

Are You at Risk of Data Loss Because of Insiders?

Insider threats are the security risks originating from within a targeted organization. The actor may not always be a part of the organization. They may also be ex-employees, business partners, consultants, or board members.

Often, the actors are not mindful enough when sharing sensitive information externally.

Hence the name, Careless Insiders.

The Careless Insider



Scenarios



BOARD MEMBER SHARING
BOARD MEETING NOTES WITH A
NON-BOARD MEMBER



EMPLOYEE SHARING COMPANY
FINANCIAL DATA WITH THE
ENTIRE ORGANIZATION



INTERN SHARING EMPLOYEE,
HR AND PAYROLL DATA WITH
WRONG AGENCY



VENDOR SENDING MARKETING
MATERIAL TO THE WRONG
CLIENT/CLIENT COMPETITOR



Average cost per incident
due to employee/contractor
negligence

Source: [Swiss Cyber Institute](#)

41%

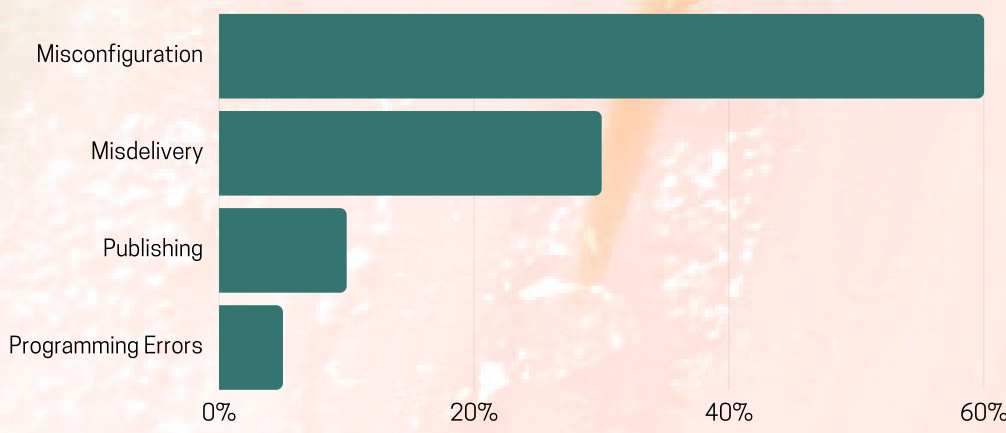
organizations have
at least **1000**
sensitive files open to
all employees

Source: [Varonis](#)



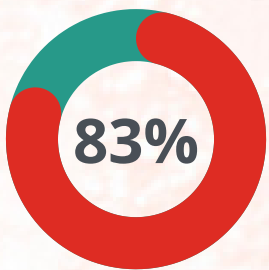
Amount spent by the
financial services sector
against insider threats

Source: [ObserveIT](#)



Top
FOUR
Errors by
Insiders

Source: [Verizon 2021 Data Breach Report](#)



security professionals believe that
employees have accidentally exposed
sensitive data at their organization

Source: [BusinessWire.com](#)

Mitigate Insider Threats with a Solution that:



Attaches Persistent Granular Usage
Controls to Documents and Emails

Tracks Activities on a Protected
Document in Real-time



Enables Organizations to Centrally Define and Modify Usage Controls Such As



WHO

can access the
information



WHAT

can they do with
the information



WHEN

does the access
begin and end



WHERE

can they access
the information