

UMAL NEWS

WINTER 2011

Beware Hack Attacks

Ben Beeson, Partner, Global Technology and Privacy Practice, Lockton is an expert in 'cyber' liability risks and insurance. His article below for UMAL brings us up to date with current issues and complements the mutual's current review of available coverage for its membership.

The much publicised 'hack attacks' suffered by Google mail (Gmail), cyber warfare allegations made by the US government against China, and the ongoing problems facing the Sony Corporation linked to malicious data breaches of its PlayStation network all clearly demonstrate the prevalence of cyber theft and the little understood phenomenon of cyber warfare.

The upshot is that cyber crime in all its guises is here to stay. With so much sensitive information accessible on the internet, and many customers, firms and services allowing remote access to this information, cyber criminals are spoiled for choice. Tools and techniques vary, but as hacking becomes more

sophisticated so the threat has spread from individual hackers, through criminals working in organised gangs to governments testing the security of other countries' networks. Even those with no malicious intent can pose a threat, and the risk of basic human error – failing to follow protocols to encrypt data or losing laptops or data sticks – is all too common.

The laws governing data breach are multiple and complex. In Europe the legal right to privacy is highly developed, and all EU member states are signatories to the European Convention on Human Rights, where article 8 provides the right to respect for "private and family life, home and correspondence" subject

to certain restrictions. EU member states must transpose the directive into national law in time and some have already done so. Other countries are still considering what steps to take.

Notifying customers

Notifying customers of a data breach is not cheap and is estimated in the UK at a minimum of £10-£20 per affected person, the average breach being £1.7M.

Continued on page 4.



AGM reports

8th December 2011

UMAL

Following the completion of his first year as Chairman, Allan Guest commented at the recent AGM that he believed the mutual would be able to reward loyal Members in what he acknowledged was a difficult financial climate. With financial performance in 2011 showing a further growth in Members' funds and importantly a refund of contributions to members, he added that "there is no doubt in my mind that the mutual concept as a working successful shared service model will be an enduring testament to the Members' intention to keep public funds within the public sector."

He continued, "We are well positioned to support Institutions in a partnership

approach to risk management appraisal, advice and solutions giving valuable control over future pricing."

Allan also welcomed two new Directors to the UMAL Board. They are Alison Holmes, Director of Procurement at Durham University, and Carolyn Pike, Director of Legal Services at the University of Birmingham. Hari Punchihewa, Deputy Chief Executive at the University of Derby, was re-elected.

UMSL

Alison Holmes, Carolyn Pike and Graham Gilbert, Director of Finance at the University of York, join the UMSL Board for the first time and Hari Punchihewa was re-elected.

UMSR

Chairman Michael Yuille announced he was standing down, having served on the Board since 2005 and as Chairman since 2006. In his chairman's remarks Michael said that the mutual continued to offer cover and pricing which was second to none and the Board had achieved a dual success - the mutual was cost efficient and members' funds were protected. Jon Gorringer, Deputy Chairman, proposed a vote of thanks on behalf of the Directors and members expressed appreciation of the leadership and drive provided by Michael during his term of office. Richard Cryer, Director of Finance at the University of London, Senate House, joins the Board for the first time. Jim Bradshaw, independent Director, and Bernadette McLellan, Insurance Manager at the University of Cambridge, were both re-elected.

Leadership is vital in business continuity planning

Leadership is critical in preparing for business critical situations, Paul May, Chairman of Concordia, told the UM Open Forum.

Mr May, whose company provides claim and risk consultancy services for the insurance industry, said: "There are two things which are important. Firstly, without the top people on board you might as well forget it. The second thing is, whatever the plan says, when the time comes, just do it."

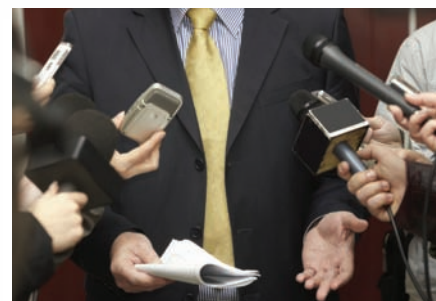
He said once an incident has happened, it is often necessary to get people in from the outside as back up, and capture everything that has happened on film, so there is no dispute later.

Preparing the media spokesperson is another important part of disaster communications.

"The organisations that do well are the ones that have chosen their spokesperson ages before. It's no good to have just a couple of hours of media training, you need to spend a few weeks in the radio or television studio to get it right," he said.

He also recommended using templates for statements, so that they can be produced as quickly as possible.

"Look through every contract you have. You are going to have uninsured losses, everybody does, so see what you can get back. Generally speaking, don't try to keep the status quo, go up. You can always improve on your



preparation for disaster situations.

"Get some satellite phones. A lot of disaster plans rely on a phone cascade, and then become meaningless when the phones don't work. Get better first aid equipment and train first aiders, because if it is a disaster, ambulances won't be providing a full service," he said.

For more information about Concordia visit www.concordiaconsultancy.com

Olympic Security Management

James Lewry of Control Risks provided an overview of material considerations and the evaluation of risk factors directly arising from Olympic and Paralympic hosting in 2012.

