Meeting of the Group Audit and Risk Committee

11.00am on Thursday, 6 May 2021
via MS Teams

Agenda

No.	*Item*	*Pages*	*Presenter*
1.	Welcome and apologies		DB
2.	Declarations of interest		DB
3.	IT recovery update	2 - 9	NL

Date of next meeting
4:00, Thursday 15 June 2021

Members: Duncan Brown (Chair), John Cole, Mark Lemmon and Rob Orr

In attendance: David Phoenix, Alison Chojna, Natalie Ferer, Richard Flatman, Kerry Johnson, Stuart Johnston, Nicole Louis and James Stevenson

	CONFIDENTIAL
Paper title:	IT Restoration Update
Board/Committee:	Group Audit and Risk Committee
Date of meeting:	06 May 2021
Author(s):	Alison Chojna, Acting Executive Director of Academic Related Resources
Sponsor(s):	Nicole Louis, Chief Customer Officer
Purpose:	For Information
Recommendation:	For the committee to review the information provided.

Executive summary

This paper provides an update on progress of the IT restoration following the cyber-attack in December 2020. Rather than restoring services and applications to their previous conditions, improvements to security have been made wherever possible.

As the restoration process is close to completion the paper identifies the main challenges encountered and also the next steps.

IT Restoration Update May 2021

Current status

The restoration process of IT Services is now in its final stages. Whilst every effort has been made to restore as quickly as possible, the guiding principle has been that security has been the highest priority. A zero-trust approach has been taken, meaning that every service has been considered as the possible attack vector. Where needed, systems have been upgraded, patched, new servers built, operating systems upgraded, old hardware replaced and processes improved. The small proportion of legacy systems unable to be upgraded have been segmented on the network and will be added to the roadmap for replacement.

By the end of April 2021, the majority of IT services and applications will have been restored. The restoration process for the remaining 11 applications has begun and expected to complete in early May. The removal of old computers from campus will continue throughout May but is a lower priority given the small numbers of staff and students on campus.

Connectivity and networks

The network redesign and replacement programme had commenced prior to the cyber-attack. The previous network design was a flat structure, which was no longer considered good practice. Network segmentation was being planned and expected to deliver in Spring 2021.

New network

A new network design has now been implemented with micro-segmentation in place. Each IT service has been grouped in a separate vlan which greatly enhances security. New firewalls have also been installed. The network hardware for Phase One of the network replacement programme will be deployed over the coming months.

On-campus devices have been moved onto the new network and internet connectivity reinstated, with the exception of a small number of research labs with bespoke configurations. These are in progress and should be completed week beginning 3rd May 2021.

Wi-Fi

Student, staff and guest Wi-Fi has been reinstated across campuses and functioning as expected.

VPN

A new VPN, Global Protect, has been deployed for staff and students. Global Protect has improved security features compared to the previous VPN, Pulse Secure. Pulse Secure has been the subject of security alerts in the sector over the previous year.

Infrastructure and IT systems

The cyber-attack resulted in the encryption of all 719 virtual servers on the IT estate. There were successful backups available of all servers. Advice from external experts CyberClan was that servers should not be restored from backup as they were prior to the attack, which could have been achieved in a matter of days. It was imperative to ensure that the attackers had not left any “hooks” in the

systems. Therefore, every server had to go through a scrubbing process, which involved being restored onto a temporary environment and running two anti-virus products, installing the latest security upgrades, being given a new IP-address and then finally moving onto a new clean network.

Servers

The server restoration process revealed that 47% of servers were running uncompliant operating systems. Rather than being able to scrub the servers and move them onto the new network, servers had to be rebuilt with compliant operating systems. This added to the time needed to restore systems but was necessary to ensure systems were restored securely. Operating system compliance is now being tracked through the IT Security and Resilience Board.

The scrubbing process for all servers will be completed during the first week of May 2021. The server estate has been reviewed as part of the process and 32% have been decommissioned as a result. This will increase space availability on the permanent infrastructure, which was running close to capacity prior to the attack.

