# Considering Cyber-insurance

“Cyber-insurance” is an idea that has been around for a long time but its appearance in standard insurance products is a much more recent phenomenon. Universities are increasingly dependent on networked computers and data across all their activities: research, teaching, knowledge transfer and administration. In many cases damage to those systems – whether accidental or deliberate, internal or external in origin – could do significant harm to the organisation. Threats are increasing as both fraudsters and vandals discover how they can use the internet for their purposes. Universities are not immune.

So should universities consider cyber-insurance?

To think about that it’s worth splitting the question into three:

* What sort of risks does insurance cover, and are they things that are high on your risk register?
* If one of those incidents does happen, is a money payment (which is what insurance policies generally provide) going to be useful in making your position better?
* Are there other ways you could deal with those risks, and how do their costs/benefits compare?

Insurance is normally used for low-likelihood, high-impact events where it’s hard for potential victims to do much to reduce either likelihood or impact themselves. So we insure against major storms, fires, thefts or accidents because, while statistics tell us those events probably won’t affect us, paying a regular insurance premium is more palatable than having to deal with them unassisted if they do. While some of the events that might affect our computer systems are indeed serious and rare, many are relatively minor and occur daily or weekly. Insurance probably isn’t the best way to deal with users clicking on the wrong attachment or giving up their password to a successful phishing attack.

Recent reports on cyber-insurance from the perspective of [businesses](http://www.computerweekly.com/news/2240202703/An-introduction-to-cyber-liability-insurance-cover)[[1]](#endnote-1) and [law firms](http://www.businessinsurance.com/article/20150330/NEWS06/150339979)[[2]](#endnote-2) suggest that it is most often used to cover costs incurred under data breach notification laws. If personal data are exposed as a result of an incident and organisations are required to notify affected individuals then there are obvious financial costs including postage and, if bank or credit card details were affected, maybe paying for credit monitoring reports as well. An insurance claim payment might well help with those. If the affected organisation needs to use external consultancy to investigate an incident or propose remedial measures then, again, the incident will result in an unplanned expense. It’s possible that universities might suffer that kind of breach and costs, though preventive approaches such as PCI DSS can reduce both the financial and reputational risks, and may reduce premiums.

However the articles also suggest that insurance can be used to transfer the risk of liability to third parties when paid hosting services suffer incidents such as website defacement. Incidents affecting university services seem likely to result in more reputational than financial harm, so an insurance payment would do less to solve the problem. As the articles note, some of these events may already be covered by existing liability and professional indemnity insurances. Having an effective incident response plan to minimise the impact of incidents may be an effective alternative approach.

When insuring against real world events insurance companies are likely to reduce claim payouts, or even declare policies invalid, if the insured person didn’t take sufficient care to avoid the incident. Thefts where a door has been left unlocked or accidents where a car wasn’t properly maintained are obvious examples. [Court cases already demonstrate](http://www.itgovernanceusa.com/blog/data-breach-cyber-insurers-wont-cover-stupid/)[[3]](#endnote-3) that cyber-insurance policies, too, will have limitations and exemptions. This could be an opportunity for cyber-insurers to influence the adoption of good security practices by way of their minimum requirements. In some cases improving security practice may even reduce the risk to a level where insurance is unnecessary.

Finally, it’s worth noting that cyber-insurance products are sufficiently new that there haven't yet been many policies taken out, or claims made under them. That probably means that neither purchasers nor insurers have much data on what the actual risks are, so policy prices are less likely to reflect the true risk/benefit balance than for other, better understood, areas of insurance [Sarah Clarke has an [excellent discussion of this](http://infospectives.co.uk/2015/04/02/cyber-insurance-is-like/)[[4]](#endnote-4)]. That situation may be even worse for universities, as insurers' data are likely to reflect commercial businesses where IT operations and risk calculations may be very different to those in Higher Education. If you are considering such insurance you may get a better deal by limiting it to areas of operation that are most similar to businesses, so where the pricing is more likely to be accurate. And look for areas where claims have resulted in pay outs, rather than court cases.

A [recent report by Marsh](http://uk.marsh.com/Portals/18/Documents/UK%202015%20Cyber%20Risk%20Survey%20Report-06-2015.pdf)[[5]](#endnote-5) found only 18% of organisations were confident they had a “complete understanding” of their cyber-risk: not a good position when considering how insurance might help. Even if universities do better than that, the biggest benefit of thinking about insurance may well be to improve awareness and understanding of the full range of risks and possible mitigations: what can universities themselves do and where do they need external help. Insurers may have some role in universities’ risk management, but internal risk reduction measures are at least as important and may well have wider benefits.

Things to consider:

* What are your main risks arising from information and communications technology?
* Does insurance exist for them and how much would a claim payment reduce their impact?
* What would you need to do to qualify for insurance (under a new or existing policy)?
* Would those (or other) mitigation measures reduce the risk sufficiently on their own?

***\*\*\****

*Our thanks to* ***Andrew Cormack****, Chief Regulatory Adviser at Jisc, for producing this briefing paper. Andrew works to keep Jisc and customers of the Janet network informed about the legal, policy and security issues around networks and networked services.*

1. <http://www.computerweekly.com/news/2240202703/An-introduction-to-cyber-liability-insurance-cover> [↑](#endnote-ref-1)
2. <http://www.businessinsurance.com/article/20150330/NEWS06/150339979> [↑](#endnote-ref-2)
3. <http://www.itgovernanceusa.com/blog/data-breach-cyber-insurers-wont-cover-stupid/> [↑](#endnote-ref-3)
4. <http://infospectives.co.uk/2015/04/02/cyber-insurance-is-like/> [↑](#endnote-ref-4)
5. <http://uk.marsh.com/Portals/18/Documents/UK%202015%20Cyber%20Risk%20Survey%20Report-06-2015.pdf> [↑](#endnote-ref-5)