Published on *The National Law Review* https://natlawreview.com

Why Data Security and Legal Should Be Friends

Article By:

Theodore F. Claypoole

Within a corporation, teams jockey for resources and promote their roles within the enterprise. It sometimes seems like important parts of the company are working at cross-purposes.

Marketing wants the freedom to make promises and compliance holds them back. Production needs a hiring spree and finance says “no.” IT finds the new systems demanded by HR to be unworkable in the current network structure.

I once worked for a huge company that was selling three different versions of PCs through three different production and sales channels, where each sales group promoted its own product and bad-mouthed the other company offerings to customers. “Buy my desktop because the other desktop versions my company makes stink.” It can be a mess.

Natural conflicts develop within and between departments. Some lawyers feel they are representing the teams they are assigned to support. Some lawyers feel they are representing the “institution” against the damage those teams could do. These frictions can be damaging, but they can also assure management that important priorities will have advocates in the company.

I have seen situations where the CISO’s team felt they were at cross-purposes with the company’s lawyers, and resented legal intrusion into their realm. But despite having different assignments and portfolios within the company, there is no reason that the information security team and the legal department shouldn’t be allies. In fact, these two internal teams can provide support for each other’s priorities.

The CISO’s people protecting the company’s networks are performing a crucial and complex function. Attacked from all sides from all over the world, these defenders not only prepare for known threats, but build a system that can resist incidents that no one even considered yet. They build, maintain, and support resilient systems – technology, policy and procedure – for all of the other company functions to operate seamlessly. They need to plan ahead for resistance to and recovery from every threat from government-sponsored attacks to asteroid strikes.

The legal department serves a similar role. Starting with the laws, rules, regulations, and contracts that dictate compliant company operations, the legal department measures risks and threats – both internal and external – and guides the company through the most dangerous waters. Legal develops a protective and resilient infrastructure of risk-resistant policies, procedures, agreements and

documentation for all functions in the company to operate seamlessly. They plan ahead for resisting litigation and regulatory investigation and improve the options of company recovery from disaster.

Both security professionals and lawyers need to train the rest of the company to function in the safest possible fashion while allowing the most freedom operate for other company units. Both data security and legal need to educate the rest of the company about the rules associated with their business function and must develop policies and procedures for minimizing risk. Both functions work with vendors and customers of the company to assure that primary relationships are not significantly increasing risk. Both are instrumental in contingency planning and disaster recovery. Both are crucial for proper governance of company operations.

Both security professionals and lawyers need to train the rest of the company to function in the safest possible fashion while allowing the most freedom operate for other company units.

In addition, the two departments can definitely help one another. The CISO’s goal of robust network protection can be aided by intra-company advocacy for more budget, more people, and better technology by the General Counsel’s office. The chief lawyers often have the ear of a company’s board and executives on risk management causes, and lawyers advocating for increased technical/data resilience can be effective. Lawyers can also support data protections with all other company teams, knowing that data privacy and security are increasingly dictated by laws and regulation, and that other critical company data, like trade secrets or factory design, will not be legally protected unless it is properly guarded by technology, policy, and procedure. Lawyers can provide the risk-management context and underpinning for all of the information security department’s priorities.

And information security can provide real-time risk examples and cyber-threat demonstrations that resonate with individual executives. It is often difficult for lawyers to illustrate the risks facing their companies. People tune out the generalized possibilities of future harm. But the daily threats and cyberattacks against the company focus executive attention and make the generalities feel real and threatening.

Plus, there is the all-hands-on-desk urgency of cyber-fraud and ransomware. As stated by the blog at Diligent, “ Past risk governance models worked well for physical and financial risks, but they fail to provide adequate protection for cyber risk. If a situation occurs, it’s better for boards and their general counsel to get involved early on to prevent a full-blown crisis. Cybercrime calls for a team effort by the board, senior executives and the CISO. All three parties need to come to an agreement on how to properly handle cyber risks.”

These two important protective functions within corporations – the lawyers and the security professionals – will benefit by finding ways to work together for the common good. Both are crucial players for conducting business in dangerous and fast-changing world.

National Law Review, Volume XI, Number 257