Meeting of the Finance, Planning and Resources Committee

4.00 - 6.00 pm on Tuesday, 24 September 2019
in Technopark, SE1 6LN

Agenda

No.	*Item*	*Pages*	*Presenter*
13.	Cyber security update	87 - 98	SW
15.	Insurance claims	99 - 110	RF

Date of next meeting
4.00 pm on Tuesday, 5 November 2019

Members: Michael Cutbill (Chair), Jerry Cope, Peter Fidler, Nelly Kibirige and Mee Ling Ng

Apologies: David Phoenix and Deepa Shah

In attendance: Pat Bailey, Michael Broadway, Richard Flatman, Paul Ivey, Nicole Louis, James Stevenson, Ralph Sanders and Shân Wareing

This page is intentionally left blank

	CONFIDENTIAL - RESTRICTED TO MEETING PARTICIPANTS
Paper title:	Cyber Security Roadmap
Board/Committee:	Finance, Planning and Resources Committee
Date of meeting:	24 September 2019
Author(s):	Alison Chojna, Acting Director of Academic Related Resources
Sponsor(s):	Shân Wareing, Chief Operating Officer and Deputy Vice Chancellor (Education)
Purpose:	For Review
Recommendation:	The committee is requested to review the Cyber Security Roadmap and consider the recommendation on the establishment of a Group Cyber Security Board.

Executive summary

The Cyber Security Roadmap outlines the actions being undertaken by LSBU in 2019/20 to improve cyber security in the key areas of people and culture; technology; governance, compliance and monitoring; business continuity and external reputational.

Three issues needing immediate resolution were identified and work is now underway to resolve them. Following this activity, LSBU should be in a position to apply for Cyber Essentials accreditation. An external partner is currently being engaged to undertake an independent review of the existing landscape, to ensure our internal review has not overlooked any vulnerabilities.

The Committee is asked to consider the recommendation to establish a cyber security board, with oversight of cyber security across the LSBU Group. Best practice places cyber security governance outside IT as an institutional leadership responsibility. As we move towards closer integration of the Group, the recommendation is for central oversight, sitting alongside GDPR.

This page is intentionally left blank

LSBU Cyber Security Roadmap
July 2019- July 2020

Alison Chojna, Interim Director of Academic Related Resources
Graeme Wolfe, Head of IT Security
July 2019

Introduction

The joint HEPI/JISC paper on Cyber Security[1], published in April 2019, highlighted the growing risk of cyber threats to universities and has challenged providers to consider the following basic questions:

- Where is data stored, who is responsible for it and who has access to it?
- Are systems patched and up to date?
- Are regular vulnerability scans performed as part of a vulnerability management policy?
- Are students/staff trained in information security, to spot fraudulent emails, to know how to look after their data and how to report when things go wrong?
- Is there an incident response plan in place?
- Who should be contacted when additional help and guidance is needed?
- Do attack monitoring and mitigation systems cover the right cyber risks?
- Is the network provider mitigating denial of service attacks, which could bring down the network?

Cyber security is the responsibility of all individuals in an organisation and should not be delegated as the sole responsibility of the IT Team.

At the time of writing, external support is being procured to provide an independent cyber security assessment. This roadmap may be revised following that assessment.

Current assessment

LSBU employs 1 x FTE staff in the role of Head of IT Security, who reports directly to the Acting Director of Academic Related Resources. It is important that this role sits outside of the IT Department structure to maintain objectivity and the ability to challenge. The Head of IT Security works closely with the Data Protection Officer.

Safeguards currently in place:

- Software: Sophos anti-virus and malicious website blocking; Mobileiron security for mobile devices.
- Next generation Palo Alto firewall in place.
- E2E external vulnerability scanning and assessment tool.
- Janet network, provided by JISC, mitigates against denial of service attacks.

[1] https://www.hepi.ac.uk/wp-content/uploads/2019/03/Policy-Note-12-Paper-April-2019-How-safe-is-your-data.pdf

Immediate issues to resolve:

- Anti-virus: Loss of institutional knowledge on current configuration and existing set-up has been flagged as a concern by the vendor. Currently working with the vendor to bring up to the latest version and bring configuration in-line with best practice.
- Not all servers have been updated in recommended timescales. Currently working on schedule of updates to be introduced.
- WWW1 server needs to be decommissioned immediately as GDPR concerns have been flagged. Take-down currently progressing.

