KnowBe4
Human error. Conquered.

United Kingdom: "Exponential" Growth In Cyber Attacks Against Higher Education Institutions

United Kingdom: "Exponential" Growth In Cyber Attacks Against Higher Education Institutions

Table of Contents

INTRODUCTION

World-ranked universities and a strong, diverse higher education system are enduring parts of the British identity, and well-deserved sources of pride for the country. The international renown of its universities, however, and the vital base the British university research system provides for global innovation, make the country's higher education system a particularly attractive target for threat actors hoping to exploit its value.

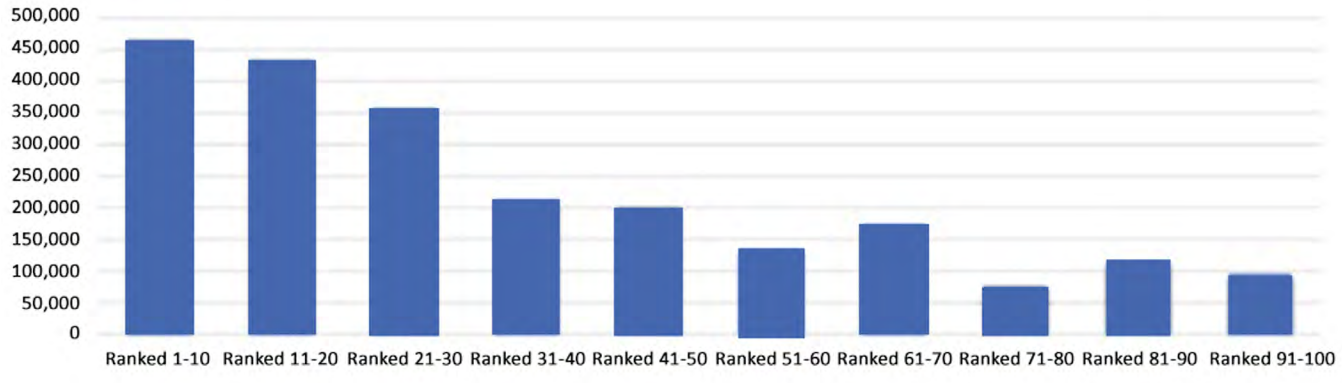
British universities are commonly affiliated with notable international research institutes, making the data that can be stolen through a cyberattack far more valuable than the phone numbers and credit card numbers they may get elsewhere. In a dramatic example, Oxford University houses one of the most advanced biology labs in the world. While the lab was studying Covid-19 its system was attacked. In February 2021, Forbes magazine reported that the hackers who had executed the attack were selling access to the lab's equipment – which could be used for the theft of data or sabotage – on the dark web.[1]

Attracting some of the world's brightest minds is both a source of national pride and a vulnerability; with a new influx of students each year, arriving students may initially be unfamiliar with UK culture and customs, making them particularly susceptible to social engineering attacks.

According to Oxford University Press's *Journal of Cybersecurity* (September 2023) the National Cyber Security Centre (NCSC) noted in 2021 that the Higher Education sector in the United Kingdom had been "exponentially" targeted by cyber-criminals.[2] The report also noted a PwC UK report that reviewed 22 Higher Education Institutions (HEIs) and found that cybersecurity and information governance was the top reported risks in the sector.

In September 2023, Crossword Cybersecurity discovered 2.2 million breached credentials available on the dark web for the top 100 UK institutions, with 57% belonging to the Russell Group Universities, the group of prestigious, research-intensive universities that includes University of Oxford and University of Cambridge. London universities have more breached credentials (506,330) than Scotland, Wales and Northern Ireland combined (465,767). Of those, 54% of the breached credentials came from UK universities with research facilities.[3]

BREACHED CREDENTIALS AT UK UNIVERSITIES BASED ON THEIR RANKING:

