June 2015

A closer look

A publication of PwC's financial services regulatory practice

Outsourcing: How cyber resilient are you?

Overview

Cyber attacks on financial institutions continue to increase, both in number and impact. While the industry's defenses against cyber criminals have been improving, recent high-profile breaches indicate that many cyber risk areas remain under addressed.

Regulators are particularly concerned that the industry's third-party service providers are a weak link that cyber attackers can exploit.[1] Financial institutions have become increasingly reliant on the information technology (IT) services these providers offer, either directly through the outsourcing of IT or indirectly through outsourced business processes that heavily rely on IT (e.g., loan servicing, collections, and payments).[2] Regardless, banks remain ultimately responsible – they own their service providers' cyber risks.

Therefore, addressing cyber resiliency as part of their third-party risk management program (TPRM) has become especially critical for financial institutions. Although regulators' recent industry surveys and reports indicate that institutions have made some progress in this area, the reports make it clear that more needs to be done.[3]

To facilitate the industry's efforts, the Federal Financial Institutions Examination Council (FFIEC) and FINRA issued third-party cyber risk management guidance this year.[4] The key message is that they expect financial institutions to heavily consider third-parties in their cyber resiliency framework, including reviewing their third-parties' cyber risk management efforts. Institutions must be able to withstand cyber attacks as well as be able to demonstrate the ability to recover from an attack and resume normal operations quickly. It's not just about prevention – firms should assume that breaches will happen.

The race to resiliency is hard, especially in the context of outsourced operations, and it will continue to get harder. Despite the challenge, however, entering the race is no longer an option.

This **A closer look** provides background regarding the industry's state of third-party cyber risk management, analyzes recent regulatory guidance, and offers our view of six actions institutions should be taking now to become cyber resilient.

---

[1] See PwC's *A closer look*, *Cyber: Think risk, not IT* (April 2015) for an overview of regulators' cyber concerns and issuances.

[2] These services can be fully or partially outsourced.

[3] This year alone, three prominent regulators have surveyed and reported on the industry's cyber risk practices: the Financial Industry Regulatory Authority (FINRA) in February, the Securities and Exchange Commission (SEC) in February, and the New York Department of Financial Services (DFS) in April.

pwc

Background

The recent trend of successful cyber attacks against both public and private entities in the US shows that despite millions of dollars spent on enhancements, cyber risk management continues to suffer from a significant gap between threat and preparedness. It is critical that financial institutions close this gap because:

- Financial institutions are highly desirable targets for cyber criminals, who have access to increasingly sophisticated tools at ever lower costs; and
- The use of cyber attacks has become a weapon in cross-border commercial or political disputes, with state-sponsored hackers having virtually unlimited resources targeting US financial institutions.

Cyber criminals often attack institutions through their third-party service provides. These service providers are often rich in the types of data cyber criminals seek (e.g., client financial information used in payment processing), and usually provide an easier target than the financial institution itself.

In April, a report by the DFS found that although nearly all of the 40 surveyed banks had policies and procedures that required reviews of third-party cyber security practices, less than 50% of the banks required any on-site assessment of the third-party.[5] The report also found that 79% of the surveyed banks required their vendors to establish minimum information security measures, but only 36% extended this requirement to the vendor's subcontractors as well.

Similar themes were noted by the SEC in its report issued in February, which was based on a survey of 57 registered broker-dealers and 49 registered investment advisors. The SEC observed a number of areas for further improvement especially among investment advisors, including periodic vendor risk assessments (which are currently undertaken by only 32% of surveyed advisors), and contractual provision around vendor cybersecurity practices (currently utilized by only 24% of surveyed advisors).

TPRM cyber guidance

In an effort to improve upon the results of the SEC and DFS reports, issuances from the FFIEC[6] and FINRA provide third-party cyber guidance with a focus on resilience (i.e., the ability to withstand and recover from a cyber attack). Consistent with the regulators' overall approach to cybersecurity, the guidance suggests an approach that is more advisory than enforcement-oriented and is principles-based rather than prescriptive. A prescriptive approach would make less sense at this stage, as cyber risks are evolving rapidly and financial institutions each have idiosyncratic exposures based on the particularities of the institution.

FFIEC

The FFIEC's guidance discusses strengthening the resilience of financial institutions' outsourced technology services, and was issued last February as part of the new "Appendix J" to the FFIEC's Business Continuity Planning IT Handbook. It addresses third-party cyber risk management in the context of business continuity planning (BCP), so it communicates the expectation that a financial institution should be able to recover critical systems and resume normal operations following a cyber attack (among other adverse situations) relatively quickly, regardless of whether the IT systems are in-house or outsourced.

To that end, the Appendix recommends that financial institutions incorporate their third-party cyber risks into their existing TPRM program and address those risks throughout the duration of the third-party relationship. This includes planning, pre-contract due diligence, contract negotiations (e.g., including contractual provisions that allow the institution to exercise necessary controls such as the testing of the third-party's systems), ongoing monitoring of the third-party, and plans for terminating/transitioning third-party relationships.

The financial institution's TPRM programs should address the institution-specific risks arising from the interconnectedness between the institution and the third-parties to which they have outsourced various activities. As a result of this interconnectedness, and the resulting concentration of some outsourced technology functions in a relatively small number of service providers, a significant breach at a major third-party can affect many institutions at once. This would be a disruption across firms and could overwhelm possible third-party outsourcing alternatives. Moreover, because of the high degree of dependence on IT to perform basic

[4] These issuances are generally consistent with previous regulatory issuances on third-party risk management. See PwC's *Viewpoint, Significant others: How financial firms can manage third party risk* (May 2015); *Regulatory brief, More third-party guidance: When should you just do it yourself?* (December 2013); and *Regulatory brief, Managing third-party relationships: It's complicated* (November 2013).

