New York State
Department of Financial Services

Update on Cyber Security in the Banking Sector:
Third Party Service Providers

April 2015

Update on Cyber Security in Banking Sector: Third-Party Service Providers

I. Introduction

In May 2014, the New York State Department of Financial Services ("the Department") published a report titled "Report on Cyber Security in the Banking Sector" that described the findings of its survey of more than 150 banking organizations. The report specifically highlighted the industry's reliance on third-party service providers for critical banking functions as a continuing challenge. In light of the increasing number and sophistication of cyber attacks, including recent breaches at both banks and insurers, the Department is now considering, among other regulations, cyber security requirements for financial institutions that would apply to their relationships with third-party service providers.

In connection with that effort, the Department sent a letter in October 2014 to 40 regulated banking organizations requesting information about the practices currently in place surrounding the management of their third-party service providers. After reviewing the responses (which included relevant policies and procedures), the Department noted a number of common issues and concerns and has drafted this update to the May 2014 report to highlight the most critical observations.

The October 2014 letter asked for information about due diligence processes, policies and procedures governing relationships with third-party vendors, protections for safeguarding sensitive data, and protections against loss incurred due to third-party information security failures. For the purposes of this report, banking organizations have been categorized as "small" (assets < $100 billion), "medium" (assets between $100 and $1 trillion), and "large" (assets > $1 trillion).

Additionally, the Department asked each of the surveyed banking organizations to describe any steps it has taken to adhere to the Framework for Improving Critical Infrastructure Cybersecurity issued by the U.S. Commerce Department's National Institute of Standards and Technology ("NIST") on February 12, 2014 concerning third-party stakeholders. The NIST framework is generally viewed as a set of baseline principles for cybersecurity. Interestingly, while the overwhelming majority of the respondents stated that they had taken or were taking steps to incorporate NIST principles, the application of those principles may vary across institutions, described in more detail below.

II. Observations

A. Due Diligence Processes

The Department asked each banking organization to describe any due diligence processes used to evaluate the adequacy of information security practices of third-party service providers.

