Crowe

September 2018

Moving From Inflexibility to Resiliency in Privacy and Data Protection

Why implementing a resilient privacy and data protection program is a smart decision that adds lasting value

An article by Pamela S. Hrubey, CCEP, CIPP/US; Adam L. Pajakowski, CIA, CFE; and Mike Varney, CPA, CIA

In a world where every day brings new developments in the area of privacy and data protection, "resiliency" – the ability to be flexible in the face of change or recover easily from difficulties – is not the word that most organizations think of when they consider their approach to privacy-related compliance with emerging regulations, evolving standards, and changing expectation of consumers and other stakeholders.

Some say steadfastness is the right approach to the constantly changing environment of privacy and data protection regulations – implying that an organization must stand firm in its use of current practices or stay strong as the legal team prepares a defense against needless or overreaching regulations.

Instead of being inflexible in the fight to stop new regulations or allowing the use of new technologies without understanding the impact of those technologies on personal data-related rights and freedoms, organizations may benefit from taking a resiliency-focused approach to privacy and data protection.

Why a resilient data protection program makes sense

Potential fines and penalties associated with the European Union's General Data Protection Regulation (GDPR) have caused senior leaders to increase attention to compliance. Also, new U.S. state privacy laws such as the *California Consumer Privacy Act of 2018*, effective Jan. 1, 2020, add additional complexity to the regulatory environment.

Looking past the possible penalties associated with noncompliance, a resiliency-focused approach makes sense in today's environment because of what happens after regulators issue a potentially large fine. The reputational costs of a privacy failure (regardless of who or what is at fault) may extend far beyond the initial fine or embarrassment associated with press releases about the failure.

What taking a resiliency-focused approach to privacy and data protection means and why it is a smart decision

A privacy resilient organization is familiar with its internal privacy and data protection landscape, and it has a robust privacy framework in place to set expectations and guide behaviors. The organization's leaders understand what policies and procedures are required of internal and external personnel working on behalf of the organization. Leaders are vocal about the importance of following the expectations set out in policies and procedures, and leaders follow those expectations themselves. Personnel are adequately trained, and regular communication reminds everyone about what is expected of them and why maintaining privacy matters. The organization takes advantage of monitoring and auditing capabilities to evaluate collective performance against expectations. In addition, the organization learns from its mistakes, taking corrective action when necessary to improve.

Based on the organization's profile and geographic reach, its leaders should consider the privacy regulations that affect it. They must recognize that privacy and data protection regulations are changing constantly – even the GDPR, newly effective in May 2018, will morph as the European Data Protection Board actively engages in creating new implementation guidance.

Lasting value comes from having a resilient privacy and data protection program that creates a competitive advantage for the organization, compared to those in the organization's peer group that might respond to privacy-related changes in the external environment on a one-off basis. Lasting value also comes from having related internal processes such as vendor management and customer relationship management in similarly resilient shape.

A resilient privacy and data protection program likely will create efficiencies and enhance effectiveness over time. Establishing a formal framework supports employee efforts to understand and live up to the organization's expectations, and it shows internal and external stakeholders that the organization takes privacy seriously.

As the privacy world continues to change, having a resilient privacy framework helps increase efficiencies over the long run by eliminating the organization's need to regularly launch large global projects to overhaul relevant elements in a patched-together privacy program. A resilient privacy framework isn't immune from the need to update practices; rather, such a program is focused on taking ongoing actions to benchmark progress, assess gaps, seek opportunities to improve, and learn from mistakes.

A structured privacy and data protection framework can provide a strong foundation for an organization to assess existing approaches to privacy and data protection or to implement improvements that support privacy resiliency.

Learn more

Pam Hrubey
Managing Director
+1 317 208 1904
pam.hrubey@crowe.com

Adam Pajakowski
+1 216 623 7539
adam.pajakowski@crowe.com

Mike Varney
Partner
+1 216 623 7553
mike.varney@crowe.com

crowe.com

MD-19001-032A