Everett Carbajal, Esq. | The Carbajal Law Firm, P.C. | Everett@GlobalBusinessLawFirm.com
October 18, 2018 | Business Law Section | Fall Meeting | Technology and Venture Law Committee

Re: Cyber Security Insurance Policy Questionnaires and Best Practices

---

Cyber security insurance application questionnaires are used by carriers to evaluate an applicant's cyber-security posture, and such questionnaires can also provide guidance on cyber security best practices. Indeed, the RAND Corporation reviewed 44 application questionnaires and issued a Working Paper[1] in September 2017 that divided the questionnaire categories into the following main groups:

- Organizational Questions (concerning the applicant company's collection and use of data);
- **Technical Questions;**
- **Policies & Procedures Questions**, and
- Legal & Compliance Questions

With a focus on the Technical and Policy & Procedure questions, I conducted a review of a handful of cyber security insurance applications. Below is a summary of the main question categories:

1. Technical

- Details about a company's use of Encryption Technology for all sensitive data
    - Material in transit; and
    - Material in mobile devices

- Existence of and details about the use of a Firewall

- Utilization of Anti-Virus Software
    - Virus Software update details
    - Virus scan processes for:
        - Emails;
        - Downloaded data;
        - Portable Devices.

- Company mechanisms to "monitor" the company's computer networks in real-time;
- Multi-factor authentication for remote network access;
- "Intrusion detection" solutions

2. Processes

- Processes to manage accounts of all who use or access data:
    - Current users
        - Including Mobile devices
    - Terminated employees (and protocols and procedures upon termination);

- Physical security controls that restrict access to computers and networks;

---

[1] Romanosky, Sasha, Lillian Ablon, Andreas Kuehn, and Therese Jones, "Content Analysis of Cyber Insurance Policies: How Do Carriers Write Policies and Price Cyber Risk?". Santa Monica, CA: RAND Corporation, 2017. https://www.rand.org/pubs/working_papers/WR1208.html

- Information about Password creation and updating
    - Examples:
        - "*Does the company enforce passwords that are at least seven characters long which contain both numeric and alphabetic characters?";*
        - *"Are passwords changed at least twice a year"?*

- The maintenance of security logs;
- The testing of data security controls;
- The auditing of all outside vendors that have access to data

- Other Written Plans, Policies, and Procedures
    - Written data contingency and disaster recovery plans
    - Written instructions for employees on how to address data security;
    - Systems to address the protection of Mobile Devices
        - Unauthorized mobile device access;
        - Lost or stolen mobile device protocols
    - Written Privacy Policy

3. <u>Personnel</u>

- Does the Company have designated individuals to monitor and implement the Technical, Policies & Procedures, and Legal & Compliance aspects of Data Security?
    - Such as, a Chief Information Officer (CIO) or designated "data security" employee

- Users / New Hires:
    - Drug testing
    - Criminal background checks;
    - Credit history checks

- Is Access to sensitive data restricted by a *need-to-know* standard?

<u>Select comments on the cyber security insurance ***application process***</u> (also attached)

1. Comments by the House of Representatives Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies on "The Role of Cyber Insurance in Risk Management" (March 22, 2016);

    "The very process of considering, applying for, and maintaining cyber insurance requires entities to assess the security of their systems and to examine their own weaknesses and vulnerabilities. The process is constructive, not only for obtaining a fairly-priced policy, but also as a means of improving the company's security in the process. Obtaining and maintaining cyber insurance may be a market-driven means of effecting a rising tide to lift all boats, thereby advancing the security of our entire Nation".

2. Federal Financial Institutions Examination Council (FFIEC) Joint Statement on "Cyber Insurance and Its Potential Role in Risk Management Programs" (April 10, 2018).

    "Purchasing cyber insurance does not remove the need for a sound control environment. Rather, cyber insurance may be a component of a broader risk management strategy that includes identifying, measuring, mitigating, and monitoring cyber risk exposure. An effective system of controls remains the primary defense against cyber threats."

* * * *

[April 10, 2018]

Federal Financial Institutions Examination Council

3501 Fairfax Drive • Room B7081a • Arlington, VA 22226-3550 • (703) 516-5588 • FAX (703) 562-6446
• http://www.ffiec.gov

Joint Statement

Cyber Insurance and Its Potential Role in Risk Management Programs

The Federal Financial Institutions Examination Council (FFIEC) members[1] developed this statement to provide awareness of the potential role of cyber insurance in financial institutions' risk management programs. This statement does not contain any new regulatory expectations. Use of cyber insurance may offset financial losses resulting from cyber incidents; however, it is not required by the agencies. Financial institutions should refer to the *FFIEC Information Technology (IT) Examination Handbook* booklets referenced in this statement for information on regulatory expectations regarding IT risk management.

