Appendix - additional documents

Newcastle University becomes latest ransomware victim as education sector fails to heed warnings

Luke Irwin 10th September 2020

Newcastle University is being held to ransom after its systems were infected with malware earlier this month.

The DoppelPaymer ransomware gang breached the university's systems on 4 September, and later that day stole backup files.

The university has apologised for the "ongoing" disruption and added that it would take "a number of weeks" to get its systems back online.

Staff and students can still access limited services, including email, office applications and video conference tools.

Meanwhile, the university said it is working with the ICO (Information Commissioner's Office) and the police to address the breach.

Ransomware epidemic

This incident is the latest in a long line of cyber attacks on the education sector. Only a few days earlier, nearby Northumbria University was forced to cancel exams and shut down its clearing hotline after a cyber attack.

It followed August's ransomware attack on the education administrator Blackbaud, in which students' phone numbers, donation history and events attendance were all compromised.

That breach affected more than a dozen universities in the UK, while another eight schools and colleges reported separate ransomware infections in August.

These kinds of attacks are becoming more common across all sectors, thanks to the ease with which they can be carried out and the potential for large financial rewards.

It only takes one organisation to go against expert advice and pay the ransom for the criminals to hit the jackpot. The average ransomware payment is about £33,000, which organisations could easily justify, but it will fuel the attacker and could help fund future, more sophisticated attacks.

Universities are especially vulnerable to ransomware, because there are severe knock-on effects if disruption lingers.

Unlike private-sector organisations, universities face risks beyond the loss of production and revenue. For example, students' classes and potentially their exams could be disrupted, which

could in turn affect their ability to submit essays or even to graduate.

Cyber criminals appear to have spotted this vulnerability in the education sector and may well exploit it in the same way that they did with the US local government sector.

There were 22 attacks on city and state governments in 2019, eventually forcing the US Conference of Mayors to instruct elected officials not to pay any more ransoms.

Universities could end up reaching a similar conclusion, but they would be better off addressing the root cause of the problem. A recent report found that many universities neglect basic cyber security best practices.

For example, 46% of university staff haven't received staff awareness training in the past year, and universities spend just £7,529 a year on average educating their employees.

Meanwhile, only 51% of universities proactively provide security training to students – although a further 37% said they provided resources to students who requested it.

Cyber Security as a Service

Most organisations are probably aware that they should be doing more to tackle the threat of cyber crime. The problem is knowing where to begin, and that's where our Cyber Security as a Service can help.

With this annual subscription service, our experts are on hand seven to advise you on the best way to protect your organisation.

- Penetration Testing
- Phishing
- Podcast
- Privacy
  - Breaches and Hacks
  - Data Protection
- Project Management
- Ransomware
- Sectors
  - Education
  - Financial Services
  - Healthcare
  - Professional Services
  - Public Sector
  - Retail
- Staff Awareness
- Training
- Uncategorised

they'll guide you through vulnerability scans, staff training and the creation of policies and procedures, which form the backbone of an effective security strategy.

About The Author

Luke Irwin

Luke Irwin is a writer for IT Governance. He has a master's degree in Critical Theory and Cultural Studies, specialising in aesthetics and technology.

No Responses

← **Tweet**

DoppelPaymer
@DoppelPaymer

Dear students of the New Castle University Congratulations with an upcoming release of your personal data. What a great start of a new educational year #doppelpaymer #ransomware #malware #doppleleaks

4:58 PM · Sep 7, 2020

8 Retweets **13** Quote Tweets **15** Likes