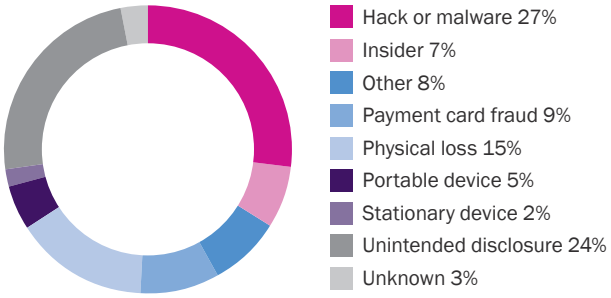
Data Privacy and Information Security for Small Banks

Threats facing small banks

The financial industry is threatened by a wide variety of cyberattacks that aim to steal financial data from institutions as well as their clients. Cybercrime is considered to be the second greatest economic criminal threat to financial institutions.[1] One institution concluded that the financial services industry experienced the highest average annualized cost as a result of cybercrime.[2]

As outlined below, Beazley's financial institution clients encountered a range of threats: from sophisticated hacking and malware attacks, to unintended disclosures attributable to simple human error – e.g., misfired emails and faxes, lost laptops, USB, and paper records.

Financial Services Incidents, 2015



Breaches managed by Beazley Breach Response (BBR) Services

Hacking and malware incidents, in particular, evidenced a sharp rise in volume from 2014 (18% of all reported incidents) to 2015 (32% of reported incidents). While hacking incidents can often involve a sophisticated attacker, many are still the result of simple strategies designed to trick users into clicking on malicious links and attachments in emails.

Beyond actual compromise of information, financial institutions are also at risk of business email compromise (BEC) and cyber extortion in the form of ransomware and distributed denial of service (DDoS) attacks. BEC is a scam targeting businesses of all sizes that regularly perform wire transfer payments, particularly with foreign suppliers.[3] The scammer compromises a legitimate business email account through either social engineering or computer intrusion in order to request a wire transfer.[4] According to the FBI, between January and August 2015, there was a 270% increase in identified victims and exposed loss.[5]

Cyber extortion is also becoming more and more prevalent. Ransomware, usually a variant of the CryptoLocker or CryptoWall virus, encrypts files on a computer's hard drive and any shared drives to which the computer has access. Users' computers become infected by opening email attachments containing the malware, or by clicking on a compromised website or pop-up window.[6] Once the computer is infected, the user is directed to a page that demands a ransom payment within a certain amount of time and contains detailed instructions about how to purchase the Bitcoins to pay the ransom.[7] Beazley insureds reported 43 ransomware incidents in 2015. And with 42 reports of ransomware within the first three months of 2016, Beazley is on track to see many more this year. In addition, small banks with online banking capabilities will be at risk of DDoS attacks. A DDoS attack can be leveraged by criminals to disrupt IT operations or even halt IT systems all together for a ransom. Often, attackers assemble botnets – networks of infected computers – to generate the traffic to paralyze a site.[8] This form of cyber disruption can target networks, a particular range of protocols, or applications.

Breach examples at small and medium sized enterprise (SME) financial institutions serviced by Beazley

Spear-phishing scheme

A small bank's systems were potentially compromised due to a spear-phishing scheme that resulted in a fraudulent wire transfer and potential exfiltration of emails with customer personally identifiable information (PII). BBR Services recommended forensics and privacy counsel, and together they concluded (after an extensive manual review of data) that the insured was legally obligated to notify approximately 3,000 individuals.

Stolen unencrypted employee laptop

A financial services company's employee had an unencrypted laptop stolen from her automobile. BBR Services quickly connected the company with privacy counsel and forensics to assist with assessing the information on the laptop based on a recent backup. Once that analysis was complete, the organization learned that the laptop had contained protected information on approximately 6,000 individuals. BBR Services continued to assist by coordinating notification and call center services, as well as credit monitoring, for the affected individuals since the laptop contained their social security numbers (SSN).

Widespread malware

A credit union discovered malware on the majority of its computers. The company's HR director's account was accessed and money was electronically transferred from a bank account. BBR Services coordinated the response, connecting the insured to privacy counsel and a forensic firm. Because the forensic firm was unable to rule out access to all member files, BBR Services connected the credit union to a notification and call center services vendor to notify all 140,000 members and offer credit monitoring.