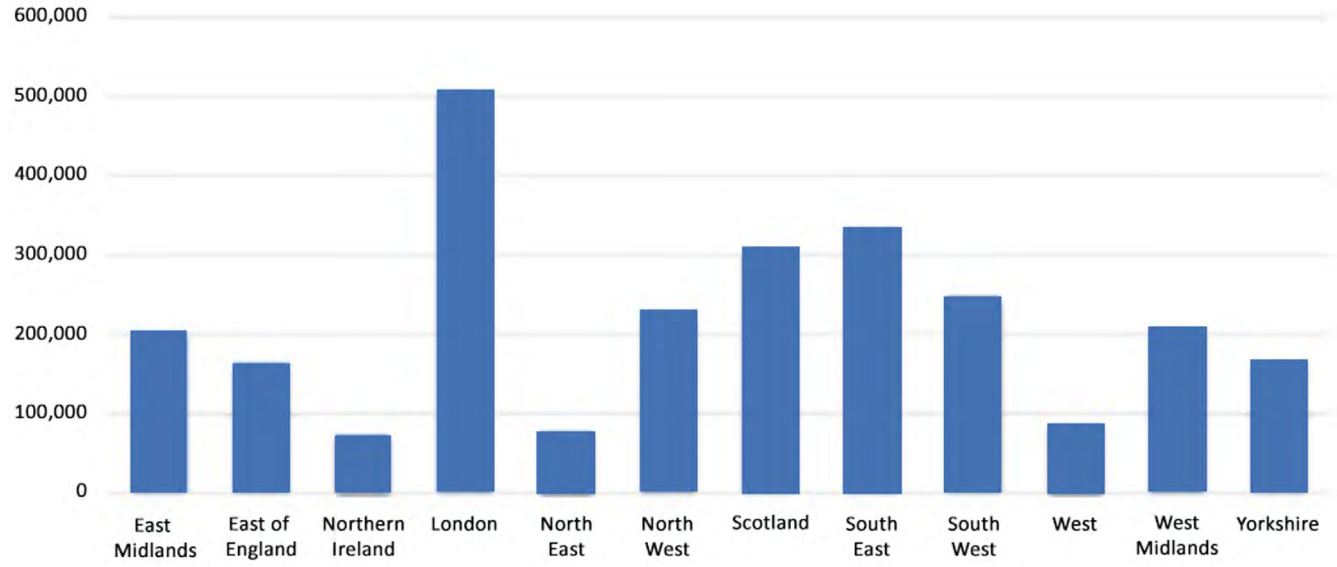


1 https://securityaffairs.com/115044/hacking/oxford-university-lab-hacked.html

2 https://academic.oup.com/cybersecurity/article/9/1/tyad019/7281495

3 https://www.infosecurity-magazine.com/news/millions-uk-university-credentials/

CREDENTIAL BREACHES IN UK UNIVERSITIES BASED ON REGION[4]



The most alarming ramifications of infiltration into the university systems may not be immediately felt. A breach at Australian National University in 2018 was a wakeup call to top universities globally. The breach, which resulted in "significant amounts of personal details dating back 19 years," was only revealed in 2019. According to the school's vice-chancellor, "Depending on the information you have provided to the university, this may include names, addresses, dates of birth, phone numbers, personal email addresses and emergency contact details, tax file numbers, payroll information, bank account details, and passport details. Student academic records were also accessed."[5]

Cyber security expert Tom Uren, a senior analyst at the Australian Strategic Policy Institute, said it was too early to say who was behind the 2018 attack but suggested China was the most likely culprit.

"They have a history of stealing large data sets and the theory is that they're putting these together to try and build a picture of people of interest to use for either counter-intelligence or intelligence purposes," he said.

"I've also heard the theory that the Chinese are interested in foreign universities because they've got a large number of overseas students ... and universities are traditionally a hotbed of radicalism and that's a concern for the Chinese state."

Universities were good places to keep track of people's histories, he said.

"I imagine quite a few university students from ANU end up in federal government. "Inevitably some of them will become important people down the track."

4 https://7723487.fs1.hubspotusercontent-na1.net/hubfs/7723487/Trillion-report-threat-briefingV2.pdf

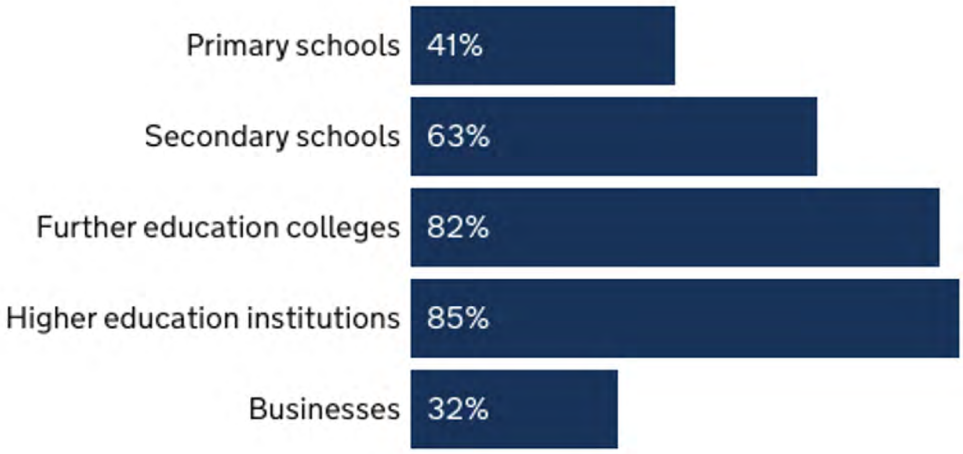
5 https://www.abc.net.au/news/2019-06-04/anu-data-hack-bank-records-personal-information/11176788

