6 STEPS TECHNOLOGY COMPANIES CAN TAKE TO HELP MINIMIZE RISK

Specific precautions a technology vendor can take to help minimize the risk of passing downstream vulnerabilities to users of their products and services.

1 PERFORM A SOFTWARE COMPOSITION ANALYSIS
and track the sources of code being deployed within a work product to locate and address known vulnerabilities more easily.

2 REGULAR CODE REVIEWS
including a static scan that validates security coding practice during development or a dynamic scan to validate vulnerabilities that occur when the software is running.

3 SECURITY TESTING
or penetration testing of a product. This can be done with an in-house team or through a third party.

4 HAVE AN INCIDENT RESPONSE PLAN
where a business anticipates that a software product is going to get hacked and has a plan to respond quickly to reduce the impact.

5 HAVE A ROLLBACK PLAN
to close vulnerabilities and limit impact.

6 MONITOR PRODUCT AND BEYOND
including dark web monitoring to identify and mitigate threats including malicious code or early chatter of exploits in existing product code.

READ MORE CYBER RISK INSIGHTS.
The Necessity of Tech E&O as Cyber Risks and Ransomware Increase

THE HARTFORD