Financial Institution Loss Scenarios

Cyber Attack

COVERAGE	CyberSecurity
Cause of action	E-Theft
Type of organization	Bank

DESCRIPTION OF EVENT

A hacker enters a bank's network by easily passing through its firewalls. While in the bank's network, the hacker sets up three phony accounts and causes the bank to debit each account for $250,000. The hacker then withdraws the money immediately by having it wire transferred to an account in Switzerland. The hacker is never found, and the money is never recovered.

RESOLUTION

The bank suffers a direct loss of $750,000.

E-Threat

COVERAGE	CyberSecurity
Cause of action	E-Threat
Type of organization	Bank

DESCRIPTION OF EVENT

Eight banking web sites in the United States, Canada, Great Britain and Thailand are attacked. The hackers claim to have 23,000 credit card numbers and threatens to post them online unless the banks agree to pay them $1 million. News of this quickly becomes public, and now the banks also need to restore customer confidence.

RESOLUTION

Ransom demand of $1 million is paid; public relations expenses are incurred to restore customer confidence.

gencorp INSURANCE GROUP

Could this happen to your organization?

Joseph J. Padula, MBA, CIC
Gencorp Insurance Group, Inc.
16 Main Street, East Greenwich RI 02818
Phone: (800)232-0582 x120, Fax: (401)884-0290
Email: jpadula@gencorp-ins.com

1/2011

Financial Institution Loss Scenarios

E-Signature

COVERAGE	CyberSecurity
Cause of action	E-Signature
Type of organization	Bank

DESCRIPTION OF EVENT

A regional bank agrees to purchase mortgages from one of its competitors. The competing bank transmits digital records representing the loans secured by real property. The regional bank relies on the faith of these digital records and pays $1.5 million to purchase the loans. The digital records, however, contain fraudulent electronic signatures.

RESOLUTION

The bank suffers a direct loss of $1.5 million.

Reputational Injury

COVERAGE	Cyber Liability
Cause of action	Reputational Injury
Type of organization	Bank

DESCRIPTION OF EVENT

One of the nation's largest banks was sued for allegedly selling thousands of unauthorized consumer credit reports to entities that were unaffiliated with the bank. The suit alleged that two bank employees obtained the reports from a credit agency and sold them to an individual outside the bank. Fewer than one-quarter of the plaintiffs in the case were bank customers.

RESOLUTION

The suit sought damages for alleged violations of the Fair Credit Reporting Act, a violation of a person's right of privacy.

gencorp INSURANCE GROUP

Could this happen to your organization?

Joseph J. Padula, MBA, CIC
Gencorp Insurance Group, Inc.
16 Main Street, East Greenwich RI 02818
Phone: (800)232-0582 x120, Fax: (401)884-0290
Email: jpadula@gencorp-ins.com

1/2011

Financial Institution Loss Scenarios

Disclosure Injury

COVERAGE	Cyber Liability
Cause of action	Disclosure Injury
Type of organization	Bank

DESCRIPTION OF EVENT

A hacker exploited known operating system flaws to gain access to the systems of several large banks conducting business on the Web. He was able to harvest tens of thousands of credit card records, which he then offered to sell for $5 per record. Almost 100,000 accounts were compromised. The financial institutions involved received customer complaints citing negligent system security in failing to protect their private records.

RESOLUTION

The customers filed a class action suit seeking compensatory damages.

Could this happen to your organization?

