FORTRA

6 Users to Put on Your Security Watch List

Table of Contents

Introduction

Are you protecting your organization from the inside out?

As an administrator, you may have processes in place to deal with security threats, like malware, spam emails, port vulnerabilities, and brute-force attacks. But though we wish it was that simple, it's not always outside hackers you have to worry about.

Sometimes, security threats come from the inside.

When implementing cybersecurity strategies in your organization, keep an eye out for these six user types and their M.O. Once you know what to look for, you can use our suggested tactics, including solutions that'll improve your business processes, to stop them before they become a serious security problem.

Meet Admin Adam

Adam is an administrator for a middle-sized retail organization. He spends his days checking emails, resolving tickets, configuring new servers, and managing internal separation of duties.

Day by day, he works alongside two other administrators to ensure the organization's private network is secured from cyber attacks and vulnerabilities. He reviews the organization's IP blacklist and whitelist, ensures network ports are properly secured, and patches employee workstations with the latest security updates.

With over a decade of experience, Adam has seen it all. He started his career by protecting the organization from the outside, but quickly learned to find internal risks and put them on his watch list. External threats, he found, aren't the only things that can cause a data breach.

Are these users on YOUR security watch list?

Adam has multiple users on his security watch list and employs different tactics to address each vulnerability. Unfortunately, some of these users are easy to miss. Adam's had his own share of blunders throughout the years—but thankfully, he's here to help you avoid them and create your own watch list.

With Adam as your guide, you'll identify six user types that might practice risky or even dangerous behaviors in your organization, then explore different methods to prevent them from doing accidental (or purposeful) damage to your business.
Let's get started.

Departed Dave

Dave left your organization a few weeks ago to pursue a new career opportunity. After several days on the job, he realizes he could get ahead if he uses a few of the documents he created for his role at your company.

Dave logs into the third-party file sharing program you use and finds he still has access to his account. Relieved by this discovery, he downloads three old files: a detailed sales spreadsheet, a monthly report template, and a customer FAQ questionnaire.

Excited that he doesn't have to create these from scratch, Dave downloads them to his new work computer and puts them to use immediately.

Adam Says:

Dave shouldn't be allowed to access his accounts once he leaves your organization. It puts your data at risk. For example, if there's critical sales information stored in those documents he downloaded (like hidden columns in a spreadsheet), he might unwittingly breach your customers' data. And if he forgets to log out of his file sharing account, this could put your organization at risk if his computer is ever compromised.

The Solution?

First, connect your file sharing programs and applications to the LDAP and Active Directory accounts you control. Then, keep track of the accounts your employees open. When a user leaves your organization, disable all their accounts directly from LDAP or AD.

Gossip Grant

Grant is a junior administrator working on your team. He's assigned a support ticket to backup data from an HR network share. While setting up the backup, however, curiosity gets the best of him. He clicks into a few files and discovers sensitive employee details, like promotional paperwork, legal documents, and termination agreements.

Grant finishes the backup, but not before copying a few of the most interesting files to his desktop. He loves sharing juicy gossip with one of his coworkers, and she'd definitely be intrigued by these documents.

Adam Says:

Personal information like payroll data, health benefits, promotional details, and incident reports should only be available to the people who need to see it (in this case, the HR department). While Grant needs to create a backup for HR as part of his job, he shouldn't be able to open or access the files on the network share.

The Solution?

Set permissions on network folders to only grant access to authorized users. Additionally protect data at rest with industry standard AES 256 encryption. That way, if a network share is accessible to an IT user, the files and folders within are encrypted so he can't access them without permission.

Jealous Jerry

Jerry has worked at your company for years and recently applied for an internal lead position he's had his eye on. When another coworker gets the promotion instead, Jerry feels his hard work hasn't been acknowledged and carries misgivings about his coworker getting the job instead.

Angrily, Jerry accesses a shared network and deletes several files, including critical spreadsheets and sales reports that his promoted coworker needs to perform lead duties. Jerry's coworker can spend time recreating them—it's the least he should have to do after getting a raise.

Adam Says:

Frustrated, jealous, or upset employees sometimes look for ways to sabotage their peers (or organization as a whole). While our solution to this scenario won't cure animosity between coworkers, it can protect your data from unauthorized access and actions.