Missing unencrypted backup tapes

A small bank discovered two backup tapes were missing. BBR Services introduced the bank to privacy counsel and a forensics firm. Forensics evaluation uncovered the tapes likely contained PII for 84,000 individuals. BBR Services coordinated a response, including notification and call center services.

Bank hack

A bank experienced a sophisticated malware attack, where hackers were in the bank's system for at least six months. The hackers set up fake accounts and money was withdrawn from the bank from those fake accounts. BBR Services coordinated a response involving privacy counsel and forensics. The forensic investigation was extremely expensive due to type of malware. BBR Services set the bank up with a notification and call center services vendor to notify and provide credit monitoring to about 30,000 individuals whose credit card numbers, SSNs and driver's license numbers may have been exposed.

Unintended disclosure by email

A credit union employee inadvertently sent an email to a third party outside the company which contained credit union member names, account numbers and SSNs. Approximately 650 members were affected, half of which included SSNs and the other half included just names and account numbers. BBR Services connected the credit union with privacy counsel, but no mailing was necessary based on the legal analysis.

State breach notification statutes and attorneys general

When faced with the type of incidents discussed above, as many as 47 different state breach notification statutes govern a financial institution's legal obligation to investigate and respond. These statutes are a messy patchwork of at times conflicting standards, with significant variations in the scope of data covered, the definition of what constitutes a "breach" in the first place, and the mechanics of how consumers are to be notified.

What's more, depending on the size of the breach, a company may have to notify various state attorneys general (AG) and potentially be subject to fines, and lengthy regulatory investigations. Below are some examples of financial institution settlements with state attorneys general.

California AG

On August 28, 2013, the California AG settled with Citibank, N.A. for $420,000 (an additional $55,000 went to the Connecticut AG) over a breach affecting over 80,000 California account holders.[9]

Massachusetts AG

In December 2014, the Massachusetts AG settled with TD Bank for $625,000 after a 2012 data breach affected 90,000 Massachusetts customers (260,000 customers total).[10]

Multistate Settlements

In October 2014, TD Bank agreed to pay $850,000 in a multistate settlement for its 2012 data breach that affected 260,000 customers.[11]

Other regulatory issues

In addition to state notification requirements, financial institutions face a web of regulatory enforcement at the federal level under the Gramm-Leach Bliley Act, as implemented by the Federal Trade Commission's (FTC) Privacy Rule. Moreover, publically traded companies and securities firms face additional layers of complex regulatory oversight and enforcement, via the Securities and Exchange Commission ("SEC") and the Financial Industry Regulatory Authority, Inc. ("FINRA"). An overview of recent activity by some of these regulatory agencies with respect to data privacy and security follows below.

SEC settlements

On September 22, 2015, the SEC announced that it reached a settlement with a St. Louis-based investment adviser, R.T. Jones Capital Equities Management, over charges that R.T. Jones failed to establish the required cybersecurity policies and procedures in advance of a 100,000 person breach. The SEC investigation found that R.T. Jones violated the "safeguards rule"; federal securities laws require investment advisers to adopt written policies and procedures reasonably designed to protect customer records (Rule 30(a) of Regulation S-P under the Securities Act of 1933). R.T. Jones settled for a $75,000 penalty, neither admitting nor denying the SEC's findings.[12]

On April 7, 2011, the SEC settled with Marc A. Ellis, the Chief Compliance Officer for GunnAllen Financial (broker-dealer), for $15,000 for willfully causing GunnAllen's violations of Rule 30. The settlement lists a number of violations, including multiple stolen laptops and a terminated employee's misappropriation of another employee's password credentials.[13]

On September 11, 2008, LPL settled with the SEC for $275,000 for a failure to safeguard customer information and an inadequate response to known deficiencies and anticipated security threats. Between July 17, 2007 – February 15, 2008, unauthorized person(s) logged into LPL's trading platform and may have had access to 10,000 customers' information.[14]

CBSL451_US_05/31

FINRA settlements

On May 22, 2015, FINRA settled with financial firm Sterne Agee for $225,000 for failing to safeguard customer information as required by Rule 30. An IT employee of Sterne Agee lost an unencrypted laptop containing information for 352,551 customers. FINRA faulted Sterne Agee for having recognized the need for encryption of laptops back in 2009 but failing to implement before loss of the laptop in 2014.[15]

On April 9, 2012, FINRA settled with Morgan Keegan & Company, Inc. for $150,000 for failing to safeguard customer information as required by Rule 30. Specifically, Morgan Keegan was alleged to have failed to detect, monitor for and timely report customer data breaches.[16]

