



## **ITI Recommendation: Addressing Liability Concerns Impeding More Effective Cybersecurity Information Sharing January 2012**

In October 2011, the Information Technology Industry Council (ITI) provided policymakers a set of recommendations to improve cybersecurity information sharing.<sup>1</sup> As we noted, information sharing is critical to improved cybersecurity. One of our key recommendations is to address liability concerns that currently impede the flow of information. We cited the need for limited safe harbors when private sector entities voluntarily disclose threat, vulnerability, or incident information to the federal government or other private entities for the purpose of improving cybersecurity.<sup>2</sup> As we explained, entities holding information about cybersecurity risks often decline to voluntarily disclose it, or delay disclosure, for fear that disclosure might be the basis for private or government lawsuits or regulatory actions.

***This paper provides concrete examples of existing liability challenges and suggests legislative approaches that, by creating limited protections, could address those challenges.*** The paper also explains why private-sector contracts cannot sufficiently address these liability concerns. Finally, it provides examples of why and how information provided to the federal government must be protected from disclosure. The liability protections suggestions below, if enacted, will help to remove disincentives to voluntary disclosure of cybersecurity information by private entities. Further, these protections will incentivize entities to share information, which will help their own cybersecurity posture as well as cybersecurity for all stakeholders.

### **Current situation**

Currently, if a private entity notifies other private entities or the federal government of a confirmed or suspected cybersecurity threat or incident immediately upon detection, in advance of a full investigation and the development of countermeasures/remediation of the threat or incident, the entity may put itself at increased risk of regulatory or legal action in the process. Subsequent investigation may even find that no incident actually occurred or that the incident was sufficiently limited that there was no legal duty to report it even though others in the industry might benefit from what the company has learned. Because of the liability risks of sharing threat information, companies are hesitant to report cybersecurity concerns early, leaving the rest of the industry unaware and more vulnerable to similar threats. Thus, the tangible benefits of sharing information (i.e., multiple companies immediately aware of a suspected cyber incident and engaged in efforts to develop countermeasures) are limited and the risks may be deemed too great.

---

<sup>1</sup> See “ITI Recommendation: Steps to Facilitate More Effective Information Sharing to Improve Cybersecurity,” October 2011.

<sup>2</sup> Liability related to voluntary sharing of information on cybersecurity threats and incidents is just one type of liability relief that must be addressed to improve cybersecurity. Other liability concerns arise from actions taken by the private sector to address cyber incidents resulting from government-declared cyber emergencies, etc.

As a result, the status quo favors “the bad guys” since fewer incidents or threats are reported at early stages, giving hackers, thieves, and spies more opportunity to conduct their crimes.

### **Desired situation**

Entities must be able to provide information at an earlier stage without fear of legal repercussions. This will reduce potential costs to the entity in question—for example, by quickly reporting an incident or suspected incident, an entity may be able to limit its own monetary losses from stolen intellectual property (IP) or the costs it might need to incur to inform customers of a data breach. This also will improve cybersecurity for the greater good, as additional entities can move more quickly to stem losses, protect their systems, their customers, and the like.

### **Examples of liability scenarios**

#### **LIABILITY RELATED TO FEDERAL REGULATORY PURPOSES**

**Scenario:** Company A voluntarily reports what may be a cybersecurity incident in an information-sharing environment, such as in an Information Sharing and Analysis Center (ISAC) or directly to the government, such as to the FBI, before the company has confirmed extent of the incident. The company’s internal investigation later finds that a database was compromised that included Individually Identifiable Health Information as defined under the Health Insurance Portability and Accountability Act (HIPAA).

#### ***Potential result:***

- The Federal Trade Commission (FTC) uses the information submitted to the ISAC or FBI as evidence in a case against Company A for violating the security provisions of HIPAA.

#### ***Liability protection needed:***

- Clarification that the information shared cannot be the basis for regulatory action (through adjudication, rulemaking, or otherwise).
- Limiting liability in this case would not aim to insulate the private-sector entity from any regulatory action. A regulatory agency could still regulate Company A using other evidence or evidence gathered from another source.

#### ***Potentially acceptable legislative language:***

- Chairman Rogers’ draft “Cyber Intelligence Sharing and Protection Act of 2011” contains language that will meet these needs:  
*(b) (2) (C) (iii): USE AND PROTECTION OF INFORMATION- Cyber threat information shared in accordance with paragraph (1)... if shared with the Federal Government—(iii) shall not be used by the Federal Government for regulatory purposes.*

## LIABILITY RELATED TO CIVIL OR CRIMINAL LAW

Four scenarios are provided below. Scenarios 1, 2, and 3 all can be addressed with legislative language offered at the end of the three Scenarios. Scenario 4 deals with the federal government requesting a delay in a company's public disclosure of information in order to preserve an ongoing criminal or national security investigation. Potential legislative language is offered for Scenario 4.

