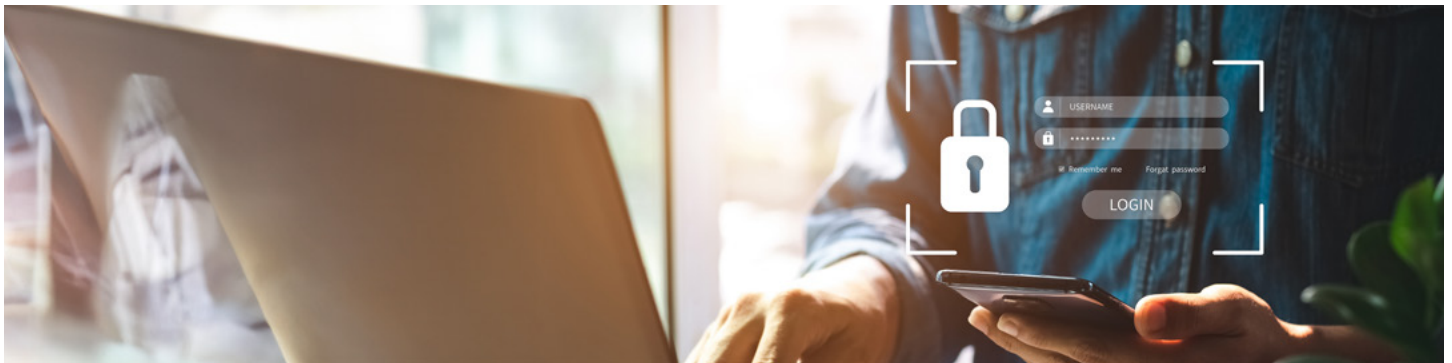


# The AvTek Chronicle



Wayne's World  
Where in the  
world is WAYNE?

**Wayne speaks at Fall 2023  
P3 Conference in Omaha  
Sep. 6th - 8th**

**Kaseya + Datto Connect  
Local: San Antonio  
Security & Compliance  
Panel - Sep. 14th**



**"Coming up" – November  
Small Business Tech Day  
in Houston**

Register here:  
[www.avteksolutions.com/tech-day-2023/](http://www.avteksolutions.com/tech-day-2023/)

**Security & Risk  
Management Conference  
Nov. 29th**

## September 2023



Wayne Hunter is the President and CEO of AvTek Solutions, Inc. where he concentrates his efforts on providing the best solution to customers.

Wayne has over 30 years of experience in Information Technology, focusing on implementing storage and data systems, IT management, and systems integration.

## How To Safely Share Passwords With Employees

If you ask a security professional, you get by-the-book advice about sharing passwords: "Don't share passwords." But we know, in reality, that doesn't work. Your office might be sharing a single password for apps like SurveyMonkey right now to save cash on buying additional users, and some social media accounts don't even give you the option to have multiple log-ins. Sharing passwords in your office is sometimes necessary for collaboration, and the best way to do this is by using a password manager. Affordable (some platforms even offer free versions), layered with security and simple to use, password managers are the safest and easiest way to store and share your company's private passwords.

### Reasons You Would Need To Share Your Passwords

Shared accounts are the biggest reason businesses share passwords, whether their employees work from a physical office or at home. It improves collaboration and makes employees' jobs a lot easier. Medical leaves, turnover, vacations and "Bob isn't coming in because he ate bad fish last night but has our Amazon log-in" are other reasons passwords get handed around like a plate of turkey at Thanksgiving dinner. However, unsafe sharing habits will put your private passwords in the hands of greedy hackers, who can fetch a high price for your data in dark web markets. IBM Security reported that in 2022, 19% of all breaches were caused by stolen or compromised credentials. So, how do you share passwords safely?

### First, Avoid These Common Password-Sharing Mistakes

When it comes to password sharing, remember:

**1. Don't send passwords via e-mail:** E-mail is the #1 target of hackers, and many e-mail services aren't encrypted.

Those that are encrypted are still risky because e-mails are stored in several servers on their way to or from your account. That means your e-mail is sitting in a Sent folder, ripe for the taking by anyone who gets into your e-mail account, encrypted or not.

