New York State
Department of Financial Services

Report on Cyber Security in the Insurance Sector

February 2015

Report on Cyber Security in the Insurance Sector

I. Introduction

Cyber attacks against financial services institutions, including insurance companies, are becoming increasingly frequent and sophisticated. Insurance firms often possess large amounts of personally identifiable information ("PII") and protected health information ("PHI"); safeguarding such information in digital format is technologically challenging and expensive. The decreasing cost of technology in general, while helpful to legitimate business entities, also makes it easier and cheaper for cyber criminals to disrupt systems and obtain access to protected data. Moreover, PII and PHI are becoming more valuable on the black market, which increases incentives for cyber attacks.

In light of such threats, the New York State Department of Financial Services (the "Department") conducted a survey with respect to cyber security at a significant cross-section of regulated insurance companies during 2013 and 2014.[1] A total of 43 entities, with combined assets of approximately $3.2 trillion, completed a survey seeking information about each participant's cyber security program, costs, and future plans. The objective of the survey was to obtain a horizontal perspective of the insurance 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 43 insurance providers that completed the Department's cyber security questionnaire, 21 were health insurance providers, 12 were property and casualty insurance providers, and 10 were life insurance providers. The reported assets of each entity surveyed range from approximately $4 million to $403 billion.

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

The Department also met with a cross-section of insurers and cyber security experts over the course of the past year to discuss industry trends, concerns, and opportunities for improvement. That dialogue provided important additional context regarding specific challenges facing the insurance industry, including the rapid pace of technological change and the increased frequency and sophistication of cyber attacks.

In addition to reviewing the cyber security programs and protections of the participating insurers, the Department also reviewed the statutorily required enterprise risk management ("ERM")

[1] The Department conducted a similar survey at several of its regulated banking institutions in 2013 and issued a report on Report on Cyber Security in the Banking Sector ("Banking Sector Report") in May 2014. *See* Governor Andrew M. Cuomo, Superintendent Benjamin M. Lawsky, Report on Cyber Security in the Banking Sector (May 2014), http://www.dfs.ny.gov/about/ press2014/pr140505_cyber_security.pdf.

reports that certain insurers filed with the Department for the first time this year to understand better how cyber security fits into those insurers' overall risk management strategy.

Notably, the Department's analysis of the insurers surveyed found that a wide array of factors – not just reported assets – affect the sophistication and comprehensiveness of the insurers' cyber security programs. Those factors include reported assets, transactional frequency, the variety of business lines (insurance and non-insurance) written, and the sales and marketing technologies associated with those lines. In other words, although it may be expected that the largest insurers would have the most robust and sophisticated cyber defenses, the Department did not necessarily find that to be the case.

Moreover, the Department found that 95% of insurers already believe that they have adequate staffing levels for information security and only 14% of chief executive officers receive monthly briefings on information security. Recent cyber security breaches at financial institutions and other major corporations should serve as a wake up call for insurers to redouble their efforts to strengthen their cyber defenses – particularly given the level of sensitive consumer information that insurers are entrusted with handling.

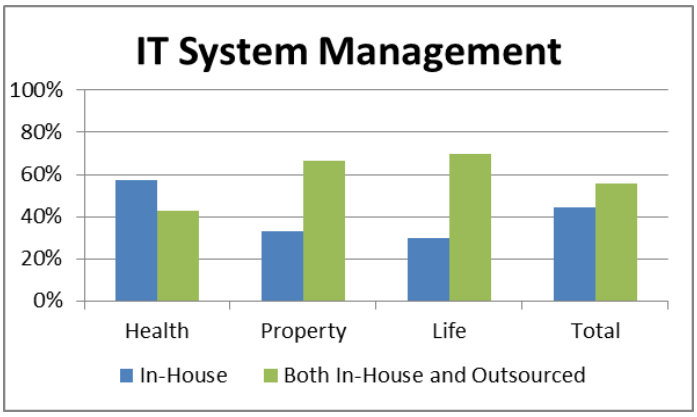
In the coming weeks and months, DFS expects to proceed with a number of initiatives to help strengthen cyber security at its regulated insurance companies. These include integrating regular, targeted assessments of cyber security preparedness at insurance companies as part of the Department's examination process; putting forward enhanced regulations requiring institutions to meet heightened standards for cyber security; and exploring stronger measures related to the representations and warranties insurance companies receive from third-party vendors, and other measures.

II. Findings

A. Management of Information Technology Systems

As illustrated in Table 1, of the insurers surveyed, 56% rely on both internal and external resources to manage their information technology ("IT") systems. The remaining 44% of insurers manage their IT systems entirely in-house.

