K&L GATES

10 CONCEPTS TO CONSIDER WHEN BUILDING AN APPROACH TO DATA SECURITY BREACH EXPOSURE

BY HOLLY K. TOWLE[1]

Data security is a hot topic in boardrooms, largely because of the increase in the size, costs and media attention regarding data breaches in recent years and the current emphasis by the US Securities and Exchange Commission (SEC) and Presidential executive orders on data security. All of this has raised data security risks and liabilities to board level. But how does a company get its arms around this topic?

Going back to basics is one way. Ten basics are described below. They are not obvious and are the source of considerable cognitive dissonance. Understanding them should advance progress towards compliance.

1. Privacy is not privacy

In the US,"'privacy" historically focused on information so personal as to be protected by the constitution or state tort laws. 'Data protection" is different. Data protection laws protect personal information that often is not private at all. However, it is newly protected because of the ease of copying, combining and transferring data in our digital age. Clinging to the belief that privacy only refers to private data can cause an organization to miss the compliance boat.

Another difference between privacy and data protection is that constitutional privacy has already been balanced with competing policies such as the constitutional right of free speech. Data protection statutes often have no such balance and risk attacks on their enforceability. The US Supreme Court recently opined that: "Facts, after all, are the beginning point for much of the speech that is most essential to advance human knowledge and to conduct human affairs". Where restrictions on data use cross the line between allowed and disallowed speech is ambiguous, and companies should assess that when assessing their use of data.

2. "Personal" information" is not personal information

When the US "data protection" wave began, the data to be protected was most often described as "personally identifying information" (PII). That has shifted. At least according to the Federal Trade Commission, protected "personal information" is (a) PII or (b) non-PII that reasonably may be linked to a person or their device (such as a computer, mobile phone or a "thing" in the 'Internet of Things').

[1] Holly K. Towle is a partner in the Seattle, Washington office of K&L Gates LLP. She can be contacted on 1 (206) 370 8834 or by email: holly.towle@klgates.com.

Failure to recognise this shift (legal or otherwise) is evidenced daily and creates risk. Consider a marketing department's internal assurance that there's no need to worry about ad campaign data because it "only" includes things like IP addresses or other device identifiers. That kind of statement is evidence that the marketing group missed the shift.

3. Data is more than data

It is not happenstance that security is a board of director concern. In 2011, the SEC started that ball rolling by issuing guidance stating that public companies must disclose timely and accurate information about cyber security risks and events that a reasonable investor would consider important to an investment decision. The guidance is not limited to data security breaches of personal information. It can include breaches targeting intellectual property and other "crown jewel" assets, including items like trade secrets, proprietary software, digital assets, "Big Databases" and so on.

The need to protect crown jewels has always existed, but doing so for digital jewels intersects with intellectual property laws. For example, in the US data tends not to be protected by copyright (although a database or other compilations can be), so other protections must be created (e.g., contractual protection) in addition to system security. Outdated assumptions can create ineffective contracts. For example, traditional NDAs (Non-Disclosure Agreements) eliminate the duty of confidentiality for information that becomes public without fault of the possessing party. That's a concept from trade secret law which assumes that trade secret protection vanishes if secrecy vanishes. That concept does not fit data protection principles: a duty to protect personal information continues even if someone else publicly posts it, i.e., secrecy is not determinative.

Another example concerns "scraping" data from a website. Some "scrapers" do this because copyright law does not protect factual data so, they reason, it must be free for the taking. Not so. Again, the focus on intellectual property law is misleading. The scraper has exposure under a variety of legal theories and a regulated "scrapee" might risk having to disclose crown jewel scraping under SEC guidance (not to mention the "scrapor's" exposure under the legal theories).

4. A plan must be more than a plan

The vast majority of US states require companies to give notice of a data security breach involving personal information as differently defined and nuanced per state. Federal "sector specific" laws also contain reporting duties. Most boards are aware of the need for a data security breach response plan (DBRP) in order timely to satisfy reporting duties just as every homeowner knows they need a basic plan for emergencies (e.g., who to call, what to have under the bed to grab on the way out of the door and how to exist once outside).

