Security & Compliance Trends That Will Affect Your Biz in 2018 and Beyond

Whitepaper

info@katabat.com | Katabat.com

KATABAT

Background

One decade after the financial crisis of 2007–2008, the introduction of significant regulations on the banking industry has slowed down. Regulations range in scope from customer protection to capital adequacy for banks. The Dodd–Frank Wall Street Reform and Consumer Protection Act (2010), the Credit Card Accountability Responsibility and Disclosure Act (2009) and Basel III[1] (2010–2011) were implemented as a result of the financial crisis. Basel III is the only major international regulatory framework introduced as a result of the crisis that remains to be fully implemented, with a final implementation date of liquidity and capital requirements due in 2019. In Europe, the General Data Protection Regulation is in the final stages of implementation, with an enforcement date of May 11, 2018.

In the US, the current administration has proposed regulatory easing of the Dodd–Frank Act, but the consensus among the major advisory firms is that a broad regulatory pullback is over-optimistic. Regulatory requirements on governance around boards, capital and liquidity adequacy, treatment of customers, and executive oversight should remain roughly the same. Therefore, the level of new investment necessary to adhere to the requirements has crested.

The decrease in spending on new regulations should free up funds for banks to invest in data protection and managing cybersecurity risk, which is the top priority for banking executives.[2]

A 2017 PricewaterhouseCoopers (PwC) survey of 9,500 executives in 122 countries found that 44% of executives do not have a comprehensive information security strategy, 54% do not have an incident response process, and 48% do not have a security awareness training program for their employees.[3]

High-profile incidents, such as the Equifax data breach, ransomware attacks, and the leak of NSA tools, are expected to continue to rise. Therefore, the banking industry, always a target for crime, must continue to invest in modernizing and securing its technology resources and data processes.

Outlook

Priorities for technology executives in the banking industry in 2018 in the United States and Europe include using this time of expected regulatory easing to invest in modernization of their technology portfolios in order to manage cyber risk, while positioning the organizations to support revenue growth. [4]

---

[1] The Basel Committee on Banking Supervision released updates to its regulatory framework, Basel III, on December 7, 2017. Known as Basel IV, this round of updates lays out stricter guidelines for the use of credit and risk models, and has a five-year phase-in period beginning in 2022 and with full implementation in 2027.

[2] Global banking outlook 2018: Pivoting toward an innovation-led strategy. EY, p. 12.

[3] The Global State of Information Security® Survey 2018: Strengthening digital society against cyber shocks. PwC, 2017, p.4.

[4] Global banking outlook 2018: Pivoting toward an innovation-led strategy. EY, p. 5

Security Trends

In the area of security, we expect that cyber threats and fraud will continue to gain sophistication and to plague the industry. The level of innovation in areas of technology platforms, cloud solutions, and vendors will continue to facilitate the externalization of technology to meet the banks' strategic goals, moving banks one step closer in modernizing their technology portfolios.[5] Banks should use this opportunity to align their business strategy with risk management and regulatory compliance so that investments in these areas support strategic priorities such as growth.

The World Economic Forum's 2018 Risk Report lists cybersecurity as one of the five main risks to watch, as both the prevalence and potential for disruption continue to increase. We expect that emerging technologies will continue to disrupt current business models and change existing industry dynamics, in addition to introducing unexpected risks and threats. For example, the number of Internet-of-Things devices outnumbers the world's population by almost one million (8.4 billion IoT devices to 7.6 billion people). While helpful to consumers, this also facilitates distributed denial of service (DDoS) attacks.[6]

"Distributed denial of service (DDoS) attacks using 100 gigabits per second (Gbps) were once exceptional but have now become commonplace, jumping in frequency by 140% in 2016 alone. And attackers have become more persistent—in 2017 the average DDoS target was likely to be hit 32 times over a three-month period." - World Economic Forum's 2018 Risk Report

As cybercrimes and criminals continue to get more advanced, thought leaders are also expected to use more sophisticated technologies and partners to minimize their risk. Use of artificial intelligence to analyze data to identify and highlight vulnerabilities will begin to gain traction as a second-line defense mechanism to protect from cyber attacks.

Given the rapidly changing landscape, it will be challenging for regulators to stay ahead of the innovation.

