March 4, 2022

This Is Not a Drill

We continue to watch the developments in Ukraine and have seen the warnings of increased cyber-threat level, largely from Russian actors. The threat is real – throughout the world, not just in Ukraine. The lawyers at Day Pitney are actively working with U.S. companies that have been recently hit with ransomware attacks. As advised by the U.S. Cybersecurity & Infrastructure Agency (CISA) in its newly published warning with the all-caps, large-font banner, everyone should have their SHIELDS UP.

So, what should you do?

Certainly review the CISA website, which offers extensive guidance for U.S. businesses facing cyber threats. Here are two more things you should do now:

1. Review your backup plan and, to the extent you can, **back up critical data to appropriate storage** to ensure you can continue operations in the event of an attack.
2. Review your incident response plan. If you do not have one, start creating it.

Day Pitney stands ready to assist in your efforts to prevent or respond to an incident.

Authors



Kritika Bharadwaj
Partner

New York, NY | (212) 297-2477

kbharadwaj@daypitney.com



Stanley A. Twardy, Jr.
Of Counsel

Stamford, CT | (203) 977-7368

satwardy@daypitney.com



William J. Roberts
Partner

Hartford, CT | (860) 275-0184

wroberts@daypitney.com