The Art of (Cyber) War: Cybersecurity Tactics for All Financial Institutions

James J. Giszczak | Tuesday, April 14, 2015

In today's rapidly changing technological age, with personal, financial and health information stored on devices, Internet, and in the cloud, cyber and data security controls and programs are critical. As financial institutions of every type and size - national, regional and community banks, thrifts, mutuals, credit unions, and non-bank lenders - increase their collection of personal information about their customers and employees, they become larger targets for a data privacy incident. Breaches can have a devastating effect to the bottom line of an organization and to its reputation. Institutions must be mindful of this battle on four fronts; external threats, intentional misappropriation by rogue employees, data accidentally lost or misplaced, and vendor negligence. Financial institutions are truly in a cyber war and proper tactics and strategy are essential for survival.

To quantify the risks, a recent study by the Ponemon Institute noted that the average total cost of cyber protection for financial service firms was an astounding $20.8 million in 2014. Because the size of institutions often dictates the resources available to stand guard against cyberattacks, middle market and smaller financial institutions present high-risk targets as cyber attackers believe smaller organizations have less sophisticated security controls and are therefore more viable targets from their point-of-view. Accordingly, such institutions face, among other cyberattacks:

- Malware attacks
- Hacking

- Ramsomware
- Insider threats
- Data or systems destruction and corruption
- DDoS and other communications disruptions
- Online credentials theft, fraud, and other business disruptions

Because of this, the Federal Financial Institutions Examination Council ("FFIEC")[1] requires that protections against such attacks be part of the formal cyber threat plans for organizations and ensuring that institutions have a comprehensive cyber resilience program will be a critical part of future regulatory examinations. Institutions must demonstrate an understanding of cybersecurity threats and how the institution's cyber plans identify, assess and address cyber risks.

To win this new war, cyber preparedness throughout the institution is critical. The recently created National Institute of Standards and Technology ("NIST") Framework creates a template that middle market and smaller financial institutions (as well as their directors and officers) can adapt to fit their organizational needs. See previous McDonald Hopkins Alert, *Board Members Beware: The SEC is watching*. The Framework is intended to establish industry standards and best practices for managing their cybersecurity risks; encouraging companies to be proactive and to identify and address complex issues and situations before institution-threatening, and (sadly) near-inevitable, cyber events occur. These best practices will likely become the baseline to assess legal or regulatory exposure, risk management, and insurance purposes:

- **Identify**: Develop an organizational understanding required to manage cybersecurity risk to systems, assets, data, and capabilities
- **Protect**: Develop and implement appropriate safeguards to ensure delivery of critical infrastructure services
- **Detect**: Develop and implement the appropriate activities to identify and avoid cyber events
- **Transfer**: Develop and implement an appropriate insurance program that deals with cyber and privacy events
- **Respond**: Develop and implement the appropriate activities to respond to a breach or other cyber event
- **Recover**: Develop and implement appropriate plans to maintain resilience and restore any capabilities or services that were impaired by a cybersecurity event

To achieve these objectives, institutions must take a deliberate approach and identify, assess, and address relevant cyber risks. This sort of analysis is often conducted by IT experts working with experienced legal counsel to ensure appropriate regulatory interests are understood and accounted for.

Identifying critical cyber assets and threats

The first tactic in identifying risk is to understand the types of information and knowledge the institution has and how such critical information is maintained as well as how it can be accessed (don't forget the Internet of Things). Next, an institution must analyze what internal and external threats to critical cyber assets exist. For example, do some employees have access to more data than is appropriate to their position? Does the manner of transfer subject data to outside threats (hacking, destructive malware, theft of online credentials, misuse of the Internet)? It is also important to understand the likelihood of attack through the internal and external threats and the potential damage that could be caused by a cyber

attack. This last element of analysis will better enable institutions to deploy resources.

Assessment and modification of existing controls and programs

Institutions need to review, and in many cases create, information security policies to protect critical cyber assets and guard against actual and potential threats. Institutions need to adjust and/or design appropriate security controls and plans to, among other things:

- Monitor and control access
- Properly encrypt and otherwise protect personally identifiable information (for customers and employees)
- Ensure that duties are properly separated amongst appropriate personal and, when appropriate, dual controls are in place
- Safely dispose of critical information
- Anticipate and avoid environmental hazards (fire, flood, etc.)