Drawing on Control Risks' understanding of the threat environment, he pinpointed the following: reviews of the control measures around accommodation, processes and physical assets; contingency planning and the security of personnel. He added that it was extremely important to ensure that all plans are "fit for purpose" and was at pains to highlight the ever more complex world of protecting people, assets and reputation.

Campaign and protest groups could be a likely cause of disruption at the London Olympic Games and there is concern that the torch relay could be a focus for protest groups as it had been during the Beijing Olympics.

"There is also a high risk of criminal activity. There are potentially rich pickings from visitors who don't know the area," he said.

Terrorist activity is always an issue at international events, and it was the Mumbai style of attack, with small arms and explosives, that caused the most concern. On the plus side, he said, the UK was arguably very well prepared with police teams in place for a rapid response.

Mr Lewry said that in several public surveys carried out recently, there was a wide gulf between perceived and actual threat. Terrorism was high in most respondents' perception as a threat, but in reality was one of the least likely to occur.

High on the list of Control Risk's client concerns surrounding the Olympics was security of venues, strain on the transport system and the NHS and having adequate evaluation and contingency planning.

There was also concern about the availability of security resources, for example temporary security fixtures and personnel. Some institutions were already training up students as temporary security guards.

The safety of guests, athletes and their families was paramount, and it is important for institutions to have a crisis management communications plan and a security plan in place.

"In reviewing your security plan, the first thing to do is to identify stakeholders. These can be the national Olympic committee, local



authorities, your suppliers, the emergency services, the athletes, student unions and department heads," he said.

"You then have to identify your responsibilities, such as the duty of care to the athletes' families.

"Be realistic with security measures. Cameras don't prevent events, they just record them. The most effective actions are changes in practices, which are far better than expenditure on security measures," he said.

"You should recognise that the games are coming and you should start security planning now," said Mr Lewry.

For more information visit www.control-risks.com

Representatives from Universities and Colleges gathered at the UM Open Forum in Tavistock Square, London, in October to hear from a selection of experts in risk and disaster management about how to prepare for the London Olympics and deal with the challenges of any unexpected events.

Protecting reputation at a time of crisis

Jonathan Boddy, Director of media training company Positive Impact, said it was vital to plan ahead as the best way to protect your reputation at the time of an incident.

"Your reputation is a very valuable facet of your organisation. A good reputation might well lower your insurance premium and help you as an organisation to present a lower risk to an insurer, but it goes beyond that," he said.

"Do people trust you? Will they do business with you? Will they give you a second chance if something goes wrong or will they walk away? Managing the media and the process of media communication at the time of a major incident is a vital step in maintaining your public reputation and the public confidence you need," he said.

Mr Boddy said the "first and golden rule" of dealing with the media is that planning and preparation is absolutely essential.

"The first step is to get the senior management team involved and supportive of the process. Only if that support exists, right from the very top down, can meaningful preparation move forward. Clear leadership is vital during incidents."

Once senior managers are on board, the departmental heads have to go through a

threat analysis process.

"Some threats are obvious, a fire, a building collapse, a death on campus, a shooting, a drug ring, financial impropriety, loss of a major investment, personal scandal with a member of staff, discovery of a terrorist ring, the list goes on.

"The 2012 Olympics adds another dimension; food poisoning to an Olympic team traced back to your venue, an assault upon or by an athlete, a terrorist attack against a team, political protest against a team or commercial sponsor."

The next step of the planning process is to consider who would be interested in your incident, and to identify these groups: students, other universities, staff, suppliers, contractors, emergency services, the local authorities, hospitals, insurers and many others.

Once an incident is underway, Mr Boddy said the important thing was to start communicating early and keep the messages coming out, even when there is not much to

say. The fact that you are engaging with the media shows them that you are concerned about the incident and are doing everything possible to resolve it. However, the rise of technology means that we are all journalists now and stories have value; preparedness to respond quickly is vital.

He said an organisation should plan to have a written response to media inquiries sent out within 15 minutes of an incident occurring. This would take the form of a brief paragraph confirming an incident had happened, where it happened and that more information would follow. A news statement within one hour, 85% of which can be pre-prepared, plus legal sign off should be the aim as emergency services will already be speaking to the media by that time.

It is important to follow this with a statement from "a talking head" confirming positive facts - the nature and time of the incident, and that the incident is being taken seriously, responded to appropriately and that thoughts are with anyone affected by the incident.

"There are five key principles in disaster media planning and response. Involve the people at the top of the organisation, have a simple and flexible plan in place, start communicating early and keep communicating, highlight meaningful action, and always put people first," said Mr Boddy.

For more information visit www.posimp.co.uk or contact jon@posimp.co.uk

Access and information is key in disaster situations

Access was one of the main problems loss adjusters came up against following the 7/7 attacks on the London transport network in 2005.

Graham Burgess, UK Technical Director of loss adjusters GAB Robins UK was involved in dealing with the aftermath of the attacks, and subsequent discussions between the Association of Chief Police Officers, the Chartered Institute of Loss Adjusters and the Association of British Insurers to establish new protocols to deal with future post crisis situations.

