2020 STATE OF CYBERSECURITY REPORT

AN IN-HOUSE PERSPECTIVE

KEY FINDINGS

ACC Foundation
Association of Corporate Counsel

586 DEPARTMENTS

20 INDUSTRIES

36 COUNTRIES

SECTION 1

THE LEGAL DEPARTMENT'S ROLE IN CYBERSECURITY

CLOs LEAD EFFORTS ON CYBERSECURITY

Seventy-one percent of organizations place their CLO in either a leadership role regarding cybersecurity strategy or as part of a team with cyber responsibilities. However, only 17 percent of organizations have their CLO directly oversee both cyber and privacy functions.

LEGAL OVERSIGHT RESULTS IN RISK-BASED COMPLIANCE

The percentage of organizations with a risk-based cybersecurity program versus a compliance-based program increases when the CLO has both the cyber and privacy function oversight. In other words, the oversight of legal appears to be driving a more proactive approach to cybersecurity.

MORE IN-HOUSE COUNSEL DEDICATED TO CYBERSECURITY

Eighteen percent of organizations have an in-house lawyer dedicated to cybersecurity, which is up from 12 percent in 2018. In a majority of cases, this lawyer is responsible for cyber across the enterprise and is in an executive level position in 56 percent of organizations.

SECTION 2

POLICIES AND PRACTICES

RISE IN EMPLOYEE TRAINING AND EVALUATION

Evaluation methods for company preparedness among employees have increased dramatically since 2018 along with the frequency of evaluations. Tracking mandatory training requirements and attendance is now in place for a majority of organizations and well over a third now conduct mock security events and tabletop exercises.

CYBERSECURITY POLICIES ARE THE NORM

For most of the cybersecurity policies listed, there has not been a significant change in those used over time. Most organizations have implemented password, social media, internet usage, and document retention policies but there has been a sharp increase over the past two years in the percentage of organizations employing data mapping, almost doubling over the course of five years.

LAWYERS ARE INCLUDED IN CYBERSECURITY RESPONSE TEAMS

Seventy-six percent of organizations have a cybersecurity response team, up from 59 percent in 2018. A vast majority (83 percent) of those organizations have a senior staff lawyer or executive member of the legal department on that team.

SECTION 3

RISK MANAGEMENT

VENDORS ARE TRUSTED REGARDING CYBER RISKS

Seventy-eight percent of organizations claim they are "somewhat" or "very" confident in their third-party vendors' ability to protect them from cyber risks. This is a substantial increase in confidence from 2018 (62.1 percent).

ONLY A MINORITY USES VENDOR MANAGEMENT PLATFORMS

Fifteen percent of organizations are now using vendor management platforms, which is up from 9.1 percent in 2018. Usage increases substantially among larger legal departments. Nearly one quarter of departments with greater than 25 staff are employing vendor management platforms and those with a dedicated cybersecurity counsel are more likely to utilize a platform regardless of the size of legal.

ONE THIRD OF DEPARTMENTS WILL INCREASE LEGAL SPEND

Thirty-six percent of departments say they will increase their legal spend as a result of their cybersecurity approach, which is up from 33.8 percent in 2018 and far up from 22.8 percent in 2015. A plurality of departments will allocate this increase in spend on outside costs (38.8 percent) but there is a clear and sizable shift toward allocating the increase to inside spend over time.

SECTION 4

BREACH AND INCIDENT EXPERIENCE

FOUR IN TEN COMPANIES SUFFERED A DATA BREACH

Forty percent of organizations surveyed experienced at least one data breach over the past year and have also experienced an average of 24 cyber incidents. Organizations in the healthcare industry experienced the highest number of incidents over the past year with an average of 58.

EFFECTS ON REPUTATION AND COMPANY BRAND ARE THE MAIN CONCERN

Damage to company reputation and brand still remains the top concern arising from a data breach for organizations. However, liability to data subjects has become the second greatest concern overall this year with a dramatic increase from 2018. Sixty-two percent of organizations rated it among their top three concerns this year compared to just 20.3 percent in 2018.

ONE IN FIVE CLOs ARE IN CHARGE OF RESPONDING TO A DATA BREACH

Typically, organizations assign an individual or group to coordinate a formal response to any data breach that occurs. This year, 21.2 percent of organizations assigned their CLO with that responsibility, which has been steadily increasing over time with only 4.6 percent in 2015.

SECTION 5

WORKING WITH GOVERNMENT/ LAW ENFORCEMENT

ALMOST HALF WORK WITH GOVERNMENT TO ADDRESS RISKS

Forty-seven percent of organizations surveyed collaborate with law enforcement or government agencies to address cybersecurity risks. This is a large increase from 2015 with only 27.1 percent. Organizations are also more likely to collaborate when the CLO oversees cybersecurity. Those who do not collaborate say that they do not have the resources or knowledge base to do so.

ONLY ONE IN SIX PARTICIPATE IN INFORMATION SHARING

Sixteen percent of organizations participate in an information sharing and analysis center to share cyber threat information with other organizations and the government. In 71 percent of cases the legal department plays a role in that information sharing process.

GDPR: MAJORITY APPOINTED A DATA PRIVACY OFFICER

Among organizations required to comply with GDPR, 58 percent were required to appoint a Data Privacy Officer (DPO) and among those not required to do so 31 percent appointed a DPO anyway. In over half of those organizations the DPO is a full-time employee reporting to legal.

ACC Foundation
Association of Corporate Counsel

HEADQUARTERS OFFICE
1001 G St., NW, Suite 300W | Washington, DC 20001 USA
Tel +1 202.293.4103 | acc-foundation.com

FOR MORE INFORMATION
research@acc.com

FULL REPORT
acc.com/cyber2020