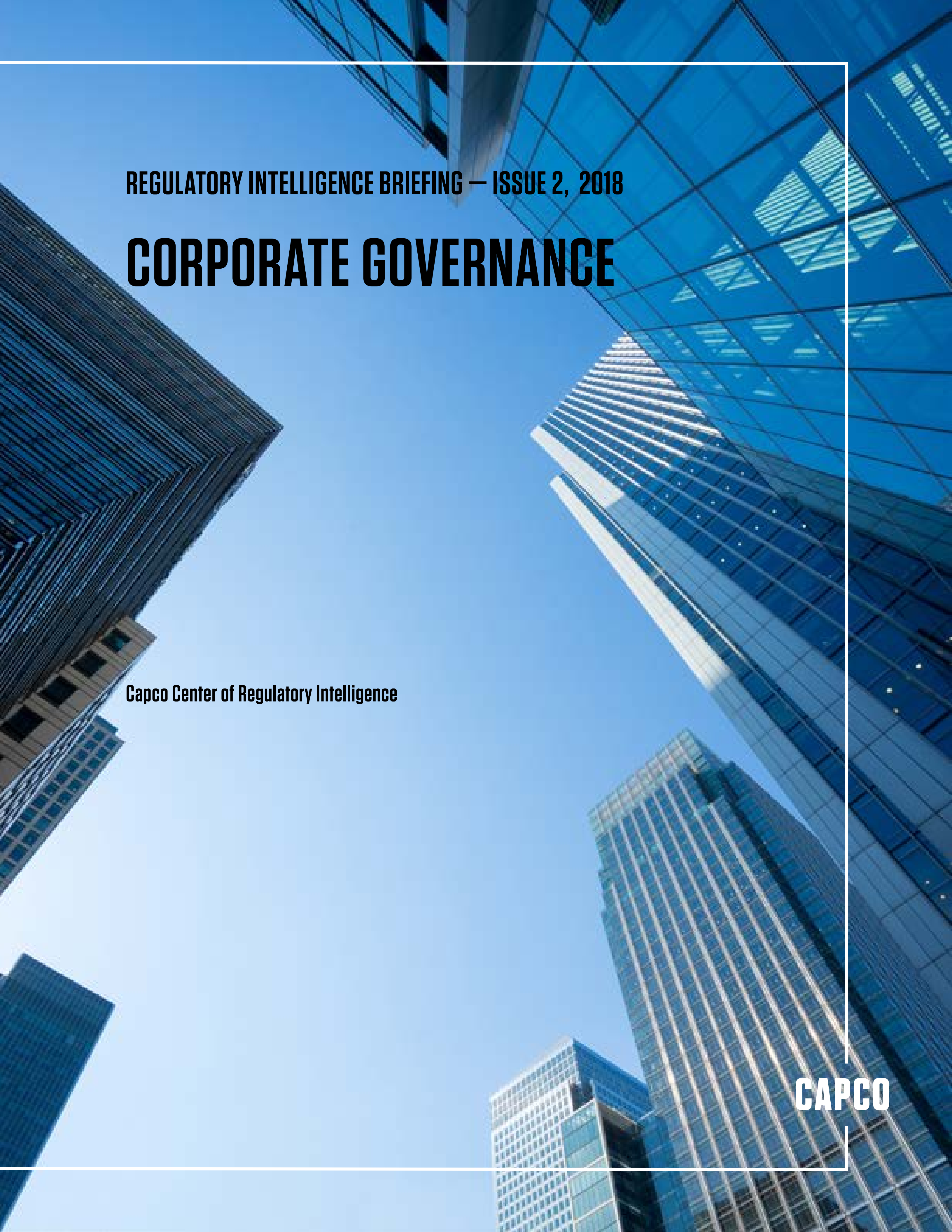


REGULATORY INTELLIGENCE BRIEFING — ISSUE 2, 2018

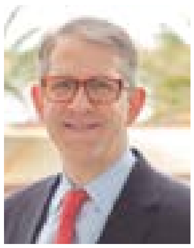
CORPORATE GOVERNANCE

Capco Center of Regulatory Intelligence

CAPCO

IN THIS ISSUE

EDITORIAL NOTE FROM THE MANAGING PRINCIPAL, CENTER OF REGULATORY INTELLIGENCE



PETER D. DUGAS
MANAGING PRINCIPAL, CENTER OF REGULATORY INTELLIGENCE

Peter has more than 16 years of government and consulting experience in advising clients on supervisory matters before the U.S. government and in the implementation of enterprise risk management programs. He is a thought leader in government affairs and regulatory strategies in support of banks' and financial institutions' compliance with the Dodd-Frank Act and Basel Accords. Prior to joining Capco, he served as a director of government relations at Clark Hill and in senior government positions, including serving as a deputy assistant secretary at the United States Department of the Treasury.

As industry trends from 2017 continue into the beginning of 2018, corporate culture and governance is becoming even more important. Throughout recent months, regulators have showcased, through enforcement actions, settlements and guidance, that a spotlight continues to shine on institutions' corporate governance. But, while the number of stakeholders and the influence the financial sector has on other industries increases the attention on governance practices in the financial services industry, best practices can be difficult for financial institutions to ascertain and execute, due to the broad nature of the principles.

In this month's Regulatory Intelligence Briefing (RIB), we explore some of the latest developments in corporate governance to help your institution stay informed and proactively protected. We start by looking into recent enforcement actions and outlining some of the tools regulatory agencies have to discipline financial institutions, painting a picture of the potential risks a lapse in effective corporate governance can pose. We then discuss some of the new guidance and legislation that impact corporate governance structures, including the Tax Cuts and Jobs Act and a proposal by the Federal Reserve Board aimed at board of directors' effectiveness. Lastly, we outline best practices to help your institution make a competitive shift toward a more efficient, current and advantageous corporate governance structure.

Our secondary article this month reinforces the importance of business continuity planning. Following a messaging error about a ballistic missile attack in Hawaii and recent storms pounding the east coast, institutions should review their messaging systems and requirements associated with disasters. Preparation and clearly defined roles can translate into shorter recovery times and mitigation of overall damage.

Our Congressional Hearing Summary aims to help institutions understand the tangle of laws and regulations that cover data security and breach notification. Currently, there is no federal standard for data security measures and the area is guided by a patchwork of laws and regulations at the state level. Also, despite recent widespread data breaches, there are still inconsistencies in breach notification requirements from state to state, as wide as some states not requiring any notification following a breach of personal data.

As always, this month's RIB is intended to keep your institution informed and abreast of changes and trends within the financial services industry that affect your compliance, operations and risk mitigation efforts. Capco Center of Regulatory Intelligence (CRI) will continue tracking these subjects and delivering updates as the areas evolve.

