INSURANCE CYBERSECURITY WORKSHOP SERIES

Cybersecurity in the Boardroom

Monday, April 3, 2017
Philadelphia, PA
AGENDA

8:00 a.m.  Registration, Breakfast & Networking

8:30 a.m.  Welcome and Overview of NAIC Model Act/State Law Requirements
Jim Gkonos, Special Counsel, Saul Ewing LLP

9:20 a.m.  New York Regulations
Fred Garsson, Partner, Saul Ewing, LLP

10:10 a.m.  Break

10:25 a.m.  Developments in Cybersecurity Litigation and Federal Law
April Doss, Partner, Saul Ewing LLP

11:15 a.m.  Board Considerations
Featured Speaker: Ignacio Rivera, Deputy General Counsel & Chief Compliance Officer, Munich Re America

11:50 a.m.  Cyber Insurance Considerations
Jim Gkonos, Special Counsel, Saul Ewing LLP

12:00 p.m.  Audience Question & Answer

12:15 p.m.  Networking Lunch

1:00 p.m.  Program Adjourned
Cybersecurity in the Boardroom

April 3, 2017
Saul Ewing LLP – Philadelphia Office
Philadelphia, Pennsylvania

The NAIC Model Act

By: James S. Gkonos
WELL KNOWN RECENT CYBERATTACKS

SONY  citi  Aol.  Target  LinkedIn  Adobe  Starbucks  Neiman Marcus  City Council  New York State Public Service Commission

WELL KNOWN RECENT CYBERATTACKS (cont’d)

Japan Public Pension  IRS  Michaels

JPMorgan Chase & Co.  STAPLES  Anthem Blue Cross  The White House
2015 Cyber Attacks

2016 Cyber Attacks
IMPORTANT FACTS

- USA Today: As of 2015, 43% of companies had a security breach.

- 1093 data breaches were reported in 2016, up from 781 in 2015

- Average cost of a data breach globally was $3.8 million, while the average cost of a data breach in the U.S. is $6.5 million
  - The cost estimate for a large data breach is approx. $163 million

- The average cost per lost or stolen record containing confidential or sensitive data was $154 per record, but the average cost of a healthcare record was $363

- In 2014, over 246 million records were exposed, while in 2015 169 million records were exposed.

Cybercrime damage has been projected to reach $6 trillion annually by 2021

- According to the FBI, ransomware attacks occurred 4000 times a day in 2016
  - According to Kaspersky ransomware attacks on businesses occurred every 40 seconds in 2016

- In Q3 2016 alone, 18 million new malware samples were captured (average 200,000 per day)

- For the last 8 years the top means of cyber attack was a combination of phishing and hacking

- Cybersecurity spending is expected to exceed $1 trillion for the next five years (2017-2021). Current cybersecurity spending is estimated to be over 35 times the level of spending 13 years ago.
According to Microsoft, the average number of days that hackers went unnoticed after a breach was 200, and according to M-trends only 47% were discovered by the breached company, with 53% brought to their attention by law enforcement, media, customers, suppliers and in some cases, the hackers.

In a Trustwave survey, 81% of breach victims reported that they did not have a system in place to self-detect data breaches, but relied on external notification. Study also showed that self-detected breaches take an average of 14.5 days from intrusion to contain, while breach notification by an external party results in an average of 154 days to containment.

Fifty-two percent (52%) of companies that suffered successful cyber attacks in 2016 are not making any changes to their cyber security for 2017.

According to Barkly, sixty-two percent of companies surveyed were not planning to increase their cyber security budgets for 2017.

Cyber attacks are not limited to computer systems alone – at least one attack was reported to have use “smart” devices such as televisions and a refrigerator. 2016 DDOS (dedicated denial of service) attack on DYN used over 100,000 DVR’s and online cameras to overload servers.

These points of access will substantially increase, as the number of internet-connected devices, not including smartphones, PC’s and tablets, are expected to reach 2 billion in the next 5 years.

According to Intel, total number of connected devices (including smartphones, tablets and PC’s) could exceed 200 billion in 2020.

Microsoft projects that online data volumes by 2020 will be 50 times greater than today.
• 1 in 4 Chief Legal Officers (CLO) experienced a data breach in the last 2 years.

• Data/cybersecurity ranks only behind ethics/compliance and mergers/acquisitions in importance to CLOs.
  - Lloyds of London also reported that by 2013 cybersecurity had risen to no. 3 on the list of concerns of boards of directors.

• Only 1 in 3 reporting companies carries data breach protection insurance.

• Banking and Insurance Regulators are looking closely at data security but - GAO recently reported that banking regulators are not adequately analyzing risks across banking enterprises and that not all IT examiners are adequately trained.

• CSO Magazine/PWC 2015 study (of 500 corporate respondents) found that:
  - 28% of the boards have no presentations from security leaders;
  - 26% of security leaders make only an annual presentation to board; and
  - 42% did not view cybersecurity as a corporate governance issue.

• 2016 study by Tanium and Nasdaq taken of 1530 non-executive directors and C-level executives in the United States, United Kingdom, Germany, Japan and the Nordic countries found that over 90% cannot read a cybersecurity report and are not prepared to handle a major attack.

• Similarly, a 2015 NY Times survey found only 11% of companies’ boards reported a high level of understanding of cybersecurity issues

• A 2015 ISACA International report concluded that only 38% of global organizations believe they are prepared to handle a sophisticated cyber attack
• Insurance Regulatory Response

• March 26, 2015 – New York Department of Financial Services issued letter to NY domiciled insurance companies requiring enhanced examination procedures relating to cybersecurity.

• NYDFS has now promulgated final regulations regarding cybersecurity

• After the March 2015 NAIC Spring Meeting, the Cybersecurity (Ex) Task Force exposed for comment the draft Principles for Effective Cybersecurity Insurance Regulatory Guidance, containing 18 principles that were derived from principles proposed by the Securities Industry and Financial Markets Association (SIFMA).

