BENEFITS, ATTRIBUTES AND HABITS

of Mature Privacy and Data Protection Programs

By IAPP Research Manager Margaret Honda and IAPP Market Research Specialist Christelle Kamaliza, CIPP/E, CIPM
CONTENTS

Executive Summary ................................................................. 03

Research objectives, methodology and demographics .............................................. 05

Why data needs to be protected and an overview of privacy program maturity levels
  Why data needs to be protected ...................................................... 11
  Privacy program maturity levels ..................................................... 15

Organizational benefits of mature privacy and data protection programs ................. 21

Attributes and habits of mature privacy and data protection programs
  Team structure ................................................................. 26
  Budget ownership and organizational support ..................................... 30
  Privacy program elements ......................................................... 35
  User data-monitoring practices ................................................... 38
  Privacy and/or security framework application ...................................... 41

Common practices and benefits of privacy programs across all maturity levels ........ 44

Conclusion .................................................. 49

Contact .................................................. 51
EXECUTIVE SUMMARY
Despite new privacy regulations and increasing data breaches, this study of more than 550 privacy programs found that privacy and data protection programs are still maturing.

It also concluded the value of a mature privacy program is clear. Perhaps more importantly, it identified key attributes and habits of mature programs that could be used to help advance your own program.

Organizations with more mature privacy programs see greater gains in almost all areas surveyed. The areas where mature privacy programs saw greater benefits were:

- Reduced privacy complaints.
- Increased operational efficiencies.
- Mitigated data breaches.
- Increased consumer trust.

Fundamentally, dedicating resources to a privacy program yields greater awareness of privacy-related issues internally, leading to better outcomes externally.

Organizations looking to mature their privacy and data protections programs should consider:

- Forming a distinct privacy team with C-level leadership and budget.
- Conducting regular privacy risk assessments.
- Mapping where personally identifiable information/personal health information is located and where it flows.
- Providing regular data protection and privacy training for your workforce.
- Automating user activity monitoring for applications that contain sensitive data.
- Following privacy and cybersecurity frameworks.
RESEARCH OBJECTIVES, METHODOLOGY AND DEMOGRAPHICS
The IAPP, in partnership with FairWarning, set out to identify characteristics and behaviors of privacy and data protection teams.

To drive this survey, we asked more than 550 professionals — in-house privacy and data protection professionals, in-house IT professionals, in-house compliance professionals — from around the world a series of questions about how privacy functions are supported through the lenses of people, process and technology.
Two-thirds of the survey respondents are in North America and work for organizations headquartered mainly in the U.S. or the EU (↓). Professionals in the software and healthcare industries are the two largest sectors represented, and almost 70% of the feedback came from chief compliance officers or privacy directors. Respondents were distributed across a range of small, medium and large organizations.

The survey gathered input on metrics, such as team structure, program priorities, use of software monitoring tools, and data breach and privacy incident reporting. Additionally, we asked respondents to provide insight into things like the level of maturity of their privacy/data protection programs and their confidence level in complying with various regulations, such as the EU General Data Protection Regulation.

<table>
<thead>
<tr>
<th>Organizations’ headquarters</th>
<th>Count</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>United States</td>
<td>297</td>
<td>53%</td>
</tr>
<tr>
<td>European Union</td>
<td>147</td>
<td>26%</td>
</tr>
<tr>
<td>Canada</td>
<td>50</td>
<td>9%</td>
</tr>
<tr>
<td>Non-EU Europe</td>
<td>27</td>
<td>5%</td>
</tr>
<tr>
<td>Asia</td>
<td>15</td>
<td>3%</td>
</tr>
<tr>
<td>Latin America (including Mexico)</td>
<td>10</td>
<td>2%</td>
</tr>
<tr>
<td>Australia or New Zealand</td>
<td>7</td>
<td>1%</td>
</tr>
<tr>
<td>Middle East</td>
<td>5</td>
<td>1%</td>
</tr>
<tr>
<td>Africa</td>
<td>1</td>
<td>0%</td>
</tr>
<tr>
<td>Indian subcontinent</td>
<td>1</td>
<td>0%</td>
</tr>
</tbody>
</table>
Breakdown of geographic location by respondent location.

