Legal Aspects of Cybersecurity

June 2016

This paper summarises cybersecurity law issues presented at the New Zealand Society Cyber Law Legal Conference held in early 2016. If you are interested in further content from the conference see the NZLS website.

Read the full article below.

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

LEGAL ASPECTS OF CYBERSECURITY

LEGAL ASPECTS OF CYBERSECURITY

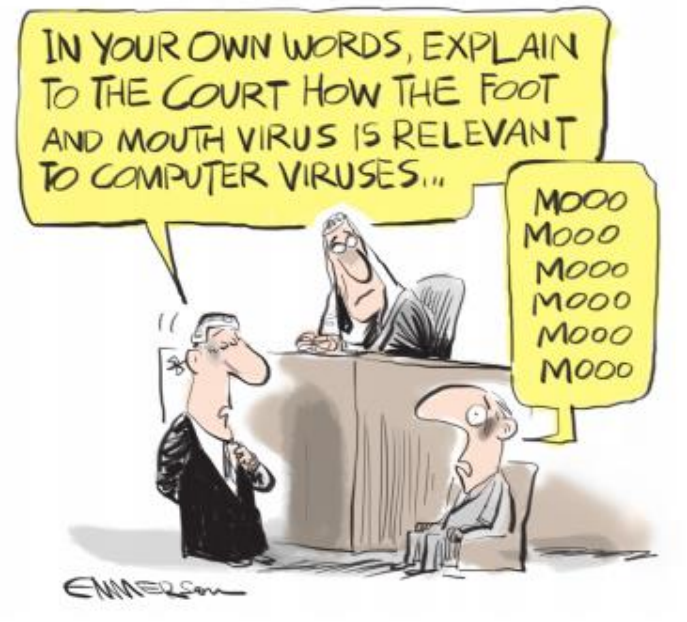
Michael Wigley
Wigley and Company
Wellington

Introduction

This paper summarises cybersecurity law issues. See some of our online articles for more detail.[1]

Our paper supplements the other two for this session and deals with the issues in the following order:

- What is cybersecurity from a lawyer's perspective?
- Overview of the types of legal exposure and the legal standard of care. This links to an appendix showing why foot and mouth disease in a piggery back in the 50s is relevant to the law of cybersecurity. A case study of a recent high profile cyber breach, looking at what happened both when the cyber breach hit, and then, 3 months later, after the company took remedial action. Plus the same company had another breach this year, raising the problem of exposure via suppliers. There's quite a few learnings from the story.
- We address fence-at-top-of-cliff issues as well as ambulance-at-bottom. The TalkTalk situation shows how a cyber breach can require very difficult decisions within hours. This is no time for possums in headlights



[1] Lessons for NZ boards in Juniper scare http://tinyurl.com/jatez65 - What John Greaves' predicament teaches us about cybersecurity obligations http://tinyurl.com/zoqfgnr It could happen to you http://tinyurl.com/z9hxox9 - Most boards breach cybersecurity legal obligations http://tinyurl.com/z2nefzj What should directors do about planning for a cyber breach? http://tinyurl.com/jhkthof Cybersecurity silver linings in clouds for directors http://tinyurl.com/zlb6vqs - Harvard Business Review: Cyber security is a bigger GC, board, CEO and CFO issue http://tinyurl.com/op2yswu The Internet of Things – ramping up privacy and security considerations http://tinyurl.com/mm3989d

and ready-to-go and experienced strong internal and external teams need to be able to move quickly.

- We outline a pragmatic approach to help de-risk companies from a legal point of view: what we call a "defensive shield", picking up on some work in the UK.
- Overviewed is the position of directors and their legal responsibility as to cybersecurity.
- We add a postscript on a significant issue: how hackers can find it easier to get at companies via their legal advisers than by a direct attack on the company.

What is cybersecurity?

We'll use a UK report, which links cybersecurity to lawyers, to illustrate this.

One methodology for lawyers as to cybersecurity is that of the so called GC100, which is the association of general counsel and company secretaries working in the UK's FTSE 100 Companies.