The Solution?

Create folder-based permissions wherever you store documents to keep users segregated by role. For files that need to be available to everyone, you can still make them "read only" to avoid document changes. Finally, enable autolock on employee PCs after 3-5 minutes to protect users from malicious tampering while they're away from their desk.

Fake Freddy

Freddy lives in a town near where your organization is headquartered. He's been observing your business for quite some time and recently discovered which file transfer solution you use to protect your data transmissions. By searching LinkedIn, he also knows the names of a few IT employees who work in your organization. Score!

Freddy gets on his laptop at home and attempts to breach your file transfer solution using common usernames, like "admin" or "root." If he can successfully guess a username and password, he can monitor file transfers directly from the service without anyone noticing.

Adam Says:

Hackers are getting smarter every day. They scour the web and use employee information (like their name, role, and even anything they share on social media) to make more personal, measured attempts to log into an organization's services and software.

The Solution?

You can use your file transfer solution to mitigate this threat as long as you have the right security features implemented. For example, your file transfer software's account security features should disable user accounts after too many failed login attempts.

Your solution administrator can also block users who attempt to use common account names, like "administrator" and "admin," and put that IP address in the blacklisted IP log.

Snoopy Sara

Sara is a contractor with access to one of your organization's FTP servers. Anytime she completes work for you, she can log in using the username and password you provided her and leave files on the server for your employees to retrieve and process.

One afternoon, Sara accidentally navigates to a different directory on the server. She realizes that she's not the only contractor who uses this server; other vendors and contractors use it to store their work, too.

Sara's been considering raising her prices for quite some time now and realizes the open FTP server gives her the perfect opportunity to evaluate her approach. She spends the rest of the day comparing her contract details with other contractors' work.

Adam Says:

FTP servers have many security limitations. Not only is the data stored unencrypted, accounts aren't limited to specific directories or folders. Most vendors won't think to browse around the server, but some might—and raising their prices could be the least of your concerns if other files contain sensitive business information.

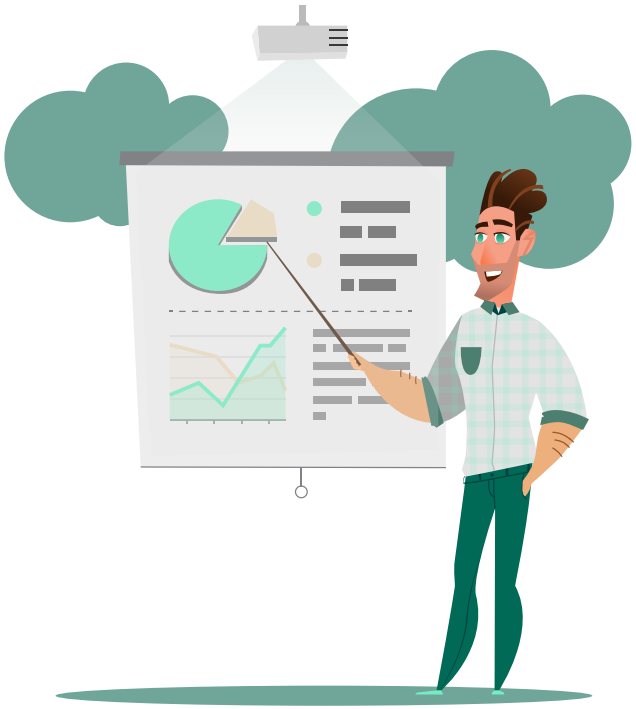
The Solution?

Don't use FTP. Use an SFTP server for security and encrypt all data in transit and at rest. For contractors, limit what they can see by giving them unique accounts segregated into roles and groups who have permission to designated folders only. This will prevent users like Sara from being able to access folders and directories outside the scope of her current responsibilities.

Cloud Storage Craig

Craig works in your marketing department. Based on the review-and-feedback nature of his work, where he must gain the approval of several stakeholders, Craig has chosen to store and share files using a cloud storage service. He likes its user-friendly interface and widespread popularity; it's easy for the whole team to use.