TABLE 1



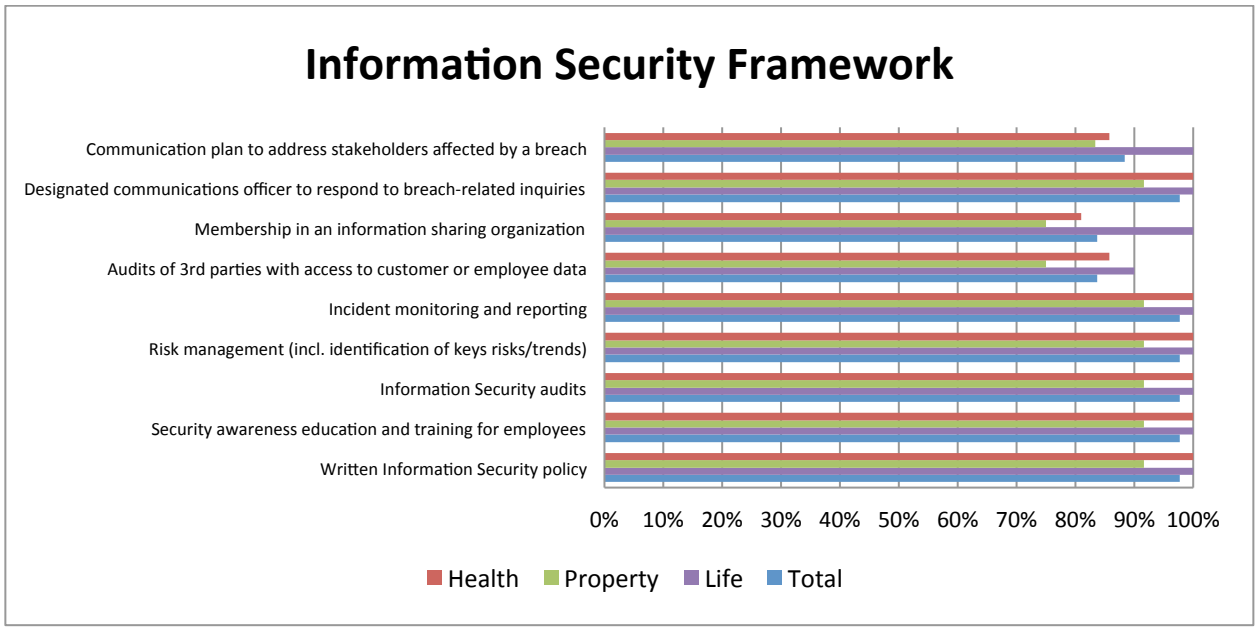
B. **Information Security Framework**

As illustrated in Table 2, nearly all insurers surveyed (98%) reported having an information security framework in place that includes what the Department considers to be the five key elements of cyber security programs: (1) a written information security policy; (2) security awareness and education and training for employees; (3) information security audits; (4) risk management of cyber risk, including the identification of key risks and trends; and (5) incident monitoring and reporting.

Similarly, approximately 98% of insurers surveyed have a designated communications officer for responding to inquires after a cyber-security breach. 88% of insurers reported having in place a communications plan for addressing stakeholders that may be impacted by a cybersecurity breach.

Of the insurers surveyed, 84% reported that they participate in information sharing organizations and 84% reported that they conduct compliance audits of third-party service providers that handle the personal data of customers or employees. While those percentages are high, the fact that some institutions – even if only a small number – do not participate in information-sharing organizations or conduct audits of their third-party service providers raises concern.

TABLE 2



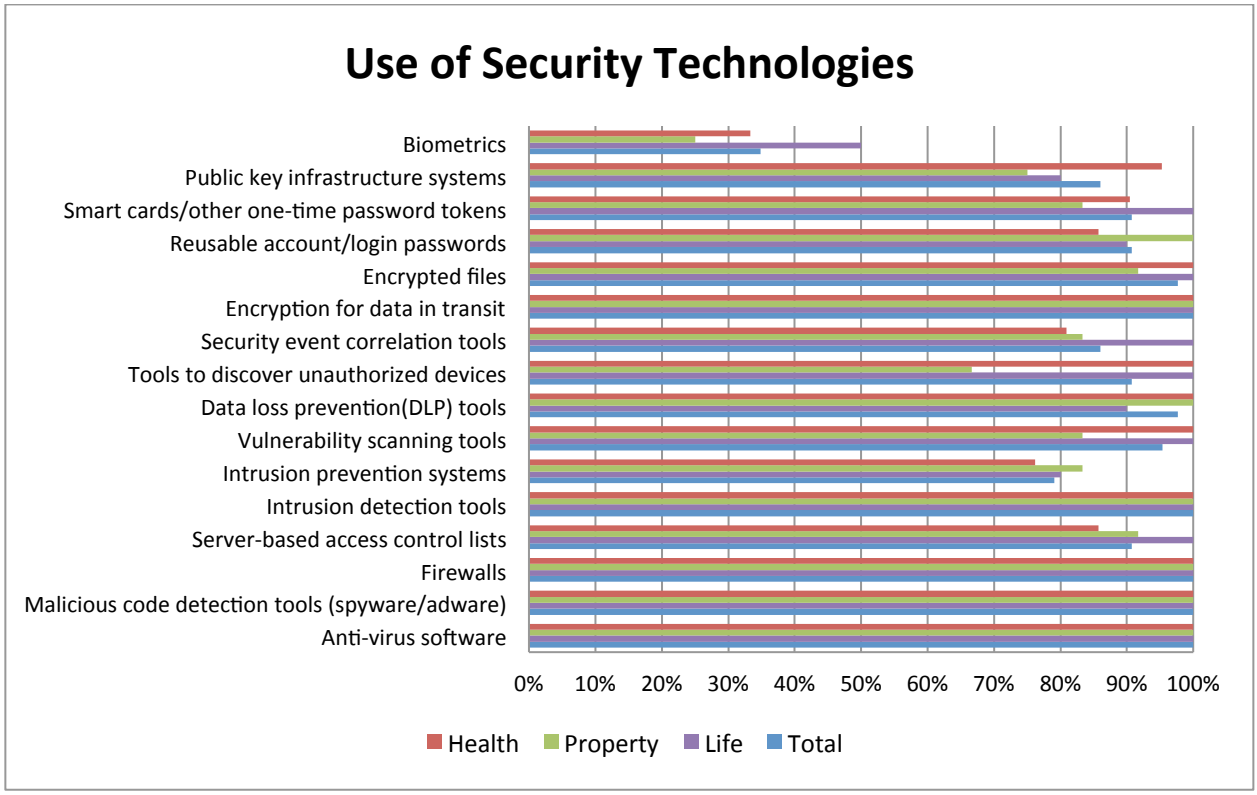
With respect to participation in information sharing groups, the Department believes that institutions of all sizes can reap benefits from membership in information-sharing organizations, such as the Financial Services – Information Sharing and Analysis Center ("FS-ISAC"), at a fairly low cost. As the Department noted in the Banking Report, members of FS-ISAC receive timely notification and authoritative information specifically designed to help protect critical systems and assets from physical and cyber security threats.

