Advisory topic: Cyber Liability

Industry Maturity Index: '***Now***'

Why this is important: In the past 4-5 years, the news of data breaches, hacks, ransomware, phishing have been pervasive. The potential impact of data breaches to compromise agency business, as well as the trust of their clients and partners should not be understated. The ACT Changing Nature of Risk work group provides the following as background for strategic discussions.

What is it? 'Cyber Liability' or 'Cyberliability' is a type of insurance designed to cover consumers of technology services or products. More specifically, the policies are intended to cover a variety of both liability and property losses that may result when a business engages in various electronic activities, such as selling on the Internet or collecting data within its internal electronic network.

Most notably, but not exclusively, cyber and privacy policies cover a business' liability for a data breach in which the firm's customers' personal information, such as Social Security or credit card numbers, is exposed or stolen by a hacker or other criminal who has gained access to the firm's electronic network. The policies cover a variety of expenses associated with data breaches, including: notification costs, credit monitoring, costs to defend claims by state regulators, fines and penalties, and loss resulting from identity theft.

In addition, the policies cover liability arising from website media content, as well as property exposures from: (a) business interruption, (b) data loss/destruction, (c) computer fraud, (d) funds transfer loss, and (e) cyber extortion.

It is important to remember that no two policies are identical and the terminology can often be confusing.

Broad Implications / Uses: This has applications across many spectrums of our lives;

- Business lost during attack.
- Loss of company assets.
- Damage to reputation.
- Litigation.
- Protection costs: staff, firewalls, encryption and software.
- Notification to affected customers.
- Potential loss of customers.
- Potential state and federal fines if security plan and other required processes were not followed.
- Decline in share value and business income.
- Costs for post-breach implementations (firewall, encryption, security plans, etc.)

It is critical to note that small and mid-sized businesses now account for 62% of all cyber-attacks. Furthermore, organizations experiencing a data breach incur costs across the board. The cumulative critical impact of this make securing and providing cyber liability coverage for customers imperative.

Economic Impact(s):

ACT Risk Advisory –
Cyber Liability

CHANGING NATURE OF RISK
"Moving from trends to critical action."

According to the recently released study from the Ponemon Institute, the average economic impact per organization is more than $2.2 million, which is only expected to rise in years to come. Unfortunately, most organizations are unprepared to address new threats and lack adequate resources to protect their data.

The largest writers of cyber liability according to FitchRatings.com are:

American International Group, Inc. (AIG), accounting for approximately 22% of the market,
Chubb Limited (CB) at 12%, and
XL Group Ltd. (XL) at 11%.

Cyber-related insurance coverage represents a significant growth opportunity for P/C insurers. Insurance broker Marsh & McLennan Companies, Inc. (MMC) estimated that in 2014 the global insurance market wrote approximately $2 billion in cyber insurance premiums, which could multiply by a magnitude of three to five times by 2020. Aggregating the cybersecurity statutory supplement data for the U.S. property/casualty (P/C) insurance industry finds that approximately 120 insurance groups reported writing cyber coverage in 2015 totaling approximately $1 billion in direct written premiums volume. Fitch analyzed cyber insurance market share and performance in a new special report, 'U.S. Cyber Insurance Market Share and Performance' that analyzes data from a new 2015 statutory supplement to compile company and industry statistics on cyber insurance.

Three ways companies can most improve their reaction towards trying to minimize an impact to their operation:

a) Detect incidents sooner.
b) Contain them faster after detection.
c) Keep good logs to facilitate a more precise determination of what occurred before the attack was stopped and how to prevent them in the future.

Insurance Industry Implications: Cyber Liability can have positive and negative impacts to many areas of our industry;

- Positive Impacts
  - Providing coverages to the marketplace allows businesses and individuals to protect their assets.
  - Stabilizing exposures and thereby providing a more stable marketplace.
  - Overall reduction of data breach costs.
- Negative Impacts
  - No standard industry form on which cyber liability policies are written.
  - Forensic investigation expenses.
  - Business interruption or extra expense due to system downtime.
  - The cost of notification and other breach response activities.
  - PCI fines, penalties and/or assessments.
  - Various Regulatory action defense, fines and penalties.
  - Significant business clientele loss post-reporting.

Recommended Actions:

Agents -

- Understand that there are federal and state regulations that your clients must be prepared to meet. Clients must keep abreast of who is holding them responsible for data they manage
- Secure all devices, including smartphones and tablets. Keep in mind your devises as well as how you connect to your network and know what data is stored on the various devises

- Know where your data is, even though the outsourcing agreement may include a requirement for the vendor to meet PCI security standards, don't assume data is safe. Businesses also should ask about the physical security at the data storage center as well as information security.
- Monitor continuously. Educate your clients that they are ultimately responsible for meeting those standards, it does not matter if the company outsourced their data management. Just signing a contract isn't enough to say I am covered. Educating the buyers of Cyber insurance as to their obligations in meeting the policy's minimum requirements to maintain that insurance is very important.
- Business clients must understand the software they are using, its security measures and vulnerabilities. Remind your clients to have policies and procedures to update the software whenever updates are available and to ensure that those policies and procedures are followed correctly and promptly by all employees.

Carriers -

- Investigate offering coverages across spectrum of impact. Provide the coverages that will help insure a policyholder will have the services and coverages needed in order to handle an event. Update coverages and limits as the marketplace changes. Provide training to agents, keeping the training current at all times.

Vendors -

- Ensure management, quoting, and contact systems have the ability to handle these as specialty products. Place the proper controls and provide assistance to your agents to educate them on your capabilities. Provide ongoing and updated training.

Examples/Resources:

AMWins – What is Cyber Liability?
First Data - The cost of data breach for Small Businesses may be higher than you think
Guiding Principles to Advance Information Security (a NY document that is appropriate countrywide)
Combat Cybercrime and Protect Your Agency (ACT)
Protecting Agency Customer Information from Identity Theft (ACT)
Cyberplanner – Build Your Own Plan (Federal Communications Commission)
Betterley Report – Cyber/Privacy Insurance Market Study (includes carrier product comparisons)
IIABA Big 'I' Markets – Cyber Liability Coverage
"Data Breach, the New Wild West? Cyber Risk Exposures and Insurance" (IIABA WEBINAR RECORDING)

Evolving Technology Caution:

Security is a moving target which requires continually revisiting standards and best practices. Make sure that hardware and software are up to date and appropriate patches are installed. W-Fi should be secured and encrypted. Back up your data. See ACT's recommendations and education in this areas on our Security & Planning web page.

Call to Action:

- Assess your situation and get a professional evaluation of your security risk
- Be familiar with relevant federal, state and local laws and requirements (State Data Security Breach Notification Laws – Mintz Levin)
- Establish a plan that addresses prevention, resolution, restitution and implementation of best practices to reduce your security risk exposure

- Educate your employees on your company's privacy policy, passwords, email usage, mobile device policy, safe web-browsing and social media

Authors: J Ted Joyce, Kathleen Weinheimer, Ron Berg