Roadmap

People and Culture

As with all other organisations, LSBU's biggest cyber security vulnerability is our own workforce. Phishing attacks are often designed to mimic existing employees, departments or suppliers and can be very convincing. It is important that training and awareness raising activities are ongoing, so that cyber security remains high in the consciousness of staff and students.

It is equally important that a no-blame culture is adopted, so that staff can feel safe to report security issues or exposure without fear of retribution or recrimination. It is essential that breaches are reported at the earliest opportunity. GDPR requires we contact the Information Commissioners Office within 72 hours of becoming aware of the breach.

	Description	Lead	Contributors	Completion Date
Mandatory Staff Training	IT Security Training Package to be launched on the Organisational Development online learning platform.	Graeme Wolfe, Head of IT Security	OD	31/10/2019
Regular campaigns to raise awareness	With Communications, design a campaign to raise awareness of cyber security, to be delivered across the year at regular intervals.	Graeme Wolfe, Head of IT Security	Communications	31/08/2019
Transparent reporting mechanisms	Update Cyber Security information on Our LSBU, clearly signposting how to report potential breaches.	Olly Miller, Business Support Officer (IT)		31/10/2019
Student Training	With the Students Union, plan induction activities on e-safety, signposting to appropriate online resources. Digital Ambassadors to be trained for peer-to-peer support activities.	Russell Goodwin, Digital Skills Training Manager	SU, Student IT Support (LLR)	17/10/2019

Technology

Some of the most common types of cyber-attack involve exploiting vulnerabilities in an organisation's IT environment. This could be to gain access to the environment or to disrupt operations by bringing services down. It is essential that systems and anti-virus databases are kept up to date, firewalls are appropriately configured, and networks are designed with cyber security as a primary concern.

	Description	Lead	Contributors	Completion Date
Network Refresh Design	The existing network needs to be refreshed in August 2020. This affords an opportunity to redesign the network in line with current best-practice recommendations, including additional security structures. Engagement is needed across LSBU to understand existing and future needs, in particular the needs of Research Centres, certain curriculum areas, Registry, Governance, International, etc.	Malvina Gooding – Acting DD of IT Services, Alex Denley – DD of Innovation, Graeme Wolfe – Head of IT Security	REI, FMI, Schools, CRIT, International and others	31/07/2020
Replace MobileIron (mobile device management software).	MobileIron to be replaced by Microsoft InTune product, which removes the existing weakness of staff configuring accounts on mobile devices without the proper security features enabled.	Raj Virdee, Head of Project Management Office		31/12/2019
Update and reconfigure Sophos Anti-virus	Work with vendor to update Sophos to recent version and reset configuration to best practice settings. Investigate requirements to move service off premises and into Cloud. Work currently progressing.	Graeme Wolfe, Head of IT Security	Sophos	31/12/2019
Decommission WWW1 server	Immediately implement project to decommission server.	Malvina Gooding – Acting DD of IT Services	MAC, LLR	31/10/2019
Update all servers	Patching policy to be drafted and agreed. Programme to update servers completed, to ensure the most recent security setting are applied.	Malvina Gooding, Acting DD of IT Services		30/11/2019 31/12/2019

Governance, Compliance and Monitoring

IT systems need to be continuously monitored and audited for suspicious activity. Monitoring also allows an organisation to ensure that systems are being used appropriately in accordance with organisational policies. Processes need to be in place to review any change or introduction of new technology against cyber security standards.