**Scenario 1:** Company A voluntarily reports what may be a cybersecurity incident in an information-sharing environment, such as in an ISAC, or directly to the government, such as to the FBI.

***Potential result:***

- Government prosecutors, law enforcement agencies, or civil attorneys use this information as the basis for establishing a violation of civil or criminal law against Company A.
  - A customer, partner, or unaffiliated entity harmed by the incident sues Company A for not informing them of the incident as soon as they were aware of it. Company A's disclosure can be seen as a "smoking gun" or "paper trail" of when Company A knew about a risk event though Company A did not yet have a legal duty to report the incident.
  - Such allegation could lead to costly litigation or settlement regardless of its validity.
- 

**Scenario 2:** Company A reports what may be a cybersecurity breach in an information-sharing environment. At the same time, Company A—which is a publically traded company—does not believe the suspected breach has reached the threshold of a reporting requirement under the securities laws. This could be because Company A is unsure if a breach actually has occurred (and is using the information-sharing environment to find further information), or because at the time information was shared the breach appeared to be minor. After a month of forensics, it becomes clear that the breach was much more serious than originally thought, triggering a duty to disclose to the SEC.

***Potential result:***

- Investors sue Company A alleging that it withheld material information by not reporting the breach to the SEC at the time it became suspected or known.
- 

**Scenario 3:** Company A voluntarily reports what may be a cybersecurity threat or incident in an information-sharing entity, such as in an ISAC. The ISAC membership includes competitors of Company A.

***Potential result:***

- A plaintiff claims that the information shared is an effort to harm competition and sues Company A for violating antitrust laws.

***Liability protection needed for Scenarios 1, 2, and 3 above:***

- Clarification that the information Company A shared cannot be used as evidence against Company A in civil or criminal litigation.
- Limiting liability in these cases would not aim to insulate the private-sector entity from any legal proceedings including criminal prosecution. The only limitation would be on the use of information learned based on it being provided in a cybersecurity information sharing environment. Prosecutors or law enforcement agencies could still prove the same violation against Company A related to a reported cybersecurity incident using other evidence or evidence gathered from another source.

***Potentially acceptable legislative language for Scenarios 1, 2, and 3 above:***

- Chairman Rogers' draft "Cyber Intelligence Sharing and Protection Act of 2011" contains language that will meet these needs:  
*Sec. (2) (b) (3): EXEMPTION FROM LIABILITY – No civil or criminal cause of action shall lie or be maintained in Federal or State court against—  
(A) a protected entity, self-protected entity, cybersecurity provider, or an officer, employee, or agent of a protected entity, self-protected entity, or cybersecurity provider for using cybersecurity systems or sharing information in accordance with this subsection or a failure to act on information obtained from such using or sharing; or  
(B) a person or entity if the person or entity relied on a good faith determination that this subsection permitted the conduct complained of by such action.*
- In addition, legislative language should explicitly provide that voluntary receipt or disclosure may not be used as evidence that the receiving or disclosing organization, as applicable, has not timely or completely fulfilled any duty to warn or other obligation (common law, statutory, or contractual) that such organization may have.

---

***Scenario 4:*** Company A voluntarily shares within an information-sharing entity, such as an ISAC, information on a cybersecurity threat. The federal government asks for a delay in Company A's public disclosure of this information, even though securities or other laws require Company A to do so, in order to preserve an ongoing criminal or national security investigation.

***Potential result:***

- A customer, partner, or unaffiliated entity harmed by the incident sues Company A for not informing them of the incident as soon as they were aware of it.

***Liability protection needed for Scenario 4:***

- Organizations cooperating with the federal government should have a defense against claims for failure to warn when a qualified law enforcement agency formally instructs that no further disclosures be made.

- This would occur after an appropriate determination by the government that disclosure could reveal law enforcement methods or sources, impede investigations, or impair national security.

