

The Legal Defensibility Era

By David Navetta

ISSA member, Denver, USA Chapter

This article discusses implementing security that is both secure and legally defensible, which is key for managing information security legal risk.

Abstract

The era of legal defensibility is upon us. The legal risk associated with information security is significant and will only increase over time. Security professionals will have to defend their security decisions in a foreign realm: the legal world. This article discusses implementing security that is both secure and legally defensible, which is key for managing information security legal risk.

The collision of the legal and security worlds seems to be increasing at an accelerating and violent pace. New and increasingly onerous data security legislation is being promulgated on a regular basis at all levels of world, federal, and state government. Most companies, especially those with a worldwide online presence, have to comply with numerous laws from multiple countries and states. All variety of lawsuits and regulatory actions have ensued after data security breaches, including consumer lawsuits, employee lawsuits, client lawsuits, security assessor lawsuits, banking lawsuits, shareholder lawsuits, FTC actions, EU regulatory actions, and state Attorney General actions. Organizations are contractually imposing security obligations (including contractual liability) on companies to whom they provide sensitive information. Moreover, the payment card industry has established a back-end dispute resolution process that results in breached merchants being held liable for fines, penal-

ties, and recovery amounts without a lawsuit ever being filed. In short, like the technology from which they arise, the legal risks associated with data security and privacy have multiplied significantly over the past decade and will likely become more prevalent this decade and beyond.

When it comes to information security, it should come as no surprise that more organizations are asking not only are we secure? but also how much legal risk does our security (or lack of it) pose? The second question that immediately follows is, in light of increased and material information security legal risk, how do we reduce that risk?

We are entering the era of “legally defensible” security. The term was coined by colleague and friend Benjamin Tomhave, and he has been writing about the concept from the security end for some time.¹ This article looks at legal defensibility from a legal perspective, and more importantly how this concept (and the concerns it engenders) is likely to bring the legal and security professions into a much tighter working relationship in the coming months and years.

What is legal defensibility?

Legal defensibility in the security context focuses on the process behind making security choices and justifying those

¹ More here: http://www.secureconsulting.net/2010/03/legal_defensibility_doctrine.html; http://www.secureconsulting.net/2009/08/defensibility_and_recoverabili.html; Ben Tomhave, “Architecting Adequacy: When Good Enough Really Is,” *ISSA Journal*, March 2010.

The focus of legal defensibility is understanding how a plaintiff's attorney, judge, jury, or regulator will view an organization's security posture in light of applicable legal requirements.

choices in a legal context in order to reduce legal risk (and the costs associated with that risk). Information security legal risk arises when a company suffers a security breach or fails to comply with security legal requirements, and must defend itself in a litigation context or a regulatory action. The issue is not solely whether an organization is "secure" but whether an organization can successfully argue that its security processes and choices were legally "reasonable" and in compliance with applicable legal requirements (e.g., regulations, contracts and common law standards).

The focus of legal defensibility is understanding how a plaintiff's attorney, judge, jury, or regulator will view an organization's security posture in light of applicable legal requirements. Under a legal defensibility analysis security choices become legal positions or arguments to be used to persuade legal decision-makers that an organization's security was legally sound, and increase the likelihood that a judge, jury, or regulator will find a company legally compliant. Ultimately, there may not be a clear "right" or "wrong" answer, but rather a more or less persuasive legal argument/position on security.

That is not to say that "actual security" is irrelevant. In fact, in most cases truly secure companies are more likely to be in better position to legally defend their security choices (better yet, they will be in a position to reduce the likelihood of a breach in the first place). However, even companies that believe they have taken reasonable steps to secure their organizations need to worry about legal defensibility. While the mantra that there is no such thing as perfect security applies, and is recognized for the most part in the law, making that case in the legal context is not easy. In most cases, organizations will be defending their security *after* a security breach, and will have to argue that *despite* the security breach their security was adequate as a matter of law. The key in the legal context is taking this into account as a company develops its security program, and having the legal arguments (and information to support those arguments) developed *before* the organization's proverbial back is against the wall in a legal proceeding.

A combined legal/security approach

Legal defensibility is ultimately a legal issue that relates to the legal exposure a company faces in light of its security posture. However, it is a legal issue that cannot be addressed without the information security professionals who are charged with securing an organization (and who also may have to take the witness stand). In order to generate legally defensible securi-

ty, an understanding of the law is required on multiple levels, including insight on the following matters:

