# Information Security & Negligence
# Targeting the C-Class

By Carter Schoenberg ©

Numerous recommendations since September 11, 2001 have been published on the evils of negligence relative to protecting one's assets (cyber & physical). In light of the articles, references, statutes, case laws and other relevant pieces of this puzzle, how do you physically "prove" negligence versus the common business practice of risk management?

Rather than analyzing a hypothetical situation where a company is hacked by one of several means or subjected to the involuntary mass-propagation of a virus or worm, let's focus on a real-life incident, dissect each component supported by fact and effectively diagram a blueprint for how you cannot only be targeted for a lawsuit or criminal prosecution, but demonstrate how you will lose. This loss will inflict a financial casualty, which may dramatically impact an organization's fiscal health.

On August 23rd, 2003, a financial institution located in Massachusetts, had its Web page defaced with an anti-American political message. Allegedly, the attacker did not specifically single out the financial institution but rather scanned for vulnerable Microsoft Windows Operating Systems running IIS 5 (Internet Information Server version 5). This particular bank supposedly was one of numerous web sites hit. The only difference in this example is that this particular financial institution operated a Web page and had a duty and responsibility for allowing customers the ability to access their financial records; view accounts, pay bills, transfer funds, etc. Local law enforcement worked with this financial institution attempting to catch the attacker.

At the same time, the financial institution in question was able to resolve the issue of their defaced Web page by simply applying a "patch". This particular patch from Microsoft existed for over three months prior to the incident. The investigators confidently stated that it did not appear any customer or financial data was compromised as a result of this attack. However, news articles published reports that customers could not reach the Web site and thus, had limited or no access to their funds over the weekend of the attack.

How does an organization manage risk? Especially when a business is strictly regulated such as banking and finance? In this example, it was not a matter of allocating resources towards applying a patch to a server not used or considered "critical" for business continuity. It was a matter of ensuring that an exposed, forward facing, Web enabled device, used by customers on a daily basis for e-commerce, be available without interruption of service. In this case, if the reported account of a simple patch installation was the resolution, then the bank is culpable under negligence. The question remains, even though it would appear that ignoring the simple task of applying the patch to the affected system is negligent, how can one "prove it"? What harm resulted in direct relation to this negligence since investigators stated that financial and personal information did not appear to be compromised?

The specifics for negligence, as defined under law, vary in each state. However, the US Federal Courts can clearly supercede a state's jurisdiction. The reason? The banking and finance sector (like many others) are regulated by the US Federal Government. Many organizations are familiar with buzzwords like "Sarbanes-Oxley", "HIPAA" or "GLBA" or "SB1386" and so on. Most view these regulatory acts as nothing more than a guideline that is only hyped by the auditors and elite few who benefit from such legislation.

Lets examine the elements (if met and cause harm) leading to a case based on negligence.

- **Duty: Does the defendant have a responsibility to protect information?**
- **Negligence: Is there evidence that the defendant did not fulfill his or her duty of care?**
- **Damage: Did the plaintiff suffer quantifiable harm?**
- **Cause: Can the breach of duty related to the damages be considered a primary cause?**

Did this financial institution have a duty to protect this asset? *Absolutely*. This particular asset (Web Server) was responsible for the e-commerce transactions of this financial institution. Was damage caused as a result of failing to meet the duty? In this case, *yes*. Clients could not access their accounts via the Web. Therefore, negligence does exist as a result that the defendant failed to fulfill his or her duty of "due care", thus causing clients of their financial institution the inability to access their financial resources. This is qualified harm under the Gramm Leach-Bliley Act and if this bank's clients incurred administrative charges because scheduled transactions could not take place such as late charges, NSF, etc., then quantifiable harm is established. Criminal issues such as motive and opportunity are relevant for this argument as well. Opportunity is a demonstrated factor because for over 90 days, this financial institution failed to mitigate this risk when a means of resolve was available for such an extensive period of time. Motive can be directly linked to "why" it was not patched. Proving the "why" component will require evidence from more than one source to ensure a judgment. However, if the "why" is proven to be a result of deferring cost or budgetary constraints, then motive has been defined.

