OLIVER WYMAN

DATA PRIVACY

GROWING EXPECTATIONS (AND RISK) FOR FINANCIAL INSTITUTIONS

Elena Belov, Allen Meyer, and Desislava Simeonova

MARSH & McLENNAN COMPANIES

Background and context

Lawmakers across the world are mobilizing to toughen laws on the data privacy of individuals. It would be unwise for Financial Institutions (FIs) to sit back and wait until all the details are firmed up. Instead, we believe FIs should treat data privacy as a top risk, like cyber risk, and adopt a proactive approach to managing it today. Lessons should be learned from cyber risk management's journey where a growing threat and several high-profile incidents (e.g., the Equifax data breach) led to significant attention and much stricter regulation over a short period of time. Data privacy could be the next discipline to be affected in this way.

In the last year, regulatory and public scrutiny of data privacy has increased globally due to highly-publicized data breaches and concern around the commercial use of personal data (e.g., Cambridge Analytica). In North America, legislators are scrambling to catch up to regions that are further ahead on data privacy (e.g., GDPR in the EU), with an ever-increasing bevy of legislation being introduced at both the state and federal levels. The most material of these legislative acts is the California Consumer Privacy Act (CCPA), which raises the bar for companies to disclose what personal information they collect, how the information is used, and whether it can be disclosed or sold. It also empowers customers with the choice to opt out of the collection and disclosure of their personal information. Other states in the US have drafted similar laws and at the federal level there is significant activity with several new laws being proposed.

Financial institutions collect and maintain large amounts of information relating to their clients, prospects, and employees. Given the numerous ways that FIs are using (and plan to use) personal information, and considering the evolution of regulation in this space, we believe that the industry needs to be both proactive and preemptive in managing data privacy risk.

An additional benefit of proactively investing in a strong data privacy culture is that banks can further their increasingly customer-centric focus. By investing in data privacy controls and processes, FIs can position themselves as the "safe bank" and even increase customer engagement.

We believe there are five no-regret steps that financial institutions should take today to get ahead:

1. Increase awareness at the senior executive and board levels
2. Understand how the organization uses personal information (today and in the future)
3. Conduct data privacy risk identification exercises
4. Determine the firm's stance on data privacy
5. Increase transparency and disclosure for consumers

Copyright © 2019 Oliver Wyman

STEP 1

Increase awareness at the Senior Executive and Board levels

Five years ago, when cyber risk was coming into the spotlight, senior executives and boards were hungry for information and education. Where are our top cyber risks? What capabilities do we have to manage these? What resources do we need to do this better? The elevation of the conversation enabled banks to get the attention and resources necessary to start properly managing the risk.

Similarly, leading financial institutions have now elevated the data privacy conversation to the Senior Executive and Board levels and have increased education and awareness of the topic. They have used these conversations to make important decisions about the future of their data privacy program – teeing up questions such as:

- "Are we in compliance with current rules and regulations?"
- "What are our biggest data privacy risks?"
- "Does our approach to data privacy support our strategy, business model and customer proposition? If not, what can we do?"
- "What are we doing to navigate the changing legislative agenda?"
- "Do we have the resources and infrastructure in place to handle the laws and regulations coming down the pipeline?"

Institutions that have not increased visibility of the topic should ensure that the board and senior management are informed about the changing data privacy landscape and how it affects the organization. Organizations should develop reporting that summarizes key external developments but also sheds light on the types of data privacy risks the firm is facing and its level of preparedness.

Copyright © 2019 Oliver Wyman

STEP 2

Understand how the organization uses personal information (today and in the future)

It is difficult to manage a risk if you don't know where you are exposed. A critical first step in managing data privacy risk is building a foundation of knowledge to understand what types of personal data is collected, where that data is stored, who can access it, and how it is used. This includes noting what data is acquired from, shared with, or sold to third parties, along with the business purpose for these arrangements. FIs should also understand what data is aggregated or anonymized, ensuring that if disclosed it is sufficiently unlinked and cannot be tracked back to an individual.

Many financial institutions have already made significant strides in understanding their IT assets, including data, from a cybersecurity perspective. This includes establishing IT asset inventories which record where data resides and how it is used. FIs can leverage these efforts as a starting point to build out comprehensive inventories of personal information, which should include the information of all relevant individuals – clients, prospects, and employees.

Most organizations with a large footprint in the west coast of the U.S. (those who need to comply with CCPA) have started creating some version of such inventories. These will be a significant asset for FIs trying to get a handle on data privacy risk. Yet, this is not where the benefits of establishing such a centralized view of personal information end. Identifying all personal information, cataloguing it, and building a centralized repository is a useful exercise for FIs to completely transform the customer experience. This treasure trove of information allows FIs to establish a customer view – a centralized view of consumer transactions and interactions with the bank – and translate that into effective marketing and product offering.

Copyright © 2019 Oliver Wyman

STEP 3

Conduct data privacy risk identification exercises

Once personal data and its uses have been identified, the next critical activity FIs need to undertake is to assess the key pockets of privacy risk they face. Many FIs already conduct top-down risk identification workshops to help identify their key non-financial risks, including cyber risk. Through these workshops, organizations can leverage business and functional knowledge to understand inherent risks as well as the effectiveness of the controls in place to protect against these risks.

We believe that financial institutions should hold similar risk identification and assessment workshops focused on data privacy, or at a minimum tailor existing cyber risk identification exercises to consider privacy as a key risk category. This can help FIs identify their biggest data privacy risk exposures (e.g., customer transparency/ consent, sharing of sensitive information with a third party with suboptimal data protection controls, aggregators), articulate potential risk scenarios, assess potential regulatory, financial and reputational impacts, and assess the efficacy of protective controls.

