West Texas Cyber Security Consortium

Banks Challenged By Cybersecurity Threats, State Regulators Acting

A new report concludes that while financial institutions have taken significant steps to bolster cyber security efforts, they will continue to be challenged by the speed of technological change and the increasingly sophisticated nature of threats.

While institutions are aware that the threat landscape is constantly evolving, they find it difficult to keep up with the latest developments amid competitive pressure to integrate new technologies into their product offerings. In light of the challenges posed by new cyber threats, the New York Department of Financial Services plans to add cybersecurity to its examination procedures. According to a report, issued by the Department, the examination will review a bank's cyber security incident response and event management, access controls, network security, vendor management, and disaster recovery procedures in evaluating the bank's overall safety and soundness.

The New York State Department of Financial Services has released a new report on cybersecurity.

The report notes that, cyber attacks against banks are "becoming more frequent, more sophisticated, and more widespread." Oftentimes not featured in the news are the attacks against "community and regional banks, credit unions, money transmitters, and third-party service providers (such as credit card and payment processors)" who have experienced attempted breaches in recent years.

Attacks have come from a variety of actors, including unfriendly nation-states, hacktivists, organized crime groups, cyber gangs, and other criminals. The report states that "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."

Portions of the report were based on a survey of 154 depository institutions, with the following findings:

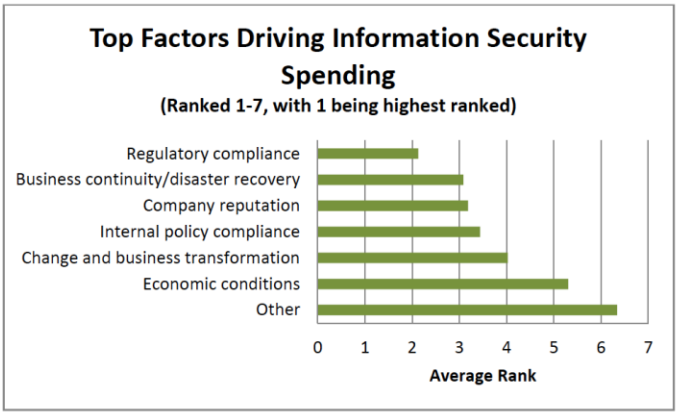
Most Institutions Manage IT Internally, Relying On Vendors For A Small Percentage Of Work. The vast majority of depository institutions surveyed, irrespective of size, rely on both internal and external resources to manage their IT systems. Of large institutions, 75% reported relying on a mix of in-house 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

Most Institutions Have The Basic Five Key Pillars Of An 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.

Most Firms Use Diversified 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.

Penetration Tests Rarely Occur More Frequently Than Annually. 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.



According to a survey conducted by the New York State Department of Financial Services, 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.

Cybersecurity Budgets Have Increased Or Remained Flat. 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 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.

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%).

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. 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%).

Long term planning more likely at larger institutions. 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.

The report ends by noting how the issue of limited resources will continue to plague small institutions. However, the Department is careful to note that the amount of money spent on a cyber program is by no means the best reflection of its strength. Specifically, "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."

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. For more on how big data can assist in risk assessments, see my prior post here.

Gregory S. McNeal is a professor specializing in law and public policy. You can follow him on Twitter @GregoryMcNeal or on Facebook.