On November 21, 2011, FINRA settled with Wells Investment Securities, Inc. for $300,000 for a number of claims, including failure to safeguard customer information as required by Rule 30. A laptop was stolen from an employee's car and contained information regarding 37,864 customers.[17]

On April 12, 2010, FINRA fined broker-dealer D.A. Davidson & Co. $375,000 for failure to protect customer information. D.A. Davidson did not have adequate safeguards in place to prevent an international crime group from hacking into its system and improperly accessing the information of 192,000 customers.[18]

On April 28, 2009, FINRA settled with Centaurus Financial, Inc. for $175,000 for failing to safeguard customer information as required by Rule 30. The breach impacted only 1,400 customers.[19]

FTC settlements

While the FTC has been active in regulatory enforcement of Section 5 of the FTC Act (unfair or deceptive acts or practices), it has not yet issued fines or penalties along with the 20-year audits. This could change in the future.

The FTC settled with two debt brokers in April 2015 for posting unencrypted documents online containing PII. Under the settlements, the defendants must establish and maintain security programs that will protect consumers' sensitive personal information. In addition, the companies must have their security programs evaluated both initially and every two years by a certified third party for 20 years.

Conclusion

Financial institutions both large and small are threatened by a wide variety of cyberattacks. With incidents of hacking and cyber extortion on the rise, companies must be vigilant in safeguarding PII and aware of the costs of incident response. When faced with a potential data breach, working with outside counsel is often necessary to navigate the legal and regulatory landscape at both a state and federal level. Other vendors, such as forensic firms, notification and call center services vendors, and identity fraud monitoring companies, may be needed to complete the response. Finally, entities that experience a data breach may face fines from a variety of regulators, including state attorneys general, the SEC and FINRA.

By Lauren Winchester & Paul Nikhinson
Privacy Breach Response Services Managers, Beazley

1 PricewaterhouseCoopers LLP, Threats to the Financial Sector: Financial Services sector analysis of PwC's 2014 Global Economic Crime Survey, available at http://www.pwc.com/gx/en/economic-crime-survey/downloads.jhtml.

2 Ponemon Institute, 2015 Cost of Cyber Crime Study: United States, dated October 2015, available for free download at http://www8.hp.com/us/en/software-solutions/ponemon-cyber-security-report/index.html?jumpid=va_fwvpqe387s. Ponemon estimates the cost of a data breach (across industries) has increased from an average of $159 to $174 per record. See http://www.ponemon.org/blog/cost-of-data-breach-grows-as-does-frequency-of-attacks.

3 Federal Bureau of Investigation, Public Service Announcement: Business Email Compromise, dated August 27, 2015, available at https://www.ic3.gov/media/2015/150827-1.aspx.

4 Id.

5 Id.

6 Federal Bureau of Investigation, Ransomware on the Rise, dated January 20, 2015, available at https://www.fbi.gov/news/stories/2015/january/ransomware-on-the-rise.

7 Id.

8 See https://www.neustar.biz/services/ddos-protection (we are using this page for informational purposes, not as an endorsement of neustar's services).

9 See https://oag.ca.gov/privacy/privacy-enforcement-actions.

10 See http://www.wsj.com/articles/td-bank-to-pay-625-000-in-data-breach-settlement-1418151389.

11 See http://www.wsj.com/articles/td-bank-to-pay-850-000-in-data-breach-settlement-1413391988. See also http://www.law360.com/articles/606359/tracking-state-data-protection-enforcement-in-2014.

12 See http://www.sec.gov/news/pressrelease/2015-202.html.

13 See http://www.sec.gov/litigation/admin/2011/34-64220.pdf.

14 See http://www.sec.gov/litigation/admin/2008/34-58515.pdf.

15 See http://disciplinaryactions.finra.org/Search/ViewDocument/51064 (No. 2014041619501).

16 See http://disciplinaryactions.finra.org/Search/ViewDocument/31594 (No. 2010022554701).

17 See http://disciplinaryactions.finra.org/Search/ViewDocument/25628 (No. 2009019893801).

18 See https://www.finra.org/newsroom/2010/finra-fines-da-davidson-co-375000-failure-protect-confidential-customer-information.

19 See http://disciplinaryactions.finra.org/Search/ViewDocument/15737 (No. 2007009780901).

20 See https://www.ftc.gov/news-events/press-releases/2015/04/debt-brokers-settle-ftc-charges-they-exposed-consumers.