# CYBERSECURITY ACT OF 2015 REVIEW

## What it Means for Cybersecurity Governance and Enterprise Risk Management

Written By:

Joseph J. Panetta &
R. Andrew Schroth

KOGOD SCHOOL of BUSINESS

AMERICAN UNIVERSITY • WASHINGTON, DC

KOGOD CYBERSECURITY GOVERNANCE CENTER

## Previous publications in The Changing Faces of Cybersecurity Governance Series

September 2015

### CYBERSECURITY REGULATION AND PRIVATE LITIGATION INVOLVING CORPORATIONS AND THEIR DIRECTORS AND OFFICERS: A LEGAL PERSPECTIVE

By Perry E. Wallace, Richard J. Schroth and William H. DeLone

# SUMMARY

Signed into law on December 18, 2015, The Cybersecurity Act of 2015 (CSA) calls on public and private entities to share information relevant to cybersecurity. The CSA is rolled up under the Consolidated Appropriations Act of 2016 and is comprised of four subsections: Cybersecurity Information Sharing, Federal Cybersecurity Enhancement, Federal Cybersecurity Workforce Assessment, and Other Cybersecurity Matters most relevant for private sector[1]. This paper specifically focuses on Title I - Cybersecurity Information Sharing and provides an executive overview as it relates to cybersecurity governance and enterprise risk management.

Key points relevant to business of the recently passed law include:

- Businesses have the option of participation
- DHS is designated as the consolidator of information to better enable organizations in a response
- Companies are authorized to monitor for cyber threat information
- Information shared must be sanitized of customer and company employee personal identifiable information (PII) so not to disclose who the provider of the information is
- The government can share a company's cyber threat indicators (if volunteered) with federal agencies and non-federal entities; albeit the information is still proprietary and can only be disclosed at the behest of the owner
- Federal agencies are authorized to receive cyber threat information gathered
- Companies are granted immunity if they are compliant in data sharing policies

The law orders The Department of Homeland Security (DHS) to take action in building up an information-sharing database called the Automated Indicator Sharing system. This database aims to create a voluntary process for distributing information between public and private entities, and sharing best practices leading up to and throughout a breach.

The database is designed to be anonymous and will be stripped of any sensitive and proprietary information. In essence, the database will act as a rolodex where different cybersecurity measures can be referenced if and when a significant event happens. These measures include threat indicators and defensive measures (collectively defined in the bill as "cyber threat information"). The database will help a private entity monitor its own information systems better because of the actionable information included in the database. Finally, CSA asks specific government entities to release best practices so companies can periodically be informed of what anomalies to look for in a possible breach, and ways to best defend against potential threats. DHS has identified small to mid-sized businesses as the first target for opting in, but ultimately hopes for large-scale participation. To further confirm this trend, The Assistant Secretary in the Office of Cybersecurity and Communications, Dr. Andy Ozment, stated in a recent interview, the idea is to start with a small number of companies and scale upward[2].

**DHS has identified small to mid-sized businesses as the first target for opting in, but ultimately hopes for large-scale participation.**

# DEFINING THE LANDSCAPE OF CSA: A GOVERNMENT CORPORATE PARTNERSHIP

Before opting into the law companies need to recognize what "information" is required to be shared in the program led by DHS. There are two main definitions within the law: cyber threat indicators and cyber defensive measures. As written in the CSA, cyber threat indicators are the "technical data that indicates how networks have been attacked," which might include how the attack initially materialized. Cyber defensive measures are "how such attacks have been successfully detected," or how the threat actor worked to disrupt and/or permeate a company's information systems[3]. The combination of these two measures is referenced throughout the new law as cyber threat information. The collection of cyber threat information is done to help share best practices of prevention, and/or containment, to improve business continuity.

For those companies that decide to opt into the sharing program, network monitoring is of the utmost importance in the law. When a private company commits to the voluntary program, it is permitted to monitor its information systems, but does not have access to other companies' raw data and networks. This provision provides the ability for a real-time data-tracking program. The action is specifically referenced within the definition of threat indicators and should solely be used for examination of a company's own network. Defensive measures to protect a company from a potential compromise or loss of proprietary information are still permitted, however "hacking back" is noted as not acceptable[4]. Information shared will remain proprietary when disclosed to DHS, but the leading federal agency has the duty to make the information available to other departments, including The Departments of Defense and Energy. However, the information shared is exempt from public disclosure[5].

