IN THE NEW NORMAL

PROTECTING HEALTH DATA

As lock down restrictions ease, many organizations are eager to reopen their doors and to recover from economic losses. In the process of reopening, organizations are adopting new measures to track employee health. Facial recognition software, temperature checks, thermal imaging, and other forms of health screening are chief among the tools used to help identify and isolate positive coronavirus cases. At least 60% of organizations are keeping data on those who contract the coronavirus.[1]

International, federal or state data compliance protocols may offer guidance on how to manage your organization's newly collected human data. However non-uniform requirements in US states, and relaxed GDPR and PIPEDA laws may mean that, to some extent, you're in uncharted waters.

Coronavirus screenings present a new level of visibility into employees' lives; one that's typically protected by legal restrictions. From a cyber security standpoint, employee health screening measures present significant data storage and data privacy challenges. By improving your cloud security, your physical security and your mobile security, you'll be able to keep your organization as safe and as healthy as possible.

[1] Protecting Employee COVID-19 Health Data: What CISOs Need to Know, Dan Swinhoe, CSO Magazine, June 10, 2020

Securely storing sensitive data in the cloud:

Some organizations are storing massive volumes of sensitive human data in the cloud. It is incumbent upon organizations to ensure that cloud data storage not only meets minimum security compliance requirements, but that organizations hold themselves to the highest standards in cyber security. The potential for a breach looms large and the ensuing damage could be even more ruinous than your businesses' economic losses from the coronavirus.

Securing sensitive cloud data requires a multi-pronged approach. Employers should assess risks, and take care to monitor, detect, prevent and respond to cyber security threats. In reshaping your organization's cloud security infrastructure to effectively protect employee data, consider:

Implementing automated security services. This enables you to continually analyze your cloud security posture, ensuring that you can zero in on risks and vulnerabilities quickly.

Developing context-aware policies and access. This allows you to permit access to data based on a user's identity, what the user is requesting, and the device type.

Optimizing threat visibility. Be sure to get insights into reports, analyses, anomalies, and how to improve your cloud security posture management.

Investing in centralized management. Consolidate security management of on-premises, cloud, endpoint and mobile assets so that they're all under a single umbrella.

Cloud security doesn't just protect your data; it protects you in the event of a legal investigation. If a federal or state agency does reach out with a coronavirus-related complaint, you'll be able to quickly provide evidence to help represent your organization's point of view.

Managing Physical Security:

In addition to temperature checks and health screenings, organizations are also relying on identity monitoring and access control points to safeguard employee health. Often, organizations do this with badge-in, badge-out cards. In the event that an employee is diagnosed with the coronavirus after having returned to the workplace, security administrators will be able to run audits on which spaces the employee entered/exited, and will then be able to determine who else he/she came into contact with. Affected employees will then be asked to self-quarantine. Employees' badge access can be suspended temporarily, ensuring a higher level of workplace safety.

Physical control systems are undergoing a digital transformation. Because of this, identity and access control mechanisms are now invaluable in stopping the spread of the coronavirus. It's a whole new level of prevention.

Identity and access control mechanisms are invaluable in stopping the spread of the disease. It's a whole new level of prevention.

Hackers may want to break into your identity and access control system either to steal personal health information, or as a means of gaining access to your corporate network. Consider separating your identity and access control system on the network, which could stop hackers from using it as an entry point to your online resources.

Moreover, be sure to adopt consolidated security and an event management system. This affords maximum visibility into your data. A consolidated management system can monitor, log, correlate and analyze every user activity for you. Your main role then transforms into communicating the necessary information to relevant parties; ensuring that the right messages reach the right people.

Protecting Mobile Devices:

In an effort to keep employees safe, organizations are growing increasingly reliant on employees' mobile devices. Thirty percent of employers use or intend to use app-based health monitoring strategies.[2]

Identity and access management information isn't only obtainable via badge-in/badge-out systems, it can also be made available via Bluetooth enabled apps. The accounting and consulting firm, PwC, recently mandated that employees allow a Bluetooth and Wi-Fi based phone app to track their proximity to one another in the office setting. This monitoring and logging of information will assist administrators in identifying who has been exposed in a coronavirus outbreak, should one occur. [3]

Another group, Pinewood Atlanta Studios, has enacted even more stringent measures to ensure worker safety. All employees must report for coronavirus testing ahead of any scheduled work. If the first lab test returns with a negative report, additional tests are mandated. Only after multiple lab tests come back negative are workers asked to complete a health questionnaire via app on their phones. When the tests and the app data align, workers are permitted badge-access to the Pinewood Atlanta Studios site. Badges will not be effective for workers who have tested positive for the coronavirus.[4]

In both of the aforementioned examples, employer mandated apps collect personal employee data. Across Europe and Canada, in non-emergency situations, requiring employees to submit to medical screenings of any kind is not permitted by law. In the US, strict regulations exist around such requests.[5] However, given the coronavirus pandemic, nations are making exceptions to legal standards. As a result, employers are now responsible for more sensitive mobile phone data than ever, and employers have an unspoken obligation to employees to protect it as best as possible.

---

[2] The Workplace Recovery from COVID-19, Deloitte, May 5, 2020

[3] Your Boss May Soon Track You at Work for Coronavirus Safety, Shannon Bond, National Public Radio, May 8, 2020

[4] It Takes a Lot of Covid-19 Tests to Keep a Movie Studio Open, Sarah Krouse, The Wall Street Journal, July 26th, 2020

[5] DLA Piper, Employment, Pre-hire checks

If your organization is currently collecting employee data from mobile apps, consider investing in a digital defense solution that will keep everyone, every app and every device safe.

If your organization is currently collecting employee data from mobile apps, consider investing in a digital defense solution that will keep everyone, every app and every device safe. Without strong digital defense, hackers could obtain sensitive information, using it for extortion purposes or as material to sell on the dark web. Advanced mobile threat prevention is no longer a 'nice-to-have'. Now, it's an absolute necessity.

Conclusion:

Your Chief Data Officer is now a Chief Data Health Officer. Step into a new mindset and be sure to secure the heart of your organization. Leaked data could potentially result in long-term repercussions on employee's lives along with legal actions against your organization. Limit your liability and upgrade your data privacy and security tools today.

A Case in Point:

The US-based non-profit medical institute, Medical Advocacy and Outreach (MAO), needed a network and security infrastructure that could effectively support the organization's growth. MAO had initially obtained security through third parties, but ultimately decided to bring activities in-house.

"As a medical provider, HIPAA compliance and data privacy concerns are critical, especially when working with HIV cases, which have stricter regulations," said Benjamin Urquhart, the Division Manager of Information Technology.

He chose to pilot Check Point's security appliances and R80 cyber security management. Before adopting Check Point's products, an auditor's visit showed cyber security weaknesses. After adopting Check Point's products, "the red findings went to green," said Urquhart.

Check Point's compliance protocols translated thousands of complex regulatory concepts into actionable security best practices.

> "Check Point gives me full confidence in our ability to grow and effectively maintain security and privacy. I've worked with most of the other products out there, and Check Point gives me the most peace of mind."[6]

To effectively secure your data, meet compliance standards and ensure privacy, choose Check Point. A wealth of resources exist to help your organization make successful infrastructure transitions. Reach out to a Check Point sales representative for more information.

[6] Medical Advocacy and Outreach, Check Point Customer Stories, 2020

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

www.checkpoint.com