June 2022 Issue

Webinar Recording Available! What Every Organization Needs to Know and Do to Mitigate Risk

Hosted by Gray, Gray & Gray's Hank Wolfson and cybersecurity expert Nathaniel Gravel, you will get a vital look at the cyber threats aimed at businesses, learn the most important actions to take to protect yourself, and gain an understanding of how current global affairs have spiked the risk of cyberattack for American companies. Here are just some of the takeaways from our information-packed webinar:

- A look into cybercrime and today's cybersecurity threat landscape
- Which cyber threats pose the greatest risk for small- and mid-sized entities
- Real-life examples of how cyber criminals infiltrate your network
- Steps you should take today to prepare for attacks against your organization
- How the combination of people, process, and technology can help reduce your attack surface

g3 gray
THE POWER OF MORE

GRAVOC

ACCESS THE RECORDING

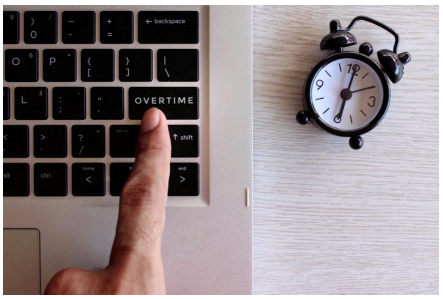
IRS Tax Tip

School is almost out for the summer, but tax planning is year-round.

Now that the April filing deadline has passed, most people are spending more time thinking about summer vacations than taxes. However, summer is a great time to review withholding and see if summer plans will affect next year's tax return.

READ THE FULL TAX TIP

DOL Seeks to Raise Overtime Exemption Limit



The U.S. Department of Labor (DOL) is expected to propose a higher salary level threshold for the management overtime exemption.

Currently, under the federal Fair Labor Standards Act's (FLSA) so-called "white collar" salary level exemption, employers are not required to pay overtime to managerial workers who earn a minimum salary of $684 per week ($35,568 annually). While no new threshold level has been announced, employee advocates argue that the DOL should match or exceed the proposed increase of $921 per week which was first introduced in 2016.

LEARN MORE

Planning Your Response to a Cyberattack

Layered defenses, penetration testing, constant monitoring, employee training, multi-factor authentication, "red team" simulated phishing – we use all the tools in our bag to identify and deter "bad actors" from accessing data or breaching networks.

But it does not always work. No plan is perfect, and cyber criminals spend millions of dollars each year developing more sophisticated methods to infiltrate defenses of organizations both large and small. Which is why two of the most important components of an effective cybersecurity defense are a response process and business recovery plan.

READ THE FULL ARTICLE

Do you have a colleague that would like to receive our news?

SUBSCRIBE HERE

Gray, Gray & Gray, LLP | www.gggllp.com

Share This Email