C. **Use of Security Technologies**

The insurers surveyed employ a number of security technologies to improve systems security and prevent data breaches, as illustrated in Table 3. Notably, 100% of institutions surveyed utilize anti-virus software, tools to detect malicious code, such as spyware or malware), firewalls, intrusion detection tools, and encryption for data in transit. Nearly all institutions surveyed employ data loss prevention tools (98%), file encryption (98%), and vulnerability scanning tools (95%). 91% of insurers reported using server-based access control lists, tools to discover unauthorized devices, and smart cards or other one-time password tokens. 86% of insurers surveyed reported using security correlation tools and implementing public key infrastructure systems, and 79% of insurers employ intrusion detection systems.

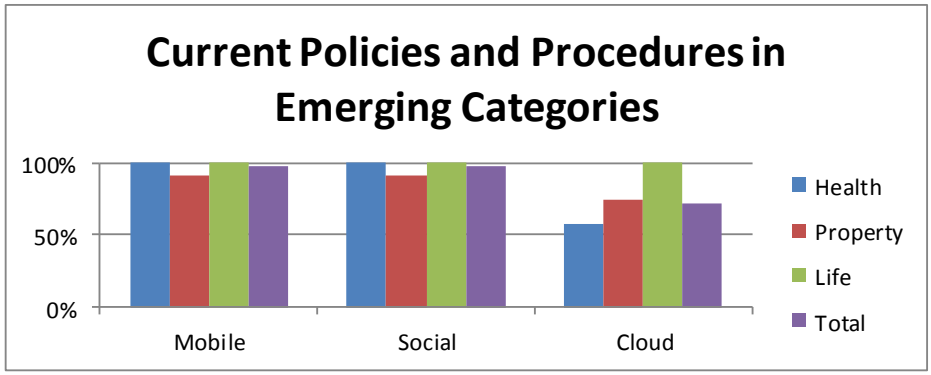
Unsurprisingly, less than half of all insurers surveyed reported the use of biometric tools, which rely on physical attributes to authenticate a person's identity, such as fingerprint or retinal scanning. As biometric technology develops, it is expected that its use will become more widespread and cost effective.

TABLE 3



As illustrated in Table 4, nearly all insurers (98%) reported having in place policies and procedures to mitigate the information security risks associated with the use of mobile devices and social media; 72% reported having in place policies and procedures to mitigate the information security risks associated with cloud computing.

TABLE 4



D. **Penetration Testing**

Penetration testing, which refers to the process of simulating an attack on a computer system, network, or application for the purpose of identifying vulnerabilities in the system, is commonly employed across the financial services industries. Indeed, 100% of insurers surveyed reported that they engage in penetration testing, and 88% reported conducting penetration tests that originate from both internal and external sources.

