

Cybersecurity Risk Management Simplified

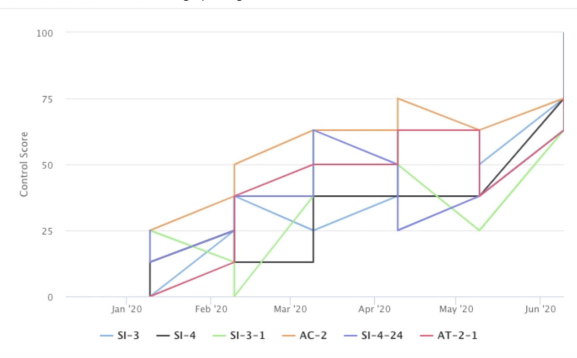
Our daily life is full of change, and even more so in offices and places of work as businesses grow, markets shift, and leadership responds to those forces. With these regular changes come even more impactful changes in cybersecurity risk, which has proven to increase dramatically as digital transformation initiatives take place, making the plethora of risks that could impact any individual organization difficult to manage. Across the enterprise, risk becomes even more elusive as the risks of commonalities such as partnerships, new product lines, and remote employees become the responsibility of the organization's cybersecurity and risk management programs.

Standardizing cybersecurity risk management on CyberStrong allows organizations to keep track of not just how many risks they have, but also how each risk impacts business growth. C-Suite leaders responsible for cybersecurity risk avoid being caught in ignorance by managing risks proactively and are ready to offer measured solutions to executives at any time. Risk teams have the opportunity to let their expertise shine by automating previously manual processes and tying the impact of their work to the organizational objectives that their leadership cares about. The risk management program is streamlined, collaborative, and responsive supported by an intuitive platform that empowers agile, impactful work. These are only a few of the advantages organizations experience when utilizing a platform that facilitates a truly integrated approach.

Identify, track, and mitigate risks proactively, protecting critical assets and demonstrating tangible value.

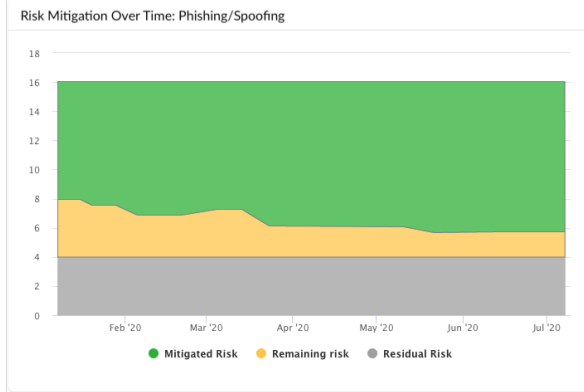
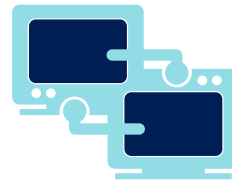
With CyberStrong, risk managers are confident they can respond to risks in a timely manner, giving them pride in their work and the ability to showcase their expertise with unprecedented accuracy. Risk leaders can speak to executive teams while confidently knowing where the organization's cybersecurity program stands against the most critical and important risks. CyberStrong is the single source of truth that allows teams to swiftly update risk mitigation actions, events, and priorities while aligning those activities to management objectives and overarching company goals.

Controls Related To Risk: Phishing/Spoofing



Quickly respond to questions about how risk is trending across segments of the organization, showcasing the risk management team's ability to act with intelligence and precision.

By leveraging CyberStrong's unmatched visibility into cybersecurity risk, risk leaders are able to shine in their role as an expert and problem-solver both in front of their teams and in the boardroom. CROs, CIOs, and CISOs are empowered by informed risk management decision making and are able to offer solutions quickly and effectively based on the most relevant and up-to-date information.



Serve up annualized solution-based plans that present the cost and impact of your risk management program on the bottom line.

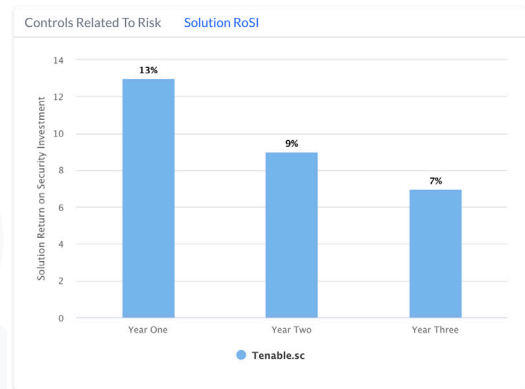
- Create more support around risk management efforts and give risk teams the mandate to do purposeful work that key stakeholders truly value. With CyberStrong, the impact of the cybersecurity risk management program can be communicated in a way that risk managers and teams can act on while also being more deeply understood by non-technical leadership. This strategic alignment across departments and hierarchy inherently gives program leaders more autonomy and support from their peers and management.

“When we saw the CyberStrong platform capabilities we were convinced it was what we needed to manage our integrated risk management strategy.”

Bruce Forman, CISO, UMass Memorial Health Care

Manage executive expectations for risk reduction, and illustrate decreased cybersecurity risk over time; whether transferred, accepted or managed, while eliminating duplicate efforts across program functions.

- Exceed risk reduction expectations of executive leadership by unifying efforts across risk, compliance, audit, and governance on a single system of record. Visualize improved posture for review and link results to mitigation actions across compliance controls, optimizing the performance of multiple functions for greater efficiency and enhanced resilience.



Create tribal knowledge of risk management across departments by leveraging measurement that all stakeholders clearly understand.

Track Key Risk Indicators (KRIs) and report on how each risk impacts the organization in dollars and cents, probability and to act fast and protect business growth.

- FAIR, NIST SP 800-30, and other unique risk measurement methodologies.
- Return on Security Investment tracking and reporting.