REGULATORY ROUNDUP

Regulatory and Compliance Alerts

IRS Proposes Rule to Eliminate Unnecessary Tax Regulations

On February 15, 2018, the Internal Revenue Service (IRS) proposed a rule to streamline IRS regulations by removing 298 regulations that are no longer necessary because they do not have any current or future applicability under the Internal Revenue Code, and by amending 79 regulations to reflect the proposed removal of the 298 regulations. **Comments are due by May 14, 2018.**

CSBS Releases BSA/AML Compliance Tool for Money Services Businesses

On February 13, 2018, the Conference of State Bank Supervisors (CSBS) announced the release of a new, voluntary tool to help money services businesses better manage Bank Secrecy Act/anti-money laundering (BSA/AML) risk. The BSA/AML Self-Assessment Tool, which CSBS and state regulators developed, aims to help institutions better identify, monitor and communicate BSA/AML risk.

GAO Reports on BSA and De-risking in Southwest Border Region

On February 26, 2018, the Government Accountability Office (GAO) published a report with recommendations to the Financial Crimes Enforcement Network (FinCEN) and the federal banking regulators regarding the impact of Bank Secrecy Act (BSA) regulations in the southwest border region of the U.S. The report was in response to consumers and businesses reporting that accessing certain banking services was becoming increasingly more difficult.

FTC Releases Paper on Key Financial Issues that Affect Military Consumers

On February 2, 2018, the Federal Trade Commission's (FTC) Bureau of Consumer Protection issued a Staff Perspective paper that examines financial issues that can affect military consumers, including servicemembers, veterans and their families, when they are purchasing and financing a car, dealing with debt collectors or making credit decisions. The paper also discusses these consumers' legal rights and remedies, and strategies to promote financial literacy and capability.

BCBS Publishes Paper on Fintech Implications for Banks and Bank Supervisors

On February 19, 2018, the Basel Committee on Banking Supervision (BCBS) published a paper titled "Sound Practices on the Implications of Fintech Developments for Banks and Bank Supervisors." The paper assesses how technology-driven innovation in financial services may affect the banking industry and the activities of supervisors in the near to medium term.

Agencies Propose Amendments to Swap Margin Rule

On February 5, 2018, the Federal Reserve Board, Farm Credit Administration, Federal Deposit Insurance Corporation, Federal Finance Housing Agency and Office of the Comptroller of the Currency jointly proposed to amend swap margin requirements to conform with recent rule changes that impose new restrictions on certain qualified financial contracts (QFCs) of systemically important banking organizations. **Comments are due by April 23, 2018.**

CONGRESSIONAL HEARING SUMMARY: PROTECTING PERSONAL DATA

With a recent rise in data breaches, consumers in today's world no longer have control over their own data — how can we regain consumer privacy?

According to the Identify Theft Resource Center, the number of data breach incidents tracked in the U.S. in 2017 increased over 44 percent from 2016 to 1,579, a new high. A 2014 report from the Federal Trade Commission (FTC), shows that there are between 2,500 – 4,000 data brokers in the U.S. operating without consumers' knowledge or consent.

On February 14, 2018, the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit held a hearing to address data security and breach notification laws and regulations. Witnesses included:

- Aaron Cooper, Vice President, Global Policy, BSA – The Software Alliance
- Kim Sponem, Chief Executive Officer and President, Summit Credit Union, on behalf of the Credit Union National Association
- Nathan Taylor, Partner, Morrison & Foerster LLP
- Marc Rotenberg, President, Electronic Privacy Information Center, and Adjunct Professor, Georgetown University Law Center
- Paul Rosenzweig, Senior Fellow, R Street Institute

For financial institutions, the issue of data breaches is particularly expensive. In her testimony, Sponem outlined some of the costs to credit unions, including: debit and credit card replacement and reissuance; fraud monitoring, including monetary and labor expenses; complaint and input management following a breach; and expenses associated with processing and refunding fraudulent charges.

The witnesses agreed that there is a great need for a solution to these issues, and that these particular areas require reform:

- Federal data protection standards
- Meaningful enforcement
- Breach notification standards

However, the differences lie in the details. This article will expand upon these three areas and summarize some of the legislative proposals introduced into Congress to address issues around data protection and breach notification.

> "Consumers are left not only facing financial harm but also the daunting task of restoring the integrity of their personal information."
>
> - Rep. Blaine Luetkemeyer (R-MO)

National Data Protection Standards

Differences across states

Due to the patchwork of state laws, consumers are protected differently across the U.S. These differences range from as broad as whether or not an institution is required to notify victims, to as narrow as what is considered "personally identifiable information."

Creating a federal standard

Sponem advocated a federal standard to "ensure that all consumers and financial institutions are protected at least at some level, without preempting any states' right to impose additional requirements," while Taylor said any bill should "include strong, yet flexible and scalable, data protection standards for all companies that handle sensitive personal information."

Potential drawbacks of rigidity

However, multiple witnesses expressed fear that a rigid mandate could potentially undermine innovation. As Cooper stated: "Organizations must be able to deploy appropriate and cutting-edge security measures and technologies to protect themselves and their customer's sensitive data effectively against current and future threats."

The issue with consent decrees

Rosenzweig argued that current guidance from regulatory agencies like the FTC comes in the form of consent decrees that "articulate an indefinite standard of reasonable behavior." Because the costs of fighting regulatory action against them (including reputational harm) are so high, many companies settle with the FTC and sign the decrees. But sometimes this means consenting to FTC monitoring for 20 years, which is an exceptionally long time in the technology space.

Creating a safe harbor

Considering these concerns, some witnesses discussed a safe harbor for compliance under a new standard, which would create a presumption of compliance for organizations that comply with recognized industry standards for data security risk management.

Meaningful Enforcement Actions

Gaps in regulation

Currently, the FTC and the Consumer Financial Protection Bureau (CFPB) serve roles in the federal regulatory process. However, the FTC's power is limited to bringing enforcement actions against unfair and deceptive practices and the CFPB only has jurisdiction over financial institutions.

The question of state involvement

This gap begs the question: how involved should the states be? According to Cooper, "A federal standard should ensure that vigorous enforcement can take place to defense consumers against businesses that fail to provide fair protection of sensitive personal data, without interfering with legitimate business." But, it may also consider state Attorneys General, which have played an important role in the past when the federal government did not step in.

Establishing a federal data protection agency

Rotenberg believes the U.S. should establish a federal data protection agency, stating, "Virtually every other advanced economy has recognized the need for an independent agency to address the challenges of the digital age." He also highlighted an independent agency that could meaningfully participate in the current process, the Privacy and Civil Liberties Oversight Board, "lies dormant."

Notification Requirements

Inadequate consumer notification

Due to the discrepancies between notification laws across the U.S., Sponem explained that oftentimes "consumers first learn that their personal information has been compromised when their financial institution replaces their debit or credit card."

