HealthManagement
Promoting Management and Leadership

Cybersecurity Risks Arising from Healthcare Employees

Cybersecurity company, Mobile Mentor, and the advisory firm, Center for Generational Kinetics (CGK), found that workers in the healthcare sector are mature, take security seriously, and want to do more to protect patient data. Despite this, the healthcare industry still has Shadow IT issues, poor password hygiene, and inefficient processes for onboarding new clinicians.

These insights were gathered as part of a joint study on how employees perceive privacy, productivity, and personal well-being in the modern workplace, focussing on how people are actually using devices in high-risk and highly regulated industries. CGK interviewed 1,500 employees in the United States and Australia across four high-risk and highly regulated industries: healthcare, finance, education, and government. Each interview consisted of 25 questions of to understand how employees are using devices in a post-pandemic world.

The study's goal was to gather data to educate and inform employers how employees use the devices in their industries, how to prevent security breaches, and how to best support productive employees.

Key Findings:

- Healthcare workers understand the consequences of a security breach.
    - 64% believe they will get fired for a data breach.
    - 57% believe executives should be fired for a privacy breach.
    - 28% know someone who exposed their employer to a data breach.
- Nearly 33% believe they have not been adequately trained to protect company data, although 59% receive security awareness training monthly or quarterly.
- Healthcare has a Shadow IT problem.
    - 35% of healthcare workers say security policies restrict the way they work.
    - 29% admit to finding ways to work around security policies.
    - 48% are more efficient using apps like DropBox and Gmail.
- Password hygiene although better than other industries is still poor.
    - 26% of healthcare industry workers store their work passwords in a personal journal.
    - 70% admit to choosing easy-to-remember passwords.
    - 20% reset their passwords every day.
- Bring-Your-Own-Device (BYOD) security issues remain unresolved.
    - Almost all healthcare workers use personal devices.
    - 51% have BYOD securely enabled.
    - 28% allow their family members to use their work devices for personal use.
- Employers need better onboarding, especially in light of staffing shortages.
    - Healthcare workers wait nearly three days new work devices to be set up.
    - They make 2-3 support calls or tickets to get fully onboarded.
- 78% of healthcare employees feel their personal well-being is more important to them than their job satisfaction.

EndPoint Ecosystem

Published on : Tue, 29 Mar 2022

© For personal and private use only. Reproduction must be permitted by the copyright holder. Email to copyright@mindbyte.eu.