SIMMONDS ON BANK INSURANCE

Edition 6–6 | Consulting On, But Never Selling, Insurance | December 2012

What Trouble Lurks Inside Your Insurance?

On average, I find more than 50 problems when I review a bank insurance program. How many are in your policies?

CLAIM 1: Hackers get into your computer system and steal the private data of 5,000 customers. Not only is your bank exposed to a lawsuit, you have to notify and help protect your customers.

CLAIM 2: Someone gets into customer accounts and drains the money from them. The bank is out $800,000. Your customers sue for the hassle and lost business opportunities this causes.

CLAIM 3: Your e-banking system goes down due to a denial-of-service attack. Customers miss deadlines on an important business transaction and sue for your failure to make their funds available.

CLAIM 4: An extortionist threatens to unleash a virus into your bank's computer system unless $1,000,000 is paid.

CLAIM 5: A tornado destroys your main office including the computer systems. Your MIS systems are destroyed. You need to buy new equipment, get it configured, and online ASAP.

The computer risks in banking are enormous. Let's look at how insurance responds.

CYBER LIABILITY INSURANCE

This policy is commonly referred to as cyber liability insurance or e-banking liability. The policy addresses the third-party liability exposure of your computer system. The policy responds when a breach of duty or negligent act by your bank causes a loss to a customer or a customer's customer and they sue the bank.

Liability claims of breach of privacy are the most common. Coverage is also included for the customer's loss of access to computer systems; also, liability that arises out of any unauthorized use of, or unauthorized access to, your covered electronic business systems. Even the smallest bank should have $2,000,000 of coverage for cyber and privacy liability.

Cyber liability can provide protection for the expenses of mitigating a privacy breach, paying the costs of notifying your customers and the other expenses you are obligated to pay as you work through figuring out what data was lost and how you can protect your customers. To me, $500,000 is the minimum

Continued on page 2

Continued from page 1

coverage a bank should have in this coverage area. The bigger the bank, the larger the exposure, and the higher the limits of coverage you should buy. I recommend $1,000,000 of mitigation coverage for a bank with over $500 million in assets. Beat your insurer up until they give you the limits of insurance you need.

COMPUTER FRAUD

Your bank's bond can do a fine job of protecting your bank from the loss of money to computer fraud. It covers the loss to the bank of funds due to a breach of computer security.

In some cases I've dealt with, hackers were able to access a customer account and transfer funds electronically — usually off-shore. These can be big claims.

Contrast this to the losses described above in the cyber liability section of this article. Cyber liability insurance protects you from lawsuits. The bond covers you for losses to the bank assets.

Small banks should have $2,000,000 of computer fraud coverage. Banks over $500 million in assets should have more than $3,000,000 of protection.

DATA DESTRUCTION BY HACKER OR VIRUS

The loss of data caused by a hacker or malicious virus is also included in the bank bond. Coverage includes the cost of cleaning up a system intrusion and restoring data from backup. Again, this is a loss to the bank — first-party losses. A lawsuit by a customer against the bank for an issue involving a computer is going to be in the realm of cyber liability.

A lawsuit by a customer against the bank for an issue involving a computer is going to be in the realm of cyber liability.

E-COMMERCE EXTORTION

Here again, we are in the bond, as an extortion claim is a loss to the assets of the bank. Most financial institution bonds include coverage for property extortion and kidnaping. You want to be sure you have specific coverage for a threat like this: "I will release the private information on all your clients unless you pay me $500,000."

EDP INSURANCE

Insurers still call your computers "Electronic Data Processing" Systems. Coverage here is on your computer hardware, software and data. This is coverage on your property — damaged by a fire, windstorm, vandalism, and the like.

Several of my bank clients have suffered tornados over the past few years. Computers don't suffer such events very well. Many policies exclude flood and earthquake damage. Consider coverage for the increased expenses of getting your computers back up and running quickly.

SUMMARY

You can't correct your insurance once you have a loss. There is no retroactive insurance fix. Identify your problems now and adjust your insurance before a catastrophe hits.

Computer theft, damage, fraud, and mistakes pull coverage from a wide range of insurance policies. Individual incidents can involve your executive risk, cyber liability, financial institution bond, and property insurance. Coverages must be coordinated to work together. Hand this article to your insurance agent to start the conversation on how well your insurance is designed. ■

The Other Side Of Privacy Liability

In the main article in this newsletter I talk about cyber liability insurance. That policy includes protection against data breaches from your computers — hackers, and thieves.

Your bank is also exposed to breaches of privacy from other, non-computer sources: A loan officer loses a printout of customer data. A briefcase is stolen at an airport. A laptop is lost.

My most laughed-at incident is the bank officer who placed the box of loan files on the roof of his car, then drove off oblivious to the storm of paper left in his trail. (Apparently this happens often enough to allow people to recognize the claim.)

None of the above are "cyber" privacy issues. Some cyber liability policies include coverage for "analog" events. Not all do. Does yours? ■

Bank Insurance Commentary

Civil Money Penalties Insurance Bites The Dust

I've had many conversations recently on the topic of civil-money-penalties coverage within the directors' and officers' insurance policy. The key question is, should CMP be included in the policy?

I have worked on dozens of D&O renewals in the past few months. Not once has the insurer or agent brought the subject of CMP up — until I prompted the conversation. Insurers and agents do not seem to be offering any guidance to banks. I see it as my job to do so.

This may be the first time I have ever thought that buying insurance could actually create problems for my clients. I think you should remove the CMP coverage from your D&O.

