

Cybersecurity Vulnerability Response Plan

OVERVIEW

Cyber vulnerabilities have become increasingly prevalent and significant as cybercriminals seek to exploit vulnerabilities to breach a company's information technology (IT) security defenses. Conducting a preliminary investigation of possible exposure to these vulnerabilities as they arise can help financial regulators evaluate the operational resiliency of their groups/domestic insurance companies and determine whether a cyber event has occurred that would require further investigation.

However, it is important to note that reported vulnerabilities do not necessarily indicate a cybersecurity breach that would trigger formal notifications and consumer protection requirements, as companies should be addressing vulnerabilities before they can be exploited. As such, many states assign the responsibility for investigation of significant reported vulnerabilities to financial regulators either as a follow-up to ongoing financial exam work in assessing and monitoring IT security controls or as part of an ad-hoc financial analysis inquiry where appropriate. Recent examples of such vulnerabilities include the Microsoft Exchange Server weaknesses, the SolarWinds remote code execution vulnerability, and the Qualys cloud storage vulnerability. Vulnerabilities include threats to the company's internal systems, as well as breaches at third parties that host, or have easy access to, company confidential data.

The primary purpose of this document is to guide examiners and/or analysts through the ad-hoc inquiry that may be necessary when a cybersecurity exposure or vulnerability has been identified or alleged in the period between full-scope examinations. It is, however, up to those examiners or analysts to use sound professional judgement when deciding to undertake such inquiries.

The results of the ad-hoc inquiry may warrant additional investigation, which could include calling a targeted examination, performing interim work, and/or follow-up on recommendations by the department analyst. If additional investigation is warranted, examiners should consult Exhibit C – IT Work Program in the *Financial Condition Examiners Handbook* to identify relevant procedures.

If, after investigating potential vulnerabilities, the domestic/lead state determines that a cybersecurity breach has occurred, information on the breach should be promptly shared with market conduct regulators and other affected states in accordance with existing regulatory guidance. Protocols in the *Market Regulation Handbook* can then be used in situations where a breach has occurred, specifically the post-breach checklist in Addendum A to Operations/Management Standard 17 Chapter 20 – General Examination Standards.

Terms & Definitions

- **Vulnerability** – Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.
- **Incident** – An occurrence that actually or imminently jeopardizes, without lawful authority, the confidentiality, integrity, or availability of information or an information system, or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.
- **Breach** – The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where: a person other than an authorized user accesses or potentially accesses personal identifiable information (PII), or an authorized user accesses PII for an other than authorized purpose.

*Definitions provided by the National Institute of Standards and Technology (NIST) glossary linked [here](#). (NIST SP 800-53 rev. 5, Page 421)

ACTION ITEMS FOR REGULATORS AFTER A VULNERABILITY HAS BEEN IDENTIFIED

The following section provides common questions and answers to help regulators determine an appropriate course of action in responding to identification of an emerging vulnerability.

1. **Which insurers should regulators contact regarding an identified vulnerability?**
Professional judgment should be used by the department in determining which insurers to contact based on previous examination and analysis work, as well as the size and severity of the vulnerability identified.
2. **Which state(s) should lead the effort of responding to notification of an emerging vulnerability?**
In recognition of the lead state approach to financial regulation and deference to a domestic regulator, as well as to reduce the number of overlapping requests and to create efficiencies for both insurers and regulators, the lead state (for groups) and/or domestic regulator should lead the effort of investigating significant vulnerabilities.
3. **What area of the department should take responsibility for investigating cyber vulnerabilities and breaches?**
It is up to each department to determine which area should take responsibility for investigating vulnerabilities, which could be affected by subject matter expertise and availability, the NAIC has primarily classified follow-up procedures for known breaches as a market regulation activity and has included such procedures in the *Market Regulation Handbook*. This is primarily due to the importance of ensuring adequate consumer protection post breach. However, given that a breach can also affect an insurer's solvency position, coordination with financial regulators in post-breach follow-up activities is encouraged.

Investigations related to significant vulnerabilities are typically viewed as following up on financial exam work to assess IT security controls. As such, it is recommended that financial regulators take the lead in addressing significant identified vulnerabilities. However, given the potential for a vulnerability exposure to turn into a breach, early coordination with market regulation is encouraged.

4. **Does the adoption status of the [NAIC's Insurance Data Security Model Law \(#668\)](#) (or other relevant state law) affect a state's response?**

As this guidance focuses primarily on addressing an identified vulnerability, as opposed to an incident or breach, it is not clear whether information on the vulnerability and how it has been addressed would be reported to the department unless or until an actual incident or breach has occurred. As a result, it may be appropriate to proactively address an identified vulnerability even if your department has reporting requirements already in place. Proactive investigation of identified vulnerabilities with insurers may help prevent breaches from occurring that the department would otherwise have to address down the line. However, before taking steps to address an identified vulnerability, the regulator should ensure that the department has not yet received a notice from the insurer on this exposure.

Those states that have passed Model #668 may find themselves at an advantage as they will be informed of breaches in a timely manner and will have greater opportunity to speak and coordinate with their licensees, as well as with other states.

