New York State

Department of Financial Services

Report on Cyber Security in the Banking Sector

Governor Andrew M. Cuomo

Superintendent Benjamin M. Lawsky

May 2014

I. Introduction

Cyber attacks against financial services institutions are becoming more frequent, more sophisticated, and more widespread. Although large-scale denial-of-services attacks against major financial institutions generate the most headlines, community and regional banks, credit unions, money transmitters, and third-party service providers (such as credit card and payment processors) have experienced attempted breaches in recent years.

The rise in frequency and breadth of cyber attacks can be attributed to a number of factors. Unfriendly nation-states breach systems to seek intelligence or intellectual property. Hacktivists aim to make political statements through systems disruptions. Organized crime groups, cyber gangs, and other criminals breach systems for monetary gain—*i.e.*, to steal funds *via* account takeovers, ATM heists, and other mechanisms. As the cost of technology decreases, the barriers to entry for cyber crime drop, making it easier and cheaper for criminals of all types to seek out new ways to perpetrate cyber fraud. A growing black market for breached data serves to encourage wrongdoers further.

With this in mind, the New York State Department of Financial Services ("the Department") in 2013 conducted an industry survey on cyber security. A total of 154 institutions were asked to complete a questionnaire seeking information on each participant's cyber security program, costs, and future plans. The objective of the survey was to obtain a horizontal perspective of the financial services industry's efforts to prevent cyber crime, protect consumers and clients in the event of a breach, and ensure the safety and soundness of their organizations.

Of the total 154 depository institutions that completed the Department's cyber security questionnaire, there were 60 community and regional banks, 12 credit unions, and 82 foreign branches and agencies.

The survey asked questions about each participant's information security framework; corporate governance around cyber security; use and frequency of penetration testing and results; budget and costs associated with cyber security; the frequency, nature, cost of, and response to cyber security breaches; and future plans on cyber security.

In addition to the survey, the Department met with a cross-section of depository institutions and cyber security experts over the course of several months to discuss industry trends, concerns, and opportunities for improvement. This dialogue provided important additional context regarding specific challenges facing the industry, including the rapid pace of technological change and the increased frequency and sophistication of cyber attacks.

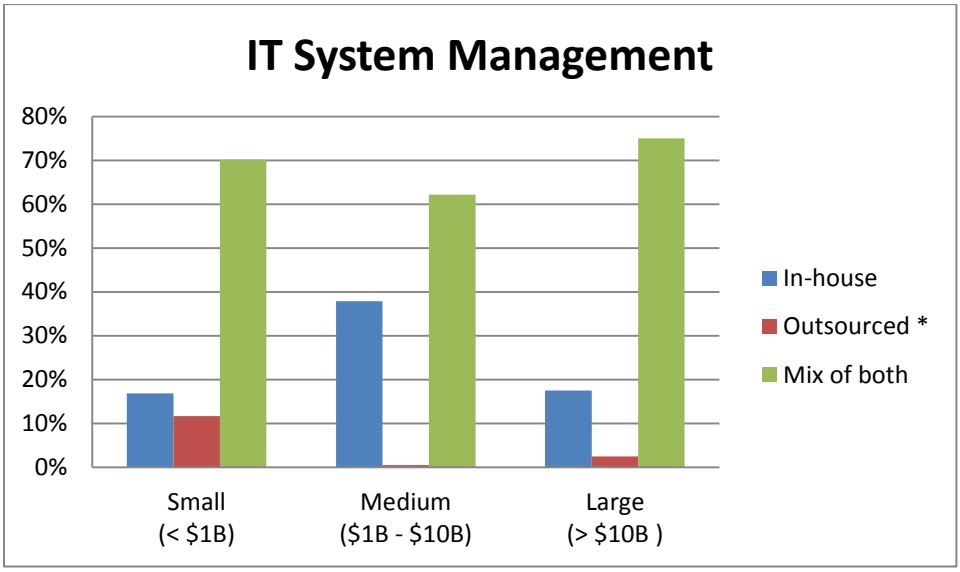
The findings described in this report represent responses of the survey participants as a whole or of specific sub-categories of participants (*e.g.*, by asset size). The findings are not indicative of

any particular institution. For the purposes of this report, depository institutions have been categorized as "small" (assets < $1 billion), "medium" (assets between $1 and $10 billion), and "large" (assets > $10 billion).