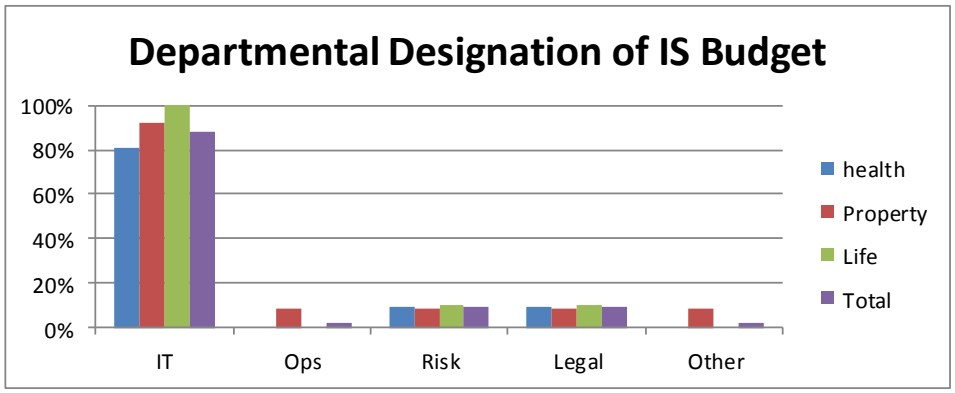
Although it is promising that all surveyed insurers perform penetration testing, the frequency with which they do so varies greatly. 44% of insurers reported conducting tests annually, 19% reported testing quarterly, and 30% reported testing monthly. As the Department noted in its Banking Sector Report, although penetration testing is an important element of an institution's cyber security program, it provides only a snapshot of an institution's vulnerabilities. The results, therefore, can become outdated quickly as new threats emerge. Ongoing vulnerability scanning is as—if not more—important than penetration testing to identify known weaknesses and potential exposures.

95% of insurers surveyed reported engaging third-party consultants to conduct penetration tests, but 65% reported that they conduct their own tests as well or instead (in the case of the 5% that did not report engaging third-party consultants).

E. **Budget and Costs**

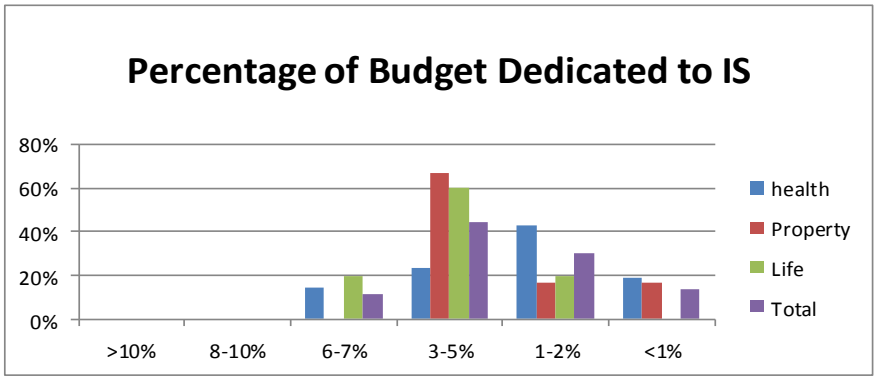
As illustrated in Table 5, 88% of insurers surveyed reported that their information security budgets are housed within their IT departments. Other departments reported to house the information security budget were operations (2%), risk management (9%), and legal (9%).

TABLE 5



As illustrated in Table 6, no institution reported having more than 7% of their overall budget dedicated to information security, and 14% of insurers reported dedicating less than 1% of their budget to security.

TABLE 6



81% of insurers reported that the percentage of their budgets allocated to information security has increased in the prior three years, and the remainder (19%) reported that the percentage of their budgets allocated to information security had remained the same. 86% of insurers reported that they expect their information security budgets to increase in the next three years, and the remainder (14%) expected it to remain the same.

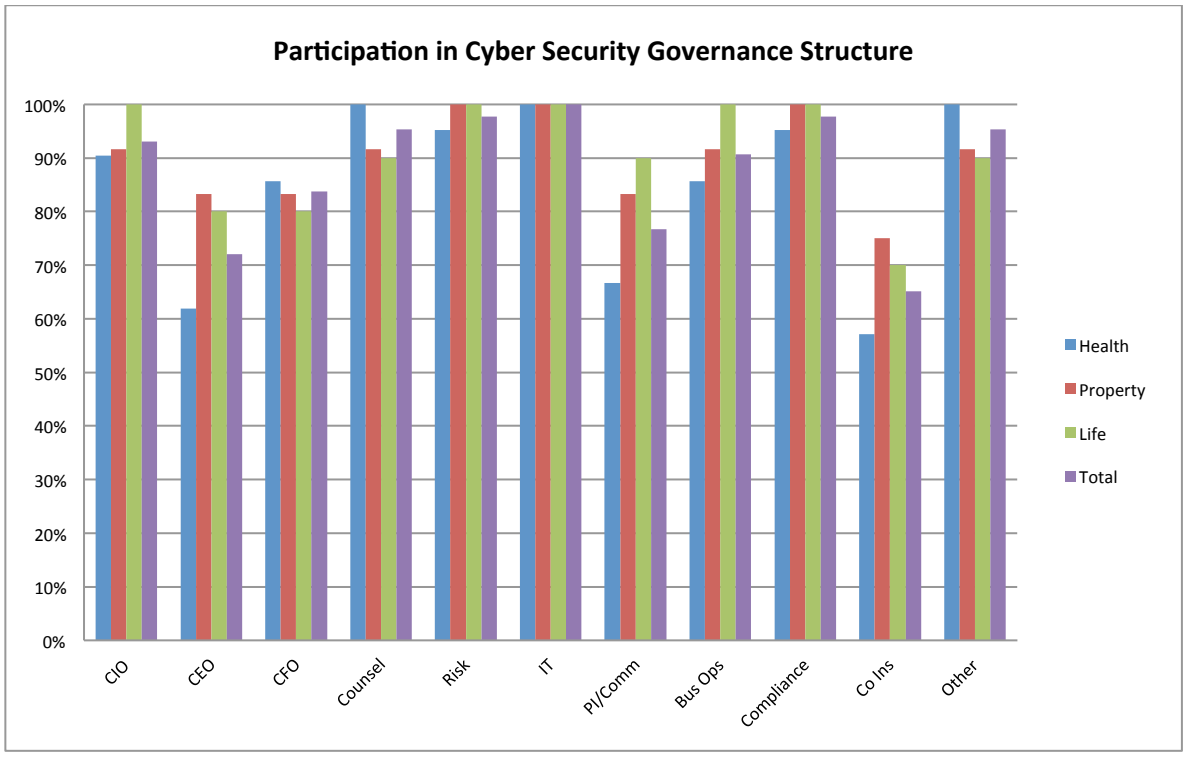
While only 51% of insurers surveyed reported having a budget specifically for cyber security events, 95% believe that they have adequate staffing levels for information security.