At the NAIC 2015 Summer meeting, the NAIC Executive Committee adopted 12 principles for cybersecurity regulatory guidance:

Principle 1: Insurance regulators have a significant role and responsibility regarding protecting consumers from cybersecurity risks.

Principle 2: Insurance regulators have a significant role and responsibility regarding the insurers’ and producers’ efforts to protect identifiable customer information.

Principle 3: Insurance regulators have a significant role and responsibility in protecting the sensitive information housed in insurance departments and at the NAIC.
Principle 4: Compliance with cybersecurity regulatory guidance must be flexible, scalable, practical and consistent with the national efforts embodied in the National Institute of Standards and Technology (NIST) framework.

Principle 5: Regulatory guidance must be risk-based and consider the resources of the insurer or insurance producer.

Principle 6: Insurance regulators should provide appropriate regulatory oversight, which includes but is not limited to, conducting risk-based, value-added financial examinations and/or market conduct examinations regarding cybersecurity.

Principle 7: Planning for incident response for insurance regulators, insurers, and insurance producers is an essential component to an effective cybersecurity program.

Principle 8: Insurers, insurance producers, and other regulated entities and state insurance regulator should take appropriate steps to insure that third parties and service providers have controls in place to protect personally identifiable financial information.

Principle 9: Cybersecurity risks should be included as part of an insurers and insurance producers Enterprise Risk Management (ERM) process.

Principle 10: Information technology internal audit findings that present a material risk to an insurer should be reviewed with the insurers and board of directors or an appropriate committee thereof.

Principle 11: It is essential for insurers and insurance producers to use and information sharing and analysis organization (ISAO) to share information and stay informed regarding emerging threats or vulnerabilities, as well as physical threat intelligence analysis and sharing.

Principle 12: Periodic and timely training, paired with assessment, for employees of insurers and insurance producers, as well as other regulated entities and other third parties, regarding cybersecurity issues is essential.
October 17, 2015 the Cybersecurity (EX) Task Force adopted the “Cybersecurity Bill of Rights,” which provides that an insurance consumer has the right to:

- Know the types of personal information collected and stored by their insurance company, agent or any business they contract with;
- Expect their insurance company/agencies to have a privacy policy posted on their website and available in hard copy;
- Expect that their insurance company, agent, or any business they contract with to take reasonable steps to keep unauthorized persons from seeing, stealing or using their personal information;
- Get notice from their insurance company, agent or any business they contract with in the event of a data breach. The notice should:
  - Be sent by first class mail or e-mail (if agreed);
  - Be sent soon after the data breach (no more than 60 days);
  - Describe the information involved in the data breach and the steps that can be taken to protect against identity theft or fraud;
  - Describe the action the insurance company, agent or business they contract with has taken to keep their information safe;
  - Include contact information for three nationwide credit bureaus;
  - Include contact information for the company or agent involved;
- Get one year of identity theft protection paid by the company or agent; and
- Consumer rights in the event of identity theft, including getting fraudulent data removed from credit reports, freeze the credit report, and stopping debt collectors.

Application (Section 3 – Definitions)

- Covers breaches of data security, but does not include unauthorized acquisition of encrypted or otherwise protected personal information and the protection process (encryption) is not also released.

- Applies to all “licensees” – insurers, producers, and other persons required to be licensed under the Insurance Laws

- Protects “personal information,” which includes:
  - financial account numbers
  - credit card nos.
  - debit card nos.
  - name
  - non-truncated social security number
  - drivers license number
  - date of birth
  - user name and e-mail address
  - biometric information, health information
  - past or present mental or physical health information
  - payments made for the provision of health care
  - information provided by a consumer to buy an insurance product
  - information about a consumer obtained in the process of an insurance transaction or in providing insurance related services to consumers, or
  - or a list or grouping of consumers that is not publically available
Information Security Program (Section 4)

- Each “licensee shall develop, implement and maintain a comprehensive written information security program that contains administrative, technical and physical safeguards for the protection of personal information.”

- The program is scalable depending on size, complexity and activities of the licensee, as well as activity and sensitivity of the information possessed, but no guidance is given on how to adapt the model act to licensees of different sizes or complexity of information.

Information Security Program (Section 4) (cont’d.)

- The security program “shall” be designed to protect:
  - Security and confidentiality of personal information.
  - Against any anticipated threats to the security and integrity of personal information.
  - Against unauthorized access and minimize the likelihood of harm or inconvenience to a consumer.
Information Security Program (Section 4) (cont’d.)

- Licensees must appoint employee(s) to identify and assess:
  - “reasonably foreseeable internal and external threats”,
  - the potential damage from such threats, and
  - the sufficiency of the policies, procedures, and safeguards to control such risks
- Licensees must address the risks in the ERM process and use an information sharing and analysis organization to share information.

Information Security Program (Section 4) (cont’d.)

- Licensee must use “generally accepted cybersecurity principles”, and adopt certain security measures, including:
  - Restrict and control information systems and access to physical locations containing personal information;
  - Encrypt electronic personal information;
  - Utilize state-of-the-art techniques, such as multi-factor authentication procedures;
  - Regularly test and monitor procedures to detect actual and attempted attacks;
  - Implement response programs when a licensee suspects that unauthorized access has been gained to personal information; and
  - Stay informed of generally accepted cybersecurity principles.
Information Security Program (Section 4) (cont’d.)

- Board or a committee of the Board, at a minimum, must:
  - approve the security program,
  - oversee the development and implementation of the program,
  - assign responsibility for the program and
  - review management reports (to be received at least annually)

- Licensees must oversee and require third party service provider compliance with the licensee’s information security requirements.

