hpc health professions council

# Finance and Resources Committee 7 September 2011

## Report on HPC's Disaster Recovery test 27 May 2011

## Executive summary and recommendations

An interdepartmental disaster recovery exercise was carried out on 27 May. The report below indicates the progress of the test, the background scenario

**Decision**

The following report is provided to note.

Changes to the crisis management process will be adopted, and a "Tactical" team consisting of CDT and others, should continue to be involved to assist resolution of business issues.

See "Recommendations to Update the plan" page 8.

**Background information**
HPC's Disaster Recovery Plan

**Resource implications**
Requirement to continue to include additional employees in the testing of the plan will require accommodation within work plans

**Financial implications**
No long term costs, but some OPEX when running future tests.

**Appendices**
None

**Date of paper**
20 July 2011

# Interdepartmental Disaster Recovery Exercise Description and Lessons Learnt 27th May 2011

On Friday 27th May 2011 HPC held its annual exercise of the disaster recovery (DR) plan involving members of most departments, at the ICM Disaster Recovery centre at Sevenoaks, or ICM Uxbridge, dependant on their assigned role in standard recovery plans. Participants were forewarned, and asked to assemble in Sevenoaks or Uxbridge at 9:30 am.

Roy Dunn created the following scenario, having consulted Marc Seale, in advance of the test. The scenario was designed to be different from previous tests, focussing on the interaction and discussion between participants.

## The scenario

The HPC's Executive Management Team is having a final offsite awayday before becoming HCPC. They are in a hotel in Sevenoaks in Kent. Meeting room space and hotel rooms are booked for Friday afternoon and all day Saturday.

The exercise involved a serious and extensive case of data breach and potential loss through sabotage of a third party, the details emerging in stages during the day, see the Appendix to this report for details.

## The participants

The following met in the meeting room at the ICM's disaster recovery (DR) centre at Sevenoaks, Kent.

Anna van der Gaag (Council Chair), Charlotte Milner (CM)(Finance), Guy Gaskins (GG) (IT), Louise Hart (LH) (Secretariat), Greg Ross-Sampson (GRS) (Operations), Georgia Akuffo-Kumih (GAK) (HR), Sarah Oliver (SO) (covering both the Communications and Policy & Standards Departments).

Ruth Cooper participated via phonecalls from Park House

Richard Watling, James Wilson and James McMahon (IT) participated remotely from the ICM Disaster Recovery centre near Uxbridge, and successfully accessed the appropriate systems remotely. This is not covered in detail in this report, as this is highly similar to previous tests.

Marc Seale (Chief Executive) had intended to take part but was unable to do so due to illness. The Education and Fitness to Practise Departments were unable to send representatives.

Tom Berrie and Roy Dunn (RD) (Business Process Improvement), attended the meeting as observers, and to advise and take notes.

## The exercise

Participants arrived as previously instructed at about 9:30 am.

Also as previously instructed, members of EMT taking part did not bring their own copies of the Disaster Recovery Plan.

The meeting received the first item of information at 10:15 hrs;

**Message 1** Background 8 am Friday 9th March, 0 hours elapsed time

Marc Seale has a 30 second conversation with Richard Houghton in the lift, before leaving for EMT awayday.

Richard Houghton in conversation with Marc Seale – Stannary Street lift

The Registrations Department has seen a drastic fall-off of online renewals, and paper forms are coming in. This could be a problem if it continues as physiotherapists still make up HPC's largest profession.

There are the usual registrant complaints that the process is too complicated needing passwords that are difficult to use and Registrations has decided to run a weekend shift and a couple of evening shifts the following week to ensure a backlog does not build up.

The initial reaction was that this would not in itself be a problem and is budgeted for, and that Communications would issue a press release and other communications such as a quick mailout to registrants promoting the online renewal system, and get the Chief Executive and Chair to contact the professional body to assist in this.

However, on further reflection, it was agreed that a sudden, unexpected and drastic fall-off in online renewals actually meant that something more is going on and needs investigating. Also, are these more than the routine complaints and moans?

**Message 2** 4 hours elapsed time

Message to Guy Gaskins from Stackspace. Friday Noon

One of HPC's key suppliers Stackspace has been targeted by "Fight against the state", as it supplies services to Central and Local Government.

A Trojan has been introduced to the Stackspace network infrastructure to duplicate, export and then randomly corrupt any original, accessible data it can locate. To date the Trojan has only been located in the Manchester Stackspace infrastructure.

