ISC16D005

Title:	***Management of UEA IT Servers not fully within remit of ITCS Managed Service***
Author:	Iain Husband (ISD) / Ian Prior (ISD)
Date:	19 Sept 2016
Circulation:	ISSC 18th October 2016
Agenda:	ISC16A001
Version:	Draft
Status:	Open

Issue

There are a number of IT Servers across the University that do not fall fully within the remit of the Managed Service offered by ITCS. A recent audit of all servers across the University network highlighted significant data security risks that the Security Project is seeking to mitigate through its Faculty Housekeeping work stream. The support of the committee is therefore being sought in respect of the specific recommendations listed below.

Recommendation

Recipients are invited:

- To note the report.
- To support the proposal that, where practical, all current IT Servers be brought within the remit of a Managed Service offering and that all future requests for the provision of IT Servers are dealt with in the same manner. Work is currently in progress to fully define the nature and content of this managed service.
- To support the proposal that the cost of the Managed Service outlined above be borne by the Server Owner.
- To support the proposal that where, in extreme cases, ISD and the Server Owner cannot agree an appropriate plan of action for an existing IT server presenting security risks, ISD will need to remove the risk and remove that server from the University Network. This will only occur after contacting the SFMs and relevant Heads of School, highlighting the lack of response and seeking their sign-off.

Resource Implications

The project has sufficient resources in place for the remainder of 2016 to support the work required to mitigate the risks identified by the current Faculty IT Servers. Further analysis is currently in progress to ensure that the increased volume of Servers requiring support can be managed as part of day to day operational management within ITCS.

Risk Implications

There is a low risk that this work may disrupt service. There is a high risk of compromise and non-compliance with regulations to which the University is bound by not completing this activity.

Equality and Diversity

The proposal is not expected to have any impact on individuals with protected characteristics.

Timing of decisions

This work has been in progress for a number of months. The recommendations outlined are to assist the project in completing the work required in a timely manner.

Further Information

Contact for further information
Iain Reeman ICT Systems Director i.reeman@uea.ac.uk ext 2926
Phillip Ayers Information Security Manager p.ayers@uea.ac.uk ext 3994
Iain Husband IT Project Manager i.husband@uea.ac.uk ext 1247

Background

Work in hand under the IT Security project requires the University to undertake a more systematic, auditable and proactive approach to the management of its IT Servers. The IT Security project board wishes to gain ISSC support for the recommendations outlined. IT Servers operated outside of the Managed service offering pose a risk to the whole institution, and therefore the intention is to ensure that all UEA-owned systems are operated within this framework.

Why carry out this process?

Keeping systems as up to date as possible and secure is one of the most important tasks that should be undertaken by ITCS. With the increasing use of malicious code to exploit known vulnerabilities on IT systems and hardware, those who wish to can now infiltrate systems, cause malicious damage and carry out financial and data theft. All of which can have major implications of cost, business continuity and reputational damage to the organisation.

Along with the ever increasing threat from those with malicious intent, requirements around governance and regulatory compliance (e.g. PCI DSS, DPA) now emphasise the securing of all systems and monitoring them on a very regular basis, including the specific need to monitor for vulnerabilities and patch systems.

The full implementation of a Managed Service for all IT Servers connected to the University network and physically relocate or replicate servers into the data centres allows their maintenance and security monitoring against data breaches to be completed more effectively and efficiently.

The potential impact of breaching regulatory compliance includes:

- fines for non-compliance
- reputational damage to the University

In addition to fines that may be imposed if there were to be a data breach in relation to Data Protection Act, the Information Commissioner's Office may impose fines up to £500,000 (expected to rise to 4% of worldwide turnover under the General Data Protection Regulation (GDPR) replacing the Data Protection Act). Further losses will arise from compensation paid to each individual affected by the breach.

Proactively managing vulnerabilities of systems will help reduce the potential for exploitation and involve considerably less time and cost than responding after exploitation has occurred.

Discussion

Some owners of current IT Servers that are connected to the University network but located and maintained outside of a Managed Service are unwilling to commit to moving to it as associated costs of doing so have not been included in their budgets. A proposal that ISD consider offering a waiver of associated costs for up to a maximum of 12 months is currently under consideration but is not sustainable in the long term thereby giving rise to the requirement for Server Owners to make future budget provision. It is this long term approach for which we are seeking the support of the committee.

Some current IT server owners are failing to respond to our communications regarding their server(s), thereby preventing progress. We are therefore seeking the support of the committee in authorising the switching off / removal of servers from the network where a number of attempts to contact the owner have failed to produce a response or where an appropriate agreement on the actions required cannot be reached.