A GROWING THREAT TO DATA SECURITY

Information, Network Security and Privacy Risk Management

Program Overview

Data security breaches continue to occur not only with alarming frequency, but also with significant severity. Identity theft continues to rise, jumping 13% from 2010 to 2011. Close to 12 million adults were victimized by identity theft, and was the number one complaint filed with the Federal Trade Commission in 2011.

It is no longer unusual for single incidents of a data breach to involve the compromise of several hundred thousand and perhaps even millions of records involving personal information. These breaches may also not be discovered for considerable lengths of time. Heartland Payment Systems provides bank card payment processing services to 250,000 merchants and businesses nationwide. A massive data breach was apparently launched in 2007, not discovered until 2008 and not made public until 2009. Over this time period, Heartland has incurred over $13 million in costs associated with the breach, incalculable damage to its corporate reputation, and a 40%+ drop in its stock price. Predictably, Heartland's directors and officers are the targets of ongoing lawsuits by shareholders, regulators, and other effected parties.

Perpetrators of data breaches range from amateur hackers to political and social activists to organized crime gangs. While intuition might suggest that larger, more sophisticated organizations would be able to fend off attacks, the reality is otherwise, as major US banks and government organizations (including the CIA and State Department) have been hacked. The Wikileaks hacks of the military and state departments have revealed extremely sensitive information related to our national security. In addition to data breaches, liability exposures can include trademark, copyright and/or patent infringement.

Data security and privacy exposures can result in massive financial loss and reputational damage for organizations and businesses of all sizes, in the public, private, for-profit and non-profit sectors. Producers need to understand the scope and extent of these exposures and the risk management and insurance strategies available to address them.

Program Objectives

As a result of this program, the producer will:

- Understand the scope and extent of network security exposures and that organizations of all sizes are at risk;
- Learn about the multiple U.S. federal and state privacy laws, and similar privacy laws in effect in the European Union, their requirements, and potential fines and penalties imposed by these regulations;
- Understand the scope of potential financial and reputational costs associated with data breaches and other privacy-related exposures;

- Learn the essential components of a network security and privacy insurance contract, definition of insureds, defense and settlement provisions and exclusions;
- Understand how the underwriting process works in assessing an applicant, and related "best practices" for identifying and quantifying a risk;
- Understand how the network security and privacy claim is processed, managed and resolved;
- Learn how to employ a holistic network security and privacy risk management program combining avoidance, reduction, retention, and risk transfer strategies.

Program Content

I. Current and Emerging Risks in Network Security and Privacy (20 minutes)

a. Types of threats
   i. Denial of service
   ii. Privacy breach
   iii. Extortion threats
   iv. Malware
   v. Sabotage, defacement and vandalism
   vi. Libel, slander
   vii. Copyright and/or patent infringement
   viii. Income loss
b. Number of breaches/trends
c. Industry-related breaches
d. Corporate breaches: case studies
e. Perpetrators
   i. Criminals
   ii. Amateur hackers
   iii. activists

II. Regulatory Environment (20 minutes)

a. U.S. State and Federal Privacy Laws
   i. HIPAA
   ii. Gramm-Leach Bliley
   iii. Children's Online Privacy Protection Act
   iv. Computer Fraud and Abuse Act
   v. Fair and Accurate Credit Transactions Act/"Red Flag Rules"
   vi. State laws
b. European Union Data Privacy Laws
   i. Information Directive of 1995
   ii. Directive on Privacy and Electronic

III. Costs Associated with Data Security Breaches (10 minutes)

a. Forensic analysis/damage assessment
b. Expense to secure compromised networks
c. Costs of mandatory notices to consumers and government authorities
d. Credit monitoring services
e. Defense costs and damages

f. Costs of compliance with government investigations
g. Fines (e.g. violations of HIPAA, GLBA, FCRA)
h. Lost business
i. Loss of trust
j. Reputational damage

IV. Liability Risks (15 minutes)

a. Defamation
b. Invasion of privacy
c. Trademark, copyright, patent infringement
d. Copyright infringement
e. Loss of access

V. First-Party Risks (15 minutes)

a. Business interruption and CBI
b. Extra expense
c. Digital asset replacement expense
d. Cyber-extortion threats

VI. Network Security and Privacy insurance/Analysis of a Sample Form (40 minutes)

a. Why This Coverage is Necessary: Shortcomings and Deficiencies in the Traditional CGL Form
b. Definition of insured
c. Definition of loss
    i. Privacy wrongful act
    ii. Security wrongful act
d. Coverage parts
    i. Security and privacy liability coverage (third party)
    ii. Privacy breach cost coverage (first party)
    iii. Business income and dependent business income loss coverage (first party)
    iv. Digital asset replacement expense coverage (first party)
    v. Cyberextortion coverage (first party)
    vi. Internet media liability coverage (third party)
e. Defense and settlement
f. Other insurance
g. Exclusions

VII. Underwriting and Application Considerations (20 minutes)

a. Recommended participants
    i. Chief Information Officer
    ii. Chief Privacy Officer
    iii. High level information technology officer
b. Identifying and quantifying the risk
    i. Business activities
    ii. International exposures
    iii. Organization and governance

iv. Network security
v. Data management
vi. Incident response
vii. Business continuity planning
viii. Loss history

c. Industry classification
d. Implications for regulated industries (healthcare, financial, commercial retailers)
e. Developing the rating basis
f. Completing the application
g. Using endorsements to modify policy terms

VIII. Handling the e-Claim (20 minutes)

a. First party claims/Third-party claims
b. Actions for injunctive relief
c. Selection of defense counsel
d. Consent to settle and the hammer clause

IX. Data Security Risk Management (20 minutes)

a. Risk management options
   i. Avoidance
   ii. Reduction
   iii. Retention
   iv. Transfer
b. Network security "best practices"

X. Conclusions/Q&A

TOTAL TIME: 180 MINUTES/3 HOURS