Global Computer Chip Security Flaw Raises Liability Concerns

By Daniel R. Stoller

Companies faced with a massive computer chip flaw should act fast to reduce their liability instead of waiting for a software fix, cybersecurity attorneys told Bloomberg Law.

Computer chip maker Intel Corp. confirmed Jan. 3 that hackers could exploit its chips to reveal users' stored personal data. Other major chip manufacturers, such as Advanced Micro Devices Inc. and ARM Holdings Plc, also produced chips with vulnerabilities.

Most computer manufacturers and operating system developers around the globe, including Microsoft Corp., Apple Inc., and Alphabet Inc.'s Google, rely on such branded chips in their computer and mobile device products.
Silicon Valley technology companies are working on a fix for the vulnerabilities, which researchers have dubbed Spectre and Meltdown, but only a few have been released. Fixes for all systems could take weeks.
Companies using products with the vulnerable chips, meanwhile, could face class actions and regulatory scrutiny if they are hacked before their systems are patched. But, companies can take immediate steps to improve security, avoiding most long-term liability, while they are awaiting software patches, attorneys said.

Companies, for instance, can step up employee training in resisting phishing attacks, closely monitor in-house computer systems and cloud computing applications, and analyze information flow for potential data leaks, Jonathan E. Meyer, cybersecurity partner at Sheppard, Mullin, Richter & Hampton LLP in Washington, told Bloomberg Law.

Courts in a consumer data breach action will look to whether a company acted reasonably to prepare for and respond to a hacking attack, Meyer said. The plaintiffs' bar "will no doubt formulate interesting theories of liability," he said.

Regulatory Scrutiny

Class action liability isn't the only risk companies should consider while awaiting a patch. They could face increased regulatory scrutiny over how they prepare for chip vulnerabilities.

Regulators can take enforcement actions against companies that were breached as a result of a failure to patch known vulnerabilities, Alex Pearce, privacy and data security attorney at Ellis & Winters LLP in Raleigh, N.C., told Bloomberg Law. But they are also interested in how companies respond to a known vulnerability before fixes are available, he said.

Federal and state enforcers will focus on the "reasonableness of a company's actions once they become aware of the vulnerability," Pearce said. Companies that do nothing, even if a patch doesn't exist, "will rarely, if ever, be viewed as reasonable if the vulnerability had the potential to compromise data the company had a duty to protect," he said.

The U.K.'s privacy watchdog, the Information Commissioner's Office, said in a Jan. 5 blog post that companies have a duty keep customer data safe even if a patch isn't available.

“The key to avoiding liability will be for companies to stay on top of the patches and software updates that are rapidly becoming available, now that these vulnerabilities are known,” Meyer said.

Patching may not be enough to resolve the chip problem.
Because the vulnerabilities are in the physical chips, rather than in the software run by the systems using the chips, patching may not fully address the problem, the Department of Homeland Security's U.S. Computer Emergency Readiness Team said in a Jan. 5 statement.

To contact the reporter on this story: Daniel R. Stoller in Washington
at dstoller@bloomberglaw.com
To contact the editor responsible for this story: Donald Aplin at daplin@bloomberglaw.com