Network and Privacy Exposures Demand Specialized Coverage and Controls

- On Jan. 30, 2008, a computer hacker broke into a database belonging to a Montana-based financial consultant, and obtained the names, Social Security numbers, account numbers and balances of 226,000 clients.[1]
- On several occasions between September 2005 and March 2006, backup tapes, optical disks, and laptops, all containing unencrypted electronic protected health information, were removed from the premises of two Pacific Northwest healthcare centers, and left unattended. The media and laptops were subsequently lost or stolen, compromising the protected health information of more than 386,000 patients.[2]
- In May 2009, residents of an apartment complex in Oregon blamed apartment management for leaving their personal information out in the open. The documents were found in an unlocked public container that was sitting off a side street in their apartment complex. The documents included Social Security numbers, addresses, phone numbers, immigration numbers, and names.[3]
- In June 2009, a Washington-based provider of wireless voice, messaging, and data services acknowledged information posted to the Full Disclosure security mailing list by unauthorized users is the company's data, but did not confirm the attackers have access to customer data and other sensitive information. The attackers claim to have "…everything, their databases, confidential documents, scripts and programs from their servers, financial documents up to 2009…"[4]
- A laptop containing private information, including names, addresses and Social Security numbers, on 97,000 employees of a large, Seattle-based coffee retailer was stolen in October 2008.[5]

These events are signs of the times, as organizations increasingly rely on digital assets to run their businesses. And despite ongoing efforts by governments and private organizations to prevent and mitigate security and privacy risk events, through legislation, regulation, and controls, there is no sign of abatement. In fact, since January 2005, 262,576,861 "records" have been compromised due to security breach.[6] In general, "records" included in this accounting are those that contain personal information and data elements useful to identity thieves, such as Social Security numbers, account numbers, and driver's license numbers.

The prevalence of privacy risk events highlights the significant risk exposures of organizations reliant on computers, data, and networks. In general, these exposures can be categorized as:

- First party risks, i.e., losses affecting the organization itself. These include, for example, loss of profits due to theft of trade secrets, destruction of property and data, business interruption due to hacker or virus attacks and software failures, etc.
- Third party risks, i.e., financial compensation for losses of third parties that occur due to shortcomings in an organization's field of responsibility. These include, for example, damage caused by forwarded computer viruses, disclosure of personally identifiable information used for identity theft, costs borne by banks and issuers to reissue credit cards that have been compromised, contractual penalties due to IT failures, intellectual property and privacy infringements after data theft, etc.

[1] Davidson Companies Reports Data Breach Affecting 226,000 Clients, Information Week, January 30, 2008 (http://www.informationweek.com/news/internet/showArticle.jhtml?articleID=206100536)

[2] HHS, Providence Health & Services Agree on Corrective Action Plan to Protect Health Information, U.S. Department of Health & Human Services Resolution Agreement (http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/providenceresolutionagreement.html)

[3] Sensitive Docs Found In Recycle Bin, KPTV.com, May 5, 2009 (http://www.kptv.com/news/19372624/detail.html)

[4] T-Mobile confirms hackers' info is legit, CSOOnline.com, June 9, 2009 (http://blogs.csoonline.com/t_mobile_confirms_hackers_info_is_legit)

[5] Missing laptop puts Starbucks workers' data at risk, Seattle Post-Intelligencer, November 24, 2008 (http://www.seattlepi.com/business/389259_starbucks25.html)

[6] Privacy Rights Clearinghouse A Chronology of Data Breaches (http://www.privacyrights.org/ar/ChronDataBreaches.htm)

Unfortunately, "traditional" insurance policies, such as Property, Commercial General Liability, Errors & Omissions Liability, and Crime, provide for scant coverage exposures to data and information systems from security threats, leaving many organizations vulnerable. An organization that wants a reasonable expectation of coverage for loss of third party data (or other network or data-related loss) must either purchase a Network, Privacy or Cyber Insurance policy, or plan to litigate claims under its "traditional" policies.

Network, Privacy or Cyber Insurance was first offered about ten years ago. Recently, the market for such products has expanded, driven by growing regulatory, enforcement, human, and technical challenges associated with protecting information assets.

Network, Privacy or Cyber Insurance can be tailored to provide first-party and/or third-party coverages, including:

- Loss/Corruption of Data – covers damage to or destruction of valuable information assets as a result of viruses, malicious code and Trojan horses.
- Business Interruption – covers loss of business income as a result of an attack on a company's network that limits the ability to conduct business, such as a denial-of-service attack. Coverage also includes extra expense, forensic expenses and dependent business interruption.
- Liability – covers defense costs, settlements, judgments and, sometimes, punitive damages incurred by a company as a result of:
  - Breach of privacy due to theft of data (such as credit cards, financial or health related data)
  - Transmission of a computer virus or other liabilities resulting from a computer attack, causing financial loss to third parties
  - Failure of security which causes network systems to be unavailable to third parties
  - Providing Internet Professional Services
  - Allegations of copyright or trademark infringement, libel, slander, defamation or other "media" activities in the company's web site
- Cyber Extortion – covers the "settlement" of an extortion threat against a company's network, as well as the cost of hiring a security firm to track down and negotiate with blackmailers.
- Public Relations – covers those public relations costs associated with a cyber attack and restoring of public confidence.
- Criminal Rewards – covers the cost of posting a criminal reward fund for information leading to the arrest and conviction of the cyber-criminal who attacked the company's computer systems
- Cyber-Terrorism – covers terrorist acts covered by the Terrorism Risk Insurance Act of 2002 and, in some cases, may be further extended to terrorist acts beyond those contemplated in the Act
- Identity Theft – provides access to an identity theft call center in the event of stolen customer or employee personal information

The market for Network, Privacy or Cyber Insurance is large and growing, and coverage is becoming more affordable. Many carriers have streamlined the application process and now underwrite based on factors such as company size, the amount of data stored, number of individuals with access to that information, security policies, whether data is encrypted, and the company's prior loss experience.

