Torii PULSE

Offboarding Security for the Remote Workforce

Employees are granted a range of privileges from the organization, including access to sensitive data, documents and software. When an employee leaves, offboarding processes serve as a way to protect the organization from intentional or accidental breaches. However, the COVID-19 pandemic resulted in a rapid switch to a distributed, remote workforce. What's the state of offboarding processes during COVID-19?

Pulse asked over 100 IT executives across a range of industries about:

- ✓ How offboarding has been affected by the switch to a remote workforce
- ✓ The biggest offboarding security threats and if they have sufficient protocols to manage them
- ✓ What their priorities are for the offboarding process going forwards

Data collected from Dec. 9, 2020 - Jan. 14, 2021 Total respondents: 118 IT executives

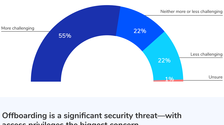
Offboarding processes have changed because of COVID-19, and become more challenging

58% of execs report that offboarding processes have changed as a result of an enforced remote workforce.

Has the remote workforce situation resulted in a change to the offboarding process for your organization?

55% of execs describe remote offboarding as more challenging.

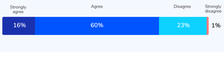
Does a remote workforce make offboarding more or less challenging?



Offboarding is a significant security threat—with access privileges the biggest concern

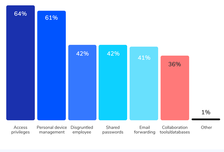
Overall, 76% of execs agree that employee offboarding represents a significant security threat.

To what extent do you agree with the following: "Employee offboarding represents a significant security threat."



Access privileges (64%) followed by personal device management (61%) present the biggest offboarding security threats.

What do you think are the biggest security threats with the offboarding process?



Two-thirds (67%) of execs believe that employees exiting the organization are more likely to cause security breaches by accident, rather than intentionally.

Are you more concerned about accidental or intentional security breaches by employees that are leaving the organization?

Overall, 86% believe that security threats have changed due to a remote workforce being in place during COVID-19.

Has the security threat landscape changed due to having a remote workforce during the COVID-19 pandemic?

Email decommission and return of company hardware the top protocols during the offboarding process—and two-thirds now use software to guide offboarding

Email decommission (78%) and reacquisition of company hardware (77%) are the most common offboarding protocols for employees.

What protocols are in place for employee offboarding?

Two-thirds use offboarding management tools, with 39% implementing internal tools and 27% using third-party tools.

Does your organization use any offboarding management tools?

34% of respondents don't use offboarding management tools.

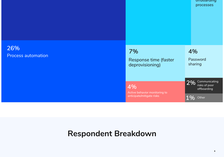
Most believe offboarding protocols are sufficient, but access management remains a priority

Overall, 77% believe that their offboarding protocols provide adequate security measures.

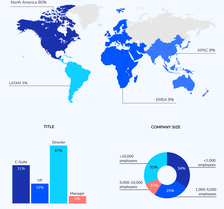
To what extent do you agree with the following: "My organization's offboarding protocols are sufficient with regards to security."

Execs are targeting access management (31%) over the next quarter, followed by process automation (26%).

What aspect of employee offboarding will you prioritize in your organization in the next 3 months?



Respondent Breakdown



Insights powered by PULSE