BACKGROUND

The increasing number and sophistication of cyber incidents affect financial institutions of all sizes, and remediation of cyber incidents can be costly. Traditional insurance policies for general liability or basic business interruption coverage may not fully cover cyber risk exposures without special endorsement or by exclusion not cover them at all. Coverage may also be limited and not cover incidents caused by or tracked to outside vendors. Cyber insurance may offset financial losses from a variety of exposures, such as data breaches resulting in the loss of sensitive customer information.

The cyber insurance marketplace is growing and evolving in response to the increasing cyber-attack frequency, severity, and related losses. Many aspects of the cyber insurance marketplace, such as terminology, claims history, legal precedents, and risk modeling continue to evolve and are shaping the nature and scope of cyber insurance.

Cyber insurance coverage options vary greatly and may be offered on a stand-alone basis or as additional coverage endorsed to existing insurance policies, such as general liability, business interruption, errors and omissions, or directors' and officers' policies. Further, cyber coverage options may be structured as first-party or third-party coverage. First-party coverage insures against direct expenses incurred by the insured party and may address costs related to customer notification, event management, business interruption, and cyber extortion. Third-party coverage

[1] The FFIEC comprises the principals of the following: the Board of Governors of the Federal Reserve System, Consumer Financial Protection Bureau, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, and State Liaison Committee.

protects against the claims made by financial institutions' customers, partners, or vendors as a result of cyber incidents at financial institutions. Understanding the scope of coverage is critical for making an informed risk management decision.

RISKS

Financial institutions face a variety of risks from cyber incidents. These can include financial, operational, legal, compliance, strategic, and reputation risks resulting from fraud, data loss, or disruption of service.

RISK MITIGATION

While cyber insurance may be an effective tool for mitigating financial risk associated with cyber incidents, it is not required by the agencies. Purchasing cyber insurance does not remove the need for a sound control environment. Rather, cyber insurance may be a component of a broader risk management strategy that includes identifying, measuring, mitigating, and monitoring cyber risk exposure. An effective system of controls remains the primary defense against cyber threats.

If institution management is considering cyber insurance, the assessment of cyber insurance benefits should include an analysis of the institution's existing cybersecurity and IT risk management programs to evaluate the potential financial impact of residual risk. As institutions weigh the benefits and costs of cyber insurance, considerations may include:

- **Involving multiple stakeholders in the cyber insurance decision**
  - Include appropriate departments across the institution such as legal, enterprise risk management, operational risk management, finance, information technology, and information security management.
  - Assess the sufficiency of existing control environments to address the potential impact of cyber risk exposures and attestation requirements for the insurance policy.
  - Communicate the cyber insurance decision-making process, including the assessment of cyber insurance options, to the appropriate level of management.

- **Performing proper due diligence to understand available cyber insurance coverage**
  - Review the scope of existing or proposed insurance coverage to identify gaps.
  - Understand insurance policy terms, coverage, exclusions, and costs for cyber events.
  - Consider the potential benefits and costs to assess the insurance coverage appropriateness.
  - Avoid overreliance on insurance coverage as a substitute for sound operational risk management practices.
  - Recognize that policy terms and language may not be standardized. Coverage may be different among insurance providers and tailored for institutions.
  - Consider how the coverage is triggered, if certain types of cyber incidents (e.g., cyber terrorism) are excluded from coverage, and the impact that sub-limits may have in the total coverage and claims process.
  - Assess the financial strength (ratings) and claims paying history of insurance companies providing coverage and their ability to fulfill obligations under the policy if multiple institutions file claims.

- Assess how the proposed policies fit within the business strategies, insurance programs, and risk management programs.
- Understand risk management and control requirements outlined in the policy and ensure the institution would be able to comply.
- As appropriate, engage outside advisors, such as attorneys and brokers, to assist in the due diligence process to assess the benefits of cyber insurance relative to the cost.

- **Evaluating cyber insurance in the annual insurance review and budgeting process**
  - Assessing the benefits of cyber insurance relative to the cost.
  - Determining the sufficiency of existing insurance coverage as cyber risk exposures, insurance products, and the threat landscape evolve.
  - Confirming that any cyber insurance includes coverage expected by the institutions.
  - Engaging the board to assess these factors in insurance program reviews.

Financial institutions ultimately remain responsible for maintaining a control environment consistent with the guidance outlined in the *FFIEC IT Examination Handbook*.

ADDITIONAL RESOURCES

The following cyber insurance resources provide institutions with practical information that may help in understanding cyber insurance.

