NAVIGANT

PROTECTING AGAINST THE 21ST CENTURY JOHN DILLINGER

CYBERSECURITY

STEVEN RAMEY
Director
646.227.4432
steve.ramey@navigant.com

MATTHEW MOHWINKEL
Director
312.583.2183
matthew.mohwinkel@navigant.com

DUSTIN S. SACHS
Associate Director
713.646.5044
dustin.sachs@navigant.com

navigant.com

About Navigant

Navigant Consulting, Inc. (NYSE: NCI) is a specialized, global professional services firm that helps clients take control of their future. Navigant's professionals apply deep industry knowledge, substantive technical expertise, and an enterprising approach to help clients build, manage and/or protect their business interests. With a focus on markets and clients facing transformational change and significant regulatory or legal pressures, the Firm primarily serves clients in the healthcare, energy and financial services industries. Across a range of advisory, consulting, outsourcing, and technology/analytics services, Navigant's practitioners bring sharp insight that pinpoints opportunities and delivers powerful results. More information about Navigant can be found at navigant.com.

Infamous bank robber John Dillinger was once quoted as saying, "My buddies wanted to be firemen, farmers or policemen, something like that. Not me, I just wanted to steal people's money!"

For as long as human civilization has used money as payment for goods and services, criminals and criminal organizations have endeavored to obtain as much of it as possible, regardless of the means.

In the nineteen century, groups and people like the James-Younger Gang, Butch Cassidy, Thomas Ketchum, and countless others attacked trains and caused mayhem in the Wild West. Often, the outlaws got away with hundreds or thousands of dollars in paper money and gold.

In the twentieth century, robberies involving money typically occurred in banks. This is the era of Bonnie and Clyde, Baby Face Nelson, and John Dillinger. It was at this time that real time radio and news reports began to track these crimes. This was also the time when new law enforcement agencies like the Federal Deposit Insurance Corporation (FDIC) and the Federal Bureau of Investigation (FBI) were chartered.

Today, sixteen years into the twenty-first century, we are faced with a new form of bank robber. This new criminal is often not known by name, is never seen on camera entering a bank, and can cause more damage to the financial infrastructure of a country than his or her ancestors.

Robbery of banks and financial crimes in the digital era has taken a new form. In 2014, just as Bitcoin was at an all-time high of $1,200, Mt. Gox, the most active digital currency exchange was the victim of a $700 million dollar hack. In August of 2016, BitFinex, one of the largest digital currency exchanges reported a massive breach where hackers stole more than $65 million worth of bitcoin.

With the increased adoption of consumer mobile banking, digital currency, online anonymity, and digital banking technology, it has never been easier for a criminal to infiltrate a bank from the comfort of his or her living room, or from anywhere in the world.

According to the Privacy Rights Clearinghouse, in 2015, there were 266 reported data breaches. Of the total breaches in 2015, 41 involved entities in the financial services industry, second only to the 82 healthcare related breaches. What is more alarming, is that of the 159,937,976 records exposed as a result of the 266 data breaches, 120,604,832 (or 75%) of those records came from the 41 financial services related breaches.

As a result of the increased cyber threats, Andrew Cuomo, Governor of New York, announced on September 13, 2016 that the NY Department of Financial Services ("DFS") will enact Part 500 of Title 23[1] of the Official Compilation of Codes, Rules, and Regulations of the State of New York. This proposed regulation is the "first of its kind" related to cyber security in the financial services industry.

Once approved, entities governed by DFS regulations will be required to meet these standards starting on January 1, 2017. These standards include, but are not limited to, cyber security program requirements, conduct annual risk assessments, and hire dedicated information security leadership[2].