DELL EMC VxRail – On-premise server estate

A temporary server environment was leased for the restoration process as the permanent environment, VxRail, had to be wiped and then reconfigured. This activity has now taken place and the migration from the temporary environment back onto VxRail will commence in early May.

Backups

The success of the restoration programme was founded on the ability to restore successfully from backups. The backup solution was previously on-premise and part of the VxRail ecosystem. Prior to the cyber-attack a new backup solution had been scoped to bring LSBU in line with current best practice, which advises storing 3 copies of backups, on 2 different media, 1 of them being offsite. The solution is currently being implemented, with the offsite element being cloud-based.

The frequency of back-ups has also been brought in-line with best practice. As well as the technical solution, a managed service contract has been introduced to support the solution and provide regular testing on the integrity of the backups.

ISIM

The identity management system ISIM is a critical service in the IT environment. ISIM provisions new staff and student IT accounts and passes data between multiple systems. ISIM is one of the few remaining legacy IBM solutions. It was highly customised at the point of installation, is extremely complex and difficult to support.

Support for ISIM is outsourced to a managed service provider and with the exception of one staff member, historical knowledge of the system no longer exists internally. The restoration of ISIM has been extremely difficult and the reliance on an external vendor to support this system resulted in a failure to restore it in the planned timeframe. An alternative vendor has now been sourced but the delays in restoring this system have resulted in time-consuming manual processes being employed by multiple teams to ensure students and staff have access to systems.

End-user applications

The majority of end-user applications have now been restored and upgraded where necessary. The continuing use of legacy applications had had downstream consequences prior to the attack. For example, the student record system, QL, had previously only been functional on Windows 7 and the changes required to move it to Windows 10 could only have been achieved by a significant amount of downtime, which would not have been possible under normal circumstances. Therefore, QL users had remained on Windows 7 even after the operating system had gone out of support. Although it would have added time to the restoration, QL is now supported on Windows 10, which has cleared a route to replace all legacy hardware on campus.

Applications that have been restored

- Tier 0 IT Systems - restored, from 38 servers.
- Salto estate access control – Full system upgrade, which had been in planning for some time.
- ITrent HR system – reinstated and then upgraded in March 2021.
- E-file - HR records systems restored.
- VT2000 hourly paid lecturers payment system - restored.
- Agresso Finance system– reinstated and addressed web access vulnerability.
- Moodle Virtual Learning Environment- reinstated, with a move to a hosted cloud solution in planning to commence when the semester ends.
- Panopto lecture capture and video hosting – direct access introduced to avoid the need for Moodle access.
- TurnItIn plagiarism checker – link re-established
- Library resources - authentication restored and second authentication route being introduced for business continuity.
- Halpo research and enterprise platform - authentication restored (SaaS product)
- AppsAnywhere virtual software store - restored and upgrade planned in coming weeks.
- Telephony – Full system upgrade.
- I-drives staff personal file drives - Moved to OneDrive cloud storage. Provides 24/7 access over a browser and releases considerable space on the VxRail.
- Departmental file shares – Moved to Microsoft Teams cloud storage. Provides 24/7 access over a browser and releases considerable space on the VxRail. Puts control of file access in the hands for the departments.
- QL – reconfigured and made available for Windows 10.
    - Core QL main database restored
    - Finance feed restored
    - Reporting and Transcripts restored (LaunchPad, Kali and Assgrid)
    - Admissions restored
    - International
- Maximiser Student Disability and Wellbeing system restored.
- SID student enquiry management system - restored.
- Salesforce - authentication re-established.
- Shibboleth – restored authentication to various systems.
- Aula virtual learning environment – authentication re-established.
- Kx student accommodation system – restored.

Please see the appendix for the remaining services and applications to restore, all of which are currently in progress.

End-user devices

On-campus computers

There are upwards of 4,000 computers of various types on campus, all of which needed to go through the scrubbing process. Like the servers, this required being scanned by two anti-virus solutions and then being moved onto the new network. As part of the process the new anti-virus product, Sophos Intercept X, has also been deployed on campus devices.

