DATA BREACH MANAGEMENT POLICY

External version including incident management plan

Last updated 9th May 2018

ROYAL COLLEGE OF MUSIC London

Introduction

Data breaches are becoming more common and can arise from a range of causes including malware or human error. As new types of technology are adopted with increasing frequency, this increases the range of ways data can be breached.

Aim

The aim of this policy is to standardise the RCM's response to a data breach and ensure its correctly logged and managed with best practice. It also to provide an overview of the RCM's Cyber Security Policy.

Definitions

A **data breach** can be defined as occurring when "personal data held by the RCM or on behalf of the RCM is lost or is accessed, modified, disclosed, stolen, or subject to any other interference".

Personal Data is defined as "any data about an individual who can be identified from that data".

Examples of Data Breaches may include:

- Sending information which is considered personal data to the wrong recipient
- Malware/Hacking attack
- Unforeseen environmental circumstances (Fire/flooding)
- Unauthorised access to data
- Lost data

Responsibilities

A range of people throughout the RCM have specific responsibilities for data use, management and protection. Key roles involved in managing information include:

RCM Council

RCM Council has overall responsibility for data protection and defines the College's data protection strategy, policies and risk appetite.

Deputy Director (Senior Information Risk Owner)

The Deputy Director is the RCM's 'Senior Information Risk Owner' with overall responsibility for information as a strategic asset of the College, ensuring that the value to the organisation is understood and recognised and that measures are in place to protect against risk.

Head of Departments / Line Managers (Information Asset Owners)

Heads of Department and Line Managers are responsible for the data held and used by their department, fulfilling the role of 'Information Asset Owners' to take responsibility for the data used and controlled by their team. Line managers are also responsible for their staff complying with policy and reporting of risks or actual data breaches.

Data handlers

Anyone who accesses university data has a responsibility to follow RCM policies and procedures for the use of data and to report any (suspected or actual) data breaches.

Additionally, data protection strategies are supported by the following individuals and teams:

Data Protection Officer (DPO)

An advisory role concerned with the RCM's compliance with data protection legislation, providing advice, assistance and recommendations to the Senior Information Risk Owner (SIRO) in relation to data protection risks. The DPO plays a key role in fostering a data protection culture within the RCM and helps implement essential elements of data protection legislation, such as the principles of data processing, data subjects' rights, data protection by design and by default, records of processing activities, security of processing and notification and communication of data breaches. The DPO reviews the planning, implementation and progress of the RCM's data protection initiatives periodically, reporting to Council. They advise the SIRO in relation to any breaches of data protection legislation, co-ordinate the response to data breaches, subject access requests (SARs) and Freedom of Information (FoI) requests, and act as the RCM's point of contact with the Information Commissioner's Office (ICO), reporting breaches to the ICO within the 72-hour deadline when required

Human Resources

The HR team ensure all staff complete GDPR awareness course which covers data breaches.

Technology (ICT)

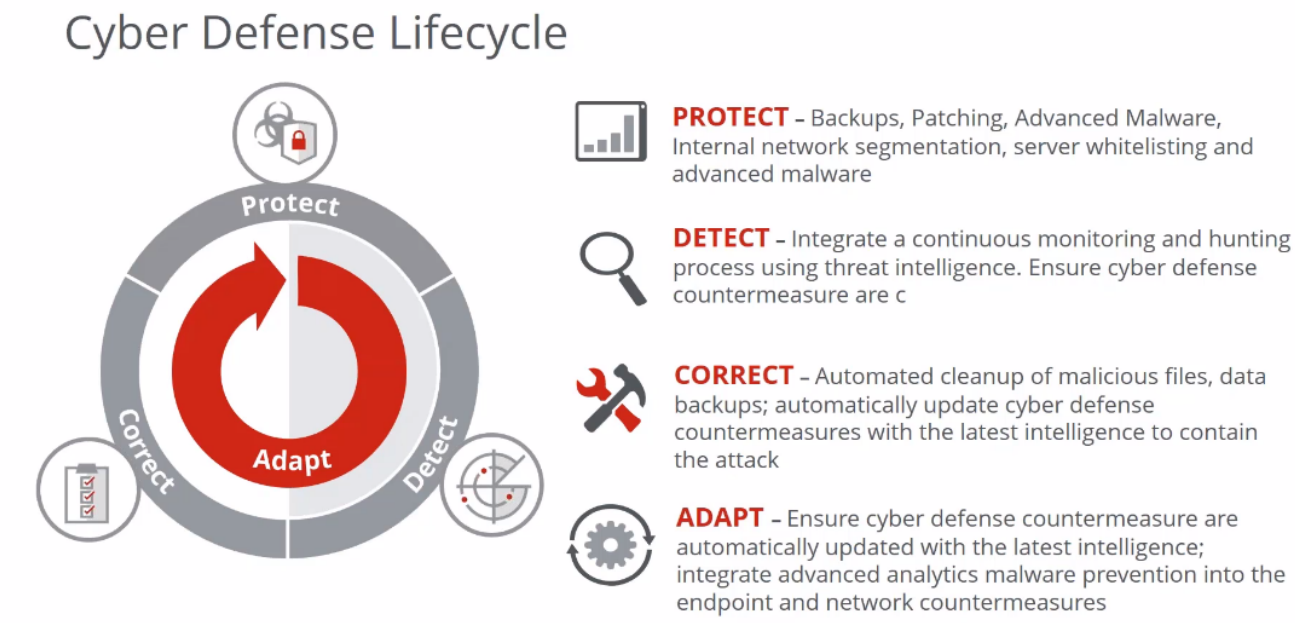
The Technology team within the RCM Digital department manage many of the technical processes associated with storing, managing and controlling data and play a leading role in preventing and responding to data breaches. Once notified of a data breach, the Technology team and DPO will follow the incident management plan and form an Incident Management Team.

Data Breach Reporting

Any suspected or actual data breaches should promptly be reported to the Technology Helpdesk via ICTHelp@rcm.ac.uk (with the title of DATA BREACH) and followed with a phone call to 0207 591 4388. This triggers a 72-hour window to report the breach to the Information Commissioner's Office (ICO) if required.

Appendix A – Cyber Defence Lifecycle

The RCM's data breach incident management plan is based on an industry-standard continuous circle of security improvement called the Cyber Defence LifeCycle. It uses the process of Protect, Detect and Correct to create a continuous cycle that allows a constant adaptation to new viruses and hacking attacks. This provides a model of continuous adaptation for the Technology team to follow as the cyber security threat landscape changes.



References

https://ico.org.uk/media/1562/guidance_on_data_security_breach_management.pdf