ISC16D035

Title:	**Data loss prevention**
Author:	Raymond Scott (ISD)
Date:	23 May 2017
Circulation:	ISSC 13 June 2017
Agenda:	ISC16A003
Version:	Draft v0.1
Status:	Open

Issue

The Information Compliance team in ISD handles personal data breaches on behalf of the University. Breaches are to be reported to the team without delay, and they are handled following a set procedure. Under GDPR (which will apply in the UK in May 2018), we are required to report more serious breaches to the UK data protection supervisory body, the Information Commissioner's Office, within a set timeframe (72 hours).

A common type of breach relates to misuse of email, where often information intended for one recipient is sent to another. Office 365 includes a standard data loss prevention (DLP) tool to reduce the chance of certain potentially sensitive or confidential data leaving the organisation, for example disclosure of credit and debit card numbers via email or OneDrive. (According to our PCI policies, we do not store cardholder data, and so there should be no legitimate requirement for anyone to share this type of information.)

While they will not remove the risk of email-related data breaches, the DLP tool will be of assistance to the University in reducing the chance of inadvertent disclosure, improving compliance, and educating users of University policies relevant to their actions.

The paper describes what the DLP tool is capable of and how the Information Compliance team intends to approach implementing it.

Recommendation

Recipients are invited:

- To consider the report.
- To approve the recommended approach.

Resource Implications

Configuration of DLP, monitoring and follow up actions would be undertaken by information compliance staff in the course of their day-to-day work. No additional resource is required.

Equality and Diversity

The proposed changes are not expected to have any impact on individuals with protected characteristics.

Timing of decisions

The tool is already available to the team. We are seeking approval for its use under particular circumstances. Once approved, the DLP tool will be configured for use across our Office 365 resources (email and filestore).

Further Information

- Raymond Scott (ISD), x3561, r.scott@uea.ac.uk

Background

The move to Office 365 for online email (Exchange) and filestore (OneDrive for Business) as well as other applications such as Skype for Business, OneNote, Sway, etc. presents the Information Compliance team with an opportunity to make use the built-in Security and Compliance Centre. This tool is designed to work with Office 365 and provides an organisation's compliance staff with tools they will need in their work. SPC has considered this tool and this document proposes how it might be used by them.

The tool is not expected to interrupt normal business activity, but will increase the chance of capturing poor practice and improving compliant behaviour before a data breach has actually occurred.

Discussion

DLP is quite sophisticated in the options available to organisations. To improve the match rate, the tool considers context for specific data types[1], and does not simply conduct a keyword search. It can be configured to look at sharing with recipients inside and outside the organisation. You can select which types of data to look for (e.g. passport numbers, NI numbers, credit card numbers). All these pieces of information have a defined structure which the tool can recognise.

When the tool finds a match, you can choose to block the action (i.e. stop the email being sent, with the option to allow a business override), offer a tip (popup message describing the issue, referring to local policy and asking the user to check before sending), or do nothing (which is useful when testing the rules).

The tool generates compliance reports which the Information Compliance team can use for monitoring purposes, follow up with staff, as well as management reporting.

Configuration

The tool will be configured as follows:

- Accept the predefined UK specific rule templates[2] created by Microsoft.
- Rules shall apply to data held in Exchange online, Sharepoint, and OneDrive for Business where that information is being shared outside the organisation.
- Rules shall apply only to data held by staff.
- The sensitive data types we are interested in are: credit card number, debit card number, NHS number, NI number, passport number, SWIFT code, driver's licence number, electoral roll number.[3]

Roll out of DLP

- Follow Microsoft's advice on the implementation of the policies.
- Initially run policies in test mode without tips (user messages) and examine the compliance reports for information on the policy performance.
- Adjust the policies if necessary to reduce the chance of false positives.
- Draft popup text relevant to UEA, and turn on tips.

Recommendation

ISSC are invited to authorise information compliance staff to use the DLP tool to reduce the risk of data loss for particular information types as described in this paper.

---

[1] https://support.office.com/en-us/article/What-the-sensitive-information-types-look-for-fd505979-76be-4d9f-b459-abef3fc9e86b

[2] https://support.office.com/en-us/article/What-the-DLP-policy-templates-include-c2e588d3-8f4f-4937-a286-8c399f28953a?ui=en-US&rs=en-US&ad=US

[3] Datasets containing the above data types should not be sent outside the organisation unencrypted, and some should not be sent at all.