The report is *Cyber security law and practice*. It is designed to help in-house lawyers deal with cyber security risk, ranging from privacy and other regulatory law to the law of negligence and as to confidential information. It works for the public sector too. While it is focussed on the UK and EU, the principles broadly apply elsewhere. They have a legal model based on a "defensive shield" for the company, designed "to protect an organisation from regulatory actions and litigation."

As the report says, cybersecurity is a wide ranging issue, relevant across all the organisation:

> "Cyber security is concerned both with the security of cyber space and the security of entities that use or rely on cyber space. For these purposes, cyber space includes:
>
> - The internet and the world-wide web.
> - The facilities and apparatus that underpin and connect the internet and the world-wide web (for example, telecommunications, internet access and internet service provision).
> - The facilities and apparatus that support the provision of content available through the internet and the world-wide web.
> - The facilities and apparatus that support data processing and data storage accessible through the internet and the world-wide web (for example, cloud computing services and the supporting infrastructure, such as data centres).
> - High profile organisations that have endured damaging publicity for cyber security failings, including falling victim to cybercrime, include eBay, Home Depot, Target, JP Morgan Chase, UPS and Apple."

GC100: Why does cyber security worry senior managers?

The report lists the issues as:

> • "Insecurity, if publicised, can damage business brand and reputation and can degrade customer trust.
>
> • A serious incident can lead to significant business interruption or degradation of services.

• Senior executives are likely to "carry the can" for failure more frequently in the future." Senior managers and the public have increased awareness for reasons that include:

• "Frequent news reports about cybercrime and cyber security problems such as:

  • hacking;

  • malware distribution;

  • denial of service attacks;

  • "social engineering" exploits (for example, phishing and pharming); and

  • state-sponsored surreptitious gathering of IP and commercially sensitive information from businesses.

• Concerted government campaigns to increase awareness of the subject matter.

• Regulatory activity to boost cyber security in key areas of the economy (for example, in the telecommunications, financial services and health sectors).

• Root-and-branch legislative reform processes nationally and internationally.

• Edward Snowden's disclosures about the surveillance of systems and networks and data gathering by the US and UK intelligence services."

GC100: What are the legal concerns for business around cyber security?

Again, quoting from the report:

Cyber security raises many legal concerns for business because:

- Companies may be subject to primary legal duties to be "cyber secure" (for example, under Data Protection [aka privacy] law or through the tort of negligence).
- The fulfilment of secondary legal duties may require a state of cyber security (for example, equitable duties of confidence can be accompanied by parallel legal duties for security through the tort of negligence).
- A state of cyber security may be expressly or impliedly required by:
  - contract (perhaps as a condition of doing business, or being qualified to participate in bids and competitive tenders); or
  - due to professional obligations (for example, as part of the Solicitors' Code of Conduct).
- Achieving an appropriate state of cyber security may require the taking of measures that interfere with other legal rights (for example, employee monitoring and vetting may interfere with the right to privacy)."

We turn now to the legal standards required of companies in managing cybersecurity.

Standard of care required of companies as to cybersecurity

A good place to start is IPP5 in the Privacy Act as that is a useful starting proxy for liability more generally:

Principle 5

Storage and security of personal information

An agency that holds personal information shall ensure—

> (a) that the information is protected, by such security safeguards as it is reasonable in the circumstances to take, against—
>
> (i) loss; and
>
> (ii) access, use, modification, or disclosure, except with the authority of the agency that holds the information; and
>
> (iii) other misuse; and
>
> (b) that if it is necessary for the information to be given to a person in connection with the provision of a service to the agency, everything reasonably within the power of the agency is done to prevent unauthorised use or unauthorised disclosure of the information.

