealing with threats. The research was carried out between January and February 2016.

Why target universities?

British universities are renowned throughout the world for the quality of their research and expertise, producing more academic research than any other country apart from the United States.[3] The value of this contribution to the economy is significant; for example, universities generated £86.6 million in IP revenue between 2012-13 alone.[4]

Due to its value, certain organisations and individuals are prepared to take any measure necessary to get their hands on university data, including committing cyber crime. According to official figures, the public sector, which includes higher education, accounted for 43% of compromised data records over the last two years; a five-fold increase over 2014.[5]

The appeal of their data and resulting IP also goes far beyond academia. Research in all fields is vital for innovation and universities carry vast quantities of sensitive information to help advance government and commercial programmes in areas such as healthcare, engineering and technology and national defence.

Higher education technology consultant, Paul Hopkins, UK HE-Shared Services, comments on the targeting of universities: "As cyber crime becomes more prevalent in society, universities will feel their share of the impact. Critical research data will become a natural target for cyber attacks."

Clearly the stakes are too high for this information to fall into the wrong hands. However, nearly eight in ten (79%) universities have experienced damage to reputation and almost three quarters (74%) have had to halt a valuable research project as a result of an attack. A significant 77% also said a breach has the potential to impact national security, due to the potentially sensitive nature of the information which could been compromised. This signifies that individuals and organised groups are targeting research and development data for a purpose. They are both determined and competent enough to access what they are looking for and universities must respond to this.

[2] Including CIOs and CISOs responsible for the IT security of the research data
[3] Global Innovation Index, 2015
[4] University Alliance, 2014
[5] Gemalto Breach Level Index report 2016

We found that attacks are already happening in UK universities:

Almost all universities (87%) have experienced at least one successful cyber attack.

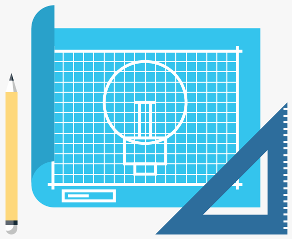
Over a third (36%) of UK universities are blighted by a successful cyber attack each hour.

83% believe cyber attacks are increasing in frequency and sophistication.

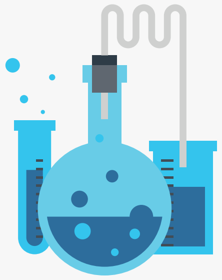
These are not just small-scale events to be brushed aside. Consequences range from threats to students' personal information, to IP loss and anti-competitive behaviour.

Attacks on student data are common, but critical research IP is also highly vulnerable:

43% have had student data attacked, including dissertation materials and exam results.



25% have experienced critical intellectual property theft.



28% have had grant holder research data attacked.

In addition, the nature of these attacks is not always sophisticated. It is not just external threats tapping into confidential university information. Over half (52%) of UK universities claim full-time domestic students pose a risk to cyber security.

> "Internal threats could be both intentional or unintentional due to lax internal policy and poor 'cyber hygiene'. For example, allowing students to re-use existing passwords, or setting those which can be too easily guessed."

Talal Rajab, Programme Manager, Cyber and National Security

Resource-stretched universities struggle to make the security grade

Many universities admit they are struggling to deal with cyber security, particularly when it comes to having the right technology to protect and manage data. As partly publicly financed institutions, universities can be more financially stretched than commercial organisations. Although further afield than the UK, it is issues like this which caused the high profile attack at Rutgers University, with the hacker who brought the system down describing the infrastructure as crumpling "like a tin can under the heel of my boot."[6]

Our research found:

Overall, nearly two thirds (64%) don't believe their existing IT infrastructure will protect them against cyber attacks in next 12-18 months.

Over a quarter (27%) see the current security of their data centre as 'inadequate' and in urgent need of updating.

85% of UK universities agree that more funding must be given to IT security to protect critical research IP.

[6] Reported by Financial Times, November 2015

As well as facing financial limitations, universities are often more open and collaborative than most businesses. While the information within private sector companies is typically only accessible to employees, and often on a 'need to know' basis, university data is shared with academics all over the world. Students and professors access resources via their own devices and come and go as they please, with universities maintaining little or no control over these personal devices. Every year, thousands of new students arrive and thousands leave, creating a tidal wave of data security risks.

> "Universities, unlike private organisations such as those in financial services, are 'open-door' societies with freer movement of data and people, which can cause problems when imposing strict security policy and protocol."

Paul Hopkins, UK HE-Shared Services

What can be done?

Advice from the experts

> "Universities must take a holistic approach to security, striking a balance to ensure critical research data is adequately protected without prohibiting or impeding researchers."

Paul Hopkins, UK HE-Shared Services

> "While UK universities continue to be world class in their quality of teaching and student experience, many are falling behind in terms of IT security. It is imperative that they are adequately able to defend against cyber criminality, investing in the appropriate technologies as necessary."

