Cybersecurity & Carrier-Vendor Integration

WHERE THE PREMIUM AUDIT INDUSTRY IS HEADED

Cybersecurity Law Updates & Explanation

History – The Rising Security Bar

- Over most of the past decade, the Massachusetts Cybersecurity law had been the top standard most Insurance Companies used as a benchmark
- CA and other states have been raising their security requirements, particularly related to consumer privacy
- New York recently passed a law related to Cybersecurity and it applies to Insurance Companies that write more than a nominal amount of business in New York and their vendor partners
- We anticipate that more states will be moving this same direction.

Massachusetts – The Rising Security Bar

- Massachusetts Law was the "High Bar" for many years
  - Effective 3/1/2010
    - Secure user authentication protocols, (PW Policy)
    - Secure access control measures, (least privilege)
    - Encryption
      - in transit and at rest
      - Specifically called out encryption of data on laptops and portable devices
    - Firewall protection and operating system security patches for all Internet facing systems containing Personal data
    - Anti-Virus and Malware detection software
    - Education & Training of Employees

California - The Rising Security Bar

- Eff. 8/31/15 – Creation of CA Cybersecurity Integration Center & Task Force
- Eff. 4/2017 – Data Breach Notification
  - Breach notification has become standard across most states & carriers
- Eff 1/1/2020, (Introduced in 2017) – Consumer Privacy Act
  - CA Consumers have a right to:
    - Know if their information is being collected. If so, what information is being collect?
    - If their information is being sold or disclosed to others? If so, to whom?
    - Say no to the sale or disclosure of their information
    - Access their personal information
    - The same level of service from a company, even if they do not allow use of their personal information
  - Connected Devices, (manufactured devices connected to the Internet
    - "requires manufacturers of Internet-connected devices – such as TVs, phones, toys, household appliances and routers – to ensure that their products have "reasonable security features." These security features should be able to protect sensitive customer information from unauthorized access."

NY DFS Cybersecurity Regulation (23 NYCRR 500)

- Effective 3/1/19
  - Law was effective 3/1/2017 but it had a 2 year implementation period
  - Applies to Insurance Carriers and their 3rd Party Vendors
- Cybersecurity Program
- Cybersecurity Policy
- Conduct Annual Risk Assessments
- Carrier must file a form annually with the State of NY to indicate compliance with the law, (needs to be signed for the Top Officer of the organization)
- Periodically review policy to update and confirm compliance
- Security Breaches must be reported to the State of NY

NY DFS 23 NYCRR 500 Requirements

- *Multi-Factor Authentication* means authentication through verification of at least two of the following types of authentication factors:
  - (1) Knowledge factors, such as a password; or
  - (2) Possession factors, such as a token or text message on a mobile phone; or
  - (3) Inherence factors, such as a biometric characteristic.
- Use of Encryption, at rest and in transit, (everywhere policyholder data is stored)
- The cybersecurity program for each Covered Entity shall, at a minimum, include:
  - (1) penetration testing of the Covered Entity's Information Systems at least annually; and
  - (2) vulnerability assessment of the Covered Entity's Information Systems at least quarterly.
- Detect Cybersecurity Events – Detection Tools:
  - Intrusion Prevention System
  - Data Loss Detection and Data Loss Prevention Systems
- Business Continuity and Disaster Recovery planning and resources (backups)
- Physical security and environmental controls
- Incident response plan

NY DFS Cybersecurity Requirements

- Annual Cybersecurity Review/Audit wording includes:
  - "due diligence processes used to evaluate the adequacy of cybersecurity practices of third parties"
  - "the right of the Covered Entity or its agents to perform cybersecurity audits of the third party service provider"
  - Vendor partners should be part of annual review
- Pushing vendors toward SSAE 18 compliance?
- Destruction of Data
  - As part of its cybersecurity program, each Covered Entity shall include policies and procedures for the timely destruction of any Nonpublic Information identified in 500.01(g)(2)-(4) that is no longer necessary for the provision of the products or services for which such information was provided to the Covered Entity, except where such information is otherwise required to be retained by law or regulation.

NY - Section 500.18 Limited Exemption

- Limited Exemption. Each Covered Entity, (*Carrier*) with:
  - (1) fewer than 1000 customers in each of the last three calendar years, and
  - (2) less than $5,000,000 in gross annual revenue in each of the last three fiscal years, and
  - (3) less than $10,000,000 in year-end total assets, calculated in accordance with generally accepted accounting principles, including assets of all Affiliates, shall be exempt from the requirements of this Part other than the requirements set forth in this section, Sections 500.02, 500.03, 500.07, 500.09, 500.11, 500.13, 500.17, 500.19, 500.20 and 500.21.

“That’s Horrible. What Next?”

