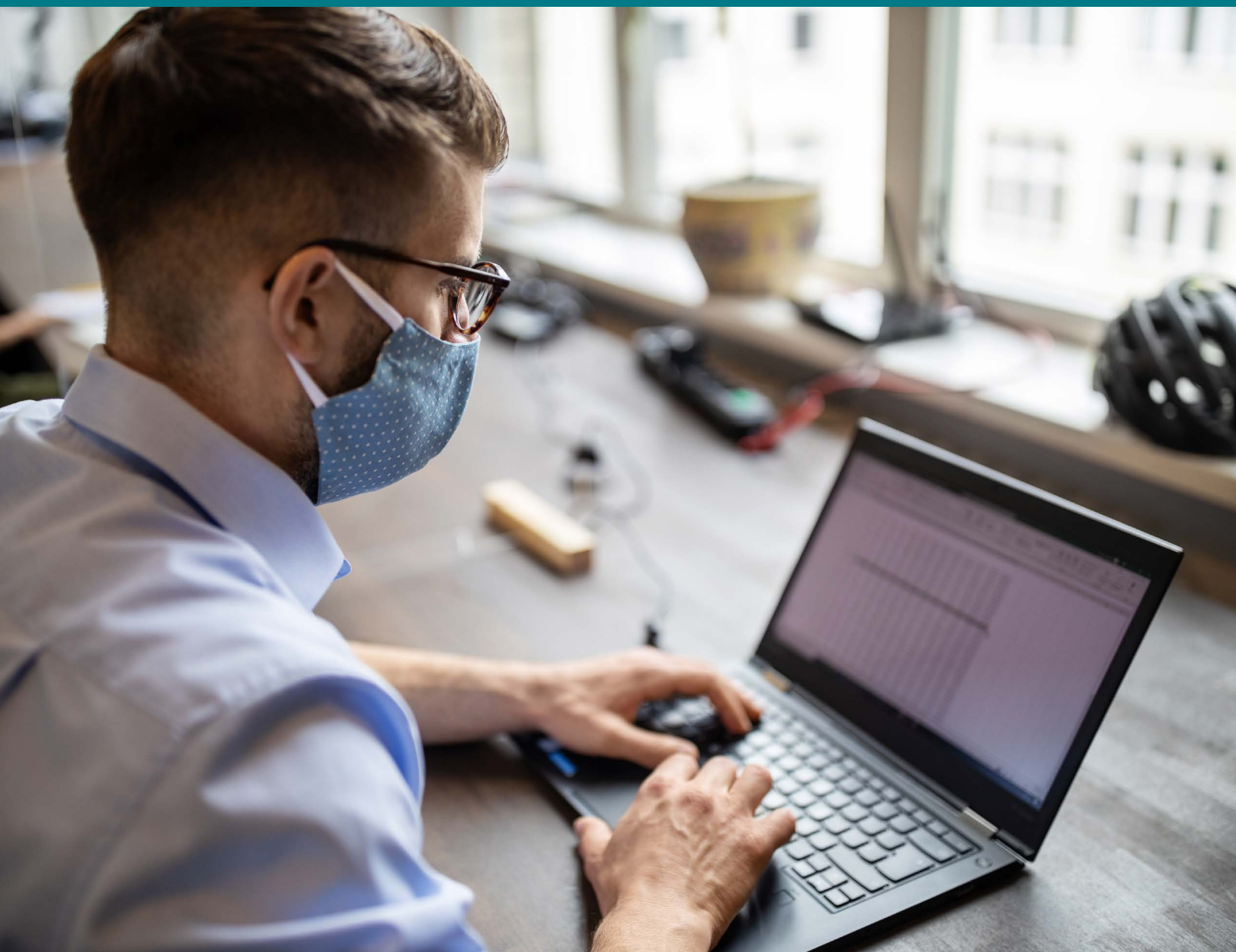
citrix

Guide

8 reasons your users are a bigger risk than hackers

How to keep your business content safe and secure



The real threat to your information security

When you imagine the causes of a security breach, what do you think of? A team of international hackers trying to ransom information? A malicious insider with a grudge to settle? Statistically, the most likely cause is much simpler, like one of your sales reps leaving his tablet behind on a plane. 54 percent of companies consider employee mistakes the biggest threat to their sensitive data, compared to external hackers (30 percent) and malicious insiders (21 percent)[1].

For your employees to be productive wherever they work, they need reliable, swift access to key files and data. But with data stored in so many locations and end users accessing sensitive files on personal devices, the "surface area" for security risks is larger than ever. This demands a content collaboration solution that safeguards critical information while simplifying access for every employee.

Here are the eight reasons why poor user security is a threat and how to protect your content collaboration accordingly.

1. Lack of file encryption

Every day, your staff shares countless files in multiple devices across your network. Without strong encryption, it's much easier for unauthorized parties to read sensitive data in these files—including both private intellectual property for your company as well as sensitive customer information. 54 percent of companies cite these factors as their primary reasons for deploying encryption[2].

So what does strong encryption look like?

- It needs to be rigorous, fitting the Advanced Encryption Standard chosen by the U.S. government and having a key length of 256 bits.
- It needs to be comprehensive, protecting your data both at rest and while it's in motion across your network.
- It needs to be controllable, allowing you to manage your own encryption keys throughout your cloud storage zone.

