Legal Information Management, 24 (2024), pp. 84–87

doi:10.1017/S1472669624000215

The British Library Cyber-Attack and Implications for Law Libraries: Some Initial Thoughts

Abstract: In the following article **Dunstan Speight** offers a few initial thoughts on the implications for law libraries of the October 2023 cyber-attack on the British Library. While the remarks apply particularly to larger institutional libraries (such as those of professional bodies like the Inns of Court) there are lessons to be learnt for all types of library and information service.
Keywords: British Library; cyber-attack

On 28 October 2023, the British Library was subject to a very serious ransomware attack on its IT infrastructure. The effects of the attack were catastrophic for the library, its staff and its readers as virtually all its operations and data were compromised. Ransomware attacks on organisations and businesses are frequently reported in the media but tend to be short-lived stories – the conclusion usually drawn is that the victim has capitulated to the financial demands of the attacker or found some means to circumvent the effects of the attack. In November, for instance, the press reported that Magic Circle firm Allen & Overy LLP had suffered a cyber-attack and threats to release confidential information were published by Russian hacking group LockBit. The removal of this published threat later in the month led to speculation that the firm had paid a ransom – a conjecture that was neither confirmed nor denied.[1]

The British Library attack was in a very different league and offers a number of lessons from which all institutions could profit. The October attack and its consequences will have had a very limited impact on most law libraries – although those with special collections have experienced higher than usual requests for access to materials usually available via the British Library. The episode should, however, act as something of a wake-up call and provide lessons to be learnt.

The scale of the attack and its repercussions show that worst-case scenarios can happen in real life, so it reinforces the message about the importance of cybersecurity. The fact that the British Library is an institution of world-class significance also means that the effects of the attack were more visible than most such attacks. As a public body, the British Library did not have the option of paying the ransom demands, which meant that it has had to live with the consequences of the attack when private organisations might have chosen to buy off the attackers and return to business as usual. Thus we have seen the implications of this cyber-attack played out in great detail. The attack and its effects have garnered more press interest than most as the British Library is a national institution. The library also recognised a responsibility to investigate the causes of the attack and make these findings public. Its initial report was published on 8 March[2] and further updates will surely follow. The scale, longevity and publicity of this episode combine to make it particularly worthy of study.

The initial effects of the attack were dramatic. The library's catalogues and other bibliographical sources became unavailable; material held by the library (whether in print or e-book form) was inaccessible and the gang threatened to release sensitive financial and other data relating to customers, staff and former members of staff.

The library catalogue was not available between the date of the attack and 15 January, when a reduced version of the original catalogue was made available. The full catalogue, available before the attack, is still not available at the time of writing (April 2024). Various ancillary resources also remain unavailable – most notably the English Short-Title Catalogue (ESTC), although the full data for pre-1700 books is available on a temporary website.

As the country's largest library with collections spread across multiple sites, the British Library relied on its systems to sign out books from the store to the reading rooms and track each volume. As a result of the attack, this too was rendered inoperable and books could not be taken from the stores. When the library reopened to readers in the late autumn, they were only able to use the very small proportion of its holdings which were on the open shelves in the reading rooms. E-books did not come to the rescue on this occasion, as although the British Library is entitled to a free copy of every book published electronically under legal deposit rules, access to these was also lost as a result of the attack.

The British Library was the victim of a serious ransomware attack on its IT infrastructure in October of last year

The third major element of the cyber-attack – the threat to sell confidential personal and financial data to criminals via the dark web – is a familiar feature of many such attacks. In the case of the British Library the consequences were potentially severe because of the scale of the organisation and the number of its readers, customers, staff and former staff (whose records were also affected).

The library's interim report provides an analysis of the specific circumstances which made the attack successful and lessons of wider application. There was a 'perfect storm' of circumstances which made the library vulnerable. It had seen an increase in remote access to its servers with the move to greater working from home and more involvement by third parties in its activities. The suspicion is that a phishing attack compromised someone's account credentials and created the hackers' entry to the systems.