- United States, 51%
- Canada, 9%
- European Union, 21%
- Asia/Pacific, 4%
- Middle East/Africa, 1%
- Non-EU Europe, 12%
- Latin America, 2%

RESEARCH OBJECTIVES, METHODOLOGY AND DEMOGRAPHICS
### Respondent’s industry and role within the organization.

#### By industry
- **Software and services**: 12%
- **Health care**: 11%
- **Banking**: 7%
- **Government**: 7%
- **Consulting services**: 6%
- **Education or academia**: 6%
- **Insurance**: 6%
- **Other**: 46%

#### By role within organization
- **Chief compliance officer**: 39%
- **Privacy director**: 29%
- **Chief information security officer**: 8%
- **Chief privacy officer**: 7%
- **Compliance director**: 7%
- **Information security director**: 5%
- **Risk director**: 4%
- **IT director**: 2%
- **Chief information officer**: 2%
- **Other**: 24%
Respondents were distributed across a range of small, medium and large organizations, though a higher proportion of health care respondents work for organizations with 5,000 employees or more.

By industry

<table>
<thead>
<tr>
<th>Size of organization</th>
<th>Software and services</th>
<th>Health care</th>
<th>Banking</th>
<th>Government</th>
<th>Consulting services</th>
<th>Education or academia</th>
<th>Insurance</th>
<th>Other</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>1–250</td>
<td>26%</td>
<td>10%</td>
<td>8%</td>
<td>5%</td>
<td>58%</td>
<td>15%</td>
<td>9%</td>
<td>13%</td>
<td>89</td>
</tr>
<tr>
<td>251–1,000</td>
<td>24%</td>
<td>11%</td>
<td>19%</td>
<td>19%</td>
<td>6%</td>
<td>18%</td>
<td>28%</td>
<td>16%</td>
<td>95</td>
</tr>
<tr>
<td>1,001–5,000</td>
<td>21%</td>
<td>19%</td>
<td>30%</td>
<td>24%</td>
<td>9%</td>
<td>39%</td>
<td>16%</td>
<td>22%</td>
<td>123</td>
</tr>
<tr>
<td>5,001–25,000</td>
<td>13%</td>
<td><strong>42%</strong></td>
<td>19%</td>
<td>22%</td>
<td>12%</td>
<td>15%</td>
<td>22%</td>
<td>24%</td>
<td>127</td>
</tr>
<tr>
<td>25,001 or more</td>
<td>16%</td>
<td>18%</td>
<td>24%</td>
<td>30%</td>
<td>15%</td>
<td>12%</td>
<td>25%</td>
<td>26%</td>
<td>126</td>
</tr>
<tr>
<td>Total</td>
<td>68</td>
<td>62</td>
<td>37</td>
<td>37</td>
<td>33</td>
<td>33</td>
<td>32</td>
<td>258</td>
<td>560</td>
</tr>
</tbody>
</table>

Statistically significant difference from the overall total.
WHY DATA NEEDS TO BE PROTECTED AND AN OVERVIEW OF PRIVACY PROGRAM MATURITY LEVELS

Why data needs to be protected
With the advent of regulations, such as the GDPR, California Consumer Privacy Act and Brazil’s General Data Protection Law (Lei Geral de Proteção de Dados Pessoais) and the increasing digitization of our lives and economies, privacy is moving beyond legal departments and to the forefront of many organization’s strategic priorities.

The importance of privacy and data protection is becoming more mainstream as organizations, regardless of size, understand customer data is core to their business and must be protected.
This survey revealed that in the last three years, 50% of all respondents reported at least one data breach (↓), and two-thirds of responding organizations documented a privacy incident. While one breach sounds low, according to the latest IBM Security-Pomemon Institute “Cost of a Breach Report, 2020,” the global average cost of a data breach is $3.86 million.

Recognising the quantity of data which could be lost with a single error or compromised account. Business has to be vigilant 24/7x365.25, a breach needs only to occur once!

