HE Briefing Note

Ransomware and Institutional Responses in the HE Sector

October 2021

Introduction

Ransomware is a rapidly growing type of cyber attack typically involving locking of systems and/or theft of data with an accompanying demand for payment before the access is restored or the stolen data returned. The motive for ransomware attacks is usually monetary, and unlike other types of attacks, the victim is usually notified that an exploit has occurred and is given instructions on how to recover from the attack. The National Cyber Security Centre (NCSC) has issued warnings to universities to be vigilant following an increase in ransomware attacks targeting educational institutions, including high profile attacks on the universities of Northumbria and Newcastle in 2020 and Hertfordshire and Northampton in 2021 with severe effects on staff and students' access to systems and data.

"ransomware presents the most immediate danger to the UK, UK businesses and most other organisations – from FTSE 100 companies, to schools; from critical national infrastructure to local councils. Many organisations – but not enough – routinely plan and prepare for this threat, and have confidence their cyber security and contingency planning could withstand a major incident. But many have no incident response plans, or ever test their cyber defences". (Lindy Cameron CEO of the NCSC)[1]

The route of a ransomware attack can be via a malicious (phishing) email or website, removable media or via an infected computer or device. Organisations need to have robust controls and procedures in place to reduce the likelihood and impact of an attack. These include overall cyber security controls such as threat detection, access controls, patching, anti-malware and user training and education. Resilient back-up and recovery processes are also crucial to ensure data can be recovered.

One of the largest ever ransomware payments (a reported $1.14m) was made by the University of California in 2020 after servers used by the school of medicine were encrypted by the attackers[2]

[1] National Cyber Security Centre https://www.ncsc.gov.uk/speech/lindy-cameron-first-year

[2] IT Governance Institute: . https://www.itgovernance.co.uk/blog/the-5-biggest-ransomware-pay-outs-of-all-time

The emphasis on more immediate service continuity needs during the pandemic has left a backlog of cyber security tasks and projects in some organisations. This has led to cyber security teams facing competing priorities. In some cases, organisations have had to choose between prioritising IT service continuity and maintenance work, and aspects of cyber security such as patching software. Post pandemic we can expect challenges within new "blended" working environments, with users perhaps less receptive to 'compliance-based' cyber security measures, and home workers facing distractions and with less focused IT and security support.

Ransomware features prominently on institutional risk registers at most of our clients and consequently is becoming a high priority within audit programmes agreed with university management and audit committees. In this paper, we outline typical university responses, key risks, and areas of best practice we have observed during our reviews.

University Responses

University 'A'

Ransomware was not seen as a corporate risk but an 'IT Issue'. There was an informal approach and the IT Director was tasked with compiling incident management and business continuity plans which dealt with the possibility of a ransomware attack. However there was a lack of engagement by business and system owners which meant that plans did not factor in business impact, service expectations and recovery times. There were no plans for ransomware scenario testing due to resource constraints and a lack of expertise within the internal team.

University 'B'

There was an IT Ransomware Playbook which included technical controls and an incident response plan covering core scenarios which may represent a ransomware attack; scenarios included phishing, servers and end user computing, and cross system infection. There was not a formally documented corporate playbook which covered SMT and system owners' roles, legal issues, and PR and media. The latter included plans for external communications via University web sites, social media and public press and broadcast media. Some scenario testing had taken place and there were plans to undertake further tests to cover different potential attack vectors.

University 'C'

The Board and Audit Committee requested a 'deep dive' into the institutional response to ransomware threats. This produced a report which outlined the current and planned cyber controls and investments covering both technical (patching, Microsoft security features, threat monitoring); user controls (training and education, multi-factor authentication) and future priorities, including staffing and resourcing. The approach emphasised the importance of cross-University ownership and communication and building and maintaining awareness over time.

