Iakyara vol.326

Know Your Employee is key to teleworking productivity amid pandemic

Takaaki Kobayashi

10.September.2020

Nomura Research Institute, Ltd.

Executive Summary

Office workers have migrated en masse to teleworking in response to the global COVID-19 pandemic. This trend will likely continue even after the pandemic has ended. However, because telework typically takes place in isolation from bosses and colleagues, it poses numerous concerns, including the risk of insider fraud or other misconduct. Such concerns can be effectively addressed with KYE (know your employee) controls already widely adopted in the UK and US.

Takaaki Kobayashi
Senior Researcher
Digital Financial Business Planning Department I

The need for KYE

With many companies shifting to a predominantly work-from-home footing amid the COVID-19 pandemic, compliance departments' KYE (know your employee) practices are garnering renewed attention.

Employees working from home do so in isolation from bosses and colleagues, whose eyes and ears normally serve as checks against on-the-job misconduct. Meanwhile, companies navigating an unfamiliar teleworking environment are susceptible to compliance lapses such as deficiencies in operational controls. The combination of an absence of watchful eyes and deficient controls is conducive to insider misconduct[1], which we define to include (1) crimes like financial fraud and misappropriation of funds, (2) customer-facing compliance breaches like violations of suitability rules or disclosure requirements and (3) violations of workplace regulations, such as sabotage and insubordination.

To mitigate the new risk of insider misconduct, companies need to adapt their employee monitoring regimes to a teleworking environment. Remote employee monitoring should not only effectively prevent insider misconduct in a teleworking environment but also boost teleworkers' productivity[2] and enable them to better identify customer needs and preferences (next best actions). Early adopters of remote employee monitoring in the US and UK offer instructive examples for Japan, where remote employee monitoring has yet to gain traction.

NOTE

1) US criminologist Donald Ray Cressey identified three factors that lead insiders to commit fraud: opportunity, pressure/motivation and rationalization. He called them the "fraud triangle."

2) Digitalization is regarded as the most effective means of increasing operational productivity but our discussion is focused exclusively on productivity in a teleworking environment.

Monitoring to prevent employee misconduct in UK and US

UK financial institutions are currently required by MiFID II[3] to make and document certain disclosures when selling financial products; they are required by the EU's Market Abuse Regulation (MAR) to implement and document controls against insider dealing; and they are required by the European Market Infrastructure Regulation (EMIR) to report data related to derivative trades. To meet these requirements, UK financial institutions monitor a plethora of data on customer transactions involving sales staff. They retain and analyze telephone conversations and messages exchanged with customers. They also analyze and long retain a broad range of order data, trade data and daily market data.

Japanese financial institutions, by contrast, retain only a relatively small subset of such data (e.g., recordings of call center staff's telephone conversations). They do not retain and analyze data across all of their operations.

In the US, employee monitoring is geared primarily toward preventing insider crime. Financial institutions on average experience 23 incidents of insider misconduct per year (see table). The average annual costs associated with such incidents has ballooned to $11.45 million per company. US financial institutions have adopted various employee monitoring tools aimed at preventing insider crime, presumably out of concern about such statistics[4]. They include tools that monitor and store employees' email and chat messages, tools that monitor the content of files that employees' computers send, receive and download, and tools that monitor what employees are doing by accessing system logs, capturing screenshots of their computer screens and even automatically activating their computers' built-in webcams.

3) MiFID II: Markets in Financial Instruments Directive II

4) In the US, companies are prohibited from surreptitiously monitoring employees. In Connecticut and Delaware, for example, state labor laws require companies to notify employees in advance that they are subject to monitoring. In states such as California and Illinois, phone tapping laws require all parties to email communications, including any external parties, to consent to monitoring of the emails.

Figure 1: Losses from insider misconduct incurred by major companies, including financial institutions

Global survey of 204 large companies, including financial institutions		
Average number of incidents per company		23/year
Annual losses/costs	Negligence	$4.58mn
	Crime	$4.08mn
	Information leaks	$2.79mn
	Total	$11.45mn

Source: Ponemon Institute, 2020 Cost of Insider Threats Global Report

According to a Gartner[5] survey, 30% of the total US workforce was already working remotely before the pandemic and 16% of companies use some type of monitoring tool to track what their employees are doing during working hours. 74% of companies intended to increase remote work after the outbreak. The percentage that remotely monitor their employees is likewise in an uptrend according to Gartner.

Three components of employee monitoring

Employee monitoring can be broadly classified into three categories of solutions, each of which fulfills a different function.

The first is process mining. Process mining software records all keystrokes and mouse clicks on computers provided to employees by their employer. It can accurately replicate the employee's work and check for evidence of improprieties. It is also capable of real-time monitoring of violations of internal regulations, such as unauthorized file access.

The second is analysis of recordings or auto-generated transcripts of conversations with customers via an employer-provided mobile phone. Its use cases include compliance checks and screening for conversations indicative of potential misconduct.

The third is detection of advance signs of potential misconduct in the form of transaction patterns that deviate from historical norms. Specifically, datasets related to, say, trades or account activity are combined with the output of process mining and/or conversation analysis software and fed into an ML-trained AI model to detect any such deviations.

Toward realization of both offensive and defensive employee monitoring

In Japan, where teleworking is still in its infancy, employers cannot confidently allow employees to do regular office work and other equally important tasks (e.g., confidential core business processes involving sensitive information) at home without a remote employee monitoring regime in place. If, on the other hand, employers limit teleworking to simple tasks of low importance, their operational productivity would be low and they are liable to end up with a workforce on de

5) "Gartner Identifies Nine Trends for HR Leaders That Will Impact the Future of Work After the Coronavirus Pandemic", May 6, 2020, Gartner (https://www.gartner.com/en/newsroom/press-releases/2020-05-06-gartner-identifies-nine-trends-for-hr-leaders-that-wi)

facto standby at home.

Japanese companies should build teleworking environments that enable high productivity by proactively embracing remote employee monitoring that fulfills the aforementioned three defensive functions. By doing so, they would gain the “offensive” capability to keep their core, high-priority business processes running even when on work-from-home footing. Additionally, we believe a remote environment is even more conducive to analysis of, e.g., customer preferences based on large volumes of transaction data or conversations with customers. Through such a hybrid approach with both offensive and defensive elements, companies should be able to maintain their competitiveness even as teleworking grows in prevalence.

about NRI

Founded in 1965, Nomura Research Institute (NRI) is a leading global provider of system solutions and consulting services with annual sales above $4.8 billion. NRI offers clients holistic support of all aspects of operations from back- to front-office, with NRI's research expertise and innovative solutions as well as understanding of operational challenges faced by financial services firms. The clients include broker-dealers, asset managers, banks and insurance providers. NRI has its offices globally including New York, London, Tokyo, Hong Kong and Singapore, and over 13,000 employees.

For more information, visit https://www.nri.com/en

Inquiries to : Financial Market & Innovation Research Department
Nomura Research Institute, Ltd.
Otemachi Financial City Grand Cube,
1-9-2 Otemachi, Chiyoda-ku, Tokyo 100-0004, Japan
E-mail : kyara@nri.co.jp

https://www.nri.com/en/knowledge/publication/fis/lakyara/