ACC FOUNDATION:

THE STATE OF CYBERSECURITY REPORT

AN IN-HOUSE PERSPECTIVE 2018

LEARN ABOUT the best practices, organizational roles, and experiences of over 600 in-house counsel in 33 countries

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

DISCOVER INSIGHT on cyberinsurance, vendor risk, GDPR, corporate practice, and more.

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*:

Mary Blatch, Director of Advocacy and Public Policy, Association of Corporate Counsel

Erika Brown Lee, Senior Vice President, Assistant General Counsel, Privacy and Data Protection, MasterCard

Carter Leuty, Vice President, Law, Target

Robin Nunn, Partner, Davis Wright Tremaine LLP

Philip N. Yannella, Partner, Co-Chair, Privacy & Data Security, Ballard Spahr LLP

Because Timing is Everything

Cybersecurity incidents can happen in a flash.
And when they do, every second counts.

Ballard Spahr's Privacy and Data Security Group
helps clients prepare and respond.
We are advisers, investigators, and advocates
with deep experience in cyber risk management,
legal compliance, incident response,
investigations, and litigation.

Visit our blog at www.cyberadviserblog.com.

Ballard Spahr LLP

Atlanta | Baltimore | Boulder | Delaware | Denver | Las Vegas | Los Angeles | Minneapolis | New Jersey | New York | Philadelphia | Phoenix
Salt Lake City | Sioux Falls | Washington, DC | www.ballardspahr.com

TABLE OF CONTENTS

The ACC Foundation: State of Cybersecurity Report (2018) is a study of more than 600 in-house counsel published by the Association of Corporate Counsel (ACC) Foundation. The ACC Foundation — a 501(c)(3) nonprofit organization — supports the efforts of the ACC, serving the needs of the more than 43,000 corporate lawyers employed by over 10,000 organizations in 85 countries. This report provides insight from corporate lawyers in 33 countries and represents a follow-up to our 2015 survey. The report aims to serve as a resource for corporations, lawyers, boards of directors, and members of the public affected by one of the greatest challenges organizations face today — cybersecurity.

Data breaches have become ubiquitous. Cybercrime is widespread, aggressive, growing, and increasingly sophisticated, and it poses major implications for national and economic security. Regardless of industry type, locality, company size, and type, security incidents can happen anywhere, anytime, to anyone. According to the Identify Theft Resource Center (ITRC), there were more data breaches in 2017 than any year prior, representing a 45 percent increase over 2016.[1] The ITRC reported 1,293 total data breaches, compromising more than 174 million records. Cybercriminals may seek monetary or other benefits, manipulation of information or networks, data destruction, or other results.

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."[2] In a just released study, 2017 Cost of Data Breach Study: Global Analysis prepared by the Ponemon Institute, the average total cost of a data breach was $3.62 million, slightly lower than $3.8 million in the 2015 study.[3] The average cost for each lost or stolen record containing sensitive and confidential information also significantly decreased from $158 in 2016 to $141 in this year's study. Despite the decline in the overall cost, companies in this year's study are having larger breaches. The average size of a data breach increased 1.8 percent. The report also noted that the faster a data breach can be identified and contained, the lower the costs.

One can label this increasing occurrence of data breaches "a new normal." While cyberthreats and data breaches may be inevitable and unescapable, companies need to be proactive in mitigating threats and actual cyberattacks. A 2016 Zurich North America and Advisen Ltd. survey of risk management officers suggests that

45%

According to the Identify Theft Resource Center, there were more data breaches in 2017 than any year prior, representing a 45 percent increase over 2016.

[1] *Retrieved from https://identityforce.com.*
[2] *Net Losses: Estimating the Global Cost of Cybercrime, June 2014. Center for Strategic and International Studies.*
[3] *2017 Cost of Data Breach Study: Global Analysis. IBM and Ponemon Institute. https://securityintelligence.com/cost-of-a-data-breach-2017/*

a growing number of companies view their general counsel as the "go-to" person for handling compliance issues related to data breaches.[4] And why not? Preventing, preparing, and responding 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 in with thwarting such attacks.

