DON'T BE FOOLED

Opening the doors again: Don't forget about protecting your data

To state the obvious, it has been a long and trying past several months for organizations of all types and sizes. As things slowly return to some semblance of normal, doors that were locked by COVID-19 are now being swung open in anticipation of the return of employees, customers and clients alike. Although it may not seem like it, now is the perfect time for businesses to assess their privacy and data security risk. Here are just a few good reasons why:

Daniel J. Altieri
Senior Associate Harter Secrest & Emery LLP

1. Attackers are everywhere, and they're active! Cyber criminals continue to mercilessly exploit vulnerabilities. Businesses that were successful in the remote work environment may now be more complacent and less alert to developing threats, such as multi-factor authentication evasion, a spike in ransomware incidents, and phishing attacks specifically targeting employees returning to work, including attacks involving bogus health surveys. It is crucial to remind employees, hopefully through the use of strategic and targeted training, to remain vigilant and watch carefully for cyber-attacks.
2. Attack surfaces have grown. Out of necessity, businesses quickly adapted to pandemic life by transitioning to virtual service offerings and remote work, which greatly expanded the scope and complexity of network environments everywhere. However, a bigger, more distributed network means more risk. As employees return to the office, businesses should consider how to close the potential holes that were created by greater access rights, including remote access rights, that may no longer be needed. Access privileges, remote work and acceptable use policies should be continually reviewed and revised, to the extent necessary, including to reflect any material changes in the work environment.
3. The good guys are active as well. Data protection concerns have not gone away. New laws are coming and old ones change. With regulators more attuned to potential privacy and security lapses, this is not the time to put compliance efforts on the back burner.
4. Even actions that are not required may nonetheless be expected. Keeping up with ever-changing laws and regulations in the privacy and data security space is challenging enough. But it's sometimes even tougher to keep up with the court of public opinion. Customers and employees are becoming more and more sensitive about data protection and the use of their personal data. Recent moves by Google and Apple to voluntarily restrict data use, even though not required to do so by law, help show how public expectations have gotten out ahead of the law. Especially in this time of increased digital interactions, an overly light touch on data protection can create problems with the very people upon which an enterprise depends.

Finding the right data protection approach begins with assessing these and other related risks. In the risk assessment process, organizations are able to address two fundamental questions: what is actually being done in relation to data stored and processed, and is more required? As businesses recover from this once-in-a-lifetime public health event, those two questions have become more important to an organization's survival than ever.

Daniel J. Altieri is a senior associate in the Privacy & Data Security practice at Harter Secrest & Emery LLP. He can be reached at daltieri@hselaw.com.