Currently there is no reason to believe HPC's data has been compromised.

The first action would be to ask the provider, Stackspace, for more details, ie what exactly was being targeted and what action they were taking. Given the scenario, the Trojan virus, would be new. GG commented that such Trojans normally targeted only on particular platform, usually Windows. It would not therefore target NetRegulate. If it were in the infrastructure, one would know more about it. The remedial action would likely be to shut down everything, depending upon the response from Stackspace, but keep the website up, because there is no confidential data on there.

Communications would put an item on the website informing registrants and potential applicants.  The Council Chair and Chief Executive would have to telephone the Chief Executive of the CSP to keep him informed so that he could inform his membership.  The renewal period for physiotherapists would need further extending.   At the same time, the number of phone calls from registrants wishing to renew would have started to increase considerably.  This and the increasing number of paper renewals would have implications for Registration staff.  The Department would likely take on more temps and GAK confirmed that there would be budgeted sums for an increase, though probably not the likely number needed.

LH in the middle of this received a simulated phone call from a News of the World reporter.  Normally, this would be answered in a previously agreed format by the Director of Communications herself.

**Message 3** 9 hours elapsed time

Stackspace message to Guy Gaskins, delivered via telephone 5pm approx;

Although the hosting site used by HPC has not been directly impacted by the Trojan, a mirror site run by the ISP has seen data corruption. It is not possible to take that “other” site off line, as it provides infrastructure for the UK Military, NHS trusts including Ambulance services and patient records. Shutting down the network would indirectly cause patient fatalities.

GG commented it appeared that HPC data was currently secure so there would appear to have been no loss of data.  However, the infection was now in a still wider environment and therefore the risk was still great.  However, if the Trojan was the same as a recent one allegedly produced by the US military against the Iranian nuclear project, the loss of data could have begun unnoticed three months previously.

There would likely now be more and more paper renewals coming in and in addition, HPC was still needing to prepare effectively for the absorption of the social work register.

An urgent, suitable, general press release would therefore be needed.

In this scenario, nobody in EMT, on Friday night in a hotel away from London would have their disaster recovery folders with them.  However, some would have access to the plan via their Blackberries.  The HR Director would attempt to contact any manager remaining at Park House, bearing in mind that this was now after 5:00 pm on a Friday evening.   All managers either there-and-then, or first thing Monday would need to hold group meetings to brief all staff.  However, there would be no problems in staff coming to work on Monday, unless the transport network were also affected.

At this point, it would be possible for a member of EMT who lived nearest to Sevenoaks to go home and get their copy of the DR plan.

RD, as head of Business Process Improvement (BPI) would now be contacted to go into Park House the following day to begin, with other relevant staff, a detailed and exhaustive check of all relevant programmes and all systems to see if there was evidence of corruption.  GG commented that BPI and IT would need to put a plan together to validate all data. The HPC system would need to be closed with no internet access, although the internet would still be running.

It was acknowledged that a number of key staff, such as the Head of Registration and other key Registration staff, but also key staff from all other departments, would likely be asked, during such an emergency, to work on Saturday.

GG commented that, typically, the corruption would either be

- random data across the file / database structure
- or
- the same data fields modified in each damaged record

There were several ways of beginning to tackle this.  One starting point would be to check the data on Council members, because these items of data were known and therefore could be checked through other sources.  Other known values would also be sought.

It was agreed that at this stage, there was still considerable uncertainty and so, although the HPC would need to issue communications, they would not need, at present, to say that much.  It would need to state that an "incident" had occurred, give assurances and that tests on data had already begun.

In any such emergency, the Chief Executive would need to keep the Chair informed as much and as early as possible.  It was commented that the current Plan stated that she would be informed "if appropriate" and agreed that this phrase be removed.

Staff would need now to investigate previous renewals, particularly the most recent, to see if the infection had indeed begun sometime before.  It could also affect other professions because of routine payments outside the renewal period.

CM commented that, in reality, if the data had been corrupted before and the Finance Department via direct-debits had started to collect money in noticeable amounts from the wrong registrants, there would have been a noticeable increase in complaints.

At some point now the Information Commissioner and CHRE would need to be informed of a likely "data breech".

GG stated that there was a likely recovery process which checked the logs on NetRegulate, recovered to six months ago and then repairing anything changed in the log. This would mean closing the online register temporarily.  To help in checking, it would also be possible to recall relevant archive boxes from DeepStore.