The end state of the law is to facilitate better communication and information sharing between private and public organizations to target cybersecurity malevolence. The law encourages the passing of cyber threat indicators to DHS by granting immunity so that private entities cannot receive lawful action for information shared with the government. Section 106 of the CSA explains that retribution cannot be taken against companies that do not participate in the sharing of information. One way a company gives up its immunity is if it violates sharing of particular information (e.g. classified material). Furthermore, it is compulsory for the sharing company to review and sanitize all cyber threat information of PII. The Department of Justice has been ordered to help companies comply with the law by providing guidance for the filtering of shareable cyber threat information.

> **"The Cybersecurity Act of 2015 will become a powerful tool that aligns both private sector and government interests toward a cleaner cyber ecosystem."**
>
> *Israel Martinez,*
> *President and CEO of Axon Global*

# SAFE HARBOR AND LIMITING LIABILITY

In the case of CSA, the law provides private entities safe harbor from certain liability for specific information sharing activities. To find protection under the concept of safe harbor, these same entities must qualify for this privilege by sharing information under specific guidelines detailed in CSA[6]. Under this concept, Safe Harbor is a provision in the law that affords protection from liability or penalty under specified circumstances or if certain conditions are met[7]. One of the issues associated with establishing safe harbor is that while a corporation may meet the "technical" standard of qualifying for such protection, two further questions need to be asked: Did that same entity act in bad faith leading up to the event by not taking the proper precautions to protect their company? And, Did the company act in a responsible manner prior to the situations? The law clearly states, that in order to benefit from the liability protections, companies must keep records evidencing its compliance.

### Why create such a clause limiting liability?

One of the greatest barriers to companies sharing cyber threat information is the perceived liability associated with reporting. With inclusion of the limited liability clause, the government is taking pressure off the private sector with the hope that companies will self-report their own issues[8]. Alternatively, this opportunity could prove potentially dangerous for companies. Given the government has opened the opportunity, it may expect companies to voluntarily comply with this method of reporting. Those companies that choose not to report may do so at an increased risk. It seems logical that shareholders and attorneys will be asking the question; "Given the organization had the opportunity to enjoy liability protection, why did the company choose not to participate?" These are the questions that corporations will face as they are confronted with this issues of anonymous reporting.

### The Governance Impact

Perhaps the biggest issue created by the Cybersecurity Act for corporate governance is the law squarely places a policy issue for information sharing on the footsteps of boards of directors. While meeting the technical standards for reporting may be relatively straightforward, the larger question that looms is "should we" report? Imagine your company has been breached, and now you are faced with the decision of sharing that information through CSA. Could the information submitted lead to further questions by the federal government? Although the law makes its case for safe harbor, currently there is no case precedent determined by the courts around the interpretation of this law and the applicability of its safe harbor provisions. It may take years of case law and challenges to sort out the foundations of such actions on a company's part.

Additional questions arise for companies conducting international business in Europe. The law does not apply to the more rigorous European hurdles for privacy and personal information sharing. Non-attribution is the critical ingredient for such success; however, we again do not know enough about how this will work. Insider threats pose another unknown variable. Should an informant or insider threat be detected in a company, it is unknown what protections the new law will provide a company around its hiring practices or internal protective mechanisms to safeguard these events that are not related to the world of cyber.

When considering the impact on the boards of directors, there are many unknowns. The guidance that a board provides management is to follow the law. However, in this case, there is a voluntary nature to the law of information sharing. At some point in the board's deliberations, there will need to be a general conversation by the board either to encourage the corporation to follow the guidelines immediately, or wait and keep the board updated

as the law matures. The other tactic that might be seen in the boardroom would be for the discussion never to take place, thereby creating a situation of plausible deniability for board members. It is unclear whether non-action will be seen as an adequate defense, or be seen as an overt action to avoid adhering to the "spirit" of information sharing.