HIGHER EDUCATION IS A MORE ATTRACTIVE TARGET THAN BUSINESS

In April 2023, a survey of 52 higher education providers conducted by the Department for Science, Innovation and Technology (DSIT)[6] showed that all types of education institutions were more likely to have suffered a cyber security breach or attack than the average UK business. 85% of higher education institutions surveyed had identified breaches or attacks within the past 12 months, compared with just 32% of businesses reporting attacks in the same period. Further education and higher education institutions experienced more breaches and attacks than schools, and experienced a wider range of attack types, including impersonation, viruses, and other malware.

Of the 44 HEIs that identified breaches, half reported experiencing attacks at least weekly. All reported phishing attacks, 86 percent suffered impersonation breaches, and 64 percent faced viruses, spyware or malware.

Percentage of organisations that have identified breaches or attacks in the last 12 months:



Bases: 241 primary schools; 217 secondary schools; 44 further education colleges; 52 higher education institutions; 2,263 UK businesses[7]

The reported types of breaches were similar to those of UK businesses. Phishing attacks are by far the most common type of breach, followed by online impersonation, then viruses, spyware, or malware.

The impact of the attacks was more severe in higher education than schools, resulting in lost money or data, or having accounts compromised for illicit purposes.

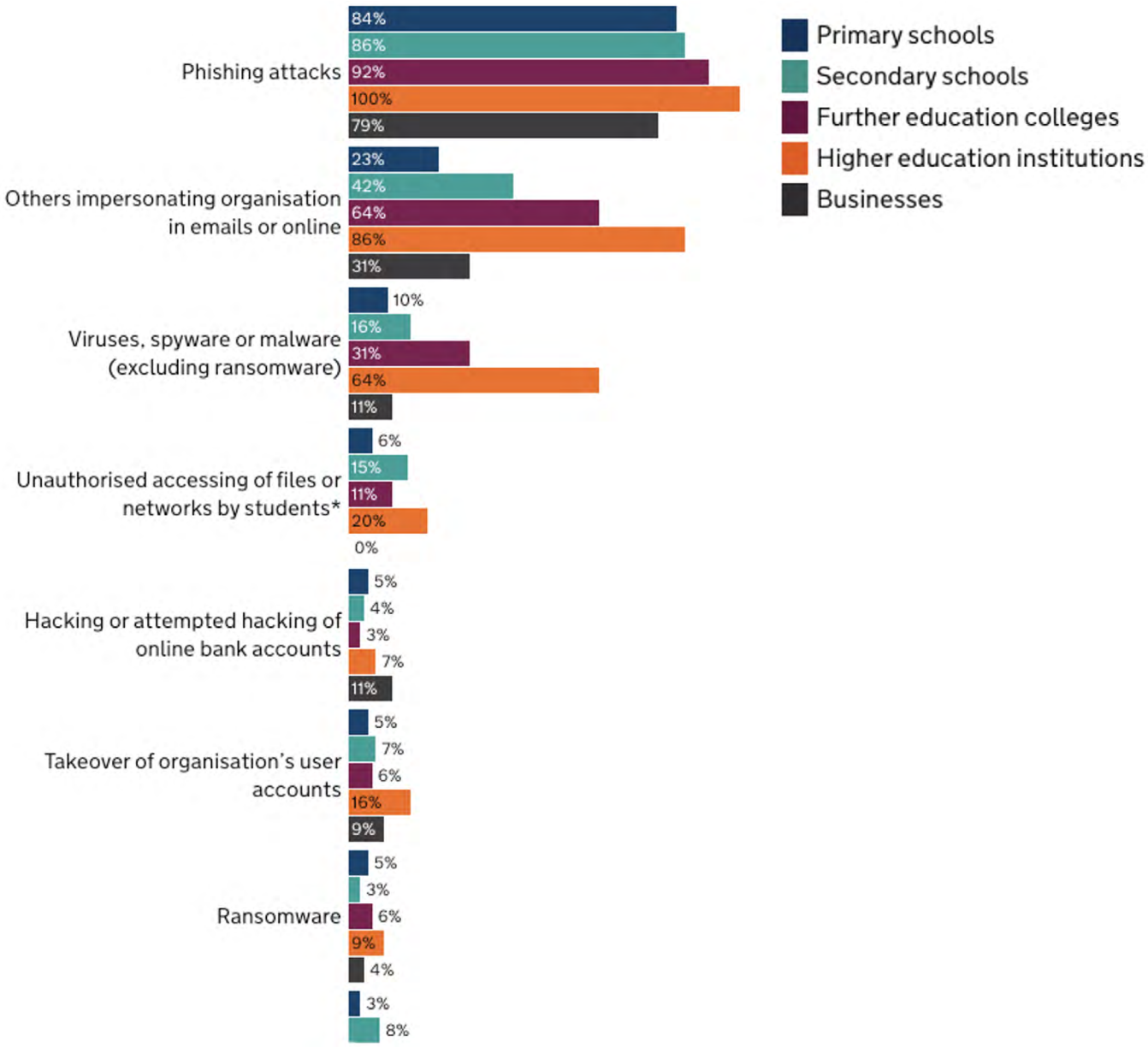
6 https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023-education-institutions-annex

