ACC FOUNDATION:

THE STATE OF CYBERSECURITY REPORT

AN IN-HOUSE PERSPECTIVE

LEARN ABOUT the best practices, organizational roles, and experiences of in-house counsel in more than 800 organizations.

FIND OUT HOW top in-house lawyers mitigate the threat of breaches and safeguard their data.

DISCOVER INSIGHT from over 1,000 in-house lawyers in 30 countries.

ACC Foundation
Association of Corporate Counsel

Published by the ACC Foundation.

The ACC Foundation wishes to acknowledge with gratitude the contributions of Ballard Spahr LLP for its underwriting support of the *State of Cybersecurity Report.*

Ballard Spahr LLP

The ACC Foundation also wishes to recognize the following members of cybersecurity project advisory group for their contributions to the development of the *State of Cybersecurity Report:*

Phil N. Yanella, Ballard Spahr LLP
Kim Phan, Ballard Spahr LLP
Edward J. Willey III, Dallas, TX
Kerry L. Childe, Richfield, MN
Neal Dittersdorf, Intersections Inc.
Jandria S. Alexander, The Aerospace Corporation

Protecting What Matters

Companies process more information about their customers than ever before. And the consequences if that information is lost or inadvertently disclosed can be catastrophic. Our cross-disciplinary team of attorneys helps clients around the world mitigate risk, respond in the event of a crisis, and recover.

- Information Risk Management
- Asset Inventories
- Employee Training
- Transactions/Vendor Management
- Privacy and Consumer Marketing Compliance
- Data Incident Response Plans
- Network Intrusion/Data Breach Response
- Litigation
- Investigations
- Plan Assessment

Ballard Spahr LLP

Atlanta | Baltimore | Bethesda | Delaware | Denver | Las Vegas | Los Angeles | New Jersey | New York
Philadelphia | Phoenix | Salt Lake City | San Diego | Washington, DC | www.ballardspahr.com

TABLE OF CONTENTS

The State of Cybersecurity Report is a special study published by the Association of Corporate Counsel (ACC) Foundation. The ACC Foundation — a 501(c)(3) nonprofit organization — supports the efforts of the Association of Corporate Counsel, serving the needs of the more than 40,000 corporate lawyers employed by over 10,000 organizations in 85 countries. Through the dissemination of cutting-edge research and surveys, the ACC Foundation developed an unprecedented study of the state of cybersecurity in the corporate sector. Considering the increasingly active role general counsel play in cybersecurity strategy, risk assessment, and prevention, this report provides insight from more than 1,000 corporate lawyers. The largest study of its kind, the report aims to serve as a resource for corporations, lawyers, board of directors, and members of the public affected by one of the greatest challenges organizations face today — cybersecurity.

50%

of GC/CLOs want to increase their role and responsibilities when it comes to cybersecurity

In an environment where data breaches are largely an inevitability, assiduous preparation is key. Threats to an organization's information security are as varied as they are dangerous. Preventing, preparing, and responding to data breaches in real time is a chief concern for today's general counsel (GC) and chief legal officers (CLOs), who are increasingly called on to guide their organizations and aid with thwarting such attacks. Knowing common practices, what works, and what your peers are doing is key in benchmarking and planning to protect your company from risk. Straddling business, IT, and legal, today's GC/CLOs are uniquely positioned to engage the multiple stakeholders that a robust data protection regime requires. Execution of incident response plans, protection of privilege, and compliance and notification requirements arising from a breach — these are just some of the unique functions that legal is charged with to manage when data is compromised or lost. And with one in four CLOs/GC reporting a breach in the last two years[1], the damage and repercussions of major cybersecurity incidents will heighten the legal department's role in strategic planning and risk management as well as in responding to cybersecurity-related incidents.

Consumer exposure and privacy concerns have begun to weigh on government agencies and regulators as well. European regulators struck down the longstanding international Safe Harbor agreement, which had enabled American companies working in the European Union to transfer data painlessly. Various data protection bills are working their way through the US Congress, including the Cybersecurity Information Sharing Act recently passed by the Senate. And at a time of tension between the world's largest economies over cybersecurity in general, the United States and China held a cybersecurity summit in September 2015, pledging to ease off the burgeoning Internet arms race. Dealing with the dual threats of breach preparedness and compliance with cybersecurity laws is not trivial—it's no wonder that data security is one of the leading issues that keep in-house counsel up at night.