The survey comprising more than 400 US and non-US companies found that one in four CLOs/GCs experienced a breach in the past two years. When asked to identify the greatest concerns of a data breach, GC/CLOs mentioned damage to reputation/brand, loss of proprietary information, and economic damage.

According to a 2016 Ponemon Institute study, there are several measures organizations can develop to deter attacks, including creating a holistic approach to cybersecurity, implementing training and awareness programs for employees, building a strong security operations team, leveraging shared threat intelligence, and investing in next-generation technology.[5] In 2017, ACC issued its first guidelines on the basic data security measures that in-house counsel should expect from their law firms. More than 40 percent of respondents in this year's survey say that their companies will need to change their data security standards, breach notification procedures, and incident response plans.

At the same time, the European Union's General Data Protection Regulation (GDPR) has had a significant impact on companies (worldwide), with 39 percent of survey respondents indicating that their company is required to comply. Any company that stores or processes personal information about EU citizens within EU states must comply by the end of May 2018 even if it does not have a business presence within the EU. According to a 2017 PwC survey of companies with more than 500 employees, 68 percent of US-based companies expect to spend $1 million to $10 million to meet GDPR requirements. Another 9 percent expect to spend more than $10 million.[6] The penalty for non-compliance could be very costly: up to €20 million or 4 percent of global annual turnover, whichever is higher.

ACC Foundation: The State of Cybersecurity Report (2018) captures the thoughts of in-house counsel of all of these areas. It also reveals best practices for preparation, crisis management, and breach response. Designed specifically for legal departments, this report contains vital information on organizational practices, insurance, the regulatory climate (including GDPR), and more. Read on to find out what worked and what didn't, why breaches happen, how to prepare, and and how to position your company for the an effective response.

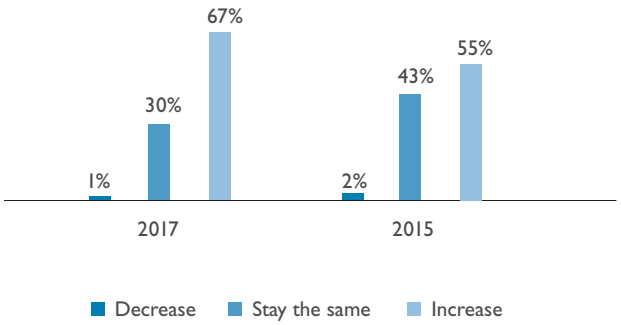
[4] *Retrieved from https://biglawbusiness.com/corporate-counsel-group-issues-law-firm-cyber-guidance.*
[5] *Retrieved from https://media.paloaltonetworks.com/lp/ponemon/report.html.*
[6] *Retrieved from https://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/pwc-gdpr-series-pulse-survey.pdf.*

KEY FINDINGS

Role of the Law Department Is Expanding

In-house counsel were asked whether their legal department's role in cybersecurity will decrease, stay the same, or increase in the next 12 months. Two-thirds of in-house counsel respondents expect that their department's role will increase, compared with 55 percent in the 2015 survey (see Figure 1).

FIGURE 1: EXPECTING ROLE IN CYBERSECURITY TO CHANGE, STAY THE SAME, OR DECREASE?



One in Three In-house Counsel Have Experienced a Data Breach

Thirty-two percent of survey respondents report that they have worked or currently work in a company that has experienced a data breach. Ten percent experienced a breach before 2015, compared with 2 percent in 2015 and 5 percent in 2016. In 2017, respondents reporting a breach reached 15 percent.

What do CLOs and GC wish they had known before it happened? Respondents identify the role of the vendor and the importance of providing employee training as things they wish they had known.

"Better prioritization of certain technology investments would have virtually eliminated the vulnerability exploited in the attack."

"We need better controls. All of our breaches were employee error (e.g., mislabeling mailings, sending sensitive documents via email to the wrong recipient)."

"Should have had more employee training with respect to external malware and phishing."

Proactive Collaboration With Law Enforcement Is Increasing

About one-third of respondents surveyed work for companies that proactively collaborate with law enforcement to address cybersecurity risks, while 43 percent do not and 22 percent say they do not know. The percentage of companies that proactively collaborate with law enforcement increased from 27 percent in the 2015 survey to 35 percent in the 2017 survey.