Referenced in the law, companies that have or are planning to gain government contracts will need to have their boards of directors understand this law. As previously stated, CSA does not create any duty to share cyber threat information, and expressly prohibits the federal government from attempting to coerce sharing by withholding cybersecurity information or other benefits such as government contracts. The corporate community has expressed concern with sharing large amounts of data and wants to ensure there is no forcible request by the government to turn over large swaths of user data[9]. Some experts say sharing cyber threat information with the federal government will not constitute a waiver of any applicable privilege or protection provided by law, including trade-secret protection, and shared cyber threat indicators. Defensive measures are exempt from disclosure under the Freedom of Information Act and other federal, state, and local freedom of information laws[10].

### On the Horizon for Boards of Directors

Jones Day, a global law firm, is following another law on the horizon that may ask of more cybersecurity details from boards of directors, and is supportive legislation to CSA. The critical issue in this law would require publicly traded companies to disclose, in its investors' filings with the SEC, whether any member of its board of directors is a "cybersecurity expert." Companies that lack a cybersecurity expert on its board would be compelled to explain, in its corporate disclosure forms, why it does not have that expert, and why an expert is not necessary for the company. In addition, it must provide information on the measures the company is taking to improve cybersecurity[11].

**"The insurance industry is potentially a major stakeholder in the success of CSA. It can and should incentivize companies to share threat information as a best practice through lower cyber insurance premium for example. Many insurers have been reluctant to do this to date citing little or no actuarial data to price risk accurately. However, CSA could be the means to help build a repository of anonymized loss data that the industry has been calling for from DHS over the last three years."**

*Ben Beeson,*
*Cyber Risk Practice Leader,*
*Lockton Companies*

# CYBERSECURITY ACT'S CORPORATE GOVERNANCE IMPLICATION

## THE CYBERSECURITY ACT OF 2015 AT A GLANCE

This chart depicts the implications of the CSA on corporate governance. It lays out selected items within the legislation, their intent, and the implications that they will have on corporate governance.

### Corporate Governance Implications

| Item in the legislation | Intent | Governance Implications |
|---|---|---|
| Participation is optional | To encourage the private sector to participate without the mandates from the government for information sharing. Provide a pressure and release and option to companies. | Boards will need to understand the pros and cons of voluntary participation. Part of the governance educational process will be to discover what this means for their company in terms of when to report, whether not to report and or whether they are best served in reporting by anonymously identified material. |
| Authorizes companies to monitor cyber threat information | Yet to be interpreted, there appears to be permission to create a more "active" monitoring environment inside of companies. Turns the tables to where good-guys can monitor bad actors that have intent to do harm. | Boards will need guidance as to the level of monitoring they would expect the company to implement outside of its own firewalls. This will require boards to begin to set parameters to concepts like "pro-active defense." |
| The government can share a company's cyber threat indicators (if volunteered) with federal agencies and non-federal entities | To increase the ability for the government (DHS) to share anonymous information with other agencies; to avoid duplication of efforts; to provide a larger pool of data to be analyzed from the various perspectives of a wide range of federal agencies. | Boards will need to get an understanding of what the risks are and advantages of becoming a cooperative partner with the Federal Government. Boards will have to collaborate with the cyber management team and/or the boards' own advisors who know the ins-and-outs of what is a stake. |
| Authorizes knowledge distribution to federal agencies | To get a big picture view of how bad actors are organizing and behaving. | Boards will want to understand the trends related to the larger cyber picture for their company. This is particularly true as it applies to valuation, reputational risks, and investor relations. |
| Immunity is granted if compliant in the private entities data sharing | Private sector can be released of liability to encourage it to report compromises systematically. | Governance and policy will need to address how to share some information without specific knowledge of certain types of breaches. The board needs to understand that the process of information sharing under the Cybersecurity Act of 2015 is still in its infancy and there has been little or no cases tried in court that have used this as a defense against prosecution. The intent is still resting on fragile interpretations depending upon how future cases are litigated. |
| The government will be required to create a portal for information sharing. It limits the government's use of threat information to cybersecurity purposes, which includes threats to minors and countering cyber-related crimes. | The government wants to make it as easy as possible to encourage a company to share its information, ultimately manifesting itself in automated exchanges between the government and companies. This will allow real time processing of new cyber threats to the community so it can defend itself more effectively. | Boards will want to discuss directly interacting with federal agencies in this fashion. Opening this line of interaction with large amounts of data has potential risks associated with the exchange. Boards will need to define the risk tolerance, risk mitigation and risk responses that allow or disallow certain reactions to threats. |