[1] *ACC 2015 CLO Survey, executive summary, page 3. www.acc.com/legalresources/resource.cfm?show=1389460*

The 2015 ACC Global Census of more than 5,000 in-house counsel in 73 countries found that in-house counsel considered cybersecurity one of the greatest challenges in complying with laws inside their jurisdiction, just behind privacy concerns, which ranked number one among all concerns.[2] In short, data security is top of mind for in-house counsel. And rightly so — data theft is a growing risk. No single metric can capture the immense cost of data breaches, but by any measure they represent a large and growing threat to virtually any company doing business today. The Center for Strategic and International Studies estimates that "the likely annual cost to the global economy from cybercrime is more than US $400 billion."[3]

Additionally, the average cost incurred per stolen record increased in 2015. The Ponemon Institute in its Cost of Data Breach Study: Global Analysis found that the average consolidated total cost of a data breach has risen 23 percent since 2013, clocking in at US $3.8 million.[4] And the average cost for each stolen record has risen as well. Costs per stolen record have risen due to mounting financial consequences of losing customers due to security incidents — likely due to high-profile news reports and consumers' increasing concern over the vulnerability of their data. Expenditures related to class-action lawsuits, compliance, damages, crisis management, and the necessity of forensic activities related to malicious data breaches have contributed to this rise in cost per compromised record as well.

No form of data is safe. Cybercriminals have come to value data that might otherwise seem difficult to monetize, such as personally identifiable information (PII), as it can be sold to third parties who specialize in exploiting such records. Data thieves have come to value data useful for long-term, insidious identity theft schemes over the "smash and grab" credit-card plots of yesteryear. Once compromised, it can take individuals years to recover and secure their information — or even to notice that it has been stolen in the first place. As such, safeguarding PII is a vital practice in maintaining the trust of the general public and regulators.

As more and more business data storage moves into cloud data storage servers, hackers have an ever-expanding trove of enterprise data to plunder. The theft of intellectual property has especially pernicious effects for industries that depend on intellectual property (IP) protection. It disproportionately affects market leaders that invest in research and development, and it discourages innovation. Corporations must now contend with increasingly sophisticated and well-resourced actors—targeting organizations rich in IP for strategic purposes or for competitors seeking to close the gap in proprietary manufacturing processes.

In keeping with the ACC Foundation's goal of generating the most comprehensive reports of its kind, and capturing as large a segment of the in-house counsel population as possible, we have surveyed mainly GC and CLOs[5] — hailing from 887 organizations in 30 countries — to chronicle information about cyber-related events that are not normally available to the public. **The State of Cybersecurity Report** therefore captures the thoughts of an unprecedented record number of in-house counsel. This survey also reveals best practices for preparation, crisis management, and breach response. Read on to find out what worked and what didn't, why breaches happen, how to prepare, and how to react.

[2] *2015 ACC Global Census, page 8. www.acc.com/legalresources/resource.cfm?show=1411926*

[3] *Net Losses: Estimating the Global Cost of Cybercrime, June 2014. Center for Strategic and International Studies*

[4] *2015 Cost of Data Breach Study: Global Analysis. IBM and Ponemon Institute. https://securityintelligence.com/cost-of-a-data-breach-2015/*

[5] *GC and CLOs constituted 77 percent of the total set of respondents for a total of 776 GC/CLOs*

KEY FINDINGS

Employee error is the number-one cited cause of breaches

Employee error is the most common reason for a breach. And while nearly half of all in-house counsel say that mandatory training exists, few have a policy of testing knowledge or tracking attendance at these trainings. Lawyers in Canada are least likely to say their company has mandatory employee training (29 percent) compared with those in the US, which has the highest percentage reporting so (48 percent). Overall, 17 percent of in-house counsel say the data accessed during a breach was encrypted.

Thirty-six percent of all respondents reported employee error as the cause of a system breach when an audit was conducted by an outside auditor compared with 26 percent of respondents when an audit was conducted by internal staff.

Reputation: the top concern worldwide when it comes to cybersecurity

Top concerns cited by in-house counsel include damage to reputation, loss of proprietary information, and economic damage. In Europe, the Middle East and Africa (EMEA), and Asia Pacific regions, government and regulatory action made the top three most cited primary concerns.

Data breaches are a reality for many

Nearly one in three in-house counsel have experienced a data breach at their company. Nineteen percent say their current company has experienced a data breach, while 10 percent say their former employer did. Nearly half (47 percent) have recent experience, reporting the breach took place in 2014 or 2015. Forty-five percent of in-house counsel in companies with 5,000 or more employees say they either work or have worked at a company that experienced such a breach.