Notification timeframe debate

Based on this, witnesses agreed that there is a need for "prompt and uniform consumer notification" after an institution discovers a breach, but there was some debate as to whether or not there should be a fixed deadline for this. As a starting point for discussion, the European Union (EU) General Data Protection Regulation (GDPR) going into effect in just a few months will require personal data breach notification within 72 hours. Rotenberg proposed that consumers and law enforcement be notified within 48 hours. However, some of the witnesses argued that institutions may not be able to accurately and effectively notify a consumer of a data breach within this timeframe.

Defining the terms

The definition for a "reasonable standard of notification" will be important. Some of the issues to consider include:

- Who must provide the notification? Is it the organization with which the consumers have a direct relationship? Is it the business or vendor responsible for the breach?
- How should consumers be notified? Which forms of notification are appropriate (e.g., email, text message, social media)?
- Should institutions provide free credit freezes associated with breaches?

Current Legislative Proposals

TITLE	SPONSOR	SUMMARY
Consumer Privacy Protection Act of 2017 (S. 2124)	Sen. Patrick Leahy (D-VT)	To ensure the privacy and security of sensitive personal information, to prevent and mitigate identity theft, to provide notice of security breaches involving sensitive personal information and to enhance law enforcement assistance; and other protections against security breaches, fraudulent access and misuse of personal information
Comprehensive Consumer Credit Reporting Reform Act of 2017 (H.R. 3755)	Rep. Maxine Waters (D-NY)	To amend the Fair Credit Reporting Act to revive requirements for disputes regarding consumer credit information a consumer reporting agency reports, limit the circumstances in which a credit reporting agency may furnish a consumer report for employment purposes, revise requirements relating to information contained in credit reports, require disclosure of free credit scores to consumers with their free annual consumer reports, require the CFPB to issue final regulations for developing credit scoring models and create a nationwide credit reporting agency registry
The PROTECT Act of 2017 (H.R. 4028/S. 1982)	Rep. Patrick McHenry (R-NC) and Sen. David Purdue (R-GA)	To require supervision and examination of large consumer reporting agencies regarding cybersecurity measures, to allow consumers to request a consumer reporting agency to place a security freeze on their reports and to prohibit consumer reporting agencies from using a consumer's Social Security number in a consumer report or as a method of consumer identification
Free Credit Freeze Act (H.R. 3878)	Rep. Ben Ray Lujan (D-NM)	To prohibit a consumer reporting agency from charging a consumer a fee for placing, temporarily lifting or fully removing a credit freeze and prohibiting a consumer reporting agency from releasing any credit information without the consumer's permission
Personal Data Notification and Protection Act (H.R. 3806)	Rep. James Langevin (D-RI)	To establish a national data breach notification standard that requires notification within at least ten days, among other things
The Data Breach Prevention and Compensation Act (S. 2289)	Sen. Elizabeth Warren (D-MA)	To create an Office of Cybersecurity at the FTC to supervise data security at consumer reporting agencies, to require the promulgation of regulations establishing standards for effective cybersecurity at consumer reporting agencies, to impose penalties on credit reporting agencies for cybersecurity breaches that put sensitive consumer data at risk and for other purposes
The Data Broker Accountability and Transparency Act (S. 1815)	Sen. Edward J. Markey (D-MA)	To prohibit data brokers from obtaining, or causing to be disclosed, personal information relating to any person by making a false, fictitious or fraudulent statement or representation, including by providing any document that the broker knows or should know to: (1) be forged, counterfeit, lost, stolen or fraudulently obtained; or (2) contain a false, fictitious or fraudulent statement or representation

FOCUS:
CORPORATE GOVERNANCE

An increased regulatory focus on corporate governance in recent months has institutions wondering what they can do to ensure best practices for enterprise management and risk governance.

WHAT "CORPORATE GOVERNANCE" MEANS TODAY

Corporate governance began with the idea that with a separation of ownership, there must be structure to who is held accountable for certain aspects of business functionality. A sort of contract between parties, the initial thought was that shareholders who appointed agents to manage their investments needed protection — and faith that their money was being handled well.

Corporate governance in today's world takes on the balance of many more contributing factors. It refers not only to the relationships among the bank's board, management, shareholders and other stakeholders, but also to the board and senior management's authority and responsibilities to manage an institution's operations and structure. This includes risk governance which necessitates the effective identification, measurement, monitoring and controlling of risks to ensure that all institutional activity is aligned with strategic objectives and risk appetite.

/ complicating considerations

However, the issue quickly becomes more complicated. We see that the separate parties' potential inability to effectively form their "contract" may require regulatory supervision — and indeed, in today's market, regulators play a large role in shaping corporate governance standards. The Office of the Comptroller of the Currency (OCC), for example, has taken on a role in this supervision process and reflects the current focus on the criticality of thorough corporate governance structures, stating, "Corporate and risk governance is the framework in which all risks are managed at a bank as well as the oversight of the framework."

/ the financial services industry in particular

While corporate governance has been a hot topic across most industries, it is particularly relevant and complicated for the financial sector. The potential for managers to profit at the expense of shareholders, which is the very opportunity that brings rise to the necessity of corporate governance, is especially in the limelight for the financial services industry. The explanation is twofold: first, banks have more stakeholders than nonbanks, including depositors, debt-holders and government (as insurers of deposits and residual claimants on systemic externalities), and there are many different interests, including that shareholders are more likely to take risks than are stakeholders who don't have as substantial of an opportunity for positive returns (depositors and debt-holders, for example). Second, the financial sector is central to the economy and exerts many influences on other industries.

The supervisory focus on corporate governance in the financial services sector is therefore tremendous, though not without confusion and burden for boards hoping to stay compliant with legislation and guidance. In a multi-year review of boards of directors' practices to support new guidance creation, the FRB found that "supervisory expectations for boards of directors and senior management have become increasingly difficult to distinguish." The agency also stated that "Greater clarity regarding these supervisory expectations could improve corporate governance overall, increase efficiency, support greater accountability, and promote compliance with laws and regulations."

/ your institution

Ensuring your institution has a strong focus on corporate governance, and ensuring best practices within the area, can help your business overall. Firstly, it mitigates risk and enforcement actions (both by actually decreasing instances of noncompliance and also by proving to regulators that you are acting in good faith and to the best of your abilities). Secondly, it increases good press and respect from shareholders, clients and the general public (therefore advancing your institution's reputation).

REGULATORY ENFORCEMENT TRENDS

Since an effective corporate governance model ensures firm-wide best practices and consequently mitigates risk exposure, the opposite can also be true; regulators finding fault within an institution's operations often find these errors to be indicative of substandard governance.

Those in the financial services industry are no stranger to the types of enforcement actions that stem from corporate governance issues. For firms who fail to comply with statutes and regulations, regulating agencies can take many types of punitive actions, most often in the form of civil money penalties.

/ OCC announces penalty

On February 7, for example, the OCC announced that the U.S. subsidiary of a foreign bank will forfeit over $360 million after pleading guilty to conspiring with several former executives to defraud the U.S. by unlawfully impeding the OCC's ability to regulate the bank, and to obstruct an OCC examination of the bank's operations throughout California. This ruling comes less than two months after the bank's former vice president entered into a deferred prosecution agreement for his role in aiding and abetting the bank's failure to maintain an anti-money laundering (AML) program that met Bank Secrecy Act (BSA) requirements.