[5] Navigating the year ahead: 2018 banking regulatory outlook. Deloitte Center for Regulatory Strategy Americas, December 2017, p. 5.
[6] Global Risks 2018: Fractures, Fears and Failures. World Economic Forum.

Regulatory Environments

On a regulatory front, regulations that remain to be implemented in 2018 that pertain to a bank's operational security (as opposed to financial health) are all front-loaded in the first half of the year. These regulations focus on the protection of private information and customer due diligence to combat money laundering.

Data protection regulations:

- January 2018: Second Payment Services Directive (PSD2) rules were implemented as national law in European Union member countries for banks and payment service providers doing business in the European Union.
- May 2018: The Security of Network and Information Systems Directive (NIS) for businesses in the European Union member countries identified by the Member States as "operators of essential services."[7]
- May 2018: EU General Data Protection Regulation (GDPR) enforcement for data processors and controllers conducting business in the European Union

Crime-prevention regulations:

- April 2018: New York State Department of Financial Services Rule 504 was implemented as an anti-terrorism measure to strengthen data quality and controls. The first compliance certification is due in April for banks conducting business in New York.
- May 2018: Financial Crimes Enforcement Network's (FinCEN) Customer Due Diligence/Beneficial Ownership Rule compliance for United States institutions that are "federally regulated banks and federally insured credit unions, mutual funds, brokers or dealers in securities, futures commission merchants, and introducing brokers in commodities." [8]

Due to the nature of their business, a failure in a financial services corporation has the potential to cause a system-wide failure. As such, regulations that strengthen cyber and data security, such as GDPR and NIS, may just be the beginning of a new set of requirements on the financial industry. High-profile incidents, such as the Equifax breach in 2017 and the Yahoo data breach reported in 2016, are expected to continue into 2018 and beyond.

[7] The Directive on security of network and information systems. European Commission - NIS Directive, July 5, 2016, accessed March 3, 2018.
[8] Customer Due Diligence Requirements for Financial Institutions FAQs. U.S. Department of the Treasury Financial Crimes Enforcement Network, July 19, 2016.

Financial Markets

February 2018 has seen the financial markets enter a period of volatility. Analysts are divided on whether it is a short-term market correction or a harbinger for a cyclical downturn, for which we are due. Each of the past recessions has brought new regulations to protect from the faults and weaknesses in the system prior to the downturn. Therefore, this is the time for banks to get ahead of the market by investing in systems and operations that can: 1) Predict an oncoming downturn; 2) Facilitate the recovery with timely and accurate data for decision-making; and 3) Respond nimbly to a changing landscape.

What Does This Mean for Your Business?

Now is the time to get ahead of the regulations, especially in the US. In areas where regulators have not set standards, such as blockchain-based systems, banks should work to influence the conversation, if they haven't already. During this period of growth, leaders should consider the organization's strategic goals in relation to mitigating cybersecurity risks and migrating to a digitally-enabled, customer-centric business model. Finally, if you are one of the 44% of executives who don't have a comprehensive information security strategy or if your organization is one of the 54% that don't have an incident-response process, 2018 should be the year to address those deficiencies.

How Prepared Are You?

Run through this checklist to see how prepared your company is:

Who may benefit from stealing our data?

- ❑ Financially-motivated attackers
- ❑ Nation-state actors

What should we be doing now?

- ❑ Are there any at-risk clients?
- ❑ Do we have a communications protocol in place in the event of a data breach?

How robust are our cybersecurity controls?

- ❑ Is our customer data encrypted?
- ❑ How strong is our firewall?
- ❑ Do we monitor anomalies in network activity?
- ❑ Do we monitor the dark web for our customers' data?

How robust are our anti-fraud controls?

- ❑ How well do we know our customers? Have we verified their information?
- ❑ Do we have a training program in place for our employees?
- ❑ Do we have multiple levels of review in our process?

How do we protect our customers' data?

- ❑ Is our customer data encrypted?
- ❑ What are our operational controls on protecting non-public, personally identifiable information (PII)?
- ❑ Are our employees adequately trained in our operational controls?

Secured. Effortlessly with Katabat.

In over 10 years, we have never suffered a breach. Learn how easy it is to work with the best by speaking to a member of our team:

- Schedule an introductory call
- Schedule a product demo
- Learn more about our lending solutions

info@katabat.com | Katabat.com

KATABAT