DISCUSSION PAPER

CREATING A COST-EFFECTIVE CYBER SECURITY SAFE HARBOR

The New Threat to Corporate Cyber-Legal Security: Litigation

Businesses face numerous cyber-threats from varying sources on an ongoing basis. These threats are generally covered by the generic term "hackers" and range from script kiddies[1] to"hacktivists"[2] to disgruntled employees/contractors to highly sophisticated state and non-state actors with long term goals and techniques.[3]

There is, however, an additional types of cyber challenge that companies are facing in addition to hackers, trial lawyers. Companies are already being sued based on allegations of cyber-deficiencies.[4] Moreover, cyber security-related litigation is closely entwined with the cyber security regulation and is seen, by some as an alternative to or supplement to regulation.[5]

Fueling the potential for expensive class action litigation is the development of federal cyber security regulations, guidance documents and "voluntary" cyber defense programs and processes since perceived non-compliance could be viewed by the plaintiff's bar as a potential legal weapon to be wielded in litigation. Recent SEC guidance, described below, is a lightening rod for litigation.

From a litigation perspective, it should be noted that the proposed cyber security legislation included some liability immunities for companies that adopted federally-approved cyber security measures. As a Discussion Paper distributed to senior Administration officials along with a draft of the cyber security Executive Order explained, however, a key difference between the Order and legislation is that the Order cannot provide any liability protections.

> *the proposed Senate bill (Lieberman-Collins) proposed extending liability protections to companies that participated in the bill 's equivalent of the voluntary program. Liability protection requires statutory authority; therefore the Executive Order cannot establish such an incentive.*[6]

---

[1] http://en.wikipedia.org/wiki/Script_kiddie

[2] http://en.wikipedia.org/wiki/Hacktivism

[3] http://en.wikipedia.org/wiki/Advanced_persistent_threat

[4] See, http://www.thecre.com/fisma/?p=4090 and http://www.thecre.com/fisma/?p=4114

[5] http://www.thecre.com/fisma/?p=4114

[6] See, page 3 of Tab A, http://www.thecre.com/fisma/wp-content/uploads/2012/11/White-House-Draft-Executive-Order-Publicly-Circulating-Copy-11-1-12.pdf

The challenge, therefore, is to develop a "safe harbor" that could provide a significant measure of liability protection for companies in the absence of legislation. As discussed below, a cyber security safe harbor has three components:

1. Threat awareness;

2. IT security controls; and

3. Reporting Requirements: the Data Quality Act (DQA)[7] and Paperwork Reduction (PRA)[8] govern federal reporting and information dissemination requirements which heretofore have not been considered in the development of cyber security programs – these requirements provide a throttle on unwarranted private sector disclosure of cyber intrusion data. For a sense of the scope of new cyber intrusion reporting requirements, please see the Bloomberg news article discussed below (see footnote 10) regarding the fact that the SEC has sent dozens of letters to private firms with respect to their guidance document.

The SEC Cyber Security Guidance – Creating a Standard of Care

The most significant federal cyber security guidance document, one with wide-ranging implications, is the Security and Exchange Commission's Cybersecurity Disclosure Guidance.[9] As Bloomberg News reports, for a number of companies, that "guidance" is effectively a binding rule since the Commission has "sent dozens of letters" to companies "asking about cyber-security disclosures and later pushing companies to disclose...."[10]

The challenge the disclosure guidance document poses to publicly traded companies, is two-fold. First, any reported cyber-breaches could be used as the basis for a lawsuit. Second, the guidance, with its requirement for corporate awareness of cyber-threats and risks, creates a *de facto* though ambiguous "standard of care." The plaintiff's bar could assert the existence and violation of such a cyber security care standard in lawsuits. On this point, it is important to note that the SEC guidance is about more than just reporting duties. With respect to the duty of companies to be aware of cyber-risks, the SEC document states that

> *we expect registrants to evaluate their cybersecurity risks and take into account all available relevant information...*

---

[7] http://thecre.com/post/

[8] http://acus.granicus.com/MetaViewer.php?view_id=2&clip_id=29&meta_id=512

[9] http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

[10] http://www.bloomberg.com/news/2012-08-29/sec-guidance-on-cyber-disclosure-becomes-rule-for-google.html

Thus, SEC guidance is about more than disclosures, the document effectively requires companies to conduct a cyber security risk assessment and to be aware of "all available relevant information."

The term "available" could be interpreted in a plain sense meaning as referring to information the company has on hand with no obligation to seek additional information. In the alternative, the phrase could be interpreted to mean that the company needs to take pro-active measures to obtain available relevant cyber-threat information.