— Survey respondent

**Data breach(es) reported in past three years**

- Zero breaches: 33%
- One or more breaches: 50%
- Unsure: 17%

**ONE OR MORE BREACHES**

- 1–9: 34%
- 10–19: 4%
- 20–29: 2%
- 30 or more: 10%
Two-thirds of organizations have documented a privacy incident in the past three years.

Documented privacy incidents in the past three years

- Zero incidents: 15%
- One or more incidents: 67%
- Unsure: 18%

One or more incidents

- 1–9: 28%
- 10–19: 10%
- 20–29: 5%
- 30 or more: 24%
WHY DATA NEEDS TO BE PROTECTED AND AN OVERVIEW OF PRIVACY PROGRAM MATURITY LEVELS

Privacy program maturity levels
For this survey, we asked respondents to rate their privacy program’s maturity level on the following five-point scale:

- Ad hoc (privacy procedures/processes are informal, incomplete or inconsistently used).
- Repeatable (privacy procedures/processes exist but are not fully documented/are incomplete).
- Defined (privacy procedures/processes are fully documented and implemented and are complete).
- Managed (reviews to assess the effectiveness of your privacy controls are conducted).
- Optimized (privacy procedures and processes to ensure continual improvement are regularly reviewed).
Based on these categorizations and for the purposes of this report, we consider those who responded with either “optimized” or “managed” to be in the advanced stages of privacy program development and thus to have more mature programs. Those who replied with “ad hoc” or “repeatable” are considered in the early stages of privacy program development and, as a result, have programs that are still maturing.

Most responding organizations view their privacy programs as still maturing — 44% responded they are in the early stages of their privacy program development, while 28% are in middle or advanced stages, respectively. Healthcare and the software and services industries, and those with 25,000 employees or more, rose to the top of the list as having mature privacy programs.

### Privacy program stages of development

- **Ad hoc**: (privacy procedures/processes are informal, incomplete or inconsistently used). 8%
- **Repeatable**: (privacy procedures/processes exist but are not fully documented/are incomplete). 36%
- **Defined**: (privacy procedures/processes are fully documented and implemented and are complete). 28%
- **Managed**: (you conduct reviews to assess the effectiveness of your privacy controls). 21%
- **Optimized**: (you regularly review privacy procedures and processes to ensure continual improvement). 7%

#### Privacy program maturity levels

- Early stages – 44%
- Middle stages – 28%
- Advanced stages – 28%
Respondents’ 2020–21 priorities for their privacy and data protection programs are consistent across maturity levels (↓). Compliance with privacy and data protection laws are the clear top priority for organizations, followed by protecting consumer/patient trust and ensuring privacy protocols apply to contractors, business associates and third parties to which data is transferred.

Analyzing the data through the maturity lens brought into focus key attributes and habits of organizations with mature privacy and data protection practices. The following sections tell the story of these organizations compared with those whose programs are still maturing. We explore topics like industry, geographical location and size of organization. The number of dedicated employees and budget ownership, the types of activities included in their programs and how user activity is monitored in applications that process personal data. We also look at confidence levels in complying with regulations and which privacy and security frameworks they follow. Finally, we report on the benefits these organizations are experiencing as a result of their existing privacy and data protection program.

2020–21 privacy program priorities
Health care and software and services industries reflect more maturity in their privacy programs.

Privacy program maturity level by industry
Organizations with 25,001 or more employees have more mature privacy programs.
ORGANIZATIONAL BENEFITS OF MATURE PRIVACY AND DATA PROTECTION PROGRAMS
This survey uncovered certain attributes and habits that contribute to an organization's confidence in their ability to respond to privacy challenges.

To better understand the key benefits, attributes and habits of organizations with mature privacy and data protection programs, we compared answers from the 28% of respondents in the advanced stages category with the 44% of respondents in the early stages of development.
When asked what benefits their organization is experiencing from their privacy program today, increased employee privacy awareness, breach mitigation and complaint reduction received top marks. In comparing replies of those whose programs are in the advanced stages with those in the early stages, more mature programs believe they experience greater gains in every category, with the largest in reducing privacy complaints (30.3% higher than early stage respondents), operational efficiencies (23.7% higher), mitigating data breaches (23.5% higher), and consumer trust (22.3% higher).

