Top 100 General Counsel position on cyber security law and practice

Speed read

The GC100, the association for GCs of the UK's largest 100 companies, has produced a valuable structure in its report, *Cyber security law and practice*,[1] 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. While it is focussed on the UK and EU, the principles broadly apply elsewhere.

Here we summarise:

- What is cyber security?
- Why does it worry senior managers?
- What are the legal concerns for business around cyber security?
- What does the GC100 recommend to deal with this?

March 2015

The Detail

What is cyber security?

As the report says, this 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."*

Why does cyber security worry senior managers?

The report lists these 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."*

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 fulfillment 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)."*

What does the GC100 recommend to deal with cyber security legal risk?

In summary:

• Understand the legal framework, which is made up of multiple aspects, both domestically and internationally;

• Apply best practice cyber security standards;

• Ask a series of listed critical questions, to raise internally and with external suppliers, including external law firms;

• Build a "defensive shield" against regulatory action and litigation:

"Organisations that track regulatory guidance, regulatory enforcement actions and court cases relevant to cyber security will be able to use their knowledge to construct a strong "defensive shield" against regulatory investigations and litigation arising from security breaches."

1. Sourced from Thomson Reuters' PLC subscription service, which is a valuable resource in this area.

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