***Potentially acceptable legislative language for Scenario 4:***

- Senator Pryor’s draft “Data Security and Breach Notification Act of 2011” (S. 1207) contains language that will meet these needs:  
*Sec. 3 (c) (2) DELAY OF NOTIFICATION AUTHORIZED FOR LAW ENFORCEMENT OR NATIONAL SECURITY PURPOSES-*  
*(A) LAW ENFORCEMENT- If a Federal, State, or local law enforcement agency determines that... notification...would impede a civil or criminal investigation, such notification shall be delayed upon the written request of the law enforcement agency for 30 days or such lesser period of time which the law enforcement agency determines is reasonably necessary and requests in writing. A law enforcement agency may, by a subsequent written request, revoke such delay or extend the period of time set forth in the original request made under this paragraph if further delay is necessary.*  
*(B) NATIONAL SECURITY- If a Federal national security agency or homeland security agency determines that notification...would threaten national or homeland security, such notification may be delayed for a period of time which the national security agency or homeland security agency determines is reasonably necessary and requests in writing. A Federal national security agency or homeland security agency may revoke such delay or extend the period of time set forth in the original request made under this paragraph by a subsequent written request if further delay is necessary.*

<p><b>Private contracts are insufficient</b></p>
--

Some policymakers have asked if private-sector contracts can provide appropriate cybersecurity information-sharing liability protections. They cannot. First, although contracts can have limits on liability, most contracts have key exclusions to these limits under which lawsuits related to cybersecurity information sharing could be filed. Examples of such exclusions are 1) intentional breach of confidentiality and 2) intentional breach of IP. Second, only parties to a contract are bound by its limits on liability. As a result, contractual provisions cannot protect an entity from civil or criminal prosecution by a third party. Third, two private parties cannot negotiate away risks associated with antitrust liability.

In addition, as a general principle from a policy perspective, the law should encourage information sharing regardless of whether someone has written a favorable contract. In the event of a cybersecurity incident, the law should encourage companies to share threat information as early as possible, without the delays associated with engaging counsel to review the liability provisions in each of their contracts.

## Addressing Freedom of Information Act (FOIA) concerns

In addition to liability protection, to encourage greater information sharing information provided to the federal government must be protected from disclosure.

**Scenario:** Company A voluntarily shares with the government information on a cybersecurity threat in the belief the information will be safe and treated appropriately. The government then must disclose this information in response to a FOIA request by a reporter.

### **Potential results:**

- Although Company A had no duty to disclose this information, it is the subject of negative press reports after disclosing to the government that it has been subject to a cyber incident and has to develop a public relations strategy to counter these impressions. In other words, Company A gets “dragged through the mud.” It loses current and potential customers due to this negative press.

### **Protection needed:**

- Information on real or suspected cybersecurity threats voluntarily disclosed to the government should be exempt from disclosure under FOIA.

### **Potentially acceptable legislative language:**

- Chairman Rogers’ draft “Cyber Intelligence Sharing and Protection Act of 2011” contains language that will meet these needs:  
*(b) (2) (C) (i-ii): USE AND PROTECTION OF INFORMATION- Cyber threat information shared in accordance with paragraph (1) ... if shared with the Federal Government—(i) shall be exempt from disclosure under section 552 of title 5, United States Code; (ii) shall be considered proprietary information and shall not be disclosed to an entity outside of the Federal Government except as authorized by the entity sharing such information...*

## Conclusion

Effective sharing of actionable information among the public and private sectors on cyber threats, vulnerabilities, and incidents is an essential component of improving cybersecurity. Of course, information sharing itself is not the goal, but one of a number of tools to enhance security of information technology (IT) systems. The objective of an effective environment for information sharing is to exchange timely and relevant information that appropriate stakeholders can use to make decisions and take necessary actions to maintain situational awareness, respond to threats and incidents, and manage and mitigate cyber risk. The more actionable and real-time information sharing that we have, the better chance we have in keeping pace with cyber adversaries rather than simply reacting after the fact.

Treating organizations as trusted partners will be an incentive for them to be more proactive in stepping forward in the interests of their customers, employees, shareholders,

and the national interest. To encourage organizations in possession of actionable threat information to come forward, Congress should introduce proposals to clearly extend liability protection to both the disclosure of the information and to the resulting impact from exploitation of a reported vulnerability.

While effective liability protections are essential to enable more effective information sharing from the private sector, at the same time—as ITI noted in our October 2011 paper—efforts also must focus on improving information flow from government to the private sector. This will enable the private sector to effectively manage risk, enable post-event response and recovery, and make decisions regarding protection strategies, partnerships, mitigation plans, security measures, and investments for addressing risk.

ITI looks forward to the opportunity to help Congress to build on these recommendations and work through the complicated issues in this area.