F. Corporate Governance and Reporting

With respect to corporate governance surrounding cyber security, a majority of insurers reported involvement from a number of different departments within their organizations. As illustrated in Table 7, 100% of insurers surveyed reported that their IT departments participated in the organization's cyber security governance. 98% reported having involvement from compliance officers and risk management personnel, 95% reported involvement from general counsel, 93%

reported involvement from chief information officers, 91% reported involvement from business operations personnel, 84% reported involvement from chief financial officers, 77% reported involvement from public information or communications personnel, 72% reported involvement from chief executive officers, and 65% reported involvement from their corporate insurance departments.

TABLE 7



81% of insurers reported having a designated information security executive (Table 8), and of those institutions, 69% reported that the information security executive reports to the chief information officer, among others, in some cases.

TABLE 8

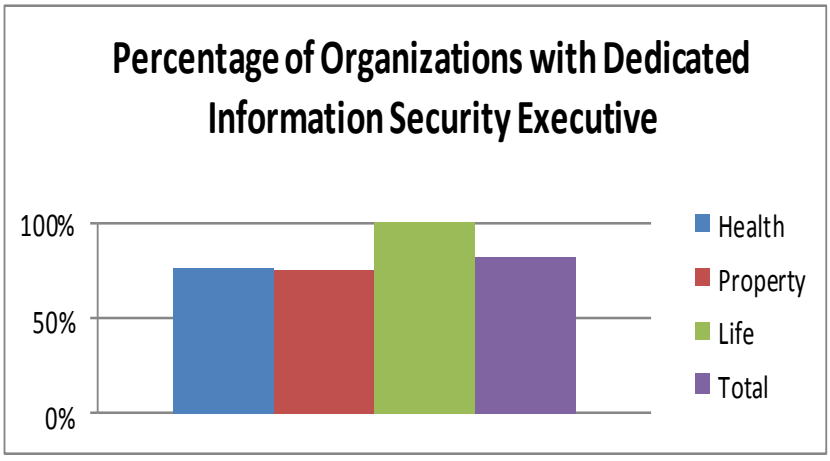
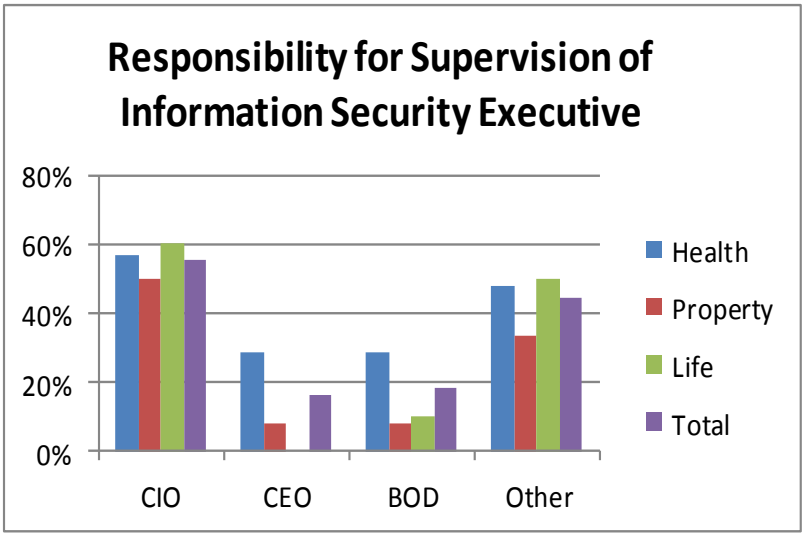


