nature

Research institutions must share knowledge of cyberattacks

Ransomware attacks that have debilitated the British Library in London and Berlin's natural history museum shows how vulnerable research institutions are to this kind of crime.

It has been more than three months since the British Library's staff and users awoke to the news that its computer systems had been hijacked. After the attack on 28 October, anything that used the Internet – the library's phone systems, its digital collections and website – became inaccessible. A hacking group called Rhysida had demanded a ransom, which the London-based library refused to pay. In November, Rhysida listed around half a million confidential files, including names and e-mail addresses of the library's staff and users, for auction on the dark web, with bids starting at 20 bitcoins (US$800,000).

Berlin's natural history museum was also attacked in mid-October. In-person visits are continuing, but research is possible only "to a limited extent". These attacks are not isolated cases. In one study, researchers analysed 58 cyberattacks between 1988 and 2022 on universities, schools and other organizations worldwide, and found that the frequency of attacks had increased since 2015 (H. Singh Lallie *et al.* Preprint at https://arxiv.org/abs/2307.07755; 2023). Information on the attacks was gleaned from publicly available online sources, such as media reports and the institutions' own websites. The scientists concluded that research and education data are "a prime target for cyber criminals". The study suggests that ransomware attacks – which permanently block access to data or systems until money is paid – were the most common form of cyberattack from an external source. Within an institution, students hacking the system to alter their grades were most often the cause.

The vulnerability of educational and research institutions is not difficult to predict. All around the world, millions of members of staff, students and alumni log into institutional computer systems daily. Moreover, since the COVID-19 pandemic, remote access from personal devices with varying levels of protection has increased massively. Some of the biggest security risks come from the use of weak passwords and computer systems that can be accessed without multi-factor authentication – in which users verify their identity through two or more independent pieces of evidence. According to an annual survey by US technology giant IBM on data breaches, only four in ten organizations, including those in research and education, require users of computer systems to verify their identities regularly with such authentication methods (see bit.ly/4bfzamz).

> "Collaboration between researchers who study computer security and those who investigate crime will bring wider benefits."

Research institutions are generally not short of information technology expertise – the British Library, for example, houses the UK national research centre for artificial intelligence and data science, the Alan Turing Institute. Yet there is a lack of in-depth, publicly available research on the extent and range of cyberattacks against educational institutions. Not all those that are attacked go public with details – the British Library did not reveal the attack was an instance of ransomware until 29 November. In many countries, organizations are required to report attacks to the relevant authorities, but governments, for understandable reasons, often do not publish this information.

Some in national security circles consider such research, and the public scrutiny associated with it, a risk for producing or increasing vulnerabilities. However, collaboration between researchers who study computer security and those who investigate crime will bring wider benefits. It could help institutions to protect themselves against future attacks, and enable organizations to handle an attack effectively and minimize damage. Sharing knowledge on how to react to a ransom demand is one example. Institutions that are subject to ransomware attacks are advised not to pay, although some have done so. Everyone would benefit if these experiences were studied, peer reviewed and published in the open literature.

Another important question is who should pay to recover and strengthen computer systems that are protecting national assets. In the case of the British Library, three months after the attack, some collections are available for people who visit in person, but it could be months more before its online records of books, journals, PhD theses and rare manuscripts are fully accessible to the library's users all over the world. The organization also needs to find in the region of £6 million ($7.5 million) to £7 million from its own resources to repair the damage.

So far, the UK government has not said whether it will underwrite the costs – a position that has left other librarians perplexed. The British Library is the United Kingdom's national library. It is important to the nation's businesses, colleges, research centres, schools and universities, and even more so to all those who do independent research. Library users are experiencing continued delays in a range of lending services, from ordering copies of books published over a span of more than three centuries, to accessing journal articles. The institution has one of the world's largest collections of maps, along with archives of sound recordings and every UK PhD thesis published over the past century. By not contributing to the repairs, the government is disadvantaging researchers who cannot access other institutional libraries.

This is not just a matter for the UK government, but for national and regional governments worldwide. Relevant authorities need to step up to support important institutions in times of crisis. And funders and researchers should consider how they can help – for example, by studying how to minimize the risk of cyberattacks happening in the future and what to do when they do take place.