# Employees Cut Security Corners When They Work Remotely


More than half of employees are cutting corners regarding cybersecurity while working from home, putting your organization at risk. The coronavirus pandemic has forced many to adjust to working remotely and new research shows that workers are taking more risks online and with data than they would at the office.

**54% of employees say they find workarounds**

Results of a recent email security survey found 35% of employees take company documents and data with them when they leave a job. Despite 91% of IT leaders trusting them to do so, 54% of employees say they find workarounds when security policies prevent them from completing tasks.

**Employees copied company data to USB drives 123% more**

According to another report, covering financial services, manufacturing, healthcare, and other businesses, employees copied company data to USB drives 123% more than before the pandemic's onset, with 74% of that data marked as "classified." Data egress over email, USB, and cloud services leaped 80%, with more than 50% of that data marked as "classified."

Accompanying the spike in data copying is a 62% increase in malicious activity on corporate networks and servers, with a 54% bump in incident-response investigations. A related data point in Verizon's new 2020 DBIR report also states that financial gain drives 86% of data breaches, up from 71% in 2019.

According to The State of Data Loss Report, some of the top reasons employees are not completely following the same safe data practices as usual include working from their own device, rather than a company issued one, as well as feeling as if they can take additional risks because they are not being watched by IT and security.

In some cases, employees aren't purposefully ignoring security practices, but distractions while working from home – such as childcare, roommates and not having a desk set up like they would at the office – are having an impact on how people operate.

**People will cut corners on security best practices when working remotely**

Meanwhile, some employees say they are being forced to cut security corners because they are under pressure to get work done quickly. People will cut corners on security best practices when working remotely and find workarounds if security policies disrupt their productivity in these new working conditions. Nevertheless, all it takes is one misdirected email, incorrectly stored data file, or weak password, before a business faces a severe data breach that results in the wrath of regulations and financial turmoil.