MAYER | BROWN

October 24, 2019

Cybersecurity & Data Privacy

Strategic Thinking and Practical Legal Advice

Internet of Things Incidents

Cyber attacks now reach a broad range of connected devices, ranging from connected toys, fitness trackers, home alarm systems, cars and medical devices to connected manufacturing and infrastructure. Attacks on this broad range of connected devices—often referred to as the Internet of Things—can raise distinct issues from incidents involving enterprise systems. Below, we highlight five key features of responses to attacks on connected devices.

High stakes of incidents. Attacks on connected devices may result in the loss of sensitive personal information or of commercially valuable information. But the gateway to the physical world offered by connected devices also introduces safety risks that are not typically present in cybersecurity incidents involving enterprise systems. A connected car could be manipulated on the highway, for example, or a medical device could be remotely tampered with so that it delivers an incorrect dosage. These potential outcomes can reorder priorities and alter approaches significantly—changing an incident's focus from what data was compromised to whether there is a risk of physical harm.

Different stakeholders. The different priorities that can be put into play by attacks on connected devices can demand the participation of a different group of stakeholders in the incident response team. Groups responsible for product quality, safety, and research and development may take prominent roles, despite often having no role under the enterprise incident response plan. This, in turn, can require the integration of established processes—and cultures—of these different groups to ensure that the combined team works effectively and collaboratively. Likewise, different external resources, including forensics teams that are expert in embedded systems, may be better suited to support the response to attacks on connected devices.

Technical challenges throughout the response process. Many incident response teams have become accustomed to a fairly robust set of technical capabilities that facilitate the response process. These technical capabilities may be replaced by challenges in responding to connected device incidents. For example, many connected devices do not support sophisticated intrusion detection or logging, making the detection and investigation of an incident very difficult. Other connected devices do not support remote patching, making remediation challenging and costly.

Practical challenges. Incident response teams may face numerous practical challenges in responding to an attack on connected devices. It may be very difficult to reach customers to inform them about a necessary patch, for example. It may not be possible to update manufacturing systems without the risk of changing their performance of critical and highly calibrated functions. Relevant suppliers may lack the necessary capabilities to support the response to an incident or may have stopped supporting a particular device, in part because

relevant contracts did not contemplate such support. Moreover, the cost to fix the problem may be greater than the replacement value of a product, particularly for less sophisticated connected devices.

Different regulatory and litigation risks. Connected device cybersecurity incidents can give rise to the regulatory and litigation risks associated with a traditional data breach, as well as the regulatory and litigation risks associated with physical safety. In the United States, for example, regulators such as the FDA, NHTSA, and the Consumer Product Safety Commission likely will have a significant interest in the response to an attack on connected products, and the agencies responsible for critical infrastructure will be keenly interested in attacks on manufacturing or infrastructure. Moreover, litigation risks may reach beyond concerns about the potential harm associated with the loss of personal data to physical injuries that are the province of product liability or mass tort litigation.

These distinctive features of attacks on connected devices place equivalent, distinctive pressures on the incident response team. As with other incidents, preparation can be critical, with experience handling these complex incidents helping companies refine their approaches appropriately over time.

For more information about the topics raised in this Legal Update please contact any of the following lawyers:

Stephen Lilley
slilley@mayerbrown.com
+1 202 263 3865

Veronica R. Glick
vglick@mayerbrown.com
+1 202 263 3389

Joshua M. Silverstein
jmsilverstein@mayerbrown.com
+1 202 263 3208