Preparing Your Organization Today to Win Its Future (Possibly Inevitable) Cyber Lawsuit: Making Crown Jewels Out of Paper

4/18/2016 by Belton Zeigler | Womble Carlyle Sandridge & Rice, LLP

One day in the not too distant future, your organization may be fighting to protect its balance sheet against high-stakes claims in a cyber tort trial. Arrayed against you will be the best of the class action plaintiff's bar, cheered on by the FTC and several state Attorneys General. They will demand that you prove that your organization used reasonable care –perhaps years ago-- to prevent a major hack of your systems or products. (WiFi enabled products, by the way, are emerging as a particular cyber tort danger, they can hang around for eons in internet time.)

In the cyber world, criminal syndicates identify new vulnerabilities daily in software and products and create new hacking technologies to exploit them. The white hats work to create technologies to counteract them just as quickly. The balance sways back and forth. But what constitutes reasonable care in cyber security is never the same month to month. Software and practices that are safe and reasonable today are one high-profile hack away from being laughably outdated. If there is one, and there probably will be, your organization's cyber trial will take place years after the hack. By then, software patches and other easy fixes for your problem may been available off-the-shelf for months or years.

In your cyber trial, if hindsight defines reasonable care, you almost inevitably lose. So how do you overcome the power of hindsight? When do you begin?

You begin now. Start by creating contemporaneous documents that prove your organization conducted an organized, intentional effort to exercise reasonable care in light of today's cyber threats, cyber protection standards and the state of the art. Create, catalogue and preserve documents to show you identified risks, benchmarked systems, vetted products against those risks, implemented countermeasures, and trained your board and employees to protect and respond to current threats.

This effort should intensely practical, oriented towards producing documents that can be used to maximum effect --as written-- in a future trial. At trial, the hack will probably be undeniable. Reasonable care will be your defense. Your contemporaneous reasonable-care documents will be the crown jewels of the defense.

At your future cyber trial, no single document is likely to be more valuable than a contemporaneous third party cyber security audit. There are a number of services that conduct such audits. For privilege purposes, they should be conducted through the General Counsel's office. The resulting reports should be carefully reviewed to insure that they contain the language and conclusions that will be most helpful *at trial*. Specifically, the conclusions should be written in a way that will allow them to be highlighted on screens in a future jury box, or quoted in in whole paragraphs in a future appellate brief. For this reason, counsel –including litigation counsel-- should be directly involved in producing the final draft of the report.

There are emerging standards to guide such audits and to suggest the standards of care that your organization may be held to at trial. Among the principal ones are:

1. The Center for Internet Security's *Critical Security Controls, Critical Security Controls for Effective Cyber Defense*, (the "CSC 20" formerly the "SANS Top 20");
2. The National Institutes of Standards and Technology (NIST) *Special Publication 800-53, rev. 4* and *Framework for Improving Critical Infrastructure Cybersecurity*;
3. In International Organization for Standardization, *ISO/IEC 27002: 2013*.

Identifying vulnerabilities in a systematic way is integral to these new standards. Accordingly, it is very difficult to meet them without conducting an enterprise-wide cyber security audit. The standards also include such requirements as maintaining an effective breach management and response plan, training your board and senior leadership in that plan, and effectively training

employees for their role in cyber security. (Employees are being identified as the greatest source of cyber vulnerability in today's environment.)

And the link between meeting these standards and proving due care in a future legal fight is being made more explicit. In February of 2016, the California Attorney General's office's issued its *Data Breach Report, 2012-2015*. The Attorney General found that the CSC 20 standards "identify a *minimum* level of information security that all organizations that collect or maintain personal information should meet. *The failure to implement all the Controls that apply to an organization's environment constitutes a lack of reasonable security.*" (p. v, emphasis added). While there are serious flaws in this document, the message is clear. Current best practices are become future tort law standards of care.

Among the CSC 20 standards is "continuous vulnerability assessment and remediation." Thus the audit that documents reasonable care is itself part of what now may constitute reasonable care.

So in preparing for your future cyber tort trial, some of the questions you should ask are these: Is your organization documenting vulnerability assessments for systems and products today in ways you can use in a future trial? Are there documents to show that implementation plans are underway today to overcome known vulnerabilities? Do your current board minutes record regular discussions of cyber security vulnerabilities and breach response planning? Do you have agendas, handouts and PowerPoints decks to show a jury that your employees are being trained currently to recognize and defend against cyber security threats?

Only if you begin now will you have the documentary evidence needed to prove reasonable care in your organization's future cyber tort trial. Lord willing, you will avoid that trial occurring. But if it does, then when the plaintiffs' bar comes calling, you will have a solid stack of documents showing reasonable care in the months and years leading up to the hack, thus allowing you to defend your organization against trial by hindsight.

RELATED POSTS

- Cyber Security IMPOSSIBLE: California AG Decides a Ceiling is a Floor
- Rebuilding Trust with the Europeans After Snowden: Obama Signs New Privacy Law
- FDIC "Framework for Cybersecurity" Highlights How Financial Institution Information Security Programs Can Better Respond to Evolving Cyber Threats

LATEST POSTS

- Formal Logic Reveals Hidden Dangers of Logical Fallacies in Patent Claim Rejections
- Next Steps: Helping Your Organization Implement the New Medicare Overpayment Rule - Part II