The new regulation will require, at a minimum that covered entities[3]:

1. Establish a Cybersecurity Program
2. Adopt a Cybersecurity Policy
3. Hire a Chief Information Security Officer (CISO)
4. Establish a policy and process to assess vendor cybersecurity
5. Conduct an annual risk assessment to include penetration testing and cyber security program review

The complexity of the new regulations will require the financial services sector partner with outside consultants and experts to ensure that all requirements are met and routinely audited. These routine assessments aid in providing an objective evaluation of the current state of the security profile, and compare that profile to industry guidance and best practices.

Establish a Cybersecurity Program

A cybersecurity program will provide a foundation and framework for the organization to govern security from procedures to personnel to training. The program will establish an organized and methodical approach for understanding the organizations risk appetite, securing the organization, identifying the correct personnel to lead practice areas, and create a hierarchy of responsibility.

Adopt a Cybersecurity Policy

The backbone of any cybersecurity program are the policies and procedures that govern the protection of information. Policies and procedures help employees and customers' guidance on controls surrounding information and access to that information. Without written policies, the constituent groups of the organization's management are left to choose their own methods for accomplishing tasks which may not align with the organizations risk appetite or be standard across the organization. Written policies provide accountability, guidance, and repeatability.

Hire a Chief Information Security Officer (CISO)

Just as a boat requires a captain, or a car requires a driver, an organization requires a leader familiar with the path forward to steer the initiative. The Chief Executive Officer is tasked with leading the entire company. The Chief Financial Officer is tasked with leading the financial performance of a company. The Director of Human Resources is tasked with overseeing employees. So, who is tasked with leading and protecting the company's critical IT assets and information?

As part of the new regulations, financial services companies will be required to hire a dedicated leader for cybersecurity. The Chief Information Security Officer ("CISO") will be directly responsible and accountable for the state of security in an organization. The CISO will be tasked with establishing a vision and strategy of the cybersecurity program, driving changes to the policies and procedures, and reporting to the Board of Directors at least bi-annually on the current state of the organizations security profile.

Establish a policy and process to assess vendor cybersecurity

It is rare for an organization to operate without assistance from a third party service. Facilities, maintenance, contractors, and IT infrastructure are just some of the areas that organizations outsource services. While outsourcing itself has many benefits, there are certain areas that are often over looked. Organizations fail to perform their due diligence on third parties. This might include a background check, prior business relationships, and history of the company or research of public records. Further, after executing their relationship, organizations may fail to properly adhere to access controls, creating a huge vulnerability and exposing the organization to risk.

1. To read more about the proposed regulation, visit http://www.dfs.ny.gov/legal/regulations/proposed/rp500t.pdf
2. To read more about Governor Andrew Cuomo's press release, visit http://www.dfs.ny.gov/about/press/pr1609131.htm
3. To read more about the regulation, visit https://www.governor.ny.gov/sites/governor.ny.gov/files/atoms/files/DFSCybersecurityRegulations.pdf

The introduction of a third party into an organization creates a new attack vector for adversaries. Establishing a vendor risk management program will allow an organization to rate, take on new relationships, and manage those relationships within the organizations threshold for risk. The program would have several elements that would create a yearly review of current relationships, background research of new relationships, and guidance from legal to IT when onboarding new vendors and negotiating contract terms.

Conduct an annual risk assessment to include penetration testing

The need for a risk assessment related to cybersecurity cannot be understated. It is impossible to develop a cohesive, forward focused plan without knowing the current state of affairs. Simply undertaking a "one-and-done" methodology will prove insufficient. Cyber threats are changing constantly, and the methods and tools necessary to detect and defend against attack are being updated just as fast. Therefore, a regular re-assessment must occur to ensure that new and emerging threats are mitigated or identified before they cause irreparable harm.

CONCLUSION

With consumers and regulators looking at cybersecurity with more scrutiny than ever before, the regulations proposed by the NY Department of Financial Services should position New York financial services institutions to have information security at the top of mind. By establishing the right leadership and strong policies and procedures, financial services organizations can demonstrate to all interested parties that they are serious about protecting personal and confidential information.