5. **If the investigation of cyber vulnerabilities identifies a need to take additional steps in addressing IT control processes, how can this work be performed so that it can be used on the next full scope exam?**

The most effective way to conduct this investigation in a manner that would allow the results to be integrated into an upcoming full-scope exam would be to use the interim work concept as defined by the *Financial Condition Examiners Handbook* (see Section 1-1, Part I). Interim work is intended to provide examiners the opportunity to conduct exam procedures in areas that are considered inherently risky but are not known to present an immediate concern. A separate examination report is not required in the interim period as information deemed appropriate for report purposes will be included within the full-scope examination report. However, results of interim work are expected to be documented in Exhibit AA—Summary Review Memorandum.

Example Scenario:

Let us assume a software vulnerability was identified. If after having received what the team has determined to be adequate information, and having thoroughly reviewed all of this information, the team should then conclude whether the insurer has taken

appropriate steps to mitigate concerns related to this vulnerability or whether additional actions are warranted. In this example, the exam team concludes it is necessary to check the insurer's patch management protocols. To investigate the vulnerability, the team performs interim work and learns that the company has an updated patch negating the vulnerability. Additionally, the team selects a sample of insurer servers to verify they are at the right version/patch level. From here, the team would inquire about the vulnerability and how the insurer handled it. The team, having received adequate responses, concludes that the insurer has taken appropriate steps to mitigate concerns related to this vulnerability.

At the time of the full-scope exam, this work could be used to help address the DSS 05.01 procedure on Exhibit C. However, before leveraging interim work, the exam team should perform roll-forward procedures to determine whether the processes tested in the interim period are still in place and substantially the same, as changes may affect the conclusions that were reached in the interim period. For additional guidance about rolling forward interim work procedures for use in the full-scope exam, see Section 1-1 in the *Financial Condition Examiners Handbook*.

POSSIBLE QUESTIONS IN DETERMINING AN INSURER'S EXPOSURE TO A KNOWN VULNERABILITY

The following questions can be used to help a regulator determine an insurer's exposure to a known vulnerability, as well as any steps taken to mitigate and address the vulnerability (if exposed). These questions should be customized to the specific situation identified. As the topics addressed and questions raised are largely in line with topics covered during an examination IT review, regulators are encouraged to work with their IT specialists, if necessary, to customize the inquiries, evaluate the appropriateness of responses received, and determine if any additional follow-up is necessary. If specialist resources are not available to a state in this area, NAIC IT security staff may be available to assist in this regard. Where appropriate, corresponding topics from Exhibit C – Evaluation of Controls in Information Technology from the *Financial Condition Examiners Handbook* have been included to assist in evaluating an insurer's response to a specific question.

1. Does the insurance company have any exposure to the discovered vulnerability?
2. If applicable, has the insurance company deployed updates to affected [*application*] servers?
 - a. What are the insurance company's patch management protocols?
 - b. Was the recommended patch applied?
 - c. What steps were taken between when the vulnerability was discovered and when the patch was applied to mitigate the risk?
 - d. If the insurance company has not been able to patch, has it followed [*application vendor/developer*] instructions for how to mitigate through reconfiguration?

See Exhibit C ITPQ question #5

- e. Has the insurance company taken steps to investigate its systems and logs for exploitation, persistence, or evidence of lateral movement? If so, has the insurance company remediated any identified exploitation or persistence and investigated its environment for indications of lateral movement?





See Exhibit C DSS 05.07

3. For vulnerabilities derived from breaches at insurer third parties:

- a. Was company data exposed, or does the third party have easy access to your data?
- b. Has access been restricted?
- c. What steps have been taken to mitigate the risk that your data was exposed?
- d. What communication has taken place?
- e. Has the insurance company addressed this issue with its third-party service providers, if applicable?

See Exhibit C ITPQ Question #3

Conclusions & Next Steps

Conclusions Reached			
<p>No breach or control issues discovered.</p> <p>Mitigating factors were strong and/or further procedures proved there was no additional material risk.</p>	<p>No breach discovered, but concerns noted on adequacy of controls.</p> <p>No signs of a breach occurring, but during inquiry and investigation concerns were noted regarding the adequacy of controls.</p>	<p>Further information still required.</p> <p>Still not certain whether a breach occurred and/or information was extracted by an unauthorized party.</p>	<p>Breach discovered.</p> <p>Information was accessed and extracted by an unauthorized party.</p>
			
<p>No further action required. Findings can be incorporated into the next scheduled exam.</p>	<p>Document the risk identified and the control processes surrounding that risk.</p> <p>Communicate with analyst for ongoing monitoring.</p> <p>Schedule a targeted exam or interim work to look into the issue further.</p>	<p>Consider calling a targeted exam regarding the issue.</p> <p>Perform additional interim work.</p> <p>Analyst provides ongoing monitoring.</p>	<p>Contact Market Conduct department (or similar department) and begin hand-off of the investigation to them.</p>

Additional Resources

Cyber Alerts & Bulletins:

<https://us-cert.cisa.gov/ncas>

Publicly disclosed cyber vulnerabilities:

<https://cve.mitre.org/>

National vulnerability database:

<https://nvd.nist.gov/>

Reported breach tracker for health information:

https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf