September 2015

A closer look

A publication of PwC's financial services regulatory practice

Cybersecurity: Enter insurance regulators

Overview

Since issuing its *Principles of Effective Cybersecurity* last July,[1] the National Association of Insurance Commissioners ("NAIC") has been making progress in the development of cybersecurity examination manuals. NAIC's regulatory guidance is intended to help state insurance regulators identify cybersecurity risks and communicate a uniform set of control requirements to insurers, insurance producers, and related regulated entities (collectively, "Insurance Companies").

Given the priority regulators are placing on cybersecurity (including NAIC's Cybersecurity Task Force) and the continued occurrence of high profile data breaches, we expect that cybersecurity examinations will commence as early as 2016 and will be performed by insurance regulators as part of their standard three-year exam cycle. While NAIC's examination manuals will act as guidelines for state regulators, actual regulation will vary by state. Thus, Insurance Companies should be tracking state regulatory developments to ensure that their cybersecurity programs are rigorous and all-encompassing.

Insurance companies can prepare for cybersecurity examinations by doing the following:

- Conducting a cybersecurity risk assessment to identify risks inherent in their operations and processes;
- Assessing how their cybersecurity program mitigates those risks; and
- Preparing documentation in advance of examinations.

As NAIC's principles reference the National Institute of Standards and Technology Cybersecurity Framework ("NIST CSF"), we believe insurance regulators will look to this framework to guide their examination approach. Insurers should review their cybersecurity programs' alignment to the NIST CSF now in advance of any examination.

This **A closer look** discusses (a) how insurance companies can better prepare themselves for upcoming examinations, (b) the challenges they will face while doing so, (c) and our suggestions for enhancing cybersecurity programs overall.

---

[1] See PwC's publication, *Cybersecurity regulatory guidance for the insurance sector*.

pwc

Cybersecurity examination preparedness

Insurers should begin preparing for examination by performing these key activities:

- **Risk assessment** – Insurance Companies should confirm that they have documented their recent cybersecurity risk assessment (ideally no more than one year old) with adequate identification of cybersecurity risks that the organization faces. The risk assessment should identify external and internal threats that may result in data breaches or operational disruptions. Wherever possible, the risk assessment should be informed by external sources of threat intelligence as well as historical data from the organization's own security functions. Finally, the risk assessment should identify priority defenses or controls to mitigate the organization's most severe threats.
- **Capabilities assessment** – The cybersecurity risk assessment should be followed by an assessment of the capabilities of the Insurance Company's current cybersecurity program. Ideally, this assessment should compare existing capabilities against the NIST CSF, although other common frameworks can alternatively be used if the organization's current cybersecurity program is tightly aligned to one. Areas for heightened scrutiny and review should be those that most directly mitigate the risks identified in the organization's cybersecurity risk assessment (top risks should be prioritized for remediation first). Insurance Companies should not rely on the audit function (internal or external) to complete these assessments; rather, they should view this assessment as a second line of defense activity that is sponsored by management.
- **Documentation** – With the NIST CSF expected to form the basis of examination approaches, Insurance Companies should review their current cybersecurity program documentation for alignment with NIST expectations. Organizations that are currently undertaking efforts to update or enhance cybersecurity policies should strongly consider aligning new cybersecurity policies to the NIST CSF. Given that many organizations have long-standing cybersecurity programs with roots in other frameworks (such as COBIT, ISO 27000 series, or NIST 800:53), these organizations should especially review their existing documentation and policies to confirm that NIST CSF components are addressed by their existing programs and policies.

Examination challenges

Insurance Companies should pay particular attention to the following challenges while preparing for cybersecurity examinations:

- **Establishing roles and responsibilities** – Risk management roles and responsibilities should be clearly defined. Often, organizations are unable to address cybersecurity control gaps because of internal disagreement on who owns the risk associated with the findings and costs of remediation. We recommend that Insurance Companies clearly define roles and responsibilities to address the various steps in the risk management lifecycle including risk identification, assessment, and remediation.
- **Managing compliance exceptions** – As Insurance Companies prepare for cybersecurity examinations, they will realize that controls implementation exceptions exist in their environment. This could be due to technical or operational limitations. In such instances, we recommend that organizations perform a formal exercise to determine the residual risk associated with the exceptions, obtain appropriate management approvals, and maintain documentation of the process.
- **Implementing a sustainable compliance program** – Although compliance could be costly, Insurance Companies should pay close attention to the sustainability of the processes that are being implemented. Organizations are often unable to demonstrate sustained compliance over a given period of time as a result of poor planning and design. Organization should ensure that sustainable compliance processes are implemented and an effective change management program is in place to address changes to processes and systems.