TABLE 9



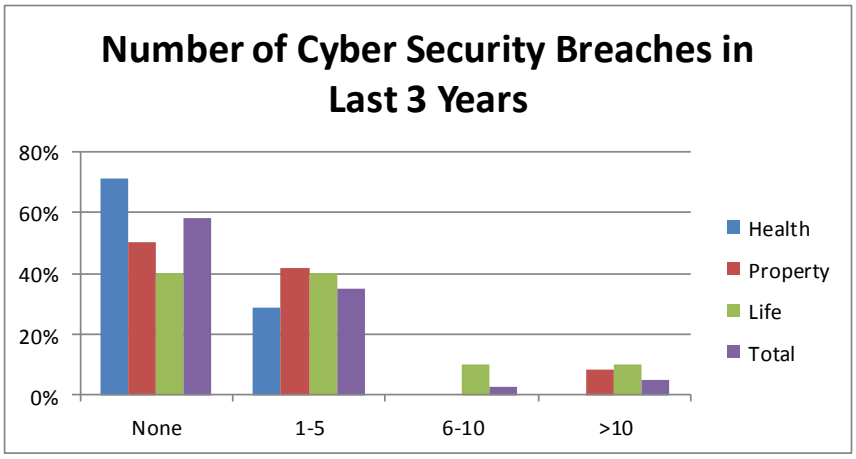
The frequency with which information security issues get reported to senior management varied across insurers. 86% of insurers reported that their senior and executive management receive information security updates on a monthly basis, but only 14% of insurers reported that their chief executive officers are updated that frequently. 53% of insurers surveyed reported that their chief executive officers are updated quarterly and 60% reported that their chief executive officers are updated on an ad hoc basis.

30% of insurers reported that their boards of directors are updated with respect to information security issues both quarterly and on an ad hoc basis, 26% reported that their boards are updated quarterly, 21% reported that their boards are updated only on an ad hoc basis, 14% reported annual updates, and 9% reported that their boards are updated annual and on an ad hoc basis.

G. Cyber Security Incidents and Breaches

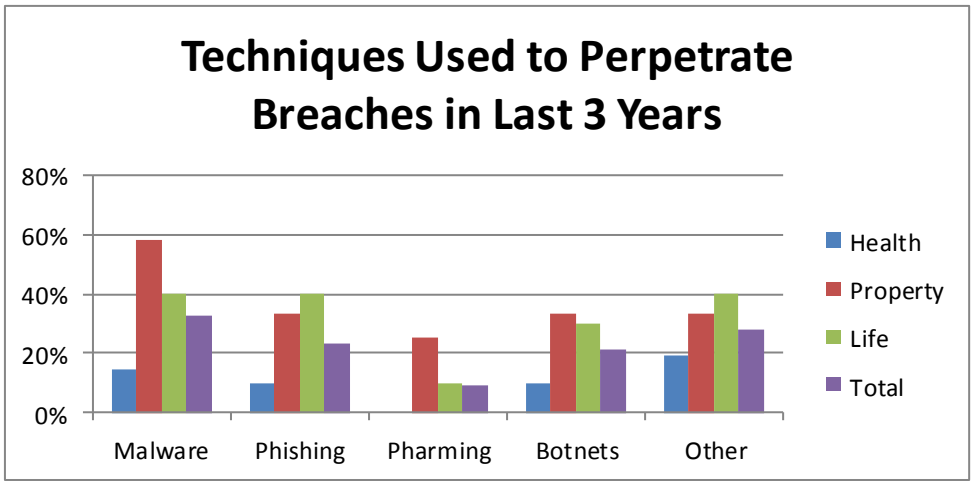
As illustrated in Table 10, 58% of insurers reported that they experienced no cyber security breaches in the three years preceding the survey, excluding failed attempts. 35% reported experiencing between one and five breaches, 2% reported experiencing between six and ten, and 5% reported experiencing more than ten breaches.

TABLE 10



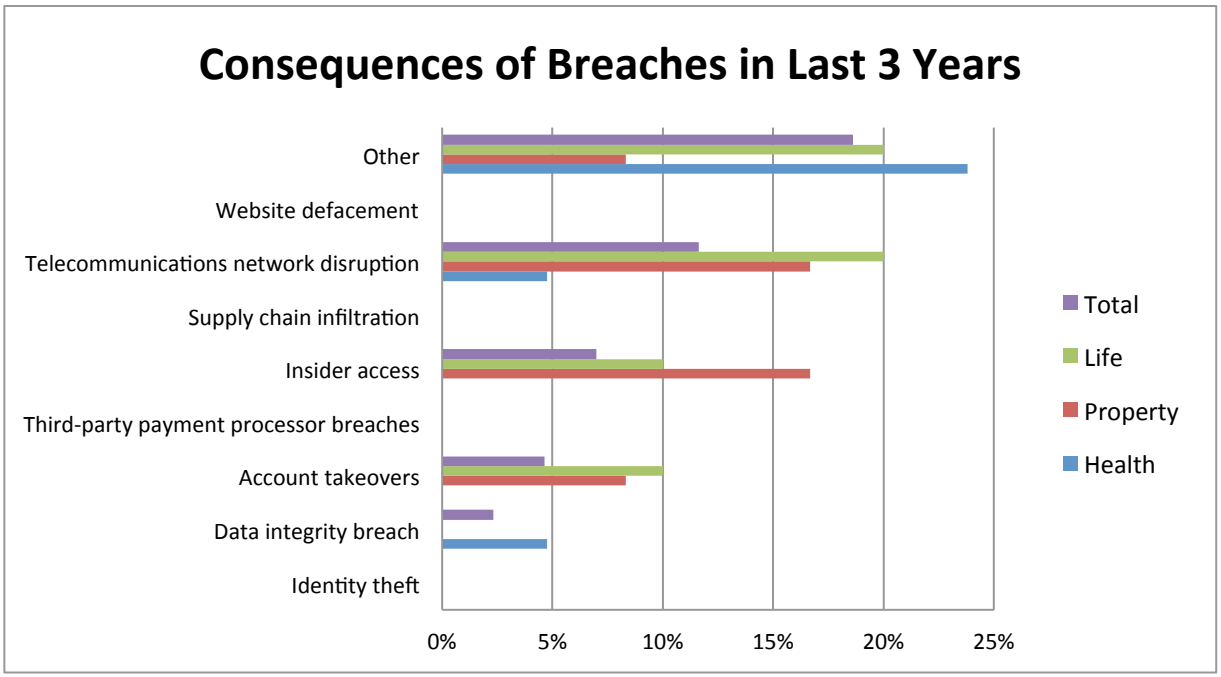
As illustrated in Table 11, the institutions reported being the targets of a range of different hacking techniques, including intrusive, malicious software or "malware" (33%), email scams or "phishing" (23%), techniques to gain control of networked computers, such as botnets or zombies (21%), and pharming attacks, which are attempts to redirect a website's traffic to a fake site (9%). 28% of institutions reported being the targets of "other" unspecified hacking techniques.

