CYBERSECURITY EVENT RESPONSE PLAN
CYBERSECURITY (H) WORKING GROUP

Introduction

The Cybersecurity Event Response Plan (CERP) is intended to support Departments of Insurance (DOIs) in their response following notification or otherwise becoming aware of a cybersecurity event at a regulated insurance entity (licensee).

This guidance follows the definitions and sections of the NAIC Insurance Data Security Model Law (#668), specifically the process detailed in Section 6, "Notification of a Cybersecurity Event." If a state has made any changes in passing its version of Model #-668 or passed other regulations or legislation, it will need to adjust the guidance herein accordingly.

Furthermore, the CERP is focused on primary actions and considerations, and it may need tailoring to suit a DOI's needs. Additionally, DOIs that implement a CERP, whether leveraging the guidance of the NAIC or not, are encouraged to ensure that CERP roles and expectations are widely understood throughout the DOI. The effectiveness of a DOI's response to a cybersecurity event may be improved if roles are clearly defined and understood. An effective CERP may assist DOIs in facilitating communication between stakeholders.

Scope

This response plan does not specifically address which events must be reported, as cybersecurity laws and regulations vary from state to state. DOIs should defer to the reporting requirements specific to their state.

Forming a Team and Communicating with Consumers

Many DOIs have divisions, such as consumer services sections, that work together 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.

Therefore, DOIs may wish to have clear and defined protocols guiding external and internal communications and to establish clear roles, responsibilities, and levels of decision-making authority to ensure a cohesive response to cybersecurity events at regulated entities.

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

As part of the information-gathering process, states should be mindful that partial information may be available, and information provided may change as the licensee's investigation into the event proceeds.

Section 6 of Model #668 requires licensees to notify the insurance commissioner about cybersecurity events and to provide the DOI with as many of the following 13 pieces of information (from Section 6(B)) as possible:

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.
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.

The items listed above may require modifications for states adopting their version of Model #668, or that have their own regulation. States may also wish to consider gathering information to help the state understand the total exposure of the incident (e.g. total individuals/policyholders, total anticipated cost (if known), and information on cybersecurity coverage in place, etc.). Such information may allow the inquiring DOI to function as a lead state regulator to respond to the cybersecurity event, which may help minimize the total number of requests to licensees.

Receiving the above information will take some time, and some types of information may be available earlier than others. Notifications can be updated after a company reports the initial cybersecurity event; therefore, notification of an event should not be held up while all pertinent information is being compiled. The licensee who notified the DOI of a breach is responsible for updating the data reported as

it becomes available. DOIs may wish to establish clear communication expectations with the licensee to ensure updates provided are timely.

If the licensee in question is the DOI's domestic licensee, it is the DOI's responsibility to ensure the company provides as much of this information as possible. It may also be appropriate to request information in addition to the examples listed above, including a corrective action plan and status of consumer notifications, which can benefit the DOI's ongoing supervisory work.

Appendix A—Cybersecurity Event Notification Form provides an optional form that can be used to help states collect information.

Process for Responding to Cybersecurity Events

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

- 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 has a limited impact on daily operations and information technology (IT) operations, the DOI may let the licensee's investigation run its course before stepping in to obtain the necessary information.

If a DOI determines that further investigation is appropriate, then examining the licensee's response and remediation of the cybersecurity event to ensure policyholder data is secured may be warranted. There are several investigative options available to state insurance regulators, which are summarized in a document maintained by the NAIC's Cybersecurity (H) Working Group under the "Documents" tab on the Working Group's page – "*Summary of Cybersecurity Tools*." At a summary level, those tools include:

- Using the Powers of the Commissioner described in Model #668, if adopted and in effect.
- Investigating via the exam process described in the *NAIC's Financial Condition Examiners Handbook*.

- Investigating via the following checklists included in the NAIC's *Market Regulation Handbook:*
  - "Insurance Data Security Pre-Breach Checklist"
  - "Insurance Data Security Post-Breach Checklist"
- Ad-hoc inquiry, which may leverage the insights in the NAIC's *Cybersecurity Vulnerability Response Plan*.

How to Receive Notifications and Acquire Required Information

There are many options a DOI has for receiving notifications from licensees. Options include an email inbox, an online form such as a PDF, or using a dedicated secure portal to complete an online form that stores the information in a database. Before a cybersecurity event, DOIs should take reasonable steps to ensure they have proper communication protocols and tools in place if the transmission of information is necessary. Communication channels established for event notification should provide reasonable security of the data in transit, commensurate with the sensitivity of the reported information.

Additionally, DOIs may provide the licensee's outside counsel or third-party mitigation firm, if any, 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 Provided		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 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.	
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 pers and authorized to act fo	