The Convergence of Law and Cybersecurity

Posted on March 7, 2018 by Melinda Biancuzzo, Chris Pogue

The term “cybersecurity” was coined in the late 1980s to describe measures taken to protect a computer or computer system against unauthorized access or attack. The 2008 National Security Presidential Directive regarding Cybersecurity Policy (NSPD-54) defines cybersecurity similarly as: “[p]revention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.” Despite (or perhaps because of) cybersecurity’s relatively static definition over the course of the last 30 years, the legal risk in this area is higher than ever before.

Part of the risk stems from the fact that cybersecurity law, policy, and practice are not yet fully developed for every industry. Even where rules are in place, there is no uniformity per country or among states or even across industries. Once an organization suspects a data breach has occurred, there is a small window of time in which an organization has to identify what information was compromised, confirm that the vulnerability has been remedied, and provide notice as applicable—e.g., to individuals, law enforcement, state attorneys general, regulatory agencies, etc.

The breach reporting deadline depends on the type of data that was compromised and the applicable jurisdiction. For example, an organization has 72-hours to report the loss of covered defense information under DFARS 252.204-7012. In contrast, the loss of personally identifiable information varies by country and by state. Whereas an organization may have 30 days or 90 days after discovery of a breach to notify U.S. residents (depending on the state), the European Union’s General Data Protection Regulation (GDPR) requires notice within 72 hours.

THIRD PARTIES COMPLICATE INCIDENT RESPONSE

Responding to an incident is further complicated where the breach involves a third-party vendor that may be less than forthcoming with objective evidence to support that the breach was remedied (e.g., an independent forensic expert’s report)—unsurprisingly, the concern is that an independent expert will draw conclusions on the cause and extent of the breach in the report that may support that the vendor was negligent. In this scenario, an organization’s legal team is now not only concerned with who must be notified and by when, but also establishing a record in the event of litigation with the vendor or consumers that shows the company secured its network access to or from the vendor while awaiting confirmation that the vendor’s breach was remedied.

Notably, cutting off the vendor’s access to your systems may pose legal issues as well in the form of the vendor filing a temporary restraining order. Even where companies make every effort to comply with data security and breach notification laws and regulations, there is no guarantee that an agency or court will find the company acted responsibly. And, these are just a few issues that might arise in responding to a data breach.

OUTSIDE COUNSEL AS QUARTERBACK

An organization’s best defense is a good offense. This means adopting a whole-team, enterprise-wide approach to cybersecurity, rather than leaving it exclusively in the hands of your information security

and information technology teams. Additionally, retain outside counsel with cradle-to-grave cyber-expertise—e.g., compliance audits, investigations, breach response and crisis management, privacy litigation, and responding to and defending against agency enforcement actions. In the event of a suspected or actual data breach, outside counsel is oftentimes thrust into the role of quarterback. This is necessitated by the ever-changing legal landscape coupled with the risk tradeoffs between what an organization may be required to do versus what they should do.

Outside counsel often acts as quarterback in the event of a data breach. Photo by Geoff Scott on Unsplash

This has never been more evident that in the post-breach litigation proceedings of organizations such as Yahoo! and Equifax (among others). The courts of public opinion and the law appear to have decided collectively that failure to provide reasonable defensive countermeasures to protect customer or commercially sensitive data is no longer palatable. The chasm between technical competence and legal or regulatory compliance has been bridged in such a way that breach fatigue has been replaced by frustration, incredulity, and sardonic cries for responsibility and action.

CHANGES ON THE HORIZON

In the 115th Congress, Democratic Senators Bill Nelson of Florida, Richard Blumenthal of Connecticut, and Tammy Baldwin of Wisconsin proposed the Data Security and Breach Notification Act. The summary of the bill states, "To protect consumers by requiring reasonable security policies and procedures to protect data containing personal information, and to provide for nationwide notice in the event of a breach of security." It also proposes a potentially game changing article in section 1041:

§ 1041. Concealment of breaches of security involving personal information 14 "(a) IN GENERAL.—Any person who, having knowledge of a breach of security and of the fact that notification of the breach of security is required under the Data Security and Breach Notification Act, intentionally and willfully

conceals the fact of the breach of security, shall, in the event that the breach of security results in economic harm to any individual in the amount of $1,000 or more, be fined under this title, imprisoned for not more than 5 years, or both.

Whether or not this proposed legislation becomes law, the simple fact that criminal charges are now are being discussed where public deception is identified puts a very fine point on the newfound lack of tolerance to the *same ole same ole*. Organizations that store, process, or transmit data of value need to take serious stock of their security posture and think long and hard about our previous admonition. Is what is presently required sufficient to establish a defensible position of reasonableness?

More importantly, are you willing to wager five years of your freedom on it? If you cannot answer "Yes" to either question with 100% certainty, you may want to adjust your optics to what should be done.

MELINDA BIANCUZZO

ASSOCIATE ATTORNEY - GIBSON, DUNN, & CRUTCHER LLP

Melinda is an associate in Gibson Dunn's Washington D.C. office with a practice in both Government Contracts and Cybersecurity and Data Privacy. She advises clients on all aspects of cyber incident and data breach response, including working with forensic security consultants, conducting internal investigations, interacting with law enforcement, and complying with data breach notification laws.

CHRIS POGUE

HEAD OF SERVICES, SECURITY AND PARTNER INTEGRATION

Chris Pogue has more than 15 years' experience and 2,000 breach investigations under his belt. Over his career, Chris has led multiple professional security services organizations and corporate security initiatives to investigate thousands of security breaches worldwide.