- The existence and applicability of data security requirements via regulations, contract, or common law, including arguments for and against the applicability of such legal requirements
- How judges and juries interpret statutes and common law (e.g., what information do courts look at to interpret an ambiguous provision of a regulation)
- The existence of common law duties, and an understanding of the elements of such duties and how they are proved or defended in court
- The meaning of *reasonable security* under the law and the proof needed to support a reasonable security argument
- Plaintiff attorney strategies and how plaintiff attorneys construct arguments in the security breach context and in general
- Litigation strategy, procedure, leverage points, and risk, including an understanding of the discovery, motion to dismiss, motion for summary judgment, and trial phases of an action
- How regulators interpret statutes and undertake regulatory actions
- The import of risk, industry standards, and general security standards (e.g., ISO 27001/2) under the law
- The use of contracts to legally bind service providers and other third parties storing, processing, or transmitting information on behalf of the organization
- The importance and use of attorney-client privilege
- The significance and impact of expert testimony
- Document retention and preservation and the impact of electronic discovery and electronic evidence on legal proceedings and legal risk

It is through this legal prism that security decisions will be scrutinized in the event of legal action. Even if security professionals believe they have taken the proper steps, those steps and their decisions will be viewed under a microscope in a completely different context from where day-to-day decisions are typically made. When taking legal defensibility into account, the security team's decisions and processes are placed in the best light and intended to put the organization on solid legal ground should a security breach occur or a regulatory action ensue.

Considerations for developing legally defensible security

Organizations that desire to implement a legal defensibility strategy should address several issues as described below.

**Ultimately, there may not be a clear
“right” or “wrong” answer, but rather a
more or less persuasive legal argument/
position on security.**

Legal and security/IT collaboration

Implementing a legal defensibility strategy first and foremost requires a collaboration between security/IT professionals and an organization's attorneys (whether in-house counsel or outside counsel). Unfortunately, the walls and communication barriers between these professionals are often very thick, and it is fairly atypical even in today's environment for close relationships to exist between legal and IT. Lawyers and security professionals must “A.C.T.”

First, they must become **Aware** of each others' worlds, the issues and concerns that are most important for each group, and the purposes and goals of each group. This awareness and a better understanding can only be achieved by active **Communication** between the professions. Lawyers need to explain the legal risks and statutory requirements that data security poses to the organization, and security professionals need to educate attorneys on how they analyze security risk and make security choices. Then each profession should **Translate** its legal issues into security actions and legal actions. For example, lawyers should be able to explain how risk or reasonable security is viewed by courts and regulators and enable the security team to translate those legal issues into legally defensible security actions.

Standardized decision-making process and documentation

The key to a legal defensibility strategy is establishing that a reasonable decision-making process was implemented to determine the security needs of an organization. Documenting the key decisions and choices made during the course of this process in a manner that anticipates legal arguments allows an organization to present its process in the best light in front of a court, regulatory body, or jury.

Having a regular and reasonable process in place that addresses relevant information security laws and legal risk elements (described below) provides consistency and a method for analyzing the evolution of an organization's security over time. It also looks much better to a court than an ad hoc, non-uniform, and completely subjective approach to making security decisions. In addition to general security decision-making, legal requirements should be baked into the process (e.g., What data security laws apply? Does our security program address specific legal requirements? etc.).

Just as important, however, is documenting the process and how the security decisions were made by the organization. This documentation serves as a historical artifact to be un-

earthed if a legal proceeding is initiated against an organization. It is also a living document that must be regularly updated and modified as security and legal conditions change. Without it organizational memory may fade (e.g., if key personnel leave), and companies may find themselves having to recreate the organization's security rationale “on the fly” in the midst of litigation. Moreover, through this documentation, with the help of legal, the security decisions made by a company can be translated into stronger legal positions that address key factors that plaintiff attorneys might attack or that judges or juries would find relevant in assigning fault. This documentation can also be viewed as a defense road map that anticipates potential legal arguments and explicitly addresses those arguments in advance. Significantly, to the extent this documentation constitutes communications between an attorney and client in the course of a lawyer providing “legal advice,” it is possible to protect it under attorney-client privilege and shield it from court scrutiny.

Information security legal risk elements

The following legal risk elements must be taken into account by legal and security personnel as an organization develops and implements a legally defensible security program.

Determine specific regulatory requirements

Depending what data they store, process, or transmit, the nature and location of the systems they operate, and the industries they are part of (e.g., financial, health, retail, etc.), organizations may be subject to multiple data security laws with specific data security requirements. It can be a challenge to even ascertain which laws may apply to a company. Nonetheless, in order to determine which laws apply, lawyers and security professionals must work together to inventory the types of data, track data flow, and understand system locations and configurations. Then lawyers and security pros must work together to ensure the company's security meets the requirements posed by these specific laws. Oftentimes, if multiple legal regimes apply, a compliance matrix cross-referencing the organization's controls against legal requirements may be a useful tool (and serve as documentation evidencing due diligence).