**2. Never text or chat passwords:** Like e-mails, SMS messages or messaging apps like Slack aren't secure. Once a text is sent, it is available for anyone to see.

**3. Stay far away from storing passwords using pen and paper and shared documents:** Sticky notes, memo pads, Google Docs – NEVER write down your passwords.

**4. Avoid the temptation to store passwords on your device:** If your device gets hacked, nothing stops that perp from taking every password you saved.

### The Best Way To SAFELY Share And Store Your Passwords

We recommend using reliable password managers because they have multiple layers of encryption so only those with a key (your master password) can see it, AND they include more robust security and sharing features like:

- **Zero-knowledge architecture:** Not even your password manager service can see the information you save in your vault.
- **Multifactor authentication (MFA):** For added log-in security.
- **Unique password generation:** Creates strong, random passwords to improve log-in security.
- **Fake log-in page warnings:** Warns you if a page is spoofed by hackers.
- **Breach or weak password notification:** Alerts you if one of your passwords was leaked or if your current password is weak.

• **Simple, secure built-in password sharing:** Some password managers let you choose which passwords your employees can see and keep others in a private vault. Others, like Keeper, let you share documents or records without exposing credentials.

To use password managers, you only need to remember one password – the master password. One downside is that whomever you share a password with needs an account for the same service. However, most password managers have corporate accounts, so this shouldn't be a problem.

**A Word To The Wise:** Look out for password managers with a

bad security track record, like LastPass, which was breached in 2022, 2021, 2016 and 2015.

**Smart Businesses Use Password Managers**

It's a good idea to avoid sharing passwords as much as possible, but when you have to, use a reliable password manager to ensure you have control over exactly who sees your credentials. Talk to your employees about safe password hygiene, host regular security-awareness training for employees and use MFA with every account. It's not just safe business – it's smart business.

If you're not sure which password manager to use, give us a call and we'll get you set up with one.



**Essential Elements of an Effective Compliance Program**

**The 6 Essential Elements of an Effective Compliance Program: Appointing a Chief Compliance Officer (CCO)**

Listed below are six foundational elements to consider for your compliance program. We will focus on the third foundation for the month of September:

1. Executive Sponsorship and Commitment to Compliance
2. Conduct Risk Assessments and BIA
3. Appointing a Chief Compliance Officer (CCO)
4. Establish or Refresh Your Data Governance Strategies
5. Monitoring, Testing and Updating
6. Routine Employee Training

**Appointing a Chief Compliance Officer (CCO)**

Appointing a CCO is not an easy job. However, having a dedicated CCO is vital to avoid non-compliance issues in the long run. A CCO:

- Drafts policies and procedures needed for the business' compliance.

- Communicates the policies, procedures, and relevant updates across the entire organization.
- Monitors the business' compliance and investigates instances of non-compliance.

Compliance programs are not one-size-fits-all programs. You will certainly need to develop a plan that meets your business' specific needs while recognizing that compliance requirements will limit your ability to make decisions based on your risk tolerance and desire to control costs. Rather than recreating the wheel, you can adopt a recognized security framework that aligns closely with your compliance requirements. The aim should be to build your compliance program to be both effective and comprehensive so that it stands up to scrutiny.

To learn more about how to tailor a compliance program to meet your organization's unique requirements, schedule a consultation with us

[www.avteksolutions.com](http://www.avteksolutions.com)

**Who Else Wants To Win A \$25 Gift Card?**

The Grand Prize Winner of last month's Trivia Challenge Quiz is Dylan Farmer! He was the first person to correctly answer my quiz question from last month. The answer was:  
b. I'm feeling lucky

You can be the Grand Prize Winner of this month's Trivia Challenge Quiz! Just be the first person to correctly answer this month's trivia question and receive a \$25 gift card to XXXXX. Ready? Call us right now with your answer!

What is the world's best-selling PC game?

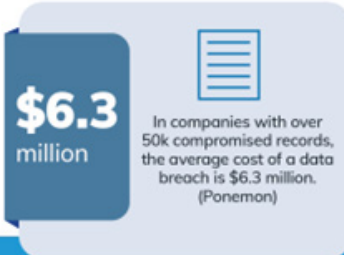
- a.) Minecraft    b.) World of Warcraft    c.) Half-Life 2    d.) Doom



## Remote Work Is No Joke

### CYBER RISK – SECURITY ESSENTIALS

While there is no universal governance, most insurers expect their clients to follow and maintain some basic security practices without fail.



