help source

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

http://bit.ly/2rN5Hon

Q Our organization has employees who work mostly in the field. Previously, they had been provided laptops and mobile phones by the organization. Now, the organization has adopted a bring your own device (BYOD) policy. The security team has implemented policies to secure these devices. The question I have is what are the privacy issues associated with these mobile teams using their own devices for the organization's work?

A There are multiple aspects in this one question. Let us break down the question into small questions:

1. While allowing users to use their mobile devices for the organization's purposes, which security settings are likely to affect their privacy?
2. What assurance does the device owner have that the organization does not monitor privacy-related information while monitoring the device for security?
3. What assurance does the organization have that the employees comply with the compliance- and privacy-related policies when accessing and using the organization's data?
4. What assurance does the organization have that employees back up organization-related data from personal devices?
5. What assurance does the organization have that employees will not install any unauthorized software that will compromise the organization's proprietary data?
6. What assurance does the organization have that employees will hand over their devices for investigation in case of any suspected/actual privacy breach?

Many organizations today have implemented technology to monitor employee communications to ensure that employee behavior is compliant with privacy laws, regulations and policies. These measures might particularly be required for organizations such as banks, utility providers, finance companies and listed companies that are highly regulated, especially to ensure the security of information, track insider breaches, and prevent crimes such as collusion and insider trading. The main challenge is to draw a line between organizational privacy, compliance and the personal privacy of employees.

This issue must be addressed by the policies of the organization so as to strike a balance between compliance and employee privacy.

Many organizations implement security monitoring processes using technology such as mobile device management (MDM) and security information and event management (SIEM). The features of MDM allow organizations to:

- Protect devices from unauthorized access
- Restrict the installation of applications (apps) to safeguard devices against malware
- Track the physical location of a device

Sunil Bakshi, CISA, CRISC, CISM, CGEIT, ABCI, AMIIB, BS 25999 LI, CEH, CISSP, ISO 27001 LA, MCA, PMP
Has worked in IT, IT governance, IS audit, information security and IT risk management. He has 40 years of experience in various positions in different industries. Currently, he is a freelance consultant and visiting faculty member at the National Institute of Bank Management, India.

- Wipe data on a device if it is lost or stolen, or if the employee leaves the company

In other words, organizations can remotely access an employee's devices and track the employee's activities. Therefore, the answer to the first question is, "Yes, organizations can remotely access devices and privacy-related information."

Monitoring of devices also answers the third, fourth and fifth questions. The organization can monitor mobile staff activities to ensure privacy-related compliance. Now, with regard to the second question, the *prima facie* answer is "none." When the organization monitors devices, the organization can access the privacy-related information of the employee/device owner. As for the sixth question, the answer is none.

To overcome this situation, an organization's BYOD and privacy policies must address it. The compliance related to privacy can be addressed by adopting the Organisation for Economic Co-operation and Development (OECD) principles for protecting privacy-related data:

- **Notice**—The organization needs to provide notice to the mobile staff that their devices are monitored for security and there is the possibility that privacy-related information may be collected by the organization. This notice should also include remote access to the device and the backup of device data that may include privacy-related information.
- **Purpose**—The organization should also inform the employees as to the objectives of remote access and monitoring, which are focused primarily on ensuring security over the organizational information contained in the device.
- **Consent**—Employees must consent to such monitoring. Some employees may refuse to comply, in which case the organization cannot monitor their devices. Of course, the organization has every right then to not allow BYOD for those employees. Employee consent should also include the handing over of their devices for investigation in case of an incident.
- **Security**—The organization is accountable for securing privacy-related information, including backup information.
- **Disclosure**—The processes of data collection, storage and disposal may be explained to the employees within the limits of the security policy.
- **Access**—Employees should be kept informed about the status of privacy-related data.
- **Accountability**—The organization is accountable for the breach of privacy-related data collected in any manner, including monitoring of mobile devices. This may be considered an extension of the principle of security. Organizations need to implement reasonable security to protect privacy-related information collected. In cases where there is a security breach resulting in leakage of privacy-related information, the organization is accountable.
- **Acceptance**—Mobile staff must be made aware of the policy and consent must be obtained before configuring the device and allowing it to be used by the employee for official business.

The monitoring of devices may be active (when a device such as a smartphone is in use) or passive (when a device is connected to the network). In either case, following privacy-related principles helps organizations monitor data usage by mobile staff.