II. Findings

A. Management of Information Technology ("IT") Systems

The vast majority of depository institutions surveyed, irrespective of size, rely on both internal and external resources to manage their IT systems. Of large institutions, 75% reported relying on a mix of in-house and outsourced vendor-provided IT systems. Similarly, 62% of medium and 70% of small institutions reported the same. Notably, very few institutions—less than 12% irrespective of size—rely on a completely outsourced IT environment.



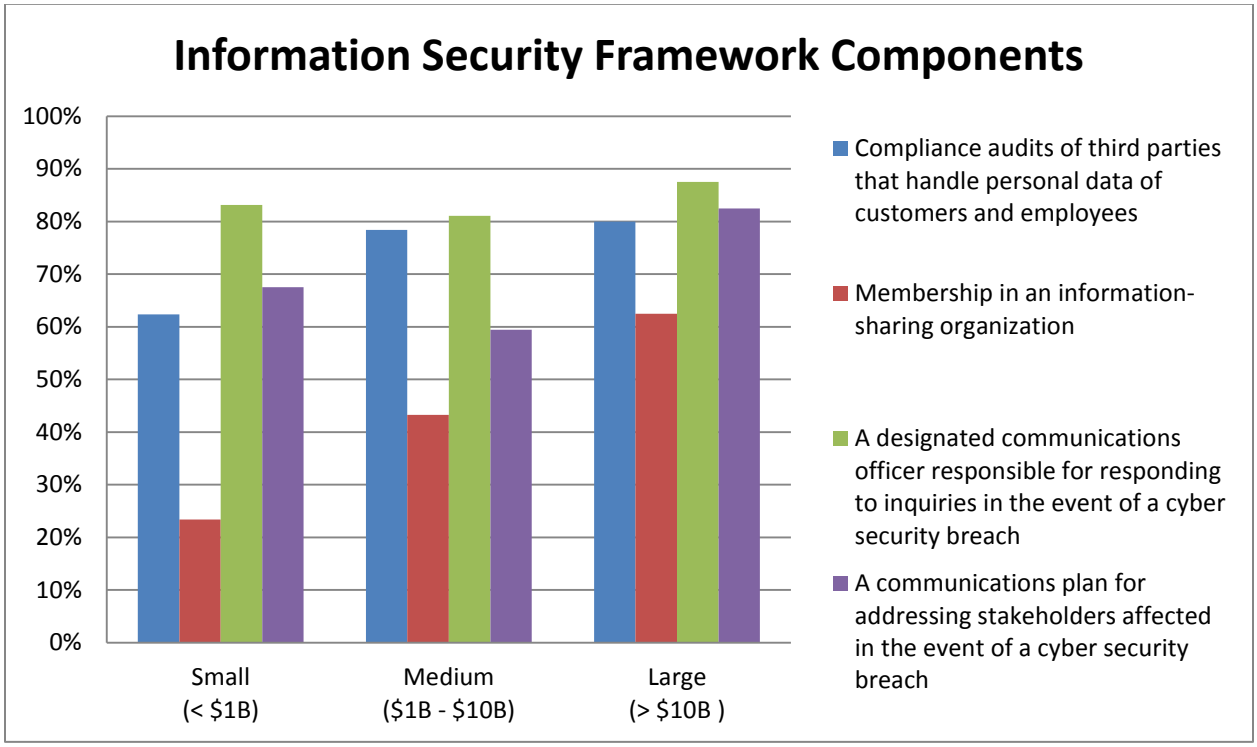
*Value of zero for medium-sized firms

B. Information Security Framework

Nearly all institutions—almost 90%—reported having an information security framework in place that includes what are considered to be the key pillars of such programs: (1) a written information security policy, (2) security awareness education and employee training, (3) risk management of cyber-risk, inclusive of identification of key risks and trends, (4) information security audits, and (5) incident monitoring and reporting. However, information security frameworks at medium and large institutions tend to be particularly well developed, with 89% and 98%, respectively, having implemented all five pillars.

Large institutions, however, are also more likely to have additional features integrated into their information security frameworks, such as a comprehensive communications plan to respond to inquiries in the event of a breach.

Approximately 84% of all institutions have a designated communications officer for responding to inquiries subsequent to a cyber-security breach. Large institutions, however, are more likely than small and medium institutions to have a communication plan for addressing stakeholders that may be impacted by a cyber-security breach. Nearly 83% of large institutions have such a plan, as compared to two-thirds (65%) of small and medium institutions.