- ✓ **Security risk assessment** - Regular IT security audits of your business will detect & identify vulnerabilities and areas with high potential risk, giving you the detailed insight needed to repair, resolve or contain threats or issues.
- ✓ **Patching strategy** - Is there a patching strategy to keep the software up to date?
- ✓ **End-of-life software/OS** - Are there any outdated software and OS in the network?
- ✓ **Security training for employees** - What level of security training do employees have?

I recently read an article in the New York Times titled *We’re Kidding Ourselves That Workers Perform Well From Home*, which I felt urgently needed a counterpoint. The article discussed the Houston-based law firm Ahmad, Zavitsanos, Anaipakos, Alavi & Mensing as they navigated the pandemic, avoided layoffs and achieved their best year on record. It’s an inspiring story, and I don’t mean to take any credit away from it.

That being said, the heart of the story is that Mr. Zavitsanos attributed the success of his business to his colleagues returning to the office during the pandemic. Mr. Zavitsanos stated, “Ambitious lawyers at firms like ours simply couldn’t thrive in a virtual setting.” That may be true for his firm, but I fear his case might scare off leaders considering a more flexible work arrangement for their workforces.

I want you to consider the alternative experience my company ghSMART saw, as we offered flexible and remote work before and during Covid-19 and produced similar results. At ghSMART, every employee has worked from home since day one, and we have never doubted ambitious professionals can function with remote and flexible work.

At ghSMART, we achieved record revenue and profits throughout the pandemic, completing a 10-year average annual revenue growth of 21% and profit growth of 24%. Client satisfaction metrics reached all-time highs. Our clients are

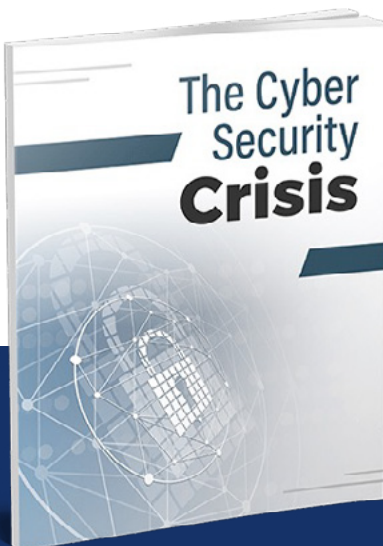
board members and CEOs of some of the largest companies in the world as well as private equity investors of the largest funds and government leaders.

If you think a remote firm can’t build a successful culture, you’d be wrong. ghSMART recently won an award for being the best management consulting firm to work for. This was out of 100,000 firms and based on overall employee satisfaction. We also hold a Glassdoor culture rating of 4.9 out of 5, which is #1 in our industry.

You’d also be mistaken if you thought a remote firm would struggle to attract top-tier talent. We have four New York Times bestselling authors and two Rhodes Scholars, and many of our colleagues have performed at the top of their peer groups. It’s clear you can attract and retain top talent at a remote firm.

For the leaders of those organizations considering flexible and remote work, I say give it a chance. It offers a level of freedom and flexibility your employees will be incredibly grateful for, and you may even see an uptick in productivity.

Dr. Geoff Smart is the chairman and founder of ghSMART, a leadership consulting firm that exists to help leaders amplify their positive impact on the world. Dr. Smart and his firm have published multiple New York Times best sellers. He stays active in his community and has advised many government officials.



### Free Guide: The Cyber Security Crisis

The Cyber Security Crisis Urgent And Critical Protections Every Business Must Have In Place NOW To Protect Their Bank Accounts, Client Data, Confidential Information And Reputation From The Tsunami Of Cybercrime  
Get your copy here: [www.avteksolutions.com](http://www.avteksolutions.com)

## Want To Become A Better Leader? Learn How To Manage Yourself First

Every business owner and leader wants to lead and inspire their team effectively, but this is easier said than done. You're going to face challenges within your business that will put your mettle to the test. Many of these obstacles will stem from your team as you learn to manage different personalities and overcome communication barriers. If you want to lead your team properly, you must take a step back and focus on yourself first.