He told the UM Open Forum meeting that he had seen similar access problems in the

aftermath of the summer riots this year, in which information was a key issue.

"The areas affected can be enormous. In the 2005 attacks we needed an early understanding of where the police cordons were because businesses were being pressed for a time of interruption and an estimate of the cost of closure whilst customers and staff could not reach them. These cordons were being moved all the time so we had to send chartered loss adjusters to walk the streets and try to establish some sort of pattern as to how wide the interruption was," he said.

"There was a paucity of information, so the talks between ACPO, CILA and ABI were about developing a protocol to address these issues. One thing that emerged from the



meetings was that the emergency services had no easy system of prioritising which premises were key to business recovery," he said.

"There are some very real risks, but there is no doubt that in the aftermath of a situation like this, information is key," he said.

For more information visit www.gabrobins.co.uk

Beware Hack Attacks *Continued from page 1*

Fines add further to costs with the UK government able to impose up to £500K on any entity breaking its data protection legislation.

From May 25th 2011 a new European e-Privacy Directive came into force imposing more restrictions on entities operating online. These include a requirement of Internet Service Providers (ISPs) to notify customers of a data breach and encourage 'voluntary notification' for all other data controller companies. It is likely that further regulation will be imposed across the EU in the future.

Causes of breaches

Looking at how data breaches come about can provide some clues to risk prevention. Research has revealed that human error and systems glitches collectively account for around 75% of UK data breaches. But it is the 24% caused by malicious or criminal activities that tend to be the most costly.

Basic IT security measures like encrypting sensitive records when in transit and on mobile devices can significantly help reduce the risk of sensitive data falling into unauthorised hands. Other good risk management practices include: allocating IT security responsibility to an accountable individual; regular external testing/auditing of IT security effectiveness; achieving certification to an approved security standard.

As technology solutions evolve, entities which store sensitive customer data online must ensure they have robust contingency plans in place to deal with a data breach. All

eventualities need to be addressed in terms of where, who and to what purpose.

Insurance solutions

To assist, cyber insurance solutions are starting to become available, designed to offset some of the costs associated with data breaches. Coverage is an evolving area but it is possible to obtain cover for the full range of risks faced. London has been particularly proactive in developing cover against reputational harm and first party network business interruption caused by viruses, denial of service attacks, and administrative and operational errors.

Cover can be tailored to the entity's needs and can be extended to the emerging issue of cyber extortion including threats to data or networks and where a ransom is demanded. Other possibilities are data breach response and privacy regulatory action defence costs.

Ultimately, though, there is no easy solution to the risks associated with a data breach and no organisation is immune to malicious attack or human error. And, with the rapid growth of electronic commerce, including online trading, the use of social networking, and the potential cost savings of cloud computing and the like, the risks continue to grow. As legislation increases, so cyber risk is set to continue to top emerging risk lists for some time to come.

Individual risks must be assessed very carefully. Senior buy-in, support for contingency planning and appropriate risk mitigation programmes are essential as the hackers are out there and are usually one step ahead.



UM Security Information Service

London 2012 Olympics and Paralympics

To give U M members the best information possible on security management and live issues during the 2012 games the mutuals are partnering with Control Risks Global Security and providing a facility whereby security updates will be provided to Members during the run up to and for the duration of the games.

This is information which will be focussed on London and the UK, but includes world-wide coverage to automatically address alerts involving hosted teams' countries of origin.

This will be available via the UM web page and 'live' alerts to nominated contacts at the Members' universities and colleges who will receive sms alerts and security information and updates. Members can also contact the Control Risks global security desk for information and advice for their institution and for individuals if they are caught up in adverse events or problems. Once this goes live early in 2012, passwords and full access information will be issued from the UM offices.

This is a crisis management 'fall back' analysis and support facility; lower level information will be issued in addition to high level security messages providing a useful update on activity as well as warnings of issues.

UMAL Members get free Business Continuity Review

Since its launch earlier this year a number of institutions have enjoyed the benefit of the Strategic Review of Business Continuity which is available free to UMAL members.

The review is carried out on behalf of UMAL by specialist business continuity advisers Jermyn Consulting.

George Hall, senior consultant with Jermyn, said: "The Strategic Review is designed to compare an institution's current business continuity capability with actual requirements and recognised best practice.

"By doing this we are able to provide the institution with an effective gap analysis and a prioritised implementation plan for

improving business continuity. We have experience of working with almost 40 Universities and Colleges so have developed a realistic benchmark based on the realities of the higher education sector."

Susan Wilkinson, CEO of UMAL, commented: "The Strategic Review is an ideal way for members to gain a clear understanding of the key business continuity issues they face. The review is as relevant to organisations that are just starting their business continuity programmes as it is for those with more developed systems and procedures".

For more information about this service or to book a review please contact Richard Gillham on 020 7847 8677 or by email richard.gillham@umal.co.uk.



7th Floor, Hasilwood House,
60 Bishopsgate, London EC2N 4AW.
Tel: 020 7847 8670 Fax: 020 7847 8689
Email: susan.wilkinson@umal.co.uk