The information security frameworks of small institutions lagged behind larger institutions in two additional areas: oversight over third party service providers[1] and membership in an information-sharing organization. While 80% of large and medium institutions reportedly conducted compliance audits of third parties that handle personal data of customers and employees, only 62% of small institutions reported doing so, which raises concerns. While small institutions might not have the resources to conduct their own comprehensive audits, they could rely on other existing resources to better understand their vendors' systems, controls, and financial health—such as the vendor's Federal Financial Institutions Examination Council

[1] Notably, all banking organizations, registered bank holding companies, and other entities supervised by the Department are required to notify the Department of any "decision to contract to receive automated data processing services from an independent firm or banking organization." Moreover, the Superintendent of Financial Services has the authority to examine all records and material of the firm or banking organization furnishing the services "to the extent he deems necessary to protect the interests of depositors, creditors or stockholders of the banking organization or licensee receiving such services." See Supervisory Procedures 101.1 and 101.2.

(FFIEC) Technology Service Provider examination report or its American Institute of Certified Public Accountants' (AICPA's) Service Organization Control (SOC) report.[2]

Large institutions were far more likely to participate in information-sharing organizations (*e.g.*, Information Sharing and Analysis Centers ("ISACs")) than small institutions—with more than 60% of large institutions reporting such a membership as compared to less than 25% of small institutions. The more limited financial resources of small institutions may contribute to their lack of ISAC participation, but small institutions can reap benefits from Financial Services-Information Sharing and Analysis Center ("FS-ISAC") membership at fairly low cost. Members receive timely notification and authoritative information specifically designed to help protect critical systems and assets from physical and cyber security threats. In fact, both the U.S. Department of Treasury and the U.S. Department of Homeland Security rely on the FS-ISAC to disseminate critical information to the financial services sector in times of crisis. In addition, the FS-ISAC provides an anonymous information-sharing capability across the entire financial services industry that enables institutions to exchange information regarding physical and cyber security threats, as well as vulnerabilities, incidents, and potential protective measures and practices.

C. Use of Security Technologies

A wide variety of security technologies aimed at improving systems security and preventing a cyber breach are employed by large, medium, and small institutions alike. The vast majority of institutions—irrespective of size—reported utilizing some or all of the following tools: anti-virus software, spyware and malware detection, firewalls, server-based access control lists, intrusion detection tools, intrusion prevention systems, vulnerability scanning tools, encryption for data in transit, and encrypted files. In addition, more than half of all institutions have deployed data loss prevention (DLP) tools, with large institutions accounting for most of the DLP use. More than half of small (57%) and medium (65%) institutions have deployed DLP, while about three-quarters (78%) of large institutions have done so.

Notably, 57% of all the institutions responded as using tools to discover the use of unauthorized devices. Perhaps less surprisingly, large and medium institutions (93% and 76%, respectively) were much more likely than small institutions (52%) to deploy smartcards and other one-time password tokens (*i.e.*, a key fob). These types of tools, when part of a two-factor authentication process, can help guard against attacks that exploit vulnerabilities in security software as the much-publicized Heartbleed bug has done in recent weeks.

Large institutions also were more likely than medium and small institutions to implement public key infrastructure systems (63% and 35%, respectively, as compared to 16%). Although large

[2] "Guidance on Managing Outsourcing Risk," December 5, 2013 (Board of Governors of the Federal Reserve System).

and medium institutions (33% and 27%, respectively) also were more likely to deploy biometric tools than small institutions (13%), the use of this cutting-edge technology was relatively modest across the industry, which is to be expected given that these tools are still developing and remain costly. As technology in this area continues to develop, the use of biometrics is expected to become more affordable and widespread.

The majority of institutions already have policies and procedures in place to mitigate the information security risks associated with mobile devices (*e.g.*, tablets and smartphones) and social media. Notably, fewer than 27% of all the institutions have already implemented policies and procedures to mitigate information security risks associated with Cloud computing, but more than 35% of institutions without policies and procedures plan to introduce them in the next three years.

D. Penetration Testing

Penetration tests (the practice of testing a computer system, network or Web application to identify vulnerabilities that an attacker could exploit) are conducted industry-wide, with 100% of large and medium institutions and 91% of small institutions undertaking such testing. Nearly 80% of the institutions conduct penetration testing on an annual basis. Approximately 13% of institutions conduct penetration tests more frequently, with 9% of institutions performing tests on quarterly basis and 4% on a monthly basis. Although penetration testing is an important element of an institution's cyber security program, such tests provide only a snapshot of an institution's vulnerabilities and can become outdated as soon as a new threat emerges. Ongoing systems monitoring through vulnerability scans are at least as—if not more—important to identify known weaknesses and potential exposures.