Company and legal department budgets are growing when it comes to cybersecurity

Despite an overall trend toward insourcing, cybersecurity spend seems to be the exception for most law departments. Fifty-six percent of GC and CLOs say their company is allocating more money to cybersecurity than one year ago, and 23 percent say their legal department spend has increased as a result of company focus on cybersecurity. Among GC/CLOs who report an increase in departmental spend, 53 percent say this is mainly outside spend, and 24 percent report spend as equally split between inside and outside. Notably, just 8 percent of GC/CLOs have a portion of their departmental budget explicitly dedicated to cybersecurity-related issues despite the growing role of the legal department.

The expanding role of legal in the cyber arena

Fifty percent of all GC and CLOs want to increase their role and responsibilities when it comes to cybersecurity. Though oversight of cyber-risk continues to sit firmly in the IT department, the legal role is also expanding, with 57 percent of GC and CLOs expecting their department's role to increase in the coming year.

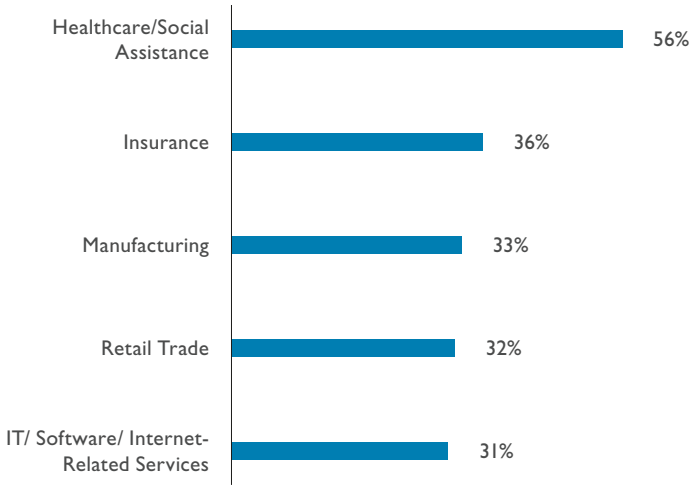
Cybersecurity insurance is becoming more common, and amount of coverage is rising

Half of all GC and CLOs surveyed say their company has cybersecurity insurance, and for companies that have this insurance, 68 percent have coverage valued at US $1 million or more. One in four say they expect their company to increase coverage in the coming year, while 58 percent expect it to remain the same. Barely 1 percent expect a decrease in cybersecurity coverage amounts. Among those who have experienced a breach, just 19 percent say the insurance policy fully covered the related damages.

Managing outside risk plays a significant role in preparing and preventing

With only 61 percent of GC/CLOs confirming that third parties are required to notify them should a breach occur, it appears outside support and risk are high for many companies. Just one in four report that their company has retained a forensic company, and one in three have retained outside counsel to help should a cybersecurity event occur. This leaves companies searching for outside support in many instances where data has been compromised. And just 7 percent of all in-house counsel surveyed are very confident that their third-party vendors and affiliates are protecting the company from cybersecurity risks. Twenty-two percent are very confident their outside service providers are managing the security of client data.

DATA BREACHES BY INDUSTRY*



*Industries with highest percentage shown

"I wish we had done a better job at educating employees on cybersecurity issues, how to recognize and what to do and to become more informed on various ways that data breaches occur and proactive ways that could eliminate or reduce exposure."

Industry trends

The healthcare industry continues to see the highest percentage of in-house counsel reporting they have experienced a data breach. Over half in the healthcare and social assistance industry say they have experienced a breach at their current or former employer compared with 31 percent of corporate counsel on average across all industries. In-house lawyers in the healthcare industry (75 percent) are most likely to report that their company has cybersecurity insurance. In-house counsel in the healthcare industry are also most likely to say their vendors and third-party agents are required to notify them of a breach (88 percent). Corporate lawyers in the retail industry have the highest percentage reporting that they proactively collaborate with law enforcement or other government agencies to address cybersecurity risks (45 percent).

Waiting to change until after the breach can be costly

We are clearly observing a dramatic increase in budget allocation toward cybersecurity issues across companies and legal departments. A major reason may be due to the lack of prevention strategies implemented. Among those who have experienced a data breach, 74 percent say that their company is making at least some changes to their security policies as a result of the breach, and 58 percent report making moderate to significant changes.