Those in the advanced stages of program development have greater confidence in their ability to comply with privacy and data protection regulations.

Mature privacy and data protection programs show greater confidence in complying with the GDPR, CCPA and U.S. Health Insurance Portability and Accountability Act. Compliance with the GDPR uncovered the biggest gap between those in the advanced stages of program development and those in the early stages — a 52% difference in confidence levels.
More mature programs experience greater benefits in every category.

Benefits realized by program maturity level

- Increased employee privacy awareness: Early stages 75.2%, Middle stages 82.8%, Advanced stages 87.6%
- Greater consumer trust: Early stages 35.5%, Middle stages 45.9%, Advanced stages 57.8%
- Reduced privacy complaints: Early stages 43%, Middle stages 52.9%, Advanced stages 73.3%
- Quality and innovation: Early stages 17.4%, Middle stages 25.5%, Advanced stages 26.7%
- Competitive advantage: Early stages 18.6%, Middle stages 22.3%, Advanced stages 34.8%
- Operational efficiency: Early stages 26%, Middle stages 37.6%, Advanced stages 49.7%
- Mitigating data breaches: Early stages 62.8%, Middle stages 76.4%, Advanced stages 86.3%

Education and training has helped to reduce the common errors that result in data breaches (e.g. sending emails to incorrect recipients).

— Survey respondent
Privacy program maturity significantly impacts respondents’ confidence in regulation compliance.

Confidence with GDPR/HIPAA/CCPA compliance by program maturity level

GDPR

- Early stages: 13% Not at all confident, 16% Moderately confident, 71% Very confident
- Middle stages: 3% Not at all confident, 42% Moderately confident, 54% Very confident
- Advanced stages: 2% Not at all confident, 31% Moderately confident, 68% Very confident

HIPAA

- Early stages: 15% Not at all confident, 6% Moderately confident, 52% Very confident
- Middle stages: 33% Not at all confident, 45% Moderately confident, 33% Very confident
- Advanced stages: 3% Not at all confident, 33% Moderately confident, 64% Very confident

CCPA

- Early stages: 17% Not at all confident, 22% Moderately confident, 62% Very confident
- Middle stages: 5% Not at all confident, 40% Moderately confident, 55% Very confident
- Advanced stages: 6% Not at all confident, 41% Moderately confident, 53% Very confident

◇ Statistically significant differences

“CCPA compliance initiative led to a greater understanding of internal data processing and transfers to outside parties, leading to a greater management of such activities not closely related to CCPA compliance.”
— Survey respondent
ATTRIBUTES AND HABITS OF MATURE PRIVACY AND DATA PROTECTION PROGRAMS

Team structure
In comparing responses from those in the advanced stages with those in the early stages, we discovered the organizations with more mature programs do things like manage programs through distinct privacy teams, have greater C-suite representation, manage a discrete budget and actively monitor user data through automated tools.

When asked to indicate how their privacy and data protection programs are supported internally — how many full-time employees make up privacy and data protection teams? — 61% of those with mature privacy programs (advanced stages) reported having a distinct privacy team compared with only 43% of those in the early stages. On average, mature privacy programs have three employees dedicated to privacy, compared with the middle and early stages with two and one dedicated employees respectively. Those who do not have a distinct privacy team indicated their programs are either handled by a team in the organization that has another primary responsibility (e.g., security, legal), handled by a team made up of people from across departments in the organization or outsourced to a third party.
Over 60% of respondents with mature privacy programs (advanced stages) reported having a distinct privacy team.

Organizational structure of privacy teams by maturity level

- **Advanced stages**: 61.5% have distinct team, 38.5% do not have distinct team
- **Middle stages**: 53.5% have distinct team, 46.5% do not have distinct team
- **Early stages**: 43.8% have distinct team, 56.2% do not have distinct team

Legend:
- **Blue**: Have distinct team
- **Red**: Do not have distinct team
Mature privacy programs have slightly more employees dedicated to privacy programs.