“Reasonable” “Adequate” “Comprehensive” “Appropriate” security

Whether required under a statute or under common law, some organizations may be legally required to maintain a level of security based on a legal standard that might seem vague. However, researching case law, understanding statutory construction, and interpreting the meaning of these words is what lawyers are required to do on a daily basis. Without understanding what these words mean and how a judge or jury might interpret them makes it very difficult to implement security that satisfies these standards. Using a legal defensibility strategy, an organization can better understand what is required when these terms apply and create stronger arguments as to why these standards have been met.

Contractual obligations imposed on an organization

Many organizations face data security requirements arising out of contracts with third parties. PCI is a perfect example – in order to accept credit cards organizations typically must contractually agree to maintain PCI-compliant controls. Moreover, some data security and privacy laws require companies to contractually impose certain security obligations on others. From a legal defensibility point of view the first issue is whether the organization's security actually lives up to these contractual obligations, and if so, whether the legal liability associated with a breach of contract is tolerable. This requires a legal interpretation of those obligations and the potential liability faced by the company, which then must be taken into account when implementing security. It also requires careful review and negotiation of these contracts to ensure that the organization is taking on the appropriate amount of risk and liability.

Data security of service providers/outsourced relationships

Increasingly organizations of all sizes and types are relying on third parties to store, process, and transmit data on their behalf. Whether in a "cloud" environment or a dedicated hosting/processing setting, customers can be held legally liable for security breaches or the non-compliant security of their service providers or partners. Legal defensibility in this context focuses on two areas: due diligence and vendor management, and data security contractual requirements imposed on service providers.

When selecting a service provider, a key legal issue is whether the customer adequately vetted the security of the service provider to ensure that it meets legal requirements and has reasonable security. In this context, from a legal standpoint, organizations should consider their service providers' information security an extension of their own internal information security set up. Potential liability may exist if the organization fails to vet (or improperly vets) its service provider, or works with a service provider whose security is weaker than, or does not match up with, the organization's internal security.

The contract between the vendor and the customer is very important in terms of legal defensibility. The contract should reflect relevant data security obligations and compliance with relevant data security and privacy laws. Security and legal should work together to contractually impose certain controls on the service provider that are necessary to meet these legal obligations. Moreover, the contract should address security assessment rights, breach response, and transfer of risk of loss.

The concept of risk and the law

As any security professional knows risk assessment is a key factor in analyzing security risk and choosing controls to mitigate risk to a reasonable level. The concept of risk is also prevalent in the law. Under common law, some courts consider risk in determining whether a legal duty exists (including a duty to implement reasonable security controls) and whether

an organization has satisfied that duty. Judge Learned Hand's formula is as follows:

If the probability be called P; the injury, L; and the burden, B; liability depends upon whether B is less than L multiplied by P: i.e., whether $B < PL$.

The concept of risk is important for determining whether an organization has implemented reasonable security. At a bare minimum this means that organizations should implement those controls that significantly reduce risk but are relatively inexpensive. On the other end of the spectrum, the law recognizes that risk need not be reduced to zero where the cost/burden would be overwhelming. In a legal defensibility paradigm risk, as viewed under common law and case law, should be taken into account and legal arguments developed to establish that such risk was adequately mitigated.

In addition, many data security laws include risk factors that allow organizations to implement "less" security if they pose less risk or have less resources, including, for example, GLB and Massachusetts's 201 CMR 17.00. PCI also addresses the concept of risk in its allowance of compensating controls. The concept of risk factors also must be understood in the legal context. Lawyers must interpret the meaning of the risk factors based on case law and statutory construction, and how they are weighed against each other, and construct arguments why their organization poses less risk and therefore need not implement the more rigorous data security controls. Under a legal defensibility approach the meaning of these risk factors in the legal context should feed into the data security choices made by an organization. The legal justification of lower risk should be documented to help establish compliance in the event of litigation or a regulatory action.

Information security standards

Implementing security that is consistent with various security standards may be helpful in reducing legal risk. It is very important for an organization to understand how courts look at standards and how they relate to legal liability. Complying with recognized standards such as ISO 27002 or NIST 800-53 may be viewed favorably by courts because both are established standards created by recognized standards bodies, and they establish frameworks based on principles that are commonly accepted in the security world. Complying with these standards instead of (or in addition to) using a purely ad hoc approach (and even better being certified by a third party as compliant) can carry significant weight in a court.

Beyond general standards, industry standards may be applicable to an organization that is part of a particular industry or a particular peer group within an industry. Again, the key from a legal defensibility point of view is understanding that many courts view industry standards as a floor for purposes of analyzing reasonable security. In fact, some courts have ruled that an entire industry may be acting unreasonably, and not within the standard of care. As such, in developing a legally defensible security program, organizations may have to go beyond industry standards.

Legally defensible security and proof

Many of the legal terms discussed above are fuzzy, leave significant room for interpretation, and require a significant understanding of the law and case law. Nonetheless, there is some more definitive evidence that may allow for a more effective legal defense of security decisions and limit legal liability. When making security decisions and developing a security program, being able to establish the following (usually through documentation and legal argumentation) can decrease legal risk and potential liability.