	Description	Lead	Contributors	Completion Date
Proactively monitor for compromised email addresses	On a Monthly basis, check for compromised LSBU email addresses and contact students/staff with advice and guidance on remedies and keeping safe in future.	Graeme Wolfe, Head of IT Security	Student IT Support (LLR)	Ongoing
Software as a Service Security checklist	Introduce a process where existing SaaS Security checklist is completed and approved before new software is procured.	Alex Denley, Deputy Director of Innovation & Transformation	Procurement	31/07/2019
Project to review firewall usage	Review Palo Alto firewall usage to ensure its full potential is exploited. Currently only make partial use of its capability.	Graeme Wolfe, Head of IT Security	Dependent on engagement from external network partners.	31/07/2020
BS 31111:2018 standard	Commission JISC BS 31111 audit and assessment service to understand our level of resilience, plan for a changing landscape and allocate resources appropriately.	Shân Wareing – COO and DVC Education, Alison Chojna - Acting Director of ARR	LSBU Board, LSBU Executive, LSBU Leadership	31/07/2020
Penetration testing	Engage external vendor (could be JISC) to undertake annual penetration testing and then ad hoc testing as new services are introduced. Dependent on financing.	Graeme Wolfe, Head of IT Security		31/11/2019
EPOS payment card terminal compliance	Currently card payment terminals are not compliant with PCI/DSS payment standards. Work is underway to resolve this issue and bring up to compliance.	Graeme Wolfe, Head of IT Security	Finance	31/12/2019

Business Continuity

Business continuity is key to building cyber resilience and there is a need to collaborate across the organisation to prepare for cyber security incidents. As well as having appropriate plans in place, it is important that these are tested and rehearsed at regular intervals.

	Description	Lead	Contributors	Completion Date
Plan mock attack	Undertake a mock cyber-attack, in collaboration with HSR, reporting on performance and using results to inform future planning.	Alison Chojna - Acting Director of ARR, Graeme Wolfe – Head of IT Security	Ed Spacey, Acting Deputy Director of HR	31/12/2019
Business continuity plans in place	Working with HSR, complete business continuity planning activity and complete documentation. Ensure staff are trained to respond. Perform an IT Disaster Recovery exercise annually.	Graeme Wolfe, Head of IT Security	Jack Newing, Safety and Resilience Adviser	31/09/2019
Cyber Security insurance	Investigate options for Cyber Security insurance.	Charles Hamilton, Legal Officer, Graeme Wolfe, Head of IT Security	Procurement	31/08/2019

External Reputation

It has become increasingly important to hold cyber security certification to reassure stakeholders that IT and data is secure and that appropriate measures are in place to maintain security. Indeed, some government contracts and funding opportunities are unavailable without proof of certification.

	Description	Lead	Contributors	Completion Date
Cyber Essentials Accreditation[2]	Assess current readiness to achieve Cyber Essential accreditation and develop a project plan. Complete actions required to submit Cyber Essentials application	Graeme Wolfe, Head of IT Security		31/08/2019 31/01/2020

[2] https://www.cyberessentials.ncsc.gov.uk/

LSBU Group

Until now, the IT departments at South Bank Colleges and the Multi-Academy Trust have operated independently of each other. The governance for cyber security has also been coordinated locally. Activity is now underway to scope the cost benefits of integrating technology across the Group. As part of this, we need to review cyber security from a Group perspective.

The recommendation is to establish a board, consisting of appropriate staff from each part of the Group, to develop a joined-up approach to cyber security. The chair should not be a Head of IT, but a senior leader who can ensure a top down approach is taken. This is best practice in terms of appropriate institutional ownership of the benefits of cyber security, and in terms of the ability to hold IT to account.

Cyber Security Roadmap

The below brings together the above actions into a single table in chronological order.

	Description	Lead	Contributors	Completion Date
Proactively monitor for compromised email addresses	On a Monthly basis, check for compromised LSBU email addresses and contact students/staff with advice and guidance on remedies and keeping safe in future.	Graeme Wolfe, Head of IT Security	Student IT Support (LLR)	Ongoing
Software as a Service Security checklist	Introduce a process where existing SaaS Security checklist is completed and approved before new software is procured.	Alex Denley, Deputy Director of Innovation & Transformation	Procurement	31/07/2019
Regular campaigns to raise awareness	With Communications, design a campaign to raise awareness of cyber security, to be delivered across the year at regular intervals.	Graeme Wolfe, Head of IT Security	Communications	31/08/2019
Cyber Security Insurance	Investigate options for Cyber Security insurance.	Charles Hamilton, Legal Officer, Graeme Wolfe, Head of IT Security	Procurement	31/08/2019
Cyber Essentials Accreditation	Assess current readiness to achieve Cyber Essential accreditation and develop a project plan.	Graeme Wolfe, Head of IT Security		31/08/2019
Business continuity plans in place	Working with HSR, complete business continuity planning activity and complete documentation. Ensure staff are trained to respond. Perform an IT Disaster Recovery exercise annually.	Graeme Wolfe, Head of IT Security	Jack Newing, Safety and Resilience Adviser	30/09/2019
Student Training	With the Students Union, plan induction activities on e-safety, signposting to appropriate online resources. Digital Ambassadors to be trained for peer-to-peer support activities.	Russell Goodwin, Digital Skills Training Manager	SU, Student IT Support (LLR)	17/10/2019
Mandatory Staff Training	IT Security Training Package to be launched on the Organisational Development online learning platform.	Graeme Wolfe, Head of IT Security	OD	31/10/2019
Decommission WWW1 server	Immediately implement project to decommission server.	Malvina Gooding, Acting DD of IT Services	MAC, LLR	31/10/2019
Transparent reporting mechanisms	Update Cyber Security information on Our LSBU, clearly signposting how to report potential breaches.	Olly Miller, Business Support Office (IT)		31/10/2019

