REDSCAN™

A Redscan report

The state of cyber security across UK universities

An analysis of Freedom of Information requests

Published: July 2020


CYBER
SECURITY
EXCELLENCE
AWARDS
WINNER
2020


teiss
Awards2020
WINNER


2019
Computing
Security
Awards
WINNER


SC 2020 awards
highly
commended


2018
Computing
Security
Awards
WINNER


SC 2019 awards
EUROPE
Highly Commended


2017
Computing
Security
Awards
WINNER


Cyber Security Awards
Winner 2019

TABLE OF CONTENTS

AIMS

As universities play a key role in training and research in the UK, the aim of Redscan's FOI request was to gain an insight into the actions they are taking to manage and mitigate cyber security risks. Because data is a particularly valuable asset to universities, a key focus for the request was to understand how they are protecting it.

METHODOLOGY

FOI requests were made to 134 universities in the UK, of which 86 responded. While the timescale for a FOI response is normally 20 working days, this was relaxed by the Information Commissioner's Office (ICO) due to the COVID-19 pandemic, meaning that many responses took longer to obtain.

KEY INDUSTRY FACTS

2.38m

students

in UK higher education institutions in 2018–19

(Source: HESA 2018–19)

430k

staff

employed by UK higher education institutions in 2018–19

(Source: HESA 2018–19)

65%

of students

say that they would be less likely to apply to a university with a reputation for poor cyber security

(Source: HEPI 2019)

£87

billion

value of leading research-focused universities to UK economy

(Source: Russell Group 2017)

WHAT IS THE VALUE OF CYBER SECURITY TO UNIVERSITIES?

“Universities are key contributors to the economy, skills development and innovation in the UK. In doing so, they handle personal and research data, intellectual property and other assets, each of which has significant value to others.”

The National Cyber Security Centre (NCSC)

UK universities are pioneers of world-leading research and hold large volumes of intellectual property and student data. This valuable information makes them an attractive target for financially-motivated cybercriminals, as well as nation states that want to gain an advantage over their international rivals.

The impact of failing to address key security vulnerabilities could be disastrous. State-sponsored espionage has the potential to inflict long-term damage on UK universities by deterring funding for research and damaging public perception.

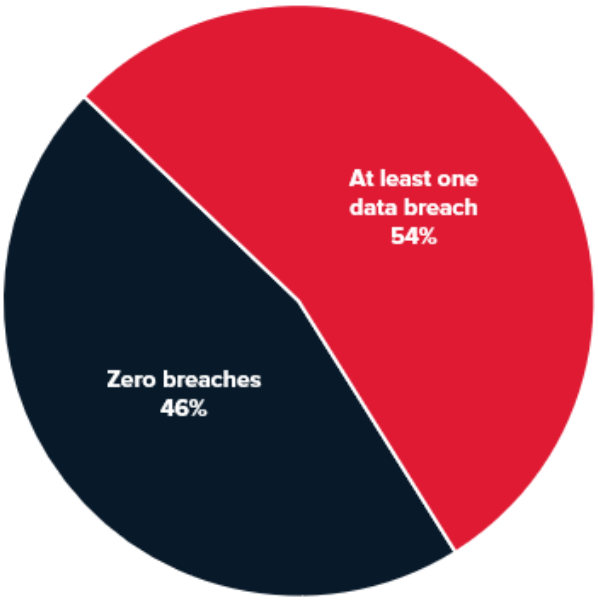
The COVID-19 pandemic has created serious problems for the sector, with research by the Institute for Fiscal Studies suggesting that as many as 13 UK universities could face financial disaster. With so many challenges, it is vital that universities effectively manage resources while mitigating the current and emerging risks of cybercrime.