A failure to prioritise the move from local to cloud-based storage meant that the hackers were able to wreak extensive damage. A complex mix of legacy IT systems at the library and the impossibility of restoring a number of key databases for which the relevant technology is no longer supported by suppliers has impeded the restoration of services. The library had achieved accreditation to Cyber Essentials Plus in 2019 but it ceased to be compliant in 2022 when the standard was upgraded. It was working to replace a number of obsolete systems to regain compliance at the time of the attack.

The importance of eliminating legacy technology is one of the 16 key lessons from the attack identified in the report.[3] Although the precise circumstances of the British Library in October last year are unlikely to be replicated elsewhere, these lessons will be relevant to most organisations. As such, the document is well worth reading and forwarding to those in your organisation responsible for cybersecurity – even if you are in the fortunate position of being confident in your organisation's IT strategy (a confidence which was clearly misplaced at the British Library).

IMPLICATIONS FOR LAW LIBRARIES AND THEIR ORGANISATIONS

Legal information services and the organisations they serve differ to a very great degree, encompassing small law firms, major international partnerships, barristers' chambers, professional bodies and academic institutions. Some legal information professionals may have some influence on issues of IT security, although many will be entirely dependent on the infrastructure provided by the wider organisation. This does not, however, mean that the profession should shrug its shoulders and heave a sigh of relief that the issue of IT security is someone else's concern.

THE UNTHINKABLE CAN HAPPEN

This may sound trite, but the British Library attack does demonstrate the reality of the threat of cyber-attacks. The fact that, as a public body, the British Library was not in a position to buy off the attackers has provided a very clear demonstration of the potential of cyber-attacks to disrupt business and the fact that it can happen.

Disaster planning can often seem divorced from reality until something of the magnitude of the British Library attack happens. In early October 2023 had anyone said "can you conceive of a situation where the country's biggest library is completely incapacitated for months?" one would have said "theoretically, yes; realistically, probably not". People reading the British Library's report on the incident may well feel smug and point to the various weaknesses in the British Library's IT infrastructure which unwittingly facilitated the attack and think that their organisation would not make the same mistakes. Had you asked a British Library employee on 22 October about the likelihood of their operations being incapacitated by a cyber-attack, I imagine most would have replied that they had rigorous systems in place to guard against this.

PRIVACY AND DATA PROTECTION

Privacy and data protection are usually the main concerns in the event of a cyber-attack and the most newsworthy aspect. It was also the prime motivation for the British Library attack where documents from the Finance and

https://doi.org/10.1017/S1472669624000215 Published online by Cambridge University Press

HR departments were stolen *en masse* and this was complemented by a wider search for documents which included words such as 'confidential' or 'passport' in their title.[4] (An obvious lesson for organisations is to change their document naming conventions).

Legal institutions, law firms and barristers' chambers are particularly tempting targets for hackers as the nature of their work frequently involves the evaluation and analysis of personal and commercially sensitive data. This is likely to be a factor behind the 36% increase in breaches of data security reported by law firms to the Information Commissioner's Office in the period 2022-23, compared with 2021-22.[5] Clients reasonably expect that their information will be held securely and there are significant penalties if their security is breached: fines of up to £17.5m or 4% of annual worldwide turnover, whichever is higher. The British Library attack involved a massive breach of personal data of staff and users. When it became obvious that it would not pay the ransom, the data was published on the dark web.

DESTRUCTION OF IT INFRASTRUCTURE

The data protection aspect of the attack was not, however, the most serious consequence for the British Library, because the modus operandi of the attackers involved destroying servers to impede detection of the breach and delay recovery from it. Although hackers are most likely to be interested in obtaining confidential information, rather than having a particular interest in frustrating academic research, there may be significant additional damage from any attack.

This incidental damage was particularly acute in the case of the British Library as so many resources were stored on local servers. The British Library report is clear that had it migrated more content and resources to the cloud it would have been less vulnerable to attack but notes that cloud storage is itself not immune from attack and still bears its own security risks.