Average number of employees dedicated to privacy

- Early stages: 1
- Middle stages: 2
- Advanced stages: 3

Team structure
ATTRIBUTES AND HABITS OF MATURE PRIVACY AND DATA PROTECTION PROGRAMS

Budget ownership and organizational support
Companies with more mature privacy programs are more likely to have C-suite privacy and security roles within their organization than those in the middle to early stages of privacy program development.

This may also explain why these organizations typically fund their privacy activities through a discrete budget instead of through budgets that sit somewhere else within the company, like security, compliance or IT, and tend to report privacy performance indicators to the board level at higher rates.
The chief privacy officer and chief compliance officer role exist more frequently in companies with mature privacy programs.

Roles that exist within organization by maturity level
More mature programs have a discrete privacy budget, followed closely by funding from compliance.

Privacy program funding by maturity level

- Through a discrete budget: 26% (Early stages), 36.9% (Middle stages), 41% (Advanced stages)
- Through a compliance program: 30.6% (Early stages), 35% (Middle stages), 34.2% (Advanced stages)
- Through an IT program budget: 18.6% (Early stages), 15.3% (Middle stages), 21.1% (Advanced stages)
- Through a security program: 17.8% (Early stages), 25.5% (Middle stages), 21.1% (Advanced stages)
- Through another method/budget: 20.7% (Early stages), 22.3% (Middle stages), 20.5% (Advanced stages)
- We don't fund any privacy program activities: 8.7% (Early stages), 3.8% (Middle stages), 2.5% (Advanced stages)
While most report privacy program metrics to their board, organizations in the early stages are less likely to do so.

Board level reporting of privacy program performance indicators

<table>
<thead>
<tr>
<th>Early stages</th>
<th>Middle stages</th>
<th>Advanced stages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>81.5%</td>
<td>82%</td>
</tr>
<tr>
<td>No</td>
<td>58.7%</td>
<td>36.4%</td>
</tr>
</tbody>
</table>

- Early stages: 58.7%
- Middle stages: 81.5%
- Advanced stages: 82%

- Early stages: 12.7%
- Middle stages: 36.4%
- Advanced stages: 10.6%
ATTRIBUTES AND HABITS OF MATURE PRIVACY AND DATA PROTECTION PROGRAMS

Privacy program elements
When asked what functions their privacy and data protection programs include, those in the advanced stages edged out both the middle and early stage respondents in almost every category.

In comparing the more mature programs with those still developing, the greatest gap occurred in the following categories: conducting regular privacy risk assessment (93% advanced stages vs. 57% early stages), knowing where most/all our personally identifiable information/personal health information is located and where it flows within and outside our environment (88.2% advanced stages vs. 60.7% early stages), and providing regular data protection and privacy training to our workforce (90.7% advanced stages vs. 69.4% early stages).
Advanced maturity organizations edged early maturity respondents in almost every program function.

Privacy program functions by maturity level:

- **Have an incident response plan:**
  - Early stages: 79.3%
  - Middle stages: 95.2%
  - Advanced stages: 96.2%

- **Have data protection policies and procedures that are reviewed/updated regularly:**
  - Early stages: 74.8%
  - Middle stages: 93.0%
  - Advanced stages: 96.9%

- **Provide regular data protection and privacy training to our workforce:**
  - Early stages: 69.4%
  - Middle stages: 87.9%
  - Advanced stages: 90.7%

- **Have identified possible threats to our data:**
  - Early stages: 69.4%
  - Middle stages: 86.0%
  - Advanced stages: 88.2%

- **Know where most/all of our personally identifiable information/personal health information is located and where it flows within and outside our environment:**
  - Early stages: 60.7%
  - Middle stages: 82.8%
  - Advanced stages: 88.2%

- **Understand the data processing activities that impact the privacy and security of data:**
  - Early stages: 75.6%
  - Middle stages: 92.4%
  - Advanced stages: 96.3%

- **Conduct regular privacy risk assessments:**
  - Early stages: 57.4%
  - Middle stages: 80.3%
  - Advanced stages: 93.2%

None of the above: 1.7%, 0.6%, 1.9%
ATTRIBUTES AND HABITS OF MATURE PRIVACY AND DATA PROTECTION PROGRAMS

User data-monitoring practices
Organizations in the advanced stages of program development monitor user activity in applications that process personal data at much higher levels than those organizations in the early stages — 80.2% and 52.1%, respectively. Fifty-four percent of the respondents with more mature programs use automated tools for data monitoring compared with only 28.1% of those with programs that are still maturing.
Mature privacy programs use automated tools at twice the rate of those in early stages of development.