This highlights three points:

1. The level of cybersecurity is what is *reasonable* in the *circumstances* (the more sensitive the information, the more care is needed).
2. Another key liability area is tort (eg negligence) and that also entails a reasonableness standard. We have illustrated the analysis of the tort of negligence causes of action in the Appendix below, *What Foot and Mouth can teach us about Cybersecurity*. Ditto duties of directors given Companies Act duties on them based on an objective reasonableness standard.
3. When, as often happens, the information is given to third parties, the agency cannot do a Pontius Pilate: it still has duties based on a reasonableness standard. IPP 5(b) also helps sharpen the focus on the key risk arising out of cyber breach via suppliers' systems.

There are other causes of action too, beyond privacy (both in tort (including privacy tort actions where the law is evolving) and under the Privacy Act) and negligence causes of action. For example, there are duties of confidentiality, and duties arising out of industry specific regulation such as the Financial Markets Conduct Act.

And here's a trap as to the company's contracts: A company may promise its customers that "We will keep your information secure" which is a legally enforceable 100% contractual commitment, quite different from "We will take reasonable steps to keep your information secure." That is not to say the commitment is not made, but it better be made, knowing the risk given 100% security is not possible.

Then there's off-shore legal risk too.

Those caveats on that reasonableness point shows that legal analysis calls for much more focus than just checking if there is a "reasonable" approach to security.

What is required for a "reasonable" standard?

Reasonableness does not require perfection and cybersecurity steps should reflect the risk as to the particular system and information. Best industry practice will be highly relevant in determining the standard of care that is required, as are industry standards, guidance and so on. That's one reason why there needs to be coordination between, at least, cybersecurity specialists and lawyers.

Teamwork and thinking like a pirate, not a Navy captain

Cybersecurity is not something for lawyers to do in a silo, just as CIOs shouldn't do so. This is a multi-disciplinary area for CEO, ICT, Legal, HR, finance and so on, plus the board too.

Additionally, cybersecurity is not something that fits neatly solely in risk registers and matrices. Says very experienced cybersecurity specialist, Michael Wallmansberger, Chief Information Security Officer at Wynyard Group:

> Working in security requires a certain mind-set (thinking like an attacker; non-linear thinking); the ability to apply a set of well-known (but not always well understood) security principles and patterns; a comprehensive understanding of the underlying technology that makes up the secure systems; and an ability to work across the business on multi-faceted issues including with the CEO and the CFO.

There's a useful Harvard Business Review article that makes similar points, entitled, *See Your Company through the Eyes of a Hacker*.[2]

HBR points out, when suggesting that companies should make security part of their mission:

> The prevailing approach to security is compliance-focused, cost-constrained, peripheral to the core business, and delegatable by C-suite leaders. Working on a team like that isn't fun inside any enterprise, and it loses against 21st-century adversaries who know that it's more fun to be a pirate than to join the Navy. Any defense is only as good as the people doing the defending. The new model of security needs to be about mission and leadership, ensuring that we have the best defenders up against the best attackers. Security is no longer delegable, and the mission of security teams must be synonymous with the mission of the company.

The HBR piece has some great tips for Boards and senior managers. The article's focus on "turning the map around" applies the military strategy of getting inside the mind of the enemy, to see the situation as they do, in order to prepare for what is to come. For example, companies tend to focus IT security in limited ways, says the article, opening up ways around the sides. The "turning the map around" focus would include, in the words of the article (but explained there in much more detail):

- Understand your major risks and how adversaries aim to exploit them
- Take inventory of your assets and monitor them continuously.
- Make security a part of your mission.
- Be active, not passive, in hunting adversaries on your network and removing them.

[2] 24 March 2015

Case study – TalkTalk is hacked – in three phases

The First Phase- October 2015

Late in October 2015, TalkTalk, a UK Telco, announced that up to 4 million customer details, including credit card information, may have been hacked (a few days later TalkTalk said that in the end this was limited to 156,000 customers). The breach was basic and could easily happen to any firm.

In the first few days, TalkTalk responded with some flat feet.