Notice (Section 6)

- Pre-breach Notice – None now required – first draft required notice of privacy policy.

- Post –breach Notice – In the event of any breach licensee must notify:
  - appropriate state and federal law enforcement agency;
  - insurance commissioner of licensee’s state of domicile and any state in which a consumer whose information was compromised resided;
  - any relevant payment card network;
  - each nationwide consumer reporting agency; and
  - the affected consumers.
Notice (Section 6)(cont’d.)

• Commissioner notification - licensee must notify the commissioner within 3 days to provide information including:
  • description of how and when the system was breached,
  • number of state consumer residents affected,
  • if, and how, the data was encrypted
  • extent of remedial efforts,
  • identification of other regulatory agencies notified,
  • the results of any internal review of whether procedures were followed, and
  • a copy of the licensee’s privacy and data breach policies

• As “expeditiously as possible” after a data breach, licensee must notify affected consumers, but a draft must be provided first to the Commissioner, which the Commissioner shall have the right to review for compliance.

• The notice must provide a summary of the steps consumers can take to protect themselves against identity theft or fraud, contact information for 3 credit reporting agencies, and an offer to provide identity theft information by the licensee.

Legal Rights (Sections 7-8)

• Commissioner can prescribe the required level of consumer protection after a breach.

• Commissioner may hold hearing if he has “reason to believe” that a licensee is engaged in conduct that violates the act.
  • Penalties can include fines and license revocation.

• Original draft provided for a private right of action and attorneys fees if person whose rights are violated prevails, but this provision was deleted from the second draft.

• Information provided to the Commissioner under the Act is confidential and not subject to discovery in third-party litigation.
Current Status: Due to numerous comments to the August amendments, the Cybersecurity Task Force is engaging in further discussions with industry members, and has produced a February 27, third draft:

- Highlights:
  - Act does not intend to require duplication of federal or other state law but other law must provide at least the same minimum level of protection
  - “Nonpublic Personal Information” (NPI) now also includes:
    - the fact that a consumer is or was a customer
    - Any information provided by customer to Licensee or agent
    - Any information collected through an “internet cookie”
    - Any information from a “consumer report”
  - NPI does not include any information that does not include any “personal identifiers”
  - Licensee’s Information Security Program must be updated in writing whenever any “substantive changes” occur but no less than annually

Highlights – 2/27 draft (cont’d.)

- Replaced concept of “generally accepted cybersecurity principles” with “best practices” and “reasonable security measures”
- Explicitly requires executive management that delegates responsibilities to oversee the security program and to receive report similar to the types it is obligated to provide the board
- Data breaches now split into those with and without “use of personally identifiable information”
  - While all breaches have to be reported to the domicile commissioner, only breaches “with” use of personally identifiable information are subject to other notification and remediation requirements
  - Notice to consumers only required in states in which PII of consumers in state is affected by data breach
Highlights – 2/27 draft (cont’d.)

- Requires notification on website or broadcast media if written or electronic notification not feasible
- Licensee can rely on third-party vendor to provide notification as long as licensee confirms notice was conforming and actually sent
- If breach occurs with reinsurer or third-party vendor with no contractual relationship with consumer or producer, Licensee shall provide notice to consumers
- 12 month minimum period of required identity theft protection now changed to “appropriate period”
- As of 3/23 no new exposure draft

What Do Insurance Companies Need To Do?

- Must be cognizant of competing or inconsistent requirements for cybersecurity in states in which they are licensed – likely will need to comply with most stringent requirements

- Depending on Size – should consider creating a specific position, such as a Chief Information Security Officer or equivalent position to focus solely on cybersecurity.
  - Outside Experts
    - Could be hired if company is not in position to hire a full-time personnel
    - Could be utilized by CIO, CTO, or CPO to assist with legal or technical issues
    - Could be utilized to audit or assess cybersecurity practices and data protection systems and suggest areas for improvement
- C-level executives, including Chief Legal Officer, need to become more technologically savvy.
  - A Law360 study from May, 2015 asked company executives to identify areas where general counsel or chief legal officers could most benefit from additional expertise.
  - 67% of executives chose cybersecurity as their first choice (by way of reference 30% of the executives suggested crisis management).
  - Given the reputational risk issues and the potential for economic harm, cybersecurity should become a regular board agenda item, including regular presentations by officers (GC, CIO, CTO).

- Board should become more conversant and educated with cybersecurity issues and the company’s cyber securities practices and protocols.
  - Some corporations (only 42 of the S&P 500) have created board level risk committees responsible for privacy and security risks, with clear lines of reporting and authority. The committee should meet regularly and report directly to the board.
  - Briefings should occur on at least a quarterly basis and the board should make adequate time on the agenda.

- Board should focus on and require that the company has identified and classified its data.
  - Health data, personal information, financial information is particularly sensitive and the subject of statutes and regulations requiring heightened security.
• Board should ensure that the company has written security standards and practices

  - Can be prepared by CIO, CTO, CPO, with outside consultant input.
  - Should be reviewed by counsel.
  - Board should ensure that they are periodically reviewed and updated.
    - While NYDFS has removed specific timing deadlines, Board should ensure that they are reviewed at least annually by CISO or senior management, and quarterly is probably a best practice due to the quickly changing technological environment.
  - A 2015 BDO study showed that only 45% of responding companies had an incident response plan.

• Board should ensure that the company establishes a cross-functional incident response team, which will

  - Investigate and respond to data breach.
  - Document the company’s efforts to address the cause of such breach.
  - Propose and effect any other remedial steps necessary.
  - Engage in case-studies or other exercises to ensure the team is adequately trained.
QUESTIONS?
Jim Gkonos focuses his practice on insurance and reinsurance regulatory matters, contract and treaty interpretation and reinsurance disputes. He is a certified reinsurance arbitrator. As a former division general counsel of a large domestic property and casualty carrier, Jim has significant experience with and knowledge of the regulatory issues facing domestic carriers. He was responsible for the drafting and interpretation of the reinsurance treaties placed annually by the division and has been involved in the commutation of hundreds of reinsurance treaties.