When considering which interpretation of "available" federal authorities, and the plaintiff's bar, will view as correct, it is important to consider the draft Executive Order on cyber security. The Cyber security Information Sharing section of most recent publicly available draft of the Order directs the Department of Homeland Security as follows,

> *(b) The Secretary, consistent with 6 U.S.C, 133(g), shall establish a coordinated process that rapidly disseminates all unclassified reports of cyber threats that identify a specific targeted entity to the U.S. targeted entity. The Secretary, in coordination with the Director of National Intelligence, shall establish a system for the tracking of these reports and notifications. Agencies making notifications are responsible for reporting to the Secretary when notifications are made.*
>
> *(c)To assist the owners and operators of critical infrastructure in protecting their systems from unauthorized access, exploitation, or harm, the Secretary, consistent with 6 U.S.C. 143 and in collaboration with the Secretary of Defense, shall within 120 days of the date of this order establish procedures to allow the owners and operators of critical infrastructure in all sectors to participate, on a voluntary basis, in the Enhanced Cybersecurity Services initiative.*[11]

Thus, it appears that the Administration *strongly favors* critical infrastructure companies participating in activities to enhance their awareness of relevant threat information. It would be reasonable, therefore, for SEC registrants in critical infrastructure industries to understand the SEC guidance's reference to "all available relevant information" as having two aspects:

1. Externally-developed information available to companies through participation in an industry-specific Information Sharing and Analysis Center (ISAC)[12] and/or through an information sharing and protection mechanisms developed under the Executive Order; and

---

[11] See, Section 4, http://www.thecre.com/fisma/wp-content/uploads/2012/12/White-House-Draft-Executive-Order-Dated-11-21-12.pdf

[12] http://www.isaccouncil.org/index.php?option=com_content&view=article&id=87&Itemid=194

2. Internally-developed information, such as that obtained through an appropriate configured and maintained information security continuous monitoring system.[13]

Given that companies are essentially required to be reasonably aware of their cyber-risks, they have obligations to institute and maintain appropriate controls. The specific security controls and configurations which are risk-appropriate depends on company and information system specific factors. There is, however, a broad consensus on a core set of 20 Critical Security Controls that were compiled by the Center for Strategic and International Studies (CSIS) with extensive input from federal officials.[14] This set of core security controls is also endorsed by the UK government.[15]

A company's existing security controls may or may not use the specific terminology of the 20 Critical Controls and/or may rely on accepted industry standards or practices. Use of such standards or practices does not mean that the organization's cyber defense controls are lacking. The draft Executive Order emphasizes reliance on voluntary industry standards. Specifically, the most recent draft states

> *The Cybersecurity Framework shall be consistent with international standards whenever feasible, and shall meet the requirements of the National Institute of Standards and Technology Act, Public Law 104-113, and OMB Circular A-119.*

Although the Technology Transfer Act and OMB Circular A-119 are often understood to refer to standards which have been through an extensive consensus standard-setting process, the OMB guidance is actually far more flexible and recognizes "consortia" standards as well as consensus standards.[16] Thus, it may be possible to cross-walk many or all of a company's existing security controls to the list of 20 Critical Controls.

The final crucial issue is what should be reported in event of a successful cyber-attack?

The SEC guidance document states that "[r]egistrants that fall victim to successful cyber attacks may incur substantial costs and suffer other negative consequences..." and provides a sample list of "substantial costs and...other negative consequences" from a successful cyber attack. It should be noted that the SEC's list

---

[13] http://www.federalnewsradio.com/494/2606114/Continuous-monitoring-requires-strong-leadership-and-software

[14] For an overview of the controls, including how they map to NIST SP 800-53, see http://www.sans.org/critical-security-controls/guidelines.php. For a more detailed discussion, see http://www.sans.org/critical-security-controls/cag4.pdf

[15] http://www.cpni.gov.uk/advice/cyber/Critical-controls/

[16] See, http://www.thecre.com/pdf/whitepaper.pdf. CRE's views on the use of consortia standards have been accepted around the world. See, for example, http://ec.europa.eu/enterprise/newsroom/cf/_getdocument.cfm?doc_id=4565 and http://wenku.baidu.com/view/0fd1d5c14028915f804dc2ea.html?from=related

of harms could serve as the template for a shareholder cyber-related lawsuit. Of particular concern is that the SEC included in their document indirect and difficult to measure harms such as "[r]eputational damage adversely affecting customer or investor confidence."

Thus, overly extensive reporting could trigger lawsuits which would benefit only the trial lawyers.

It is clear, however, that not all information should be reported. In addition to directing companies to "avoid generic 'boilerplate' disclosure" the guidance document emphasizes that "federal securities laws do not require disclosure that itself would compromise a registrant's cyber security."

There are, however, two additional limitations on registrant disclosure, the Data Quality Act[17] and the Paperwork Reduction Act (PRA).[18]

The DQA sets quality standards that information must meet before federal agencies are allowed to disseminate it. The DQA and its implementing guidance documents also require more stringent quality controls for more important information. Of particular note, the DQA applies to third-party data,[19] such as data provided by SEC registrants.

Among the DQA's standards, is that "Utility" requirement. As the SEC explains "Utility" in their own agency-specific DQA implementing guidelines,

> *The Commission evaluates and determines the audience for whom the information to be disseminated is intended and will benefit. The Commission is committed to maximizing the utility of the information it disseminates to the public. To this end, information and the appropriate form and vehicle for its dissemination should be evaluated and reviewed by the relevant subject matter experts on a given project, along with appropriate levels of management within the Commission, before the information is disseminated to ensure its usefulness to the intended audience.*[20]

Unless data reported by third-parties meets relevant quality standards, federal agencies cannot make use of the data.