/ FRB issues unusual penalties

But, as we recently saw in a Federal Reserve Board (FRB) ruling against a large bank, civil money penalties are not the only way in which regulators can take action against institutions for corporate governance issues. After finding the bank had not met corporate governance expectations, the FRB has disallowed the bank to increase its total consolidated assets to above December 31, 2017, levels until the FRB lifts the restriction.

The FRB also sent letters of disapproval to the bank's board, former CEO and a past independent director, demanding a larger focus on corporate governance from the individuals. In addition to the asset growth cap, the bank has also agreed to replace four board members. Further, the FRB plans to investigate "present or former officers, directors, employees, agents, and consultants" of the bank who were involved in the activities.

Through these actions, FRB focused on specific governance practices that all institutions should apply, including enhancing board effectiveness and oversight; improving firm-wide compliance and operational risk management programs; holding senior management accountable for implementing and maintaining policies in accordance with board guidance and risk tolerance; and ensuring senior management provides "an effective and independent firm-wide risk management function" that "covers all material risks" facing the institution and has the "requisite stature, authority, and resources." Additional lessons learned in these types of scenarios include that corporate governance issues can also impact a financial institution's ratings, including credit ratings and other bank ratings.

/ different penalties for different institutions

These examples show two dire scenarios and outcomes, the magnitude of which is largely influenced by the size of the institutions in question. In smaller banks, problems within governance, and consequences for these problems, still exist. Earlier this year, the FRB banned a man who served as the president, chairman and CEO of a failed state bank from the industry, after finding that he used his position to benefit from improper loan decisions.

/ authority from different regulators

Recently, regulators have issued certain enforcement actions that the financial services industry does not commonly see. It begs the question: what types of enforcement actions can regulators take against those under their jurisdiction? Below, we've outlined action types for two regulators, the OCC and the SEC.

As a federal banking regulator, the OCC can take punitive action against institutions and institution affiliated parties (IAPs; including individuals and entities) it supervises through:

Institutions

Formal Agreements

Institutions agree to take actions or follow proscriptions in a written agreement

Prompt Corrective Action Directives

Institutions are required to take actions or to follow proscriptions the OCC imposes

Safety & Soundness Orders

Institutions are required to take actions or to follow proscriptions the OCC imposes

Institutions and IAPs

Cease & Desist Orders

Institution/IAP is required to take actions or follow proscriptions in the orders

Civil Money Penalty Orders

Institution/IAP must pay fines

Notices Filed

Institution/IAP has an opportunity to litigate the matter before an Administrative Law Judge after receiving Notice of Charges and/or Notice of Civil Money Penalty Assessment

Securities Enforcement Actions

Institutions/IAPs engaging in securities activities may receive action including censures, suspensions, bars and/or restitution, pursuant to the federal securities laws

IAPs

1829 Notifications

IAPs who have been convicted of, or entered into a pretrial diversion or similar program for certain criminal offenses, are notified by letter that they are prohibited from participating in the affairs of any insured depository institution without prior regulatory or judicial approval by operation of law

Removal/Prohibition Orders

IAPs are prohibited from participating in the affairs of any insured depository institution without prior regulatory approval

Restitution Orders

IAPs are required to reimburse banking organizations or FDIC for losses caused or for unjust enrichment

As a market regulator, in order for the SEC to take action, the agency must file a complaint with a federal court, an administrative law judge or both to ask for a sanction or remedy against broker-dealers, investment advisers and other regulated entities, as well as individuals associated with those entities. These are some potential actions:

Injunction	Disgorgement	Barring	Civil money penalties
SEC obtains a court order enjoining an individual or an entity from further violations of the securities laws; can require audits, accounting for frauds or special supervisory arrangements	Individual or entity must return money obtained from illegal conduct	A firm can no longer act as a securities firm or an investment adviser; an individual may not associate with any securities firm or investment adviser; a professional may not practice before the SEC	Individual or entity must pay fines

NEW GUIDANCE AND LAWS

With this increased focus on corporate governance, we have concurrently seen the adoption and expansion of new and updated legislation and guidance surrounding these issues, across federal agencies and even within the Tax Cuts and Jobs Act.

/ Tax Cuts and Jobs Act

The "Modification of limitation on excessive employee remuneration" section of the Tax Cuts and Jobs Act (Section 3801 of Subtitle I -- Compensation), undoes Section 162(m) of the Internal Revenue Code, severely limiting the deduction companies can claim for senior executive compensation under "pay-for-performance" arrangements. The "pay-for-performance" model has been tied to short-run financial metrics, and some believe it is a major reason for the overwhelming focus on near-term profits and stock prices rather than longer-term investments and practices that safeguard and benefit institutions and the financial system overall.

The House Committee on Ways and Means reflects this sentiment, and takes it further by stating that Section 162(m) could have, in certain instances, influenced dishonestly in quarterly reporting: "The significant exceptions to the current limit on the deductible executive compensation by publicly traded corporations have resulted in a shift away from cash compensation paid to senior executives in favor of stock options and other forms of performance pay...This shift has led to perverse consequences as some executives focus on — and could, in rare cases, manipulate quarterly results (off of which their compensation is determined), rather than on the long-term success of the company."

Many view this this cap on executive compensation as an opportunity for reform in terms of executive expectations, and a reflection of the trending societal call for better practices from institutional leadership. Though the effects on institutional practices due to this loss of deductibility for executive compensation remain to be seen, with some more left-leaning sources doubting the change's ability to influence corporate behavior, it seems to be symbolic of a shift toward mandated accountability of top executives and directors.

/ FRB Guidance

In August, the FRB requested public comment on a corporate governance proposal to enhance the effectiveness of boards of directors. The agency outlined institutions' boards' return to core duties, which it defined as:

- "guiding the development of the firm's strategy and the types and levels of risk it is willing to take (also referred to as risk tolerance);
- overseeing senior management and holding them accountable for effective risk management and compliance among other responsibilities;
- supporting the stature and independence of the firm's independent risk management and internal audit functions; and
- adopting effective governance practices."

The corporate governance proposal comprises three measures:

1. **Identifying the attributes of effective boards of directors.**
   / For the largest institutions, The FRB will use these attributes to inform a new set of guidelines, which the agency will use in evaluating a firm's governance and controls.

2. **Clarifying that in most situations, supervisory findings should be directed to an institution's senior management, rather than to its board of directors, for corrective action.**
   / The FRB will revise SR 13-13/CA Letter 13-10, "Supervisory Considerations for the Communication of Supervisory Findings," to clarify that FRB examiners and supervisory staff would direct Matters Requiring Attention (MRAs) and Matters Requiring Immediate Attention (MRIAs) to boards of directors only when a board needs to address its corporate governance responsibilities or when senior management does not take appropriate remedial action. The proposal makes it clear, however, that boards would remain responsible for holding senior management accountable for remediating supervisory findings.