Penetration testing	Engage external vendor (could be JISC) to undertake annual penetration testing and then ad hoc testing as new services are introduced. Dependent on financing.	Graeme Wolfe, Head of IT Security		30/11/2019
Update all servers	Patching policy to be drafted and agreed. Programme to update servers completed, to ensure the most recent security setting are applied.	Malvina Gooding, Acting DD of IT Services		30/11/2019 31/12/2019
Replace MobileIron (mobile device management).	MobileIron to be replaced by Microsoft InTune product, which removes the existing weakness of staff configuring accounts on mobile devices without the proper security features enabled.	Raj Virdee, Head of Project Management Office		31/12/2019
Update and reconfigure Sophos Anti-virus	Work with vendor to update Sophos to recent version and reset configuration to best practice settings. Investigate requirements to move service off premises and into Cloud. Work currently progressing.	Graeme Wolfe, Head of IT Security	Sophos	31/12/2019
Plan mock attack	Undertake a mock cyber-attack, in collaboration with HSR, reporting on performance and using results to inform future planning.	Alison Chojna - Acting Director of ARR, Graeme Wolfe – Head of IT Security	Ed Spacey, Acting Deputy Director of HR	31/12/2019
PDQ POS payment card terminal compliance	Currently card payment terminals are not compliant with PCI/DSS payment standards. Work is underway to resolve this issue and bring up to compliance.	Graeme Wolfe, Head of IT Security	Finance	31/12/2019
Cyber Essentials Accreditation	Submit Cyber Essentials application	Graeme Wolfe, Head of IT Security		31/01/2021
Network Refresh Design	The existing network needs to be refreshed in August 2020. This affords an opportunity to redesign the network in line with current best-practice recommendations, including additional security structures. Engagement is needed across LSBU to understand existing and future needs.	Malvina Gooding – Acting DD of IT Services, Alex Denley – DD of Innovation, Graeme Wolfe – Head of IT Security	REI, FMI, Schools, CRIT, International and others	31/07/2020
Project to review firewall usage	Review Palo Alto firewall usage to ensure its full potential is exploited. Currently only making partial use of its capability.	Graeme Wolfe, Head of IT Security	Dependent on engagement from external network partners.	31/07/2020
BS 31111:2018 standard	Commission JISC BS 31111 audit and assessment service to understand our level of resilience, plan for a changing landscape and allocate resources appropriately.	Shân Wareing – COO and DVC Education,	LSBU Board, LSBU Executive, LSBU Leadership	31/07/2020

		Alison Chojna - Acting Director of ARR		

Last update: 18th September 2019

	CONFIDENTIAL
Paper title:	Insurance Claims
Board/Committee	Financial Planning & Resources Committee
Date of meeting:	24 September 2019
Author:	James Rockliffe – Director of Procurement Antonia Goodyer – University Solicitor
Executive/Operations sponsor:	Richard Flatman - Chief Financial Officer
Purpose:	The Executive recommends that the Finance, Planning & Resources Committee notes this report.
Recommendation:	The Committee is requested to note this report.

Executive Summary:

This paper is presented to Committee for information and to report the extent to which the University's insurance policies were relied upon in the 2018/19 period.

The University remains a member of the London Universities Purchasing consortium for insurance purposes, with Zurich Municipal being the principal insurer. The claims experience in 2018/19 is summarised in Appendix 1 and is considered to be low.

