PKF O'CONNOR DAVIES
ACCOUNTANTS AND ADVISORS

The Iran Conflict May Be Overseas. The Cyber Disruption May Not Be.

By Thomas DeMayo, Partner

You don't know what you don't know.

And in cybersecurity, that's not a figure of speech. It's where almost every serious incident begins.

This matters right now for CEOs trying to understand their real exposure, for boards asking whether the organization is truly prepared and for IT and security teams who know where the gaps are but haven't always had the platform to say so. Because with tensions involving Iran escalating and cyber activity rising with it, the question isn't whether the threat is real. It's whether your organization is ready for it.

Think about how your business actually runs. Whether your critical systems live on-premise, in the cloud or spread across a mix of software as a service (SaaS) platforms and third-party vendors, the risk picture extends well beyond your own four walls. And most organizations have never fully mapped what that looks like end to end.

Then something goes wrong. The call comes in. And in that first hour, the most common thing we hear isn't panic. It's disbelief. "We thought we had that covered."

Stryker is a good example of why that matters. A global medical technology company confirmed a cyberattack that knocked out parts of its worldwide network this week. A group with ties to Iran took credit. The detail that stands out isn't the who. It's the what. A company most people would never put on a geopolitical target list, disrupted because they were reachable.

That's the moment we're in right now.

The Motive Has Changed. That Changes Everything.

Most cyber threats have a financial motive. There's a negotiation. Life hopefully goes on.

When the motive is disruption, there's no negotiation. No path to resolution. Just the outage, the confusion and a leadership team scrambling to respond while customers are watching. Iranian-affiliated groups have run this playbook before and the current environment has elevated the risk it gets run again.

This is a different kind of threat than most organizations have been planning for.

Ask Yourself the Harder Questions

Most of us start by asking whether we're a target. That's a reasonable question. But in our experience, the organizations that fare best aren't necessarily the least exposed. They're the ones that were most prepared.

The questions worth asking right now go a little deeper than that. Most organizations we talk to haven't fully stress tested what happens if a critical application goes offline, if remote access fails or if leadership is suddenly making decisions under pressure with incomplete information and customers watching. Not because they don't care, but because there's never been a reason to stop and ask until now.

In the unfortunate circumstances when we do get called in after something goes wrong, what we find is almost never a sophisticated failure. It's usually something that was on someone's list but never quite made it to the top. Vendor access that hadn't been reviewed in a while. A system that needed attention. A backup everyone assumed was working.

Three Things That Actually Matter Right Now

- **Know what's exposed, including what you don't directly control.** Whether you run on-premise, in the cloud or rely on SaaS platforms for core operations, your attack surface includes every vendor and third party connected to your environment. Don't assume your providers are protected just because the application is hosted somewhere else. Iranian actors go after accessible targets, not impressive ones. Know what's reachable across your entire ecosystem and who's actually responsible for securing it.

- **Know who has access to what.** When access gets compromised, operations stop. Revenue stops. And the hardest part is that most leadership teams genuinely don't know what's out there until someone maps it. Who can get in, from where, with what level of privilege, across your own systems and your key vendors. What we find almost never matches what leadership assumed was in place. Multifactor authentication, privileged access, unusual login activity. Get someone to map it honestly and with objectivity. You may be surprised what you find.

- **Know if you can actually recover.** Everyone has a plan. Not everyone has tested it. And remember, recovery isn't just about your own systems. If a critical SaaS platform or third-party application goes down, whether because they were hit or you were hit through them, can your business keep running? Do you know who to call and what your options are? That dependency is part of your recovery plan whether you've written it in or not.

The Best Response Isn't Alarm. It's Calm Readiness.

And the difference between the two is preparation.

For boards, that means asking hard questions about resilience, not just compliance. For management, it means knowing who's in charge when something escalates and how decisions get made under pressure. For IT and security teams, it means having the authority to move quickly when conditions change, not waiting for approvals that cost critical hours.

The organizations that come through moments like this aren't always the most sophisticated. They're the ones that already knew where their gaps were.

Close the ones you know about. Surface the ones you don't. Because when something does happen, and in this environment for some organizations it will, the difference between a contained incident and a full crisis comes down to one thing.

What you knew before it started.

Contact Us

Helping you know what you don't know before it matters is our core mission. Not to show up after something goes wrong, but to help make sure our clients are never caught off guard in the first place. That's not just a service we provide, it's the responsibility we take seriously as your advisors.

If you have questions or want a straight conversation about where your organization stands, please contact your PKF O'Connor Davies client service team or either of the Cybersecurity and Privacy Advisory team members below:

Nick DeLena, CISSP, CISA, CRISC, CDPSE,
CMMC-CCA
Partner
ndelena@pkfod.com | 781.937.5191

Thomas J. DeMayo, CISSP, CISA, CRISC, CIPP
Partner
tdemayo@pkfod.com | 646.449.6353

This article was originally published on March 12, 2026.

PKF O'Connor Davies provides the information in this e-newsletter for general guidance only and it does not constitute the provision of legal advice, tax advice, accounting services, or professional consulting of any kind.