With respect to all of the aforementioned and other controls and plans, consistent staff training and evaluation are critical; a perfect plan is useless if it is simply in a drawer.

Third-party vendor management

An essential part of assessing existing controls and plans is reviewing vendor relationships and how vendors can affect an institution's risk profile. This process must be conducted by management and at the board of director level. Institutions must assess the complexity of each relationship, including:

- Legal and compliance risk (e.g., privacy, information security, Bank Secrecy Act/Anti-Money Laundering, fiduciary requirements)
- Volume of activity
- Potential for subcontractors (including the potential need for foreign support)
- Technology needs
- Access to the institution systems and information

Institutions should also specifically analyze the nature of customer interaction with the vendor and potential impact the relationship will have on consumers—including access to customers' confidential information and handling of customer complaints—and outline plans to manage these impacts. The scope and depth of vendor due diligence is directly related to the importance and magnitude of the institution's relationship with the third-party.

Setting expectations and establishing marching orders at the outset of the vendor relationship is critical. It is important to define, agree upon, and document expectations at the start of the engagement, and to review such expectations at least annually and after a change in services. This process is also consistent with regulator expectations and should be documented in your third-party vendor management policy. Specific contract topics to be thoroughly analyzed include:

- Scope
- Performance (including setting up specific metrics and benchmarks)
- Communication plans
- Risk assessment and audit rights (perhaps with triggers for same)
- IP rights

- Data security
- Indemnification
- Response to consumer complaints
- Regulator oversight
- Insurance
- Termination

After entering into a contract with a third-party, management should dedicate sufficient staff with the necessary expertise, authority, and accountability to oversee and monitor the relationship. Management should also ensure that employees charged with managing third-party relationships are trained with respect to the vendor relationship and monitoring procedures. Regular site visits are useful to understand the third-party's operations and ongoing ability to meet contract requirements.

Addressing cyber events

A critical aspect of any cyber preparedness plan is the development and implementation of an incident response protocol. The response protocol should address unauthorized access to or use of critical information that could result in substantial harm or inconvenience to others. The components of an effective program include:

- Assessment of the nature and scope of the incident and identification of what customer information has been accessed or misused
- Prompt notification to its primary federal regulator once the institution becomes aware of an incident involving unauthorized access to or use of sensitive customer information
- Notification to appropriate law enforcement authorities, in addition to filing a timely Suspicious Activity Report, in situations involving Federal criminal violations requiring immediate attention
- Measures to contain and control the incident to prevent further unauthorized access to or misuse of customer information, while preserving records and other evidence
- Notification to customers when warranted

Considering the importance of the controls, plans and protocols, institutions should routinely test their Incident Response Plan effectiveness and conduct tabletop exercises to evaluate existing response programs and make modifications as warranted. Institutions must understand that regulator examinations should not be considered system tests. Rather, examinations will be focused on evaluating whether management and boards understand how emerging cyber attacks could affect their business. Thus, institutions should be prepared to show their regulators that they have identified and understand the risks they face. Cyber preparedness is a process, not an event.

Board supervision – Increased involvement will decrease potential liability

Board members must truly fight the cyber war on multiple fronts, as regulators have indicated that directors and officers who fail to demonstrate knowledge of cybersecurity programs could be held individually liable for any lapses that occur. Accordingly, boards must work with management to assemble the proper teams and prepare plans to prevent and respond to any cyber breaches. A speech from Securities and Exchange Commission Commissioner Luis Aguilar in June 2014 made this point crystal clear:

> *When considering the board's role in addressing cybersecurity issues, it is useful to keep in mind the broad duties that the board owes to the corporation and, more specifically, the board's role in corporate governance and overseeing risk management. It has long been the accepted model, both here and around the world, that corporations are managed under the direction of their boards of directors.*

******

> *Good boards also recognize the need to adapt to new circumstances — such as the increasing risks of cyber-attacks. To that end, board oversight of cyber-risk management is critical to ensuring that companies are taking adequate steps to prevent, and prepare for, the harms that can result from such attacks. There is no substitution for proper preparation, deliberation, and engagement on cybersecurity issues. Given the heightened awareness of these rapidly evolving risks, directors should take seriously their obligation to make sure that companies are appropriately addressing those risks.*

Further, as noted by *The Wall Street Journal* in its March 30, 2015 article "Regulators Intensify Scrutiny of Bank Boards," institution regulators are "holding frequent, in some cases monthly, meetings with individual directors at the nation's biggest banks, demanding detailed minutes and other documentation of board meetings and singling out boards in internal regulatory critiques of bank operations and oversight." Per the article, the lead director at one national bank holds monthly calls with supervisors at the Fed and OCC while board committee leaders meet in person with supervisors several times a year. At another, Fed supervisors have attended some board committee meetings and directors meet regularly with supervisors outside of the formal board meetings.