Jim assists clients on issues relating to financial guarantees, surety bonds and the intersection between insurance and the capital markets. He frequently represents clients that have problems and issues with insurance companies in runoff and liquidation. He has structured securitized international financial transactions backed by insurance guarantees and has substantial international experience in the restructure of financially impaired, insolvent or bankrupt entities. Jim also conducted, managed and supervised substantial litigation in the United Kingdom, Japan, China, Argentina, Brazil and the Virgin Islands and brings more than 25 years of domestic litigation experience to the Insurance Practice.

Jim also previously served for nine years as senior counsel advising the Rehabilitator of one of the largest insurance insolvcencies in the United States - Mutual Fire Marine and Inland Insurance Company, In Rehabilitation. In that position, Jim was responsible for interpretation of insurance insolvency laws, negotiation and commutation of reinsurance treaties, documentation of more than 13,000 claim settlements and managing reinsurance arbitrations and the litigation against the insolvent company’s MGA’s and accountants.

As complex regulations governing the insurance and re-insurance continue to evolve, Jim has become a frequent speaker and author on numerous insurance topics, including the impact of the subprime defaults on the insurance and capital markets, changes in state and federal regulatory environments and how the challenging economic climate impacts the insurance and financial markets.
He is admitted to practice before the U.S. Court of Appeals for the Third Circuit, the U.S. Court of Appeals for the Federal Circuit, the U.S. District Court for the Eastern District of Pennsylvania, the U.S. Court of International Trade and the Supreme Court of Pennsylvania.

Honors and Awards

- Named to “Who’s Who Legal” list for Insurance and Reinsurance, 2016

Memberships and Affiliations

- Member, Federation of Regulatory Counsel
- Member, ABA Litigation Section
- Member, ABA International Law Section
- Member, ABA Accountants’ Liability Subcommittee of the Professional Liability Committee, Litigation Section
Ten Things Insurers and Insurance Producers Need To Know About New York’s Cybersecurity Regulation

April 3, 2017

Frederic M. Garsson

1. What is the Purpose of the Cybersecurity Regulation?
1. What is the Purpose of the Cybersecurity Regulation?

   • “[T]o promote the protection of customer information as well as the information technology systems of regulated entities.”

2. Who does the Cybersecurity Regulation cover?
2. Who does the Cybersecurity Regulation cover?

- “Covered Entities” defined as “any Person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law or the Financial Services Law.”

3. What does the Cybersecurity Regulation require of Covered Entities?
3. What does the Cybersecurity Regulation require of Covered Entities?

• “This regulation requires each company to assess its specific risk profile and design a [cybersecurity] program that addresses its risks in a robust fashion.”

4. What are the six (6) “cybersecurity functions” that Covered Entities must perform in connection with their Cybersecurity Programs?
4. What are the six (6) “cybersecurity functions” that Covered Entities must perform in connection with their Cybersecurity Programs?

- Remember by Acronym: I-P-D-R-R-F (This is a joke)
  1. IDENTIFY (and Assess) RISKS
  2. PROTECT
  3. DETECT
  4. RESPOND
  5. RECOVER
  6. FULFILL

5. What are the requirements for the Cybersecurity Policy and what areas must be addressed?
5. What are the requirements for the Cybersecurity Policy and what areas must be addressed?

- Must be written
- Must be approved by a Senior Officer or the Board of Directors
- Must be based on the Covered Entity’s Risk Assessment and address the following (“to the extent applicable”):

  Cybersecurity Policy – “address”:
  
  (1) information security;
  (2) data governance and classification;
  (3) asset inventory and device management;
  (4) access controls and identity management;
  (5) business continuity and disaster recovery planning and resources;
  (6) systems operations and availability concerns;
  (7) systems and network security;
  (8) systems and network monitoring;
  (9) systems and application development and quality assurance;
  (10) physical security and environmental controls;
  (11) customer data privacy;
  (12) vendor and Third Party Service Provider management;
  (13) risk assessment; and
  (14) incident response.
6. What is an Incident Response Plan and what are the seven (7) areas must be addressed in the Incident Response Plan?

- A written plan, designed to promptly respond to, and recover from, any Cybersecurity Event that materially affects the Covered Entity’s Information Systems or the continuing functionality of the Covered Entity’s business or operations.
(1) the internal processes for responding to a Cybersecurity Event;
(2) the goals of the incident response plan;
(3) the definition of clear roles, responsibilities and levels of decision-making authority;
(4) external and internal communications and information sharing;
(5) identification of requirements for the remediation of any identified weaknesses in Information Systems and associated controls;
(6) documentation and reporting regarding Cybersecurity Events and related incident response activities; and
(7) the evaluation and revision as necessary of the incident response plan following a Cybersecurity Event.

7. Are there any Notices and/or Reports that must be filed?
7. Are there any Notices and/or Reports that must be filed?

- Notice to the Superintendent of a Cybersecurity Event.
- Annual Written Statement to the Superintendent.
- At least Annually, a written Report of the Chief Information Security Officer to the Board of Directors or Governing Body.

8. Is there a Transition Period? Yes
8. Is there a Transition Period? Yes

- The regulation became effective March 1, 2017.
- First Certification of Compliance will be due on February 15, 2018.

