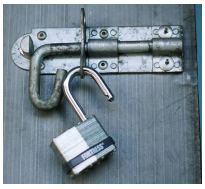
Duty of Care Laws

by Kevin D. Murray, CPP, CISM, CFE



Duty of Care Information Security Laws May Directly Affect You

All these things have something in common…

- Tea
- Silk
- Paper
- Porcelain
- Gunpowder

All were very valuable Chinese ***trade secrets***. The penalty for stealing these secrets was death. The spies were not deterred. All of the secrets were stolen. China's fortunes changed, dramatically.

What we can be sure of...

- Secret information attracts spies.
- Business spying changes history.
- **Punish-the-Spy** laws didn't work then, and they don't work now.
- History repeats itself.

In 2012, a short article called, **A Cunning Plan to Protect Us from Business Espionage**,[1] laid out a solution to the problem by adding some common law to the counterespionage solution. The old *duty of care* legal concept is being dusted off. Anyone responsible for safeguarding: trade secrets, intellectual property, strategic conversations, or information security in general, will want to take notice.

Get Ready

Duty of Care, an established legal theory, is gaining new precedence in the fight against economic espionage. Basically, *duty of care* requires the custodian of valuable information to pro-actively protect it with above average security measures. Locks, alarms and guards are just average. For example, they don't protect C-suite conversations, or off-site meetings, from electronic eavesdropping.

Fiduciary responsibility and *trade secret* status are important cousin concepts to be aware of as well.

[1] https://spybusters.blogspot.com/2012/03/cunning-plan-to-protect-us-from.html

Duty of Care Laws

by Kevin D. Murray, CPP, CISM, CFE

Statewide

The **Pennsylvania Supreme Court** recently held that an employer had a *duty of care* to protect the employee information they collected, that was subsequently hacked.[2]

Nationally

The United States Senate is currently working on *duty of care* law, too…

The Data Care Act of 2018 – A new bill introduced in the Senate proposes to hold large tech companies, specifically "online service providers," responsible for the protection of personal information in the same way banks, lawyers and hospitals are held responsible.[3]

This bill, introduced on December 12, 2018, is designed to protect users information online and penalize companies that do not properly safeguard such data.

The bill would be defined and enforced by the Federal Trade Commission. It would establish three basic duties, including:

- the *duty of care*,
- the *duty of loyalty*,
- and the *duty of confidentiality*.

If passed, the FTC would go through the normal notice and comment rule-making process to further establish how authorities will define, implement and enforce concepts like "reasonable" security measures.

There have been no shortages of Federal initiatives seeking heightened protection for consumer personal data in the past couple of years, in particular since enactment of the EU's GDPR, and its only a matter of time before one of them finally sticks.[4]

---

[2] https://www.jdsupra.com/legalnews/pennsylvania-high-court-decision-22440/

[3] https://assets.documentcloud.org/documents/5547713/Data-Care-Act-of-2018.txt

[4] https://www.natlawreview.com/article/data-care-act-2018

Duty of Care Laws

by Kevin D. Murray, CPP, CISM, CFE

The news media is also picking up on the duty-of care trend with articles like, **Why 2019 Will Introduce Stricter Privacy Regulation.**[5]

Internationally

South Korea just upped their industrial espionage laws with *duty of care*…

> The government is increasing the protection of key technologies…Not only will **companies guilty of leaking national defense technologies be criminally prosecuted,** they will also be prohibited from participating in any future defense-related projects.
>
> "Our technologies are being targeted for hijacking," Prime Minister Lee said. "In order to prevent technologies from being leaked, **we need to tighten up internal security and secure technologies and equipment**."[6]

Corporate Awareness

Corporations are letting executives know *duty of care* is expected. In an SEC filing, under **Global Corporate Governance Guidelines**, we see a good example of this…

> AllianzGI believes that officers and directors should only be eligible for indemnification and liability protection if they have acted in good faith on company business and were found innocent of any civil or criminal charges for duties performed on behalf of the company. We do not support proposals where liability cover extends beyond legal costs, and which can:
>
> - Limit or eliminate all liability for monetary damages, for directors and officers who violate the duty of care; or
> - Expand indemnification to cover acts, such as negligence, that are more serious violations of fiduciary obligations than mere carelessness.[7]

Impact to Business

1. ***Punish-the-spy* laws will no longer be the only deterrent to business espionage and losses via electronic surveillance.** The next step, holding

---

[5] https://www.techrepublic.com/article/why-2019-will-introduce-stricter-privacy-regulation/

[6] koreajoongangdaily.joins.com/news/article/article.aspx?aid=3057714

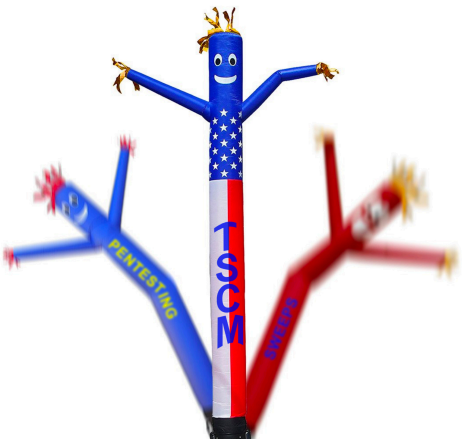
[7] https://www.streetinsider.com/SEC+Filings/Form+N-CSR+CHINA+FUND+INC+For:+Oct+31/14957651.html

business responsible for instituting above average security measures—especially for information considered vital to the national economy.

2. **Information security audits and technical surveillance countermeasures (TSCM)[8] will become the foundation of the "above average" information security requirement.** Governments and successful businesses already do this.

3. **Sending the question, "Do we need to do more to protect our information from espionage?" to the *risk assessment committee* wastes valuable defensive time.** The proven economic losses, and new *duty of care* penalties will automatically make taking a risk not worth it.

4. **Finding *above average* security help isn't easy.** The internet is littered with inflatable noodle men waving promises about their capabilities. **Tip:** Hire the best people you can find, or engage the services of a technical information security consultant. Buy on competence, not price.[9] Do it now, before all the good people are engaged elsewhere.



A Tip of the Tongue Answer

When management asks,[10] **"When was the last time we conducted an information survey and checked for bugs?"**[11] You want to be able to say, **"Recently."**

###

Kevin D. Murray CPP, CISM, CFE is a business counterespionage consultant and TSCM specialist with over four decades of experience.

Murray Associates is an independent security consulting firm, providing eavesdropping detection and counterespionage services to business, government and at-risk individuals.

Headquartered in the New York metropolitan area, a Murray Associates team can assist you quickly, anywhere in the United States, and internationally. v.190114

---

[8] https://counterespionage.com/advanced-tscm-explained/

[9] https://counterespionage.com/competent-tscm-consultant/

[10] https://counterespionage.com/wp-content/uploads/2017/08/How-to-Handle-Counterespionage.pdf

[11] https://counterespionage.com/advanced-tscm-explained/scheduled-tscm-inspections/