The Committee is requested to note the report.

1. BACKGROUND

1.1 The University's Financial Regulations require that the University Secretary and Chief Financial Officer ensure;

1.1.1 That appropriate insurance cover is provided for all aspects of the University's activities;

1.1.2 The verification of insurance of any incidents which may give rise to a claim;

1.1.3 The submission of a full claim where appropriate.

1.2 The University is a member of the London Universities Purchasing Consortium (LUPC) and retains the brokerage services of Arthur J Gallagher as part of a LUPC group insurance arrangement.

1.3 Effective from 1 January 2010 the insurance claims process has been administered by the University Governance, Information and Legal Team.

1.4 The University's claims record is reviewed annually with the appointed broker and insurers as part of the annual policy renewal process.

1.5 With effect from 1 August 2019 Insurance cover and Claims experience will be merged with South Bank Colleges to provide a LSBU Group.

2. INSURANCE POLICIES

2.1 Insurance policies held by the University are renewed annually with effect from 1 August. A detailed report is submitted to Financial Planning & Resources Committee each year in advance of renewal.

2.2 For the period 1 August 2018 to 31 July 2019 the University maintained the following insurance policies:

Policy	Insurer	Covers maintained	Claims in 2018/19 period
All Risks Policy	Zurich Municipal	Material damage Works in Progress Business Interruption Money Public Liability Employers Liability Libel & Slander Motor Engineering Computer Engineering inspection	Yes
Professional Indemnity	Royal Sun Alliance	Professional Negligence Management Protection (D&O) Employee & Third Party Fraud	No
Terrorism Policy	UMAL	Property reinstatement Contents Business Interruption	No
Travel & Personal Accident	RSA	All risk travel cover for Students, University Employees including those living and operating outside of UK territorial limits.	No
Fine Arts Policy	Blackwell Green	Cover for the Sarah Rose Art Collection.	No
Medical Malpractice	Newline Group	Cover for students and staff in practice placement based teaching or providing support for learning and assessment in practice settings	No
Special Contingency	AIG		No

3. UNIVERSITY EXPOSURE TO RISK UNDER 2018/2019 CLAIMS

3.1 Although unsettled claims were carried forward to 2019/2020 in the following All Risks categories – Public Liability (3 cases) and Employers Liability (4 cases) – the University carries no excess for these types of claim, so the insurer Zurich effectively carries all the risk exposure.

3.2 A full breakdown of claims for 2018/19 is detailed in Appendix 1

4. DECLARED LOSSES WITHIN POLICY EXCESS

4.1 The University is also required to declare to its insurers the incidence of insured perils which fall within policy excess and do not result in the submission of a claim.

4.2 There were no incidents falling into this category during 2018/19.

APPENDIX 1

LSBU POLICY WITH ZURICH MUNICIPAL NHE-01CA07-0013
CLAIMS SUMMARY - 1 AUGUST 2018 TO 31 JULY 2019

Insured risk	Excess Value	Claims brought forward from last period	New claims in this period	Claims carried forward to next period	Value of payments made on claims open in this period
Material damage	£20k	1	0	0	£138,527.80
Works in Progress					
Business Interruption					
Money					
Public Liability	Nil	0	3	3	£0
Employers Liability	Nil	4	0	4	£38,582.65
Libel & Slander					
Professional Negligence					
Governors Liability					
Motor					
Engineering					
Fidelity Guarantee					
Personal Accident					
Travel					
Computer					
Engineering inspection					
Fine Arts Policy					
Medical Malpractice					
Special Contingency					

This page is intentionally left blank

	CONFIDENTIAL
Paper title:	Insurance Claims
Board/Committee	Financial Planning & Resources Committee
Date of meeting:	24 September 2019
Author:	James Rockliffe – Director of Procurement Antonia Goodyer – University Solicitor
Executive/Operations sponsor:	Richard Flatman - Chief Financial Officer
Purpose:	For information
Recommendation:	The Committee is requested to note this report.

Executive Summary:

This paper is presented to Committee for information and to report the extent to which the University's insurance policies were relied upon in the 2018/19 period.

The University remains a member of the London Universities Purchasing consortium for insurance purposes, with Zurich Municipal being the principal insurer. The claims experience in 2018/19 is summarised in Appendix 1 and is considered to be low.