For the first few months, Craig only shares email drafts, ad ideas, and meeting agendas in the cloud. But after a while, he finds the cloud storage service convenient for quickly sharing other information, like monthly sales-qualified leads, customer survey responses, and sales reports.



Adam Says:

Cloud storage services like Google Drive or Dropbox are harmless in most cases, as long as IT knows about their use and how they're implemented. The encryption capabilities of these services may not be up-to-par, however. They may be limited to the cloud server and not mobile devices, and if someone hacks one of those accounts, the data within won't be protected.

The Solution?

Whenever possible, use a secure file transfer solution to share files with employees and stakeholders. Files are encrypted in transit, tracked with audit logs, and protected with extensive key management. It's also good to educate employees on what information is acceptable to share on these services, and remind them not to put sensitive data outside the internal network unless it's encrypted.

Build a Cybersecurity Toolbox for Improved Data Security

When determining cybersecurity strategies for your organization, we highly suggest implementing security practices to keep your internal users from leaking, accessing, sharing, or stealing sensitive information.

A secure file transfer solution like **GoAnywhere MFT** can introduce strong user management and security controls for most of these scenarios, as well as help you meet multiple data compliance regulations for file transfers and streamline your workflows and processes.

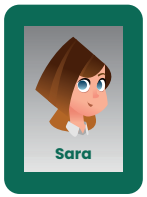
Here are the users GoAnywhere can help you address:

Departed Dave

With a secure file transfer solution like GoAnywhere MFT, you can use Active Directory and LDAP to restrict users to specific home directories and subfolders. If a user leaves, your administrator can disable them from the administration dashboard.

Gossip Grant

GoAnywhere MFT offers protection for data at rest using AES 256-bit encryption. By using GoAnywhere to encrypt sensitive data that's sitting on a shared network drive, your employees can complete daily responsibilities on that drive without having access to the files within.



Snoopy Sara

Implement an SFTP, FTPS, or SCP server with GoAnywhere MFT to replace FTP or other unsecure file transfer processes. GoAnywhere can also be used to apply user roles and file-based permissions for trading partners, vendors, and contractors while they access information on a GoAnywhere file server.

Fake Freddy

GoAnywhere MFT uses a combination of security controls to block hackers from brute-force hacking into the software. An IP blacklist automatically adds anyone who tries to log-in as "admin" or "administrator" too many times, and an auto-lock account feature can be triggered to temporarily disable any user who incorrectly types their password more than a few times.

Cloud Storage Craig

Modules like Secure Mail and GoDrive allow GoAnywhere users to collaborate securely, without putting sensitive data at risk. Files are always encrypted, comments can be added where they're needed, and revisions can be tracked. Furthermore, GoAnywhere is mobile-friendly, so you can take your file sharing on-the-go.

Cloud Storage Craig

Protect your business data with our other cybersecurity solutions:

Security Policy Management

Policy Minder automates security policy adherence by identifying, fixing, and reporting on security misconfiguration errors across your on-premises servers and public, private, or hybrid cloud infrastructure.

Learn more at www.fortra.com/policy-minder
Windows | Linux | PowerLinux | AIX | IBM i

Identity and Access Management

BoKS Server Control transforms your multi-vendor Linux/UNIX server environment into one centrally managed security domain.

Learn more at www.fortra.com/BoKS
Linux | PowerLinux | UNIX | AIX

Virus and Malware Protection

Stand Guard Anti-Virus scans systems for viruses, worms, and malware. It's built specifically for your systems' unique features, which means it's fast, stable, and more secure than using AV software for PCs.

Learn more at www.fortra.com/anti-virus
Linux | PowerLinux | UNIX | AIX

Threat Identification and Response

Powertech Event Manager translates critical data into actionable intelligence, allowing users to identify and respond to real time security events.

Learn more at www.fortra.com/event-manager
Windows | Linux | PowerLinux | UNIX | AIX | IBM i

Professional Security Services

With our professional security services, your organization can get the security it needs by partnering with our team of cybersecurity experts. We offer a consultative approach to services you can benefit from.

Learn more at www.fortra.com/mss
Linux | PowerLinux | AIX | IBM i

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.

fta-ga-gd-1122-r1-79d