Security matters.

At Western Alliance Bank, we are committed to maintaining the best cyber security practices to keep private client information private. We often advise our clients and others how to best secure their places of business. It starts with the realization that anyone—from the newest intern to the C-level executives—can become a target of digital crime and leave your company exposed.

According to an IBM 2016 Ponemon Cost of Data Breach Study, the average consolidated cost of a data breach is around $3.8 million—that’s an increase of 23% from 2013. Records or data stolen loses money, and the average amount of money lost for each record or piece of information stolen comes to $154. That’s a 6% increase from $145 in 2013.

The major causes of breaches according the Identity Theft Resource Center:

- Hacking, 22%
- Insider theft or accidental exposure, 12%
- Subcontractors or third-party companies, 11%

Experian, a credit information company, noted that 80% of the breaches that they often handle are directly tied with employee negligence. So what can you do to protect your company?
The Department of Homeland Security urges all CEOs to ask themselves the following questions:

- How is our executive leadership informed about the current level and business impact of cyber risks to our company?
- What is the current level and business impact of cyber risks to our company? What is our plan to address identified risks?
- How does our cybersecurity program apply industry standards and best practices?
- How many and what types of cyber incidents do we detect in a normal week? What is the threshold for notifying our executive leadership?
- How comprehensive is our cyber incident response plan? How often is it tested?

At Western Alliance we advise our clients to first understand that Cybersecurity is NOT implementing a checklist of requirements; rather it is managing cyber risks to acceptable level and should be part of an organization’s governance, risk management and business continuity framework.

Make sure to stay informed through real-time and trend data on cyber events, lean on business-line managers to help identify potential supply chain risks created through third-party vendors or cyber dependencies.

Above all, regardless of company size, be sure to implement these simple practices that can help reduce the risk of cybercrimes at the office and when doing business remotely from mobile devices or home offices.

- Designate Specific Computers For Banking and Business Activities. Restrict personal activities on these systems such as internet browsing and access to personal email boxes.
- Review Financial Statements As Soon As They Arrive. Monitor monthly statements for discrepancies and unknown activity.
- Install and Maintain Anti-Virus/Anti-Spyware. Ensure you have a layered security approach that includes anti-virus/anti-financial malware solutions appropriate to your environment and update them regularly.
- Back-Up Data. Perform regular backups of critical data and store in multiple locations.
- Use Caution With WiFi Hotspots. When accessing business-related accounts and documents using WiFi at a coffee shop, airport or any public space, practice extra caution.
- Enable Security Features On Home Networks. Prevent unwanted access on home networks by enabling security features, using a strong password and encryption.
- Use Care When Social Networking. Do not reveal sensitive information when using social networks such as Facebook and LinkedIn. Modifying settings to prevent strangers from viewing you page is also recommended.
- Sector Information. Sharing and Analysis Centers, government and intelligence agencies, academic institutions, and research firms also serve as valuable sources of threat and vulnerability information that can be used to enhance situational awareness.

WesternAllianceBank.com

Western Alliance Bank
Banking Divisions:
Alliance Bank of Arizona
Bank of Nevada
Bridge Bank
First Independent Bank
Torrey Pines Bank

Member FDIC