Cybersecurity

Craft Industry Report: Cybersecurity Scores & Analysis by Industry

Share

Analyzing cybersecurity health by company, sector and size is a critical yet often overlooked aspect of holistic risk assessment and mitigation. After all, ransomware attacks have increased by almost 300% within 2021, and overall supply chain attacks spiked by nearly 50% as well. While this has created a justifiably heightened

interest among companies to shore up their cybersecurity across the board, industries still vary in their cybersecurity health. For example, with robust legislation such as HIPAA, the healthcare industry is heavily regulated and sees more investment in privacy and protection than the hospitality industry. This means that organizations should take into account more precise data when establishing and measuring against industry benchmarks.

Analysis & Methodology

Using a combination of Craft's data ecosystem and innovative machine learning models, cybersecurity scores were compiled, organized by industry, and analyzed on how well they fare compared to other industries. More specifically, the analysis used percentiles to clearly demarcate the proportion of scores that fell below a particular score (the higher the score, the better the industry's cybersecurity health with 100 being the best).

Findings: Best & Worst Performing Industries

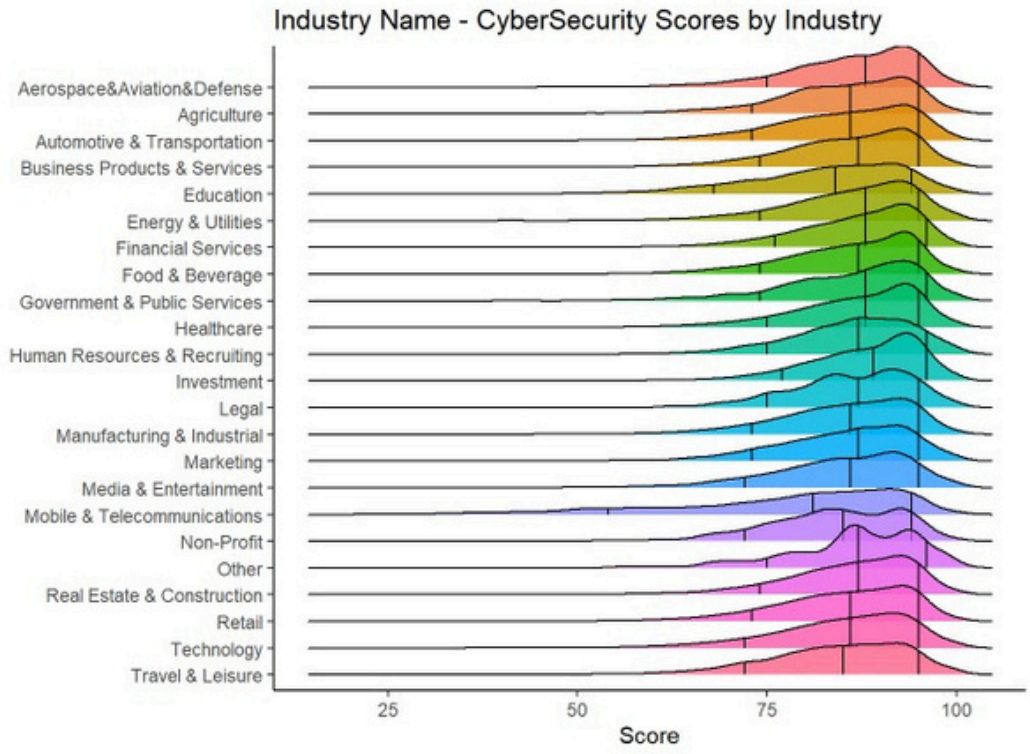
Best Performing

The best performing industries are Financial Services and Investment, as they both have a higher value in the lower percentile than the average value. Specifically, financial service companies in the top 10th percentile have a cybersecurity score of 76 or higher, compared with 73 on average. For firms in the top 10th percentile within the investment industry, scores were 77 or higher.