The Chair would now need to call an emergency Council meeting to confirm actions taken and proposed.

**Message 4** 28 hours elapsed time

Message to Greg Ross-Sampson from David Waddle – phoned in. Saturday lunchtime

A small paper fire has occurred in the Registrations area of the Stannary street building, after a weekend shift working on paper renewals with the ICR process.

The fire is out, and there is only damage to a small part of the floor, adjacent to the scanners used for ICR work. However a large number of paper renewal forms (several archive boxes full) have been destroyed. Up to 4000 unprocessed renewals have been destroyed in two archive boxes being used for storage.

*A Registration advisor that had gone to collect extra milk from the main kitchen in Park House put out the fire after discovering it. Slight burns to the hands and arms are not life threatening.*

Initial comments suggest the fire was caused by a small electrical heater overheating after being on too long. Fire Brigade had attended but now leaving.

The building has been secured by another employee, who was not on the floor at the time.

EMT are still on their awayday. They would need to check how much damage had been caused by the fire, including likely water damage from the fire services putting it out. The Registration Department would be transferred nextdoor, and PCs would be available, if necessary asking other “nonessential” staff to lend theirs temporarily. It was also important to ascertain whether the member of staff injured needed further assistance and make sure that HR were kept informed as to their condition.

**Message 5** 30 hours elapsed time

Message to Guy Gaskins from Stackspace. – via SMS Saturday 2pm approximately

The Trojan has now been identified in the server infrastructure in Slough where HPC data are hosted. It may have been present for some time (may be days).

HPC’s data have potentially been compromised. Latest thoughts on how the Trojan works indicate HPC’s data may have been duplicated. Any IT infrastructure connected to the Stackspace infrastructure is potentially compromised.

This was now technically a “data breech” and likely data-loss, and a designated member of staff would now need formally to inform the Information Commissioner.

GG commented that relevant departments such as Partners, Fitness to Practise and Education would be asked to begin “active look-ups” and validation of data. Some problems may have been picked up already. All relevant staff would be involved. There were currently no credit-card details in NetRegulate and so these could not be accessed or corrupted now. By March 2012, after which the scenario was envisaged, all bank account details will be encrypted. None of these items of data would therefore be open to abuse or misuse as they would not be available.

**Message 6** 32 hours elapsed time

Message to Guy Gaskins from Stackspace. – via SMS Saturday 4pm

The group “Fight against the state”, claim to have obtained large amounts of data, including some possible HPC registrant data. It is difficult to determine if this is just public register information or part of a larger dataset as some information may come from public stage FTP activity.

The information is part displayed on a website put up by the “Fight against the state” group, but could well be a trap to infect Police or government agency IT with further harmful content. (A honey trap set up by the anarchists)

IT staff would need to check the website concerned, although it was pointed out that the Government would have ensured that it was shut down relatively quickly. They would check the data using a laptop outside the network via a wireless connexion, then completely wiping and rebuilding, or discarding, the laptop.

**Message 7** 33 1/2 hours elapsed time

News item from IT News web site Saturday 7.30pm

Stackspace Inc, the US parent company have sold off its entire European assets and liabilities to ARPED, a Middle East based ISP start-up with very significant financial backing but presumably limited experience of running a highly available and secure infrastructure. Some in the IT press consider this an attempt (by Stackspace) to avoid massive financial liability resulting from the data losses suffered following the “Fight against the state”, attacks.

ARPED was a local service provider to Stackspace, in the Middle East based in Qatar, and claim to have been replicating Stackspace’s European data as a fail over site to Stackspace, for the last 9 months.

This was now an added, major problem as the data was now outside the EEA and, under the data protection legislation for the UK and EU required the HPC to ensure that the control of the data was adequate. This would in fact be very difficult to establish. Bircham Dyson Bell would need to be contacted as a matter of urgency for full legal advice. It could in fact be regarded, amongst other things, as “data theft” as the transfer and replication of data owned by HPC had been carried out without approval. To ensure that HPC could demonstrate that it was complying with the data requirements and legislation, it would need to take immediate steps to find an alternative supplier within the EEA and, immediately, block this ARPED site from holding any more HPC data and remove that which was already there.

GG commented that a permanent transfer would take about three months but that there were immediate, temporary measures which the IT Department could take to carry out the Stackspace function in house.

The Communications Director would need now to issue a further press release giving further updates and assurances, and possibly call a conference for relevant journalists.