Middle market and small institutions should expect similar treatment from their regulators, as -- per Camden Fine, president and CEO of the Independent Community Bankers of America -- "[d]irectors at small banks are also being pressed, including on how much they understand the kinds of loans banks are making and the associated risks…"

To properly prepare, institution management and directors should understand the NIST Cybersecurity Framework to ensure compliance. To that end, management and boards should be able to answer the following important questions:

- What is the board's familiarity with cybersecurity?
- Have the company's critical cyber assets been identified and are they properly protected?
- Can the board articulate its cyber risks and explain its approach and response to such risk?
- Has the board assigned clear roles and responsibilities for identifying, evaluating, monitoring, and responding to cybersecurity incidents?
- What are the company's crisis communications plans in the event of a cyber attack?
- Is the company properly managing third-party vendors who have access to their IT environment?
- Does the company's insurance cover a cyber event?

Board preparedness and planning can be critical to insulating directors from liability or at least minimizing damage. In a recent decision, *Palkon v. Holmes*, No. 14-CV-01234 (D.N.J.), a federal district court dismissed a shareholder class action against directors, the president/CEO, and general counsel of Wyndham alleging breaches of the fiduciary duties of care and loyalty and the wasting of company assets following three data breaches between April 2008 and January 2010 resulting in the theft of over 600,000 customers' credit card information. Critical to the court's decision making was the Business Judgment Rule, which the court found protected the board from liability because the organization:

- Held 14 quarterly meetings in which it discussed the cyber attacks, company security policies, and proposed security enhancements
- Appointed the audit committee to investigate the breaches, and that committee met at least 16 times to review cybersecurity
- Hired a technology firm to recommend security enhancements, which the company had begun to implement
- Had cybersecurity measures in place that had been discussed numerous times by the board prior to the security breach

Therefore, with respect to cybersecurity issues, courts are employing a more stringent standard and specifically analyzing how boards are identifying, assessing, and addressing cyber risk; making board preparedness and planning critical to insulating directors from liability. Boards should have a high-level understanding of the nature of cyber risks facing the institutions and the board or an appropriate committee needs to understand and oversee the systems (policies, controls and procedures) that management has put in place to identify, manage and mitigate risks related to cybersecurity, and respond to cyber events (including data breaches). Boards that conduct self-evaluations may want to survey their members to better understand the skill sets that they have and to better prepare them for understanding the skill sets they may want to seek out, or ensure proper education. Finally, public company boards need to provide oversight of related disclosures, and disclosure controls and procedures.

Conclusion

Critically, with increased regulations come increased regulatory scrutiny, enforcement actions, and litigation. It is likely that state and/or federal regulatory actions in conjunction with cyber security breaches will become common and will likely trigger subsequent shareholder derivative actions and/or other claims against directors and officers. Understanding and avoiding such regulatory actions will be critical to avoiding the significant costs associated with the ongoing cyber war: loss of critical cyber assets, reputational damage, potential for increased propensity for attack, fees paid to professionals to prepare and fight battles, and penalties from regulators; all can be devastating to an organization. Because financial institutions must comply with a myriad of state, federal and regulatory information security laws and standards, it is critical to have a multidisciplinary approach, involving the integration of multiple legal specialties and service teams, to data privacy and cybersecurity to limit institutional risk and exposure with proactive controls, plans and programs to minimize the risk of cyberattacks and data breaches. As Sun Tzu observed in The Art of War: "Victorious warriors win first and then go to war, while defeated warriors go to war first and then seek to win."

---

[1]The Council is a formal interagency body empowered to prescribe uniform principles, standards, and

report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Consumer Financial Protection Bureau (CFPB), and to make recommendations to promote uniformity in the supervision of financial institutions.

For more information, please contact the attorney listed below.

James J. Giszczak