Hey! What's New? 2026-38

What Cybersecurity Signals About Your Business

According to an article by Michael Paull in *CFO*, "Cybersecurity reviews are now integral to sales and vendor diligence, with operational trust and preparedness evolving from IT concerns into critical finance and leadership priorities."

When responding to a prospect's RFP, there will very likely be a section on cybersecurity, Paull says. "Certain controls should now be considered table stakes, but depth and operational maturity increasingly differentiate vendors. Prospects are not simply evaluating whether controls exist. They are evaluating whether your company operates with discipline, accountability and preparedness. Strong internal policies, frequent updates and executive oversight, preferably from a chief compliance officer, all help reinforce that confidence."

He points out that "an RFP will generally include a section on cyber insurance and the commonly requested certificate of insurance. It is important to make sure that your coverage is adequate. Adequate cyber liability coverage has become an expected part of vendor diligence."

Current clients and their auditors, he says, "will also be inquiring about system and organization controls audits. SOC audits have become standard diligence requests for critical vendors and service providers. These requests are now less about checking a compliance box and more about validating operational trustworthiness."

In many cases, Paull says, "cybersecurity reviews now occur well before pricing, implementation discussions or contract negotiations. A slow, incomplete or disorganized response can create uncertainty long before product functionality or service quality are fully evaluated. Operational trust has become part of competitive positioning. Prospects are asking earlier in the process and with greater specificity. In many situations, they are repeating questions driven by their own auditors, procurement teams, compliance requirements or internal risk reviews."

Often, the prospect may not fully understand the technical details behind the request, Paull continues. "They simply know they are expected to ask the question and document the response. Cybersecurity expectations are increasingly cascading through vendor ecosystems as companies respond to pressure from auditors, customers, regulators and vendor risk management programs."

Consider how businesses now evaluate critical software providers, he suggests. "Whether it's a payroll platform, ERP system, CRM solution or accounting software vendor, prospects increasingly expect detailed responses around cybersecurity, business continuity, insurance coverage and operational resilience before signing an agreement."

According to Paull, "companies are now being evaluated not simply on product quality, pricing or service capability, but on operational trustworthiness, including their ability to safeguard information, maintain continuity, respond under pressure and operate with discipline. Cybersecurity has become one of the clearest and most measurable indicators of that trust."

Prospects may not fully understand the technical nuances behind every policy, audit or continuity procedure, he writes. "What they do understand is what those items represent: preparedness, accountability, governance and operational maturity. Companies that respond

quickly with organized documentation, clear ownership and tested continuity plans reduce uncertainty in the buying process. Companies that struggle to answer basic diligence questions may unintentionally signal broader concerns about responsiveness, leadership oversight, and operational discipline. Cybersecurity preparedness is being interpreted as visible evidence of how well a company is managed overall."

The strongest companies tend to treat cybersecurity diligence materials the same way they treat financial statements, contracts, or investor materials: organized, timely, accurate and ready to provide quickly, Paull says. "The goal is not merely compliance. The goal is to reduce uncertainty and accelerate trust."

"Responsiveness itself becomes part of the evaluation. Companies that can confidently articulate their controls, continuity planning, governance structure and incident preparedness often create confidence beyond cybersecurity itself. Well-run companies reduce uncertainty. Poorly prepared companies introduce it."

Paull stresses that "companies are no longer evaluated solely on the quality of their products or services. They are also being evaluated on whether they appear capable of operating reliably under pressure, protecting sensitive information and responding effectively to disruption."

Learn a whole lot more at What cybersecurity signals about your business | CFO.com.