10 ways to stay CyberSavvy while employees return to work

James J. Giszczak, Dominic A. Paluzzi, Miriam L. Rosen, Amanda Rose Martin | Wednesday, May 6, 2020

After quickly transitioning employees to remote work arrangements in response to the COVID-19 crisis, employers are now turning their focus to bringing employees back to the workplace. Employees returning to the office after weeks of remote work creates data privacy and cybersecurity challenges that businesses need to confront head on. These considerations are especially critical as many states and regulators are requiring employers to collect COVID-19 related health information from employees and customers.

To combat the potential cyber risks, below are 10 ways to stay CyberSavvy while returning to work.

1. **Make data privacy and cybersecurity a cornerstone of your return to work plan.** The return to work offers a reset button for many organizations and provides an opportunity to make data privacy a focus of their operations. This is especially important considering the increase in data privacy challenges posed by the pandemic and remote work arrangements. Your COVID-19 response team should consider the privacy implications of any new policies and procedures and how to keep employee and customer information safe.
2. **Understand compliance obligations relating to employee privacy.** Ensure that you understand what state and federal laws apply to your organization and the information you plan to collect. Discuss with legal counsel whether any of your organization's regulators have addressed the collection and protection of employee information in the COVID-19 landscape. Importantly, understand whether the collection of employee health information will require compliance with any additional obligations.

3. **Do not disclose names of COVID-19 positive employees.** In the event that an employee tests positive for COVID-19, do not disclose the employee's health information or COVID-19 status to other employees.
4. **Understand what data is required to be collected, and how.** We anticipate that states will require some amount of data collection from employees. Before asking your employees to come back to the office, ensure that you understand the laws or orders that apply to your organization, the information required to be collected under those orders, and then, work with your response team to collect that data legally.
5. **Transition from personal to company devices.** Some returning employees will be transitioning from use of personal devices while telecommuting back to company devices. In that process, ensure that sensitive personal or business information does not remain on personal devices and is not susceptible to access or acquisition by bad actors.
6. **Educate employees on new and improved methods of scamming and fraud.** Take the opportunity to provide a refresher and additional security training to employees as they return to work. Employees should be warned about recent trends in cyber incidents and the increase in phishing and ransomware incidents as a result of COVID-19. An overview of these recent types of scams and frauds can be found here.
7. **Establish strong data retention policies for employee COVID-19 data.** With the collection of more employee personal and health related information, ensure that your organization has policies in place to regularly and properly dispose of this data. Holding large collections of personal information (especially if it is legacy data) is not viewed favorably by regulators, and poses a risk to organizationsthat may experience data security incidents.
8. **Review and update policies and procedures accordingly.** Review your policies and procedures and make sure they properly reflect any changes recently made as a result of COVID-19. We recommend that you work with your legal team to ensure compliance with applicable law.
9. **Assess whether separate employee consent is required for newly collected information.** Consider whether your organization must obtain employee consent to collect and save new types of personal and health information. Work with your legal team to determine if consent is required from employees and how to obtain that consent in an appropriate and legally binding way.
10. **Keep your IT team in the loop.** Your IT team is your first line of defense against threat actors taking advantage of confusion caused by the pandemic. Ensure that they are kept in the loop and given opportunities to provide input as to how best to protect data and to move employees from personal devices to company devices. Empower your IT team to build out any additional cybersecurity infrastructure required to protect employee data.

If you have any questions about your data privacy obligations as you prepare for your employees to return to work, or would like assistance drafting appropriate policies and procedures, reach out to our national data privacy and cybersecurity team.

James J. Giszczak

Team member bio

10 ways to stay CyberSavvy while employees return

Dominic A. Paluzzi

Team member bio

Miriam L. Rosen

Team member bio

Amanda Rose Martin

Team member bio