It would be advisable for HPC to contact all other victims of this transfer, to produce a joint strategy in their response.

So far, there was still no indication that HPC could not continue with the transfer of the social work register in two months, on time.

It was acknowledged that the effects, such as greatly increased stress levels, on the "front-line" staff, for example in Registration, could be longer term and that provision for help and possibly counselling in this area would need to be considered.

**Final discussion and conclusions**

1. Whilst it was unfortunate that a number of members of EMT were not available to take part in the exercise, in the event, all who did were able to make a valuable contribution; and those who were delegated by their departments who would not otherwise have attended were given the opportunity to make important contributions.

   This also allowed CDT members, not usually included in tests to participate. This was a suggestion from previous years tests.

2. This particular exercise was essentially about the detailed, practical implications of such an emergency, and having participants who would be doing the actual work in such cases was in fact a bonus. It became clear from discussions during the day that if participants were allowed to think laterally, important suggestions and ideas would emerge, quite often from unexpected sources.

   The exercise drew clear attention to the need to be vigilant and look for unusual and unexpected changes, such as increased complaints that the online procedure is "very difficult" or "not working properly" or passwords they normally use suddenly do not work properly, that direct debits are being collected from the wrong people, or that an unusual number of registrants' addresses are suddenly wrong. These are "triggers" for an investigation.

   The communications dimension is vital if registrants, the public and Ministers are to retain their confidence in the HPC as an organization. Good communications between departments is also vital.

   It is important to recognise and locate the balance between openness and discretion in such very sensitive cases. Regular assurances that HPC is dealing with the situation are vital, provided they are reasonable and believable.

3. It is also important to recognise that, in any emergency and under the inevitable durance it brings, mistakes will be made. The important principle, as in English law, is that you do what is reasonable and adequate under the circumstances, provided you set out your reasons.

4. As suggested at the end of the 2010 exercise, it was recommended that exercises for individual departments be organized as well, for example for the Communications Department or the Cross Department Team. The Communications department will have two test periods in this financial year.

5. A number of participants for the day felt that Friday was not an ideal day, particularly the Friday before a Bank Holiday. However, the need to schedule between other planned activities constrained the dates available for testing. [November has been suggested as a better time for the 2012 test, date to be published with other key HPC dates at the start of the year.]

6. It would be useful to have a short document available which would give the current cash and cash-flow situation, so that in emergencies, management could immediately assess what is currently available. [Finance will determine what information can be provided that is useful. A suggestion was a weekly snapshot sent to Blackberry users in the Business Continuity group]

7. Throughout discussion, the emergency use of temps came up several times. In future, it would be helpful if HPC has one or two “preferred” agencies to draw upon immediately in the case of emergencies and which HPC managers and HR know are reliable.

8. In respect of IT, it is now a basic principle not to rely upon one back-up only. Monthly physical back ups (on tape) are stored long term securely off site. Restoration of data would be possible as long as the tape drive equipment are available and tape degradation has not occurred.

**Scenario information to be supplied at the start of the test.**

HPC’s EMT are having a final offsite away day before becoming HCPC. They are in a hotel in Sevenoaks in Kent. Meeting room space and hotel rooms are booked for Friday afternoon and all day Saturday. Spouses and partners are attending on Saturday night, funded directly by EMT members.

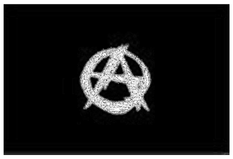
HPC’s current largest profession the Physiotherapists are in an extended renewal period after 2 months of postal strikes, and the Social Work register is about to be transferred in approximately 3 months.