59% of companies consider employee mistakes and system malfunctions the most significant threat to their confidential or sensitive data[1].

2. Relying on easily lost external drives for large files

As your staff creates large files for videos and other graphics-rich assets, email file-size limitations make it tempting to store and share these files on thumb drives and other portable hardware. However, each of these external drives represents an unsecured endpoint. All it takes is an employee leaving a thumb drive behind at a coffee shop for your private information to be available to whomever picks it up.

This risk makes it vital to store your files in a secure private cloud solution. You want to provide secure access to large files from anywhere on any device, whether the files are hosted in your on-premises datacenter or in the cloud. This allows your employees to collaborate from wherever they work without the risk of storing critical files on an easily-lost thumb drive.

3. Weak passwords and no two-factor authentication

Too many users rely on simple, easy-to-enter passwords across multiple sites, making them a prime target for hackers. You should require employees to create stronger passwords that do not contain personally-identifiable information or common phrases. A strong password has at least 10 characters, and includes numbers, symbols, capital letters, and lowercase letters. Better yet, employees should adopt an easy-to-remember

passphrase made of random words, numbers, and symbols that will be difficult for a hacker to guess. For example, "The first home I ever lived in was 615 False Street and rent was $500 per month" is a simple, nonsensical sentence. You can turn that sentence into a passphrase by using the first characters of each word, so your password is "Tfhleliw615FSaRw$5pm."

It's also important for your employees to have unique passwords for each site and application they use at work. One way to simplify this is by adopting a password manager like LastPass to create strong, unique passwords for all relevant logins. You should also choose a content collaboration solution that requires regular password changes (such as every 60 days), and supports two-factor authentication—especially when signing in from a new device.

4. Sharing sensitive files on personal devices

When employees handle customer information, they're handling sensitive data subject to numerous regulations and governance requirements. If a user downloads this sensitive data to an unauthorized device, your company could face a lawsuit or significant fines for being out of compliance. You need to ensure only the right internal and external collaborators can access files with private information.

This makes it essential to control file sharing across your organization with data loss prevention (DLP), which blocks unauthorized users from opening downloaded files outside of apps you approve. Also, look for a content collaboration platform that offers integrations with Cloud Access Security Brokers like Skyhigh and Avanan to help you enforce DLP policies for files stored in the cloud.

5. Screenshotting confidential information

Preventing the distribution of sensitive data takes more than securing the files themselves. Sometimes users will screenshot parts of confidential files for notetaking purposes, then share these screenshots without permission. This makes it important to ensure your intended recipient cannot capture and share this sensitive information with unauthorized users.

The answer is content collaboration that supports information rights management (IRM). This adds extra protection to sensitive data by applying a digital watermark that is specific to the recipient's name, email address, and IP address. IRM thus mitigates the risk of unauthorized screen capture by only allowing watermarked users to see the shared document.

6. Lost or stolen mobile devices

As you empower your employees to work anywhere and on any device, you increase the chances your staff may lose a device containing sensitive information. Compared to the risk of losing an external drive with sensitive, the consequences of losing a smartphone or tablet can be even worse by allowing bad actors access to your network via the stolen device.

In addition to the data loss prevention strategy mentioned earlier, your solution should include remote wiping capabilities. This protects against data leakage by empowering your IT team to remotely remove content collaboration access and documents from lost mobile devices. Remote wiping also makes it easy to instantly close off access from any employees who depart your organization.

7. Printing and manually signing documents

Sales reps have relied on signed paper contracts to close deals for decades. However, in a digital age these printed documents represent a significant security risk. Paper contracts can be lost, photographed, or illicitly copied, and these risks increase the more places the contracts go and the more people who interact with them.

Instead of printing a contract and exposing it to these risks, choose a content collaboration solution with e-signature capabilities. This electronic verification

is both legally-binding and much more secure than transporting a paper document. While third-party e-signature providers are available, adopting content collaboration solutions that integrate e-signatures into the product itself can cut admin time by 93 percent.

8. Lack of security auditing and reporting

If a breach occurs, you don't want to waste precious hours trying to determine the source before you identify the threat and neutralize it. This makes it important to keep track of how your users share and download files across your network.

The best way to monitor how employees use your files is adopting a content collaboration solution with security auditing and reporting features. This allows you to audit, track, and log all user activity for better visibility into data usage and easier compliance with regulatory requirements. And by setting up reporting and alerts, you can ensure any suspicious activity gets flagged immediately so you can take action.

Empower your users without neglecting information security

Now that you're aware of the security risks posed by your users, it's important to provide them with support rather than suspicion. The best way to alleviate these user security risks is not to lock down all their workspaces and devices, but rather to set your employees up to do their best work on a secure content collaboration platform. With the right solution, you can deliver the work anywhere on any device access your staff wants alongside the information security your business needs.

For more on secure content collaboration, visit sharefile.com.

Sources:

1. This and other citations are from the 2019 Ponemon Global Encryption Trends Study. go.ncipher.com/rs/104-QOX-775/images/2019-Ponemon-Global- Encryption-Trends-Study-es-ar.pdf

2. 2019 Ponemon Global Encryption Trends Study

citrix

Enterprise Sales
North America | 800-424-8749
Worldwide | +1 408-790-8000

Locations
Corporate Headquarters | 851 Cypress Creek Road, Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway, Santa Clara, CA 95054, United States