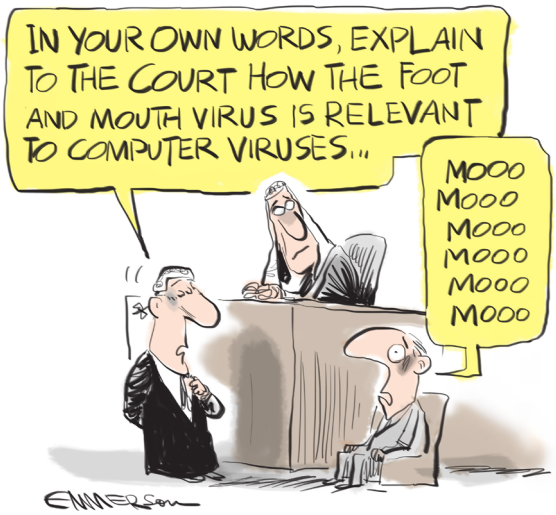
What Foot and Mouth can teach us about cyber security

Speed read

The threat of a digital computer virus is a world apart from the ravages of Foot and Mouth disease. Or is it? In a 1966 negligence case, the Foot and Mouth virus escaped from a UK research institute and infected neighbouring cattle. The institute was found to owe a duty of care to the affected farmers.

We think the same principle would apply to modern companies that allow digital viruses to escape and infect "neighbouring" users. The law of negligence often proceeds by analogy and here's a last century analogy for a modern time digital issue.



Below, we outline how negligence principles work in practice, and why it's so important to ensure that cyber security measures are up to industry standards.

The General Counsels of the UK's top 100 companies recently published a report about cyber security, which we discuss in an article here. We think their recommendations are a good representation of industry practice, which informs the standard of care required of commercial entities as to digital threats. The risk of a claim for negligence is one facet dealt with in that report.

April 2015

The Detail

The year is 1959. The Foot and Mouth Disease Research Institute of Surrey, England, has just imported a new virus from Africa for experimental purposes.

The virus escapes, cattle neighbouring the Institute become infected, and the Minister of Agriculture is forced to temporarily close the Guildford and Farnham markets to quarantine the disease.

The market closures (which lasted for 6 days in all) did not please the local auctioneers, Weller & Co, who were unable to carry out cattle auctions during this period. Weller & Co decided to claim for financial losses by suing the Foot and Mouth Institute under the law of negligence.

The court found that, if the virus were to escape from the Institute, it was a foreseeable fact that neighbouring cattle could die.[1] The Foot and Mouth Institute consequently had a legal duty towards the owners of neighbouring cattle to take reasonable care to prevent the disease from spreading.

In the case of Weller & Co, however, their relationship with the Institute was too remote to create such a duty. The auctioneers' claim for financial loss was dismissed.

What Foot and Mouth can teach us about cyber security

Why is Foot and Mouth relevant to cyber security?

Imagine a more modern situation. The year is 2015. A company with inadequate cyber security has managed to attract a deadly computer virus. The virus spreads, infecting the company's internal network and online systems. A few hours later, the company goes into digital lock-down to prevent the disease from spreading.

Unfortunately, the damage is done. The virus has already infected the systems of sub-contractors, personal devices used by employees, business contacts, website users, and thousands of other third parties.

To whom does our fictitious company owe a duty of care under the law of negligence?

If such a case were to unfold, the court's approach would likely involve applying the same sort of legal principles relied upon last century, well before cyber threats even existed.

Under the law of negligence, a duty of care is owed to another party where there is "*a sufficient relationship of proximity*" that an act of carelessness by the defendant will likely cause them harm.[2]

The rule is problematic in the context of viruses and other electronic threats. It is quite reasonable to hold that there is "*a sufficient relationship of proximity*" between any two entities who exchange digital information, or in the case of an internet website, to extend a duty of care to everyone who visits the site. For a large company, this could result in thousands, or even millions, of potential claimants.

Equally, the courts are cautious about imposing a degree of liability which is so wide as to be indeterminate. There may be policy considerations which justify limiting the scope of a duty of care, such as the extent to which victims could reasonably have protected themselves, or that the defendant is only liable if it had (or should have had) specific knowledge about the harm other parties would suffer.[3]

Note that a claim for pure financial loss is certainly possible under the law of negligence (and is the most likely harm caused by a computer virus).[4] The reason Weller & Co did not succeed against the Foot and Mouth Institute was because their relationship was too distant to create a duty of care, not because the type of claim was invalid. Will the same rule apply to a computer spreading a virus to third parties beyond direct contacts?

To be clear, this 50 year old case is not the full answer on cyber security negligence liability, for the law of negligence has evolved since then. A full answer to a particular scenario involves more detailed review of up to date cases, etc. But it remains a great illustration of how the law works in this area.

What standard of care must a company exercise to avoid negligence liability?

Where a duty of care is found to exist, we move to the second consideration: the defendant must also have failed to exercise a reasonable standard of care. The required standard will generally take account of best practice in the relevant industry, and the nature of the particular virus.

It also adjusts to the conduct and expertise of the defendant. For companies which profess to be IT experts, or rely heavily on digital use as part of their business, the standard of care expected of them will be higher.

What best practice experts and standards on cyber security say should be done will guide what is the required standard of care. That does not require perfection, as no system can be 100% immune from problems.

While courts are willing to consider the difficulty of taking necessary precautions, that is unlikely to be a compelling argument here, as the threat of a computer virus is both widely known and relatively inexpensive to prevent (compared to the risk posed).

Also important is that the obligation to uphold a standard of care is "*an obligation which keeps pace with the times. As the danger increases, so must… precautions increase*".[5] Relying on virus protection software is an insufficient precaution if it is not regularly updated.

What this means in practice

Much like the Foot and Mouth Institute in 1959, modern businesses have a legal obligation to protect their "neighbours" from the threat of viruses. In practice, this means taking care to ensure cyber security measures are up to industry standards.

1. *Weller v Foot and Mouth Disease Research Institute* [1966] 1 QB 569, QBD.
2. *Anns v London Borough of Merton* [1978] AC 728.
3. NZ Law Commission "Electronic Commerce: A guide for the legal and business community" (1998), Chapter 4: the law of torts.
4. *Hedley Byrne & Co Ltd v Heller & Partners Ltd* [1964] AC 465.
5. *Lloyds Bank v Railway Executive* [1952] 1 All ER 1248.

Wigley+Company
PO Box 10842
Level6/23 Waring Taylor Street, Wellington
T +64(4) 472 3023 E info@wigleylaw.com
and in Auckland
T +64(9) 307 5957
www.wigleylaw.com