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 (MDL-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 MDL-668 or passed other regulations or legislation in its state, it will need to adjust the guidance herein accordingly.

Furthermore, the CERP is focused on primary actions and considerations and 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 among 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 DOI's 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 & Communicating with Consumers

Many DOIs have divisions that work together to protect insurance consumers. Some DOIs have consumer services sections. Knowing the structure of the response team helps the communication process. In the case of a disruptive cybersecurity event, providing the consumer services section with up-to-date and accurate information and scripts will allow for better consumer assistance.

Communication with Law Enforcement & 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, provided the relevant state regulation permits this communication, opens interaction, helping to improve collaboration.

CYBERSECURITY EVENT RESPONSE PLAN
CYBERSECURITY (H) WORKING GROUP

Understanding & 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 MDL-668 requires licensees to notify the insurance commissioner about cybersecurity events and to provide the DOI with as many of the following thirteen pieces of information (from Section 6(B)) as possible:

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 person who is both familiar with the cybersecurity event and authorized to act for the licensee.

Again, remember that the items listed above may require modifications for states adopting their version of MDL-668, or have their own regulation.

CYBERSECURITY EVENT RESPONSE PLAN
CYBERSECURITY (H) WORKING GROUP

Receiving the above information will take some time, as some information may be available earlier. 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 company's responsible for updating the data reported as it becomes available. Clear communication expectations with the licensee help provide information expeditiously.

If the licensee in question is the DOIs domestic licensee, it is the DOIs 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.

Appendix A (Cybersecurity Event Notification Form) provides an optional form that can be used to help states in the collection of information.

When a company asserts trade secrets or attorney-client privilege that would exempt it from providing important event information and therefore is not responsive to DOI inquiries, the DOI should be prepared to cite the authority used to gather the requested information or offer alternatives to review information, where appropriate. For example, in limited circumstances, it may be appropriate to perform an eyes-only review instead of receiving copies of sensitive 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 undue burden on the licensee. To illustrate, consider three general points where a DOI can engage with a licensee after a cybersecurity event: upon notification, after the initial investigation, or upon completion. The more capabilities a licensee has at the beginning of a cybersecurity event, the less necessary it is for a DOI to involve itself. As such, the DOI needs to decide how to proceed. Some questions to consider when making such a determination:

- What is known about the compromise, and is there an ongoing threat?
- Is there a greater threat to the insurance industry, for example, 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?

CYBERSECURITY EVENT RESPONSE PLAN
CYBERSECURITY (H) WORKING GROUP

For a cybersecurity event that has been remediated and has a limited impact on daily operations and information technology operations, the DOI may let the licensee's investigation run its course before stepping in to obtain the necessary information.

How to Receive Notifications & Acquire Required Information

There are many options a DOI has for receiving notifications from licensees. Options include an email inbox, an online form like 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 fillable form containing the requested information. The law firm will provide as much information as possible. It should be noted that information may be available at different times throughout the cyber event lifecycle.

CYBERSECURITY EVENT RESPONSE PLAN
CYBERSECURITY (H) WORKING GROUP

Appendix A: Sample Template (we have this in Excel – I am including pdf so everyone can see the information)

	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	
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	
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.	