As well as being scrubbed, computers running non-compliant operating systems needed to be upgraded to Windows 10. The older 32-bit computers are unable to accommodate Windows 10 so these are either being swapped or upgraded with additional RAM and discs. This activity began in April and is happening throughout May 2021. Priority users and spaces have already been migrated. By the end of the exercise, campus devices will all be on complaint operating systems.

Staff devices

Throughout the pandemic a sizeable minority of staff have been working remotely from personal computers. Over the course of the year, 702 LSBU laptops have been deployed to staff and the remaining permanent and fixed term staff without a corporate device will be in possession of an LSBU laptop by the end of May 2021. As well as being more secure and easier to control, access to a portable device is essential to our future ways of working strategy and has enabled the removal of legacy equipment from the estate.

Printing

Due to low levels of activity on campus, printing was lower down on the priority order for restoration. However, with campus activity increasing this has now been prioritised and the printing fleet is due to be restored by the end of April 2021. All devices need to be moved onto the new network and the associated software is currently being re-enabled.

Security

An IT Security and Resilience Board (ISRB) has been in place since 30/10/2020 and is meeting on a 6-weekly basis. KPIs are being tracked through the ISRB on measures such as frequency of patching, network availability, number of intrusion attempts, training session completions and IT outages.

In parallel to the IT restoration, actions continue to be completed on both the IT Security Roadmap and BDO audit. An update will be provide at the June 2021 Group Audit and Risk Committee.

Anti-virus

A subscription has been taken to a next generation anti-virus solution (Sophos Intercept X) which will be a requirement for users to connect to the network. As well as a software product, the solution comes with a 24/7 security operations centre (SOC), which monitors for threats and proactively blocks any suspicious activity.

All devices with the anti-virus client installed are also monitored and controlled through a central console by key internal staff in Security and IT Services.

Restoration Challenges

Suppliers and managed service partners

Support and development for many key services and applications are outsourced either through managed service contracts or purchased service/development days. Whilst some suppliers have been able to respond quickly, others have required lead times of several weeks, have not been able to scale for the additional staff resources needs or in the case of ISIM, have failed to deliver the service needed. Almost all bottlenecks can be attributed to delays with suppliers' availability or the ability of suppliers to provide additional staff. The restoration has been running 7 days a week and only some suppliers have been able to support that level of activity.

Network design

Working to the new network design has been challenging when working at pace. Micro-segmentation means that only servers that need to communicate are allowed to communicate so service re-established has required changes to firewall rules, ports to be opened and closed, vendors being granted access to specific servers, etc. This activity can only be undertaken by the network managed service provider and has proved to be the most significant bottleneck. Although the provider has been able to provide some additional staffing resource, it has not been to the level needed to increase the pace.

Legacy systems and operating systems

Had systems been on the most current version prior to the cyber-attack and had all operating systems been compliant, the time to recovery would have been quicker. Additional time and effort was needed to bring everything back and then upgrade to a compliant position.

Predicting timescales

There has been a need to estimate when each service or application will be restored in order for departments to plan for workarounds to business processes and communicate with their users. Establishing accurate timeframes has been very challenging due to the complexity of each restoration, the interdependencies and reliance on third-parties. The priority order has been communicated and reviewed at the fortnightly Recovery Operations Group meeting, attended by Schools and Heads of Services. However, timeframes have had to be refreshed several times and this has proved a source of frustration to staff.

BAU and projects

As the restoration has progressed, BAU activities have been re-established and major projects, such as LEAP and the Campus Development Programme, needed to be supported in parallel to restoration activities. This has been challenging to manage and resource.

Staffing

The staff in IT and associated departments have been outstanding in their efforts and have regularly worked evening and weekend overtime. As this has been happening throughout a pandemic, staff have also had personal challenges, bereavements and ill-health to deal with. This is to be expected but has also proved challenging to manage when trying to deliver on tight deadlines.

Next steps

The recovery element of the restoration is close to completion now so the next phase of activities will need to commence:

- Lessons learned exercise from the technical perspective.
- Business impact analysis and investigation by an independent person.
- Rectify any temporary technical solutions put in place behind the scenes.
- Forward roadmap of change to factor in legacy systems in need to replacement.