More than half of all institutions conduct penetration tests that originate from both internal and external sources, which is considered to be a best practice. Although external threats tend to grab headlines, insider breaches from employees, consultants, and others can do just as much—if not more—harm to an institution.

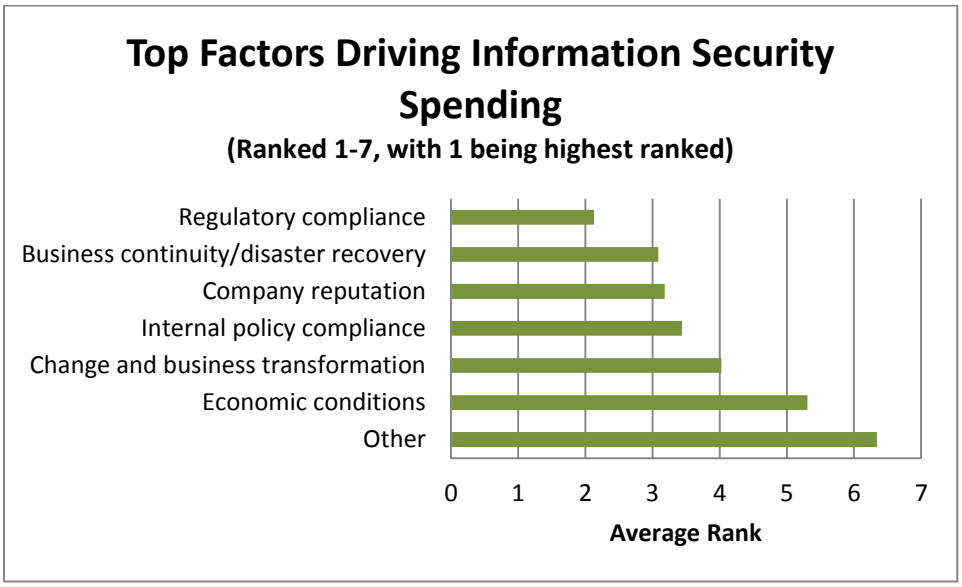
More than 85% of institutions rely on third-party consultants to perform penetration testing. Some institutions also reported conducting their own tests and/or supporting the tests performed by consultants. Nearly 38% of large institutions, 24% of medium institutions, and 10% of small institutions had their IT staff lead or support penetration tests in some fashion.

E. Budget and Costs

At most institutions, the budget for information security/cyber risk-management is housed either within the institution's IT or operations budget. More than three-quarters (77%) of all institutions experienced an increase in their total information security budget in the past three years, with most of the remaining institutions (18%) reporting that information security budgets

have remained the same. Almost no institutions reported a decrease in spending in the past three years.

The vast majority of institutions—approximately 79% industry-wide—reported that information security budgets were expected to increase in the next three years. Notably, small and medium institutions were more likely than large institutions to report that their information security budgets would remain the same over the next three years, with nearly 16% to 21% of small and medium institutions, respectively, anticipating no change to their budgets as compared to only 10% of large institutions. The top three factors cited by institutions as driving information security spending were (1) compliance and regulatory requirements, (2) business continuity and disaster recovery, and (3) reputational risk.