FDIC and OCC are quite clear — no insurance coverage (or indemnification) to pay for fines and penalties should be attached to anything the bank does.

I am not agreeing with the regulator's position on this. Bankers should be able to buy this coverage — as insurers should be able to sell it. Right now, though, the regs seem clear to me. I have zero interest in seeing any regulator look harder at a bank client of mine.

I'm working to find an insurer who will offer stand-alone insurance for bank directors and officers.

Different insurers are taking different approaches. Travelers, ABA Insurance/Everest and several other insurers are continuing to include CMP coverage in their D&O policies for "qualified" banks. Banks can request that the coverage be removed.

Zurich and FinSecure offer CMP to their clients. They charge a per-officer/director fee that is to be paid directly to the bank by the directors — reimbursement by the directors to the bank. Cincinnati Insurance has removed CMP from all their bank D&O policies.

I have discussed this with FDIC officials. Having CMP insurance on a bank insurance policy is a no-no according to regulators.

I'm working to find an insurer who will offer stand-alone insurance for bank directors and officers. My idea is an insurance policy bought by an individual in a transaction that has nothing to do with the bank. Director/officer buys, director/officer pays for the insurance. I'm working on it.

Comments? Ideas? Call or email me. Always glad to talk.

Scott Simmonds, CPCU, ARM

Conference Calls to Help Your Board Understand Their Insurance

Every month I conduct conference calls for bank boards. We discuss the bank's insurance, the insurance marketplace, and insurance strategies.

In 20 minutes your board can be more comfortable with their insurance and their risks. Call me at 207-284-0085 to discuss what your board needs. ■

Newly Updated Bank Insurance Limit Recommendations

HOW MUCH COVERAGE SHOULD WE BUY? Do you have enough? Are your limits of insurance in the right places? Includes bond, executive risk, umbrella liability, cyber liability, and property insurance. This paper answers the most common question I get: "How much coverage should we buy?"

Get your free copy by emailing *Scott@ScottSimmonds.com.* ■

STAY CURRENT ON BANK INSURANCE ISSUES.

JOIN OUR INNER CIRCLE FOR FREE, PRACTICAL INSURANCE ADVICE DELIVERED DIRECT TO YOUR INBOX.

EMAIL *SCOTT@SCOTTSIMMONDS.COM*.

Simmonds on Bank Insurance
Consulting On, But Never Selling, Insurance
20 Sofia Road
Saco, Maine 04072

PRSRT STD
U.S. POSTAGE
PAID
THE NEWSLETTER
COMPANY

Insurance Renewal Assistance

How are you going to manage your next insurance renewal? Same insurer? Multiple agents? Same coverage? Are you missing protection?

Is your agent working as hard as she should? Are you missing opportunities? Is this really the best there is? What insurers should be in on the process? How do you select other agents to participate?

The best time to start working on your renewal is 120 days before the expiration of your current policies. (However, my tactics can help even if you are days away from the due dates.)

Contact me now to discuss your bank's situation: *Scott@ScottSimmonds.com* or 207-284-0085. ■

Unbiased Bank Insurance Coverage Review

HERE'S A TYPICAL TIMELINE FOR AN UNBIASED INSURANCE REVIEW:

■ **DAY 1:** The CFO of ABC Bank emails me. He is interested in a review of his bank's insurance. We discuss his bank's situation, current insurance, and his objectives. The call takes less than twenty minutes. In a few hours he has a proposal outlining costs, my approach, objectives, and value.

■ **DAY 5:** The CFO decides to move forward. The bank emails me copies of the policies. I forward a survey of exposure questions to help me understand the bank. I start my review.

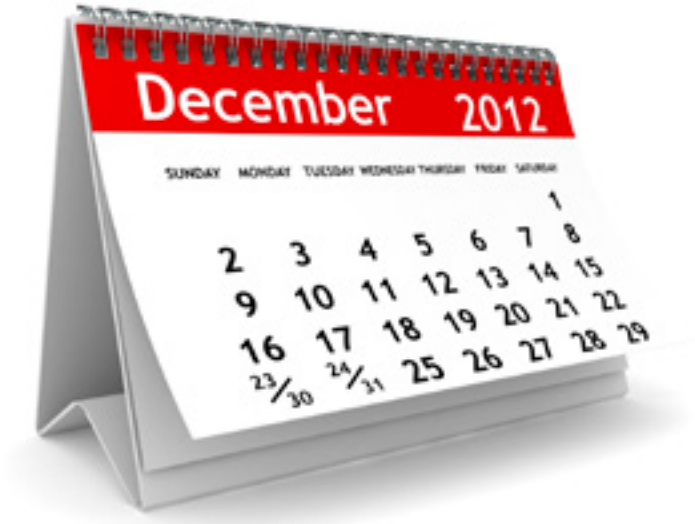
■ **DAY 15:** I email the CFO a copy of my findings to be used in our phone call later in the day. We review the issues and I provide my recommendations. The CEO, CFO, and SVP of the bank are in on the call. We set action plans and accountabilities for each issue.

■ **DAY 16:** I send the call participants a summary of the issues we discussed clarifying my recommendations. The CFO calls me with questions as the issues are addressed. I often talk with the bank's agent about my suggestions. We are all on the same team.

My clients get better insurance, better premiums, and easier insurance administration.

Imagine having confidence in the quality of your bank's insurance.

Send me an email at *Scott@ScottSimmonds.com* or call 207-284-0085. ■



 | ISSN 2159-7596