# Incident Response Plan – An Indispensable Tool for Cyber Preparedness

By: Matthew H. Meade, Chair, Data Security & Privacy Group, Eckert Seamans Cherin & Mellott, LLC

Alexander Graham Bell once said: "Before anything else, preparation is the key to success." This certainly rings true in cyber incident response. To help be prepared against cybersecurity risk, organizations should have a written incident response plan that provides guidance on how to navigate a cyber incident. An effective and efficient incident response plan is essential to help minimize any potential harm to the organization and other interested parties, especially potentially affected consumers. However, having a comprehensive plan is only the start to preparation. The plan must be regularly evaluated through tabletop exercises that assess the organization's ability to respond to hypothetical cyber incidents.

As football season approaches, a comparison to the Gridiron is relevant to this issue. Imagine a National Football League (NFL) team that did not have a playbook – that team would not do too well. Next, imagine an NFL team that had a playbook but never practiced the plays. That team would have trouble succeeding on the field as well. This highlights why having a battle-tested incident response plan is so critical to cyber preparedness. In the height of a cyber incident like a ransomware attack, organizations should not have to figure out who is managing the issue, which experts to consult, who to notify, or the steps to take in the investigation. All these items and more can be prearranged before an incident occurs in a carefully written and concise incident response plan.

For an incident response plan to be successful, the organization must be able to identify and locate important data within its network. The plan must also create a process for how to report a suspected breach as well as determine who makes up the incident response team, including who will be overseeing the investigation.

The incident response team should include at least the following representatives from your organization:

- Information Technology;
- Legal;
- Compliance;
- Risk Management;
- Impacted Business Unit;
- Human Resources; and
- Communications.

Each person's full contact information should be noted along with information for a back-up resource if the individual is unavailable. The above list clarifies that an effective team is one that promotes cross-functional ownership of incident response and requires regular communication and information sharing within the organization.

If you do not have a plan, take the time to collaborate with your counsel and consultants to draft one. If you have a plan, test it, and adjust as needed.