Joseph J. Padula, MBA, CIC
Gencorp Insurance Group, Inc.
16 Main Street, East Greenwich RI 02818
Phone: (800)232-0582 x120, Fax: (401)884-0290
Email: jpadula@gencorp-ins.com

1/2011

Financial Institution Loss Scenarios

Bank Officer Makes Liberal Use of Cashier's Checks

COVERAGE	Crime (Fidelity Bond)
Cause of action	Employee Dishonesty
Type of organization	Bank

DESCRIPTION OF EVENT

"Mountain River Bancorp" was a typical, rural, community bank, providing highly personalized service to its business and individual customers. As it grew, the bank decided to organize itself into branch clusters managed by area presidents. One of the bank's area presidents was approached by her brother, a key financial officer in several affiliated area businesses with which the bank had commercial loan and deposit relationships. The president's brother convinced her to help him bolster some "temporary" cash shortages at his companies by providing him with a cashier's check that he could deposit to pay expenses. He promised to provide funds to cover the check within a few days. The area president agreed to the arrangement; after all, the prospect of local companies unable to meet payroll did not bode well for her friends and neighbors, and she trusted her brother to cover the transaction quickly. She obtained and issued a cashier's check and held the paperwork at her desk. A few days after issuing the cashier's check, she received funds from her brother to cover it. She then submitted the paperwork through the normal process without incident. Over time, this scenario was repeated many times, with the check amounts becoming increasingly larger and the associated activities becoming bolder. At times the area president would obtain a check, forge her brother's endorsement, and then present the check to be cashed, saying that she would deliver the cash personally. At other times she deposited the check into the company's account, and then processed debit memos against the same account with the offsetting deposit made to her own personal account. A total of 294 cashier's checks were floated in the scheme, totaling $5.9 million.

RESOLUTION

When the bank discovered the scheme, the area president was terminated, along with another employee whose collusion in later months came into play. Almost $1.2 million of outstanding cashier's checks had not been paid for. Copies of these checks were subsequently found in the former area president's desk. The bank notified the family of companies on whose behalf the cashier's checks were issued. The companies terminated the employment of the brother who had been involved in the scheme. Despite their verbal commitment to make full restitution, the financial ability of the businesses to do so was far from certain. The Federal Bureau of Investigation was notified.

gencorp INSURANCE GROUP

Could this happen to your organization?

Joseph J. Padula, MBA, CIC
Gencorp Insurance Group, Inc.
16 Main Street, East Greenwich RI 02818
Phone: (800)232-0582 x120, Fax: (401)884-0290
Email: jpadula@gencorp-ins.com

1/2011

Financial Institution Loss Scenarios

Trusted Employee Has Gambling Habit To Support

COVERAGE	Crime (Fidelity Bond)
Cause of action	Employee Dishonesty
Type of organization	Bank

DESCRIPTION OF EVENT

An assistant branch manager at a small local bank was a long-time, trusted employee. In addition to his management responsibilities, this individual acted as a loan officer for the bank. Unfortunately, he had a gambling habit to support, and he embezzled in excess of $350,000 over three years via fictitious loans (all in the names of real borrowers). The loan amounts were within the loan officer's authority. During the investigation, it was noted that the officer seldom took vacation over successive days.

RESOLUTION

The employee pled guilty and was sentenced accordingly. He also will be pursued for restitution and repayment.

Loan Officer Shows Favoritism

COVERAGE	Crime (Fidelity Bond)
Cause of action	Employee Dishonesty
Type of organization	Bank

DESCRIPTION OF EVENT

A bank vice president/loan officer purchased a home from one of the bank's construction borrowers for less than half of its market value. He then proceeded to falsify construction reports on other properties under development by the borrower, allowing the borrower to draw down loan proceeds when no construction progress was actually being made. Subsequently, the loan went into default and the bank foreclosed on the undeveloped properties. The loan officer is also alleged to have solicited unqualified and rather naïve friends and relatives and approved loans for them to purchase and develop properties in the same area. He is alleged to have taken (skimmed) consulting fees from these other, unsophisticated borrowers.

RESOLUTION

Construction loan risk management begins, as with all lending, with a sound knowledge of the client, a clear division of internal responsibilities, adequate operational controls, and an independent audit function.

gencorp INSURANCE GROUP

Could this happen to your organization?

Joseph J. Padula, MBA, CIC
Gencorp Insurance Group, Inc.
16 Main Street, East Greenwich RI 02818
Phone: (800)232-0582 x120, Fax: (401)884-0290
Email: jpadula@gencorp-ins.com

1/2011