Benchmarking the state of cybersecurity

Key variables in prevention, preparedness, and response cross organizational boundaries and functional areas. However, several items related to the legal department, both directly and indirectly, are excellent benchmarks for evaluating preparedness. The checklist in this section provides a summary of these items. Inside the report, benchmarks from more than 800 organizations can be found along with this checklist for comparison purposes. These items are commonly recommended as foundational best practices for the prevention or preparation of a data breach. While few have all of the items listed, it is useful to examine your practices in comparison and take steps to plan for data security.

Sample cybersecurity checklist with benchmarks.
See full report for complete benchmarking checklist.

2%	Organization retained outside counsel to assist
7%	Company collaborates proactively with law enfor
1%	Organization retains a forensic company to assi
	Organizational Policies
0%	Password policy
3%	Social media policy
%	Document retention policy

Cybersecurity Checklist
Self-Assessment Tool

Organizational Prevention and Preparedness	✓
Organization conducts a cybersecurity audit of the entire organization at least annually	
A member of the legal department is on the company's data breach response team	
Organization has cybersecurity insurance	
Organization has mandatory training on cybersecurity for all employees	
Organization tests employee preparedness/knowledge of cybersafety practices/data polices at least annually	
Organization retained outside counsel to assist you should a breach occur	
Company collaborates proactively with law enforcement or other governmental agencies to address cybersecurity risks	
Organization retains a forensic company to assist should a breach occur	
Organizational Policies	✓
Password policy	
Social media policy	
Document retention policy	
Website privacy policy	
Employee manual acceptance policy	
Internet privacy policy	
Identity and access management	
BYOD policy	
Data map	
Organizational Staffing	✓
Chief Infromation Officer (CIO)	
Privacy/Security Manager	
Chief Information Security Officer (CISO)	
Chief Risk Officer (CRO)	
Chief Privacy Officer (CPO)	
Chief Security Officer (CSO)	
Organizational Preparedness Evaluation	✓
Conduct cybersecurity audit of entire organization at least annually	
Use a standard (e.g., SSAE, NIST, ISO) to prepare for, manage, and reduce cybersecurity risk	
Track mandatory training requirement and attendance for all employees	
Test employees' knowledge of mandatory training	
Conduct mock security event	
Conduct tabletop exercises	
Review disciplinary actions for violations	

PROJECT OVERVIEW & INTERPRETING THE DATA

Project Overview

This survey opened on August 31, 2015, and closed October 10, 2015. An email invitation to participate in the survey was delivered to 15,176 chief legal officers, general counsel, and assistant general counsel. Those holding the title of group general counsel and head of legal are included in the GC/CLO sample. The population includes members of ACC and nonmembers. A total of 1,015 responses were received; 760 were from ACC members, and 255 were from nonmembers. This represents an overall response rate of 7 percent. Seventy-seven percent identified as GC/CLO, and 14 percent are assistant general counsel. The remainder hold other titles not included in the GC/CLO group. Those not in the GC/CLO or AGC role may have been invited to complete the survey by their GC, CLO, or AGC on behalf of their organization. Participants represent 887 unique organizations as determined by their email address and/or pre-identified employer.

Interpreting the Data

The full report contains an introduction, key findings, executive report, and overall results. Although many pertinent topics are covered in the key findings, other thought-provoking findings are exhibited in the overall survey results. Overall results touch upon all survey questions, and responses from all respondents are stratified by a number of relevant segments such as region/country; industry; company revenue; number of employees in the company; department size; GC/CLOs and those with other titles; ever worked where a cybersecurity breach has occurred; and company domestic only or global. By analyzing responses in this way, we are able to decrease the influence of overrepresentation across audience segments. Cross-tabulations were conducted in order to assess the influence of these segments of the survey population, and t-tests were used when appropriate to determine whether differences between groups or between time points were statistically significant at the .05 α level.

ACC FOUNDATION: STATE OF CYBERSECURITY REPORT
IN-HOUSE COUNSEL PERSPECTIVES

Published by the ACC Foundation.

The ACC Foundation – a 501(c)(3) nonprofit organization – supports the efforts of the Association of Corporate Counsel, serving the needs of the in-house bar through the dissemination of research and surveys, leadership and professional development opportunities, and support of diversity and pro-bono initiatives. The ACC Foundation partners with corporations, law firms, legal service providers, and bar associations to assist in the furtherance of these goals.

1025 CONNECTICUT AVENUE, NW
SUITE 200, WASHINGTON, DC 20036 USA
TEL +1 202.293.4103

WWW.ACC-FOUNDATION.COM