Get Onboarding and Offboarding Right to Ensure Cyber Security

By Isaac Kohen

I've posted about why I view onboarding as a critical time period for remote workers. One of the reasons it's so important to me is it offers a unique opportunity - when an employee is extremely engaged - to ensure my new team member is aware of the importance of data security. Offboarding is another critical time when data security should be top of mind. Whether your team is onsite or remote, getting the beginning and end of the employee relationship right goes a long way to ensuring the security of your corporate data.

Onboarding: Starting Right

We typically think about onboarding as a time when a new employee receives some standard PowerPoint-based training and signs a few forms. However, when it comes to ensuring the security of your valuable corporate data, it pays to take a fresh approach to cyber security awareness to ensure employee engagement. There will likely be no other time in the employee's tenure when he/she is as motivated and as willing to receive and act on information. Take advantage of this heightened motivation to ensure all employees are all-in on data security.

Ensure HR and IT collaborate. Onboarding starts before the employee first accesses your network. HR and IT should be communicating around the basics like start date and equipment access, but they should also be collaborating around role and data access to ensure the new employee has access to just the data needed for job execution.

Determine the need for employee monitoring. For privileged users, or users with extensive access to valuable corporate data, you should consider employee monitoring software. If you determine monitoring makes sense to safeguard data - and comply with regulations or compliance needs - be upfront with the employee regarding its implementation and who has access to view the employee's activity.

Define the value of your data. Don't just assume that a new team member understands the sensitive nature of your corporate data. Take time during orientation to describe the data the new employee has access to, why it's critical to the organization, and the potential impact if it is leaked. Share examples of what is and isn't ok regarding data use and storage.

Deliver impactful training. You won't make a memorable impact with a dry PowerPoint presentation on security. Instead, consider using:

- Bite-sized learning nuggets delivered through an email campaign
- Elearning courses that include real-world examples and quizzes to test comprehension
- Gamification and rewards for reporting phishing schemes
- Simulated phishing emails to test readiness

You can reinforce data security best practices by sharing how these practices can protect an employee's personal data, as well.

Finally, ensure your new employee knows how to comply with 'if you see something, say something' by being clear about how and to whom to report a possible security incident.

Deliver policies that match the employee's use case. For example, if you have employees who will be using personal devices to access your corporate data, ensure your policies document what is and isn't permitted and how to ensure BYOD security. Onboarding should include sign off on these security policies.

Offboarding: Ending Safely

A recent report found that 87% of surveyed employees admitted that when they left a company, they took with them data they created during the course of their employment. A further 28% of those employees admitted to taking data created by others upon departure.

Whether through negligent or malicious intent, an employee may leave with some of your valuable data. So, offboarding is a another critical time to ensure your data is protected.

HR and IT should be closely collaborating to properly offboard, and this collaboration should start before the employee's last day. Obviously, you should be taking basic steps such as ensuring that HR notifies IT in order to revoke access to applications and facilities, but you should be proactively listening during the offboarding process to protect your data.

Most insiders steal data within a month of departure, so an employee giving notice may signal a need for increased IT vigilance. When HR is aware of upcoming termination or layoff procedures, IT should be in the loop on this as well. Privileged users may warrant increased scrutiny around departure time. Employee monitoring software can be useful in watching an employee's activity before his/her departure date.

You should also review signed non-disclosure agreements and security policies with the employee during an exit interview as a way to reinforce what is and isn't permitted.

A good onboarding and offboarding program marks the start and end of a positive employer-employee journey. Employee onboarding and offboarding are critical points in the lifecycle of your corporate data as well.