3. **Eliminating or revising certain existing supervisory expectations for boards of directors.**
   / FRB has identified 27 Supervisory and Regulation (SR) letters for potential elimination or revision, which collectively include more than 170 supervisory expectations for holding company boards. The agency hopes to refocus its supervisory guidance through identifying and evaluating these SR letters relating to boards of directors of banks and savings and loan holding companies of all sizes. For firms with more than $50 billion in total consolidated assets, this means being in line with the new standards discussed in measure one, above. For firms with less than $50 billion in total consolidated assets, this will mean aligning with SR 16-11.

SR 16-11

(Supervisory Guidance for Assessing Risk Management at Supervised Institutions with Total Consolidated Assets Less than $50 Billion) includes "supervisory expectations for the roles and responsibilities of the board of directors for an institution's risk management, such as approving the institution's overall business strategies and significant policies; understanding the risks the institution faces and having access to information to identify the size and significance of the risks; providing guidance regarding the level of acceptable risk exposures to the institution; and overseeing senior management's implementation of the board-approved business strategies and risk limits."

/ OCC Booklet

In July 2016, the OCC announced its new "Corporate and Risk Governance" booklet of the Comptroller's Handbook, which "provides examiners with an overview of corporate and risk governance, the associated risks, the board and management's roles in these activities, and examination procedures to use during supervisory activities that focus on evaluating [banks'] corporate and risk governance." WIthin the booklet, the OCC defines the core duties of a board as the responsibility to:

- Set the bank's strategy, objectives and risk appetite
- Establish the bank's risk governance framework
- Identify, measure, monitor and control risks
- Supervise and manage the bank's business
- Protect the interests of depositors, protect shareholders' or members' obligations and take into account the interests of other stakeholders
- Align corporate culture, activities and behaviors with the expectation that the bank will operate in a safe and sound manner, operate with integrity, and comply with applicable laws and regulations

CHALLENGES AND SOLUTIONS

On August 30, 2017, FRB Governor Jerome Powell gave a speech at the Large Bank Directors Conference in Chicago, IL on the role of boards at large financial institutions. He listed five common attributes that effective boards should exhibit, reflecting supervisory expectations on the matter:

1. "First, an effective board should guide the development of a clear and coherent strategy for the firm and set the types and levels of risks it is willing to take. Alignment of business strategy and risk appetite should minimize the firm's exposure to large and unexpected losses. In addition, the firm's risk management capabilities need to be commensurate with the risks it expects to take.

2. Second, an effective board should actively manage its information flow and deliberations, so that the board can make sound, well-informed decisions that take into account risks and opportunities.

3. Third, an effective board should hold senior management accountable for implementing the firm's strategy and risk appetite and maintaining the firm's risk management and control framework.

4. Fourth, an effective board should ensure the independence and stature of the independent risk management and internal audit functions. It is difficult to overstate the importance of this. Risk management systems and controls may discourage or limit certain revenue-generating opportunities. Failure to ensure the independence of these functions from the revenue generators and risk takers has been shown to be dangerous, and this is something for which the board is accountable.

5. Finally, an effective board should have a composition, governance structure, and set of established practices that are appropriate in light of the firm's size, complexity, scope of operations, and risk profile. Boards need to be aware of their own strengths and weaknesses, and to ensure that directors bring an appropriately diverse range of skills, knowledge, experience, and perspective. Significant events, such as an unexpected loss or compliance failure, should cause boards to reflect and reassess their structure, composition, and processes. An effective board takes a preventative approach and engages in probing self-assessments regularly and systematically."

But, while many boards aim to follow these guidelines (or similar frameworks), it's often easier said than done. Below, we've listed three best practices for boards of directors to help achieve these attributes. We additionally outline what potential influences following these practices could have on your institution's business functionality and growth.

Best practice:

Increasing board diversity

How it might help:

Keeping employees engaged and committed; keeping shareholders happy by showing commitment to input and requests; better board oversight; more ethical behavior; better returns and more growth

/ demographic diversity

While there is a positive trend toward more inclusion of women and minority board members, a December 2017 article from Harvard Law asserts that this evolution may be happening too slowly. Despite the change in new director appointment trends, 48 percent of boards in the study added no directors and low board turnover continues to impede momentum toward more inclusive compositions of U.S. boardrooms. Today approximately 22 percent of all directors are women, up only slightly since 2016, and minority representation at top firms is low. Only 17 percent of directors of the top firms are male or female minorities, and the percentage has not significantly changed over the past five to 10 years.

In addition to the implications these numbers hold for overall gender and racial equality, studies also suggest that this non-inclusive structure can actually be detrimental to a firm's overall success. According to a 2015 report from a US-based financial index provider, firms with a strong-female influence — defined as having three or more female directors, or a female CEO and another female director — on their boards performed 36 percent better in terms of return on equity than those that didn't. Those firms had a 10.1 percent return on equity.

The findings continue, with studies showing a connection between boards with gender diversity and better corporate governance and board oversight, less unethical behavior and fewer instances of fraud.

Additionally, boards with a higher percentage of women have better attendance records and women are more likely to sit on monitoring-related committees. One study even showed that more diverse boards are more likely to hold CEOs accountable for poor stock price performance.

/ social trends

In addition to the tangible business-related benefits of a more diverse board, it is also important to note that a proven commitment to diversity is in line with growing social demands. In November 2017, a Maryland-based proxy advisory group recommended that shareholders withhold votes from companies' nominating committee chairpersons, or board chairpersons, in cases where a company has no female directors and no formal diversity policy. The company says that this change reflects growing demand from institutional investors and regulators alike for such initiatives.

/ enhancing employee engagement

Proving a commitment to diversity also has beneficial effect within an institution's culture, and therefore for an institution's success. A global survey of more than 50,000 employees found that employees' commitment to their managers was a critical factor in engagement; one managerial characteristic most cited for effective engagement was "shows strong commitment to diversity." Since managers are an important link between employees and the organization, there can be a significantly positive impact of a trickle-down effect when a board decides to exemplify this commitment to diversity. Employees who are engaged consistently perform better, and one study showed that when LGBTQ communities feel supported from the top, through company diversity policies, all employees perform better.

Best practice:

Reviewing policies for board turnover and appointment; and redefining "conflicts of interest"

How it might help:

Separation of duties; director independence; making shareholders happier and avoiding activist investors

/ mandated board turnover

It is important for an institution to review its mandated turnover policies. While regulators, rating firms and other interested parties show a difference of opinions on tenure limits, age limits and other factors that would produce forced board turnover, the most critical safeguard for an institution is proof that the board reviews and updates these policies regularly.

/ independent directors

When seeking new board members, it is important to also strive for experiential diversity. Having directors both associated with the institution and not, and both experienced in the particular industry and not, is beneficial for institutions.