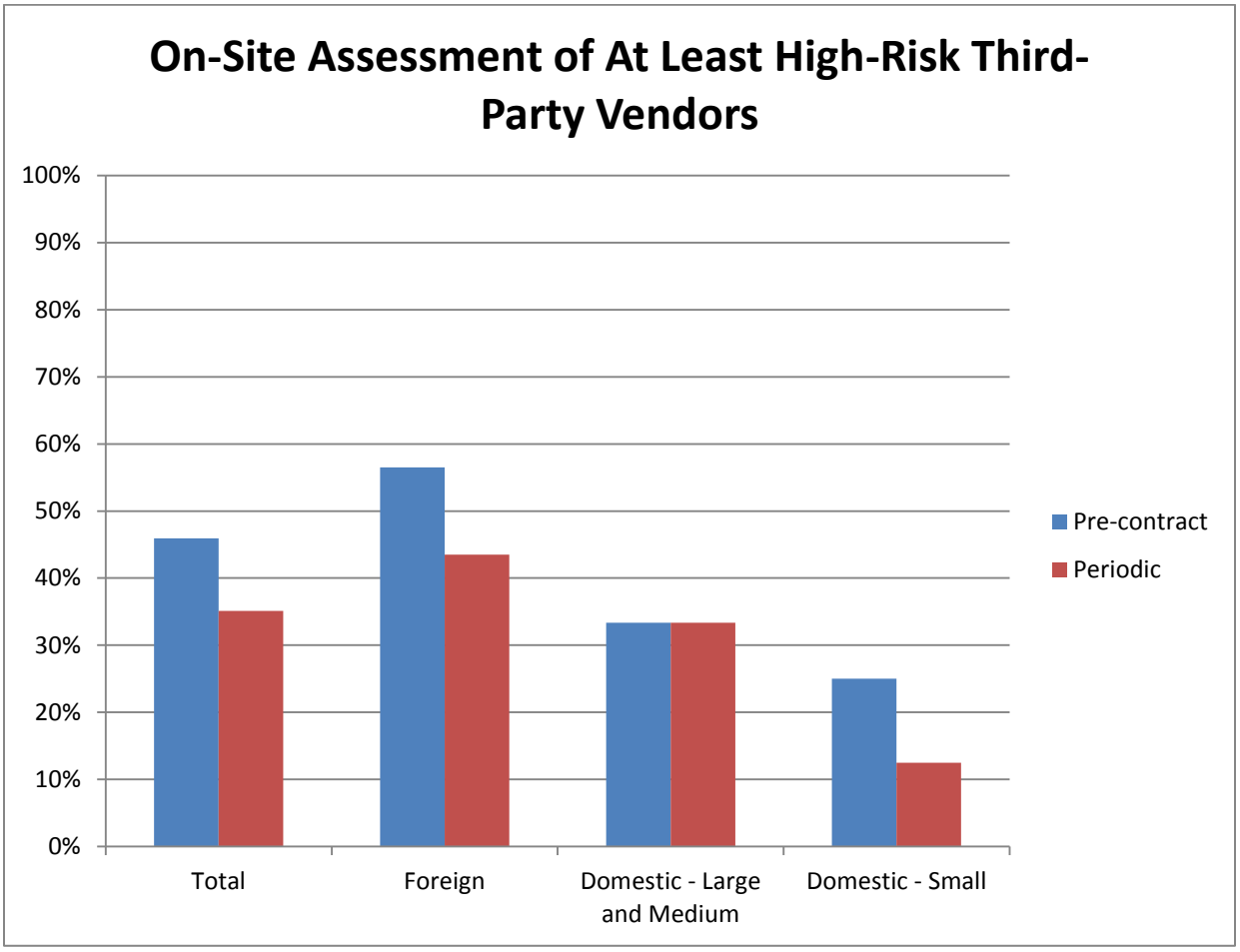
All but one of the surveyed banking organizations classify their third-party service providers by risk and 95% of the surveyed banking organizations conduct specific information security risk assessments of at least their high-risk vendors. Banking organizations typically classify any vendors with access to sensitive bank or customer data as high-risk, material, and/or critical.

Examples of third-party vendors that were classified as high-risk or material include check/payment processors, trading and settlement operations, and data processing companies. However, some banking organizations have exemptions from their customary due diligence for individual consultants and professional service providers (*e.g.*, legal counsel). Examples of third-party vendors that were classified as low-risk include providers of office supplies, printing services, food catering, and janitorial services.

Ninety percent of the banking organizations surveyed have information security requirements for their third-party vendors, although the nature and specificity of these requirements vary. Some large institutions set forth specific requirements, including data encryption, access controls, data classification, and business continuity and disaster recovery plans, while other institutions (both large and small) merely require compliance with more general information security standards.

While nearly all of the surveyed banking organizations have policies and procedures that require reviews of information security practices both during vendor selection and as part of their periodic review, fewer than half of the institutions surveyed require any on-site assessments of their third-party vendors, as illustrated in Table 1. Only 46% of the surveyed institutions are required to conduct pre-contract on-site assessments of at least high-risk third-party vendors, while only 35% are required to conduct periodic on-site assessments of at least high-risk third-party vendors.