University 'D'

There were detailed Ransomware incident response procedures which were approved by management and covered: detection, responding to an incident, key roles and responsibilities, communication with key stakeholders, recovery and post-incident reviews. Resilience priorities and recovery times for the main systems were approved by the relevant academic and professional services owners.

Ransomware Playbook

Whilst universities will have general incident response plans, business continuity and back-up processes, and varying levels of investment in cyber security, from our work in the sector these are rarely designed to specifically tackle ransomware attacks. Best practice is to develop a 'playbook' of actions which are focused directly on the correct ransomware response, co-ordinated across the institution and with senior executive leadership (and Board approval if necessary). This should include:

- Policy on whether to pay a ransom or not (backed up with suitable legal advice) and how this would be enacted, including acquisition of cryto-currency
- Establishing an incident management team including IT management, support and network staff, system owners and PR/media and establishing meeting protocols
- Escalation to relevant gold / silver teams
- Incident response steps / instructions for users to prevent spread of infection (depending on the origin / nature of the threat)
- Reporting of the incident to external stakeholders e.g. Information Commissioners Office, OfS, NCSC
- Communication response based on clear messages and the right information at the right time

- Co-ordination of forensic investigations and evidence gathering to assess technical solutions e.g. the likelihood of success of a restore of back-up systems and data
- Recovery process such as rebuilding of hardware and software, and re-installation of relevant security and monitoring
- Review of lessons learnt and recommendations / actions to identify weaknesses and prevent recurrence / minimise impact.

Policies on paying a ransom are crucial because in the real world this is happening. In May 2020 at least seven UK universities were hit by ransomware attacks as part of a sustained global attack against their US based cloud provider Blackbaud (a major provider of education administration, fundraising, and financial management software). Blackbaud released a statement on its website revealing details of the attack and that they had paid an undisclosed ransom to the hackers, who promised in return to delete all the data that was stolen from their systems.3

Some organisations have purchased cyber insurance which may help with cover against a ransomware attack. Some insurers offer cover for ransomware payments (a move which has been criticised by law enforcement agencies as it may encourage future attacks) and we have also been made aware from our HE audit work that some universities have been refused cyber insurance cover due to perceived weak controls or have decided that the limitations on cover are unacceptable. This is a complex area which we suggest should also be included in a corporate ransomware response.

Best Practice

Whilst it may be difficult to prevent a ransomware attack, like many such incidents they are opportunistic so the impact can be controlled. Patching, malware controls, user education and awareness are all key. Universities need to understand their data and information security environment and apply resilience as appropriate to key assets. It should also be recognised that this is a corporate not just an IT issue and that oversight and governance are vital.

JISC recommend institutions should:

- Keep systems and software updated and patch known vulnerabilities
- Implement architectural controls to segment networks
- Check email attachments – disable macros on externally received documents and scan for malware
- Keep isolated backups.

[3] BBC https://www.bbc.co.uk/news/technology-53528329

Multi-factor authentication is now widely used and if implemented on key systems reduces the likelihood of an account being compromised. Device management of all personal devices accessing university systems is also important. Data loss prevention can be installed (for example on Microsoft Office 365) which reduces the risk of user error. Institutions should ensure that there is a back-up strategy which is focused on clear best practices and covers which data is to be backed up, location (on premise, cloud, offline), frequency, staff member responsible and oversight and how often test restores are to be performed. Plans should be updated based on a full business impact assessment involving system owners and key stakeholders across the institution. If it has not been carried out, institutions should agree a target date for a ransomware simulation exercise. This could be an in depth or desk-based exercise and should include all relevant parts of the University, including SMT, Marketing / PR and the IT operational response. The output should document the exercise and feed into both IT disaster recovery plans and the corporate ransomware playbook.

Ian Musgrave
Client Director
t: 07799343457
e: imusgrave@uniac.co.uk
www.uniac.co.uk

For further information on how we can help, or for any other aspect of Uniac's internal audit and assurance service, please do get in touch.