# CONCLUSION

The CSA provides companies with a voluntary program, as delivered in Title 1- Cybersecurity Information Sharing, and emphasizes the importance of sharing data across private and public entities. In particular, the law is a basis for knowledge management, and builds upon what Information Sharing and Analysis Centers (ISAC) have been working to do for over fifteen years. The CSA is focused on getting the most recent cybersecurity related material catalogued so it can analyze and send out information to the companies that have opted in. There are a plethora of actions required by the almost dozen federal agencies referenced in CSA, and on February 16, 2016, DHS released guidelines for sharing threat indicators through the department's Automated Indicator Sharing system. The guidelines deliver transparent actions for participation and expectations of the program[12]. At this juncture, it is the priority of DHS to work with the small to medium sized companies that may not think in terms of being "cyber-secure," but large companies with corporate boards need to begin to understand what is expected now. This newly enacted policy aims to drive the private and public sector into a stronger relationship geared towards being cyber secure, and it underscores the importance of a shared responsibility against potential cyber threats.

## ABOUT THE KOGOD CYBERSECURITY GOVERNANCE CENTER (KCGC)

The Kogod Cybersecurity Governance Center at American University aims to promote "good governance" in the preparation for, prevention and detection of, and response to cybersecurity breaches. The Center conducts collaborative, objective, multidisciplinary research related to cybersecurity governance, enterprise risk management, and cyber risk management across business, legal, public policy, and public administration disciplines. The Kogod Cybersecurity Governance Center focuses on management, leadership, and governance issues faced by corporate board members, C-level executives, and IT leadership.

## METHODOLOGY

In order for the Kogod Cybersecurity Governance Center to remain objective, research was driven by actual explanations in the recently passed Cybersecurity Act. This formal review is to summarize the Cybersecurity Act of 2015 and break down its importance for the private sector. It is a compilation of what industry professionals are reporting about the law, and is designed to help the reader better decide whether to opt in or not. The white papers and government documents used to research the CSA were sought out for their neutrality to ensure this descriptive report does not express any individual point of view.

**Disclaimer**

The information in this paper is intended to provide an executive view of the Cybersecurity Act of 2015, with particular attention spent on aspects of cybersecurity information sharing. This is a business impact review and not intended to be legal advice.

# END NOTES


[1] H.R. 2029, 114th Cong. (2015) (enacted).

[2] Ozment, Andy. "Information Sharing and Cybersecurity." Interview by Rebecca Blumenstein. Wall Street Journal 10 Feb. 2016, CIO Network sec.: R4. Print.

[3] Segalis, Boris, Andrew Hoffman, and Kathryn Linsky. "Federal Cybersecurity Information Sharing Act." Data Protection Report. Norton Rose Fulbright, 03 Jan. 2016. Web. 28 Jan. 2016.

[4] Sullivan, Cromwell. The Cybersecurity Act of 2015. Rep. Sullivan & Cromwell, LLP, 22 Dec. 2015. Web. 3 Jan. 2016. https://www.sullcrom.com/siteFiles/Publications/SC_Publication_The_Cybersecurity_Act_of_2015.pdf.

[5] "S. 754 Cybersecurity Information Sharing Act." Benton Foundation. Web. 28 Jan. 2016. https://www.benton.org/initiatives/tracking-legislation/s-754-cybersecurity-information-sharing-act.

[6] Sullivan, Cromwell.

[7] "What Is Safe Harbor? Definition and Meaning." BusinessDictionary.com. WebFinance, Inc., n.d. Web. 12 Feb. 2016. http://www.businessdictionary.com/definition/safe-harbor.html.