- European Union’s General Data Protection Regulation, (GDPR)
  - Effective May 2018 and includes banking & financial institutions
  - “applies to all companies processing the personal data of data subjects residing in the EU, regardless of the company’s location.”
  - Breach Notification
  - Right to Access, (request copy of your the personal data stored)
  - Right to be Forgotten, (delete your personal data)
  - Privacy by Design, (“hold and process only the data absolutely necessary for the completion of its duties”)
  - Financial penalties for non-compliance
- Other states are sure to follow in New York’s footsteps

Cybersecurity Takeaways

- The bar will only continue to go up. It never goes down
- Vendors
  - Working for Carriers that write in NY will bring the New York law into play
    - The carriers must sign off that their 3rd Party Vendors are also compliant
  - Cybersecurity Insurance Coverage is Important
    - Costs to notify insureds can be significant. Most carriers limit the coverage related to notification
    - Vendors should have Cybersecurity coverage, (usually separate from Professional Liability coverage and is excluded from Umbrella coverage)
    - Limit your exposure by contract whenever possible

Cybersecurity Takeaways

- Costs
  - Another word for "Cybersecurity" is "Money". There is almost nothing a company can do to improve its cybersecurity strategy that does not cost money
  - What does a professionally hosted NY Compliant environment cost?
    - Physical Security
    - Intrusion Prevention System
    - Data Loss Prevention System
      - All Hosting Environment(s)
      - Email System
    - Vulnerability Detection Software, (Application Security)
    - Quarterly Vulnerability Reviews
    - Annual Pen Test
    - Log review system
  - What do the technical contractors or employees needed to set this up cost?
  - What does SSAE 18 compliance cost?

Cybersecurity Links

- Massachusetts Cybersecurity Law
  - https://www.mass.gov/files/documents/2017/10/02/201cmr17.pdf
- CA Law Effective 1/1/2020 (Overview)
  - https://www.securityweek.com/california-iot-cybersecurity-bill-signed-law
- NY Regulation:
  - https://www.pbwt.com/content/uploads/2016/09/rp500t.pdf
- NY - Memo from the chief:
  - https://www.dfs.ny.gov/system/files/documents/2019/01/cyber_memo_12212018.pdf
- NY - Helper links (there are many – just research 23 NYCRR 500)
  - https://www.mdsny.com/how-to-meet-dfs-23nycrr-500-in-five-steps/
  - https://www.protiviti.com/sites/default/files/united_states/insights/decoding-nydfs-part500-protiviti.pdf
- EU GDPR
  - https://eugdpr.org/

Carrier – Vendor Integration

TO SUPPORT "STRAIGHT THROUGH PROCESSING"

Where is the Industry Headed?

- "Straight Through Processing" – "Automated Rating"
  - Many carriers want to be able to automate their back end processing. Instead of manually entering the final audited exposures into their policy system, they want to automate that process
  - Many carriers already do this today and many more will be moving to this in the coming years. Why? $
- Not all vendors in the industry are able to provide the data in a format reliable enough for automated rating
  - Collectively, as an industry, we need to get to a better place

State	Class Code	Description	Estimated Exposure	Final Exposure
AZ	9083	RESTAURANT - FAST FOOD	250,000	287,547
AZ	8810	CLERICAL OFFICE EMPLOYEES	50,000	78,953

WC Audit Summary – Anything Missing?

Policy Number	Policy Type	Policy Period	Audit Period
987766778	WC	1/1/2018 - 1/1/2019	1/1/2018 - 1/1/2019

Workers' Compensation Summary – Policy # 987766778

Entity	Location	State	Class Code	Classification Description	Exposure Type	Estimated Exposure	Final Exposure	Diff. %
1	1	AZ	9083 - 03	RESTAURANT: FAST FOOD	Payroll	250,000	**287,547**	15%
1	1	AZ	8810 - 01	CLERICAL OFFICE EMPLOYEES	Payroll	50,000	**78,953**	58%
1	2	AZ	9083 - 03	RESTAURANT: FAST FOOD	Payroll	200,000	**268,965**	34%
1	2	AZ	8810 - 01	CLERICAL OFFICE EMPLOYEES	Payroll	30,000	**25,123**	-16%
					Final Exposure:	**530,000**	**660,588**	**24.64%**

Entity & Locations

Entity #	Entity Type	Entity Description	Location Number	Location State	Location Description
1	Corporation		1	AZ	123 Main St Phoenix, AZ 12345
1	Corporation		2	AZ	432 Sunny St Mesa, AZ 54321

General Liability Summary – Policy # 6548321654

Entity	Location	State	Class Code	Subline	Classification Description	Exposure Type	Estimated Exposure	Final Exposure	Diff. %
1	1	CA	51116	334	AIR CONDITIONING EQUIPMENT MFG	Sales	2,000,000	**2,537,675**	27%
1	1	CA	51116	336	AIR CONDITIONING EQUIPMENT MFG	Sales	2,000,000	**2,537,675**	27%
1	2	AZ	51116	334	AIR CONDITIONING EQUIPMENT MFG	Sales	1,500,000	**1,235,655**	-18%
1	2	AZ	51116	336	AIR CONDITIONING EQUIPMENT MFG	Sales	1,500,000	**1,235,655**	-18%
						Final Exposur	**7,000,000**	**7,546,660**	**7.81%**

Entity & Locations

Entity #	Entity Type	Entity Description	Location Number	Location State	Location Description
1	Corporation		1	CA	234 Sunny Street Thousand Oaks, CA 12345
1	Corporation		2	AZ	432 Main Street Phoenix, AZ 54321

Straight Through Processing Takeaways

- The Summary Level Data sent back to the Carrier:
  - MUST BE ACCURATE 100% of the time
  - The carrier is doing the final transaction based off of the data returned
  - This is real money. Incorrect summary level data returned to a carrier could result in financial loss
  - Potential Professional Liability, (E&O) risk to vendors
- Make sure your systems can return location level and subline data at a minimum.

Thank You for Not Sleeping!

Mike Nahlovsky, MBA, CPCU, APA, CIPA

Nexus Insurance Services & Solutions, Inc.

President/CEO

mike@nexaud.com

952-697-4403