Many employees look to their leaders for support, encouragement and guidance. As their leader, you have to remember you are setting an example for your team, so you must stay aware of every action you take. Pay attention to how you talk to people and how you're spending your time while at work. You should be acting in the same manner you would expect from every other member of your team. If you're not, it's time to make some adjustments. Your business's success and your employees' behavior begins and ends with you. Become the leader you would want to work for, and your employees will respond positively.

## IS IT TIME FOR A VACATION FROM WORK?

Business leaders want their companies to be profitable and often dedicate hours of overtime every week to ensure everything runs smoothly. While this might give your business a boost, it can be damaging to your mental health. Many leaders have a hard time taking a break from their business and end up

burning out before reaching the pinnacle of success. Don't fall into this trap. Here are a few warning signs to pay attention to that tell you it's time to take a break from work.

**You feel anxious or nauseous every morning before work.** Your body will tell you when it needs a break. Listen to it!

**You make careless mistakes.** Overworking ourselves can take away from our focus, which causes us to make mistakes we wouldn't normally make.

**Your motivation has vanished.** If you feel like you have to force yourself through the motions at work, it's likely time for a vacation.

## Experience Fewer Errors With New Hires By Refining Your Onboarding Process

Onboarding is an essential part of the hiring process. While interviewing allows you to select the right person for your open position, onboarding gives you an opportunity to train them before they start their day-to-day responsibilities. This is your chance to set them up for success. If you haven't already done so, document the tasks for every position in your company in the coming weeks. Speak with the person currently in that role to ensure you don't miss any critical functions. This will give you a great start for a flawless onboarding system. From there, you can document any questions or concerns that arise in future onboarding sessions to cover any holes. With time, your onboarding process will soon run itself!

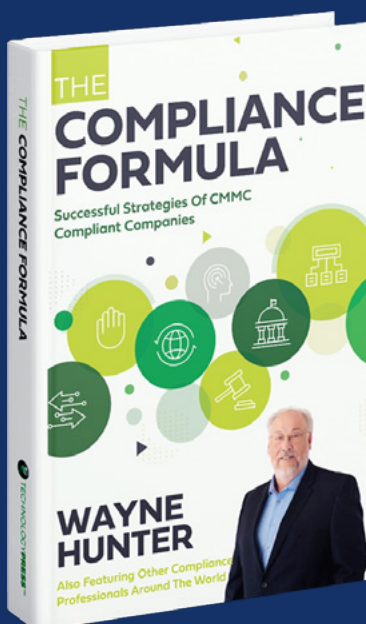
## READING CORNER

### Join The 7 Figure Club By Mark Anthony

Most business owners have a difficult time stepping away from their work. They want to profit as much as possible, which means they believe they must give all of their time, effort and attention to the business. But what if you could run a profitable business without sacrificing everything else? In Join The 7 Figure Club by Mark Anthony, you'll learn how to increase sales, improve staff accountability, devise ways to reclaim your free time and much more. Anthony offers practical advice for readers and shares the seven pillars of a thriving business. If you're ready to take your business to the next level, add Join The 7 Figure Club to your reading list.



## The Compliance Formula: Successful Strategies Of CMMC Compliant Companies



The definitive guide to understanding and implementing CMMC: everything you need to know to win DoD contracts and squash your company's vulnerabilities from hackers, data theft, and ransomware.

You must make implementing CMMC a priority. Right now, crime organizations are paying up to \$90,000 a month plus full benefits to people who will hack into your business. Without CMMC compliance, you will lose DoD contracts, stunt future business growth, and risk your business survival. We've gathered 21 top CMMC compliance experts to help you figure out which level of CMMC compliance is right for you and provide a blueprint to make it easier to put these standards in place, so you can secure your company against criminals, win more business, and create a powerful, competitive advantage.

This Amazon Best Seller book titled The Compliance Formula...Successful Strategies Of CMMC Compliant Companies co-authored by Wayne Hunter gives businesses like yours the knowledge, strategies and action steps protect your business from hackers.

## CHECK IT OUT NOW