TABLE 1



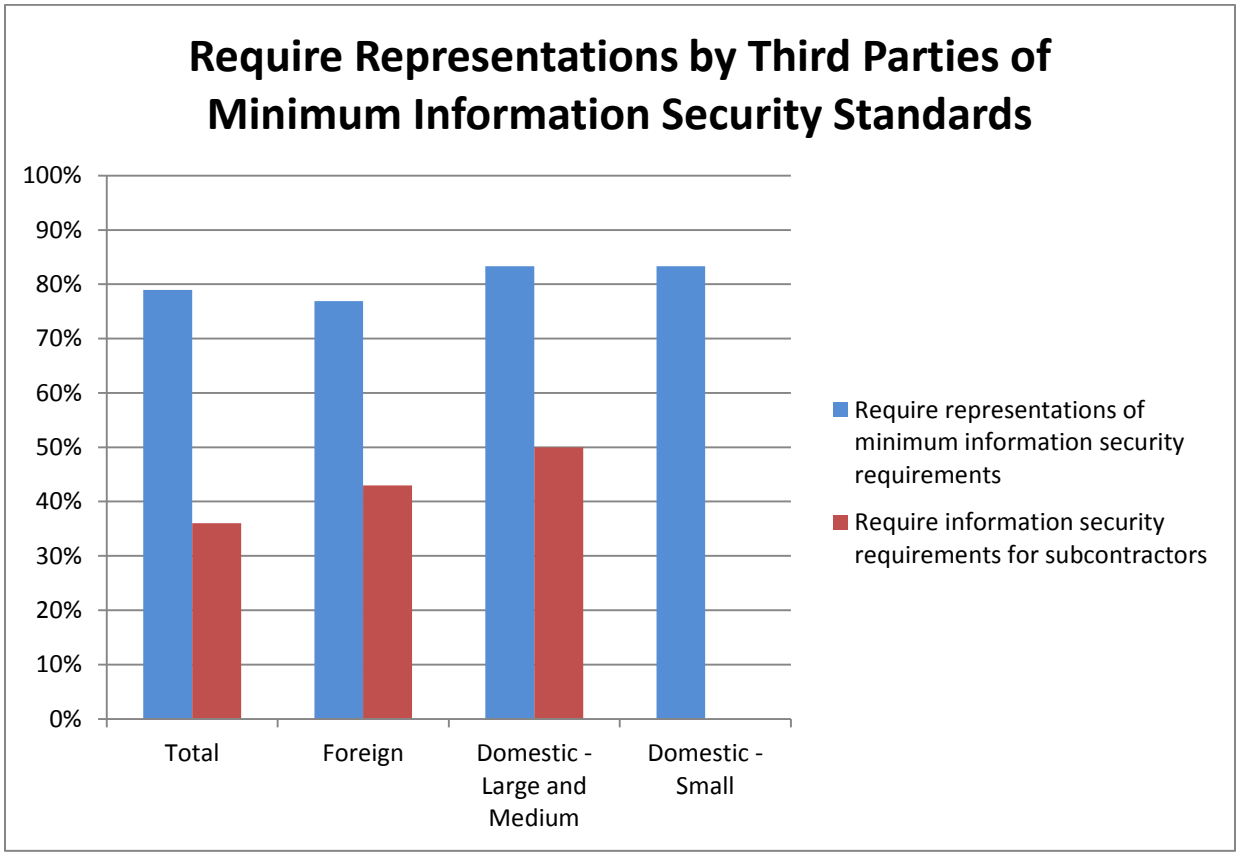
B. Policies and Procedures Governing Relationships with Third-Party Service Providers

The Department asked each banking organization to provide a copy of any policies and procedures governing relationships with third-party service providers that address information security risks, including setting minimum information security practices or requiring representations and warranties concerning information security.

All of the institutions surveyed have written vendor management policies, and all but three have written procedures for selecting third-party vendors. Most of these policies appear to have been written and/or updated within the last several years.