Enhancing the cybersecurity program

As guidance develops and state regulations evolve, Insurance Companies should consider enhancing their cybersecurity programs. Based on our market expertise, we believe there are seven critical steps an Insurance Company could take to become more coordinated in cybersecurity risk management:

- **Enhance management oversight for cybersecurity** – Insurance Companies could enhance their governance and oversight functions to ensure that there is adequate Board and senior management oversight for cybersecurity. For example, key initiatives could be subject to Board and senior management approval. Furthermore, the Chief Information Security Officer might consider presenting the results of cyber risk assessments (and associated business impact analyses) to the Board and senior management.
- **Identify critical business processes and assets** – Insurance Companies should consider maintaining an accurate inventory of systems within and outside the organization that contain critical data. Creating an inventory will help Insurance Companies determine the scope of their cybersecurity programs.
- **Provide oversight for third party relationships** – Insurance Companies could enhance any current third party risk management ("TPRM") programs with additional cybersecurity risk assessments and evaluation. A risk-based assessment to identify where IT outsourcing exists and where key data is stored can identify and prioritize sources of risk. Cybersecurity risk management over third parties would address risk through the full lifecycle of the third party relationship (i.e., vendor selection, planning, due diligence, contracting, monitoring, and termination). Once there is a clear understanding and classification of the data the third party collects and distributes on behalf of the organization as part of the service agreement, an organization's TPRM program could include control reviews or required safeguards to better understand and protect any confidential, personally identifiable information.[2]
- **Improve incident response processes** – Insurance Companies could update their cybersecurity incident response plans and train IT and business stakeholders in implementing the plans. Practice exercises would assess the organization's preparedness for responding to cybersecurity incidents.
- **Integrate and align enterprise risk management ("ERM")** – Enhanced ERM processes that address cybersecurity would help the organization map cybersecurity risks to particular business and operational risks. ERM risk and control libraries and reporting metrics could include cybersecurity to further ensure an effective understanding of the business impact of any cybersecurity gaps.
- **Evaluate the second line of defense (i.e., compliance department)** – Insurance Companies should consider a second line of defense between the controls performed by the first line and the assessment work performed by the internal audit function. Consideration should focus on how each function can help monitor the effectiveness and reliability of controls implemented by the first line of defense. IT departments will have to provide guidance on the technical content of controls, while compliance departments provide guidance on control objectives and control implementation.
- **Establish cybersecurity training and awareness program** – Periodic training could be offered to employees and contractors on cybersecurity risks and associated safeguards. Any offered trainings should be updated to address the latest trends in cybersecurity risks. Insurance Companies could make the training mandatory for employees and contractors and also maintain records of training completion.

[2] For more information on TPRM, see PwC's *A closer look, Outsourcing: How cyber resilient are you?*

Additional information

For additional information about this **A closer look** or PwC's Financial Services Regulatory Practice, please contact:

Dan Ryan
Financial Services Advisory Leader
646 471 8488
daniel.ryan@pwc.com

Adam Gilbert
Financial Services Global Regulatory Leader
646 471 5806
adam.gilbert@pwc.com

Sean Joyce
Financial Crimes Leader
703 918 3528
sean.joyce@pwc.com

Joseph Nocera
Financial Crimes Cybersecurity Leader
312 298 2745
joseph.nocera@pwc.com

Chris Joline
Financial Services Regulatory Partner
646 471 5659
chris.joline@pwc.com

Armen Meyer
Director of Regulatory Strategy
646 531 4519
armen.meyer@pwc.com

Contributors: Joseph Dubbs, Tom Swoboda, and Harish Siripurapu.

To learn more about financial services regulation from your iPad or iPhone, download PwC's Regulatory Navigator App.

Follow us on Twitter @PwC_US_FinSrvcs