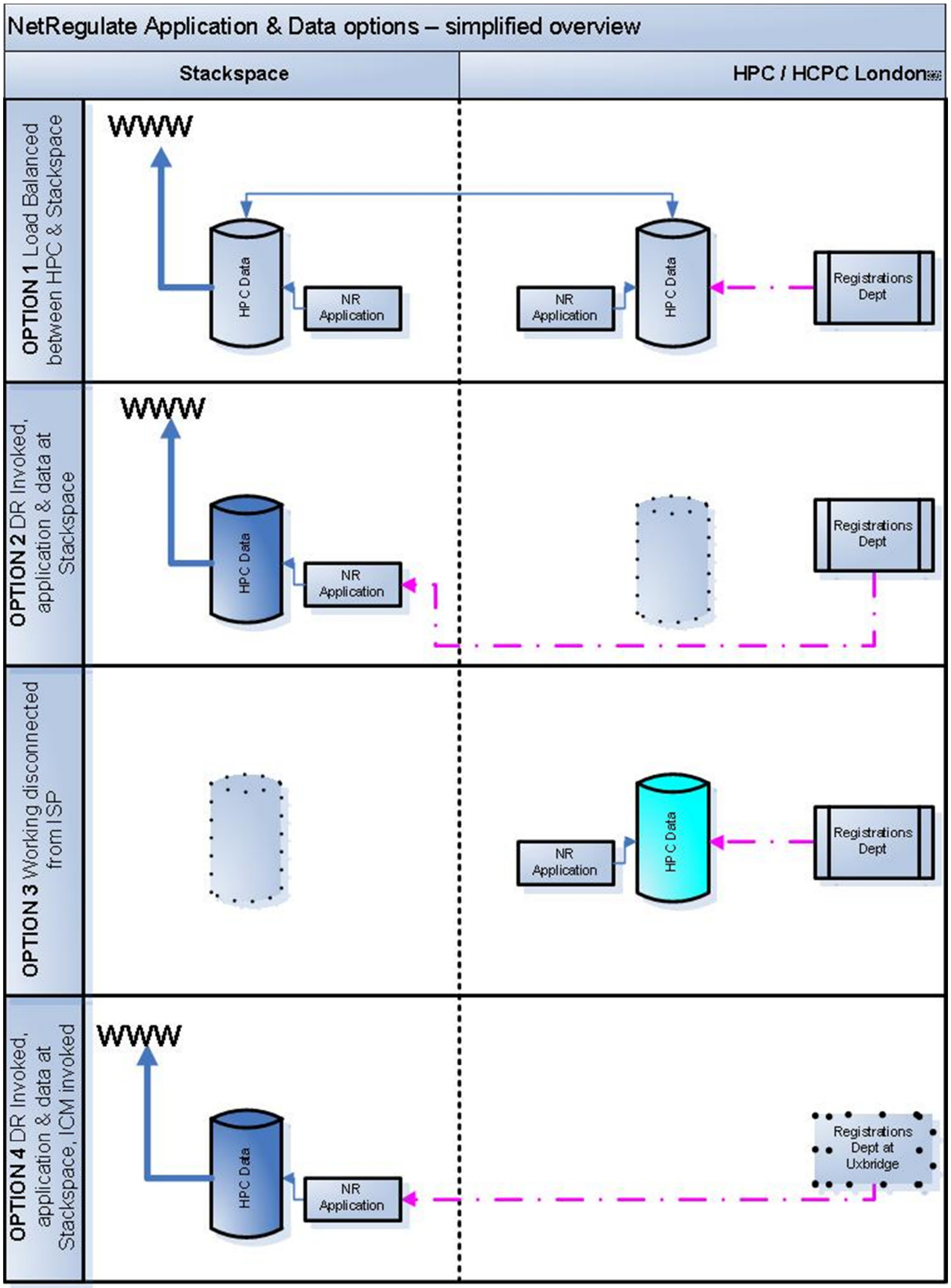
Cost savings by Central Government, including redundancies are in the press, and HPCP has been highlighted as a way in which the work is being redistributed to lower cost operations whilst still in the UK. UK unemployment stubbornly sits at just under 3 million. Even the IT sector has contracted, leaving tech savvy people sitting on the “dole”.

As the UK runs up to the Olympics in summer 2012, the re-elected Mayor of London announces that the London infrastructure is ready for anything, anti-terrorism measures are in place, traffic flows for athletes and dignitaries are guaranteed, although a late winter snap with snow and ice may require remedial work to the outdoor running tracks.

In the same vein, Central Government have promised a smooth Olympic experience, for overseas visitors, maximising the opportunity to earn foreign currency, helping pay off the national debt incurred fighting the banking crisis 4 years ago.

This proves to be too much of a target for “Fight against the state” a break away group of tech savvy political anarchists.




