

# Ransomware: Protect Your Business and Yourself

---



What is Ransomware?

Ransomware is a type of malicious software that infects a computer and restricts users' access to it until a ransom is paid to unlock it. In other words, if you want to continue to do business, you may need to pay someone a sum of money to regain access. This was the number one cause of loss in small-midsize businesses in 2022. If not equipped with the security, it could cost a company, their ultimate existence.

The perpetrators don't typically steal data but hold it hostage until they are paid, sometimes twice. Always evolving, ransomware attacks main drives as well as back-ups, preventing in-house restoration of files and data. Businesses who hold personal client information or rely on technology to operate their business are most at risk to an attack.

A subset of ransomware can be the infiltration into the business finances and determining whether they hold cash reserves. Typically, these funds are not insured and become very attractive. If a business does not have a need to hold large amounts of funds in their account, it is highly recommended they transfer those funds to a private investment account outside of their business where the funds are protected and hidden from any potential ransomware attack.

Being proactive in putting cyber security protocols in place at one's business is highly advised. Besides hiring outside cybersecurity companies to monitor and oversee your business, there are a number of things a company should consider doing:

- Regular and updated education and training for employees regarding phishing.
- Constant monitoring and maintenance of your computer systems including patching.
- Use Extreme Caution with Email Attachments and Links, regardless of the sender.
- Adopt a defensive strategy with multi-layer approach to firewalls.
- Anti-spam or Antivirus software.
- Use Multi-factor authentication.
- Cloud technology and security.
- Backup of files and stored separately.
- Avoid disclosing personal information.



Here at Griffiths, Dreher & Evans, we are actively executing each of the above bullet points with the intent to not only protect our client's interests but our own as well. In addition, our custodian, Charles Schwab & Company, Inc, where everyone's assets are held, provides another secure layer of cyber protection. In addition, your assets are insured through FDIC, SIPC and Lloyds of London for up to \$150 million for each account.

The more attention and focus you can place on cybersecurity as a real threat among every employee who has access to a computer is crucial in protecting your business. The threats continue to become more sophisticated and aggressive and the only way to deter these attacks is through continual education, awareness and active monitoring of your protocols and overall system.