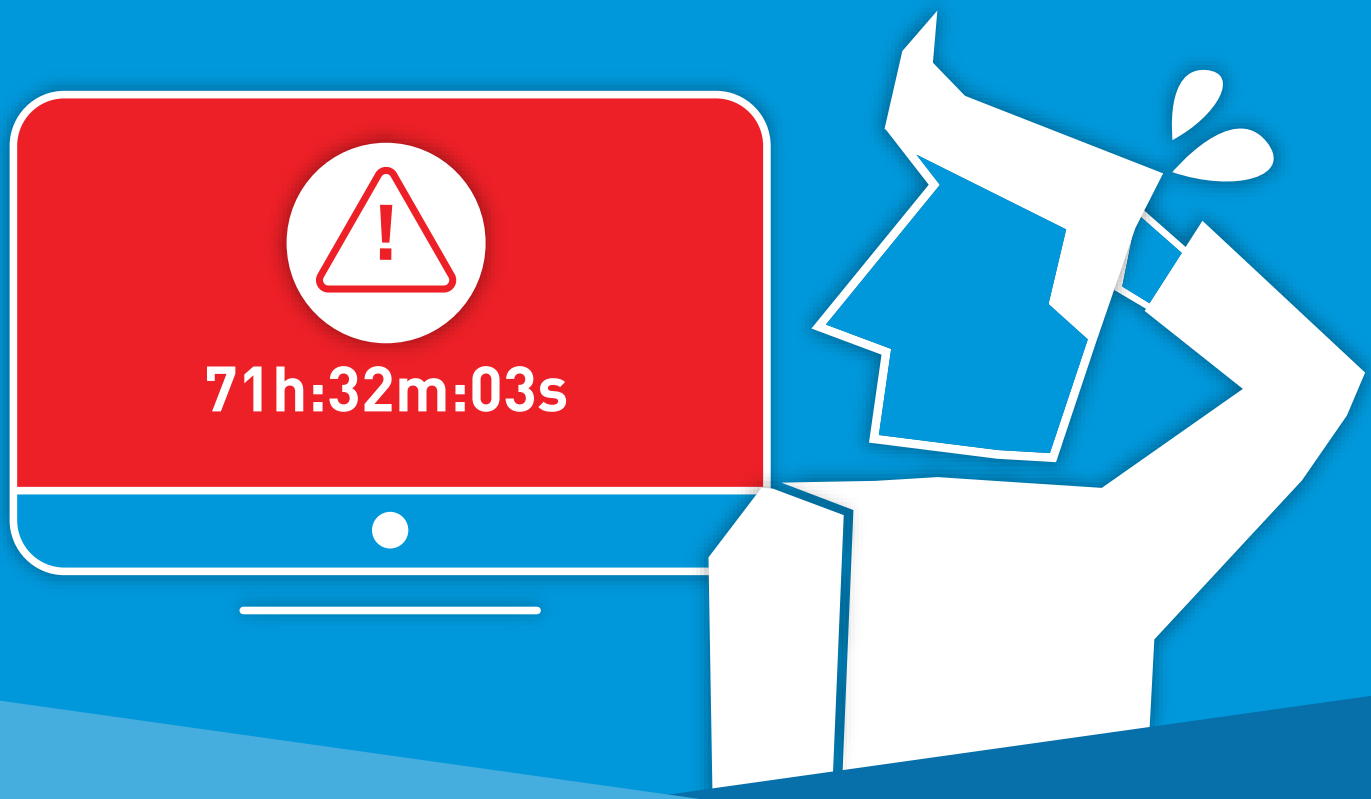
When an employee unwittingly triggers a ransomware attack



SecuriSync®

Advantage #2: Instant rollback and immediate access to hostage files

Six tips to ensure your users never lose another file

We're sure you've seen the news. New concerns over data security pop up regularly. In fact, our crypto-ransomware study[1] confirms that IT decision makers are highly concerned about ransomware.

With SecuriSync® by Intermedia, the all-in-one automated backup, file sharing and collaboration solution, you can get employees back to work quickly when a ransomware attack occurs and eliminate the most costly impact: downtime.

1 Be prepared

While many businesses have emergency plans for natural disasters, power outages or other disruptions, fewer have "e-crisis" responses for cyber threats. To protect your organization from attack, create a business continuity plan that includes SecuriSync in advance to shield your files, help contain the damage and limit the cost of lost sales, angry customers and bad PR.

2 Contain any outbreak immediately

As soon as you recognize there is an outbreak, remove any affected devices from the network so they cannot exploit an internet connection to infect others, or worse, send information back to the hackers. Shut down the network if you have to, then determine the scope of the infection, including source, type, number impacted and how much data is at risk. Once you have a handle on it, it's also time to consider contacting law enforcement.

3 Instantly roll back to clean files

SecuriSync files are backed up and synced in real time so they stay up-to-date whenever a change is made and can easily be restored to any previous versions. Leveraging its administrator controls on an uninfected computer, IT can complete a mass rollback of users' files and folders to the moment in time just before the infection occurred. **BONUS: This means there is no reason to ever pay a ransom demand.**

4 Get users back to work on alternate devices

With SecuriSync, files are accessible from virtually any device and browser so productivity can resume immediately after rollback, and the outbreak becomes just a mild disruption instead of a major disaster.

5 Rebuild the original machine(s)

The best practice to remove malware completely is to do a NIST secure wipe or replace the hard drive and install a fresh image of Windows. SecuriSync can then restore and sync files and folders, including any edits users make while on alternate devices.

6 Reassess your protection plan

Once order is restored, conduct a postmortem and roll out any necessary updates to your business continuity plan. Be sure to include end-user education/training to make sure everyone understands what caused the infection and how to avoid having it happen again.

SecuriSync is an easy-to-use file management service, which also helps secure and manage your critical business data. SecuriSync enhances traditional file sync and share by adding real-time backup and restore capabilities. It integrates with Exchange, Office 365, Outlook, Office and existing file servers and is backed by Intermedia's 24x7 phone support and 99.999% uptime SLA.

[1] http://www.intermedia.net/ransomware