The Committee is requested to note the report.

1. BACKGROUND

1.1 The University's Financial Regulations require that the University Secretary and Chief Financial Officer ensure;

1.1.1 That appropriate insurance cover is provided for all aspects of the University's activities;

1.1.2 The verification of insurance of any incidents which may give rise to a claim;

1.1.3 The submission of a full claim where appropriate.

1.2 The University is a member of the London Universities Purchasing Consortium (LUPC) and retains the brokerage services of Arthur J Gallagher as part of a LUPC group insurance arrangement.

1.3 Effective from 1 January 2010 the insurance claims process has been administered by the University Governance, Information and Legal Team.

1.4 The University's claims record is reviewed annually with the appointed broker and insurers as part of the annual policy renewal process.

1.5 With effect from 1 August 2019 Insurance cover and Claims experience will be merged with South Bank Colleges to provide a LSBU Group.

2. INSURANCE POLICIES

2.1 Insurance policies held by the University are renewed annually with effect from 1 August. A detailed report is submitted to Financial Planning & Resources Committee each year in advance of renewal.

2.2 For the period 1 August 2018 to 31 July 2019 the University maintained the following insurance policies:

Policy	Insurer	Covers maintained	Claims in 2018/19 period
All Risks Policy	Zurich Municipal	Material damage Works in Progress Business Interruption Money Public Liability Employers Liability Libel & Slander Motor Engineering Computer Engineering inspection	Yes
Professional Indemnity	Royal Sun Alliance	Professional Negligence Management Protection (D&O) Employee & Third Party Fraud	No
Terrorism Policy	UMAL	Property reinstatement Contents Business Interruption	No
Travel & Personal Accident	RSA	All risk travel cover for Students, University Employees including those living and operating outside of UK territorial limits.	No
Fine Arts Policy	Blackwell Green	Cover for the Sarah Rose Art Collection.	No
Medical Malpractice	Newline Group	Cover for students and staff in practice placement based teaching or providing support for learning and assessment in practice settings	No
Special Contingency	AIG		No

3. UNIVERSITY EXPOSURE TO RISK UNDER 2018/2019 CLAIMS

3.1 Although unsettled claims were carried forward to 2019/2020 in the following All Risks categories – Public Liability (4 cases) and Employers Liability (2 cases) – the University carries no excess for these types of claim, so the insurer Zurich effectively carries all the risk exposure.

3.2 A full breakdown of claims for 2018/19 is detailed in Appendix 1

4. DECLARED LOSSES WITHIN POLICY EXCESS

4.1 The University is also required to declare to its insurers the incidence of insured perils which fall within policy excess and do not result in the submission of a claim.

4.2 There were no incidents falling into this category during 2018/19.

APPENDIX 1

LSBU POLICY WITH ZURICH MUNICIPAL NHE-01CA07-0013
CLAIMS SUMMARY - 1 AUGUST 2018 TO 31 JULY 2019

Insured risk	Excess Value	Claims brought forward from last period	New claims in this period	Claims carried forward to next period	Value of payments made on claims open in this period
Material damage	£20k	1	0	0	£138,527.80
Works in Progress					
Business Interruption					
Money					
Public Liability	Nil	0	4	4	£0
Employers Liability	Nil	2	0	2	£38,582.65
Libel & Slander					
Professional Negligence					
Governors Liability					
Motor					
Engineering					
Fidelity Guarantee					
Personal Accident					
Travel					
Computer					
Engineering inspection					
Fine Arts Policy					
Medical Malpractice					
Special Contingency					

APPENDIX 2

Employers Liability Claims Detail

Claim Number	Notification Date	Accident Date	Cause	Location	Description	Current Position	Total Outstanding	Total Paid	Total Cost
1153064414	05/08/2015	27/05/2015	Broken Bones - Supervisory	LSBU	FINGER CAUGHT WHERE 2 DOORS MEET	Claim has been statute barred (means they are out of time to do anything). Claim was settled on 10th September 2019	£35,878.00	£0.00	£35,878.00
1163064695	06/10/2016	04/10/2016	Other - Manual	LSBU	This is the result of an Employment dispute	Negotiations are ongoing between Clyde & Co and the other side	£3,625.00	£21,375.00	£25,000.00