COMMUNITY INSTITUTION & ASSOCIATION RISK SUMMARY

TLP: Green CTL: Guarded WEEK OF MARCH 23

This Week's Top Risks

- Cyber Insurance – How Much *is* Enough?
- FBI Alert: Commercial & Government organizations at Risk of Cyber Espionage

Cyber Threat Level

The Cyber Threat Level is remaining at **GUARDED**. There are no credible threats posed to the financial services sector at this time. FS-ISAC recommends members maintain a guarded level of awareness, and apply critical updates as soon as possible. Update AV and IDS/IPS signatures and ensure constant diligence in monitoring and quick response to any malicious events.

CYBER INSURANCE – HOW MUCH *IS* ENOUGH?

Summary:

Premera Blue Cross announced on Tuesday, March 17, 2014 that it was a victim of a cyberattack that may have exposed medical data and financial information of 11 million customers.

The attackers may have gained access to claims data, including clinical information, along with banking account numbers, Social Security numbers, birth dates and other data. Acknowledgement of the breach comes 10-months following the attack that occurred on May 5, 2014.

Last week open sources revealed that Target agreed to a $10 Million settlement for the breach involving up to 40 million consumers.

With the rise in number of high profile breaches, cyber insurance is a topic that FIs should strongly consider as part of their strategic plan.

How Much Insurance *is* Enough?

As reported last week, Anon's report on the average cost of a data breach stated: "the average cost for such a breach is $7 million. Yet, **the average portion of that cost borne by cyber-risk insurance is just $3 million, leaving a $4 million gap**, since damage to a brand's reputation and "future lost sales" after a business interruption generally aren't covered."

The current question involves just how much insurance is enough is sufficient recourse to make the FI whole? The answer: there is no one size fits all for FIs.

One reason is that the threats continue to change and increase, making it difficult for underwriters to properly assess the environment. It is one thing to build a premium model involving certain types of data such as a breach of social security numbers and other personally identifiable information, but due to insufficient history it can be difficult to assess the value of unrealized future earnings.

Risk to Community Institutions:

While there is a gap between coverage and loss, arguably a measure of insurance is preferable to having no or insufficient cyber insurance. Clearly then, FIs are faced with the following risks:

- **Financial**. A failure to assess the value of corporate, information and physical assets place the FI at risk of financial loss. The risk increases for smaller FIs that may lack sufficient resources to perform a thorough assessment.
- **Legal**. In addition to losses associated with fraud, victims may file lawsuits resulting in further loss and tarnish the reputation of the FI.
- **Regulatory**. The FFIEC states it is important for management to understand the financial institution's inherent risk to cybersecurity threats and vulnerabilities when assessing cybersecurity preparedness.

Remediation:

- While there is currently no requirement for FIs to have cyber insurance, it makes good business sense. If not already done, FI Risk Management Committees should contemplate FFIEC recommendations concerning insurance.
- When evaluating the need for insurance to cover information security threats, financial institutions should understand the following points:
  - Insurance is not a substitute for an effective security program.
  - Traditional fidelity bond coverage may not protect from losses related to security intrusions.
  - Availability, cost, and covered risks vary by insurance company.
  - Availability of new insurance products creates a more dynamic environment for these factors.
  - Insurance cannot adequately cover the reputation and compliance risk related to customer relationships and privacy.
  - Insurance companies typically require companies to certify that certain security practices are in place.
- Financial institutions can attempt to insure against these risks through existing blanket bond insurance coverage added on to existing policies in order to address specific threats.
- When considering supplemental insurance coverage for security incidents, the institution should assess the specific threats in light of the impact these incidents will have on its financial, operational, and reputation risk profiles.

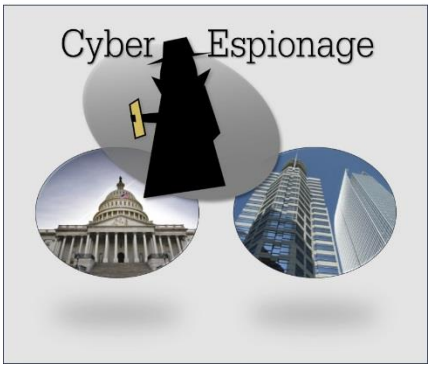
Reference Material:

- Additional information regarding insurance can be found at the FFIEC web site:

  http://ithandbook.ffiec.gov/it-booklets/information-security/security-controls-implementation/insurance-.aspx

---

FBI Alert: Commercial & Government organizations at Risk of Cyber Espionage



Summary:

The FBI has obtained information regarding one or more groups of cyber actors who have compromised and stolen sensitive business information from US commercial and government networks through cyber espionage.

Analysis indicates a significant amount of the computer network exploitation activities emanated within China. Any activity related to these groups detected on a network should be considered an indication of a compromise requiring extensive mitigation and contact with law enforcement.

These groups have been observed across a variety of intrusions leveraging a diverse selection of tools and techniques to attempt to gain initial access to a victim. Leveraging their initial access to gain further access to protected information resources on other systems, they collect legitimate credentials or even misuse legitimate certificates introduced into that compromised system or endpoint. These techniques include:

- Using VPN credentials acquired during previous intrusions.
- Scanning for web-facing devices that are not fully patched and for which there are publically known vulnerabilities.
- Using malicious documents in spearphishing emails leveraging older vulnerabilities.
- Using a more sophisticated variant of a Remote Access Trojan to harvest information.

Risk to Community Institutions:

- The risk to FIs lie within the vulnerability of their commercial client accounts, especially those with no information security personnel and inexperienced or outsourced IT personnel.
- Commercial clients that have military contracts may be susceptible to attacks in order to destroy, disrupt or steal sensitive information that could jeopardize US interests and national security.

- Compromised client accounts may enable the attacker to perform account reconnaissance, change administrator privileges, add users, initiate large transfers of funds to disrupt US commerce and support Chinese interests.
- Financial, legal and regulatory risks could impede financial earnings and lead to a devalued place in the market where they do business.

Remediation:

- While some of the information is at a technical level, board and leadership teams will want to ensure that their CISO & Corporate Security personnel devise a communication plan to share the information with their commercial clients as appropriate. (FS-ISAC member to access below Tracking ID)
- Develop an ongoing commercial security awareness information vehicle which advises commercial clients about security threats and recommends industry best security practices.
- Educate internal staff of ongoing threats to customer information and their assets.

Reference Material:

- FS-ISAC Tracking ID: 914205.

Questions:

If you have any questions about this week's report, please contact Community Institution & Associations.