7 https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023-education-institutions-annex

HALF OF HIGHER EDUCATION INSTITUTIONS ARE UNPREPARED FOR AN ATTACK

According to the survey only half of further and higher education institutions have a cyber security strategy, far behind the large business community, where seven in ten have a strategy. Some reported difficulty in raising their concerns with senior management.

The DSIT noted that "One higher education institution interviewee noted that their board had a manual for how to deal with major physical incidents such as fires, floods, bomb threats and pandemics, but this did not cover cyber incidents."



WHAT MAKES HIGHER EDUCATION AN ATTRACTIVE TARGET?

The higher education sector is at risk from attacks by opportunistic criminals as well as highly skilled threat actors, including those sponsored by nation states attempting to access sensitive research data.

According to Cyber Security and Universities: Managing the Risk (published by Universities UK with the National Cyber Security Centre and Jisc, (Joint Information Systems Committee), motivations of attackers targeting higher education fall into four categories: those seeking to directly extort a payment through ransomware or other methods; theft of research data / knowledge; use of universities' digital infrastructure to directly monetise assets, through bitcoin mining for example; and those seeking to disrupt and destroy. They are further attracted by the fact that universities, particularly the prestigious research-intensive institutions, have attempted to remain open and accessible in support of research and education; this openness combined with the university's size create a large attack surface of networks.[8]

Other challenges facing HEIs include high turnover in an increasingly casual workforce, and onboarding thousands of new students every year in a constricted period of time, creating challenges to the protection of high value intellectual property within an institutional culture that at times does not priorities following rules, and budgetary constraints.

A CULTURAL SHIFT

Higher Education institutions must navigate the delicate balance between remaining open for the sake of research and education, while protecting themselves against an increasingly sophisticated and varied array of cyber threats. With only half of the higher education institutes boasting a cybersecurity strategy, it's clear that enhancing cybersecurity remains not just a technological challenge, but one which needs to look at the processes and the cybersecurity culture it fosters and builds both internally and externally. An immediate and concerted action to build a strong security culture will be key to safeguarding the future of higher education in the digital age.

8 https://www.universitiesuk.ac.uk/sites/default/files/uploads/UUKi%20reports/279%20FINAL%20-%20Cyber%20Security%20and%20Universities%20(002).pdf

Additional Resources

Free Phishing Security Test
Find out what percentage of your employees are Phish-prone with your free Phishing Security Test

Free Automated Security Awareness Program
Create a customized Security Awareness Program for your organization

Free Phish Alert Button
Your employees now have a safe way to report phishing attacks with one click

Free Email Exposure Check
Find out which of your users emails are exposed before the bad guys do

Free Domain Spoof Test
Find out if hackers can spoof an email address of your own domain

About KnowBe4

KnowBe4 is the provider of the world's largest integrated security awareness training and simulated phishing platform. Realizing that the human element of security was being seriously neglected, KnowBe4 was created to help organizations manage the ongoing problem of social engineering through a comprehensive new-school awareness training approach.

This method integrates baseline testing using real-world mock attacks, engaging interactive training, continuous assessment through simulated phishing attacks and enterprise-strength reporting to build a more resilient organization with security top of mind.

Tens of thousands of organizations worldwide use KnowBe4's platform across all industries, including highly regulated fields such as finance, healthcare, energy, government and insurance to mobilize their end users as a last line of defense and enable them to make smarter security decisions.

For more information, please visit www.KnowBe4.com

KnowBe4
Human error. Conquered.

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755
Tel: 855-KNOWBE4 (566-9234) | www.KnowBe4.com | Email: Sales@KnowBe4.com

01E02K01