The impact of independent directors on a firm's board has been widely studied and is often accepted as best practice:

- A 2010 study of 266 companies listed on the Shanghai stock exchange found firms whose board has a higher percentage of independent directors or a lower percentage of "parent" directors (i.e., directors who are representatives of the parent companies of the listed firms) are less likely to engage in transfer pricing manipulations.
- A 2011 study found, using local director pools as an instrument for board independence, that among small and mid-sized firms, board independence has a positive effect on firm value and operating performance and CEO fraction of incentive-based pay and turnover.

Additionally, some regulators have commented on the benefits of director independences, with the OCC's *Director's Book* stating, "Independent directors bring experiences from their fields of expertise. These experiences provide perspective and objectivity because independent directors oversee bank operations and evaluate management recommendations. This mix of inside and outside directors promotes arms-length oversight. A board that is subject to excessive management influence may not be able to effectively fulfill its fiduciary and oversight responsibilities."

/ concern over conflicts of interest

While having independent directors is beneficial to a board's composition, it must also be noted that a multitude of external factors has made rapid changes in strategic focus common for all types of institutions — therefore, conflicts of interest for independent directors is difficult to predict. Companies are expanding the types of services and products they offer consumers; the lines between which "industry" a firm belongs to become blurred; and determining whether or not an independent director's other business endeavors will become conflicts of interest becomes increasingly difficult.

In January, two prominent executives and board members of an entertainment giant stepped down from the board for potential conflicts of interest. Though both of the former directors work in the tech industry, the quick evolution of business comprisal in today's market means a successful board must constantly reassess concepts of "competition" and reevaluate conflict of interest policies.

With a holistic approach, conflicts can be particularly challenging to avoid; it may be necessary to revise the types of information directors are required to disclose so that the board may highlight and track more relevant conflicts. Adjusting the conflicts of interest policy to reflect potential disruption from all relevant officers' and directors' companies, and ensuring proactive coordination between committees responsible for conflict identification and director independence enforcement, can mitigate the threats of these types of business overlap or interference.

/ ensuring shareholder mutualism

When looking to fill board positions, it is also important to take note of shareholder expectations. The consequences of ignoring this input can be severe. Earlier this year, a Delaware court ordered a southern bank to pay a six-figure sum to an activist investor who claimed the bank tried to prevent opposing director nominations, forcing the bank to restate its fourth-quarter results, lowering the profit by seven cents per share. A lack of communication and understanding between a board and its shareholders can be detrimental not just when nominating new leadership, but throughout the lifecycle of the governance relationship.

In a speech SEC Commissioner Kara Stein gave on February 13, 2018, she emphasized the importance of shareholders, stating, "the entire corporate ecosystem's success actually rests on effective communication and collaboration between corporations and their shareholders. When a company, its management, its shareholders, and its employees work together, companies tend to be more resilient and prosperous. In turn, this benefits companies, their corporate stakeholders, and the economy as a whole."

This call for director-shareholder communication reinforces that shareholder engagement is critical to the overall well-being of the firm. It may be prudent for boards to self-reflect and pursue opinions and perspectives outside of what management provides. Boards should consider their competition, noting differences between the institution's own operational and governance policies and those of their peers. These discrepancies may be reflective of weaknesses or strengths, and the board should asses these issues to better educate shareholders on the institution's standing. Boards that proactively provide shareholders with this type of valuable perspective may be less likely to be caught off-guard by activists or proxy votes. It is also likely that significant, long-term shareholders will show support when institutions prove their ability to assess their own industry standings. This process should be a conversation, with mutualism between both parties held as a foremost goal. A shareholder liaison committee may be a valuable instrument, and some firms have already begun utilizing such methods.

/ enhancing shareholder communication

There have been some initiatives in the industry to help boards and shareholders better engage. For example, the Shareholder-Director Exchange (SDX) working group, which includes issuer and investor representatives, began researching and advising on shareholder-director engagement in the fall of 2013. SDX published a 10-point guide for appropriate engagement between public company boards and shareholders to provide suggestions for meaningful and mutually beneficial engagement.

Some companies are using new technologies to help better engage shareholders. These practices range from CEO video messages to social media. Another practice some companies use is providing easy-to-digest summaries of board meetings, whether or not the content is controversial. An advantage of using such technologies is being able to link what an institution sends out to automated analytics. Institutions may then be able to combine this with historical voting trends to garner a better understanding of how shareholders may respond to issues before the votes come in.

Best practice:

Review board committees

How it might help:

Decreases overlap of responsibilities; increases efficient time management; avoids detrimental innovation-based business disruption; enhances support across all aspects of business functionality; mitigates exposure to certain risks

/ deciding where to focus

A common problem for many boards is deciding which areas require focus. Often, there is overlap when an issue falls into the jurisdiction of multiple committees. Sometimes, important issues are overlooked when no committee claims them. It is best practice to not only review which issues are delegated to which committee, but also to review if the board comprises the most efficient, effective committees for its particular risks and growth goals. Below, we provide some suggestions to complement the more common (and still necessary) committees such as audit and nominating.

If a board decides not to create committees or subcommittees in these areas, it is critical the directors stay abreast of changes and trends within these areas that could affect business operations, clients, employees or other aspects of institutional functionality. These issues should be repeat agenda items, and board communication surrounding these subjects (with senior management, appropriate information providers, employees, clients, third-party partners and any other relevant parties) should reflect and spur ongoing updates to a written plan for each area. Understanding and overseeing these aspects of an institution's operation will be crucial for the institution's risk management and business successes.

Serious issues that may require creating board-level committees or subcommittees include:

/ Social and Environmental Issues

/ social issues and sexual harassment

With the current social climate surrounding ethical misconduct in the workplace, at the forefront of which is the multitude of recent sexual harassment allegations, many institutions are wondering what they can do to protect their employees, associated parties and themselves. Creating an ethics committee will not only provide an institution the opportunity to create clear standards and guidelines around these issues, but also help with "tone from the top." According to the OCC's *Director's Book*, establishing an "appropriate corporate culture" is a key board responsibility, and in the wake of recent troubling allegations, creating a corporate culture that disallows inappropriate behavior and mitigates employee misconduct should be a top priority for institutions.

According to a 2017 survey that polled directors from both public and private companies of varying sizes, despite recent events, 77 percent of boards had not discussed accusations of sexually inappropriate behavior and/or sexism in the workplace; 88 percent had not implemented a plan of action to mitigate or address these issues; and 83 percent had not reevaluated the company's risks regarding sexual harassment or sexist behavior at the workplace. Among the most commonly cited reasons for not addressing these topics was the perception that these matters were not a problem in the company; but, the data shows that sexual harassment and gender-based ethical misconduct permeates all industries.