The organization's security risk has been reduced to a reasonable level

A security program should show that least cost/high risk reduction controls have been implemented. In addition, it is important to establish that more expensive controls that reduce too little risk do not fall into the zone of reasonable security. A risk assessment process and corresponding documentation is a key deliverable to help establish legal defensibility with respect to risk and reasonable security.

The organization has complied with its own security policies

Failing to comply with its own security policies is a sure route to potential liability for an organization. It does not matter if those policies are reasonable or consistent with law. If a company assumes duties and does not follow them, it is very problematic in the legal context. When designing a security program, in order to maintain legal defensibility it is very important that the organization (and all of its subsidiaries) are able to actually comply with its security program. While this may seem like common sense, many complex and diverse organizations implement policies that cannot be adhered to universally within a company, and those policies sometimes fail to provide for a "risk exception" process or allow for compensating controls.

The organization has not over-promised or misrepresented its security

Even if an organization's security is relatively sound, if that company over-promised on their security, it could lead to liability. This often happens in privacy policies that state something like the following: "we are 100% secure and your data will never be compromised." Of course, if a breach occurs then it potentially renders this statement a misrepresentation, which can lead to a fraud or negligent misrepresentation claim, or result in a regulatory action under the FTC Act (as a deceptive practice).

The organization has complied with specific requirements of applicable information security laws

For example, GLB, HIPAA, EU Data Protection Directive, Massachusetts Law, Nevada Law, etc. This is a two-step process. First the organization must determine which data security laws apply to it and then must be able to show that it implemented all of the specific controls required by such laws. In some cases, these organizations will also have to es-

Some courts have ruled that an entire industry may be acting unreasonably, and not within the standard of care.

tablish compliance with more vague security mandates (such as adequate, comprehensive, or appropriate security). For some laws, organizations will have to use risk factors to argue that they were compliant with legal requirements under these laws.

The organization has complied with general established security standards

For example, ISO 27002. As discussed above certification or compliance against an established industry standard developed by a reputable standards organization can help to reduce legal risk (e.g., it can help establish reasonable security and appropriate risk reduction).

The organization has complied with its industry's security standards

For example, information security practices specific to financial industry. As mentioned above, compliance with industry standards is viewed as a floor. For legal defensibility an organization needs to be able to document this compliance. In order to do this it needs to do the groundwork to determine what those industry standards are (and document where that information was obtained).

The organization has complied with the security standards of similar peers within its industry

An organization should not stop at the standards that apply to the industry as a whole, but should investigate the security standards utilized by similar peers within an organization. My local credit union is likely to have different security requirements and controls than a bank like Citibank. A larger multinational bank should, therefore, have a control infrastructure more approximating the Citibanks of the world.

The organization has properly scrutinized and managed its vendors with respect to information security

As discussed above, organizations that use vendors must conduct some due diligence to determine whether their vendor's security control posture is consistent with the organization's internal control structure. Organizations can spend significant resources reducing their risk to a manageable level. But the minute they provide sensitive data or system connectivity to a vendor, they are completely reliant on that vendor's security. If the vendor's security is weaker or does not reduce risk to the same level as the organization's internal security controls, that piece of information can and will be used against the organization in court and by regulators. Developing a process for vetting and managing vendors is important for maintaining legal defensibility, including in some cases written security assessments, documenting decisions concerning the adequacy of a vendor's security, and imposing contract

terms requiring certain controls/levels of security and transferring risk of loss should something go wrong.

Conclusion

Overall, legal defensibility is another important factor for security professionals and organizations to consider when implementing and maintaining an information security program. However, it cannot be stressed enough that the general goal of “good security” cannot and should not be replaced with a narrow focus on reducing legal risk. In fact, good security and legal defensibility go hand-and-hand with good security being a strong indicator of legal defensibility. The processes of building a security program and reducing legal risk should be viewed and treated as complimentary.

Nonetheless, failure to recognize the overlap between the law and security and to prepare for the time when an organization’s security will be scrutinized in an entirely different world (e.g., the legal world) may be detrimental. Now is the time for security professionals and lawyers to get together

and begin the collaboration that will be necessary to deal with legal risk and information security holistically. As the legal risk environment becomes more complex and liability risk more common, implementing a legal defensibility strategy will continue to grow in importance.

About the Author

David Navetta, Esq., CIPP, is one of the founding partners of the Information Law Group (www.infolawgroup.com). David has practiced law for over twelve years, including technology, privacy, information security, and intellectual property law and currently serves as a co-chair of the American Bar Association’s Information Security Committee. He has spoken and written frequently concerning technology, privacy, and data security legal issues and can be reached at dnavetta@infolawgroup.com.

