www.hdtech.com FEBRUARY 2026

THE HD TECH WAY

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

CYBER RESILIENCE:

WHY IT MATTERS MORE THAN YOU THINK

Most businesses still picture Cybersecurity like an old-school castle.

Big walls. Heavy gates. Keep the bad guys out and hope for the best.

But the modern workplace isn't a castle anymore. Your team works from home, the office, coffee shops… your data lives in the cloud… and your systems talk to dozens of other services every day.

There is no wall now. And cybercriminals know it.

That's why the big focus in cybersecurity has shifted from "stop every attack" to "be ready to bounce back fast when something happens".

That's what cyber resilience is all about.

Because here's the truth no one loves to hear: Even well protected businesses get hit. Someone clicks the wrong link. A supplier has a breach. A new AI-powered scam slips past a filter. It happens.

What matters is what happens next.

A cyber resilient business can spot trouble quickly, shut it down before it spreads, and get everything back on track with minimal fuss. It's less "panic stations!" and more "okay, we've got this".

A big part of that is having systems that constantly keep an eye out for odd behavior. Things that look suspicious even if no one has pressed a big red alert button.

Modern tools (many using AI) are brilliant at this. They can catch weird logins, unusual file movements, or signs that someone is trying to sneak into a system.

And then there's the safety net: Backups.

Not just any backups either. Proper, secure, tamper-proof backups that can't be wiped or encrypted by an attacker.

When these are set up right, recovering from an incident can be surprisingly fast. Sometimes so fast your customers don't even notice anything happened.

But technology is only half the story. The other half is people.

continued on page 2…

...continued from cover

Cyber Resilience & Your Team

Your team needs to know what a shady email looks like. Leaders need a simple, clear plan for who does what in an emergency. And everyone needs to know that speaking up early is always better than hiding a mistake.

Cyber resilience isn't about perfect systems. Cyber resilience is about being prepared, staying calm, and recovering quickly.

Does your business need help building a cyber resilience strategy? Get in touch.

INSPIRATIONAL QUOTE OF THE MONTH

> *"Your most unhappy customers are your greatest source of learning."*
>
> **Bill Gates, American businessman and philanthropist.**

Q: How do I know if our cybersecurity tools are working?

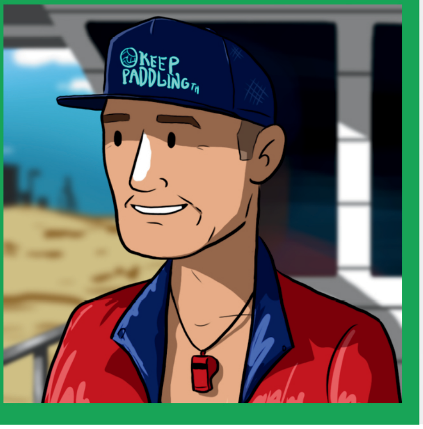
- Answer: Good security tools should give regular reports, alerts and logs. We can review these with you and check whether anything looks unusual or needs improving during your strategic business review (SBR).

Q: What's the difference between a backup and a disaster recovery (DR) plan?

- Answer: A backup saves your data. A disaster recovery plan gets your whole business running again quickly after an outage utilizing those backups. You need both.

Q: How can we tell if one of our suppliers is a security risk?

- Answer: Ask whether they use multi-factor authentication, encryption, and regular security audits. We have forms you can send to vendors to assess their cyber security, and we are happy to help you assess their risk level.



DID YOU KNOW...

AI Usage Policies - Why You Need One

There's been a lot of talk about AI being used to launch fully autonomous cyberattacks, but new research suggests that reality is still a long way off.

The way AI is being used effectively is to allow hackers to be faster and cover more attacks vectors than ever before. AI is used as a force multiplier for hackers, not as a stand-alone tool.

The other big risk is employees inadvertently exposing company data to the AI engines. An AI usage policy for employees is a must have-employees are using AI it's up to you to protect your company data thru education and governance.

OPERATIONAL EXCELLENCE

PART 5: EMPLOYEE EMPOWERMENT & STRATEGIC ALIGNMENT

For decades, organizations have launched "continuous improvement" initiatives, yet many of these efforts fall short—not because the tools are ineffective, but because employees are not meaningfully engaged in the process. Operational excellence takes a different view: employee empowerment and strategic alignment are not optional; they are foundational.

In this segment, we introduce the **Kaizen philosophy**, a proven approach that places continuous improvement directly in the hands of the people closest to the work. Kaizen is derived from the Japanese words Kai (*change*) and Zen (*good*), meaning "good change."

At The Hampton Group, we frequently guide clients through a **Kaizen Blitz**—also known as a Rapid Improvement Workshop. Over three to five focused days, a cross-functional team works together to solve a specific problem or improve a targeted process—while building stronger engagement and ownership.