How user activity is monitored by maturity level:

- **We use an automated tool to monitor user activity**:
  - Early stages: 28.1%
  - Middle stages: 47.8%
  - Advanced stages: 54.7%

- **We manually review user activity logs**:
  - Early stages: 24%
  - Middle stages: 24.2%
  - Advanced stages: 25.5%

- **We don't currently monitor user activity on our systems**:
  - Early stages: 47.9%
  - Middle stages: 28%
  - Advanced stages: 19.9%
ATTRIBUTES AND HABITS OF MATURE PRIVACY AND DATA PROTECTION PROGRAMS

Privacy and/or security framework application
Framework prioritization is consistent across maturity levels, with higher adoption rates by advanced maturity organizations.

The two most followed frameworks across the board are NIST cybersecurity and ISO 27001, followed by internal or custom frameworks.

While cybersecurity frameworks still lead the pack, more than a quarter of respondents have adopted the NIST Privacy Framework less than a year after its launch. The advanced stage programs follow both the NIST Cybersecurity and Privacy Framework at much higher rates than those programs in the middle and early stages. Earlier adoption of new frameworks as represented by the quick adoption of the NIST Privacy Framework launched in 2020 may be differentiator of advanced maturity organizations.
Framework prioritization is consistent across maturity levels, with higher adoption rates by organizations in the advanced stages.

Privacy and/or security frameworks followed by maturity level

- AICPA GAPP: 7.4% Early stages, 11.2% Middle stages, 14.6% Advanced stages
- Internal and/or custom framework: 33.9% Early stages, 34.8% Middle stages, 14.9% Advanced stages
- CIS Critical Security Controls: 10.7% Early stages, 11.5% Middle stages, 14.9% Advanced stages
- ISACA’s Control Objectives for Information and Related Technology: 8.7% Early stages, 8.7% Middle stages, 8.7% Advanced stages
- Health Information Trust Alliance: 1.7% Early stages, 2.5% Middle stages, 3.7% Advanced stages
- ISO 27001: 46.3% Early stages, 51.6% Middle stages, 54.7% Advanced stages
- NIST Privacy Framework: 20.2% Early stages, 23.6% Middle stages, 38.5% Advanced stages
- NIST Cybersecurity Framework: 39.3% Early stages, 42.7% Middle stages, 55.9% Advanced stages

Legend:
- Early stages
- Middle stages
- Advanced stages
COMMON PRACTICES AND BENEFITS OF PRIVACY PROGRAMS ACROSS ALL MATURITY LEVELS
When looking across all maturity levels, a few key common practices and benefits of privacy programs surfaced.

Nearly all respondents stated their organizations offer some privacy and data protection training, with the majority as a separate module from any other data security training.

Respondents were asked how often they or their privacy team interact with the following departments: legal, human resources, information security, compliance, corporate ethics and information technology. The answers uncovered that interactions with other departments are similar, regardless of maturity level. Further, respondents consistently interact with legal, information security, compliance and information technology on a daily or weekly basis.
Over 50% of all respondents stated having a separate privacy training module.

Privacy and data protection training by maturity level

<table>
<thead>
<tr>
<th>Yes, as a separate module from any data security training</th>
<th>Yes, in the same module as our data security training</th>
<th>No, we only have data security training</th>
<th>No, we don't have privacy or security training</th>
</tr>
</thead>
<tbody>
<tr>
<td>58.3%</td>
<td>27.3%</td>
<td>8.3%</td>
<td>6.2%</td>
</tr>
<tr>
<td>66.9%</td>
<td>29.3%</td>
<td>2.5%</td>
<td>1.3%</td>
</tr>
<tr>
<td>66.5%</td>
<td>29.8%</td>
<td>2.5%</td>
<td>1.2%</td>
</tr>
</tbody>
</table>

Early stages | Middle stages | Advanced stages

58.3% | 27.3% | 8.3% | 6.2%

29.3% | 29.3% | 2.5% | 1.3%

29.8% | 29.8% | 2.5% | 1.2%

66.9% | 66.9% | 6.2% | 66.5%

29.3% | 29.3% | 2.5% | 2.5%

2.5% | 2.5% | 1.2% | 1.3%
Respondents interact most often with the legal, information security, compliance and information technology teams.