Transition Period

1. **180 days Requirements:**
   - Cybersecurity program (sec. 500.02)
   - Cybersecurity policy (sec. 500.03)
   - Designate CISO (sec. 500.04(a))
   - Least privilege access (sec. 500.07)
   - Qualified cyber personnel with training (500.10)
   - Written incident response plan (500.16)
   - Notification to NYDFS (500.17)

2. **One Year Requirements:**
   - Annual Report to the Board (sec. 500.4(b))
   - Penetration Testing (sec. 500.5)
   - Risk Assessment (sec. 500.9)
   - Multi-Factor Authentication (sec. 500.12)
   - Personnel Training (sec. 500.14(b))

3. **18 Month Requirements:**
   - Audit Trail (sec. 500.6)
   - Application Security (sec. 500.8)
   - Limitation on Data Retention (sec. 500.13)
   - Monitoring of Authorized Users (sec. 500.14(a))
   - Encryption of Nonpublic Information (sec. 500.15)

4. **Two Year Requirement:**
   - Third Party Service Provider Security Policy (sec. 500.11)
9. What is required with respect to a Third Party Service Provider Security Policy?

- Covered Entities are required to have a TPSP Security Policy (two-years to comply).
- Must be written.
- Based on the Risk Assessment, and must address (“to the extent applicable”) four (4) areas.
- Limited exception.
10. Are there any exemptions (for example, for small companies)?

1. “Limited” Exemption for certain small entities.
2. Exemption for an employee, agent, representative or designee of a Covered Entity, who is itself a Covered Entity, to the extent it is covered by the cybersecurity program of the Covered Entity.
3. “Limited” Exemption for a Covered Entity that does not directly or indirectly operate, maintain, utilize or control any Information Systems, and that does not, and is not required to, directly or indirectly control, own, access, generate, receive or possess Nonpublic Information.
   1. (1), (2), (3) and (4) must file a Notice of Exemption.
5. Exemption (provided such Persons do not otherwise qualify as a Covered Entity): Charitable annuity societies; Risk retention groups not chartered in this state; and any accredited reinsurer or certified reinsurer.
Fred Garsson is a seasoned insurance and reinsurance regulatory attorney who concentrates his practice on advising insurance industry clients on matters involving U.S. federal and state insurance laws and sophisticated national and international regulatory matters.

Fred has vast experience representing and counseling insurers, reinsurers and insurance producers in corporate and regulatory matters, including holding company transactions compliance, reinsurance and assumption transactions, organizing and licensing of insurance companies, insurance producers, reinsurance intermediaries and independent insurance adjusters. He also has experience drafting and analyzing insurance policies, annuity contracts, reinsurance agreements and other complex contracts, including agency and brokerage agreements.

In addition, Fred has represented clients in connection with the regulatory aspects of sales and mergers and acquisitions of insurance and reinsurance companies. He has also represented clients before numerous state insurance agencies, and advises insurance industry clients with respect to corporate and insurance regulatory and compliance matters. Such matters include rebating, transacting an unauthorized insurance business, aiding unauthorized insurers, statutory accounting issues regarding obtaining financial statement credit for unauthorized ceded reinsurance, financial condition examinations, the permissibility of insurance company investments, policy cancellation and non-renewal requirements, stock redemptions, quasi-reorganizations, demutualizations, forming purchasing groups and captive insurers, piercing the corporate veil, declaring and paying policy and corporate dividends, Regulation XXX securitizations and life settlements securitizations.

In addition to his New Jersey and New York bar admissions, Fred is admitted
to practice before the U.S. District Court for the District of New Jersey.

Experience

- Coordinating multijurisdictional insurance and reinsurance research projects for major U.S. and non-U.S. insurers
- Advising U.S. insurers concerning the Terrorism Risk Insurance Program Reauthorization Act of 2007 and the nonadmitted insurer and reinsurance requirements of the Dodd-Frank Act
- Advising the U.S. claims and underwriting personnel of a global insurer concerning antitrust issues
- Representing individual insurance brokers in disciplinary matters before the Insurance Division of the New York Department of Financial Services
- Advising an offshore captive insurer in connection with its redomestication to the U.S. and its ongoing onshore insurance regulatory requirements
- Reviewing a major U.S. insurer’s compliance program and training in-house attorneys concerning identifying compliance gaps
- Advising the governments of foreign countries concerning drafting and amending their insurance laws and regulations
- Advising a leading insurer and its non-insurer parent on insurance and reinsurance regulatory matters in connection with a private offering of insurance related securities and a subsequent initial public offering

Memberships and Affiliations

- Member, Federation of Regulatory Counsel
- Insurance Law Committee, New York City Bar Association
What to Expect in 2017: Cybersecurity Threats and the Federal and International Landscape

April Doss
April, 2017

Key Trends to Watch in 2017

- Cybersecurity threat landscape
- Federal agencies
  - What will change with the new administration?
- U.S. federal action
  - Legislation
  - Executive orders
  - Guidance and standards
- International cybersecurity requirements
  - Preparing for GDPR
Cybersecurity Threat Landscape

- Data breach
  - PII, PHI, IP, business information
- Ransomware
- Internet of Things
  - Physical effects from virtual attacks
- Insider threat
- Spearphishing and whaling
- Nation-states
- Information operations

Federal Agencies

- What to expect in a new administration?
  - FCC
  - FTC
  - CFPB
  - SEC
  - DHHS OCR
- Two priorities in tension:
  - Rolling back regulations
  - Increasing emphasis on cyber
U.S. Federal Developments in 2017

• Executive action:
  ▪ Cybersecurity Task Force
  ▪ Cybersecurity Executive Order (Draft)

• Congressional action:
  ▪ Main Street Cybersecurity Act (Bill)

• Guidance and best practices:
  ▪ NIST Framework update

Global Cybersecurity Requirements

• European data protection law
  ▪ Existing Data Protection Directive being replaced by General Data Protection Regulation (GDPR)
  ▪ GDPR takes effect May 2018
  ▪ Requires notice of breach within 72 hours
  ▪ Heavy fines for failure to protect personal data:
    ▪ For data controllers, €20M or 4% global annual turnover
    ▪ For data processors, €10M or 2% of global annual turnover

