THE HD TECH WAY

Insider Tips To Make Your Business Run Faster, Easier And More Profitably

TRUTHS ABOUT CYBERSECURITY

EVERY BUSINESS LEADER SHOULD KNOW

There are many common myths when it comes to cybersecurity, and, unlike harmless stories, these myths can leave you with gaping holes in your company's cybersecurity defenses. Here are five common myths and the truth behind them.

Myth #1: It Won't Happen To Us.

There's a common belief among small and medium-sized businesses that they are too small to be a target for attackers. But this isn't the case; in fact, some cybercriminals target SMBs specifically, with the knowledge that SMBs are less likely to have the resources for reliable cybersecurity.

Cyberattacks happen to organizations of all sizes, in all verticals and geographies, and hit 80% of businesses. The global financial toll? A projected $9.5 trillion. And while large corporations can take the hit and recover, a single ransomware attack has the potential to put an SMB out of business.

So, regardless of what type of business or organization you have, you must protect yourself from cyberattacks and reduce your exposure. Always assume you are a target – because you are one.

Myth #2: If It Worked Then, It'll Work Now.

It's very common for decision-makers to reason that since they've never been breached in the past, they won't be breached in the future either. However, that belief doesn't account for the rapid pace at which technology – and cybercrime – are evolving.

The threat landscape is constantly changing and there is a very real game of cat-and-mouse at play. If you're not moving forward, you're moving backward. Effective security is a cycle of anticipation, adaptation and action.

Myth #3: Once Secure, Always Secure.

Unfortunately, technology is fluid – just like your business. Every time you bring on a new member of staff and add new devices, your technology's configuration shifts. As it does, it creates new avenues of attack from cybercriminals.

That's why continuous monitoring

continued on page 2...

...continued from cover

and management are necessary to maintain security integrity. The attack surface stretches beyond common focus areas. Because of this, strong cybersecurity demands a holistic, proactive, continuous approach.

Myth #4: Business Optimization Is Incompatible With Security.

Many organizations still assume that security initiatives create operational friction – delaying releases, adding red tape and increasing costs. This outdated thinking frames security and business optimization as mutually exclusive, as if improving one compromises the other.

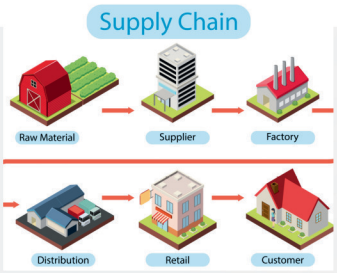
While these perceptions may have roots in the past, they don't reflect modern practices. Today, security enables optimization. That means minimizing both waste and risk – including security risk.

In the end, secure systems are more resilient, predictable and cost-effective. This makes security a driver of business performance, not a barrier.

Myth 5: A Strong Password Is All I Need.

Creating a strong password (at least 16 characters long and a blend of letters, numbers and special characters) for each account is important, but it's not the only step needed to keep your data secure. For one, every account and device needs a unique password. If you reuse passwords, it means that if one of your accounts is hacked, all of your other accounts are at risk. To store all your unique passwords, we recommend a password manager!

Enabling MFA for every account will double your protection. The few seconds required to enter a code sent to your phone is well worth the extra security. That said, there are plenty of other vulnerabilities that savvy hackers can exploit to attack your business's data. That's why working with an MSP is a critical component of maintaining your company's cybersecurity.



FREE Supply-Chain Attack Vendor Security Scan

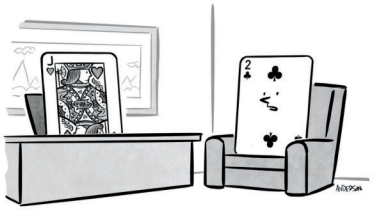
One of the most critical aspects of Cyber Preparation is understanding the concept of a "Supply-Chain Attack."

This type of attack occurs when an adversary targets the less secure elements within a supply chain to gain access to the primary target. The consequences of such breaches can be far-reaching, affecting not only the compromised entity but also its business partners and clients. To mitigate this risk, it is imperative for businesses to work closely with their partners to identify and address potential vulnerabilities.

As part of our commitment to enhancing cybersecurity, we are offering a free Security Scan to ANY of your vendors who, if they were to go down, would impact your workflow and business operations. We'll conduct a comprehensive evaluation on your behalf that will identify potential weaknesses in their (Vendors') network and provide actionable recommendations to fortify defenses. By taking advantage of this offer, your business can gain valuable insights into the current security posture of your most important vendors and take the necessary steps to enhance their resilience against cyber threats.

To Get Started and Claim Your COMPLIMENTARY Supply-Chain Attack Security Assessment Now, Call Our Office At 877-540-1684 or email Vendor Security Scan to help@hdtech.com.

CARTOON OF THE MONTH



"Where do I see myself in five years? Maybe a 5 or 6."