A recent blog post from Harvard Law asserts that boards should be far more proactive in their approach to these types of sensitive issues, and outlines a series of steps boards may take to stay informed and ensure accountability in this complex area. Likewise, a recent article from National Law Review provided advice to boards hoping to be more attentive to this trending and critical topic. With the idea of "tone from the top" at the forefront of these discussions, the suggestions for board action included:

- Reviewing institutional policies and procedures regarding sexual harassment or assault allegations
- Asking for briefings on employee training and protocols for preventing, reporting and addressing sexual misconduct
- Considering what role the board plays in oversight, including an understanding of what criteria determines a certain incident be escalated to board notification
- Discussing with the appropriate legal counsel the litigation risk, disclosure requirements and the attorney-client privilege the area entails
- Improving hotline and other reporting functions and vertical reporting mechanisms
- Analyzing relevant aspects of risk management, particularly with respect to any situations that involve senior leadership, repeat offenders or a pattern of complaints; potentially conducting a confidential internal review of prior allegations
- Developing a crisis response plan that includes human resources, public relations and legal counsel

/ environmental issues

In addition to these types of social trends, another hot-topic issue is environmental policy. An institution that stays abreast of environmental trends safeguards itself not only from potential detrimental environmental changes, but also from the social consequences of being behind the times.

For example, institutional investors have shown an interest in understanding institutions' environmental policies and impacts. Earlier this year, a proxy advisory firm announced its launch of an environmental, social and governance QualityScore calculator that will rate institutions' environmental disclosures "based on multistakeholder initiatives" and standards of applicable climate-related groups. The environmental analysis will consider disclosures related to factors such as waste and toxicity, carbon and climate and the firm explains that the launch spurs from increasing demand for these disclosures from institutional investors.

Another type of risk a financial institution faces in approaching environmental issues is how these issues may affect the institution's ratings. A recent blog post from a credit rating giant outlined how environmental risks and opportunities can affect a firm's ability to meet its financial obligations, and therefore how the agency incorporates these considerations into its ratings methodology and analytics. The agency found that between July 2015 and August 2017, environmental and climate concerns affected corporate ratings in 717 cases (approximately 10 percent of corporate ratings assessments), and resulted impacted a firm's rating in 106 cases.

/ Business Disruption

With the potential for business disruption becoming more daunting as technology and businesses develop, it is critical that boards stay proactive in their approach to safeguarding their institutions. Some studies show that boards with independent directors can predict disruptions, but a National Law Review article specifically discussing innovation-based business disruption shows that this ability must be supported by a strong communication and partnership between an institution's board and its management: "An effective response to innovation-based business disruption [exists when] the board encourages management to identify business disruption threats and to develop responsive strategies, and then monitors the evolution of such strategies. Management, on the other hand, informs the board as to the nature and source of disruption threats, implements a responsive plan, and supports the board's ability to monitor the success of that plan." This structure suggests that board focus on managing business disruptions is an inherent aspect of governance practices and the obligation to ensure long-term business progression.

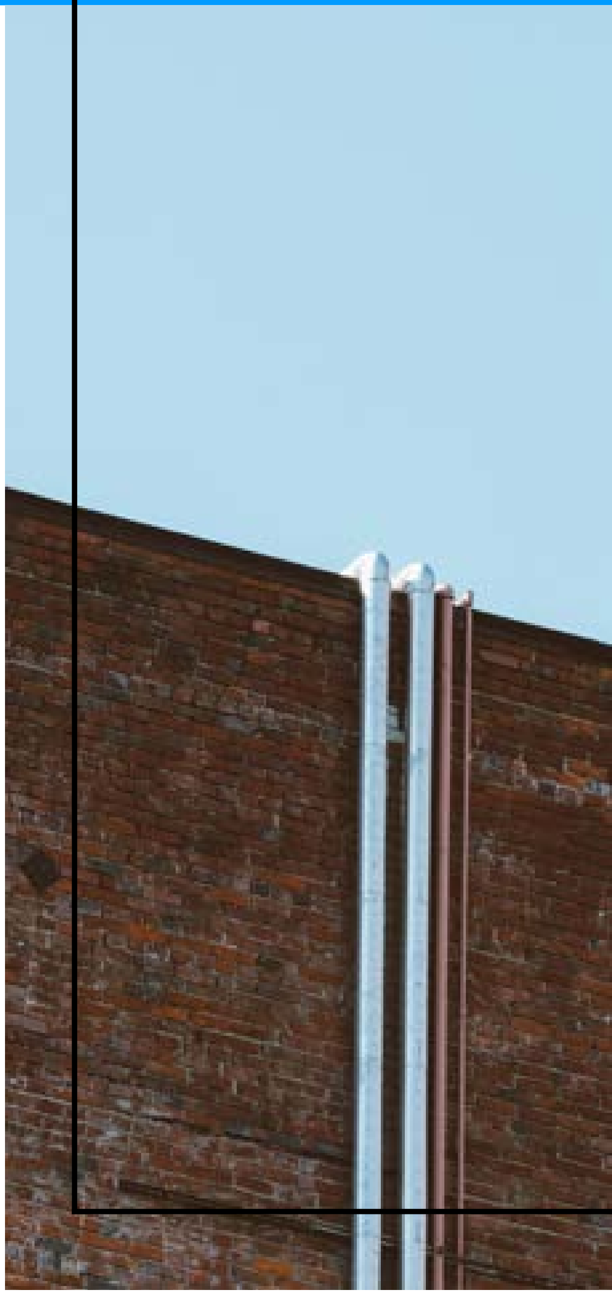
/ IT and Cybersecurity

According to a report in the Wall Street Journal, only four Fortune 100 companies have board committees dedicated to information technology (IT) risks and strategies, and it is often left to the audit committee to take on this aspect of operations risk. With cybersecurity guidance such as the SEC's new cybersecurity interpretive guidance (released February 21, 2018) focusing on oversight responsibilities as a key aspect of cyber risk management, it is imperative that this issue have appropriate owners. If an institution decides against creating a specific committee, it is critical that the chief information security officer or any other associated experts (including, in some cases, trusted third parties) continue to clearly and consistently update, educate and prepare the board for the rapid changes in this field.

The SEC guidance not only outlines cybersecurity in terms of network threats and vulnerabilities, but also as a main component of enterprise risk management, and potentially corporate governance. The guidance portrays a system in which officers and directors are ultimately and immediately responsible for program development and oversight responsibilities. This requires that directors are knowledgeable and up-to-date regarding cybersecurity risk and that they prioritize cybersecurity oversight. ❖

BUSINESS CONTINUITY PLANNING:
HOW TO ENSURE YOUR INSTITUTION IS PREPARED

In January, the Hawaii Emergency Management Agency sent out an emergency notification that a ballistic missile threat was inbound to Hawaii. Minutes later, the notification was confirmed to be a false alarm.



