






HARDWARE CEO SCORE CARD

Below is a table that describes maturity levels of cybersecurity areas impacting hardware: objectives, protection, suppliers, compliance, and testing.

	POOR	OK	EXCELLENT
<div>Cybersecurity aligned with business objectives</div> <div></div>	Cybersecurity risks and conversations may or may not be happening but are definitely not part of greater enterprise conversations	Cybersecurity comes up when there is something major in the news. We react to these topics as they appear.	Our team actively looks at and considers cybersecurity risks and our enterprise risk team informs our cybersecurity team of changes to consider. There is constant dialogue back and forth.
<div>Hardware is protected against cyberattacks</div> <div></div>	The hardware we produce has limited or no security testing.	We have some basic testing and have controls for designing secure hardware that is followed.	We actively test our hardware against industry standards such as NIST 800-147 BIOS Protection, NIST IR 8320, and Secure Hardware Assurance Dataset to test hardware security.
<div>Suppliers and partners are assessed against cybersecurity</div> <div></div>	Cybersecurity is not involved in our procurement process, and we may look at a suppliers' cyber controls if they give it to us.	We have an operating procurement process that includes some cybersecurity components that we assess.	We engage our suppliers and partners to participate in tabletop exercises involving cybersecurity to proactively identify weaknesses
<div>Cybersecurity assessed based on new regulations</div> <div></div>	New regulations occur or we decide to work in new markets and may or may not know if there are technology or cybersecurity controls.	We tap our cybersecurity / technology governance team to understand if there are new regulations that we need to follow and include.	We have created a standardized cybersecurity control framework that addresses a wide range of regulations and requirements. We can use this to fully cover or partially cover most regulatory changes.
<div>Firmware and third-party software are tested</div> <div></div>	The firmware or third-party software we load onto our hardware is not tested.	We have a general process to test any firmware and third-party software we use in our hardware.	We have a robust process to assess firmware and third-party software components that frequently assess their efficacy. We have also created contingencies if there are issues identified with firmware / third-party software.