AS THE PRIVACY WORLD TURNS... SO MUST YOUR CYBER RISK MANAGEMENT LENS
BY NADIA HOYTE, SENIOR VICE PRESIDENT

The concentration of popularly known cyber breaches has involved retailers and health care providers, but there is undoubtedly a greater concern in the financial services industry. As digital banking increasingly becomes customers’ preferred way of banking, and banks continue to develop and use Big Data in efforts to deliver greater customer satisfaction and brand superiority, the cyber threats in the industry will only intensify.

Financial institutions have a long history of attaching increased levels of confidentiality and privacy to bank records. However, the execution of this practice is often inconsistent and, in most cases, has not kept pace with the different types of growing cyber warfare. No longer are cybercriminals only nefarious fringe groups interested in gaining access to private information to commit identity theft. They also now include innovations by hacktivists interested in advancing their social or political agenda, state actors who want to cause damage to the U.S. financial system, as well as corporations interested in stealing another’s intellectual property and other business processes to gain competitive advantage.

The financial services sectors that may be impacted by this constantly evolving risk landscape include large banks to small banks, community banks, investment banks, retail banks and the myriad of subsectors in between. All of these entities store, protect, manage and/or transact a diversity of data. Given the interconnectivity of the internet, today’s rapid digital advances and social media platform, a cyber crisis at one or more banks can result in financial catastrophe, not only to customers and banks, but to the country’s financial system as a whole. It is no surprise then that regulatory agencies at all levels of federal and state government (and globally) have focused on cyber security guidelines and framework for financial institutions.

FEDERAL CYBER SECURITY GUIDELINES
The National Institute of Standards and Technology, in February 2014, recommended best practices that financial institutions of all sizes and other businesses that support critical infrastructure can use to evaluate, maintain and improve the resiliency of their network security. Similarly, the Federal Financial Institutions Examination Council is expected to release a new cyber security tool this quarter. The tool, which expands upon on a pilot program last year involving a review of 500 financial institutions, will assist banks in assessing their levels of cyber risk and will also recommend certain risk management measures banks can take to minimize their risks based on the self-assessment. While some have opined that the tool may become mandatory in the future, it is for now expected to be a voluntary (but recommended) self-assessment tool. Small banks without dedicated IT staff have the most to gain from the tool, but large banks may also derive significant benefit from the self-assessment.
Moreover, in October 2014, the U.S. Senate Committee on Banking, Housing and Urban Affairs issued a letter to the Department of the Treasury, the Federal Deposition Insurance Corporation, the National Credit Union Administration, the Federal Reserve System and the Office of the Comptroller of the Currency seeking more information on how each agency:
- Acquires information on cyber-attacks
- Shares information
- Coordinates and interacts with each other and with law enforcement, Homeland Security and the intelligence community

STATE CYBER SECURITY GUIDELINES
At the state level, the New York State Department of Financial Services (NY DFS) has been at the forefront of driving change around cyber security. In May of 2014, the agency conducted a survey of 154 financial institutions, including large global banks, community/regional banks and credit unions. Key findings from the survey showed that, regardless of size, most of the institutions rely heavily on third-party vendors. The respondents noted that their critical challenges included the speed of technological change, the increasing sophistication of the threats, the increasing reliance on third parties and the limited resources devoted to cyber security. Five months later, on October 21, 2014, the NYS DFS sent a letter to CEOs, GCs and CIOs of dozens of banks requesting information on third-party vendors’ information security risks. On December 10, 2014, NYS DFS delivered on its recommendations when it advised all Chartered/Licensed Banking Institutions that bank examinations will focus more attention on cyber security, including that of third-party vendors. Other states have followed suit by issuing similar guidance.

TURN THE LENS ON YOUR CYBER RISK MANAGEMENT PLAN
While there is no one-size-fits-all risk management strategy, the following practices can help financial institutions be better prepared to meet growing cyber threats as well as regulatory requirements and thus mitigate financial loss, operational risks and brand damage:
- **Establish and Enforce Cyber Governance**: Identify the C-Suite level and Board of Directors members responsible for the organization’s cyber risk governance framework, including operating processes and reporting structures. The governance framework should connect individuals and departments, such as disaster recovery, crisis management and business continuity within the organization.
- **Identify Vulnerabilities**: Understand where the organization’s data is stored, accessed and transmitted. Additionally, it is important to identify all individuals (including employees, vendors, service providers and/or customers) that may have access to the data. In this regard, vendors’ and other service providers’ contracts must be carefully reviewed and vetted to understand the potential cyber liability and indemnification issues that may arise from or because of these contracts.
- **Protect the “Crown Jewels”**: Identify the organization’s most valuable trade secrets, sources of revenue, intellectual property and other assets, as well as their location and who has access to the information/data.
- **Identify and Monitor Threats**: Invest in adequate IT resources and controls that will enable the organization to quickly identify and monitor threats.
- **Collect, Analyze and Report Information**: After threats are identified, collect and analyze the threats, prioritize and allocate resources to the greater threats, and provide leadership with the cyber risk information to allow them to quickly make informed decisions and proactively respond to attacks.
- **Plan and Respond**: A playbook that outlines the plans set forth above is critical along with testing the playbook through tabletop exercises and similar simulations of steps to be taken in the event of a cyber incident. The playbook should also include guidelines for technology upgrades and cyber liability insurance consideration, which the government has recommended should be part of financial institutions’ overall cyber risk management strategies.
HOW WILLIS CAN HELP
Through our proprietary and world-class risk assessment tools, including PRISM™, our experienced team of cyber risk brokers will work with your organization to identify your cyber risk, evaluate and stress test your current risk management programs, review your third-party vendor contracts and design an insurance program that is suitable for your organization based on your specific risk retention and risk transfer philosophy.

2 US Senate Committee on Banking, Housing and Urban Affairs letter dated October 21, 2014.
7 “Cyber insurance will not stop hackers, but it can help banks improve their broader cyber controls.”- Treasury Deputy Secretary, Sarah Bloom Raskin.

For additional information, please contact your Willis Client Advocate® or FINEX NA@WILLIS.COM.

For past issues of our publications on other topics of interest, please visit the Executive Risks website.

FINEX Alerts and Newsletters provide a general overview and discussion on a wide range of topics. They are not intended, and should not be used, as a substitute for legal advice in any specific situation.

Willis North America Inc.
Brookfield Place
200 Liberty Street, 7th Floor
New York, New York 10281-1003
United States
Tel: +1 212 915 8888

www.willis.com