This event is a a wake-up call for institutions, and reinforces the need to shore up business continuity plans (BCPs). Communication with internal and external members of an institution regarding disaster, and the policies and procedures of how businesses deal with disaster, is unfortunately becoming more and more important every day. Having an underdeveloped plan, distributing disaster messages in error or not properly training staff on disaster protocol can significantly impact an institution's ability to recover.

A business continuity strategy should incorporate a financial institution's short-term and long-term goals and objectives. When developing or amending a business continuity strategy, financial institutions have many considerations, from personnel to communication, all the way to setting aside proper funds for potential disasters.

Short-term goals are more tangible. These include an institution's ability to:

- mitigate problems
- designate critical personnel and infrastructure
- recognize the resources required for recovery

Long-term goals focus on more nebulous aspects of the BCP, like:

- budgetary considerations
- an enterprise-wide strategic plan
- supervision of third-party resources

Regardless, an institution should update its BCP at least annually or after significant changes to business operations, or if there are gaps or shortcomings revealed through training or testing.

Personnel

An institution needs clear and defined tasks when it comes to personnel. By identifying which employees are integral to the BCP, an institution and its employee will be more prepared, which can shorten the recovery window. If this is not all identified beforehand, altering a policy during a triggering event can be even more difficult.

In preparing for these events, is the institution hosting, at a minimum, annual emergency trainings to make sure identified personnel know their overall role in the recovery process?

A well-trained staff is more likely to remain calm during an emergency, which can minimize the negative effects of a triggering event. There should be cross-training of personnel and sufficient designation of back-up personnel throughout the entire organization.

If someone can't be reached, is there a succession plan?

Does the person identified know they are part of the succession plan? Financial institutions also need to establish what their plan is if an employee is unable or unwilling to return to work due to extenuating circumstances.

If there is substantial damage, what type of accommodations will displaced staff members require?

Is there a plan to shift employees to a different corporate site, branch, back-up location or other facility outside of the disaster area? Is the institution prepared to provide basic necessities, including transportation, prior to a disruptive event?

If there is an emergency lodging program in place, has management accounted for the business needs of the employees, like a secure internet connection, if required?

The institution should identify a recovery team to help displaced employees get up and running at their new location on recovered predefined critical business functions. The better financial institutions treat their employees, the more likely those employees contribute and commit to recovery operations when faced with a disruptive event.

Communication

"Communication" in relation to a BCP covers communication with:

- Employees
- Emergency personnel
- Regulators
- Vendors and suppliers
- Customers
- Media

When communicating with employees about a pending disaster and specific evacuation instructions, is prompt notification guaranteed?

As the most important activity, an institution should include this plan in the BCP. Communication should reach all employees, including those in isolated areas and management should be aware of each employee's evacuation plans.

Does the institution still utilize a manual telephone calling tree or has it switched to an emergency notification system?

The Federal Financial Institutions Examination Council (FFIEC) Appendix G states "emergency notification systems should be evaluated to determine their cost effectiveness." However, whatever system an institution utilizes will be ineffective if the institution does not make sure it has accurate contact information for all employees. Oftentimes, employees are not proactive with changing their addresses when they move, and may only make updates if contact information on file with their employer is incorrect and results in negative personal consequences.

There are certain ways a financial institution can improve its employee notification, including some of the following:

- Two-way polling phone system for confirming contact and message delivery
- Providing remote access to employees, including security measures like virtual private networks (VPNs)
- An ultra-forward service that allows incoming calls to be rerouted to a predetermined alternate location

Has the financial institution incorporated external communication into its BCP?

While the need to plan for emergency messaging to personnel is apparent, a strong BCP will also allow an institution to facilitate conference calls and meetings between financial sector trade associations, financial authority working groups, emergency response groups and international exchange organizations to help with the recovery process. Determining the impact and operational disruptions across an institution's regionalized industry is important.

Technology

As the potential for technology allows financial institutions to innovate and reach customers in different ways, an institution's technology reliance has grown into a dependence.

When a disruptive event takes place, is there a strong understanding of what is considered "critical business unit data"?

The institution can store this information in physical places like individual workstations, back-up servers or the cloud, if the institution has made the investment. Regardless, disrupting events highlight the importance of information backup, back-up schedules and storage of vital records.

Do employees understand their ability to work on personal computers after a disrupting event if they do not have a work-issued laptop or do not have access to something similar to a VPN?

Further, when identifying "critical" and "non-critical assets," an institution should pay attention to how they label their mobile, internet and telephone banking tools, as well as email capabilities. In the event of a disruption, an institution's access to automated-teller systems may be limited, and using telecommunications to access bank accounts may become paramount.

Data Recovery Facilities

The FFIEC handbook also emphasizes the importance of financial institutions for "formal arrangements for alternate processing capability in the event that their data processing site becomes inoperable or inaccessible."

Has the institution considered expectations based on its size and complexity, and its impact on the overall financial system?

An institution that is considered critical to the overall functioning of the financial system may need to have same-day business resumption, however there may be circumstances allowing other financial institutions to respond less quickly.

There are a number of different back-up recovery facility models. Some of the models include:

- Hot Sites: a site fully configured with compatible computer equipment that can usually become operational within hours
- Cold Sites: provides a backup location without equipment, but with power, air conditioning, heat, electrical, network and telephone wiring
- Warm Sites: a mix of a hot site and cold sites, usually stocked with computers and external communication links. Will require more work, including potentially delivering certain workstations and restoring data.
- Duplicate Facilities/Split Operations: two or more sites provide inherent backup to one another
- Tertiary Location: a "backup to the backup"

Other Considerations

As touched upon in the previous section, with an increased reliance on access to payments electronically, disrupting events can make those systems inoperable. ATMs rely on mainframe systems to help validate withdrawal requests. Additionally, a disrupting event could impact electronic funds transfers systems; financial institutions should consider pre-established withdrawal limits for customers and alternative solutions, including sending payments to correspondent banks.

Has the institution considered which of its automated tasks could be performed manually if systems are inoperable?

The BCP should outline things such as what duties employees can fulfill, the distribution of hard copy documents and reconciling general ledger accounts once systems are operational. ❖

ABOUT CAPCO

Capco is a global business and technology consultancy dedicated to the financial services industry, plus a dedicated energy division. Capco delivers innovative solutions in Banking & Payments, Capital Markets and Wealth & Asset Management, designed to withstand market forces, continual regulatory change and increasing consumer demand.

WORLDWIDE OFFICES

Bangalore	Hong Kong	Singapore
Bratislava	Houston	Stockholm
Brussels	Kuala Lumpur	Toronto
Chicago	London	Vienna
Dallas	New York	Warsaw
Dusseldorf	Orlando	Washington, DC
Edinburgh	Paris	Zurich
Frankfurt	Pune	
Geneva	São Paulo	

CONTACT US

Capco Center of Regulatory Intelligence
1101 Pennsylvania Ave., NW Suite 300
Washington, DC 20004
E: capco.cri@capco.com
P: 202.756.2263

@CAPCO

WWW.CAPCO.COM

CAPCO