The Most Dangerous Risks in Your Business Don't Swim on the Surface

On the surface, the water looks calm.

That's what makes Shark Week fascinating every year. The danger is never visible on the surface. It’s what’s already moving underneath.

Cybercriminals operate the same way. The threats businesses face right now are designed to blend in with normal operations until the moment something breaks, money moves, or systems go down.

During the summer months, when schedules shift, employees travel, and oversight gets thinner, cybercriminals know businesses are often paying less attention.

Here are three ways they're circling right now.

1. Fake invoices and vendor impersonation

Attackers don’t need to hack anything. In many cases, they need to send just one believable email.

This is called business email compromise (BEC), and it works by impersonating a vendor, supplier, or executive your team already trusts.

The email arrives looking completely normal, someone on your team pays the “vendor,” and by the time anyone realizes the request wasn't legitimate, the damage is done.

These attacks spike during vacation season for a simple reason. When the person who normally approves payments is out, requests get rerouted to people who don't always know what normal looks like. Temporary stand-ins are less likely to question urgency, and attackers know it.

The fix is simple to implement: Build a verification process for any financial request received via email. A quick confirmation call to a known number, not the number listed in the email, is enough to stop most of these before they go anywhere.

2. Phishing attacks that target distracted employees

Phishing works because it’s engineered around how people behave when they’re busy.

Cybercriminals design these moments deliberately. A distracted employee sees a password reset notification and clicks the link. Someone gets a text that looks like it came from IT. An email lands right before a meeting asking for urgent approval on a wire transfer. Nobody stops to verify because stopping feels like losing time.

The most effective protection isn’t a software solution; it’s culture.

Employees need to feel comfortable slowing down when something seems off:

- An unexpected login request

- A payment instruction that came out of nowhere
- A link in an email they weren't expecting

Speed is a weapon attackers use against you. Slowing down is how you take it away from them.

3. Third-party risks that travel fast

When a vendor with access to your systems is compromised, the threat doesn't stay contained to them. It travels directly into your environment through whatever connection they have to your business.

This is supply chain exposure, and most businesses have significantly more of it than they realize. Software tools connected to their network, service providers holding credentials and contractors whose access was never removed after a project ended all present a path that most business owners have never mapped out.

Outsourcing a service doesn't outsource accountability.

Knowing where you stand with supply chain exposure means being able to answer three questions:

1. Which vendors can access your data or systems?
2. What are they connecting to?
3. Who is responsible internally for managing those relationships?

If those answers aren't clear, your exposure is opening you up to risk.

By the time you see it, it's already moving

Sharks don't announce themselves and neither do the cybercriminals targeting your business right now.

The companies that get hit aren't always the ones that ignore obvious warning signs. They're the ones who assume everything is fine because nothing looks wrong.

Summer is when schedules get loose, attention drifts and the water looks the calmest. It's also when attackers are most active.

We help businesses get a clear picture of where they're exposed across vendors, employee activity and day-to-day operations before something goes wrong.

If you don't know where your business stands, schedule a **15-minute discovery call** at https://calendly.com/tritter-kdatechsolutions. Or call us at 717-912-4796 Ext. 202 or visit www.kdatechsolutions.com.