OPERATIONAL EXCELLENCE

PART 2: PROCESS OPTIMIZATION AND EXECUTION

Written by
Thomas Willingham
The Hampton Group
www.thampton.com

The Roman Emperor Marcus Aurelius is attributed with the quote "A well-defined process will give a well-defined result". **Plan-Do-Check-Act** (PDCA for short) is a fantastic methodology to use on small pilot projects to begin your journey towards Operation Excellence because it also supports improved Execution. Organizations that execute well do four things very consistently:

1 Have a Plan

Their people know the Goals. In other words, they have a **PLAN** and there is clarity around an expected outcome or Key Performance Indicator. At the individual process level, this means clear target production rate, customer service level, or similar metric including a target date.

2 Define the DO

Their people know what to do to achieve their goals. Defining what to **DO**, or the tasks/action items to achieve the goal is often the hardest step. Clear documentation of the process steps, including individual roles and responsibilities, is necessary to ensure a team is aligned, correctly prioritizing and sequencing tasks so they are pulling in the same direction.

3 Make a CHECK

Their people know the Score. CHECKing progress against the performance measures and goals is vital feedback for a team. Imagine a baseball game where balls and strikes were not called but the batter is suddenly called "out". Some best-in-class manufacturing companies have electronic display boards showing cumulative production or status boards where each department can meet at scheduled breaks to review progress.

4 Act

There is clear accountability for results. **ACT**ing on the results does not mean being punitive if a goal is missed. It means evaluating the progress, making mid-course corrections, and beginning the PDCA Cycle again.

Operational Excellence - Building upon the Methodology

With each iteration of the Operational Excellence methodology, an incremental improvement can be made, and employees will begin to embrace being part of the process.

SHINY NEW GADGET OF THE MONTH

BenQ ScreenBar Halo Monitor Light

The BenQ ScreenBar Halo is a sleek USB-powered LED monitor light designed with an asymmetric optical system that directs soft, glare-free illumination onto your desk while avoiding screen reflection. With adjustable brightness and color temperature, you can dial in the perfect lighting using the wireless controller. It even has a backlight to reduce contrast with your surroundings. Plus, the auto-dimming feature adapts to your room's lighting, so it's always just right. No messy cords or mounts – just clean, functional lighting that protects your eyes and keeps your setup looking sharp.

Event Wrap-Up:

Mercy House Golf Tournament 2025

For the last couple of years, we've had the honor and privilege of teaming up with our friends at Mercy House and were sponsors and attendees for the event. We had an absolute blast and loved making memories and sharing a bit about our team, all while raising money to fight homelessness.

If you're interested in a recap or want more information on the Mercy House tournament, head on over to our LinkedIn/Website to see the posts covering our fun day on the course and our "Spot the Threat" Challenge!

Thanks to everyone who participated in this great event, we had a great time meeting you!

5 SIGNS

YOU'RE DUE FOR A TECH UPGRADE

At first, hanging on to old technology for as long as possible seems like a great way to stretch your IT budget. However, the cost of doing so is much higher than simply replacing the tech.

Continuing to use old hardware and outdated software can cost your business in productivity, budget and security.

The Real Cost

There are a few ways that outdated technology is costing your business. First, old systems move slower, causing your team to move slower and impacting productivity. These systems can also fail completely, causing unexpected downtime and putting a major dent in your deliverables.

There's also the risk factor to consider.

Outdated software and hardware are more vulnerable to cyberattacks, because they are no longer being patched to protect against known vulnerabilities.

Hackers are able to exploit these vulnerabilities and access your business's data. Because of this latent risk, your business also runs the risk of failing compliance audits. That's why it's so important to update to the latest software or hardware to stay secure.

Here are a few signs it's time to upgrade your technology:

1 Your Systems Are Still Running On Windows 10 Or Older

Windows 10 is rapidly approaching end of life; Microsoft will end support for it on the 14th of this month. This means any new vulnerabilities will no longer be patched by security updates. Continuing to use Windows 10 past its end-of-life date is a major cybersecurity and compliance risk. To keep your business protected, start planning your upgrade path now and make the switch to Windows 11.

2 You Frequently Call IT For The Same Tech Problems

Frequent crashes and lagging systems aren't just annoyances, they're also indicators that your technology is failing. Slow systems, crashes, frustrated team members and constant tech support add up – and mean a significant impact on your productivity.

3 Your Existing Software Isn't Compatible With New Tools

If you're still using legacy software, it may not integrate with mobile apps or cloud platforms. This limits your ability to adopt new technologies, serve clients efficiently and scale your business.

4 Your Devices Are Slowing Down Your Team

If your team's computers are taking ages to boot up, or freeze or crash during video calls, they're slowing down your entire workflow. At the end of the day, time is money. Inefficient systems harm both. Devices more than three to five years old should be audited for performance and energy efficiency to ensure they aren't having a negative effect on your productivity and energy consumption.

5 You're Relying On Outdated Security Mechanisms

If your business's firewall or antivirus hasn't been updated in years, you're taking serious risks with your data. Cyberthreats evolve quickly; to keep your business safe, your defenses need to evolve too. Outdated systems are often the first point of entry for ransomware attacks.

If you're worried that upgrading tech will break the bank, we hear you. But hanging on to slow, outdated systems can cost more in lost productivity, security gaps and patchwork fixes. The good news is there are plenty of affordable, strategic upgrade paths to keep your business running smoothly without blowing your budget.