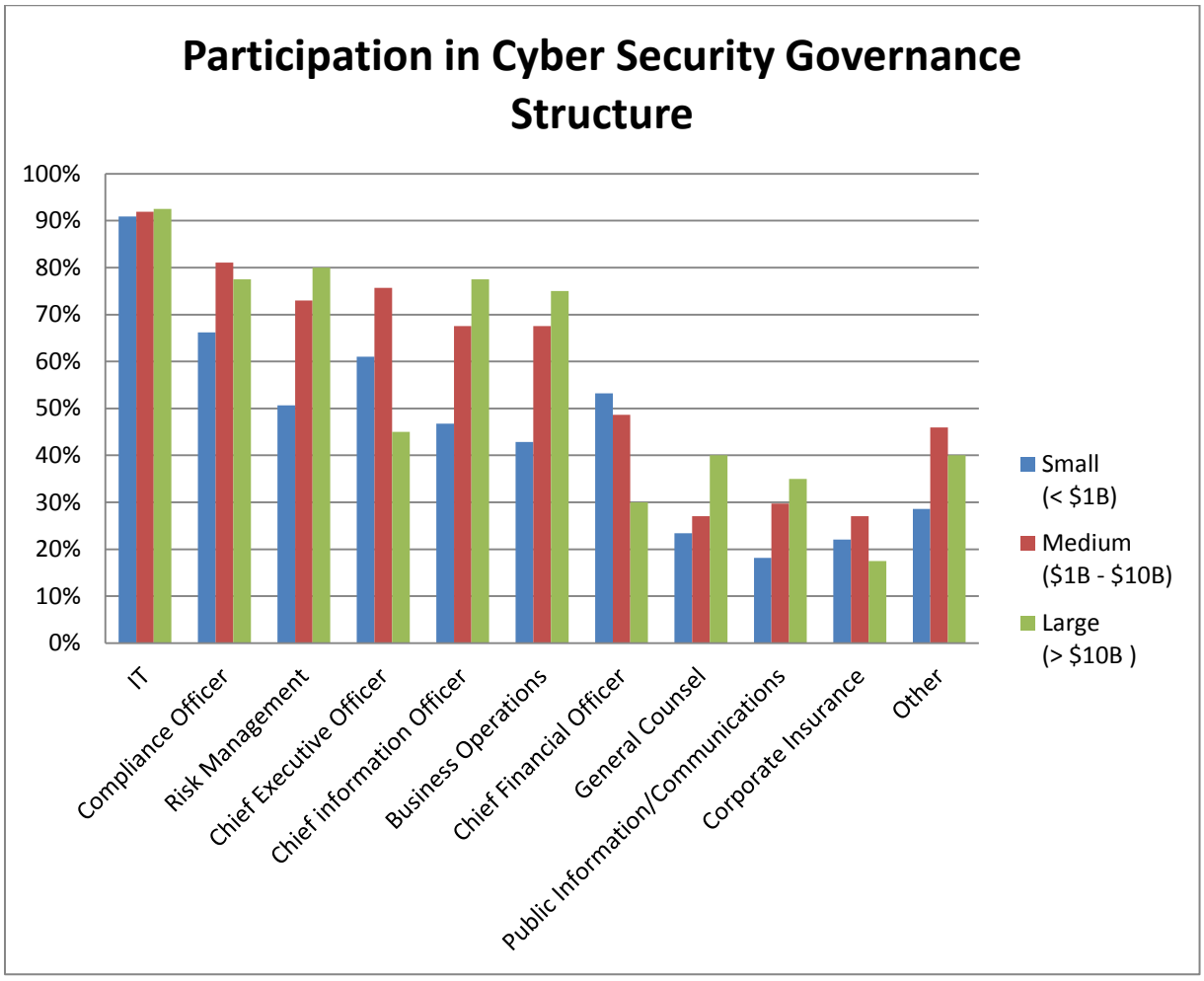
Although fewer than 21% of institutions reported budgeting specifically for a cyber event (*i.e.*, a successful breach or other major systems disruption), many institutions reported that funds could be reallocated from within the IT (or other) budget(s) as needed should a cyber event occur.

More small institutions (66%) reported having external insurance coverage to help manage cyber security risk relative to medium (62%) and large (60%) institutions.

