MARSH

INSIGHTS | NOVEMBER 2018

Protecting High-Value Assets: Insurance Implications of Cybercrime for Financial Institutions

Cybercrime is undeniably on the rise, with security breaches and stolen funds becoming a daily occurrence and attacks growing in complexity. Several high-profile attacks have been aimed at banks, against which cybercriminals have used malware to target money processing services and ATMs.

While banks are a common target for hackers, banks also tend to apply more advanced security measures. Banks devote considerable resources and management focus to safeguarding high-value assets, including proprietary and customer data and bank and customer monies and securities. But loss control and mitigation alone cannot eliminate the risk; the new reality is not "if" but "when" a cyber-attack will occur. And insurance, while effective at reducing the financial impact of cyber events, has also raised questions for banks — as well as disputes with insurers — about how coverage should respond to a cyber event involving multiple types of loss.

The Coverage Dispute

As seen in at least one case currently working its way through the federal court system, policy response in practice is not always a certainty. In *The National Bank of Blacksburg v. Everest National Insurance Company*, an insurer is denying coverage sought by a bank under the computer and electronic (C&E) crime rider of the bank's financial institution (FI) bond. The bank alleges that it is the victim of losses suffered as a direct result of two unauthorized hacking intrusions into its computer systems, totaling nearly $2.5 million. According to the bank, these intrusions allowed perpetrators to "illegally withdraw funds from the accounts of National Bank's customers, post fake deposits, and remove illegal transactions from customer accounts," among other things. Within days of being informed of the first intrusion, the bank engaged a forensic investigator. The bank contends that none of the losses arose out of plastic card or debit card information stolen from customers.

The insurer, however, has denied coverage for the losses under the bank's C&E crime rider, which carries an $8 million single-loss limit. The insurer instead claims that the losses fall under the bank's FI bond debit card rider, which has a much lower $50,000 single-loss limit. The insurer asserts that the bond's C&E crime rider excludes coverage for "loss resulting directly or indirectly from the use, or purported use, of credit, debit, charge, access, convenience or other cards... in obtaining credit or funds" or "loss involving automated mechanical devices."

Cyber or Crime?

Some media coverage of the *Blacksburg* case has described it as a cyber coverage dispute, erroneously confusing cyber (network security liability) and crime (FI bond) coverage. However, the coverage dispute arising from this incident does not involve a

cyber policy. At issue instead is whether the loss resulting from this attack triggers coverage under the bank's C&E rider to its FI bond.

The *Blacksburg* case raises two key questions:

1. Which policies should respond to various types of loss — cyber (network security and liability) or crime (FI bond)?
2. Has the FI bond form sufficiently kept pace with evolving exposures to provide meaningful coverage to financial institutions?

While the outcome of the suit is yet to be decided, the *Blacksburg* matter has brought the issue of highly choreographed fraud schemes involving ATM hacks to the forefront of bond coverage discussions. Some insurance industry professionals may view such attacks as covered C&E crime incidents. Under this view, the losses suffered by the bank were directly due to hacking and phishing threat vectors that allowed perpetrators to gain unauthorized access into its computer systems and network, rather than the skimming of debit or plastic cards.

The two exclusions the insurer is relying on to disclaim the loss under the C&E crime rider, commonly referred to as the plastic card and ATM exclusions, are standard in forms developed by the Surety & Fidelity Association of America, including the computer crime form. Some may question whether these exclusions apply to the current situation. However, should the court determine that they do, the language in these exclusions may be broad enough to bar coverage under the computer crime section of the bank's FI bond — especially if applied in tandem. This would result in only the debit card rider being applied to the loss.

If a cyber policy had been in place, it might have responded to this breach. Subject to a deductible, and to specific policy terms and conditions, such a policy might have covered costs associated with the bank's forensic investigation, legal representation, and customer notification and public relations expenses. The network intrusion and any subsequent business interruption losses would also likely be considered insurable cyber losses.

Actual theft of funds, however, may be excluded in cyber policies. In some instances, cyber policies may endorse coverage for theft of funds, but often at a low sublimit.

Securing Broad and Effective Coverage

Banks should look at their coverage broadly and address cyber risk through multiple policies, because cyber threats can cause losses that are covered under more than one policy.

Financial institutions with plastic card and ATM exposure should consider seeking to amend the plastic card and ATM exclusions in those policies during upcoming renewals. The simplest remedy to the FI bond may be to add carve-backs to both exclusions for losses covered under the computer system fraud insuring agreement.

By working with their brokers and insurers, financial institutions can help ensure that all relevant policies — including property, casualty, directors and officers liability, errors and omissions, employment practices liability, fiduciary liability, crime, and cyber — are aligned. Risk professionals should pay specific attention to potentially broad exclusionary language to ensure these policies provide appropriate coverage for otherwise covered losses caused by cyber perils, such as first- and third-party bodily injury and property damage, loss arising out of a failure to render professional services, theft of funds, and trade losses.

In addition to addressing potential coverage gaps, financial institution risk professionals should consult with brokers and insurers to understand where potential overlaps may exist with in-force cyber policies, and prioritize the order of policy responses to maximize recovery arising out a cyber-related incident.

For more information, contact your Marsh representative or:

THOMAS F. ORRICO
Financial Institutions Practice Leader, FINPRO
+1 212 345 5404
thomas.f.orrico@marsh.com

BEN ZVITI
Financial Institutions Cyber/Crime Leader, FI Center of Excellence
+1 212 345 4150
ben.zviti@marsh.com