THE RESULTS

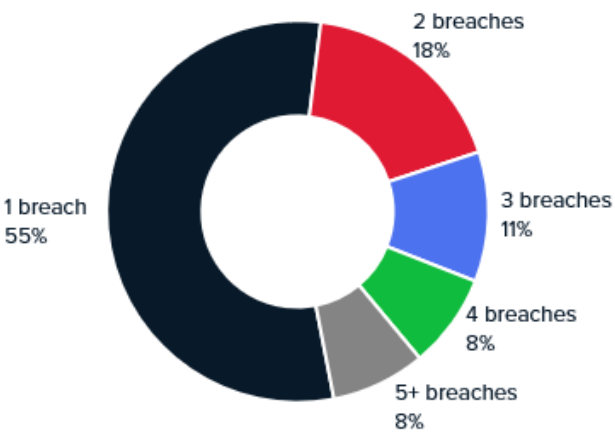
DATA BREACHES

To gain an insight into the challenges organisations face in protecting the sensitive data and assets they hold, we asked universities about the data breaches they have experienced. The response revealed that 54% of universities have reported a data breach to the ICO in last 12 months*, with an average of two reports per university. Two universities reported six breaches each. The second chart below shows the spread of the volume of data breaches experienced by universities.

Percentage of universities that reported a data breach to ICO in the last year



Breakdown of universities that submitted a report to the ICO



*It should be noted that data breaches reported do not relate solely to cyber incidents.

What we say

"The fact that more than half of the universities surveyed reported a data breach to the ICO this year simply underscores the scale of the challenge universities face protecting data.

"These figures only include the data breaches that universities are aware of. Without the appropriate controls and procedures in place, identifying a breach can be like finding a needle in a haystack. Attacks are getting more and more sophisticated and, in some cases, universities will be unaware they've been compromised."

Mark Nicholls, Redscan CTO

PHISHING ATTACKS

According to our FOI analysis, several universities received millions of spam and phishing emails each year, with one institution reporting a high of 130 million. Phishing and spam were described as being “endless” by one university, with another reporting that the volume of attempts had increased by 50% since 2019.

What we say

“Phishing is a problem for all organisations and the results of our latest FOI request reflect this. In the light of COVID-19 and the rise of remote working for staff and students, it is more important than ever that universities take an active stance towards this threat.”

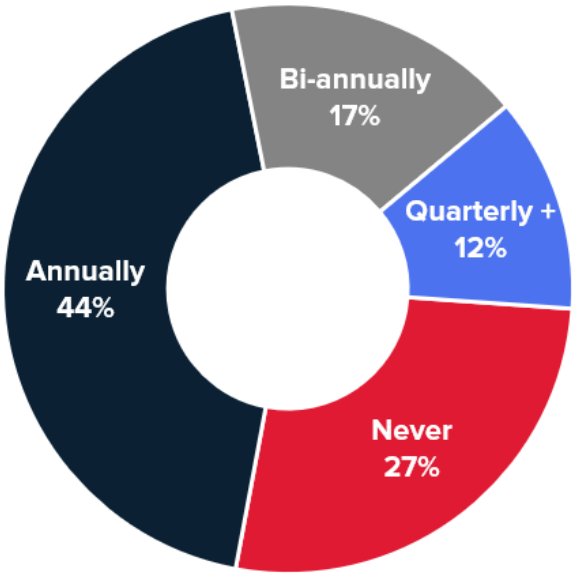
Mark Nicholls, Redscan CTO

PENETRATION TESTING

Regular penetration testing is vital in helping organisations identify areas of their security which need to be improved. Testing is especially important for universities because they have large IT estates, a high number of users, and lots of specialist equipment. However, our FOI analysis reveals that a quarter of universities have not commissioned a pen test from a third-party provider in the last year.

Of those universities that commissioned pen testing from a third-party, the average number of tests was almost three per university. Only 29% of universities commissioned more than one third-party penetration test.

How often third-party penetration tests are undertaken by UK universities



What we say

"The number of universities that didn't conduct a pen test in the last 12 months is surprisingly high. Universities hold a lot of sensitive data and without regular security testing it's impossible to know whether existing controls in place are effective at protecting it. Penetration testing ensures universities can better understand and mitigate the threats to their security and demonstrate compliance with the GDPR and PCI DSS."

Mark Nicholls, Redscan CTO

QUALIFIED SECURITY PROFESSIONALS

The FOI found that universities employ, on average, three qualified cyber security professionals. A cyber security professional is defined as any member of staff with a recognised cyber security or data security qualification.

