# 2021 Industry Cyber-Exposure Report (ICER): FTSE 350 Recommendations at a Glance

In the 2021 Industry Cyber-Exposure Report (ICER): FTSE 350, Rapid7 researchers identified five areas that FTSE 350 CISOs in the FTSE 350 can do, today, to reduce their exposure to the most common issues associated with internet exposure and risk. For more background and findings on these and other areas of cybersecurity, please see Rapid7's research work at https://www.rapid7.com/research/.

**Email Security:** If you're on the Domain-based Message Authentication, Reporting & Conformance (DMARC) path, like 75% of the FTSE 350, that's great! Now is the time to plan out how you'll move from a p=none to a p=quarantine policy, and ultimately a p=reject policy. This is not an easy journey, since you will certainly uncover pockets of shadow IT running their own email infrastructure, but the confidence of being able to authenticate mail from your major brand domains is a pretty great feeling, and a nice item to report to your board of directors.

**Web Security:** HTTP Strict Transport Security (HSTS) is rapidly becoming table stakes for running a reasonably secure website, and this is the kind of security feature that browser manufacturers like Google, Apple, Microsoft, and Mozilla are likely to enforce in future versions of Chrome, Safari, Edge, and Firefox. It's a relatively easy switch that CISOs can flick (compared to the universe of nice-to-haves in cybersecurity, anyway), so take some time to investigate whether your organization is using HSTS and if not, why.

**Version Dispersion:** For the mega-corporations that roam the fields of capitalism, mergers and acquisitions are a fairly common activity throughout the year. That means the FTSE 350 CISO is never truly "done" with ensuring version consistency across the enterprise, even after investing in an excellent asset and vulnerability management toolchain. New networks and network services will join your ranks, and that means undertaking a fairly continuous modernization and normalization effort for those new assets. Taking on this continuous effort will pay off in easier, more straightforward planning for the next patch cycle, scheduled or surprise.

**High-Risk Services:** Telnet, SMB, and RDP have no business being exposed directly to the world at large, and are just waiting for the next self-replicating cyberattack to sweep across the internet. An up-to-date inventory of exposed services, sourced from internal and external scanning, is worth its virtual weight in Bitcoin, and will help you enforce a no-nonsense policy of network service exposure to the internet.

**Vulnerability Disclosure Programs:** As a CISO, you might have hired on the best of the best software, QA, and platform engineers. But, without a good way to harness the smarts of the tens of thousands of talented hackers around the world, you may never learn about the most critical vulnerabilities in your products and services. A VDP is a bridge to that enormous community of well-meaning investigators who have goals aligned with your own: a safer and more secure internet. Getting that program spun up now will give you plenty of time to practice safer software production. As a bonus, most of the pioneering work is already done for you, in the form of ISO 29147 and ISO 30111.

To learn more about these five areas of cybersecurity, check out our 2021 Industry Cyber-Exposure Report (ICER): FTSE 350: http://rapid7.com/2021-ICER-UK