Tim Hearn, Director, UK Government and Public Services, VMware

Six steps for fighting cyber attacks

1 Take it to the top

To make cyber security a board level issue, it needs to be placed firmly on a university's risk register, alongside other issues such as funding, health and safety and international relations.

A study by The Economist Intelligence Unit, launched by VMware at the 2016 RSA conference[7], has shown there is a systematic disconnect and misalignment between corporate and IT leadership on cyber security investment and cyber protection priorities. More than 30% of IT security executives globally expect a major and successful attack within 90 days, but only 12% of corporate leaders believe this. A cultural shift needs to start at the top, in both the private and public sector. If the Vice Chancellor, the IT leaders and the board are prioritising security, the internal culture will soon filter down so that everyone understands the severity of the threat and their role in mitigating risk.

2 Create a security conscious culture

Although technical sophistication is essential in protecting universities against cyber attacks, the tools alone, unsupported by users, are not sufficient. Creating a security-conscious culture, where everyone in the organisation is aware of the risk and knows their role in protecting this information, is vital.

While universities need to be open and collaborative, this can go too far, leading students and staff to be too lax about their security processes. Make sure all students and employees are informed of the practical steps that they should be taking to keep data safe. This may involve campus-wide awareness campaigns and specific training sessions for some.

3 Think more like a business

Universities need to be aware of the value of their own research in the same way that businesses understand the importance of customer data to their success. They must shed outdated practices and processes and keep pace with the rate of innovation to maintain a competitive edge in their own right. Talal Rajab, techUK, recommends learning from the finance industry's rigorous approach:

"Due to the nature of their transactions, the financial services industry is a natural target for criminality and constantly under enormous strain from attack and network infiltration. To counteract this, many have begun introducing 'information sharing sessions' for employees in-branch and in the back office. The focus is on sharing knowledge on cyber attacks and fraud in order to promote a stronger culture of data protection and online security awareness."

[7] The cyber-chasm: How the disconnect between the C-suite and security endangers the enterprise, 2016

4 Open yet secure

Managing security profiles is not easy given the unique nature of universities and achieving the balance of enhancing learning while protecting data is an added challenge. However, it is important to control user profiles for confining access to highly sensitive information and so security profiles should be aligned to individuals' needs. For instance, a researcher's profile may give them access to certain servers, applications and data, but not everything. They may also be limited in how they can share this data whether this be over email, or accessing it on certain devices, for example. This will require an adaptive and responsive IT infrastructure.

5 Implement an architecture that aligns to the cloud

Universities are now increasingly moving towards cloud computing to deliver applications to students, staff and research teams. Whilst this brings tremendous flexibility, mobile working and can reduce costs, it also adds to the complexity minefield that universities now need to navigate when managing security. According to VMware's CEO Pat Gelsinger, a typical business application - whether this is research, academic or financial - connect to seven different clouds. Add in the explosion in the number of devices and the interdependency of all of these services and network elements, and it's no surprise that security has become so complex.

The biggest challenge is ensuring that universities can bridge all of this together, including all of the different security policies and innovations. Virtualization of the underlying infrastructure provides this much needed layer between the physical infrastructure below and the applications above, enabling a ubiquitous layer that cuts across compute, network, storage, and even clouds.

6 Protect within the perimeter

Data centres typically take a perimeter-centric approach to network security strategy. This means once a threat enters the network, it has free rein to move between applications, accessing all kinds of data. Micro-segmentation in a virtual data centre is different; it shrink-wraps security around each workload, enforcing firewall rules at the level of each Virtual Machine.

"Universities need to be able to automate, organise and secure data to the level of confidentiality the ethic committee or research facility requires. That is where network virtualization tools - such as VMware's NSX - are invaluable. It enables teams to effectively lock down data by type, subject and product level to ensure maximum confidentiality and confidence for both the university and researcher."

Paul Hopkins, UK HE-Shared Services

Conclusion

As the threat of cyber attacks continues to rise across the higher education sector, the role of the IT department has never been more important in protecting growth and reputation. IT leaders need to collaborate closely with the rest of the university board to ensure protection against hacking, cyber theft and espionage. Through the automation, organisation and securing of data, alongside the creation of a security-conscious culture, universities can ensure maximum confidentiality and confidence.

This holistic approach will protect valuable research data, without obstructing the open, collaborative culture that is so important to the UK's continued academic and economic success. It is only with conscious effort that we will start to see the number of successful cyber attacks on our universities diminish.

About VMware

VMware is a global leader in cloud infrastructure and business mobility. Built on VMware's industry-leading virtualization technology, our solutions deliver a brave new model of IT that is fluid, instant and more secure. Customers can innovate faster by rapidly developing, automatically delivering and more safely consuming any application. With 2015 revenues of $6.6 billion, VMware has more than 500,000 customers and 75,000 partners. The company is headquartered in Silicon Valley with offices throughout the world and can be found online at www.vmware.com.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com