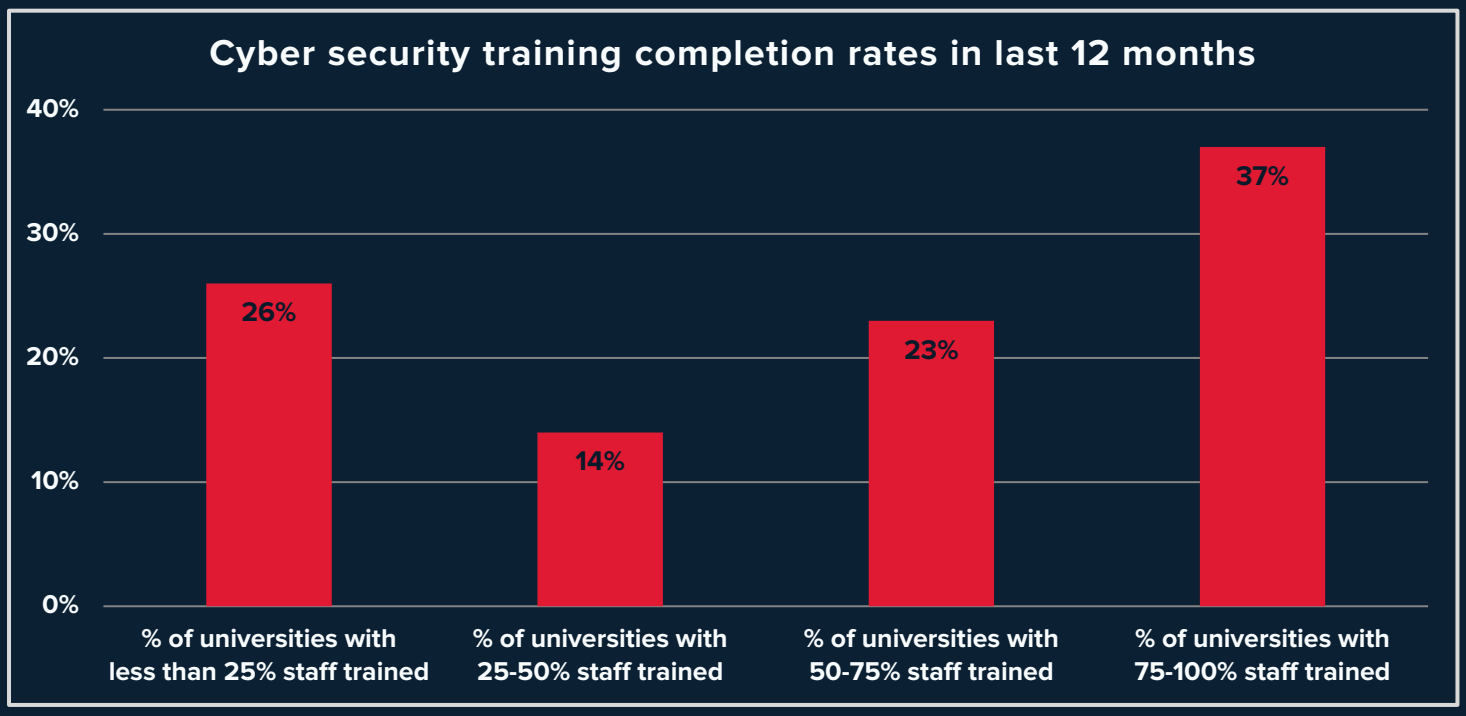
What we say

"Cyber security demands specialist expertise and knowledge of the latest and emerging threats. Universities need to have a strategy for ensuring key cyber security roles are staffed with appropriately skilled individuals. Given the global shortage of cyber security professionals, organisations should consider upskilling existing staff in other IT roles and outsourcing requirements."

Mark Nicholls, Redscan CTO

EMPLOYEE TRAINING

Training is key to building cyber security into any organisation's culture, but our FOI analysis suggests that it is not being delivered by universities as a matter of course. The figures reveal a significant disparity amongst universities. The chart below shows the uneven spread of cyber security training completed across UK universities.



Nationwide, only 54% of university staff have received security training. One Russell Group university has trained just 12% of its staff in cyber security.

The FOI request also reveals that universities spend an average of just £7,529 per year on security training for staff, with investment ranging from £0 to £49,000.