The fallout for TalkTalk included:

- Share price dropped 27%.
- Loss of 95,000 of its broadband customers since the breach was reported.
- It came out that this was the second unrelated major breach in a year.
- Remedial costs of £60M.
- The UK equivalent of the Privacy Commissioner criticised TalkTalk for not notifying it sooner. (Although the delay was only a few hours, it was talked up in the media and it's hard to avoid the impression that TalkTalk's transgressions were talked up overall, beyond the reality: but this is the real world in which companies have to operate).
- Press reports that scammers had phoned customers and, by pretending to be TalkTalk staff and leveraging off credit card details, persuaded them to part with large sums. (In fact the actual position may be that little has been lost but that didn't stop early days' press such as the widow whose husband recently died of cancer said to have been scammed out of £15,000).
- The company faced extremely difficult judgment calls in the first few hours on when to release information publicly, when the information on what had happened was sketchy and there were differing perspectives (for example, the Police asked them to defer announcing the breach).
- The ages of the UK based people arrested in relation to the hack are 15 to 20, illustrating the range of potential hackers.
- The Daily Telegraph and other media have focused on the crisis and that's fuelled the problem for TalkTalk. For example, the Telegraph reported:

> Several customers have come forward to say that TalkTalk ignored them after they rang the company in recent weeks to warn them that they had been contacted by suspected scammers.
>
> Paul Moore, an information security consultant with Urity group, said he had warned the telecoms giant about its security problems last September.
>
> TalkTalk had changed the way it processed credit and debit card payments, but it reportedly ignored his concerns about a lack of encryption.
>
> Mr Moore said usernames and passwords for email accounts were not encrypted, making them accessible to data breaches, despite the firm's chief executive's office assuring him that "we are squeaky clean on security".
>
> TalkTalk now admits that "more should have been done" and apologised for the "worry and frustration this attack has caused our customers.

And this happened where cybersecurity was a big issue for the board. All that happened, even though cybersecurity was an item at every board meeting and that over the 9 months up to the breach, the board had three in-depth cybersecurity sessions. And that's a level of focus that is unusually high for a New Zealand board. By an order of magnitude.

That highlights that:

- There is no fool proof solution to cybersecurity;
- Planning for breach is critical.
- It will be important to make sure there is sufficient management focus on the right things instead of – as experts say happens too much – spinning wheels on the wrong things (one option but not the only one is for the board to get advice); and
- Boards are increasingly strongly concerned about cybersecurity risk. Boards in turn will, or should, drive compliance in their companies. In a series of articles,[3] we have outlined why it is essential, to meet legal obligations, for the board to have a close focus on cybersecurity, based particularly on Companies Act requirements. A board, by its documented attention to cybersecurity, may avoid directors' liability: for the TalkTalk board, that may have eliminated directors' liabilities as to a company that some pundits thought might go under due to the cyber breach. Of course, every board wants to see their company prosper, but it's also right to take steps to protect themselves against personal liability. The by-product is that the company is less likely to have problems, for a mere going-through-the-motions approach won't get the board off the hook.

Planning for a cyber breach

When the CIO or a reporter phones the CEO, the CIO or the Chair to say there's been a cyber breach, that's not a great time to learn how breaches work and what to do about them. Nor is it a good time for the company's internal people, and external advisers such as comms, legal and technical, to upskill in this area. They must hit the ground running, as a team.

This is not just a commercial and reputational issue: it is a legal duty issue too.

Good plan. Good people. Reduce company's (and directors') legal exposure.

For example, as the Australian equivalent of the Privacy Commissioner pointed out in October:

> All entities should have a data breach response plan. Your actions in the first 24 hours after discovering a data breach are often crucial to the success of your response. A quick response can substantially decrease the impact on the affected individuals.

