March 2016

Time to Evaluate Your Cyber Insurance Coverage

Earnings Performance Consulting

M&A Integration | Risk & Compliance

For the Intelligent Banker

2016 Intelligent Bank Management Series

The 2016 Intelligent Bank Management Series focuses on insights, strategies and development priorities for improved profitability, operating efficiency, compliance and risk management at U.S. financial institutions.

Hello Mr. Insurance Agent, Am I Covered for a Data Breach?

If you have not already done so, a pro-active understanding and evaluation of insurance coverage protecting your financial institution from data compromises, digital theft and extortion and other cyber events is certainly warranted.

Please allow the presentation of the following analogy. If you have a car, chances are that you are required to carry a minimally prescribed insurance policy as dictated by your state's motor vehicle laws. Typically, this is a policy written to protect anyone that you might injure, property you might damage or yourself, while driving your car. It is likely a basic automotive insurance policy that does not cover your own automobile from damage. If you add comprehensive or collision coverage, you will have coverage for repairs or replacement to your own vehicle if it is damaged, destroyed or stolen. As such, it is only a policy with comprehensive or collision coverage that provides the peace of mind as a car owner that if something bad happens to your car, you have limited loss exposure for your own vehicle.

Think of the customer data that you hold as an asset, with intrinsic value just like the car in the previous example. When your organization holds the risk for data loss, either from a breach that compromises the security of confidential data, or if an uninvited saboteur threatens, destroys or prevents you from accessing your data, isn't insurance an effective risk and loss mitigation strategy? Of course it is. The key question is what are the right policy types and coverage? As the article subtitle implies, it may be too late to understand and verify your coverage after an event has occurred.

Do You Have Coverage?

If you, as the executive in charge, face the unfortunate call to your insurance agent to determine if you have coverage for a data breach or an electronic-originated financial loss, the likely response from your insurance agent is that coverage may come from one or more of several policy types, depending upon the type of claim:

- A Cyber Insurance policy could provide coverage for claims that are related to theft of customer personal information.
- The Financial Institution Bond could provide coverage for claims that are related to the

electronic theft of money from the bank.

- A Debit Card endorsement to the Bond would provide coverage for losses related to Debit card fraud. This coverage is also known as Plastic Card coverage.

- Social Engineering insurance may provide coverage if a bank employee acting in good faith makes a payment to a masquerading criminal.

- The D&O policy may be implicated if there is a data breach involving a bank that has registered investment advisors.

There are a number of considerations in determining your coverage needs. Both the landscape of electronic theft of data and financial losses are evolving as are insurance coverages. For example:

- Does your current policy cover a demand for payment to prevent an attack on your website that could make your institution unavailable to the internet and harm your reputation with your customers? A loss has not occurred.

- What about if a fax was received with apparent authority from a customer, and a wire is sent from a customer's account to an account outside US law enforcement jurisdiction, and is not recoverable? Are you covered? Social engineering to 'snooker' an employee into providing criminals funds is a hotly debated coverage topic today, with several highly disappointed institutions finding they lacked coverage.

- A federal regulator recently fined a financial services company for failing to adopt policies and procedures that are reasonably designed to safeguard customer records and information. Is this fine a covered claim? What about a shareholder suit brought against management and directors as a result of the fine?

As to a specified Cyber Insurance policy or rider, what is defined as your coverage? You would expect to find the cost of notification and credit monitoring after detection of a breach of your secure environment.

- What about the costs to employ forensic expertise to determine the root cause and restore or rebuild compromised technology?

- What are your limits and will they enable you to reasonably recover the costs of a cyber event, which has an extremely wide range of cost per account running from $30 to $200.

- Is coverage limited to your customers, or all confidential data you may hold that has been compromised (closed relationships, denied loan applicants and prospect data as examples)?

- Does your policy coverage extend to your third-party providers who hold your protected sensitive data within their data processing infrastructures?

- Are there any requirements for you or restrictions with regards to provided third-party coverage?

