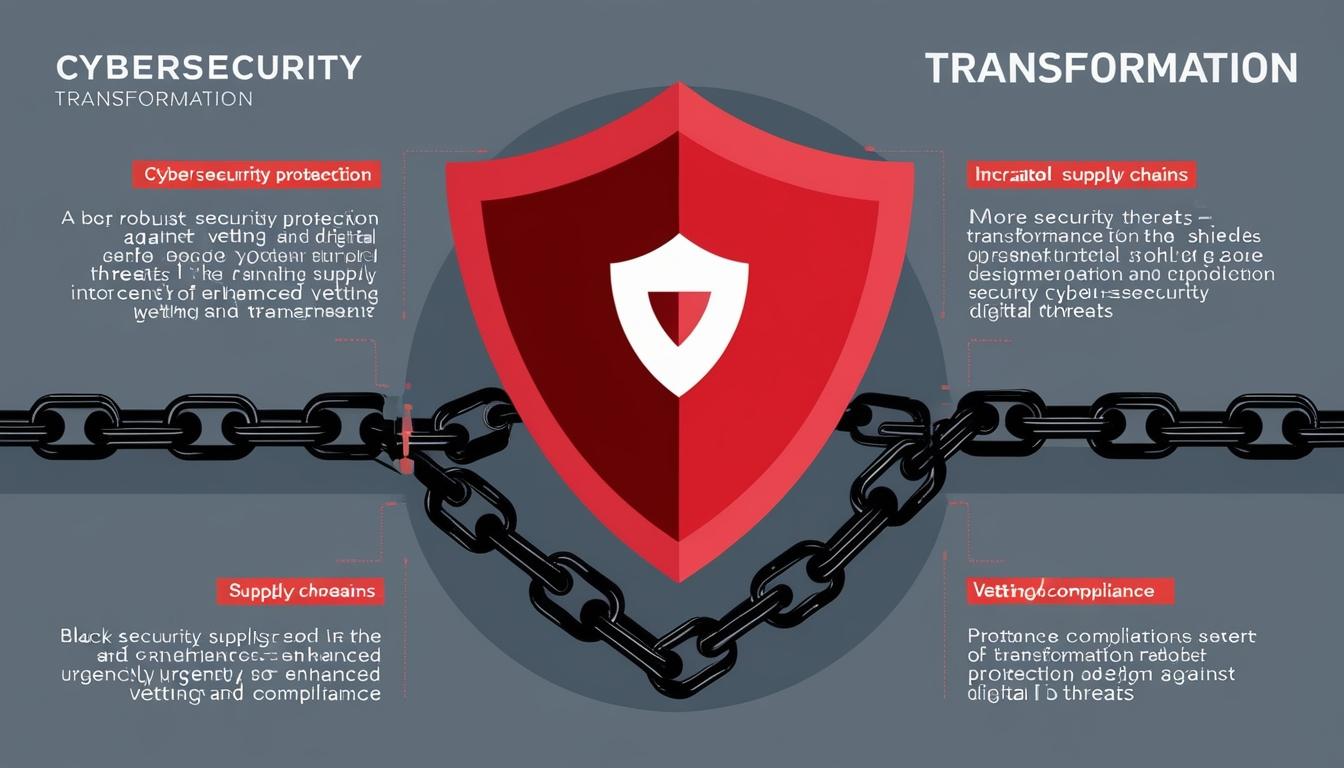
# Predictions for cybersecurity: A shift towards supply chain risk management



Edward Tuorinsky, the CEO of DTS, has made a significant prediction regarding the future of cybersecurity within U.S. businesses, suggesting that 2025 will mark a pivotal shift towards enhanced focus on cybersecurity supply chain risk management (C-SCRM). This forecast comes amid growing compliance requirements and an urgent need to secure data connections against potential cyber threats.

In his delineation of the cybersecurity landscape for the coming years, Tuorinsky likens the complexities of managing cybersecurity risks to a party game where miscommunication leads to increasingly convoluted outcomes, although in this context, the repercussions of a data breach are potentially disastrous. The essence of his prediction is that businesses must assess and manage the cybersecurity risks posed by all partners with whom they share data. He articulated that “bad actors target easy marks” — often small or inadequately protected companies that are looped into larger corporate ecosystems, underscoring the vital importance of thorough vetting of partners and suppliers.

A notable impetus for these changes is the recent implementation of the Cybersecurity Maturity Model Certification (CMMC) by the U.S. Department of Defense (DoD). This initiative mandates that its over 200,000 contractors adhere to stringent cybersecurity protocols, which will subsequently cascade downwards. As Tuorinsky observes, while the U.S. has more than 33 million businesses, thousands of subcontractors, vendors, and suppliers aligned with DoD contractors will be compelled to demonstrate their own security compliance. This development will lead to millions of businesses needing to meet new cybersecurity standards and furnish evidence of compliance, signalling a significant industry-wide transformation.