Appendix – Remaining Restoration Timeline

Week beginning 26th April 2021	
QL – Appeals, ECs and DBS	To be completed by end of this week
QL – Data Feeds	To be completed by end of next week
Wozzad	To be completed by end of week
KX	Completed early this week
Modern.Gov	Small network change required, expected early this week
Printing	Printing provided for Transcripts, wider campus roll out continuing for next two weeks.
Intruder Alarm	Almost completed, expected first half of week
CCTV	Work underway, expected this week
Card Exchange (ID Cards)	Works underway final completion this week
SharePoint Online	Works underway, completion this week
Week beginning 4th May 2021	
QL data feeds	Schedule for completion by end of the week.
My LSBU	Work underway for last 2 weeks, completion this week due to significant upgrade required
Building Management System	Work commenced week beginning 19/04/2021 but to be completed by end of this week
CMIS	Work commenced week beginning 19/04/2021 but to be completed by end of this week
ProAchieve	Work commenced week beginning 19/04/2021 but to be completed by end of this week
OurLSBU	Work commenced week beginning 19/04/2021 but to be completed by end of this week
Appraisal System	Work commenced week beginning 19/04/2021 but to be completed by end of this week
Learning Station	Work commenced week beginning 19/04/2021 but to be completed by end of this week
InVu	Completed by end of this week.
ISIM	New provider sought timeline to be confirmed at the earliest
Moodle Admin	Cannot be completed until ISIM recovered completely
Mahara	Requires Moodle Admin to be available first.

Finance Systems Recovery Update

1. **Agresso**

Recovery:
Agresso has been restored and staff are now able to use most functionality. Some interfaces are still not operational including those with QL, online payments and the accommodation system. Bacs software is also not yet fully functional. Sharepoint, which is used to process new supplier requests is not yet restored but is expected to be operational this week.

Issues with new user accounts has meant that temporary staff brought in to help bring records up to date have not been able to access all systems, but this matter seems to have been resolved this week. Some staff are still not able to access QL through remote desktop which has prevented them responding to student payment queries and carrying out credit control activities.

Good progress is being made bringing accounting records up to date. The transactions that are still to be brough up to date inlcude:

- Supplier invoices dated from mid March to the end of April
- Invoices received from new suppliers
- Around 300 supplier invoices where a PO has not been raised and the team need to investigate who should approve before payment
- Income and expenditure through the Accomodation system interface
- Some bank transactions where the team are still investigating posting details
- Sales invoices through the QL interface where fee invoices have not been raised

March management account have been produced and April accounts will be produced next week. It had been estimated that it would be Mid May before the team have caught up with financial processing but this is dependent on resolution of the remaining IT matters.

Supplier payments are now being made. The team are working through a back log of around 3000 invoices and, as many of these do not have a PO to match against, processing is slower than it would be otherwise.

Workarounds:
We continue to maintain a manual spreadsheet cashbook is being maintained to record all bank transactions.

A manual process is in place to transfer transactions from QL to Aggresso.

2. **Student Sales Ledger**

Some semester 2 fee income still to invoice.

3. **Payroll**

Payroll records have been updated and tax year end processes are under way. There are approx £85k of manual payments still to recover from staff – mainly HPLs with 10-15 staff owing more than a few pounds. In SBC only one advance, for £35, is still unrecovered.

4. Reporting

The Group's next VAT return is due on 7th June and is likely to be less accurate than if accounts payable records were up to date. An estimated return was sent on 7th March and we will engage KPMG to advise on providing HMRC with actual figures once records are up to date.

5. Audit

Internal Audit:
BDO are now progressing with reviews postponed during the IT outage and in additional will do some work on the finance recovery later this year. BDO is preparing an updated audit progress report for Exec next week. it is still expected that the planned audit programme will be completed by the end of July 2021.

Year end Audit and Accounts:
We are still expecting records to be brought up to date and not impact on the year end process. KPMG have said that they will be undertaking more substantive testing as part of their year-end work as a result of the IT outage rather than reliance on data analytics.

Natalie Ferer
5th May 2021