U.S. Department of Homeland Security:

Cybersecurity Insurance
Cyber Incident and Analysis Working Group White Paper

REFERENCES

FFIEC IT Examination Handbook booklets:

"Audit"
"Business Continuity Planning"
"Development and Acquisition"
"Information Security"
"Management"

[House Hearing, 114 Congress]
[From the U.S. Government Publishing Office]

THE ROLE OF CYBER INSURANCE IN RISK MANAGEMENT

==========

HEARING

BEFORE THE

SUBCOMMITTEE ON
CYBERSECURITY, INFRASTRUCTURE
PROTECTION, AND SECURITY
TECHNOLOGIES

OF THE

COMMITTEE ON HOMELAND SECURITY
HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

SECOND SESSION

_____

MARCH 22, 2016

_____

Serial No. 114-61

_____

Printed for the use of the Committee on Homeland Security

[GRAPHIC NOT AVAILABLE IN TIFF FORMAT]

Available via the World Wide Web: http://www.gpo.gov/fdsys/

_____

U.S. GOVERNMENT PUBLISHING OFFICE
22-625 PDF WASHINGTON : 2016

For sale by the Superintendent of Documents, U.S. Government Publishing Office, http://bookstore.gpo.gov. For more information, contact the GPO Customer Contact Center, U.S. Government Publishing Office. Phone 202-512-1800, or 866-512-1800 (toll-free). E-mail, gpo@custhelp.com.

COMMITTEE ON HOMELAND SECURITY

Michael T. McCaul, Texas, Chairman

THE ROLE OF CYBER INSURANCE IN RISK MANAGEMENT

Tuesday, March 22, 2016

U.S. House of Representatives,
Committee on Homeland Security,
Subcommittee on Cybersecurity, Infrastructure Protection,
and Security Technologies,
Washington, DC.

The subcommittee met, pursuant to call, at 10:14 a.m., in Room 311, Cannon House Office Building, Hon. John Ratcliffe [Chairman of the subcommittee] presiding.

Present: Representatives Ratcliffe, Perry, Clawson, Donovan, Richmond, and Langevin.

Mr. Ratcliffe. Good morning, everyone. Before we begin today, I want to take a moment and recognize a moment of silence to remember the victims of the terror attacks this morning in Brussels.

Thank you.

You know, attacks like these really cement the need for this committee to move forward with urgency on all fronts to try and prevent and protect Americans from attacks like these here in the United States.

With that, the Committee on Homeland Security, the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies will come to order. The subcommittee today is meeting to examine the potential opportunities to promote the adoption of cyber best practices and more effective management of cyber risks through cyber insurance. I now recognize myself for an opening statement.

The House Homeland Security Committee, Subcommittee on

Cybersecurity, Infrastructure Protection, and Security Technology meets today to hear from key stakeholders about the role of cyber insurance in managing risk. Just yesterday, the Bipartisan Policy Center came out with a publication on the room for growth in this market and the barriers that it faces. Specifically, today we hope to hear about the potential for cyber insurance to be used to drive companies of all sizes to improve their resiliency against cyber attacks and develop a more effective risk management strategy, thereby leading to a safer internet for all Americans.

The cyber insurance market is in its infancy, but it is easy to envision its vast potential. Just as the process of obtaining home insurance can incentivize homeowners to invest in strong locks, smoke detectors, and security alarms, the same could be true for companies seeking to obtain cyber insurance. It is for that reason that I look forward to hearing from our witnesses today on the current state of the cyber insurance market and what can be done to develop and to improve and to expand the availability of cyber insurance in the future.

As news of the recent hacks and breaches and data exfiltrations demonstrates, cyber vulnerabilities impact every American and cause significant concern. The interconnectedness of society exposes everyone to these risks now. The interconnectedness of society--the breaches at Home Depot, Target, and JPMorgan Chase are just a few examples of the cyber incidents that have significantly impacted Americans every day.

According to the World Economic Forum's 2015 Global Risk Report, technological risks in the form of data fraud, cyber attacks, or infrastructure breakdowns, rank in the top 10 of all risks facing the global economy. In light of these risks and their enormous significance to individuals, families, and companies, we really need to be exploring market-driven methods for improving the security of companies that store all of our personal information. I believe cyber insurance to be one such solution.

The very process of considering, applying for, and maintaining cyber insurance requires entities to assess the security of their systems and to examine their own weaknesses and vulnerabilities. The process is constructive, not only for obtaining a fairly-priced policy, but also as a means of improving the company's security in the process. Obtaining and maintaining cyber insurance may be a market-driven means of effecting a rising tide to lift all boats, thereby advancing the security of our entire Nation.

Today, those acquiring cyber insurance largely consist of leading companies that have the most to lose. These market leaders have looked down the road and recognize that the best way to mitigate their own vulnerabilities is to ensure against as many cyber risks as possible. However, we need to explore ways for this marketplace to expand to create a wide array of diverse, affordable products that will benefit small and medium-sized entities as well.

The Department of Homeland Security's Cyber Incident Data and Analysis Working Group, or CIDAWG, has facilitated discussions with relevant stakeholders, including many of the witnesses today, to find ways to further expand the cyber insurance market's ability to address emerging risk areas. The DHS working group has examined the potential value of creating a cyber incident data repository to foster the voluntary sharing of data about breaches, business interruption events, and industrial control system attacks to aid mitigation and risk-transfer approaches. Additionally, they are looking to develop new cyber risk scenarios, models, and simulations to promote the understanding about how a cyber attack might cascade across infrastructure sections.