Cyber Liability: Financial Institutions

Can you think of any entity today that maintains more personal information than a financial institution? Take a moment to ponder the depth of information requested when you apply for a mortgage/refinance, a college student loan or even a car loan. In particular, banking institutions have become more stringent in their lending practices and have required more personally identifiable information in order to facilitate the loan process. The vast amount of information collected may cause some to believe that their local banking institution is operating as a data storage warehouse as well as a bank.

Cyber Issues Every Financial Institution Should Know About

Securities Exchange Commission (SEC) Oversight

On October 13, 2011, the Securities and Exchange Commission “SEC” weighed in with CF Disclosure Guidance: Topic No. 2 “Disclosure Guidance,” addressing the situation faced by public companies in the United States. It is important to note this guidance is not a rule, regulation or statement. Nor has it been approved or disapproved by the Commission. Nevertheless, it provides guidance to assist in assessing what, if any, disclosures should be conveyed about cyber security matters. This SEC disclosure guideline could have an impact on financial institutions as the heightened level of awareness that this brings may expand to publicly traded and nonpublicly traded financial institutions through additional banking regulations.

Distributed Denial-of-Service Attacks

Most of the largest U.S. banks have acknowledged Distributed Denial-of-Service (DDoS) attacks in regulatory filings or annual reports. DDoS results when hackers flood a computer system with information to shut it down. Most banks said they didn’t have material losses or that customer data wasn’t stolen. Only one major banking institution among the largest U.S. banks has disclosed losses from DDoS and other cyber attacks to investors this year. Banks give DDoS their top concern because they do not want a DDoS to cause prolonged website outages that may damage their reputations or have their network data compromised due to a weakened security system.

Cyber Attack Nets $45 Million From Thousands of ATMs Worldwide

An alleged international gang of cyberthieves managed to steal $45 million from thousands of ATMs in carefully coordinated attacks conducted in a matter of hours. It was disclosed in a four-count indictment that eight members of an alleged gang in New York City stole approximately $2.4 million from nearly 3,000 ATMs across the metropolitan area. The New
York cell was just one part of a coordinated global heist in which $45 million was withdrawn from cash machines in 27 countries.

This was one of the largest 21st century cyber-thefts yet uncovered, according to federal authorities. The attacks are known in the cyber underworld as “Unlimited Operations”—because using sophisticated computer-hacking techniques enabled those involved to gain access to virtually unlimited proceeds. The schemes involve hacking into the computer systems of credit card processors, stealing information involving prepaid debit card accounts and eliminating the withdrawal limits and balances of those accounts. The moves enable international organized crime cells that work in swift, surgically coordinated attacks to withdraw unlimited amounts of cash from ATMs before the operations are shut down.

Continued Increase in Breach Activity
Verizon released recently their 2014 Data Breach Investigation Report (DBIR), which was compiled by a global team of government and private organizations analyzing computer security incidents over the past year. This annual report shows that companies of all sizes and types are likely to experience some sort of data breach attack, if they haven’t already, and highlights the concern that financial institutions should have over the safeguarding of personally identifiable information. According to the report, no industry was immune, but financial organizations bore the brunt of these attacks, alone accounting for 37% of known data breaches. Further, 75% of all attacks were driven by financial motives. Finally, the 2014 DBIR data continues to show that the majority of breaches still consistently come from outside threats, despite conventional wisdom to the contrary.

Cyber Solutions for Financial Institutions
Gallagher Cyber Liability offers meaningful solutions to financial institution clients seeking peace of mind and balance sheet protection from the ever-increasing scrutiny to properly safeguard and secure personally identifiable information. The increasing potential for a cyber liability event requires financial institutions to fully understand their exposures, create a proactive plan to mitigate cyber liability and structure an appropriate incident response plan to address cyber liability events. Even the most vigilant network security and most comprehensive privacy policies are still vulnerable to hackers, rogue employees, social engineering and human error.

Solutions include:
- Gallagher Cyber Risk Management Portal
  - Breach preparedness plans
  - Access to respected breach response attorneys and notification and credit/identity monitoring services
- Contract Review
- Insurance Gap Analysis
- Cyber Liability Insurance
  - Privacy/Network Security Liability
  - Breach response
  - Cyber regulatory defense/fines and penalties
  - Cyber extortion
  - PCI Fines
  - Network business interruption
  - Media Liability
  - Technology Errors & Omissions
- Limits Analysis, Benchmarking & Program Design

Arthur J. Gallagher & Co.