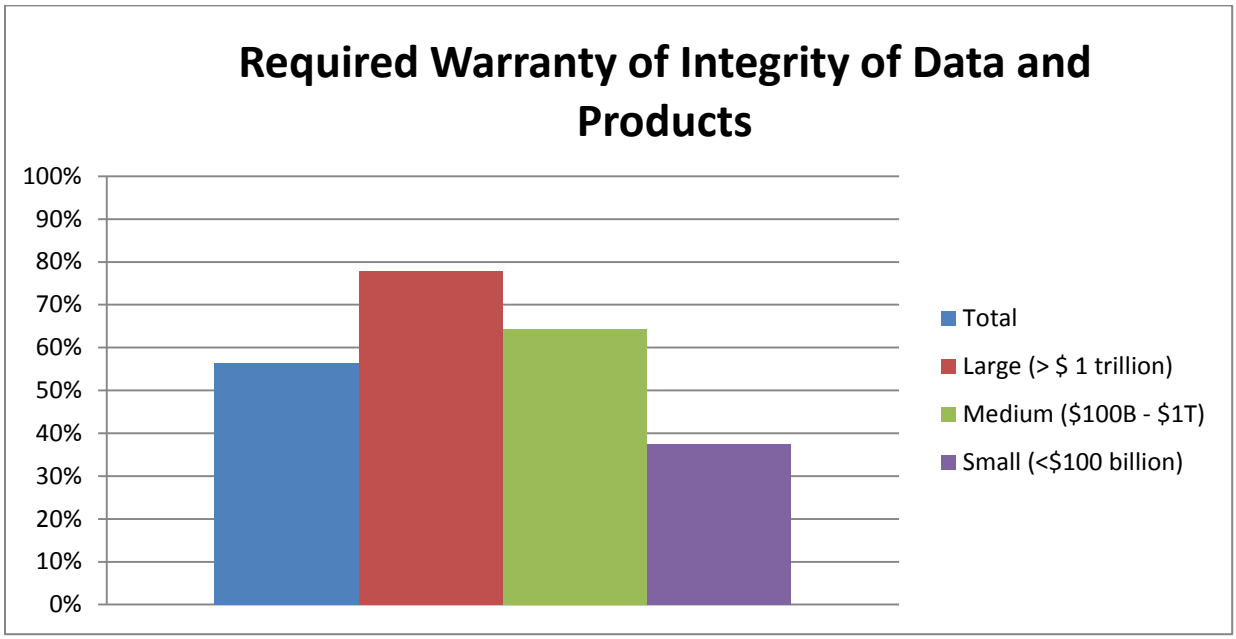
Most of the institutions surveyed require third-party vendors to represent that they have established minimum information security requirements, although 21% of them do not, as illustrated in Table 2. Only 36% of the surveyed banking organizations require those information security requirements to be extended to subcontractors of the third-party vendors.

TABLE 2



Most of the surveyed banking organizations require the right to audit their third party vendors, although 21% of them do not. Nearly half (44%) of the institutions do not require a warranty of the integrity of the third-party vendor's data or products (*e.g.*, that the data and products are free of viruses). Larger institutions are more likely to require such warranties than small and medium-size institutions, as illustrated in Table 3.

