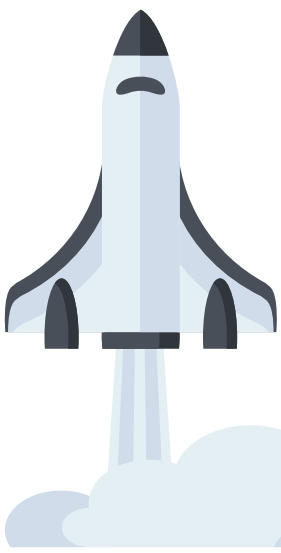
5 WAYS REMOTE WORK IS FUELING DATA LOSS AND WHAT TO DO ABOUT IT

REMOTE WORK IS PUTTING YOUR DATA AT RISK

In an effort to quickly roll out collaboration solutions and enable remote work, have we sacrificed the security of business-critical data?

New reports suggest data loss from within the organization or insider threats — stemming from employee negligence and theft — is a big problem now, more than ever.

Get the facts about this alarming trend and the steps your organization can take to address data loss that has been amplified by working from home.



DATA LOSS HAS INCREASED SINCE THE ONSET OF COVID-19

123% increase in data being copied to USB drives, with;

74% of that data marked as "classified"

72% increase in file uploads to cloud storage services

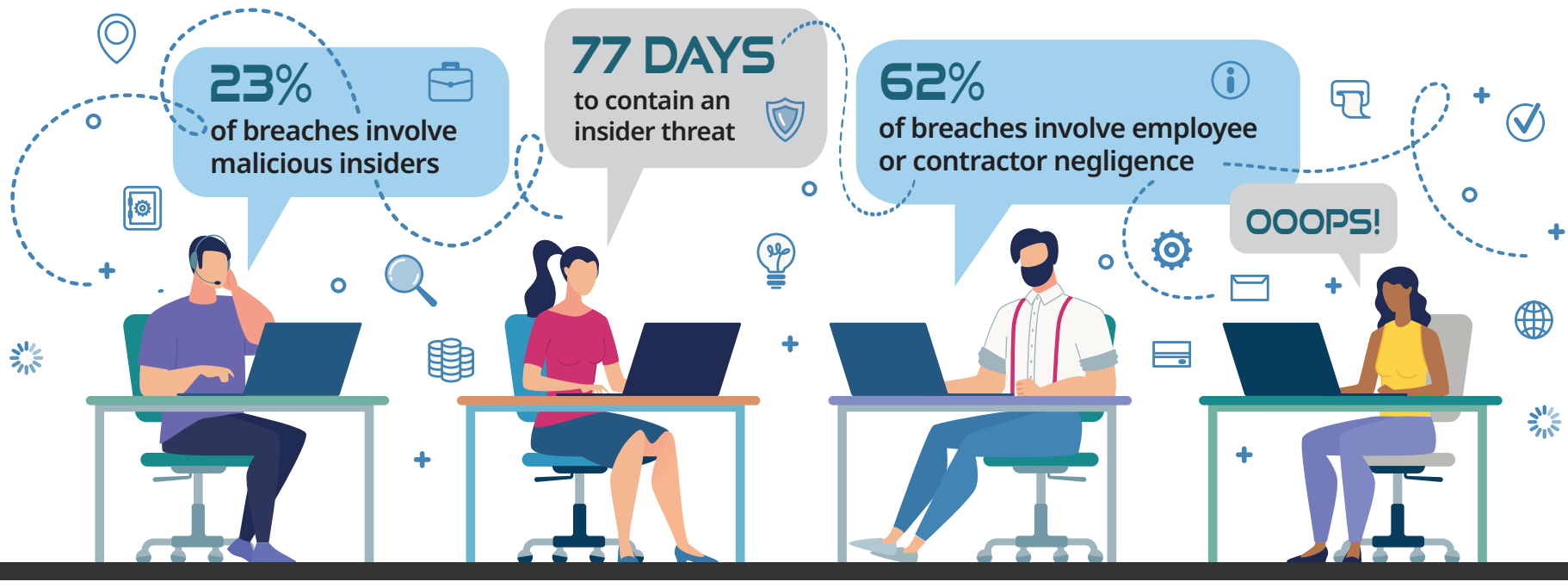
49% increase in email attachments

42% increase of printing work documents at home

24% increase of saving to home office network attached storage

MAILCIOUS USERS AND HUMAN ERROR

Employees have putting your data at risk long before the surge in remote work. You may be surprised to learn that insider threats from trusted users – your employees, contractors and partners – outweigh threats from hackers and malware. And they take longer to detect and resolve.



WHAT WILL AN INSIDER BREACH COST ME?

Average cost of an insider or contractor breach
$307,111 per incident

Average of
$4.58M per year – per organization

PREVENT DATA & REVENUE LOSS FROM YOUR TRUSTED USERS

1 Make a Plan and Share It

- Document your security policy. Write or update your company policy to lay out what data you want to protect and who or what should have access to create, read, and modify each type of data.
- Take into account legal, regulatory, and contractual requirements as well as what data is important to your company, its tolerance for risk, technology environment, culture, processes, and budget.
- Educate your workforce with annual security awareness training, policy acknowledgment, and light hands-on training to ensure everyone understands your data policies.

2 Know Where Your Data Is

- Know where the data you want to protect is stored and collaborated on. The specific technologies that store your data greatly affect which tools are most effective and appropriate to protect your data (e.g. Microsoft SharePoint, Teams, OneDrive, Nutanix Files, Dropbox, Google Drive, or other file shares? On-premises or in the Cloud? Hybrid?).

3 Balance User & IT Needs

- Keep the right balance between what users want from a collaboration perspective and what the organization demands from a security perspective.
- Go too far in either direction and you can make your situation worse. Too lax and your data can be shared far too freely. Too stringent and your users find an alternative way to share and collaborate. In either situation you lose visibility and control of your sensitive data.

4 Automate Data Protection

- Find, deploy, and operate an appropriate information protection solution to secure collaboration.
- NC Protect provides the context and content awareness to adapt access controls and sharing rights down to the file or chat message level to ensure your employees and third party users can collaborate securely.
- Get granular security without the complexity of native tools to start securing content in hours, not days or weeks.
- Discover how NC Protect's advanced information protection capabilities can help boost your data security and governance simpler, faster, and cheaper.

Digital Guardian Digital Trends Report, May 2020
2020 Cost of Insider Threats Global Report, Ponemon Institute

NUCLEUS CYBER

www.nucleuscyber.com

Advanced Information Protection Made Simpler. Faster. Cheaper.