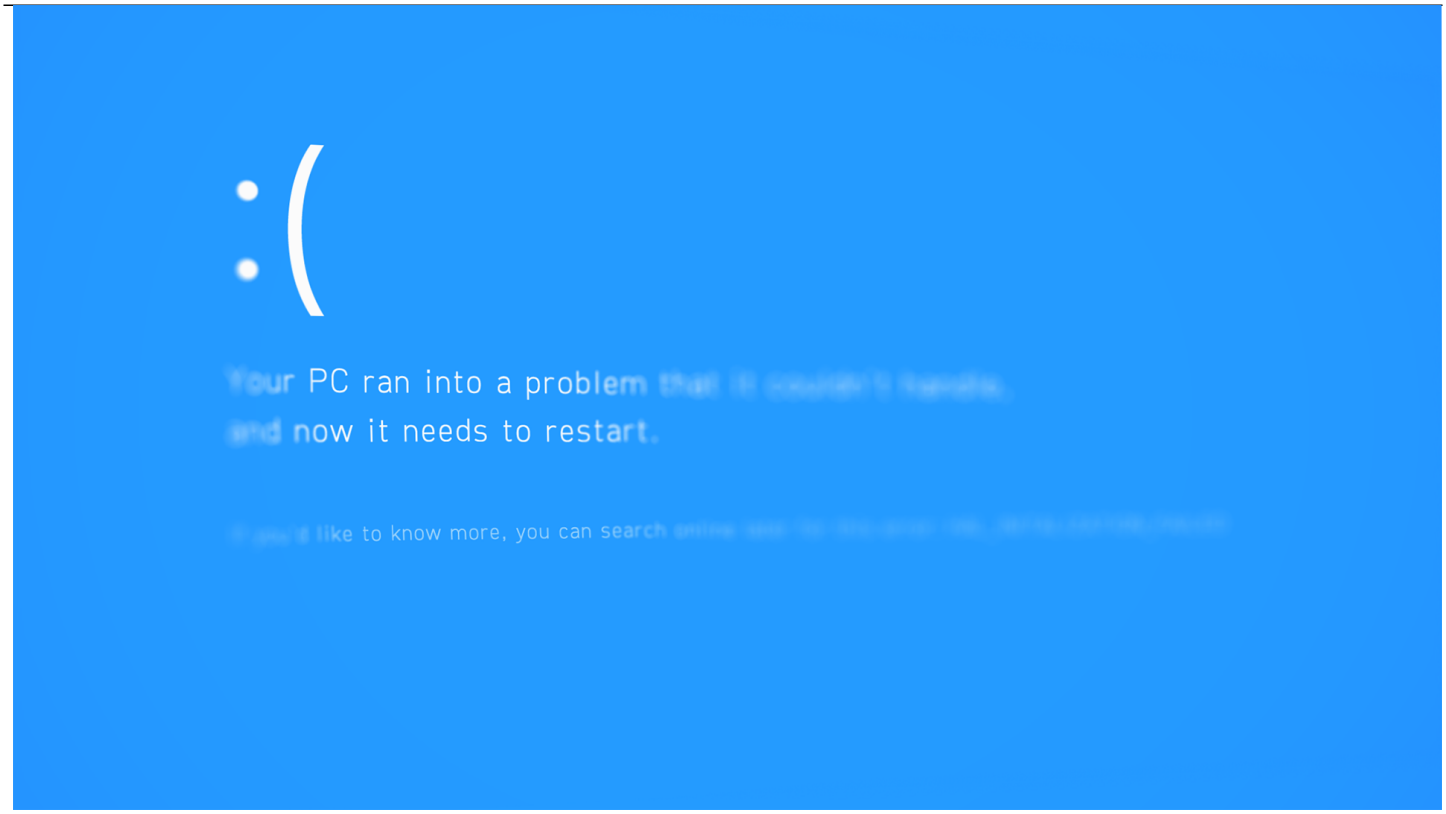
Massive IT Outage: Fact Sheet and Tips for In-house Lawyers

Commercial and Contracts

Insurance

Technology, Privacy, and eCommerce



Banner artwork by Oleksii Arseniuk / *Shutterstock.com*

It's been reported that an update from a cybersecurity firm caused outages for millions of Microsoft Windows-powered devices worldwide, grounding flights and impacting operations of banks, emergency services, media companies, and other businesses.

Reports note that affected machines crash and then get stuck in a reboot loop, becoming inoperable. There is currently a manual workaround that can be rolled out device-by-device, but such intervention could take hours — or days — at large companies.

In-house lawyers play a key role in helping the business prepare and respond to these types of events. Consider the informative tips below as part of your preparation:

1. **Business continuity plans.** Ensure your company has mapped out its mission-critical systems and vendors, and has developed contingency plans in case service from these vendors is degraded or interrupted.

[ACC Sample Plan: Disaster Recovery/Business Continuity Plan**]**

2. **Seek information from the vendor.** When a service interruption or degradation occurs from a vendor, get information directly from the vendor whenever possible. The hours after an IT outage occurs are ripe for bad actors to cause further damage with fake "fixes" that may infiltrate critical systems.

3. **Service levels agreements (SLAs).** Pay attention to SLAs when negotiating contracts with

technology vendors — scope of the SLA, incident reporting process, target resolution times, remedies in case of failure to meet resolution targets (e.g., credit or termination). When an incident happens, review your contract with the vendor and hold them to the agreed SLA.

[ACC Members-only Resource: Essentials of Technology Licensing Agreements: Tips for In-house Counsel**]**

4. **Customer service.** If interrupted or degraded service from a vendor is impacting your ability to serve your own customers, consider whether you have a workaround, or if you will maintain degraded service, or if you have to suspend service — and promptly define a communication plan to inform your customers.

5. **Data and cyber incidents.** If the vendor has access to your systems or data, monitor (and inquire) for any indication that there was a cyber incident or data breach on the vendor side.

6. **Insurance aspects.** Consider what notifications you may need to make to your company's insurance carriers when a mission-critical system is down and impacts your operations, and/or when a cyber incident is involved.

[ACC Members-only Resource: Guide to Handling Contract Negotiations for IT Technology License, Employment Agreements and Commercial Leasing Contracts (United States)**]**

Stay up-to-date by joining ACC!

Disclaimer: The information in any resource in this website should not be construed as legal advice or as a legal opinion on specific facts, and should not be considered representing the views of its authors, its authors' employers, its sponsors, and/or ACC. These resources are not intended as a definitive statement on the subject addressed. Rather, they are intended to serve as a tool providing practical guidance and references for the busy in-house practitioner and other readers.

Staff

ACC