TABLE 3



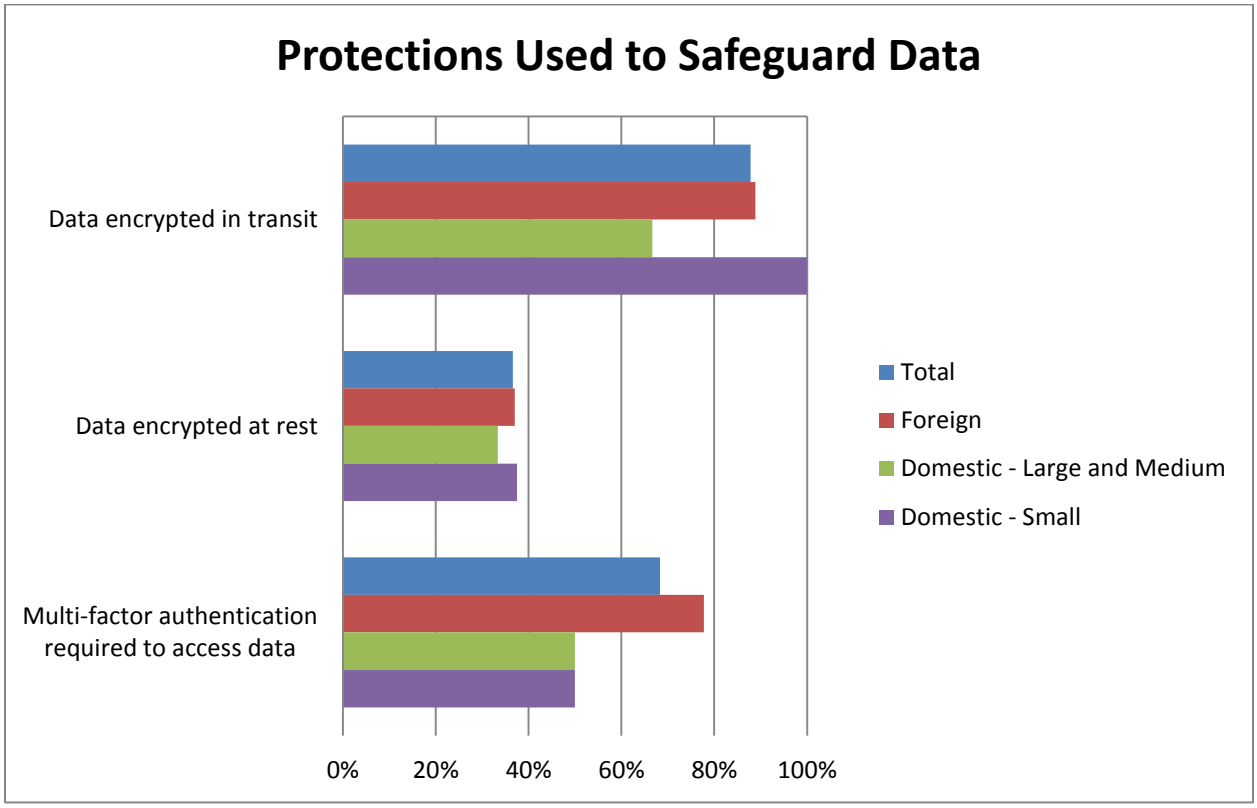
Thirty percent of the banking organizations surveyed do not appear to require their third-party vendors to notify them in the event of an information security breach or other cyber security breach.

C. Protections for Safeguarding Sensitive Data

The Department asked each institution to describe any protections used to safeguard sensitive data that is sent to, received from, or accessible to third-party service providers, such as encryption or multi-factor authentication.

Ninety percent of the surveyed banking organizations utilize encryption for any data transmitted to or from third parties. However, only 38% of the surveyed institutions (50% of large institutions) use encryption for data "at rest." Seventy percent of the surveyed institutions require multi-factor authentication ("MFA") for at least some third-party vendors to access sensitive data or systems. However, the surveyed foreign banks (primarily large institutions) require MFA much more than large or small domestic institutions. When used, MFA is primarily required for third-party vendors that remotely access sensitive data or banking systems, either on computers or portable devices.