F. Corporate Governance

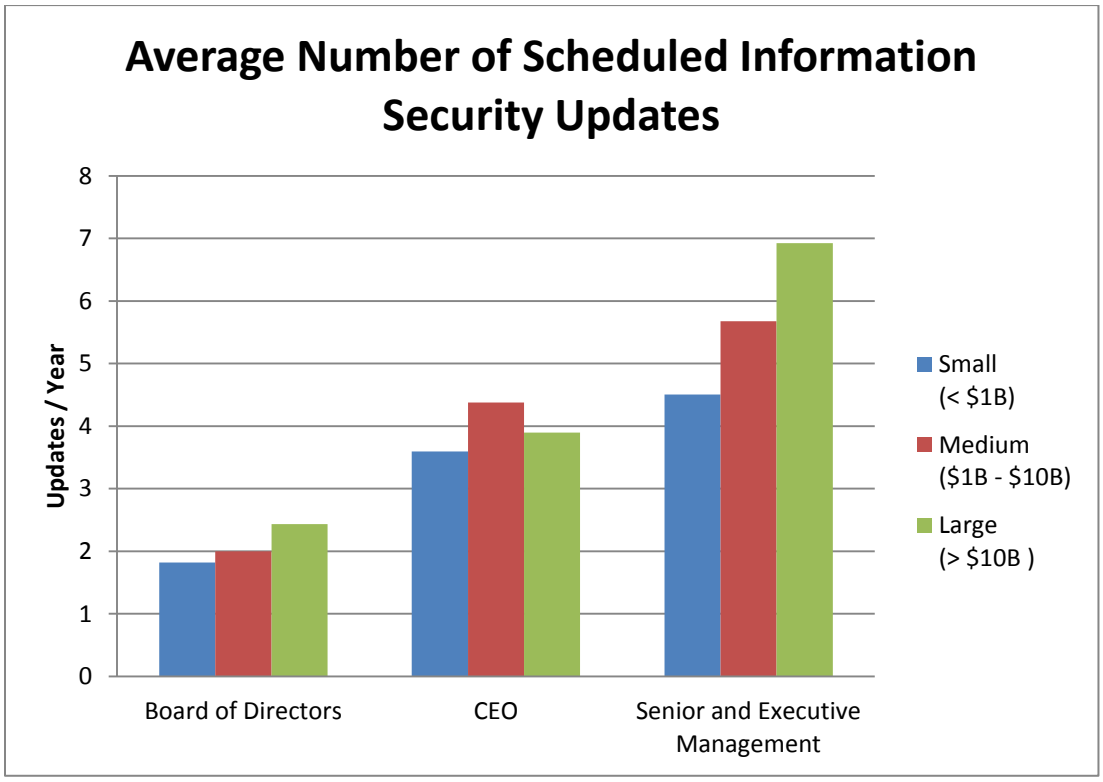
Corporate governance around cyber security tends to be highly IT-centered. When asked which divisions and employees participated in their organizations' cyber security governance structure, institutions cited IT departments most frequently (92%), followed by Compliance Officer (73%), Risk Management (64%), Chief Executive Officer (61%), Chief Information Officer (60%), and Business Operations (57%). Notably, certain divisions and employees appeared to be

underrepresented in institutions' cyber security governance structure—specifically, General Counsel (29%), Public Information/Communications (25%), and Corporate Insurance (22%).



The inclusion of these divisions could only serve to strengthen cyber security governance within an institution and to ensure a holistic approach to managing cyber risk and addressing the consequences of a cyber breach. The General Counsel should advise on potential legal liabilities arising from a cyber event, as well as any indemnifications of potential litigants following a breach. Corporate Insurance should evaluate the need for (or adequacy of an institution's) cyber risk coverage or, alternatively, determine the extent to which Directors and Officers liability policies might apply in the absence of a cyber-specific policy. Similarly, an institution's Public Information/Communications team should identify potential stakeholders requiring feedback in the aftermath of a cyber attack, as well as anticipate the number and types of inquiries that may arise.

Approximately 64% of institutions reported having a dedicated information security executive. Large institutions are more likely to have this dedicated position (80%) compared to small institutions (52%). However, the reporting line of that information security executive varied dramatically amongst institutions, with information security executives alternatively reporting to the Board of Directors (25%), the Chief Executive Officer (33%), or the Chief Information Officer (22%). The frequency at which specific managers within an institution received information security updates depended largely upon their level, with Boards of Directors receiving updates less often than senior management. More specifically, 73% of institutions reported that the Board of Directors received information security updates quarterly or annually, whereas 33% of institutions reported that senior managers received monthly updates. The frequency of information security updates to Chief Executive Officers varied dramatically amongst institutions, ranging from annually (30%), quarterly (24%), and monthly (22%).



Many institutions also reported providing *ad hoc* information security updates across their organizations (likely in response to a specific incident or risk), including the Board of Directors (21%), the Chief Executive Officer (37%), and senior management (34%). A small number of institutions reported never providing information security updates to the Board of Directors (<7%), the Chief Executive Officer (<4%), or senior management (<1%). While limited to a small number of institutions, this lack of information security reporting, as well as some institutions' exclusive reliance on *ad hoc* reporting, represents an area needing improvement. Periodic information security updates should be provided to all levels of management, including the Board of Directors, to ensure that an institution's cyber risk is appropriately weighed and managed. IT departments may find themselves unable to compete for financial resources within

their organizations if the Board or executive-level management cannot fully appreciate the institution's cyber risk.

G. Cyber Security Incidents and Breaches

Most institutions irrespective of size experienced intrusions or attempted intrusions into their IT systems over the past three years. The attempted methods ran the gamut, with most institutions reporting incidents involving malicious software (malware) (22%), phishing (21%), pharming (7%), and botnets or zombies (7%). The larger the institution, the more likely it appeared to experience malware and phishing attempts. About 13% of small institutions reported being attempted targets of malware, as compared to 21% of medium institutions and 35% of large institutions. Similarly, about 16% of small institutions reported attempted phishing, as compared to 22% of medium institutions and 33% of large institutions. It is unclear whether the variation between large and small institutions represents an actual difference in the type of attempted intrusions experienced by these organizations or whether it is an indication that larger institutions are better equipped to identify systems intrusions.