• Data protection laws in other countries
Predictions for 2017

- Continued growth and expansion of threat landscape
  - Continued or increased vulnerability to insider threat
  - Increased focus on third party liability/risk
- Regulatory landscape
  - Uncertainty in federal regulatory landscape
  - Increase in state regulatory efforts
  - Increase in sector-specific efforts
  - Voluntary standards or model laws and regulations
- Increased cost and complexity in international context
- Continued business impact
  - Customer fatigue
  - Uncertainty in litigation
  - Business interruption and reputation

Questions?
April F. Doss  
**Partner**

Baltimore Office  
500 E. Pratt Street  
Baltimore, Maryland 21202-3133

Phone: (410) 332-8798  Fax: (410) 332-8178  
Email: adoss@saul.com

Data privacy and cybersecurity have emerged as top concerns facing corporations and other organizations today. As the former Associate General Counsel for Intelligence Law at the National Security Agency (NSA), April Doss offers clients significant insight into some of the most highly regulated activities in the United States intelligence community. In this role, she gained significant experience with legal issues relating to big data, including privacy and compliance programs, particularly within the telecommunications, technology, and defense sectors of the economy. April advises clients on regulatory and corporate ethics and compliance best practices. She also provides a wide range of legal services to intelligence, defense, and homeland security sector clients who are engaged in cleared conversations with the vast network of federal agencies that govern and impact those arenas. Her experience as in-house counsel to a private college allows her to apply her cybersecurity perspective to the needs of higher education sector clients.

April’s substantial experience makes her well-qualified to provide practical, hands-on legal advice that takes into account the real-world implementation challenges of data privacy and cybersecurity programs. Over the course of her career at the NSA, April managed operations; oversaw a complex, multi-site compliance program; and she served as part of the senior management team for NSA’s new technology development. Based on her many years of experience as in-house counsel, she understands the need for legal advice to be specifically tailored to the budgetary, operational, and cultural realities of each institution and client that she serves. This practical approach, coupled with her deep understanding of technology, has earned her a reputation as a lawyer who “gets it” – whose advice translates easily from advising corporate boards and officers on strategic and reputational risk, to advising business units on the cybersecurity and privacy risks associated with their operations.

**Areas of Experience**

April advises clients in the following areas:

**Practices**
- Business and Finance
- Commercial Litigation
- Technology and Manufacturing Litigation
- Higher Education
- Corporate Governance
- Regulatory, Compliance and Government Defense and Government Contracts
- White Collar and Government Litigation
- Telecommunications
- Health Care

**Education**
- J.D., University of California, Berkeley, Boalt Hall School of Law, 1992
- M.F.A., Goucher College, 2001
- B.A., magna cum laude, Yale University, 1989

**Bar Admissions**
- California, Maryland
• Security breach preparation and response
• Data privacy and cybersecurity litigation
• Regulatory matters and internal compliance programs
• Big data governance and privacy in technology development
• Electronic surveillance and national security, including cooperative and compulsory process
• Strategic counseling and board governance
• Corporate counseling for providers of cybersecurity services

Honors and Awards

• Two-Time Recipient of the National Intelligence Meritorious Unit Citation
• Recipient of the Torchbearer Award, recognizing innovation in privacy and compliance

Memberships and Affiliations

• International Association of Privacy Professionals (IAPP)
• The Sedona Conference
  • Working Group 6 (Electronic Information Management, Discovery and Disclosure)
  • Working Group 11 (Data Security and Privacy Liability)
• Member, Maryland State Bar Association
• Member, American Bar Association, Section of Science & Technology Law
• Member, Board of Directors, Maryland Volunteer Lawyers for the Arts
"Boards that choose to ignore, or minimize, the importance of cybersecurity oversight responsibility, do so at their own peril."

Business Judgment Rule

The following test was constructed in the opinion for Grobow v. Perot, 539 A.2d 180 (Del. 1988), as a guideline for satisfaction of the business judgment rule. Courts apply the business judgment rule and presume that directors and officers:

- acted in good faith;
- acted in the best interests of the corporation;
- acted on an informed basis;
- not be wasteful;
- not involve self-interest (duty of loyalty).

A Board’s Duty to Monitor and Oversee Corporate Risk

In In re Caremark International Derivative Litigation, 698 A.2d 959 (Del.Ch. 1996), Delaware courts outlined the scope of a board’s duty to monitor and oversee corporate risk.

However, they noted that liability for failure to monitor risk can only be imputed to individual board members where: "(a) the directors utterly failed to implement any reporting or information system or controls; or (b) having implemented such a system or controls, consciously failed to monitor or oversee its operations thus disabling themselves from being informed of risks or problems requiring their attention."
Numerous demand and derivative complaints to sue the officers and directors of Target for breach of their fiduciary duties of good faith, loyalty, and due care;

The Target Special Litigation Committee spent 21 months investigating and reviewing Target’s pre and post breach status and many other factors, the Committee determined that it was not in Target’s best interests to pursue claims against the officers or directors identified in the Demand and derivative complaints.

The Minnesota District Court, in granting the motion to dismiss the derivative actions, adopted the report of the Special Litigation Committee. The report basically provides an extensive roadmap about corporate, officer and director responsibilities before, during and after a massive data breach.