Departments most often interacted with and frequency

DAILY

<table>
<thead>
<tr>
<th>Department</th>
<th>Early stages</th>
<th>Middle stages</th>
<th>Advanced stages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legal</td>
<td>42.1%</td>
<td>42%</td>
<td>48.4%</td>
</tr>
<tr>
<td>Information security</td>
<td>38.6%</td>
<td>42%</td>
<td>43.5%</td>
</tr>
<tr>
<td>Compliance</td>
<td>27.3%</td>
<td>34%</td>
<td>40.6%</td>
</tr>
<tr>
<td>Information technology</td>
<td>31.8%</td>
<td>32%</td>
<td>32.9%</td>
</tr>
</tbody>
</table>

WEEKLY

<table>
<thead>
<tr>
<th>Department</th>
<th>Early stages</th>
<th>Middle stages</th>
<th>Advanced stages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legal</td>
<td>26%</td>
<td>29.9%</td>
<td>40.4%</td>
</tr>
<tr>
<td>Information security</td>
<td>22.3%</td>
<td>33.5%</td>
<td>40.4%</td>
</tr>
<tr>
<td>Compliance</td>
<td>21.7%</td>
<td>31.8%</td>
<td>33.8%</td>
</tr>
<tr>
<td>Information technology</td>
<td>31.4%</td>
<td>36.6%</td>
<td>36.6%</td>
</tr>
</tbody>
</table>

"Serving as subject matter experts to internal project teams, working with them at early stages to ensure privacy controls are built into new processes. This has prevented and/or reduced risk, prevented the need to do costly re-work, and helps keep customer privacy and regulatory compliance a key component in company operations."

— Survey respondent
When asked to tell us what element of their privacy/data protection program has had the most positive impact on their organization, “increased employee privacy awareness” rose to the fore among respondents of all stages and levels of maturity.

“We’re at the beginning of our program, but just having one has been beneficial. It reduces customer angst and increased privacy awareness among employees has improved their behavior and reduced risk.” — Early stages respondent

“Training and awareness program for employees and subcontractors. It costs little to implement and the benefits are huge in order to protect our data privacy assets.” — Middle stages respondent

“Training — awareness increases privacy compliance as well as incident reporting which leads to improvement where needed” — Advanced stages respondent

“Centralizing the privacy organization — we have increased awareness, training, and knowledge resulting in reduced breach incidents and incident response rates.” — Advanced stages respondent
Privacy and data protection programs are still maturing, but the value of simply having one is clear.

Dedicating resources to a privacy program yields greater awareness of privacy-related issues internally, leading to better outcomes externally.

Organizations with more mature privacy programs — those that regularly review privacy procedures and processes to ensure continual improvement and conduct reviews to assess the effectiveness of privacy controls — see greater gains in almost all areas asked about in this survey. When asked what benefits organizations are experiencing from their existing privacy programs, those with mature privacy programs saw the biggest improvements with:

- Reducing privacy complaints.
- Increasing operational efficiencies.
- Mitigating data breaches.
- Consumer trust.

Organizations looking to mature their privacy and data protections programs can consider the attributes and habits identified in this report:

- Have a distinct privacy team (full-time employees dedicated to privacy and working in a company’s privacy program).
- Budget ownership and C-level representation.
- Implement a comprehensive program, including things like having an incident response plan, providing regular data protection and privacy training to the workforce, and data protection policies and procedures that are reviewed/updated regularly.
- Actively monitor user activity in applications that process personal data.
- Follow privacy and cybersecurity frameworks.
CONTACT

Robin Hackney
Chief Marketing Officer
Robin.Hackney@FairWarning.com
Office: 727-897-8911