The most frequent types of wrongful activity resulting from a cyber intrusion reported by institutions were account takeovers (46%), identity theft (18%), telecommunication network disruptions (15%), and data integrity breaches (9.3%). Third-party payment processor breaches were also reported by 18% and 15% of small and large institutions, respectively. Large institutions also cited mobile banking exploitation (15%), ATM skimming/point-of-sale schemes (23%), and insider access breaches (8%).

Although institutions reported numerous attempted systems intrusions over the prior 12 months, very few institutions experienced successful breaches resulting in significant monetary damages. But a greater number of large institutions than small and medium institutions reported experiencing financial losses resulting from cyber breaches.

For those institutions that experienced a monetary loss in the past three fiscal years due to cyber security breaches, the top two factors included in calculating the monetary loss as reported by the institutions were: (1) customer reimbursements (76%), (2) audit and consulting services (52%), and (3) deployment of detection software, services and policies (45%). Although many institutions factored loss of customer business (38%) and damage to brand/reputation (31%) into their total loss calculations, these losses in many cases were likely too difficult to quantify for institutions to factor into their overall monetary loss resulting from a cyber breach.

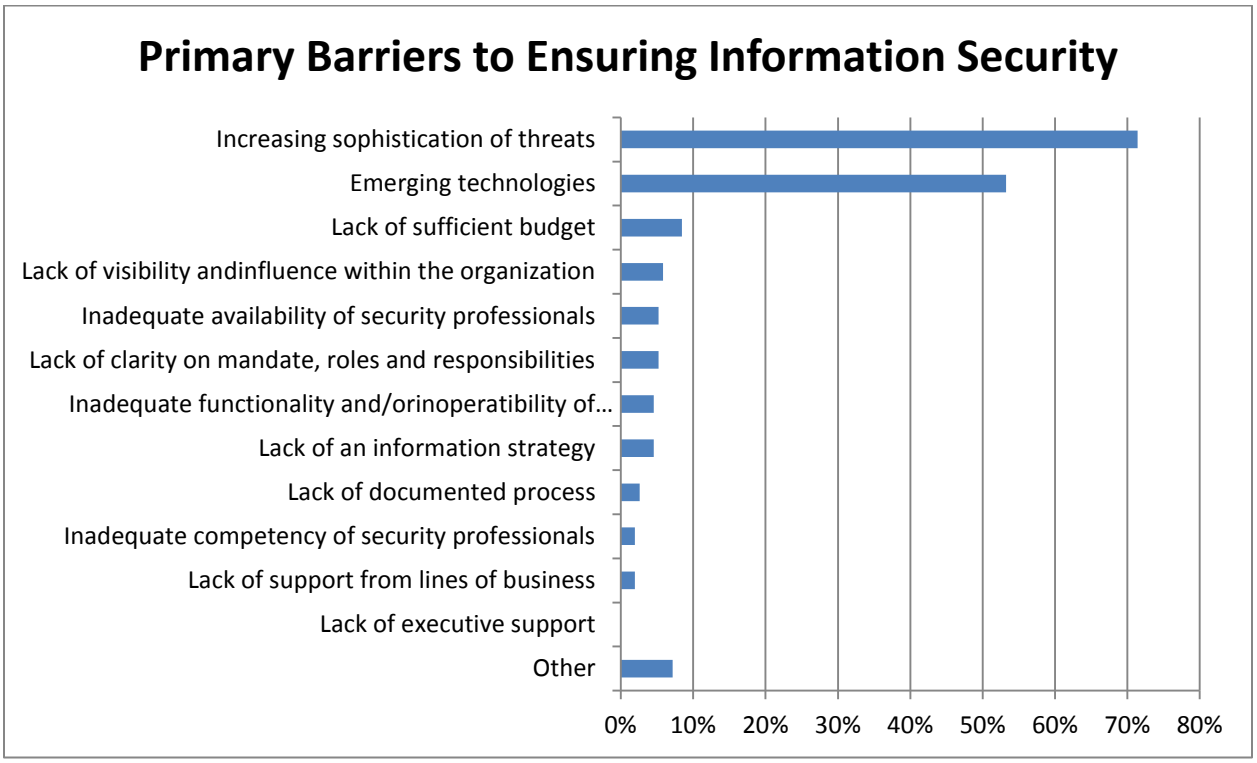
In nearly all instances, institutions that experienced a cyber security breach notified law enforcement and/or the relevant regulatory agency. Survey results indicated that institutions tend to inform law enforcement and regulators as a matter of course, but notify consumers and/or investors only when they are directly impacted.

H. Planning for the Future

Although the majority of institutions reported having a documented information security strategy in place for the next one to three years, large and medium institutions were more likely to have a

plan than small institutions. More than 90% of large institutions and nearly 80% of medium institutions had a documented information security strategy, as compared with 62% of small institutions. Approximately 49% of institutions reported that their information security strategy adequately addressed new and emerging risks, while 31% said they need to modify their strategy to assess new risks and another 22% said they need to investigate further to understand the risks.

Most institutions indicated that the greatest challenge to building an adequate cyber security program arises from external factors. The barriers to ensuring information security most cited by institutions were the increasing sophistication of threats (71%) and emerging technologies (53%). Although reported less frequently, lack of visibility and influence within the organization (6%) and lack of sufficient budget (8%) were also cited as barriers in some instances.



III. Continuing Challenges

Although financial institutions have taken significant steps to bolster cyber security efforts in recent years, banks and other financial services companies will continue to be challenged by the speed of technological change and the increasing sophisticated nature of threats. While institutions are aware that the threat landscape is constantly evolving, they may find it difficult to keep up with the latest developments amid competitive pressure to integrate new technologies into their product offerings (*e.g.*, remote deposit capture). Experts have noted that when competition surrounding new product development is fierce, security can lag behind.

The rapid pace of change makes it more critical than ever that institutions take advantage of the information-sharing and analysis resources available to them. With this in mind, the Department has recommended that all New York State-chartered depository institutions, irrespective of size, become members FS-ISAC.[3] While the most sophisticated institutions are developing in-house intelligence-gathering capabilities focused on cyber security, most institutions will be limited to information received externally. Although institutions seem more willing than in the past to share information regarding threats and attacks, many remain hesitant to reveal perceived or actual security weaknesses to competitors. Through conversations with the Department, institutions have indicated that information-sharing is most productive when it focuses on specific threats (or types of threats) and solutions. This is particularly important for small institutions, which may need tangible information in order to direct limited financial resources to where they can be most effective—*i.e.*, toward specific threats and solutions.

Another continuing challenge is the industry's reliance on third-party service providers for critical banking functions. As indicated above, all institutions irrespective of size rely on third-party vendors for cyber security. In addition, most small and medium institutions outsource functions such as payment processing and most of their web application and online banking systems to external companies. This interconnectedness suggests that an institution's cyber risk level depends in large part on the processes and controls put in place by third parties. Institutions may not be permitted by their vendors to undertake penetration testing. Even more likely, small and medium institutions may not have the resources to do so. To the extent that institutions do not have adequate insight into the sufficiency of the processes and controls of their third-party service providers, this may represent an area in need of heightened due diligence and monitoring. Cyber security and data protection requirements should be incorporated into institutions' third-party contracts from the outset.

Finally, although the issue of limited resources will continue to plague small institutions in particular, the amount of money spent on a cyber program is by no means the best reflection of its strength. Costly software that is rarely updated, deployed in an ineffective manner, or fails to take into account social engineering does little to contribute to an institution's cyber program. Much more relevant is an institution's ability to identify its top cyber risks and design a program around those risks. The Department recognizes that cyber security does not have a "one-size-fits-all" solution and that a successful cyber program will be based an institution's size, its business model, and sensitivity of data collected. It is essential that an institution's view of its cyber risk remains dynamic as those factors change and evolve over time.

[3] See "Banking Division Industry Letter: FS-ISAC Participation Recommended For All NYS-Chartered Depository Institutions" (NYS DFS, February 6, 2014), *available at* http://www.dfs.ny.gov/banking/bil-2014-02-06.pdf.

IV. Conclusion

The Department is deeply committed to supporting the financial services industry in the area of cyber security. As part of its continuing efforts in this area, the Department plans to expand its IT examination procedures to focus more fully on cyber security. The revised examination procedures will include additional questions in the areas of IT management and governance, incident response and event management, access controls, network security, vendor management, and disaster recovery. The revised procedures are intended to take a holistic view of an institution's cyber readiness and will be tailored to reflect each institution's unique risk profile. The Department believes this approach will foster smarter, stronger cyber security programs that reflect the diversity of New York's financial services industry.