Factors the Committee Considered:

- The pre-breach existence and content of Target’s policies and procedures designed to establish a reasonable information security program;
- The pre-breach existence and content of Target’s compliance policies and procedures and audit procedures;
- Management’s reports to the Board’s Audit and Corporate Responsibility Committees covering Target’s data security program, including compliance efforts and assessments of Target’s data security and privacy programs;
- Target’s pre-breach plans for continuous improvement of its data security systems and controls;
- Target’s utilization of third-party experts and consultants to help it evaluate its data security program;
- Reports that were made to Target’s officers, Directors and Audit Committee that it had been assessed as compliant.
Palkon ex rel. Wyndham Worldwide Corp. v. Holmes

April 2008 to January 2010, Wyndham sustained three data breaches that resulted in the theft of credit card and other personal information of over 600,000 customers.

Plaintiff filed a derivative action alleging that Wyndham’s board of directors, president/CEO and general counsel breached their fiduciary duties of care and loyalty to the company, and wasted corporate assets, by (1) failing to implement adequate data security mechanisms and internal controls to protect customers' personal and financial information and (2) failing to timely disclose the breaches and causing the company to conceal the breaches from investors.

In a footnote, the court noted that, although it did not need to consider the merits of the proposed action, the claims were potentially weak because the company had installed cybersecurity measures before the first data breach, and the board had addressed such concerns numerous times.

Securities and Exchange Commission Disclosure Guidance

The Securities and Exchange Commission released disclosure guidance regarding public company disclosure obligations relating to cybersecurity risks and cyber incidents. Specifically, the Disclosure Guidance addresses disclosure considerations applicable to both cybersecurity risks and cyber incidents under the following provisions:

1. Risk Factors
2. Management’s Discussion and Analysis of Financial Condition and Results of Operations
3. Description of Business
4. Legal Proceedings
5. Financial Statement Disclosures
6. Disclosure Controls and Procedures
7. Form 8-K
Executive Order

Framework for Improving Critical Infrastructure Cybersecurity

1) Describe their current cybersecurity posture;
2) Describe their target state for cybersecurity;
3) Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process;
4) Assess progress toward the target state;
5) Communicate among internal and external stakeholders about cybersecurity risk.

Insurance Data Security Model Law

Oversight by Board of Directors:

1) Oversee the development, implementation, and maintenance of the company’s Information Security Program;
2) Require the company’s executive management to report in writing at least annually, the following information:
   (a) The overall status of the Information Security Program and the company’s compliance with this Act; and
   (b) Material matters related to the Information Security Program, addressing issues such as risk assessment, risk management and control decisions, Third-Party Service Provider arrangements, results of testing, Data Breaches or violations and management’s responses thereto, and recommendations for changes in the Information Security Program.
NYS DFS Cybersecurity Requirements

- Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity’s Information Systems;
- Each Covered Entity shall implement and maintain a written policy or policies approved by a Senior Officer or the Covered Entity’s board of directors;
- Each Covered Entity shall designate a qualified individual responsible for overseeing and implementing the Covered Entity’s cybersecurity program and enforcing its cybersecurity policy;
- The CISO of each Covered Entity shall report in writing at least annually to the Covered Entity’s board of directors;
- Each Covered Entity shall establish a written incident response plan designed to promptly respond to, and recover from, any Cybersecurity Event.

Cyber-Risk Oversight

Directors need to understand:

- Cyber risk is broader than the annual IT budget;
- Understand the specific cyber threats that are most material to the organization.
- What are the company’s most critical data assets?
- Where are they located?
- Who has access?
- How are they protected?
Given the pace of change, Directors should routinely be kept up to date on legal implications of cyber risks as they relate to their company’s specific circumstances.

Requires staying informed about the changing legal and regulatory landscape;
Director Education;
Meeting at least annually with CISO and CIO;
Consider Cyber Expert on Board

Consider bringing in cybersecurity expertise, and cyber-risk management issues should be given regular and adequate time on board meeting agendas.

- Bring additional expert perspectives on cybersecurity into the boardroom by scheduling deep-dive briefings with third-party experts;
- Leaders from law enforcement, and/or
- Leveraging the board’s existing independent advisors.
- Document discussions in Board minutes;
Directors should challenge management to make sure an enterprise-wide cyber-risk management framework with adequate staffing and budget is established.

Board Committee on Enterprise Risk or Technology;
Dedicated CISO
Incident Response Plan;
   Cyber breach coach;
   Forensics experts;
   Communications;
   Notification/call centers;
   Credit Monitoring;
   Detection tools;

Board-management discussions should consider cyber risks in all aspects of the organization

- New business plans and product offerings/market entry;
- Mergers and acquisitions/due diligence;
- Deployment of new technologies;
- Major capital investment decisions such as facility expansions or IT system upgrades;
- Vendor Contracts/Outsourcing;
- Reputational Risk;
Our Experience

- Established an enterprise-wide Risk Management Committee;
- Considered ourselves a low profile target (no credit cards, customer accounts, etc.);
- It was not on our radar until after the well publicized cyber breaches;
- Began seeing the issue in vendor contracts/allocation of cyber breach liability;
- Led to purchase of Cyber liability insurance;
- Material increases in IT budget spend;
- Acceleration of Cyber Incidents;
- Table top exercises/employee phishing testing/weakest link/auditing

The Risk Management Committee

Our Risk Management Committee was established in 2008 and is comprised of representatives appointed by the Board of Directors of the participating Regional Operating companies for the primary purpose of reporting and recommending to the Board of Directors the overall enterprise risk management framework of the US companies. The Committee has oversight responsibility for the establishment, ongoing implementation and effective operation of an appropriate risk management process, its policies and procedures. “Risk” in this context means the degree of uncertainty involved in attaining planned goals and thus embraces not only risks of loss but also of opportunities for profit.
Available third-party coverages include:

- **Litigation and regulatory.** (lawsuits, judgments, settlements or penalties)
- **Regulatory response.** (legal, technical or forensic services necessary to assist in responding to governmental inquiries coverage for fines, penalties, investigations or other regulatory actions.
- **Notification costs.** (the costs to notify customers, employees or other victims)
- **Crisis management.** (Covers crisis management and public relations expenses)
- **Credit monitoring.** (credit monitoring, fraud monitoring or other related services)
- **Media liability.** Provides coverage for media liability, including coverage for copyright, trademark or service mark infringement resulting from online publication by the insured.
- **Privacy liability.** (liability to employees or customers for a breach of privacy).