TABLE 11



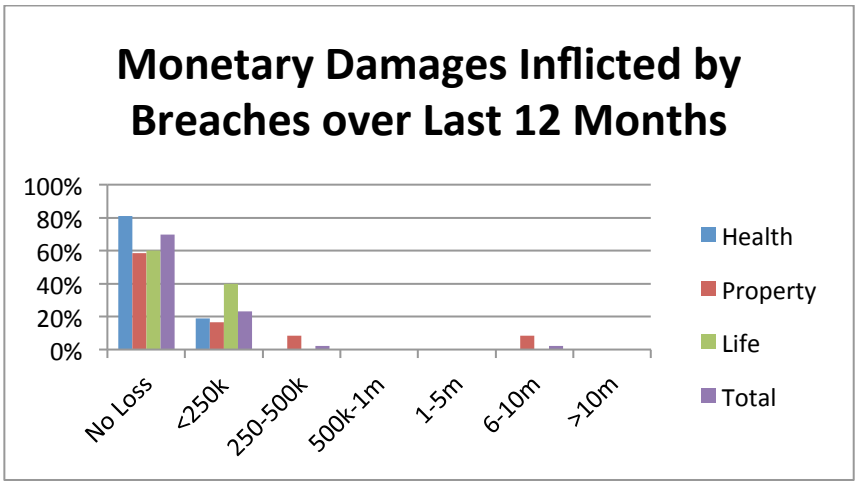
Despite the variety of hacking techniques employed against the insurers surveyed and the number of breaches they experienced collectively, the institutions reported experiencing relatively few negative effects as a result of the breaches or hacking attempts. As illustrated in Table 12, 12% reported disruption to their telecommunications networks as a result of a breach, 7% reported insider access breaches, 5% reported account takeovers, and 2% reported data integrity breaches. While 14% of insurers surveyed did report experiencing "other" activities as a result of a breach, none reported identity theft, third-party payment processor breaches, supply chain infiltration, or website defacement.

TABLE 12



As illustrated in Table 13, the majority of insurers (70%) reported suffering no financial loss in the past 12 months as a result of cyber security breaches, 23% reporting suffering a loss of less than $250,000, 2% reported a loss of between $251,000 and $500,000, and 2% [one institution] reported a loss of between $6 million and $10 million.

TABLE 13



Of the insurers that suffered a financial loss in the preceding 12 months as a result of a breach, we asked them to specify which factors they considered in calculating monetary damages. 58% reported considering their need to deploy detection software, services, and policies, 50% reported considering loss of customer business, 50% reported considering reimbursements, 50% reported considering legal defense costs, 28% reported considering damages to brand or

reputation, 17% reported including audit and consulting service costs, 11% reported including court settlements, and 58% also reported considering other, non-listed factors.