[5] This report followed the DFS's examination guidelines issued last December which emphasized third-party cyber risk management in addition to the governance and monitoring/testing of banks' cyber defenses. See note 1 for more information.

[6] The FFIEC is a regulatory council composed of the Federal Reserve Board, Office of the Comptroller of the Currency, Federal Deposit Insurance Corporation, Consumer Financial Protection Bureau, and the National Credit Union Administration.

operations, it is no longer feasible for financial institutions to operate manually on an interim basis.

The Appendix also emphasizes the importance of systems testing with third-parties to ensure that critical services can be restored in the event of a widespread disruption at the institution, its third-party service provider, or both (e.g., in case of simultaneous cyber attacks). In the case of a third-party providing services to a large number of financial institutions, accomplishing sufficient testing will be challenging.

In addition, the Appendix recommends that financial institutions, and by extension their third-party service providers, address cyber resilience by having:

- Data architecture and technology that minimize the potential for data loss or corruption
- Data integrity controls
- Multiple, independent communications service providers
- A layered anti-malware strategy[7]
- Increased awareness of potential insider threats
- Enhanced incident response plans reflecting the current threat landscape
- Prearranged third-party forensic and incident management services

Finally, as a part of incorporating the threat of cyber attacks into their BCP planning, the Appendix recommends that institutions also include a framework for responding to such incidents when they occur.

FINRA

FINRA's guidance was issued as part of its report on cybersecurity practices of surveyed broker-dealers last February. Similar to the FFIEC's guidance, the FINRA issuance highlights the significance of managing cyber risk throughout the life cycle of third-party relationship. Examples FINRA provides include performing pre-contract and ongoing due diligence on third-parties, considering third-party relationships and outsourced systems as part of the firm's ongoing risk assessment process, and implementing procedures to terminate third-party's access to firm systems immediately upon contract termination.

[7] A strategy that implements security measures at multiple levels, e.g., application, internal network, and gateway.

Six things to do now

Given the increasing impact of successful cyber attacks, and the regulatory emphasis on third-party risk management and resilience, financial institutions should already be taking at least some of the following six actions:

1. **Identify and assess sources of third-party cyber risk.** As part of their TPRM programs, financial institutions should identify and assess risks (and related controls) arising from both direct outsourcing of IT services and indirect outsourcing that is incidental to an IT-reliant outsourced function (e.g., loan servicing). IT risk from services that are subcontracted by a third-party to other third-parties should also be included. However, the reality is that some insitutions will have thousands of outsourced and subcontracted services, so risk-based prioritization will be needed.
2. **Address cyber risk and resiliency throughout the entire third-party relationship lifecycle.** A strong TPRM program should address cyber risks and resiliency across the full lifecycle of the third-party relationship, including the planning, due diligence, contracting, monitoring, and termination phases. This means both identifying and addressing direct and indirect exposures to third-party cyber risk and resiliency issues within each phase of each relevant third-party relationship.
3. **Emphasize cyber resilience as part of business continuity plans.** Similar to money laundering or sanctions risks, motivated criminals will continue to try to find ways to circumvent any protections that financial institutions put into place. Therefore, it is imperative that financial institutions not only try to prevent cyber attacks, but also be prepared to deal with the impact of successful attacks. An insitution's BCPs should anticipate the potential harm of successful cyber attacks on the institution, its related third-parties, and its customers. Sources of threats to consider include malware, insider threats, data or systems destruction/corruption, and communications infrastructure disruption.
4. **Understand IT interconnectedness and dependencies.** As the FFIEC guidance emphasized, the interconnectedness and interdependencies between financial institutions and third-parties could create significant risk by overwhelming service providers that a large number of institutions would use as an alternative to an incapacitated primary service provider. Thus, it is important that firms fully understand their exposure to such interdependencies and plan accordingly (e.g., by having arrangements in place for multiple third-party alternatives).

5. **Perform appropriate resilience testing.** Although it is important for financial institutions to identify cyber risks and create plans to mitigate them, mere planning is not enough. Institutions must supplement their planning with resilience testing that is sufficiently robust to demonstrate the ability of the institution and its third-parties to continue operations should a cyber event occur. Institutions should proactively work with their third-party sources of cyber risk to develop acceptable protocols for testing.

6. **Integrate cyber risk expertise into the TPRM program.** A risk-based TPRM program that is designed to address cyber risk must be informed by the same analysis, regulatory guidance, and information that are used to manage the institution's cyber risk generally. Thus, it is important that financial institutions' TPRM program integrate the participation of subject matter specialists with cyber security expertise.

Additional information

For additional information about this **A closer look** or PwC's Financial Services Regulatory Practice, please contact:

Dan Ryan
Financial Services Advisory Leader
646 471 8488
daniel.ryan@us.pwc.com

Adam Gilbert
Financial Services Global Regulatory Leader
646 471 5806
adam.gilbert@us.pwc.com

Joseph Nocera
Financial Services Cybersecurity Leader
312 298 2745
joseph.nocera@us.pwc.com

Sean Joyce
Financial Crime Leader
703 918 3528
sean.joyce@us.pwc.com

Daniel Morrison
Director, Third Party Risk Management
602 206 3273
daniel.morrison@us.pwc.com

Armen Meyer
Director of Regulatory Strategy
646 531 4519
armen.meyer@us.pwc.com

Contributors: Bruce Oliver, Roozbeh Alavi, Garit Gemeinhardt, Amandeep Lamba, and Joe Walker.

To learn more about financial services regulation from your iPad or iPhone, click here to download PwC's new Regulatory Navigator App from the Apple App Store.

Follow us on Twitter @PwC_US_FinSrvcs