NetRegulate Application & Data options – simplified overview
Stackspace
HPC / HCPC London
OPTION 1 Load Balanced between HPC & Stackspace
WWW
HPC Data
NR Application
NR Application
HPC Data
Registrations Dept
OPTION 2 DR Invoked, application & data at Stackspace
WWW
HPC Data
NR Application
Registrations Dept
OPTION 3 Working disconnected from ISP
NR Application
HPC Data
Registrations Dept
OPTION 4 DR Invoked, application & data at Stackspace, ICM invoked
WWW
HPC Data
NR Application
Registrations Dept at Uxbridge

Option 1 = e.g. day to day operations – normal working

Option 2 = e.g. operations in week following power outage in November 2010

Option 3 = e.g. untried, and expensive to test or simulate, in reality only likely to be considered if ISP's were under attack (eg Wikileaks & Anonymous, December 2010)

Option 4 = e.g. May 2010 BCM test

SCENARIO STARTS
Message # 1 Background 8am Friday 9th March, 0 hours elapsed time

Marc has a 30 second conversation with Richard in the lift, before leaving for EMT away day.

Richard Houghton in conversation with Marc Seale – Stannary Street lift

The registrations department has seen a drastic fall off of online renewals, and paper forms are coming in. This could be a problem if it continues as Physiotherapists still make up HPC's largest profession.

There are the usual registrant complaints that the process is too complicated needing passwords that are difficult to use and  Registrations have decided to run a weekend shift and a couple of evening shifts the following week to ensure a backlog does not build up.

Message # 2 4 hours elapsed time

Message to Guy Gaskins from Stackspace. Friday Noon

One of HPC's key suppliers Stackspace has been targeted by "Fight against the state", as it supplies services to Central and Local Government.

A Trojan has been introduced to the Stackspace network infrastructure to duplicate, export and then randomly corrupt any original, accessible data it can locate. To date the Trojan has only been located in the Manchester Stackspace infrastructure.

Currently there is no reason to believe HPC's data has been compromised.

Message # 3 9 hours elapsed time

Stackspace message to Guy Gaskins, delivered via telephone 5pm approx;

Although the hosting site used by HPC has not been directly impacted by the Trojan, a mirror site run by the ISP has seen data corruption. It is not possible to take that "other" site off line, as it provides infrastructure for the UK Military, NHS trusts including Ambulance services and patient records. Shutting down the network would indirectly cause patient fatalities.

Message # 4 28 hours elapsed time

Message to Greg Ross-Sampson from David Waddle – phoned in. Saturday lunchtime

A small paper fire has occurred in the Registrations area of the Stannary street building, after a weekend shift working on paper renewals with the ICR process.

The fire is out, and there is only damage to a small part of the floor, adjacent to the scanners used for ICR work. However a large number of paper renewal forms (several archive box fulls) have been destroyed. Up to 4000 unprocessed renewals have been destroyed in two archive boxes being used for storage.

*A Registration advisor that had gone to collect extra milk from the main kitchen in Park House put out the fire after discovering it. Slight burns to the hands and arms are not life threatening.*

Initial comments suggest the fire was caused by a small electrical heater overheating after being on too long. Fire Brigade had attended but now leaving.

The building has been secured by another employee, who was not on the floor at the time.

Message # 5 30 hours elapsed time

Message to Guy Gaskins from Stackspace. – via SMS Saturday 2pm approximately

The Trojan has now been identified in the server infrastructure in Slough where HPC data are hosted. It may have been present for some time (may be days).

HPC's data have potentially been compromised. Latest thoughts on how the Trojan works indicate HPC's data may have been duplicated. Any IT infrastructure connected to the Stackspace infrastructure is potentially compromised.

Message # 6 32 hours elapsed time

Message to Guy Gaskins from Stackspace. – via SMS Saturday 4pm

The group "Fight against the state", claim to have obtained large amounts of data, including some possible HPC registrant data. It is difficult to determine if this is just public register information or part of a larger dataset as some information may come from public stage FTP activity.

The information is part displayed on a website put up by the "Fight against the state" group, but could well be a trap to infect Police or government agency IT with further harmful content. (A honey trap set up by the anarchists)

Message # 7 33 1/2 hours elapsed time

News item from IT News web site Saturday 7.30pm

Stackspace Inc, the US parent company have sold off its entire European assets and liabilities to ARPED, a Middle East based ISP start-up with very significant financial backing but presumably limited experience of running a highly available and secure infrastructure. Some in the IT press consider this an attempt (by Stackspace) to avoid massive financial liability resulting from the data losses suffered following the "Fight against the state", attacks.

ARPED was a local service provider to Stackspace, in the Middle East based in Qatar, and claim to have been replicating Stackspace's European data as a fail over site to Stackspace, for the last 9 months.