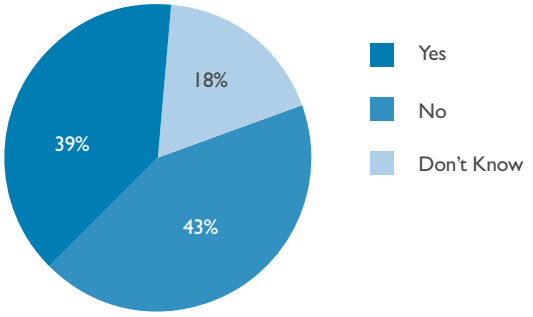
Even when not legally responsible, 30 percent of respondents indicate that their company policy is to notify those affected by a breach.

Companies Are Responding to GDPR Requirements

Survey respondents are split on the percentage of companies required to comply with GDPR. Thirty-nine percent say their company is required to comply, while 43 percent say their company is not (see Figure 2).

As a result of GDPR, more than 40 percent of respondents state that their company plans to change the following: data security standards (47 percent), breach notification procedures (45 percent), and incident response plans (43 percent).

FIGURE 2: COMPANY MUST COMPLY WITH GDPR



Training and Testing Knowledge Are Common Practices

Sixty-one percent of survey respondents report that their organization has mandatory training on cybersecurity for all employees. Almost half of respondents report that their company tracks mandatory requirements and attendance for all employees as a means to evaluate preparedness at the employee level (46 percent), followed by 36 percent who report that their company tests employee knowledge of training.

About 30 percent say their company holds a mock security event/simulated response exercises.

Company Preparedness Is Important

Twenty-nine percent of respondents retain a forensic company to assist if a breach occurs; over half report that their employers do not retain such a company.

Four in 10 respondents report that their organization conducts a companywide cybersecurity audit on an annual basis. Two in three report that their company has an incident response plan. Among companies that have data incident response teams, 90 percent are represented by either a CLO/GC or other legal staff member.

Cybersecurity Insurance Is up 10 Percentage Points Since 2015

Fifty-seven percent of respondents report that their company has cybersecurity insurance, representing a 10 percentage-point increase over 2015. Respondents who indicate that their organization does not have cyberinsurance cite cost and no/low risk of a cybersecurity breach as reasons. Average cybersecurity insurance coverage is about $12 million, with a median of $5 million.

Confidence in Level of Protection Provided at the Vendor and Law Firm Changed Little Since 2015

Only 6 percent of in-house counsel report high confidence in their vendors' protecting the company from cybersecurity risks, while a majority (56 percent) say they are somewhat confident. Twenty-one percent are not at all confident. These results are very similar to two years ago (7 percent highly confident, 60 percent somewhat confident, and 17 percent not at all confident).

Seventy-two percent of respondents are at least somewhat confident that their outside law firms are appropriately managing their data security. Nine percent are not at all confident.

Company Budgets for Cybersecurity Are Growing

Asked whether the company was allocating more, less, or the same amount of company budget to cybersecurity compared with one year ago, 63 percent say the company budget would be more. Respondents who report that their company is allocating more money represent an 8 percentage point increase over two years ago. On average, respondents say that about 5 percent of the law department budget is dedicated to cybersecurity issues, with a median of 1 percent.

Best Practices Center on Preparing for a Breach

While it may not be possible to eliminate all data breaches, survey respondents share many best practices and important lessons that may help mitigate cybersecurity risk and/or a breach. First, mandatory training is clearly an important component, including testing employee knowledge. Second, at the organization level, a cyber response team with personnel from different departments is critical, with an emphasis on obtaining buy-in from all levels of management. Third, cybersecurity insurance is an essential tool to cover any costs associated with a breach as well as access to experts who will be more knowledgeable about the latest regulations and able to provide tools to reduce possible exposure.

"Issues relating to cybersecurity risks are not limited just to the IT and legal departments but ultimately impact groups across the entire organization, so it is important to include everyone in assessing these risks and formulating policies and plans on dealing with them."