Having any plan is better than having none, but a basic plan will go only so far. A company that accepts credit cards might understand that it will need to comply with payment card industry standards, card brand program rules and its 'merchant bank' contract, but how many companies have an addendum to their DBRP outlining those rules? If that analysis is not done before the breach, it is more likely that a contractual deadline will be missed as the company struggles to wade through the volume and ambiguity of rules post-breach. Another example of waiting too long is waiting to review insurance coverage until after the breach or getting the wrong kind – the resulting coverage may be "too little, too late".

Advance planning cannot solve everything, however. For example, a company can choose "breach counsel" to advise on breaches, but what if the actual breach several years later involves service providers that conflict out the pre-selected counsel? A better approach may be to select counsel that can take a swat team approach (e.g., at least

help with immediate, non-conflict-inducing advice and then treat or refer out aspects of the breach as appropriate to the then circumstances).

The best advance planning is to decrease the risk of a breach fire with pre-breach efforts to get rid of the flammable brush, such as with training and compliance programs, including analyzing at-risk data and updating contracts, policies and procedures.

5. The bell tolls for thee

In the health insurance data breach experienced by Anthem, Inc., related health insurance companies and employers were impacted. This illustrates the need for companies to consider where they sit in an impact-chain and to include scenarios for that in their DBRP. For example, when an employer receives a notice from a breached third party, is that notice (i) merely letting the employer know what has happened, or (ii) triggering an employer duty to provide notice to employees under breach notice laws?

6. It takes an exclusive village

Companies use service providers like payroll and payment card processors, advertising companies, and data analytic companies and so on. Laws and industry standards increasingly dictate data protection clauses for those contracts and sometimes limit which service providers may be used (e.g., for payment card software applications). Decreasing data security exposure can require narrowing the village of eligible providers.

7. A call is not a call; consent is not consent

In data protection realms, words can have surprising meanings. Many companies do not realize that US federal law prohibits initiating a "call' to a cellular phone number absent a prior express consent of the person to be called and that a text message is a call. Also, the express consent is much more than that and statutory damage awards start at $500 per text. This is an example of the ability of routine activities to create significant liability absent a relevant compliance program.

8. Paranoia might not be paranoia

Some companies governed by a comprehensive sector specific privacy regime (such as the Gramm Leach Bliley Act for financial institutions or the SEC's privacy Regulation S-P), have a nagging feeling that there might be even more laws. Their "paranoia: is justified. There is an entire world of "other" data protection and security laws that are often not pre-empted by the sector-specific scheme. Private contracts also create requirements. For example, how many companies using social media widgets or plug-ins on their website have reviewed the social network's applicable "developer" rules or other contracts? Similarly, various programs popular with employers deserve data security worrying such as Bring Your Own Device programs.

9. Industry codes are not merely codes

Traditionally, companies committing to adhere to industry codes, standards or best practices assume that because their commitment is voluntary, there can be no legal repercussions. In contrast, in early 2012 the Obama administration issued its Consumer Privacy Bill of Rights allowing the National Telecommunications and Information Administration to work with industry, privacy advocates and other stakeholders to create and implement voluntary "codes of conduct." The document encourages voluntarily commitments to the resulting industry codes. According to the document, however, failing to fulfill the commitment converts the voluntary action into a legally actionable

unfair act or deceptive practice.

10. Corporate shield is not necessarily a shield

The FTC has spent over a decade amassing voluntary consent orders settling FTC claims of unfair acts or deceptive practices regarding data protection and security. One thing those orders make clear is that corporate boards are not automatically protected by the corporate shield. The details of why and when are beyond the scope of this article, but it is safe to say that automatic reliance on the corporate shield is misplaced.

Any "top ten" listing means that there are more than 10 things to consider. These 10 items, however, might help make more understandable those further considerations.