WATKINS CONSULTING

Compliance Monitoring ♦ Litigation Support ♦ Forensic Accounting

CYBER THREATS TO THE FINANCIAL INDUSTRY KEEP GROWING

Contact: Michael Block
Executive Managing Director
Watkins Consulting, Inc.
888 Bestgate Road, Suite 401
Annapolis, MD 21401

mblock@watkinsconsulting.com
(240) 479-7273

DUNS: 792834293

NAICS Codes:
541219 – Other Accounting Services
541611 – Administrative Management and General Management Consulting Services
541618 – Other Management Consulting Services

www.watkinsconsulting.com

Cyber Threats to the Financial Industry Keep Growing

Introduction

J.P. Morgan, HSBC, Anthem, Home Depot, Target, the White House, and the State Department.

The list of companies, financial institutions, and government branches subject to cyber-attacks continues to grow. However, for all of the high profile attacks that we have read about, risk management and IT executives should be most concerned about undiscovered attacks. Cyber-attacks have been so common in recent years that the traditional wisdom has shifted from a mindset of if an attack will occur, to when. This is especially true of financial institutions, where cyber-attacks are becoming more frequent and sophisticated. Instead of a traditional, direct attack against a high-value server or asset, strategies have evolved that employ a patient, multi-step process; thereby blending exploits, malware, and evasion into a relentless, aggressive, and coordinated network attack. Where denial-of-service was once the most visible form of attack, perpetrators are constantly searching for creative new ways to extort money through fraud and cybersecurity vulnerabilities.

As consumers and businesses rely more on computers and smartphones to bank and shop online, vulnerabilities increase. Opportunities for exploitation increase exponentially due to the increase in interconnected services and the wealth of available information. This is due in part to the increased access points and connection types used to provide enhanced products and services (i.e. online and mobile banking, ATMs, cloud computing). These products and services have developed from consumer demand for streamlined end-user solutions. However, this demand for convenience carries a high cost for financial service providers as perpetrators develop techniques designed to target specific products and services. For example, financial institutions offering ATMs may be vulnerable to ATM "cash-out" scams.

With formal regulations in a continual state of flux, federal and state regulatory agencies (e.g., the OCC, FDIC, and New York State) have been proactively promoting cyber vigilance as part of their examinations of financial institutions. Consequently, it should be expected that during examinations, regulators will request information from institutions including:

- Copies of the institution's information security policies inclusive of an incident response plan and business continuity plan,
- Process for approval, review, and monitoring of the operations of third-party vendors,
- Organization chart of the institution's IT and information security functions and
- Qualifications of the institutional officers in charge of information security.

In order to comply with these requirements, financial institutions must define specific inherent risks regarding cybersecurity and then take action by designing and deploying responsive, best practices for mitigating those identified risks as part of the institution's overall risk management process. Accomplishing these tasks requires understanding, analyzing, and documenting the threats and vulnerabilities posed by the precise activities applicable to the type, volume, and complexity of its operations and product offerings. This analysis must involve executive level management and boards of directors to ensure the implementation of an effective, comprehensive policy. This policy must then be supported by clear, concise operational procedures designed to ensure compliance.

Mike Block
Email: mblock@watkinsconsulting.com
Phone: (240) 479-7273

Risk Management and the Control Environment

In 2014, The Federal Financial Institutions Examination Council (FFIEC)[1] conducted an assessment of over 500 community financial institutions to evaluate their preparedness to mitigate cyber risks and raise awareness to Chief Executive Officers (CEOs) and Boards of Directors (BODs) of factors to consider. While the level of preparedness varied, it was found that most financial institutions implement preventive controls to impede unauthorized access, have anti-virus and anti-malware tools to detect previously identified attacks, and have a process for implementing corrective controls to address previously identified vulnerabilities by installing patches on their primary IT system.

These results are reassuring and seem to indicate that financial institutions recognize their vulnerability to cyber-attacks. However, it was found that many institutions rely on media reports and third-party service providers to gather information on cyber events and vulnerabilities. This practice leaves a financial institution exposed to weaknesses of these vendors and may not be as effective as initially perceived, leaving the institution more vulnerable than suspected by its CEO and BOD. It is easy to understand why a financial institution would reply on third party information. The ability to identify, track, and predict cyber capabilities, requires obtaining information from multiple sources in real time in order to analyze and monitor current threats—an expensive and time consuming proposition; therefore, financial institutions must choose their vendors wisely.

To assist bank CEOs and BODs in meeting their duties to mitigate cybersecurity threats, the Conference of State Bank Supervisors (CSBS) issued in December 2014 **"Cybersecurity 101: A Resource Guide for Bank Executives"** (the Guide). The Guide compiles industry-recognized best practices for financial institutions regarding cybersecurity risk and is designed to elevate the involvement of executive management, including the CEO. This guidance is centered around five core elements set forth in the National Institute of Standards and Technology's (NIST's) 2014 Cybersecurity Framework. Specifically:

- **Identify** internal and external cyber risks,
- **Protect** organizational systems, assets, and data,
- **Detect** system intrusions, data breaches, and unauthorized access,
- **Respond** to potential cybersecurity event and
- **Recover** from a cybersecurity event by restoring normal operations and services.

