THE BIGGEST LESSONS FROM TODAY'S SUPPLY CHAIN CYBERATTACKS

01 TRUST IS NO LONGER A SECURITY CONTROL

Organizations give trusted vendors access to systems, data, and infrastructure. Attackers increasingly use that trust as an entry point.

Key Takeaway: Treat every third party as a potential attack path—not an automatically trusted partner.

02 A VENDOR BREACH CAN BECOME YOUR BREACH

Even a well-secured supplier can be compromised. If that supplier connects to your environment, its breach can quickly become your risk.

Key Takeaway: Don't just ask who you trust. Ask **what happens if that trust is compromised.**

03 YOUR SUPPLY CHAIN IS BIGGER THAN YOUR VENDORS

Your vendors may depend on their own suppliers, SaaS providers, subcontractors, and technology partners—creating layers of interconnected risk.

Key Takeaway: Look beyond Tier 1 vendors and understand your **extended and fourth-party ecosystem.**

04 POINT-IN-TIME ASSESSMENTS AREN'T ENOUGH

A vendor that passed an assessment six months ago may have changed its technology, operations, ownership, or security posture since then.

Key Takeaway: Shift from periodic assessments to **continuous third-party risk visibility.**

05 THE SOFTWARE SUPPLY CHAIN IS AN ATTACK SURFACE

Open-source components, APIs, software updates, development pipelines, and managed services can introduce vulnerabilities into otherwise trusted environments.

Key Takeaway: Secure the **entire software supply chain**—not just your internal applications.