Cybersecurity Checklist Self-Assessment Tool	
General prevention and preparedness	✓
Conducts a cybersecurity audit of the entire organization at least annually	
IT and/or legal department audits legal service providers	
Has a data incident response team	
A member of the legal department is on the company's data breach response team	
Has a data incident response plan	
Incident response plan was updated in past 12 months	
Has cybersecurity insurance	
Has mandatory training on cybersecurity for all employees	
Collaborates proactively with law enforcement or other governmental agencies to address cybersecurity risks	
New vendor contracts contain termination right in case of security issues	
Has rights to audit subvendors	
Requires third parties to notify of cybersecurity risk issues	
Participates in OPSEC	
Retains a forensic company to assist should a breach occur	
Has data map	
Tracks mandatory training requirement and attendance for all employees	
Tests employees' knowledge of mandatory training	
Conducts mock security event	
Conducts tabletop exercises	
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	
Encryption policy	
Staffing	✓
Chief Information Officer (CIO)	
Privacy/Security Manager	
Chief Information Security Officer (CISO)	
Chief Risk Officer (CRO)	
Chief Privacy Officer (CPO)	
Chief Security Officer (CSO)	
Confidence	✓
You have high confidence third-party affiliates and vendors protect you from cybersecurity risks	

PROJECT OVERVIEW & RESPONDENT PROFILE

The sample frame for the *State of Cybersecurity Report* (2018) included 11,006 ACC members and 5,029 non-ACC members. ACC committees and chapters, an advertisement in Lexology, and social media were used to publicize the study. An e-mail invitation to participate in the survey was sent on Nov. 29, 2017. Six e-mail reminders were sent to the entire sample to encourage survey participation. The survey field period closed on Dec. 27, 2017.

A total of 617 responses were received, for an overall response rate of about 4 percent.[7] Participants represent 412 unique organizations as determined by their email addresses and/or pre-identified employers. Respondents to the survey were promised a complimentary electronic copy of the report, and the ACC Foundation donated US $2 to the American Red Cross for international disaster response for each completed survey.

The full report contains an introduction, key findings, executive summary, and overall results. Although the key findings cover many pertinent topics, other thought-provoking findings are exhibited in the overall survey results. Overall results touch on all survey questions, and responses from all respondents are stratified by a number of relevant segments, including

- regional category
- organization's total gross revenue for the past fiscal year (US $)
- total employees in organization/company
- size of law department (all staff in all locations)
- employer's primary industry — top seven categories

By analyzing responses in this way, we are able to decrease the influence of over-representation across audience segments. Cross-tabulations were conducted 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.

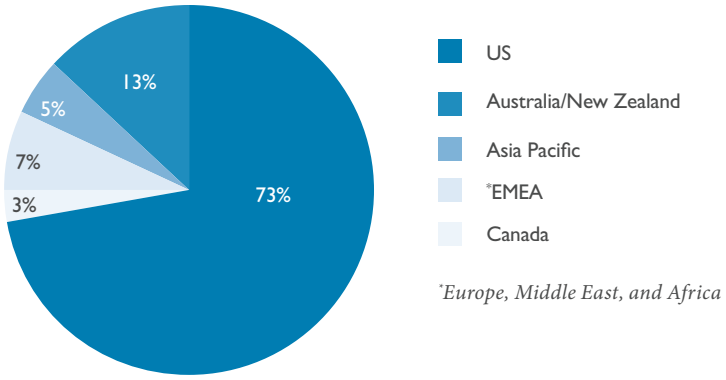
[7] *An additional 104 responses were received but removed from the analytic file because respondents either submitted a survey with no responses or answered only Question 1.*

Respondent Profile

Two thirds of respondents identified the US as the location of their office, followed by Australia/New Zealand (see Figure 3). Respondents were asked to provide the total gross revenue for the last fiscal year, including affiliates and subsidiaries. Thirty-eight percent indicated that revenues were less than $100 million, 22 percent between $100 million and $499 million. About one-quarter of companies had revenues between $500 million and 2.9 billion.

Respondents identified a wide range of their employer's primary industry. The top seven industries constituted about half of all the industries identified. Table 1 provides the complete list of industries and number of respondents selecting each one.