A complicated mixture of old systems also meant that many processes involved manual transfers of data and multiple copies of data being stored on the system. The library's legacy systems made the duplication of data a particular problem but there are many reasons why other organisations might suffer from the same problem. Even where organisations have clear policies about the storage of data, employees may store documents locally while working on them, especially if working from home.

The manual transfer of data between systems made the British Library's systems vulnerable, while a more modern system would pose much less of a risk.[6] Although more secure, the trend for suppliers of software services to the legal sector to take responsibility for as many of the business administration functions as possible does mean that many legal businesses are becoming dependent on one or two major suppliers. Were the security of one of these suppliers to be compromised, the impact on clients could be very significant.

COLLECTION MANAGEMENT POLICIES

An unexpected consequence of the attack has been the impossibility of using e-books across the country's network of copyright deposit libraries. The decision of the copyright libraries to acquire digital rather than print copies as a solution to the problem of storage space was understandable but the failure to coordinate a system where at least one print copy might be held by one of the institutions does seem short-sighted. The fact that all the electronic copyright deposit was managed by the British Library has meant that all six copyright deposit libraries in the UK and Ireland have therefore lost access to their e-books.

This is a timely reminder that, although digital publications have huge numbers of advantages, there is still a place for print collections. Although the IT infrastructure of the major legal publishers is, one hopes, far more advanced than that of the British Library, it would seem wise to assume that no system can be guaranteed to be 100% secure. As law firms and barristers' chambers move increasingly away from print to online, the incident only serves to strengthen the argument for professional bodies retaining comprehensive reference libraries for the professions.

YOUR INSTITUTION'S OWN DOCUMENTS

Law libraries and other information services tend to think of their information provision in terms of purchasing and storing material produced by professional publishers but may well be responsible for maintaining archives of documents generated in-house. These may be papers relating to the organisation's administration (i.e. an archive in the traditional sense) or client documents / know how etc. In any case, such material will almost certainly be 'born digital' and only stored digitally.

The types of documents generated will differ widely between different types of legal information system. For the Inns of Court and other professional bodies they will include membership information, property management and maintenance records as well as financial and administrative information. Some of this information (e.g. finance and accounting records) will be created and held on specialist software but others may well be held in the organisation's local or cloud storage. The British Library attack highlights the importance of reviewing the security of whatever systems you have in place for storing and retrieving this material and the advisability of having a back-up system (such as Preservica, the digital preservation software, used by the National Archives and many other organisations).

As the Library notes in its report, the issue of a cyber-attack, regardless of precautions is always a question of "when" not "if".

https://doi.org/10.1017/S1472669624000215 Published online by Cambridge University Press

Endnotes

[1] Catherine Baksi, 'Hackers hit lawyers with cyberattacks' *The Times* (20 February 2024)
[2] Learning lessons from the Cyber-attack: British Library cyber incident review (*British Library*, 8 March 2024) <www.bl.uk/home/british-library-cyber-incident-review-8-march-2024.pdf>
[3] *ibid.* pp. 17–18
[4] *ibid.* p.7
[5] Catherine Baksi, *op. cit.*
[6] *ibid.* page 3

Biography

Dunstan Speight, Librarian of Lincoln's Inn, has spent 27 years working as a law librarian in a number of different libraries. After a trainee post at Nuffield College, Oxford and the MSc in Library and Information Studies at the University of Wales, Aberystwyth, he moved to London and the Middle Temple (as post-graduate trainee and then Assistant Librarian). This was followed by two and a half years as an Assistant Librarian at the Law Society, before spending 16 years in City law firms. He joined Baker & McKenzie LLP as a Research Librarian in 2000, later becoming a Library Manager there, before joining Berwin Leighton Paisner LLP as Library Manager in 2006. He has been Librarian of Lincoln's Inn since July 2016. He was President of BIALL in 2019 and is currently Honorary Secretary.

https://doi.org/10.1017/S1472669624000215 Published online by Cambridge University Press