A Failure to Plan Is a Plan to Fail: Developing a Written Incident Response Plan

July 6th, 2022 | and K. Dailey Wilson

On October 27, 2021, the Federal Trade Commission finalized its long-awaited updates to the Safeguards Rule. The changes require financial institutions, including auto dealers and finance companies, to dust off their existing information security programs and likely make some significant changes. My March *Spot Delivery* article discussed one key change—encryption requirements for emails containing customer information. This article highlights another key change—the requirement to establish a written incident response plan.

Security breaches happen every day, and it's only a matter of time before it happens to you. As we've all heard, a failure to plan is a plan to fail. Developing a plan for how your company will respond to a breach will help you quickly and efficiently react while also allowing you to avoid the reputational harm associated with failing to appropriately address a security breach.

What is a written incident response plan?

On December 9, 2022, financial institutions will be required to have a written incident response plan. A written incident response plan explains how a financial institution will respond to a security event—an event resulting in unauthorized access to, or disruption or misuse of, an information system, information stored on such information system, or customer information held in physical form.

What are the requirements for a written incident response plan?

A compliant written incident response plan must include specific elements.

- **The goals of the written incident response plan.** The written incident response plan should describe the goals the financial institution seeks to achieve by implementing the written incident response plan. Examples of such goals include detecting and reacting to security events, determining the scope and risk of security events, responding appropriately to security events, communicating the results and risks to key stakeholders, and reducing the likelihood of the security event reoccurring.
- **The internal processes for responding to the security event.** The written incident response plan should address what steps the financial institution will take when it discovers that a security event has occurred, such as conducting an investigation into which information systems have been affected, the type of information systems affected, the type of customer information

accessed, the jurisdictions in which affected individuals reside, and the "how," "what," and "when" of the specific security event. The necessary response to a security event will vary based on several different factors, so nailing down the facts of each security event is paramount.

- **The definition of clear roles, responsibilities, and levels of decision-making authority.** The written incident response plan must, at a minimum, specify the individual responsible for handling any security events that may occur. Creating clear lines of authority will help make the security event response process more efficient.
- **External and internal communications and information sharing.** Several types of notifications may be required when a security event has occurred. Of course, a financial institution must notify those internally who need to know of the event. The financial institution may also need to notify various third parties, including third-party vendors, law enforcement agencies, state government agencies, and the affected consumers. Many of these notification obligations will vary from state to state. Identifying relevant state data breach law requirements is key in determining who must be notified, when notifications must be made, what form(s) the notification must take (i.e., electronic, physical mail, posting), and what must be included in the notifications.
- **Identification of requirements for the remediation of any identified weaknesses in information systems and associated controls.** The written incident response plan must require the financial institution to engage in a root-cause analysis. The financial institution must evaluate the security event and determine why it occurred. Once the "why" has been identified, the financial institution must take whatever steps are necessary to correct the problem (e.g., issuing a software patch, imposing new access controls, or requiring encryption of certain categories of information to the extent not already required).
- **Documentation and reporting regarding security events and related incident response activities.** The written incident response plan should require the preparation of documentation summarizing the security event. This documentation should be provided to senior management and the board of directors.
- **Evaluation and revision of the incident response plan as necessary following a security event.** After a security event has occurred, the financial institution should evaluate the security event to determine what lessons it can glean. For example, the financial institution should consider what happened to allow this particular security event to occur, whether the financial institution responded well to the security event, and what the financial institution should do differently in the future to better respond to a security event. Based on this information, the financial institution should make any necessary changes to the written incident response plan that would allow for improved handling of future security events.

What should you do now?

The first step in satisfying the Safeguards Rule's requirement to establish a written incident

response plan is to identify the steps you have in place to address a security event. Your business may have already experienced a security event, so think through what you did to address any previous security events, and write that information down. Next, compare what you did to what steps the Safeguards Rule requires you to take, determine what necessary information is missing, and then figure out how you will address any holes in your incident response plan—or work with your compliance counsel to complete this step. It is also important to inventory any applicable state data breach laws to ensure that your incident response plan incorporates requirements arising under those laws as well. Putting in a little bit of work on the front end will allow you to efficiently and effectively respond to security events when they occur—and they *will* occur.