FIGURE 3: DISTRIBUTION OF REGION



Europe, Middle East, and Africa

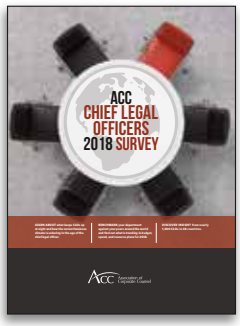
TABLE 1: WHAT IS YOUR EMPLOYER'S PRIMARY INDUSTRY?

	n=
Information Technology/Software/Internet-related Services	79
Finance/Banking	59
Manufacturing	49
Insurance	48
Not-for-profit Organization (i.e. , Charity, Environment)	26
Healthcare/Social Assistance	25
Professional, Scientific, and/or Technical Services	23
Retail Trade	20
Educational Services	19
Energy	18
Real Estate/Rental and Leasing	17
Pharmaceutical/Medical Devices	11
Defense	11
Construction Engineering	11
Biotechnology/Life Sciences	11
Wholesale Trade/Distribution	10
eCommerce/Online Sales	10
Transportation Warehousing	9
Telecommunications	9
Service Company and Organization	9

	n=
Chemicals Plastics	9
Technical/Research Development	7
Aviation/Aerospace	7
Arts, Sports, Entertainment/Recreation	7
Advertising/Marketing/Public Relations	7
Trade Association	6
Oil /Gas	6
Utilities	5
Agriculture/Forestry/Fishing/Hunting	5
Administrative/Business/Support Services	5
Accommodation/Food Services	4
Mining Quarrying	3
Management of Companies Enterprises (i.e., Holding Companies)	3
Broadcasting Media	3
Public Administration/Government Regulation and Support	2
Prepared Food Stuff Beverages	2
Fast Moving Consumer Goods/Consumer Services	2
Waste Management, Remediation Environmental Services	1
Intellectual Property	1
Other	50

YOUR MOST TRUSTED SOURCE FOR RESEARCH

As the world's largest association for in-house counsel, ACC offers the research and benchmarking in-house counsel and their partners need to stay on top of important trends in the legal profession.



Chief Legal Officers 2018 Survey

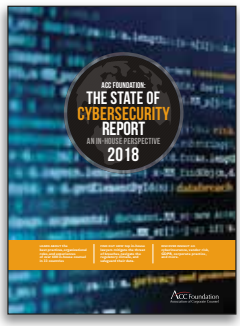
This global survey of nearly 1,300 CLOs and GC gauges the importance of issues, attitudes, and opinions on legal and business topics, including those commonly used for benchmarking. If you are looking for data to make your case on resource allocation, staffing or budget changes, this is the report you need.

Members: $495 | Non-Members: $895

Global Perspectives: ACC In-house Trends Report

An omnibus survey covering many important topics, this report highlights trends affecting global corporate legal practitioners. Over 2,000 in-house lawyers across 51 countries participated in the survey. Thirty-one percent of respondents are from countries outside the US and 19 percent work in departments with 50 or more lawyers. Get up-to-date on the state of the in-house profession with data on career mobility, in-house privilege dynamics, cross-border work, the regulatory environment, and more! The full report also feature industry and regional profiles.

Members: $150 | Non-Members: $450



ACC Foundation: State of Cybersecurity 2018 Report

Underwritten by Ballard Spahr, LLP this comprehensive report outlines what more than 600 in-house counsel say about their cybersecurity experiences, role, and practices. The full report includes common preventative tactics, lessons learned from those who experienced a breach (including how the breach occurred and who was affected), the impact of regulatory requirements, insurance decision making and coverage information, and managing risk through outside support.

Members: $595 | Non-Members: $695

ACC Global Compensation 2018 Survey

Coming: Summer, 2018

This global compensation survey reports on base salaries, performance-based bonuses, total compensation, equity-based pay, and retirement/pension plans. The report further segments by 13 in-house job titles, company tenure, legal practice area, department size, geographic location and more!

Need custom benchmarking reports?

The ACC research team can provide you with the custom benchmarks you need on legal department spend, budget, resource allocation, and staffing numbers, to name just a few. Reports can be customized to your organization, industry, and more.

For more information, contact us at:
+1 202.293.4103 • research@acc.com

» **www.acc.com/surveys**

ACC Association of Corporate Counsel

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

WWW.ACC-FOUNDATION.COM