[8] Martinez, Israel, and Richard Schroth. "Decoding New Cyber Regs for Midsize Businesses." Middle Market Growth. Association for Corporate Growth, 9 Feb. 2016. Web. 12 Feb. 2016. http://www.middlemarketgrowth.org/decoding-new-cyber-regs-for-midsize-businesses.

[9] Rosenzweig, Paul. "The Cybersecurity Act of 2015." Lawfare. The Lawfare Institute, 16 Dec. 2015. Web. 12 Feb. 2016. https://www.lawfareblog.com/cybersecurity-act-2015.

[10] Rosenzweig, Paul.

[11] Paez, Mauricio F., Randi C. Lesnick, and Michael La Marca. "Proposed Cybersecurity Act Misunderstands Role of the Board." Jones Day. Jones Day LLP, Dec. 2015. Web. 12 Feb. 2016. http://www.jonesday.com/proposed-cybersecurity-disclosure-act-shows-deep-misunderstanding-of-the-role-of-the-board-of-directors-12-28-2015/.

[12] U.S. Federal Government. Department of Homeland Security. Statement by Secretary Jeh C. Johnson on Implementation of the Cybersecurity Act of 2015. N.p., 16 Feb. 2016. Web. 16 Feb. 2016. www.dhs.gov/news/2016/02/16/statement-secretary-jeh-c-johnson-implementation-cybersecurity-act-2015.

# ABOUT THE AUTHORS

## JOSEPH PANETTA

Joseph Panetta is an MBA Candidate at American University's Kogod School of Business, where his concentration is in IT Service Management and Cybersecurity Governance. Joe is an Army Captain who has served in various leadership positions within the tactical and technical arena. A former Armor officer, he transitioned to the Signal Corps where he served as a communications and information systems chief, and later as a company commander responsible for deploying tactical communications equipment. He serves as the graduate operations leader and research assistant for the Kogod Cybersecurity Governance Center. His research is in cybersecurity educational applications for executive leadership, and cybersecurity effects on enterprise risk management policy.

## R. ANDREW SCHROTH

R. Andrew Schroth is an MBA Candidate at the American University Kogod School of Business where he serves as a Graduate Research Assistant in the Kogod Cybersecurity Governance Center. He completed postgraduate training certificate at Southern Methodist University in Intelligence. Andrew focuses on cyber business analysis and advanced intelligence discovery with special interest in the Board of Directors and cybersecurity governance. Since graduating with honors from Elon University he has had work experience in Account Management at MICROS Systems Inc., cyber advanced intelligence analytics with Axon Global Services, and has embarked on many entrepreneurial endeavors, most recently he has held the position of COO at a start-up company in the Washington D.C. area.

## ADVISORY COMMITTEE

**Ben Beeson**,
Lockton

**John Brady**,
FINRA

**Dr. Erran Carmel**,
Dean

**Steve Cooper**,
US Department
of Commerce

**Jim Dinegar**,
Greater Washington
Board of Trade

**Donna Dodson** (liaison),
NIST

**Tracie Grella**,
AIG

**Bruce Hoffmeister**,
Marriott International

**John Honeycutt**,
Discovery
Communications

**Gary LaBranche**,
Association of Capital
Growth

**Scott Laliberte**,
Protiviti

**Israel Martinez**,
Axon Global Services

**Jim Messina**,
The Messina Group

**Hitesh Sheth**,
Vectra Networks

**Stuart Tryon**,
U.S. Secret Service

**Dr. David Swartz**,
American University

**Ralph Szygenda**,
Senior Fellow

**Leif Ulstrup**,
Executive in
Residence

**David S. Wajsgras**,
Raytheon

## KCGC LEADERSHIP

**Dr. William DeLone**,
Executive Director

**Dr. Richard Schroth**,
Executive Director

**Dr. Gwanhoo Lee**,
Director of Center Operations

**Dr. Parthiban David**,
Faculty Research Director

THIS PUBLICATION IS SPONSORED BY

Discovery COMMUNICATIONS
FINRA
Marriott
protiviti
Raytheon

KOGOD SCHOOL *of* BUSINESS
AMERICAN UNIVERSITY • WASHINGTON, DC