The Paperwork Reduction Act, which controls the flow of information from third-parties into the federal government, requires that information have "practical utility" which has been defined by OMB as meaning that the information has,

---

[17] http://thecre.com/quality/index.html

[18] http://thecre.com/ombpapers/PaperWorkReductionAct.htm

[19] http://www.circleid.com/posts/20120816_the_federal_cybersecurity_regulation_already_in_place/

[20] http://www.sec.gov/about/dataqualityguide.htm

> *actual, not merely the theoretical or potential, usefulness of information to or for an agency, taking into account its accuracy, validity, adequacy, and reliability, and the agency's ability to process the information it collects (or a person's ability to receive and process that which is disclosed, in the case of a third-party or public disclosure) in a useful and timely fashion.* 5 CFR 1320.3(l)

Taken together, the DQA and the PRA mean that companies may report only cyber-risk and attack information which complies with federal information quality requirements, including requirements that the information possess utility to intended users, such as investors.

Consistent with the DQA's principle that the "more important the information, the higher the quality standards to which it should be held" [67 Fed Reg 8452, col. 3] the greater the importance of cyber attack-related information, the more stringently it needs to be checked and verified to ensure compliance with all applicable standards and requirements prior to reporting.

The four primary components of a cyber security reporting safe harbor can be summarized as follows:

Cyber Security Reporting Safe Harbor	
Component	**Implementation**
Threat Awareness	Use Continuous Monitoring, Critical Control #4, and Participation in federally-sponsored cyber security information sharing processes
Security Controls	Use of the 20 Critical Controls and mapping company-specific practices and industry standards to the set of critical controls.
DQA and PRA compliance on all reporting decisions	Decision-making criteria developed in consultation with DQA/PRA experts
Adopt the Safe Harbor Provisions of the Proposed Legislation	Establish a National Cyber Repository; an organization which would be the keeper of reported intrusions upon reporting the SEC registrant is immune from action by any federal party

Next Steps

The litigation threat a corporation faces from cyber-intrusions is best summarized by SEC spokesman John Nester:

> *This year, the SEC sent dozens of letters to some companies, asking about cyber-security disclosures and later pushing companies to disclose*.[21]

Trial attorneys are following the SEC-initiated developments very closely as indicated in the earlier sections of this document. The combination of an expansive yet largely ambiguous SEC reporting program coupled with a very active plaintiffs bar presents a growing litigation threat to SEC registrants.

The challenge to SEC registrants is to inform the SEC of the "balance" needed in its guidance and regulation without appearing as an obstacle.

CRE is not a registrant and is a recognized regulatory watch dog who regularly intervenes in regulatory proceedings.

1. ***Present a Proposed Safe Harbor to the SEC***. The safe harbor outlined above should be presented to the SEC for their review and consideration.

2. ***Present the SEC with a White Paper on the Applicability of the Paperwork Reduction Act and the Data [Information] Quality Act to the SEC Cyber Security program***. There are two statutes which govern SEC information collection and information dissemination policies; the Paperwork Reduction Act and the Data [Information] Quality Act.[22] Although these two statutes play a dominate role in federal information policy they have not entered the cyber security debate in part because of the silo effect generated by cyber security technical personnel and the SEC bar.

   Nonetheless the two aforementioned statutes are two mechanisms which could be used to curtail the essentially unlimited reporting of cyber intrusions to a SEC registrant's network.

3. ***Subject the SEC Cyber Guidance to Notice and Comment***. Given the imminent promulgation of the Executive Order on cybersecurity, the SEC cyber guidance should be subject to Notice and Comment. Fortunately one need not request the SEC to perform such

---

21 http://www.bloomberg.com/news/2012-08-29/sec-guidance-on-cyber-disclosure-becomes-rule-for-google.html

22 http://www.thecre.com/pdf/20120301_NavalLawReview.pdf

a task; instead stakeholders can utilize in the Interactive Public Docket[23]:developed by CRE to vent Regulatory Cyber Security[24] issues.

4. ***Petition the SEC to Perform A Benefit/Cost Analysis of its Cyber Reporting Guidance***. As numerous reports in the media state, SEC registrants are going to try their best to accommodate the wishes of the SEC. For this reason their cyber "guidance" is for all practical purposes a regulation. The *de facto* regulation should be subjected to a benefit-cost analysis.

5. ***Review SEC Compliance with the Paperwork Reduction Act***. The SEC has reporting requirements in its existing regulation as well as its recently released guidance on cyber security. Analyses should be undertaken to review compliance with the Paperwork Reduction Act, in particular a review of the burden it places on SEC registrants.

6. ***Establishment of Public-Private Partnerships***. Public-private partnerships are essential components of any effective cyber defense strategy. For more information, see FISMA Focus here, http://www.thecre.com/fisma/?p=4068.

---

[23] http://en.wikipedia.org/wiki/Interactive_Public_Docket

[24] http://www.thecre.com/fisma/