Tuorinsky predicts a behavioural shift among companies that have historically been hesitant to sever relationships with partners or suppliers due to cybersecurity concerns. He acknowledges that “the potential risks associated with cybersecurity are a strong motivator for change,” stating that enhanced vetting processes represent one of the most cost-effective strategies for strengthening cybersecurity. This emphasis on supply chain security is seen as instrumental in fortifying the broader cyber ecosystem.

There is a growing recognition among companies that cybersecurity must be treated as a fundamental business concern rather than merely a technical issue. Tuorinsky points to the adoption of a zero-trust approach, which operates under the assumption that all connections and users are untrustworthy until proven otherwise. In this environment, businesses will increasingly require their partners, suppliers, and vendors to provide documentation and certifications that attest to the robustness of their cybersecurity controls.

While Tuorinsky anticipates increased scrutiny and potentially even publicised “breakups” among companies unable to meet these new documentation and standards, he argues that cybersecurity will dominate discussions across the technology sector and beyond. The evolution of compliance requirements, particularly those initially driven by federal contractors, will eventually permeate other facets of U.S. businesses, influencing even the smallest enterprises that engage in electronic transactions or maintain an online presence.

By addressing these emerging trends and pressures, U.S. businesses are likely to view securing their supply chains as not just a precautionary measure but an essential progression in navigating an increasingly digital and interconnected world. As cybersecurity continues to evolve, its implications for business practices promise to reshape the operational landscape in the years to come, fundamentally altering how companies assess and manage risk in their networks and relationships.

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://www.intelligentcxo.com/2025/01/07/editors-question-what-challenges-and-growth-opportunities-do-you-predict-for-businesses-in-2025/> - This article supports Edward Tuorinsky's prediction on the importance of cybersecurity supply chain risk management (C-SCRM) and the impact of the Cybersecurity Maturity Model Certification (CMMC) on U.S. businesses.
2. <https://www.intelligentcxo.com/2025/01/07/editors-question-what-challenges-and-growth-opportunities-do-you-predict-for-businesses-in-2025/> - It explains how bad actors target vulnerable companies and the need for thorough vetting of partners and suppliers to manage cybersecurity risks.
3. <https://www.youtube.com/watch?v=gj8Po3oMr0M> - This video discusses how to assess and manage the cybersecurity risk of partners with whom you share data connections, aligning with Tuorinsky's views on C-SCRM.
4. <https://www.securitymagazine.com/blogs/14-security-blog/post/100945-small-businesses-need-to-secure-data-before-tapping-into-ai> - The article emphasizes the importance of data security and cybersecurity compliance, especially for small businesses, which is in line with Tuorinsky's predictions.
5. <https://www.prweb.com/releases/dts-industry-experts-share-2023-predictions-offer-insight-into-cybersecurity-leadership-operations-human-capital-training-technology-and-transformation-840708085.html> - This press release details the Cybersecurity Maturity Model Certification (CMMC) and its implications for businesses, supporting Tuorinsky's points on compliance and security standards.
6. <https://www.prweb.com/releases/dts-industry-experts-share-2023-predictions-offer-insight-into-cybersecurity-leadership-operations-human-capital-training-technology-and-transformation-840708085.html> - It highlights the need for businesses to achieve CMMC compliance and the cascading effect on subcontractors, vendors, and suppliers.
7. <https://www.intelligentcxo.com/2025/01/07/editors-question-what-challenges-and-growth-opportunities-do-you-predict-for-businesses-in-2025/> - The article discusses the behavioral shift among companies towards enhanced vetting processes due to cybersecurity concerns, as predicted by Tuorinsky.
8. <https://www.intelligentcxo.com/2025/01/07/editors-question-what-challenges-and-growth-opportunities-do-you-predict-for-businesses-in-2025/> - It explains the adoption of a zero-trust approach and the requirement for partners and suppliers to provide documentation and certifications for their cybersecurity controls.
9. <https://www.securitymagazine.com/blogs/14-security-blog/post/100945-small-businesses-need-to-secure-data-before-tapping-into-ai> - The article underscores the importance of treating cybersecurity as a fundamental business concern rather than just a technical issue, aligning with Tuorinsky's views.
10. <https://www.prweb.com/releases/dts-industry-experts-share-2023-predictions-offer-insight-into-cybersecurity-leadership-operations-human-capital-training-technology-and-transformation-840708085.html> - It discusses the broader impact of evolving compliance requirements on U.S. businesses, including the smallest enterprises engaging in electronic transactions or maintaining an online presence.
11. <https://www.intelligentcxo.com/2025/01/07/editors-question-what-challenges-and-growth-opportunities-do-you-predict-for-businesses-in-2025/> - The article highlights the future implications of cybersecurity trends on business practices, reshaping the operational landscape and altering how companies assess and manage risk.
12. <https://appdevelopermagazine.com/Cybersecurity-supply-chain-risk-management-predictions-for-2025/> - Please view link - unable to able to access data