Financial institutions should implement a proactive rather than reactive approach to data privacy risk management, by understanding the firm's pockets of risk and investing in protective measures, rather than investing significant operational resources to deal with privacy issues after the fact.

Copyright © 2019 Oliver Wyman

STEP 4

Determine the firm's stance on data privacy

The scope and boundaries of data privacy are not as clear-cut as is the case with other risk types such as cyber, particularly in the context of still-evolving laws and regulations. As a result, the onus is on financial institutions to define what is in scope for their data privacy management and what the institution will or will not do regarding personal information. FIs should set an ambition and approach towards data privacy risk management considering the evolving nature of data privacy laws and regulations. The following questions should be considered when setting the ambition:

- **What do we consider to be personal information?** The nature of personal information has evolved significantly and under new regulations like the CCPA includes IP addresses, geolocation, profiles associated with a person or household, etc. Even if the legal definition in certain states/jurisdictions does not include these broader considerations, companies should consider including them for completeness.
- **How do we use and share personal information?** FIs should make conscious decisions about how information is collected, used, aggregated and shared by the organization (now and in the future) after weighing up the benefits and risks of each use.
- **How do we inform consumers about data use?** Organizations need to decide the level of granularity to provide in their disclosures and cover dimensions, including what data, how is it used, who is it shared with and why.
- **What rights do we give consumers?** Access, control, portability and deletion rights, as well as the right to challenge auto-decisions based on data, are likely to become standard. FIs need to determine the most customer-friendly yet operationally-feasible ways to provide these rights to consumers.

Copyright © 2019 Oliver Wyman

STEP 5

Increase transparency and disclosures for consumers

Most financial institutions have taken the minimal steps to update their consumer-facing privacy policies in a manner consistent with applicable regulations (e.g., GLBA in the US and PIPEDA in Canada).[1] Yet few institutions are thinking about ways to truly increase transparency and arm consumers with real knowledge about the privacy risks they face and what their financial institutions are doing to protect them.

We believe this is a quick-win measure that can have a positive impact on FI's brand perception. FIs can learn many lessons from technology companies that are the furthest ahead. For example some companies are making their disclosures more accessible, interactive, and informative. Some firms are also incorporating resources into their websites to help educate individuals on key privacy concepts and ways individuals can take steps to increase their privacy by adjusting settings.

1 Personal Information Protection and Electronic Documents Act.

Copyright © 2019 Oliver Wyman

Long-term vision

To manage data privacy risk in the long-term, financial institutions should transition towards a traditional risk management approach. This includes defining their privacy risk management operating model, with well defined division of roles across the three lines of defense, incorporating privacy impact assessments as part of their product approval processes, and integrating privacy within the broader risk management ecosystem, particularly across closely interlinked risk types such as cyber and third-party risk.

Financial institutions should also consider fundamentally shifting their approaches to data governance and technology implementation. Incorporating privacy by design principles early on in product, process, and technology design (for example, product systems are designed to rely on data collected and stored by other product systems to minimize the amount of data stored) can have a significant risk mitigation impact. This can position FIs in an advantageous position ahead of potentially increasing regulatory and consumer scrutiny.

Conclusion

Financial institutions should treat data privacy as a top risk and elevate the discussion with Senior Executives and the Board. Institutions should gain an understanding of what personal information is collected today and which data privacy risks they are most exposed to. A stance on data privacy should be taken – with tough decisions made around the degree of transparency, access, and control afforded to individuals. After the approach is firmed up, increasing transparency and disclosure to consumers will help reduce the risk of data privacy events or issues in the short term. These thoughtful steps will help elevate data privacy to a true strategic risk management discipline that considers a firm's reputation, good industry practices, and consumer expectations, rather than only waiting for legislation to dictate the approach.

Copyright © 2019 Oliver Wyman

About the Authors

ELENA BELOV

Partner in Financial Services, Lead for Data Privacy in North America
elena.belov@oliverwyman.com

ALLEN MEYER

Partner in Financial Services, Head of the Compliance practice in North America
allen.meyer@oliverwyman.com

DESISLAVA SIMEONOVA

Principal in the Risk & Public Policy and Digital practices
desislava.simeonova@oliverwyman.com

The authors would also like to thank Monica Hu for her contribution to the paper.

Oliver Wyman is a global leader in management consulting that combines deep industry knowledge with specialised expertise in strategy, operations, risk management, and organisation transformation.

For more information please contact the marketing department by email at info-FS@oliverwyman.com or by phone at one of the following locations:

AMERICAS	EMEA	ASIA PACIFIC
+1 212 541 8100	+44 20 7333 8333	+65 6510 9700

www.oliverwyman.com

Copyright © 2019 Oliver Wyman

All rights reserved. This report may not be reproduced or redistributed, in whole or in part, without the written permission of Oliver Wyman and Oliver Wyman accepts no liability whatsoever for the actions of third parties in this respect.

The information and opinions in this report were prepared by Oliver Wyman. This report is not investment advice and should not be relied on for such advice or as a substitute for consultation with professional accountants, tax, legal or financial advisors. Oliver Wyman has made every effort to use reliable, up-to-date and comprehensive information and analysis, but all information is provided without warranty of any kind, express or implied. Oliver Wyman disclaims any responsibility to update the information or conclusions in this report. Oliver Wyman accepts no liability for any loss arising from any action taken or refrained from as a result of information contained in this report or any reports or sources of information referred to herein, or for any consequential, special or similar damages even if advised of the possibility of such damages. The report is not an offer to buy or sell securities or a solicitation of an offer to buy or sell securities.

This report may not be sold without the written consent of Oliver Wyman.

OLIVER WYMAN