CYBERSECURITY EVENT RESPONSE PLAN
CYBERSECURITY (H) WORKING GROUP

Introduction

The Cybersecurity Event Response Plan (CERP) is intended to support a Department of Insurance (DOI) in its response following notification or otherwise becoming aware of a cybersecurity event at a regulated insurance entity (licensee). Early communication with licensees about how a DOI intends to develop their processes, including where and how to send cybersecurity event notifications, will assist with compliance.

This guidance follows the definitions and provisions of the NAIC Insurance Data Security Model Law (MDL-668), specifically the process detailed in Section 6, "Notification of a Cybersecurity Event," and related sections. If a state has made any changes in passing its version of MDL-668 or passed other regulations or legislation, it will need to adjust the guidance herein accordingly. Confidentiality parameters for reported cybersecurity event information vary depending on whether a state has adopted MDL-668, passed its own version of MDL-668, or passed its own legislation. Every state must defer to its specific confidentiality requirements.

Scope

The CERP does not specifically address which events must be reported, as laws and regulations vary from state to state. DOIs should defer to the reporting requirements specific to their state, regardless of whether the state has adopted MDL-668, a revised version, or its own legislation.

Forming a Team and Communicating with Consumers and Licensee Officials

DOIs must establish clear roles, responsibilities, and levels of decision-making authority to ensure a cohesive team response to cybersecurity events at regulated entities. Furthermore, many DOIs have divisions, such as consumer services sections, to inform and protect insurance consumers. In the case of a disruptive cybersecurity event, providing the consumer services section with accurate, up-to-date information and scripts will enable better consumer assistance and will help avoid duplicative or inconsistent information being provided to the public, consumers or otherwise.

Similar to the company's practice of naming a single point of contact to drive communication with a DOI (see "Understanding and Receiving Notifications and Required Information - #13), a DOI may also wish to name a single point of contact who can help coordinate inquiries on behalf of the DOI to the licensee.

Communication with Law Enforcement and Other Regulators

During a cybersecurity event, law enforcement agencies and other regulators may request information from the responding DOI. Engaging with law enforcement officials and regulators can benefit overall cybersecurity and inform the DOI's response, provided such communication is permitted under the relevant state regulation.

Understanding and Receiving Notifications and Required Information

States should be mindful that only partial information may be available in the early stages of the information-gathering process. As a licensee's investigation into a cybersecurity event proceeds, new information may become available, and information previously provided may change.

Section 6 of MDL-668 requires licensees to notify the state insurance commissioner about reportable cybersecurity events and to provide the DOI with as many of the following 13 pieces of information, set out in Section 6(B), as possible, given the relevant state-specific required reporting timeframe:

1) The date of the cybersecurity event.
2) A description of how the information was exposed, lost, stolen, or breached, including the specific roles and responsibilities of third-party service providers, if any.
3) How the cybersecurity event was discovered.
4) Whether any lost, stolen, or breached information has been recovered and if so, how this was done.
5) The identity of the source of the cybersecurity event.
6) Whether the licensee has filed a police report or has notified any regulatory, government, or law enforcement agencies and, if so, when such notification was provided.
7) A description of the specific types of information acquired without authorization. Specific types of information means particular data elements including, for example, types of medical information, types of financial information, or types of information allowing identification of the consumer.
8) The period during which the information system was compromised by the cybersecurity event.
9) The number of total consumers in this state affected by the cybersecurity event. The licensee shall provide the best estimate in the initial report to the commissioner and update this estimate with each subsequent report to the commissioner [pursuant to this section of MDL-668].
10) The results of any internal review identifying a lapse in either automated controls or internal procedures, or confirming that all automated controls or internal procedures were followed.
11) A description of efforts being undertaken to remediate the situation which permitted the cybersecurity event to occur.
12) A copy of the licensee's privacy policy and a statement outlining the steps the licensee will take to investigate and notify consumers affected by the cybersecurity event.
13) Name of a contact person who is both familiar with the cybersecurity event and authorized to act for the licensee.

A state may make changes when passing its version of MDL-668 or other legislation that varies from the requirements set out in Section 6(B) of MDL-668. In this case, the state must adjust this guidance to comply with the information it requires a licensee to report under its legislation.

Receiving the information listed above may take some time, and some information may be available earlier than others. Since some information may never be ascertained, like the identity of the source of a cybersecurity event (or other responsible parties), event notifications should be sent out promptly without waiting for all relevant information to be gathered. After a licensee notifies the DOI of the initial cybersecurity event, the licensee can update its notification.

Appendix A of this document, *Cybersecurity Event Notification Form,* provides an optional form that can be used to help states collect information.

The licensee notifying the DOI of a breach is responsible for reporting updated data, as required, in accordance with relevant state law. If the licensee in question is the DOI's domestic licensee, it is the DOI's responsibility to ensure the licensee provides as much of this information as possible.

The license is not required to provide specific documents, such as an investigatory report or other documentation, to comply with the information reporting requirements of Section 6(B). While an investigatory or other document may contain the information required by Section 6(B), Section 6(B) does not require that the documentation itself be provided to the DOI. MDL-668 requires that the licensee need only send a description of the required information.

If a DOI determines that it needs to review the underlying documentation, the DOI may want to consider bringing an investigation pursuant to MDL-668 Section 7(A) in the event this section is applicable. Information received pursuant to an investigation brought under Section 7(A) is subject to greater confidentiality protection. If Section 7(A) or a similar section is not applicable, the DOI may consider opening a limited-scope investigation or another similar style of examination that provides explicit confidentiality protection to a licensee. To the extent a DOI wishes to gather information beyond the required information listed above, either through an examination or otherwise, DOIs may wish to minimize information requests to the minimum necessary information needed to perform the examination.