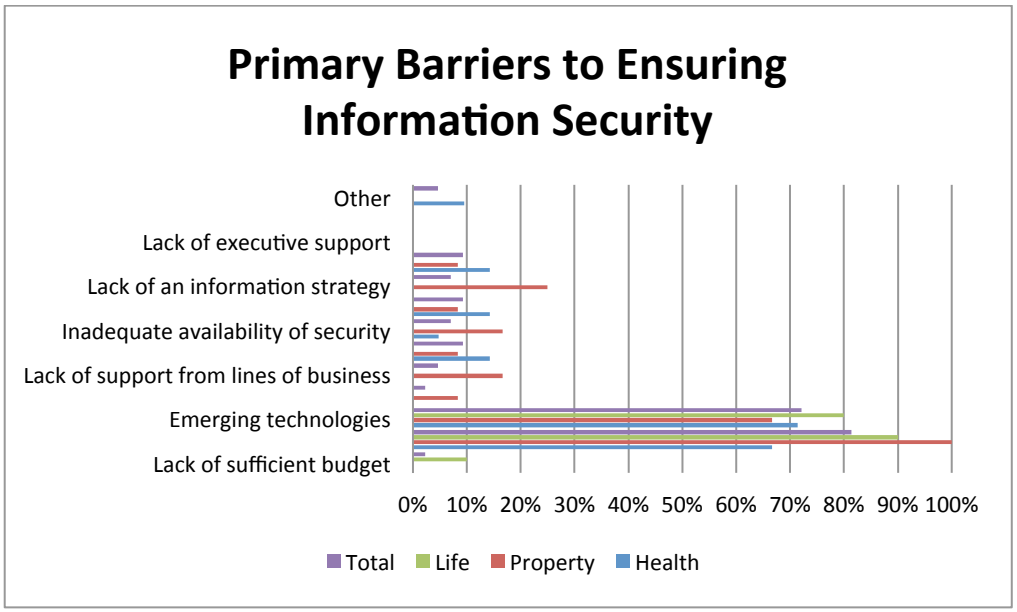
72% of the insurers that experienced a cyber security breach notified a regulatory agency, 67% notified law enforcement, and 56% notified consumers and/or investors. 33% of insurers that reported experiencing a breach stated that the institution did not consider the breach to be sufficiently significant to warrant notification of any third parties.

H. **Planning for the Future**

Over half of the insurers surveyed reported that their organization's current information security strategy adequately addresses new and emerging risks, while 40% reported a need to modify their strategies to address new and emerging risks, and 14% believe they need to investigate further to understand new and emerging risks.

When asked which factors are the primary barriers to ensuring information security at their organizations, a large majority of insurers surveyed reported the increasing sophistication of cyber security threats (81%) and emerging technologies (72%), as illustrated in Table 14. The remaining insurers cited a wide variety of factors as their primary challenges to information security, including: lack of clarity surrounding mandates, roles and responsibilities (9%); lack of documented process (9%); inadequate functionality or interoperability of security products (9%); inadequate availability of security professionals (7%); lack of information strategy (7%); lack of support from business lines (5%); insufficient budget (2%); and lack of visibility and influence within the organization (2%).

TABLE 14



I. Cyber Security and Enterprise Risk Management

As of 2014, Insurance Regulation 203, 11 N.Y.C.R.R. Part 82, requires certain insurance entities to file an annual enterprise risk management ("ERM") report with the Department identifying material risks to their ongoing operations. Several insurers surveyed in conjunction with this report, therefore, filed such ERM reports with the Department for the first time this year.

Of the ERM reports filed by surveyed insurers, most did not specifically identify or discuss cyber security as a stand-alone material risk. To the extent cyber security was specifically addressed, it was most often discussed in broad terms as a subset of material operational risk. In some instances, although cyber-security was not addressed explicitly, the reports broadly identified and discussed operational risk, which may have been intended to account for cyber security risk. Only one ERM report filed by the surveyed insurers provided in-depth identification and analysis of cyber security risks specific to the particular entity and discussed specific steps and ongoing projects to mitigate those risks.

As awareness surrounding cyber security increases, it is expected that future ERM filings will include more frequent explicit references to cyber security.

IV. Continuing Challenges

For financial institutions in general, and insurance firms in particular, cyber security is an increasingly important area of focus within their organizations. Nevertheless, most institutions report that they continue to be challenged by the sophistication of cyber security threats and the speed at which technology is changing. In light of the continuing cyber security challenges facing the financial services industry, the Department has been focusing its attention on how it can foster improved cyber security across the industry and provide guidance to better protect both financial institutions and their customers.

Accordingly, the Department has recently surveyed banking institutions about their management of third-party service providers that handle sensitive or confidential employee or customer data, and it plans to do the same with insurance institutions. Ensuring that each institution obtains the appropriate representations and warranties from its third-party service providers, for example, would be a solid step in bolstering the institution's own cyber security.

The Department is also considering the use of various security technologies in financial institutions, including such processes as multi-factor authentication, to determine where, and in what contexts, such technologies and processes are most worthwhile and effective in preventing breaches.

Finally**,** the past several months, the Department has met with a number of insurance providers and brokers to better understand the evolution of the cyber insurance market and the various types of cyber security insurance products and service that are currently on the market. As with

other types of insurance in the past, the growth of the cyber security insurance market could foster higher standards across the market. The Department is currently considering the ways in which it can support and encourage the development of the cyber security insurance market.

V. Conclusion

Bolstering cyber security in the financial services industry has been, and will continue to be, a high priority for the Department. Just as the institutions regulated by the Department are encouraged – and expected – to stay current on the changing landscape of cyber security, the Department plans to do the same. The Department will continue to engage in discussions with financial institutions and cyber security experts to understand the evolving challenges the institutions face. The Department is also in the process of revising its cyber security examination processes, which includes the development of extensive training programs for its IT examiners so that they are prepared to identify vulnerabilities in the institutions and work with the institutions to implement the appropriate solutions. The Department believes that such cooperation and dialogue is essential to developing smart and effective cyber security programs across New York's financial services industry.