***Example of a negligence time-line:***

Point of discovery 10 days 30 days 2 months 3 months 6 months 1 year

*----------→

**Manageable Risk----------Borderline----------Negligence--------Gross negligence**

The ability for plaintiff's counsel to obtain information about the defendant such as security policies, protocols, guidelines, disaster recovery, business impact statements, etc. during discovery via a federal subpoena or court order is considerable and should not be trivialized. Security policies, protocols, guidelines, remediation, risk management, business impact statements, virtually everything. Furthermore, the ability to discover who is ultimately responsible for the defendant's computer systems? It may come back to the Chief Information Officer or Chief Technology Officer. Were any of the "C-class" members advised of the potential impact by failing to address this Web server for this financial institution? If so, why was the patch not applied prior to the incident? More importantly, did they document the reason for their actions? It is also important to consider in some instances, the cost of responding to such actions may be so cost intensive that the organization may go bankrupt. This scenario will ultimately lead to share holders targeting corporate executives as being personally liable seeking seizure of personal wealth and even criminal sanctions.

Here's how it works.


Prior to the defendant being advised of a pending suit, a skilled attorney familiar with these new tactics and strategies will demonstrate that the standard of due care & due diligence had not been met, most likely yielding damaging evidence. There are a limited number of widely used security vendors currently in operation. An attorney will execute a federal court order directing any and all contact each security vendor has had with the defendant. The defendant is the financial institution in the scenario above. If contact was made, what was the context of that contact? Do these security companies have records that supports that a thorough analysis or testing of security policy and protocols were completed? If so, what were those results? Can an independent third party validate the testing?

Not only will the outlay of the defendant's network topology and security posture be demonstrated, but also within the scope of obtainable evidence are the results as to how well/poor did they score. More importantly and perhaps more critical to establishing proof, what recommendations were provided by the security vendor? Were the recommendations for remediation of existing risks followed? If not, why? The hunt will start off initially as a broad investigation, which begins to spiral inward and finally one or multiple key pieces of information will provide great value for the plaintiff's case.

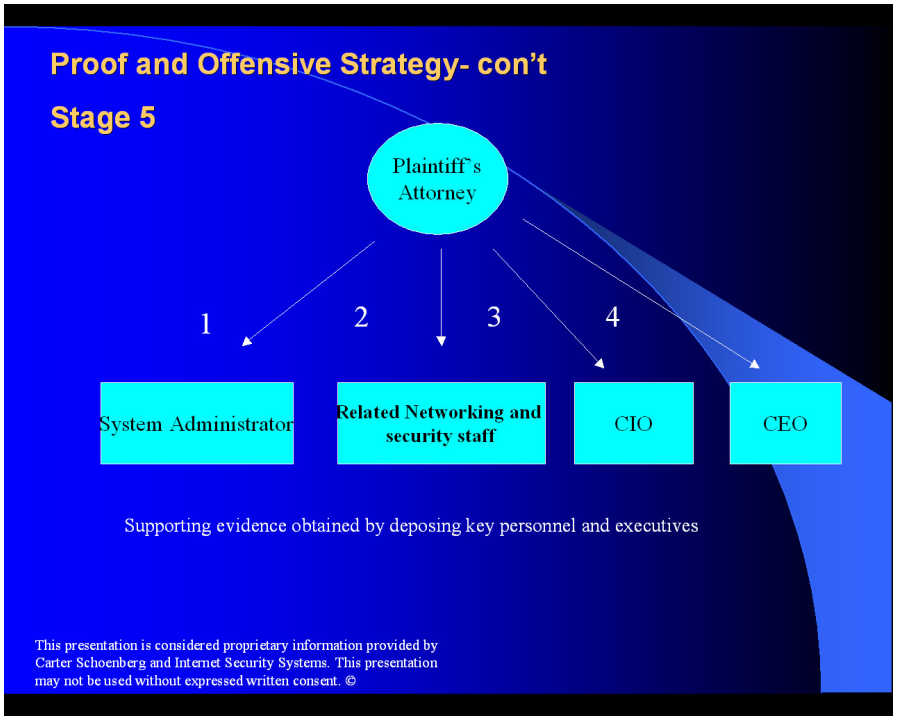
Once the preliminary evidence is obtained through cursory searches aided by subpoena or court order, the next step would be to notify the defense of plaintiff's intent outlining the general basis of the charge(s) and what is to be expected in return. (i.e. terms of settlement) This is a mere formality and the defendant is now aware of anticipated legal action. The plaintiff's counsel will have the defendant's System Administrators and IT staff deposed to obtain additional evidence independent of the subpoena for corroboration. Issues that will be addressed will include: years of experience, certifications held, education, criminal history, and previous employment.

