



Due Care or Do Not Care?

By David R. Furnas and Robert M. Wilson

One of the most important challenges facing today's business enterprise and the information security professional is that of regulatory compliance. Whether you work for government or the private sector, the portfolio of federal and state law affecting your planning and operations for information security has grown with each session of the U.S. Congress or state legislature in recent years.

Now, don't get me wrong; I'm not saying this is a good thing or a bad thing. Everyone has his or her own opinions on that subject and I'm not attempting to get anyone to see things *my way*, whatever my way might be. However, what I am saying is simply this: It's the law, and you need to think about how you're going to defend the decisions you make and the actions you take to establish compliance. Compliance with the law is not optional.

How, then, do we effectively establish, maintain, and defend a reasonable and appropriate program of both information security assurance and regulatory compliance? Start by acknowledging, accepting, and incorporating compliance as an explicit element of the mission goals of your information security organization. Everything your organization accomplishes and everything you do as a member of that organization should contribute directly or indirectly to the achievement of those goals. If your organization doesn't have a mission statement, feel free to use the following as-is or revise it to meet your specific requirements.

The mission of [your security organization] is to establish and maintain the confidentiality, integrity, and availability of information assets through the application of people, process, and technology in a manner that:

1. *Facilitates compliance with applicable law*
2. *Demonstrates due care and due diligence*
3. *Satisfies documented technical, functional, and business requirements*
4. *Conforms to recognized standards, guidelines, methods or practices*
5. *Establishes and maintains an acceptable level of risk using recognized risk management practices and appropriate administrative, physical, and technical safeguards*

So, what is "due care" and why is it important? I'm going to offer some definitions and propositional logic to illustrate this. At first, this may seem a little excruciating. However, it is important so please bear with me for just a few paragraphs.

A widely recognized definition of due care is "the care that a reasonable person would exercise under the circumstances; the standard for determining legal duty". Conversely, then, we can define "neglect of due care" as "the care that a reasonable person would *choose not to exercise* under the circumstances; the standard for determining legal *liability*". More about neglect shortly.

Now, we will examine the definition of "due diligence" and its relationship to due care. A widely recognized definition of due diligence is "the effort a party makes to avoid harm to another party". If "avoiding harm to another party" is equivalent to "legal duty", we can also define due diligence as "the effort a party makes to observe its legal duty". Since we have already shown that legal duty is equivalent to due care, we can now define due diligence as "the effort a party makes to (1) *demonstrate due care* (2) *avoid neglect of due care*".

Here is a very important point I want all readers to understand about neglect: If "due care" is the inverse of "legal liability" and we believe that "under the circumstances" people will think before they act, we can now define neglect of due care as "the conscious omission or commission of actions that a reasonable person would expect will result in legal liability". That is why neglect of due care is actionable under the law and why any information security professional who is neglectful is placing their enterprise, their management, and potentially themselves, at risk of suffering direct and indirect losses that might result from fines, incarceration, loss of brand image, and reduced competitiveness.

Now, replace the word "person" with the term "information security professional" in each of the previous definitions. Under the law, the reasonable information security professional will be held to a higher standard of due care than a reasonable person of generic qualification and cognizance. Just as doctors and lawyers are held to a higher standard of due care because of their specialized training, knowledge, and professional codes of ethics, so, too, should the information security professional expect to be held similarly accountable.

I like to think of the information security life cycle as a "continuum of care" in much the same way a health care provider thinks of how they deliver services to their patients. Due care and due diligence provide the foundation on which that continuum is constructed and defended. Our challenge, then, is to understand what standard of due care should be applied in a given circumstance and what process of due diligence should be employed to validate due care.

The best way to accomplish this is to ask your legal staff for an opinion. This is, after all, a legal issue and even though law, investigation, and ethics comprise one of the ten domains of the (ISC)² Common Body of Knowledge, most information security professionals are not lawyers. Unfortunately, if your enterprise does not employ full-time counsel this may not be feasible. Outside counsel may be an option, but only if your management is able and willing to incur the additional operating cost. You may choose to consult your own counsel, but this option is dependent on the extent of your own financial resources.

If none of the previous options are available to you, you may wish to use a form of the due care assessment process I am going to describe. The first part of the process is to properly prepare by developing a reasonable understanding and interpretation of the regulation in question. Get a hard copy and read it in its entirety. Using a red pen, write your questions or comments on the document itself. Read it again. Discuss it with your peers.

Review comments or opinions available from legal discussion forums or other Internet resources. If you have any friends who are lawyers or paralegals, ask them if they are familiar with the regulation and if they have any comments or opinions about it. Optionally, take a business law class at your local community college or through a professional organization like the SANS Institute.

Now that you are properly prepared:

1. Imagine you are on the witness stand in a court of law.
2. You are an expert witness for the prosecution.
3. The defendant has been charged with a violation of the regulation that has resulted in identity theft affecting 1,000 people (victims) with combined losses exceeding \$1,000,000.
4. The violation resulted from the error, fault, failure, or absence of the safeguard being considered to facilitate compliance with the regulation.
5. When asked by the prosecutor, what would you assert as the standard of due care that should have been applied by the defendant in the selection, implementation, and use of the safeguard that would have effectively mitigated the breach?
6. Imagine you are one of the victims and you have personally lost more than \$10,000 that you may never recover.
7. Now, what would you assert as the standard of due care?
8. Imagine you are the defendant.
9. Now, what is the standard of due care that will enable you to effectively defend your decisions and actions regarding the selection, implementation, and use of the safeguard? Will you select the safeguard? If so, why? If not, why not? How will you choose to implement, operate, maintain, support, and ultimately retire the safeguard or an alternative safeguard? Why and how will you defend these choices as "reasonable and appropriate"?
10. Document the assessment process and the standard of due care.
11. Review and, if appropriate, revise your due diligence process to incorporate the standard of due care.

I hope this examination of due care and due diligence both as concepts and as processes has been helpful. I also hope you may now have a better understanding of neglect of due care and its implications. In future articles I will discuss related issues including the examination of specific regulations. In the meantime, I'll see you at the chapter meetings. ✍️

David R. Furnas, CISM, CISSP is Vice-President of the Sacramento Valley Chapter of the ISSA and Senior Enterprise Security Engineer for Deltanet Inc. Mr. Furnas may be contacted at dfurnas@issa-sac.org.

Robert M. Wilson, Attorney-at-Law, also contributed to this article. Mr. Wilson may be contacted at RWilson@BusinessCounsel.net