What we say

"Employees are crucial in helping to defend organisations against the latest security threats. It is vital that universities provide regular staff training and ongoing support. Universities must also ensure that awareness programmes are constantly updated to reflect the latest threats and phishing lures."

Mark Nicholls, Redscan CTO

STUDENT TRAINING

The figures for student awareness and training varied in a similar way to those for staff training. 51% of universities proactively issue security training and information to students while 37% only offer reactive support to students who request it. 12% of universities do not offer any kind of security guidance, support or training to their students.

What we say

"It is positive to note that over half of the universities surveyed are proactively educating their students about cyber threats by running workshops and making intranet announcements. Students are commonly targeted by phishing campaigns and need to be alert to the risks. With remote learning on the increase due to the COVID-19 pandemic, providing effective training and support is more important than ever."

Mark Nicholls, Redscan CTO

CYBER ESSENTIALS

Cyber Essentials is a government scheme backed by the NCSC (National Cyber Security Centre). It is designed to help organisations demonstrate their commitment to cyber security and sets out five basic security controls to protect them from around 80% of common cyber-attacks.

Our research found that 66 out of the 134 universities have Cyber Essentials certification. Of these, 21 have Cyber Essentials Plus.

What we say

"Good cyber hygiene is essential to reduce the potential for cyber-attacks and data breaches. Adhering to approved and high-quality accreditation schemes like Cyber Essentials is vital for helping to instil good practices such as patching and access management.

Mark Nicholls, Redscan CTO

THE UNIVERSITIES LEADING THE WAY

We wanted to highlight just a few of the best responses from the universities who are leading the way in educating their staff and students to improve their cyber security measures:

"The university routinely communicates cyber threat information to whole staff and student communities. This is a mixture of general awareness topics such as phishing or secure your device, and specific awareness about current threats, such as COVID scams."

"We provide information to students about cyber security as a part of the digital capabilities certificate that is available to all students via our virtual learning environment. We also provide face-to-face workshop sessions at induction for our students that include components of cyber security."

"The University runs a Cyber Security Week annually to coincide with the start of the academic year."

"Aside from the online advice and resources offered via the IT Services website, we offer awareness campaigns tailored to students - the usual posters and flyers, as well as in person advice at welcome events and the Student Laptop clinic, not to mention via the Service Desk or enquiries answered directly via a specific mailbox."

LOOKING AHEAD

Universities are under significant financial pressure, particularly given the impact of COVID-19. However, it is important they maintain a clear focus on cyber security and identify ways to assure the security and safety of their data and that of their students. The financial and reputational damage of failing to do so is too great.

Our FOI analysis highlighted that, while the majority of universities are addressing some of the issues, there is much more to be done across the sector to improve core cyber hygiene and data protection.

What we say

"UK universities are among the most well-respected learning and research centres globally, yet our analysis highlights inconsistencies in the approach institutions are taking to protect their staff, students and intellectual property against the latest cyber threats.

"The fact that such a significant number of universities don't deliver cyber security training to staff and students or commission independent penetration testing is concerning. These are foundational elements of every security programme and key to helping prevent data breaches.

"Even at this time of intense financial pressure, institutions must ensure that their cyber security teams receive the support they need to defend against sophisticated adversaries. Breaches have the potential to seriously impact organisations' reputation and funding.

"The threat posed to universities by nation state attackers makes the need for improvements even more critical. The cost of failing to protect scientific research is immeasurable."

Mark Nicholls, Redscan CTO

ABOUT REDSCAN

Redscan is an award-winning provider of managed security services, specialising in threat detection and integrated response.

Possessing a deep knowledge of offensive security, Redscan's experts are among the most qualified in the industry, working as an extension of clients' in-house resources to expose and address vulnerabilities plus swiftly identify and shut down breaches. Services offered include CREST-accredited Penetration Testing, Red Teaming and Managed Detection & Response.

By understanding how attackers operate, leveraging cutting-edge threat intelligence, and offering highly acclaimed services, Redscan's cyber security professionals can be trusted to provide the insight and support needed to successfully mitigate information security risk and achieve compliance standards.

Call us
0800 107 6098

Email us
info@redscan.com

Twitter
@Redscan

LinkedIn
/Redscan

Company number 09786838
Version 1-0-0720