Memo

To:	Miguel Romero, NAIC Financial Examination Advisor (and ITEWG NAIC Staff)
CC:	Patrick McNaughton, ITEWG Chair
From:	LeeAnne Creevy and Philip McMurray, RRC
Date:	February 6, 2015
Subject:	Input to the ITEWG on Cyber Security Risks and Examination Testing

Background

In January, the NAIC asked for input about what examination teams are seeing in the field on examinations regarding how cyber security risks are addressed. The NAIC requested that examiners provide recommendations regarding additional procedures (for instance, related to TPA risks and disaster recovery, etc.). Also, as examinations progress, the NAIC requested to advise if examiners have any insight to share on the charges listed in your January email to summarize for future Working Group calls.

Below we offer our specific thoughts related to the two questions posed in your email. Please do not hesitate to reach out to us if you have any questions. We appreciate the opportunity to share our perspective with you and the ITEWG.

Question 1: Are existing procedures sufficient for cyber security risks?

We believe that existing examination procedures afford adequate guidance for the examiner to evaluate cyber security risks. Through the C-level interview process (e.g., the CIO role and other C-suite executives), review of critical documents related to risk management and other documentation during Phases 1 and 2, examiners are likely to have identified cyber security risks as a significant solvency risk. On several examinations of large insurers over the past 12+ months, cyber security risk has been cited by the top executives (e.g., CEO, CFO, etc.) at the group holding company level as well as by audit committee members as one of the most significant risks that "keeps them up at night." To illustrate, on one current examination of a global P&C insurer, we are seeing more attention to this important risk area at the corporate governance and enterprise risk management ("ERM") level. This particular company has established a cyber risk task force, which is responsible for overseeing the risk management efforts related to the company's internal risks (i.e., penetration of its own networks and systems) and also the risk assessment associated with writing cyber risk products. Through the C-level management interview process, the company's Chief Risk Officer described a robust, highly disciplined approach to risk assessment and risk mitigation efforts in this area. In addition, through review of the ERM framework supporting documentation, it is evident that cyber risk is right at the top on ERM heat maps and enterprise risk listings in terms of management's assessment process.

Additionally, through the IT examiner's work, inquiries related to cyber security awareness and risk management/preparedness should be made. Accordingly, with the knowledge gained early on in the exam process (through C-level interviews, as described above, and through other means), examiners should be incorporating cyber security risk as a high inherent prospective risk area on the Exhibit V and also should address

this risk through the work of the IT examiner as part of the Exhibit C process.

Question 2: Have you identified efficiencies or improvements in general from the updated guidance (for example, in leveraging work of external/internal audit or in documenting results and conclusions)?

Yes, we have been able to identify examination efficiencies by leveraging the work of others (e.g., internal and external auditors as well as third-party vendors conducting vulnerability assessments and penetration tests) on examinations of large insurers, in particular. Not surprisingly, we tend to see that large insurers have more rigor and discipline incorporated into their risk management programs. As such, we have found in these instances that the work of others can be relied upon and/or leveraged from these parties.

The increasing growth of cyber-crime and the associated risks are forcing most organizations to focus more attention on information security, and we have noted this increase in attention at all organizational levels. The information provided below describes significant aspects of a recent examination highlighting what specific areas were reviewed by the examiner, and how the work of others was leveraged and incorporated into the examination process. For example, some of the key IT related documents and evidence of IT programs reviewed by the examiner are outlined in the bulleted list provided below. **Note that many of these areas outlined below are regularly assessed by the organization's information risk function, and they are also reviewed during periodic internal audits (therefore the examiner was able to leverage the work through the internal audit reports, databases containing the test workpapers, etc.).** The vulnerability management process, documented policies and programs, and having the right third-party vendors assist in penetration and vulnerability testing are all part of this particular company's effort to mitigate information security risks.

- This company has a robust information security program, including detailed aspects such as (1) identifying and remediating risks, (2) defined security capabilities, (3) security design and governance, and (4) information security education and awareness.
- Well documented information security policies are updated regularly.
- A process is in place to help the Company manage high risk/visibility vulnerabilities whereby the company took a multi-tiered approach to penetration testing. Specific examples include: (1) a reputable third party vendor conducts approximately a dozen (sometimes more) penetration tests a year, (2) internally, the company's information security group conducts vulnerability scans using purchased software (to date, this company has conducted over 300 scans) and (3) the company also has a contract with another third-party vendor to conduct monthly vulnerability assessments. This vulnerability assessment includes a process to identify high risks, analyze those risks to validate vulnerabilities, notify appropriate members of senior management to advise action required, detect and re-scan, as needed.
- The company uses a reputable vendor product for its core firewall, Intrusion Detection System (IDS) and Intrusion Prevention System (IPS), for which this vendor provides ongoing analysis and notifies the Company's help desk of any incidents. The company also has a documented incident response policy that is tested regularly.
- Specific written guidelines regarding vulnerability assessments are in place and updated periodically. The company recognizes the substantial risks associated with potential vulnerabilities in IT; as such, these areas are identified and the risks of these vulnerabilities are evaluated. This evaluation leads to correcting the vulnerabilities and removing the risk or leads to management developing a formal risk acceptance (e.g. in case the impact of an attack would be low or the cost of correction does not outweigh possible damages to the organization). The program involves implementing vulnerability management and working to remediate vulnerabilities reported by the company and the contracted third-party vendor solution. Specifically, this process includes: (1) roles and support escalation, (2) vulnerability

management implementation, (3) vulnerability management requirements, and (4) risk assessment. Working with company personnel, the contracted third-party vendor assists in management of vulnerabilities identified through to resolution. Using software development engineers and security analysts, the company is notified immediately of any critical security vulnerabilities detected within the company network, and the vendor also produces a vulnerability dashboard of the Company's vulnerabilities for management to review regularly.

On this particular exam of a large global insurer, we also evidenced that the independent auditor performed an IT risk diagnostic benchmarking survey (benchmarking the company's controls over various IT activities). Information security was one of the many areas reviewed in this survey, including evaluating threat and vulnerability management (meaning answering the question, "*How well does the organization identify threats and protect itself against them?*"). This benchmarking survey was shared with the company's board of directors and was leveraged by the IT examiners in conducting the exam work.

In addition to the operational risk-oriented elements listed above, this particular company also had an effective "tone at the top" regarding cyber risk, as evidenced by the documents supporting their ERM function. This top-down recognition of the significant threats posed by Internet connectivity has been noted as a key differentiator between organizations that have effective vs. ineffective cyber security controls. Indicators of executive-level awareness of cyber risks include the requirement for a company's internal audit department to provide periodic updates to the board of directors on IT risk-related matters, including discussing the topic of cyber threats and the company's ability to respond accordingly. As this was an established process, documentation produced by the company's internal auditors was leveraged by the IT examiners and evidenced the on-going commitment and discipline as part of its risk management program to devote the necessary time, resources and energy to this critical risk area.