The object is to establish a documented level of expertise and knowledge in the field of information technology and security. The criteria mandated under current compliance regulations can be construed as subjective by the defense; However, this is where the *Prudent Man Doctrine* and *Neighbor Policy* apply. Although defining one's abilities against a written standard may vary and prove difficult to overcome in court, the ability to compare one's ability against similar professional standards is admissible. This may include technical expertise, education and past work experience of similar professionals in other companies. This can help define a qualified standard. Obviously, it is the responsibility of the plaintiff to argue the standard to the defendant and ultimately a court. Would an IT professional with several years of experience running a network for a banking & financial service, and who holds one or several certifications, and well as having a college education in computer science, not be aware of the risk associated by not simply patching a Web server used for e-commerce on a daily basis? What about after being made aware that a solution was available for more than 90 days?

The ability to show "cause" in this case is proven by effectively illustrating that as a result of the Microsoft patch failing to be successfully deployed, according to their spokesperson, prior to the incident, directly impacted the Web interface for customers and thus, was no longer an available financial service. The impact is not limited to multiple customers unable to use this financial services commercial Web site. It also may have afforded the successful attacker the means to obtain personal and financial information not yet used. These attackers who, in turn, will sell this information to criminals that specialize in identification fraud and Identity-theft. An "Assumption of Risk" for the clients of this financial institution is not implied as a result that the financial institution holds a "duty" to ensure the ability for their clients to have access to their funds in compliance with state and federal regulatory acts. The counter-argument utilized in most negligence cases is "Contributory Negligence". What this means is layman terms is that the plaintiff in this case, held a degree in holding some level of responsibility for this incident. Unless the plaintiff was the attacker seeking out a website vulnerable to the Microsoft WebDav issue, then no, there is no argument for contributory negligence.

Since contributory negligence cannot be established against the plaintiff by defense counsel, the liability associated with comparative negligence is now removed. Comparative and contributory negligence will apply however in cases involving third parties, contractors, service providers, etc. And just as effectively and efficiently will plaintiff's counsel articulate a case against the defense, so will the defense then attempt to attack the plaintiff.

Now the ultimate fact comes into play. Does the burden of responsibility fall on the System Administrator or does it go up the food chain? Hence, deeper pockets.




One of two things will occur when the plaintiff's counsel deposes the System Administrator. One, he/she states that the policy of their enterprise was followed to the letter. They were made aware of the remedy but that the CIO (or other authority) selected to not allocate manpower and resources to fix the issue. As a result, the System Administrator was limited in what could be done under his/her authority. Or two, the System Administrator exclusively failed in using due care. See stage "2" of the diagram above. In both circumstances, this evidence needs to be confirmed by third parties, co-workers, contractors, etc.

If the end result is a matter of material fact that the System Administrator failed in his/her responsibility, the target of the civil/criminal suit is defined and you can go no further up the chain. This ultimately works in favor of the C-Class. However, if the end result is a matter of the CIO or other corporate officer(s) directing the System Administrator to ignore proper procedure as a result of budgetary restrictions, (sound familiar?), then the plaintiff's counsel just won the lotto. Budgetary constraints do not negate negligence if the cost of protection does not outweigh the ultimate loss.

Example:

Average time to successfully patch a server: 4 hours

Average System Administrator/IT hourly rate: $80 per hour

4 * $80 = $320.00 vs. the mandatory fines under GLBA and Federal Sentencing Guidelines for Corporate Officers. (More than $100,000) + (Incurred administrative fees not yet determined)

Negligence is defined and the defense has to consider settlement or risk not only going to court facing either civil or criminal sanctions, but also risk public exposure. This could result in loss of confidence in the enterprise, lower stock valuation, and increased financial burden impacting the businesses bottom line.

Now what is interesting about this lifecycle of tactically going after an enterprise is the simple and obvious fact that the first call made by a named defendant is to whom? Their attorney or legal representation, correct? Ultimately, any organization can mitigate much of the exposure I have outlined so far by placing an increased value on their legal representation, whether in-house or third party counsel. The expertise and experience many legal practitioners now have in the field of IT negligence is increasing from just a mere handful to a growing level of competent litigators providing new service offerings. It provides the attorney's clients an increased value proposition by affording document retention, peripheral services such as actually using the legal representative to perform the due diligence, penetration testing, policy development and best yet, be covered under attorney client privilege. Hence, information is not a forcible obligation under a court order(s).

It is important to note that the common practice of risk management can only be taken so far before it traverses over into negligence. Good intentions for providing minimal acceptable standards for security may not be enough. An honest intention may only show a state of mind for the defendant in court showing a presumed level of innocence. Please remember one important fact in law, "innocent" is not the same thing as a verdict of "not guilty". Good intentions do not outweigh the common criteria for minimum standards in information security. The road to hell, or in this case, federal court, is always paved with good intentions.