Notwithstanding anything provided in this CERP, a DOI must comply with its responsibilities under MDL-668 Section 8, "Confidentiality," or with the confidentiality requirements in its own legislation, and ensure that all reported cybersecurity event data is properly secured.

Process for Responding to Cybersecurity Events

A DOI's process of responding to a licensee's cybersecurity event should allow it to consistently gather as much required information as possible without unduly burdening the licensee, and a DOI's engagement with a licensee may vary depending on the facts and circumstances of each cybersecurity event. To illustrate, consider three general points where a DOI can engage with a licensee after a cybersecurity event: 1) upon receiving notification or becoming aware of the event; 2) after the DOI's initial investigation; or 3) upon the DOI's completion of the investigation. Some questions a DOI should consider when making the determination of when to engage with the licensee include:

- What is known about the compromise, and is there an ongoing threat?
- Is there a greater threat to the insurance industry (e.g. through the involvement of third-party software many insurers use)?
- Has the licensee lost the ability to process transactions? Can they process claims? Premiums?
- Can the licensee communicate with policyholders? Are their telephones, email, and website working?
- Has the licensee engaged in any general communication with policyholders? Is the licensee able to post a notice on its website? If so, when was the notice posted?
- Has law enforcement responded to the licensee's situation? Are they on-site?
- Are there other professionals on-site assisting with the recovery? What are their roles?

For a cybersecurity event that has been remediated and had a limited impact on daily operations and information technology (IT) operations, the DOI may consider allowing the licensee's investigation to run its course before engaging to obtain any necessary information.

Cybersecurity events that have occurred at a third-party service provider require a different approach by the DOI. Often, a licensee will avail itself of MDL Section 6(D)(3), which allows a third-party service provider to fulfill its notification or investigative requirements pursuant to the terms of an agreement with a licensee. In any event, the licensee must acquire the information required to be reported from the third-party service provider.

If a DOI determines that further investigation is appropriate to ensure policyholder data has been secured, an examination by the DOI of the licensee's response and remediation of the cybersecurity event may be warranted. There are several investigative options available to a DOI, summarized in a document titled "*Summary of Cybersecurity Tools,*" which is maintained by the NAIC's Cybersecurity (H) Working Group under the "Documents" tab on the Working Group's page. These tools include:

- Using the Powers of the Commissioner to examine and investigate and take appropriate enforcement action Under Section 7(A) and (B) described in MDL-668, if adopted and in effect;
- Bringing an investigation via the exam process described in the *NAIC's Financial Condition Examiners Handbook*; and

- Using the following checklists included in the NAIC's *Market Regulation Handbook to assist the DOI's inquiry:*
  - "Insurance Data Security Pre-Breach Checklist," and
  - "Insurance Data Security Post-Breach Checklist"."

A DOI must be prepared to address concerns about the confidentiality and protection of cybersecurity event information that has been reported to it, either under MDL-668 Section 8 or under state confidentiality and information privacy legislation. When a licensee asserts that information required by MDL-668 is exempt from reporting because it falls under the attorney-client privilege, or that information required by MDL-668 constitutes a trade secret, a DOI must consult its legal counsel as to how to proceed.

If a licensee expresses concern about the sensitive nature of a particular document (for example, a forensics report), a DOI should consider performing a formal investigation pursuant to Section 7(A) of MDL-668. As discussed above, documents received pursuant to Section 7(A) of MDL-668 are subject to greater confidentiality protection than is provided by Section 6(B) of MDL-668. If a state's version of MDL-668 does not provide confidentiality protections comparable to those provided by Section 7(A) of the MDL-668, a limited-scope examination to determine compliance with MDL-668 may offer a licensee similar confidentiality protection.

How to Receive Notifications and Acquire Required Information

There are many options a DOI has for receiving notifications from licensees. DOIs should take reasonable steps to ensure they have proper communication protocols and tools in place in advance of becoming notified or aware of a cybersecurity event. Communication channels established for event notification should provide security for cybersecurity event data-in-transit and data-at-rest, commensurate with the sensitivity of the reported information.

Additionally, DOIs may provide the licensee's outside counsel or third-party mitigation firm, if appropriate, with a form requesting information. As noted above, information may be available at different times throughout the cyber event lifecycle, and notifications can be updated after a licensee makes the initial report.

Appendix A: Sample Template (This is available in Excel):

	Information Requested	**Company Response**
	Company Name	
1	Date of the cybersecurity event.	
2	Description of how the information was exposed, lost, stolen, or breached, including the specific roles and responsibilities of third-party service providers, if any.	
3	How the cybersecurity event was discovered.	
4	Whether any lost, stolen, or breached information has been recovered and if so, how this was done.	
5	The identity of the source of the cybersecurity event.	
6	Whether licensee has filed a police report or has notified any regulatory, government, or law enforcement agencies and, if so, when such notification was provided.	
7	Description of the specific types of information acquired without authorization. Specific types of information means particular data elements including, for example, types of medical information, types of financial information, or types of information	
8	The period during which the information system was compromised by the cybersecurity event.	
9	The number of total consumers in this state affected by the cybersecurity event. The licensee shall provide the best estimate in the initial report to the commissioner and update this estimate with each subsequent report to the commissioner **[**pursuant to this section **of MDL-668]**.	
10	The results of any internal review identifying a lapse in either automated controls or internal procedures, or confirming that all automated controls or internal procedures were followed.	
11	Description of efforts being undertaken to remediate the situation which permitted the cybersecurity event to occur.	
12	A copy of the licensee's privacy policy and a statement outlining the steps the licensee will take to investigate and notify consumers affected by the cybersecurity event.	
13	Name of a contact person who is both familiar with the cybersecurity event and authorized to act for the licensee.	