Crisis communications - reflection

1. Background & discussion points

1.1. We have had a crisis communications plan (CCP, available at imperialcollegeunion.org/crisis) in place for approximately 18 months, with infrequent real-life use since then.

1.2. A recent data breach incident led us to make use of the plan, giving us the opportunity to review its effectiveness in a real-life scenario around the following discussion points:

1.2.1. What benefits did the CCP bring to the situation?
1.2.2. What developments can be made to the CCP to make it more effective in future?
1.2.3. *What other lessons did we learn from this crisis situation?*

2. Data breach

2.1. On 15 February 2018 our Systems team first identified evidence that a malicious attack had taken place on a subset of our membership database. On 16 February further investigation revealed more detail of the breach, and we activated the CCP and convened a crisis response team (CRT), which I chaired.

2.2. The communication sent to all members affected by this data breach is at the end of this paper; it explains the issue and how it was addressed.

3. Reflection on the CCP

3.1. The *three steps* at the start of the CCP were useful to direct the matter to a member of the Strategic Management Group and to call for a crisis response team to convene. In this situation, the MD and the SMG member responsible for Systems happened to be off-site; however the clear instructions that a CRT was to be convened and that an SMG member must own it immediately clarified lines of responsibility.

3.2. The *checklist* was used explicitly to guide the discussion and to generate actions, which significantly aided the effectiveness of the CRT and confidence in its decisions. Participants commented that the focused nature of the CRT was very effective and reassuring, and that the only 'slowdown' in the process was on the part of College. Participants also noted that the CCP ensured that everyone reacted in a calm and professional manner, which I believe was important to minimising the effect of this data breach on the welfare of some colleagues.

3.3. The *stakeholder engagement guide* and contact details were not relied upon as the ICU staff members involved were already familiar with the relevant College figures and had good working relationships with them. However they would have proved useful had the task fallen to different officers and members of staff.

4. Future developments and lessons

4.1. As not all SMG members are always available, we should have full confidence that all members of SMG are familiar with the CCP and are able to convene and chair a CRT and execute the checklist. They should be able to do this for matters relating to any part of Imperial College Union, not just those within their directorate.

4.1.1. Recommendation: MD to ensure SMG are all familiar with CCP

4.2. In this matter, 'managing the crisis' and 'communicating the crisis' were broadly the same tasks. This will not always be the case, and we may lack institutional knowledge of how to manage a crisis and manage its communication when those two tasks are very different – for example, accidents, natural disasters or violence within our activities.

4.2.1. Recommendation: MD to continue exploring a crisis scenario to test incident management as well as communication

4.3. The CCP is not necessarily well-known to staff, and it is possible that without an SMG member involved early in the situation, one team may have attempted to handle the issue without applying the procedure. It later transpired that several senior staff were not aware of how to access the plan quickly.

4.3.1. Recommendation: HoSVC to reiterate CCP to all staff

4.4. **Communications Committee are invited to make further observations and suggestions.**

5. Communication to members affected by data breach

Dear <Name>,

I am writing to inform you of a data breach which occurred on 8 February 2018 when a malicious third party gained access to an Imperial College Union-controlled database containing student records.

Data associated with 267 members of Imperial College Union was extracted, including a limited amount of personal information – detailed below. You are one of those 267 individuals, and I wanted to ensure you were fully aware not just of the occurrence but the actions undertaken as a response.

Imperial College Union became aware of the breach on 15 February 2018 when it was discovered that one of our databases had been breached and some limited information pertaining to our members had been extracted. In line with College protocols, ICT Security were immediately informed and the platform disabled to allow a full diagnosis to occur, the breach to be contained and preventative measures implemented to prevent such actions being repeated.

It is our assessment that the attack did not originate from within the Imperial community and that it was not targeted at Imperial College Union or any of its members. The method used strongly suggests that this was an automated attack 'crawling' the web in general and searching for

vulnerabilities in databases in order to extract information that would later be reviewed to determine its value.

The range of information which was accessed is as follows, although the amount of information breached varies for each individual student, and in most cases it will be less than this full list. The data accessed was accurate as of <either 2014 / 2015 / 2018 dependent on data table accessed>.

- Full name
- CID number
- Faculty, department, programme and study year
- Hall of residence if applicable
- Date of birth
- Gender
- Global region of origin (using the United Nations geoscheme)

Following a review of the information breached, in partnership with College's Data Protection Office, we have found nothing to suggest that your personal information is at greater risk of being misused as a result of this breach. Please be assured that the database accessed did not contain any financial information such as bank details or National Insurance number and that Imperial College Union's membership database only holds information that is necessary for the effective functioning of the organisation.

Accordingly, whilst there are no actions that we suggest that you now need to take, if you become aware that any action adverse to you has been, or is being, taken as a result of this incident, please let us know as soon as possible.

I would like to take this opportunity to personally apologise for this occurrence and for any personal inconvenience caused to you. The trust of our members is important to Imperial College Union; if you would like to know more regarding this incident and how it relates to you specifically, please don't hesitate to get in touch.

Kind regards

Andrew Keenan