Talk to experts in the field and they'll say the same thing. Michael Wallmansberger notes:

[3] Lessons for NZ boards in Juniper scare http://tinyurl.com/jatez65 - What John Greaves' predicament teaches us about cybersecurity obligations http://tinyurl.com/zoqfgnr It could happen to you http://tinyurl.com/z9hxox9 - Most boards breach cybersecurity legal obligations http://tinyurl.com/z2nefzj What should directors do about planning for a cyber breach? http://tinyurl.com/jhkthof Cybersecurity silver linings in clouds for directors http://tinyurl.com/zlb6vqs

> Cyber incidents are analogous to fire. A well-drilled evacuation plan should prevent loss of life and serious injury if fire breaks out in a modern building. However, unless adequate fire suppression systems are in place and fire trucks are ready to respond, fire may still cause significant economic damage. In cyber security, a good plan will minimise the worst impacts, for example the damage to reputation that comes with appearing uncoordinated and ill prepared. However, a response plan cannot entirely compensate for inadequate protective security controls or limited response capability.

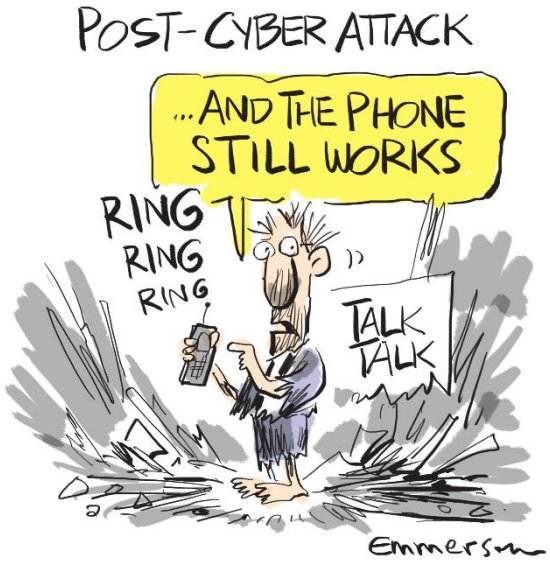
Says Anna Kominik, a specialist in crisis comms, (who presents the IOD's course on Leading through a Media Crisis):

> Be clear on roles and responsibilities, to connect the internal/business continuity with the external/ reputation management in a pressured and time poor environment, where companies and boards are often working with partial information. The plan needs to be kept up to date (for example, cyber security issues change frequently) and road tested. Four out of five business leaders expect their companies will experience a media crisis in the next year, but barely half have a plan to deal with it. Crisis can put board members in front of the media and the public in a way they never anticipated. The best advice to boards is 'have a plan', not just for cyber breaches, and make sure they've practiced it.

TalkTalk – The Second Phase: 3 months later

Fast forward to TalkTalk's January quarterly briefing to the market for the fourth quarter: the quarter when the First Phase problems occurred. Despite those problems, the brand is in fine shape as TalkTalk worked through the problems carefully. It overcame some of the flatfooted steps at the outset, aided by expert assistance from cybersecurity specialists. They've recovered some of the losses, financially and reputationally and even improved the company's reputation and brand. But being better prepared would have stopped some problems and sped up recovery.

Half a million customers took up a free upgrade offered as a retention sweetener by the telco. The briefing also confirmed that independent external research shows that customers perceived the company handled the problems honestly, openly and could be trusted, in the interests of the customers. So much so that the rating for honesty and trust is even higher than it was before the breach happened. As a challenger telco up against the incumbents like BT, TalkTalk is even pushing its branding overall as acting openly and honestly for customers against the bigger players. This goes to show how cybersecurity integrates with the broader picture, as it does with comms, HR, IT, legal.



So the TalkTalk CEO predicted a bright future financially. Quite a change from a few months earlier when some pundits predicted the company might collapse.

The Third Phase: Another problem at TalkTalk

But TalkTalk will need to be careful not to have too many more incidents. As it happened, another problem did crop up around the time of the fourth quarter briefing, although it hasn't caused too much grief for TalkTalk … yet. What happened is

that some customers – not many it's said – who had visits to their homes by TalkTalk engineers, got follow-up calls from people who had full details of those visits. The caller got the customer to load TeamViewer on their computers, the customer of course thinking the caller was a genuine TalkTalk person. That's the sort of software most of us are familiar with, that tech support use to fix problems remotely on our computers. The caller then tried to make financial transactions using the remote access.