Another consideration with these policy types is when they were last visited and renewed. It tends to be tradition with some organizations to complete a multi-year renewal for coverage. While this is certainly convenient for those that manage this function, if your insurability for cyber security is buried within the bond or professional liability policies, it might be wise to reflect upon a multi-year renewal. According to Larry Mongeau, J.D. of Carey, Richmond & Viking Insurance who was consulted in the development of this article**, "**Cyber risks is fast moving and evolving. If you have a multi-year policy, we always recommend to our clients an annual policy review to ensure their coverage keeps pace and provides adequate protection." For this very reason, many organizations have found Cyber Insurance as a separate policy option. Specified Cyber Insurance policies are in as much of an evolving state as the perpetrations, with a limited number of major insurers writing coverage. You may need (and want) to find coverage from an insurer outside your existing portfolio of providers.

Thoughts to Evaluate

Presented below are a series of fourteen considerations that we believe you need to ask intuitional management and your insurance partner.

1. Where is cybercrime insurance defined within your current insurance policy suite?

2. When was it last reviewed? When does it renew?

3. If you expand coverage, is it retroactive in covering a breach that has occurred prior to the start of coverage, but has remained inactive or undetected until after coverage is in place?

4. Are there specified exclusions or reduced limits identified in the covering policies?

5. Are there defined coverage requirements, such as encryption for data at rest as an example?

6. What if the data breach was a result of a loss or exposure of physical records, such as checks or loan applications? Banks should make sure their Cyber policy covers personal information that is not in electronic form.

7. What is the test for suspected or identified employee criminal collusion? Does the policy require you to levy law enforcement charges for coverage? Do you have the systems capability to detect nefarious behaviors after the fact?

8. Do you have coverage for social engineered losses, i.e. your employee transfers or provides money unknowingly to a fraudulent account or individual?

9. We know that Information Technology and Insurance are

typically on opposite ends with differing mind sets of an organization, but these two groups need to confer to identify the potential magnitude of a data breach in regards to unique customer records, and the costs to rebuild in the event of breach.

10. Where are your Directors and Officers covered with regards to any action taken against them as a result of a cyber-derived incident?

11. Thought should be given to limiting the on-line availability of non-active customer confidential data. This could even include isolating from your technology network systems such as a data mart or warehouse, HR systems, or even a marketing (MCIF) solution designed to predict consumer behavior and produce marketing campaigns.

12. What coverage amounts should you have? Data from several insurers on just community banks indicate that cyber insurance policy limits for organizations of $3 billion in assets or less have not traditionally exceeded $3 million dollars at the high end, yet industry guidance that we found on Electronic/Computer Systems Bond coverage is recommended at almost a 3 times higher coverage rate. The often represented cost of a data breach is $5.5 million. Could a ratio of $2.85 million in coverage to every $1 billion in assets be a reasonable rule of thumb?

13. What coverage extends to you from your vendors who hold your confidential client data? Do they proclaim to have a cyber insurance policy and if so, given the likely vast amount of data they hold, can you rely upon the coverage limits within their policy? Can they self-insure? Most importantly, what are they contractually obligated to provide in the event of a breach?

14. How do you organize and validate your incident response plans with regards to a breach? Do you validate and test these plans similar to any continuity or recovery process? In an unannounced mock-breach event, how quickly is the flag raised and action undertaken?

Our view is that we remain at the infancy of data exploitation for criminal gain. Just last night as this was being written, NBC News reported on how a hospital was forced to pay a $17,000 ransom to regain control of their own computer systems. Based upon the continuing revelation of long-standing data intrusions and exposure, there is some truth to the assertion that you either know you have been breached or have yet to find out. As with the auto policy that includes comprehensive and collision coverage, if you have not already, financial institution leadership needs to step back and take a comprehensive view as to digital and physical confidential and operational data risk that includes the validation of effective risk mitigation through insurance as but one strategy and backstop.

As a solutions provider and consulting firm serving the Financial Institution industry, CMPG would welcome the opportunity to provide guidance with regards to education and establishment of governance policy and disciplines around effective risk management.

Give us a call.

Jay G. Fitzhugh

Executive Consultant and Partner
jfitzhugh@cmpg.com
(443) 204-4553