These core elements are briefly described below.

Identification of Internal and External Cyber Risks

The first core element is identification of cybersecurity risk posed by the financial institution's activities, data connections, and operational procedures—a process referred to as 'Information Classification.' Information Classification involves determining what are the most critical and important elements to the institution's operations, then requiring specific security classifications, access controls and authentication controls for those

[1] The FFIEC members are the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation (FDIC), the Office of the Comptroller of the Currency (OCC), the Consumer Financial Protection Bureau (CFPB), the National Credit Union Administration (NCUA), and the State Liaison Committee.

Mike Block
Email: mblock@watkinsconsulting.com
Phone: (240) 479-7273

elements. This flexible approach recognizes that not all information assets need to be protected the same way—as information disclosure ramifications will vary from severe to no impact.

This identification requires a risk assessment that includes, but is not limited to, the classification of the most critical information assets based upon sensitivity ranking. These assets can be people, tangible or intangible property and data.

In addition to the classification of the information assets, the institution needs to identify the threats and vulnerabilities, both internal and external, to the information assets. Some of the tools utilized to identify potential vulnerabilities include scanners that can probe well-known network protocols and methods.[2]

Protection of Organizational Systems, Assets, and Data

Protection of organizational systems, assets, and data is designed to ensure that the institution has controls in place to mitigate cyber threats. This includes the appropriateness of policies and procedures, including, but not limited to,

- Staff and customer authentication,
- Access controls for sensitive and critical information,
- Data security based upon the complexity of the institution's operations,
- Review of third party providers to ensure they are taking appropriate steps to protect the security and confidentiality of information,
- Maintenance of secure hardware and software configurations,
- Use of a firewall and unified threat management tools and
- Proper training and knowledge of personnel to implement and effectively manage all protocols.

Detection of System Intrusions, Data Breaches, and Unauthorized Access

Controls and sensors are tools that prevent or limit unauthorized access to computer networks, systems, or information. These controls and sensors can include an array of systems such as intrusion detection systems, network behavior anomaly detection tools, security information and event management systems, and configuration management tools. These tools gather and analyze information to identify possible security breaches from both inside and outside an organization. They are designed to detect anomalies enabling timely responses to cyber-attacks. Consequently, establishing a measure of "normal" operations is the basis of any detection strategy. To remain effective, these detection tools and associated processes must be regularly upgraded to enable continuous monitoring and real-time detections of constantly evolving threats.

[2] Per the Guide, additional external resources include the Financial Services-Information Sharing and Analysis Center (FS-ISAC). The FFIEC issued a statement recommending that financial institutions participate in the FS-ISAC as part of its process to identify, respond to, and, mitigate cybersecurity threats and vulnerabilities.

Response to Potential Cybersecurity Events

Institutions should develop an incident response plan which includes forming a response team that coordinates the efforts between the bank's departments as well as outside legal counsel and consultants. The plan should have clearly defined steps, timelines, and checklists including how a data breach should be communicated to customers, regulators, law enforcement, and other stakeholders. The institution's plan should include conducting preparedness training.

Recovery from a Cybersecurity Event by Restoring Normal Operations and Services

After the institution responds to a cyber-attack, that institution must recover. A thorough, well-documented and tested recovery component of the Business Continuity plan can significantly shorten the recovery period. An effective plan not only resolves the operational components to get the institution functional again but also includes provisions, processes and procedures for restoring confidence in the recovered systems and data. Depending upon the breach, this may include rebuilding the infrastructure (i.e. servers, databases, networks), restoring the data, reconnecting services, determining what improvements are necessary to prevent similar attacks from recurring, analysis of the effectiveness of the response plan and the response team. There is no time during the crisis of a cyber-breach to develop this plan, as time is of the essence. The time and money saved by having an effective plan, and team, in place prior to a breach is cost effective.

Watkins Wisdom for the Cyber Security Challenge

Regulators are making cybersecurity a priority for enforcement. Ever more sophisticated cyber-criminals are focusing on stealing and monetizing data. The potential risks faced by the finance industry are increasing exponentially. Fortunately, by proactively putting the appropriate cyber security measures in place, financial institutions can reduce the risk of cybercrime and the cost of complying with potential cyber regulations. In a period of profit margin compression, where spending trade-offs must be made, every firm needs to make cyber security a priority. First, the CEO, along with the BOD, must establish a clear and concise cyber security policy. Second, senior level management must develop, test and implement operational procedures designed to enact this policy. Next, the institution must construct a detailed business continuity plan designed to ensure continuation of business operations and procedures in the event of a breach or other catastrophic event. Finally, the institution must adopt a strategy of on-going training, monitoring and vigilance, empowering every employee to identify and report suspicious activity.

Mike Block
Email: mblock@watkinsconsulting.com
Phone: (240) 479-7273