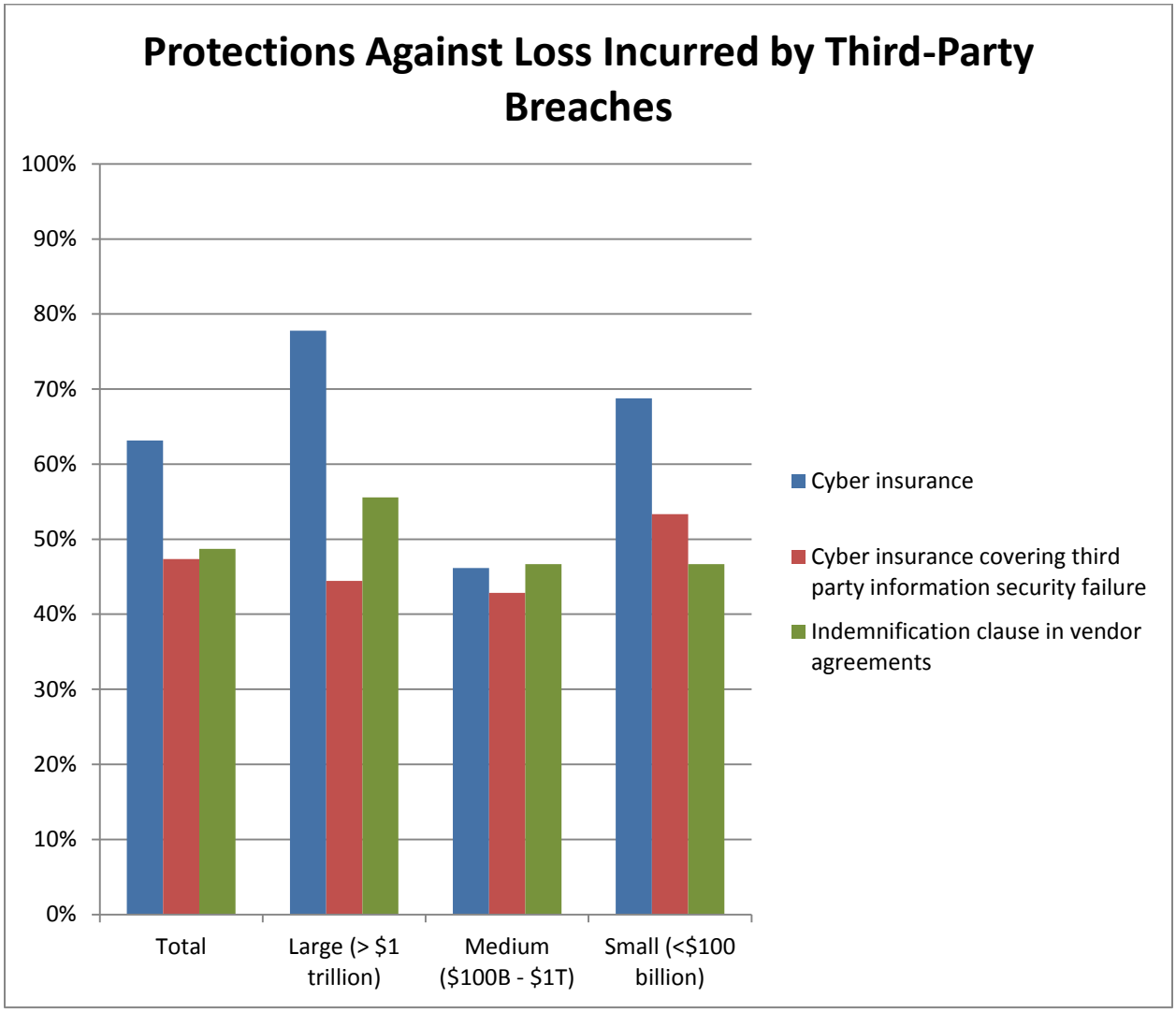
TABLE 4



D. Protections against Loss Incurred by Third-Party Information Security Failures

The Department asked each banking organization to list any and all protections against loss incurred as a result of an information security failure by a third-party service provider, including any relevant insurance coverage. Sixty-three percent of the surveyed institutions (78% of large institutions) informed the Department that they carry insurance that would cover cyber security incidents. However, only 47% of the surveyed institutions reported having cyber insurance policies that explicitly cover information security failures by a third-party vendor. Only half of the banking organizations surveyed require indemnification clauses in their agreements with third-party vendors.

TABLE 5



V. Conclusion

Based on the responses that the Department received, banking organizations appear to be working to address the cyber security risks posed by third-party service providers, although progress varies depending on the size and type of institution.