What makes the IT supply chain so complex and vulnerable?
The IT supply chain encompasses the manufacture, transport, storage, delivery and installation of hardware and software components that make up an end-user product or service that enables digital operations. Every component may have multiple subcomponents from multiple vendors in multiple countries, which creates tremendous depth, complexity and risk. Even if an organization uses the typical arsenal of security controls, it may inherit vulnerabilities from one of these third-party components. That’s why it’s so important to know your vendors and how they ensure the origin and integrity of components in their own supply chains.

What business and IT challenges interfere with the delivery and maintenance of a secure IT supply chain?
One issue is organizations don’t use the latest cybersecurity protections on their laptops, printers and other endpoints, which is increasingly important as workforces move to hybrid work. In addition, most organizations don’t invest the time or money to know the vendors that assemble or provide their products. They don’t have a clear picture of their suppliers’ financial stability, how they screen workers, who else they do business with, where their components come from and so on. Finally, they don’t independently verify that suppliers are doing what they say they’re doing in terms of a secure IT supply chain.

How can state and local governments use CISA, NIST and other federal guidelines as a starting point to securely managing their IT supply chain?
Governmental bodies and industry working groups bring to bear significant expertise and focus on these issues. Although not required by federal law to do so, states and local governments can — and should — adapt federal models and recommendations to strengthen their risk posture. The CISA Information and Communications Technology Supply Chain Risk Management Task Force publishes very useful guidance on assessing and managing risk in IT supply chains. The NIST 800 series is also an important reference, as is the Cyber Maturity Model Compliance (CMMC) framework, which can be used to verify whether IT vendors have used appropriate cybersecurity controls and best practices in developing their products.

How can organizations strengthen IT supply chain security in their existing environment?
One of the most important steps is modernizing endpoints and legacy systems, and then regularly updating them. Today’s devices often have built-in or pre-installed security functions that operate in the background and don’t impact the user experience or performance. For example, advanced enterprise printers automatically detect and self-heal from malware, and top-of-the-line laptops and workstations automatically isolate and contain emails, websites or files from untrusted sources. Then of course, there are also all the usual network controls such as multifactor authentication, encryption and Zero Trust access control.