A Brief Absence:
How much grief can it possibly cause?

Spoiler Alert – a Lot!

In the ever-evolving landscape of data security, it's easy to focus attention on external threats posed by hackers and cybercriminals. However, an oft-underestimated aspect of data security lies within our own organizations.

It's not uncommon for workers to leave their computers unattended in a bustling office environment at various times throughout the day. In these seemingly innocuous moments, the potential for breaches from within the organization can arise.

Such breaches can take on various forms – intentional actions aimed at siphoning sensitive data, or inadvertent leaks caused by a momentary lapse in judgment. While external threats demand vigilance, it's crucial to also recognize the enemy within can be just as formidable. Implementing robust security protocols is an essential step to guard against both external and internal threats, ensuring the integrity and confidentiality of sensitive information.

Below we present an example of how an insider breach might unfold and the way KSI’s thermal presence detection technology would prevent it from occurring.

Setting

Large financial firm, midday, busy floor with analysts, traders, and managers moving about.

Staff Members

Alice is a senior financial analyst who’s been working on a confidential report for a high-profile client. Bob is Alice's coworker, a junior analyst who's new to the company and wanting to make his mark.

Sequence of Events

Moment of Distraction: Alice is engrossed in her work and doesn't realize she's late for a meeting. Hearing her name called, she rushes to the conference room, neglecting security protocol and unintentionally leaving her desktop computer unlocked.

Opportunity Arises: Bob, curious about the sort of work senior analysts do and hoping to exploit Alice's work to bolster his status at the company, sees her walk away from her unlocked computer. Given the bustle on the floor, he believes he can quickly glance through her projects without being noticed.

Unauthorized Access: Within seconds, Bob opens a document titled "Confidential Report - Q3 Predictions." Surprised at the depth of information he sees on the screen, he quickly photographs each page and sends the photos to his personal email, thinking his newfound knowledge will help him get ahead in his job.

Compromised Data: Bob retrieves his personal email and sends Alice’s document to a former colleague at a competing firm in anticipation of discussing its content.

Data Leak: One week later, portions of the confidential report appear on a dark website notorious for data leaks, leading to a potential loss of millions of dollars for the high-profile client. The firm's reputation is at stake, and a forensic IT team is brought in to trace the leak.

Repercussions: The source of the leak is traced back to Bob's personal email. Bob is terminated and now embroiled in resulting legal consequences. Alice, despite being an unwitting part of the breach, also faces scrutiny for her lapse of judgment in leaving her desktop unsecure. The financial firm suffers reputational damage along with potential fines and monetary losses.

How KSI Thermal Human Presence Detection Would Have Averted the Breach

- The moment Alice stepped away from her workstation, the integrated Therma-Lock sensor embedded within her KSI keyboard would have detected a swift drop in the heat signature caused by her absence. The sensor would have detected the immediate environmental temperature shift between the time Alice was seated in front of her keyboard and the instant she left.

- In response, the LEDs on her keyboard would have started flashing, serving as an indication of the thermal sensor's detection of the temperature alteration. Within 10 seconds of her departure, the keyboard would have securely locked the PC.

- Bob would be unable to access Alice’s computer unless he was in possession of her password. Alice's KSI keyboard would have, however, effectively countered this intrusion as well, being a password-less authentication solution. The privilege of logging onto the system would have been reserved solely for Alice, granted through placement of her finger on the keyboard’s integrated fingerprint sensor.

- Further, Alice's security would have been bolstered by a dual layer of authentication. She would have also been required to validate her identity by either tapping her RFID badge against the integrated RFID reader on the keyboard or using her KSI RFID wearable wristband.

With a KSI keyboard in place, Alice's computer would have been fortified at both logoff and logon. The unauthorized intrusion from Bob and any other unwelcome individuals would have been repelled, shielding the organization from potential harm.

KSI Keyboards
14494 Wicks Blvd., San Leandro, CA 94577
(510) 562-5000
sales@ksikeyboards.com
ksikeyboards.com