However, the market for Network, Privacy or Cyber Insurance is in a state of flux, and there are no "standard" Network, Privacy or Cyber Insurance policy forms. Organizations can choose from a dizzying array of specialty insurance products designed to cover this area of risk. This is one line of business where working with an expert broker is essential. Policy wording and premiums vary greatly and need to be negotiated correctly.

A competent, experienced, and tech-savvy broker like Kibble & Prentice will take the time to understand your business operations, identify your exposures and complete a cost benefit analysis to support a sound business decision regarding Network, Privacy or Cyber Insurance. Kibble & Prentice can also be a risk management resource, helping design non-insurance solutions to minimize exposures.

©2009 Kibble & Prentice Holding Company, All rights reserved

Notable factors triggering heightened interest in Network, Privacy or Cyber Insurance include:

- In 2007 TJX, a Massachusetts-based retailer, announced intruders had obtained unauthorized access to its computer systems in 2005 and 2006, enabling them to seize cardholder data and other personally identifiable information.[7] A year earlier, hackers captured consumer credit card data while it was in transit between TJX stores and the authorizing banks, compromising at least 100 million credit card transactions. Investigations, security infrastructure improvements, and data recovery stemming from these incidents reportedly cost TJX about $250 million, and the total cost to TJX of the breach was more than $320 million.[8] This total excludes reputational costs (lost sales and confidence among customers and partners) and costs borne by victims to recover their identities or change account information.
- Most U.S. states have enacted security breach notification laws in response to an escalating number of breaches of consumer databases containing personally identifiable information.[9] (States with no security breach law: AL, KY, MS, MO, NM, and SD.[10]) The first security breach notification law, the California data security breach notification law (Cal. Civ. Code 1798.82 and 1798.29), was enacted in 2002 and became effective on July 1, 2003.
- In February 2009, President Obama signed into law the Health Information Technology for Economic and Clinical Health (HITECH) Act, which includes new privacy requirements that experts have called "the biggest change to the health care privacy and security environment since the original HIPAA privacy rule."
- The European Union and Australia have tabled Bills or passed Acts legislating mandatory data breach disclosure. Other jurisdictions, such as Canada and Japan, have instituted voluntary guidelines.
- According to a new study by Ponemon Institute,[11] employees routinely engage in activities that put sensitive data at risk: downloading data onto unsecured mobile devices (61%), sharing passwords (47%), losing data-bearing devices (43%), and turning off their mobile devices' security tools (21%). And, reflective of the blurring of the lines between personal and professional lives, they are using web-based personal email in the office (52%), downloading Internet software onto an employer's devices (53%), and engaging in online social networking while in the workplace (31%). With the exception of social networking, measured for the first time in 2009, each of these risky behaviors represents an increase compared to 2008 results.
- Costs of a data breach continue to increase, to $202 per record in 2008.[12] These costs include:
  - Investigation and forensics
  - Audit & consulting services
  - Outbound contact costs
  - Inbound contact costs
  - Public relations/communications
  - Legal services – defense and compliance
  - Free or discounted services
  - Credit monitoring services
  - Lost business (due to churn)
  - Customer acquisition

Seth Shapiro, Senior Vice President, Risk Strategist, Risk Strategies Group
(206) 441-6300
www.kpcom.com

[7] Attorney General Announces Multi-State Settlement with Major Retailer Over Consumer Data Breach, New Jersey Office of the Attorney General (http://www.nj.gov/oag/newsreleases09/pr20090623b.html)

[8] TJX Settles Data Breach Damage Claims with 39 States, Channel Insider/Ziff Davis Enterprise Holdings Inc. (http://blogs.channelinsider.com/secure_channel/content/network_security/tjx_settles_data_breach_damage_claims_with_39_states.html)

[9] Security Breach Notification: State Laws Chart, Perkins Coie (http://www.perkinscoie.com/statebreachchart/)

[10] Ibid.

[11] Trends in Insider Compliance with Data Security Policies: Employees Evade and Ignore Security, Ponemon Institute, LLC, 2009

[12] 2008 Annual Study: Cost of a Data Breach, Ponemon Institute, LLC, February 2009

©2009 Kibble & Prentice Holding Company, All rights reserved

Network and Privacy Exposures Demand Specialized Coverage and Controls

IRS Circular 230 Disclosure: Kibble & Prentice Holding Co. and its affiliates do not provide tax advice. Accordingly, any discussion of U.S. tax matters contained herein (including any attachments) is not intended or written to be used, and cannot be used, in connection with the promotion, marketing or recommendation by anyone unaffiliated with Kibble & Prentice Holding Co. of any of the matters addressed herein or for the purpose of avoiding U.S. tax-related penalties. Also, the information contained in this brochure should not be construed as medical or legal advice and is intended for educational purposes only. Kibble & Prentice operates in the State of California under the name of Kibble & Prentice Holding Company dba Kibble & Prentice Insurance Agency (0E28835).

Kibble & Prentice
A USI Company

©2009 Kibble & Prentice Holding Company, All rights reserved