Wipro, a major multi-national Indian outsourcing company, which provides services in New Zealand too, provides call centre services to TalkTalk and three of its India-based employees have been arrested in connection with this breach. This is an example of the importance, of ensuring cybersecurity is sufficiently robust at the company's suppliers too: that is the IPP 5(b) issue described by Katrine. That's a legal issue for both the company and its board.

Closer to home

According to Aura Information Security general manager Peter Bailey, it's not just international companies that should be putting cyber-risk on the agenda. The automation of attacks, the global nature of hacking and the ability of hackers to make cold hard cash out of their activities combine to make every business a target. It is therefore necessary for every company to prioritise information security and take reasonable measures to ensure safety.

> Mr Bailey: "Information security (InfoSec) should be a standard practice along with the many others necessary to run a good operation. The New Zealand IoD's Cyber-Risk Practice Guide provides a framework to help boards monitor cyber-risk, develop strategies for seeking assurance and to oversee management. As we have outlined in the articles referred to our introduction above, the IOD Guide is likely to be a pivotal document in assessing legal liability."

The legal 'defensive shield' for cybersecurity

The GC 100 has a legal model based on a "defensive shield" for the company, designed "to protect an organisation from regulatory actions and litigation." The model works well for companies and their senior managers and boards. It's defensive in the sense of reducing risk and being able to respond quickly to a cyber breach. And it's defensive in reducing litigation risk in the event of parties being sued.

A Footnote – Cybersecurity weak points in Law firms

Law firms can be juicy places for hackers to dig up their clients' confidential information, ranging from IP and patents to M&A information (thereby getting around the company's own cyber security defences). US and UK data shows a fair bit of activity, as IT industry reporter, The Register, outlines in its 16 April 2015 article, *Miscreants rummage in lawyers' silky drawers at will, despite warnings*.

For example, the article reports that at least 80% of the largest law firms in the USA have been involved in breaches since 2011.

That's a heads-up for both companies and law firms. Companies with great security might see their confidential information walking out via another back door. Similar issues arise too as to other external advisers such as accountants and consulting firms.

In the UK, the equivalent of our Privacy Commissioner – the Information Commissioner – warned lawyers to be careful around data security.[4] Plus the English Law Society issued cloud computing guidelines for solicitors.[5] Those guidelines have been picked up by our own Law Society in *Practice Briefing: Cloud Computing Guidelines for Lawyers*.

The Register, in the article above, noted that 173 UK law firms were investigated last year by the Information Commissioners (although we expect quite a few will not be IT breaches, eg, they would include paper based breaches). Raised are issues such as encryption, use of Dropbox, cloud computing, etc.

A recent Bloomberg article, *Cyber Attacks Upend Attorney-Client Privilege*, gives useful examples of attacks in the US and what law firms and their clients are doing about it, especially at the big end of town:

> Many Wall Street banks, including Bank of America and Merrill Lynch, typically require law firms to fill out up to 20-page questionnaires about their threat detection and network security systems. Some clients are even sending their own security auditors into firms for interviews and inspections.

[4] '*Information Commissioner 'sounds the alarm' on data breaches within the legal* profession' (2014) Information Commissioner's Office.

[5] *'Practice note: Cloud computing'* (2014) The English Law Society.

Appendix: What foot and mouth can teach us about cybersecurity

Overview

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 from a legal perspective.

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.[6] 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.

Why is Foot and Mouth relevant to cyber security?

Imagine a more modern situation. The year is 2016. 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.

[6] *Weller v Foot and Mouth Disease Research* Institute [1966] 1 QB 569, QBD.

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.[7]

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.[8]

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).[9] 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.

[7] *Anns v London Borough of Merton* [1978] AC 728
[8] NZ Law Commission "Electronic Commerce: A guide for the legal and business community" (1998), Chapter 4: the law of torts.
[9] *Hedley Byrne & Co Ltd v Heller & Partners Ltd* [1964] AC 465

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".[10] 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.

[10] *Lloyds Bank v Railway Executive* [1952] 1 All ER 1248