The types of first-party coverage available include:

- **Theft and fraud.** (destruction or loss of the policyholder’s data as the result of a criminal or fraudulent cyber event, including theft and transfer of funds).
- **Forensic investigation.** (legal, technical or forensic services necessary to assess whether a cyber attack has occurred, to assess the impact of the attack and to stop an attack.
- **Business interruption.** (lost income and related costs where a policyholder is unable to conduct business due to a cyber event or data loss).
- **Extortion.** (costs associated with the investigation of threats to commit cyber attacks against the policyholder’s systems and for payments to extortionists who threaten to obtain and disclose sensitive information).
- **Computer data loss and restoration.** (physical damage to, or loss of use of, computer-related assets, including the costs of retrieving and restoring data, hardware, software or other information destroyed or damaged as the result of a cyber attack).
Identify Your Unique Risks.
Understand Your Existing Coverage.
Buy What You Need.
Secure Appropriate Limits and Sublimits. Your company should try to match its limits of liability with its realistic exposure in the event of a cyber loss.
Beware of Exclusions. Often, coverage for a loss or claim depends on the language in policy exclusion as opposed to the language in the grant of coverage.
Get Retroactive Coverage.
Consider Coverage for Acts and Omissions by Third Parties.
Evaluate Coverage for Data Restoration Costs.

Involve All Stakeholders.
Take Advantage of Risk Management Services.
Dovetail Cyber Insurance with Indemnity Agreements.
Understand The “Triggers.” Some policies are triggered on the date the loss occurs, while others are triggered on the date that a claim is made against the insured.
Consider Coverage for Loss of Information on Unencrypted Devices.
Consider Coverage for Regulatory Actions.
Questions? Thank You.
Ignacio Rivera is Deputy General Counsel, Chief Compliance Officer and Assistant Secretary of Munich Reinsurance America, Inc. Ig has been with Munich Re America since 1991. During his time at Munich Re America, Ig has advised on corporate governance for the board of directors and its committees, compliance with annual and periodic financial reporting requirements under the insurance laws, prepared registration statements in connection with the offering of equity and debt securities to the public, managed numerous mergers, acquisitions, divestitures and strategic and infrastructure investments, as well as taking the U.S. Holding Company public and then private again. He has also represented the Company in real estate matters, general corporate contracts, and the registration and maintenance of an NASD registered broker-dealer.

As the Chief Compliance Officer for MRAm he has primary responsibility for the Company’s corporate compliance programs including Code of Conduct and a broad range of other corporate matters including Privacy, Financial Crime, Antitrust and Financial Sanctions.

Prior to joining MRAm, Ig was an associate in the Corporate Department of Dewey, Ballantine, Bushy, Palmer & Wood where he gained experience in public and private financings, mergers and acquisitions, federal securities law and state insurance laws.

He is a graduate of Brooklyn Law School where he was a recipient of the Dean's Academic Achievement Scholarship and the Rotenburg Prize in Antitrust Regulation. He received his Bachelor of Science in Business Management from Long Island University at C.W.Post.
Cybersecurity in the Boardroom

April 3, 2017
Saul Ewing LLP – Philadelphia Office
Philadelphia, Pennsylvania

Cyber Insurance –
An Introduction

By: James S. Gkonos
Cybercrime damage has been projected to reach $6 trillion annually by 2021.

According to the FBI, ransomware attacks occurred 4000 times a day in 2016. According to Kaspersky ransomware attacks on businesses occurred every 40 seconds in 2016.

In Q3 2016 alone, 18 million new malware samples were captured (average 200,000 per day).

Cybersecurity spending is expected to exceed $1 trillion for the next five years (2017-2021). Current cybersecurity spending is estimated to be over 35 times the level of spending 13 years ago.
• 2015 Association of Corporate Counsel Study

  • 1 in 4 Chief Legal Officers (CLO) experienced a data breach in the last 2 years.

  • Only 1 in 3 reporting companies carries data breach protection insurance.

• A note about insurance coverage

  • Coverage is in its formative stage, so policies can greatly differ.
    • Companies would likely find it useful to hire a knowledgeable broker.
    • Carriers are often paired with cybersecurity consultants who analyze the company’s security deficiencies for underwriting purposes.
    • Insurance considerations
      • Company must figure out what it can afford to pay out-of-pocket for a cyber loss – will determine retention or deductible.
Cyber Insurance Coverage – still primarily manuscripted

- Recent Cambridge Business School report found coverage can come from
  - Stand alone Cyber cover
  - Affirmative Cyber endorsements
  - Gaps in explicit Cyber exclusions
  - Silent Cyber exposure
- Cambridge report found 35 insurers offering 26 different insurance products offering collectively coverage for 19 types of losses, but...
  - Only 81% covered incident response costs
  - Only 69% covered business interruption
  - Only 62% offered regulatory and defense coverage
  - Only 13% offered officer and director liability coverage

- Cyber Insurance coverage
  - Understand what event triggers coverage – must be suited to company’s data usage and systems.
  - Exclusions – must ensure that primary risks are included.
  - Data coverage – policy must be consistent with company usage.
  - Breach response costs – should cover at least crisis management and breach notifications, credit monitoring, loss of business income, privacy regulatory defense and penalties, forensic investigations, legal fees, hacker damage costs.
  - Vendor/counsel selection – can company select its own?
- Very important for insureds to read and understand coverage carefully due to the wide variety of coverages and the manuscript nature of policies