The Kaizen Blitz Approach

1. Learn to See Waste

Teams are trained to identify waste within the process using **Value Stream Mapping**, introduced in Part 3. Documenting the current state of the process makes inefficiencies visible and creates a shared understanding of the process.

2. Learn to See Waste

Teams brainstorm solutions using root cause analysis and design the future state of the process. Emphasis is placed on no-cost and low-cost solutions that can be implemented and tested quickly.

3. Implement & Validate Improvements

This is where Kaizen delivers real impact. Teams are empowered to implement their ideas and generate quick wins. The **DMAIC framework** (Part 4) provides structure to measure results and document improvements.

4. Share Results & Align with Strategy

Teams present their results to management, celebrate successes, and discuss lessons learned. Leadership helps teams connect their improvements to broader organizational goals and identify additional opportunities.

The Results We Commonly See:

- Increased employee trust and confidence that their ideas matter
- A 20% reduction in loan processing time
- A 46% reduction in machine changeover time

After completing your first Kaizen Blitz, you don't just gain process improvements—you build a team of improvement champions ready to lead future Kaizen efforts. Empowered employees, aligned with strategy, are the engine of operational excellence.

Next Month: Part 6: "Cultural Transformation to Sustain Excellence"

GADGET OF THE MONTH

Creative Pebble V3 Minimalistic Desktop Speakers

If you want great sound on your desk without spending a fortune (or filling your workspace with giant speakers), the Creative Pebble range is a brilliant pick.

These compact little spheres deliver surprisingly rich, deep audio. Far better than you'd expect for the price.

They're perfect for Teams calls, focus music or a bit of background LoFi while you work. Plus, they take up hardly any space and look stylish on any desk. A small upgrade that makes a big difference.

$35.99 from Amazon.

HD Technology Update

Use guest chat in Microsoft Teams *with caution*

Microsoft Teams recently introduced a guest chat feature that lets anyone start a conversation with you using just your email address, even if you don't normally use Teams.

Handy. But researchers have spotted a gap. When you join someone else's Teams environment as a guest, you're protected by their security settings, not your own. That means a malicious host could send phishing links or harmful files without your usual security tools spotting them.

It's unlikely to affect most people but only accept Teams invites from people you trust. And be cautious with unexpected messages, no matter which platform they arrive on. If you don't know who the message is from-don't respond.

FAKE-ALERT PROTECTION TOOL FOR MICROSOFT EDGE

1. What is Scareware?

When was the last time you saw one of those scary pop-ups claiming your computer was infected?

You know the ones. They come complete with flashing red warnings and a fake phone number to "call Microsoft support".

It's called **scareware**, and it's designed to panic you into handing over money or access to your device.

And even the most careful among us can be caught off guard.

You may be as happy as I am to hear that Microsoft is fighting back. In a big way.

In an update to its Edge browser, Microsoft has rolled out a new scam protection tool that uses artificial intelligence (AI) to stop these fake alerts before they even reach you.

It's part of a wider effort to make Edge one of the most secure browsers for both Windows and Mac users.

Edge now includes something called a Scareware Blocker. This is switched on by default for most newer computers.

2. Introducing Scareware Blocker

It uses a clever AI model that can "see" the kind of full-screen scam pages designed to look like real system alerts.

The ones that say, "your device is infected" or "call support immediately."

And when it spots one, it shuts it down instantly, before you or your team have a chance to click anything dangerous.

If someone does happen to report a scam, it helps everyone else too. Microsoft's Defender SmartScreen system learns from that report and blocks the same scam for others. Sometimes hours or even days before it would normally appear on global threat lists.

In tests, just one report stopped about 50 other people from being targeted.

3. Scareware Sensor for Edge

There's also a brand-new scareware sensor built into the latest version of Edge. This helps Microsoft's systems spot new scams in real time, without sending your personal data or screenshots anywhere.

It's switched off for now, but Microsoft says it will soon be enabled automatically for anyone with SmartScreen turned on.

Unfortunately, scams are everywhere, and they're getting worse. One wrong click on a fake warning can lead to serious consequences from stolen passwords and drained bank accounts to full-on ransomware attacks.

While many scams target individuals, SMBs are increasingly in the firing line.

Criminals know that even one employee slipping up can be the weak link.

Tools like this new protection in Edge help to plug those gaps. They use AI to react faster than a human ever could. And that means one less thing to worry about when your team is busy getting real work done.

So, if your business uses Microsoft Edge, make sure you're running the latest version. The new scam protection could save you a lot of trouble and maybe even a few heart-stopping moments.

If you're not sure how well protected your systems are against scams like this, it might be time for a **security audit**.

Our team can help with that – get in touch.