Why Security Advisory Services Are Surging

Security challenges today aren't coming from just one place—they're being shaped by several forces at once. That growing pressure is driving organizations to seek out security advisory services for expert guidance to assess risk, prioritize what matters, and strengthen their overall strategy.

What Cybersecurity Metrics Reveal Today:

83%
Of organizations experienced more than one data breach in the past year
(IBM Cost of a Data Breach Report)

75%
Of organizations say their attack surface is expanding faster than they can secure it
(Palo Alto Network / Cortex Xpanse Report)

65%
Of organizations say regulatory requirements are their top driver for cybersecuity investment
(PwC Global Digital Trust Insights Report)

3 Forces Driving Demand for Security Advisory

Threats Are Getting Smarter

Ransomware-as-a-service, AI-driven phishing, and supply chain attacks are increasing in scale, speed, and impact.

Environments Are Getting More Complex

Cloud, SaaS, hybrid work, and unmanaged devices are expanding the attack surface and reducing visibility.

Accountability Is Getting Stricter

New regulations, cyber insurance requirements, and board-level scrutiny are increasing security obligations, liability, and executive accountability.

3 Gaps We're Seeing Across Security Advisory Engagements

Based on nearly 80 security advisory engagements completed over the past year, TPx advisors are seeing consistent gaps in how organizations approach security—gaps that make it harder to manage risk and move forward with confidence.

Undefined Frameworks

Many organizations don't follow a clear security framework, making it harder to prioritize risks and align investments to what matters most.

Gaps in Expertise

Internal teams often don't have the certified expertise needed to effectively manage threats and keep up with evolving risks.

Shallow Penetration Testing

Penetration testing is often treated as a compliance exercise, leaving real-world attack paths untested and creating a false sense of security.

Key Takeaway

As cybersecurity complexity evolves, gaps in strategy, expertise, and execution are leaving organizations more exposed. Addressing these gaps is critical to reducing risk and making smarter security decisions—and security advisory services provide the clarity needed to prioritize what matters and build a stronger, more resilient strategy.