Worst Performing

As far as the worst performing industries, telecommunications and education firms showed the lowest scores in the analysis. The tenth percentile score for the former is 53 and 69 for the latter, and with an average score of 73 across all industries, it's clear that these two sectors could use work towards strengthening their cybersecurity infrastructure. In other words, the vast majority of telecommunications

companies – 90% to be exact – have a score less than 53. For the education sector, most scores are lower than 69.



Why Financial Services & Investment Industries Have Better Cybersecurity Health

From various disclosure rules to cybersecurity standards, financial services are a notoriously regulated industry both within the US and Europe. Due to the sensitive information stored during financial transactions, places like the EU have created a framework and compliance policy known as the General Data Protection Regulation (GDPR), which has also been used as a framework for other personal data protection rules in other countries, including the US. And because of the international nature of financial services, and particularly within the investment sector, GDPR compliance often ends up being a requirement, even if company headquarters are located outside of Europe. Hence, even if one country does not pass robust cybersecurity legislation, industries that are international in nature often end up having to comply with stricter countries as well.

Other frameworks heavily advised and adopted by financial institutions include the ISO/IEC 27001 and for the US, the National Institute of Standards and Technology (NIST). The Sarbanes-Oxley Act of 2002 is a robust piece of American legislation that not only advises but requires certain cybersecurity measures and aims to prevent

investors from financial scams. The impetus for some of these stronger standards have come directly from real-world examples of financial fraud or hacks, such as the tech firm Ubiquiti's 2015 cyberheist in which $47 million were stolen.

More recently, the Securities & Exchange Commission (SEC) and the New York Department of Financial Services (NYFDS) proposed new cybersecurity rules in July, which includes a mandated notification for cyber ransom payments within 24 hours, annual cybersecurity audits conducted by an independent party, and higher expectations placed on the board for security expertise.

Why Telecommunications & Education Sectors Have Worse Cybersecurity Scores

While the telecommunications sector, like the financial services industry, also contains personally sensitive data attractive to hackers, it lags behind in terms of stricter cybersecurity measures. In 2021, the industry experienced 1,079 attacks weekly per organization, a 51% increase from the previous year. And in the first quarter of 2021, the telecommunication sector was the most targeted industry for distributed denial-of-service (DDoS) attacks, which involves flooding the traffic of a server or network with enough bots to cause a server crash or similarly destructive effects.

While telecom is generally speaking less regulated than financial or healthcare services, the low security scores could also be a testament to the increasing vulnerabilities that have surfaced as 5G networks are still developing and expanding in their infancy stage. For example, 5G carriers typically use numerous levels of spectrum frequencies, resulting in an opportunity for attackers to interrupt certain avenues of communication.

In terms of the education sector's low scores, it appears that multiple factors are at play. The industry typically sees lower levels of investment as a whole, and it's safe to assume that prioritizing investment in cybersecurity in the face of other obstacles the sector faces is not commonplace. Since 2016, there has been a five-fold increase in cyber incidents, with 1,180 occurring within US public schools.

But the COVID-19 pandemic also created an immediate and stark schism between technology demands and capabilities. With a sudden shift towards remote learning for millions of students and teachers, the existing infrastructure – already

compromised in key areas — simply gave way to even more security vulnerabilities as a result of the newly surging demand.

Because personal data — such as social security and phone numbers among others — are stored in educational and school systems, it's become an attractive source of attack for cyber criminals.

Earlier in the year, for example, the EdTech platform Illuminate Education experienced a service shutdown for several weeks due to a cybersecurity incident. The company's tools are used by school districts across the country, including New York's public school system, meaning hundreds of thousands of individuals were impacted.

Other Findings

Overall, Craft's analysis found that smaller companies were more likely to maintain less-than-optimal cybersecurity practices and scores than larger companies. This could be a result of the limited amount of cybersecurity data that small, and often private, companies tend to disclose. It could also be associated with the lower amount of investment and resources that they are able to commit to cybersecurity.

Accurate cybersecurity benchmarks are one of the most important risk domains for firms to measure, but they're not always prioritized when it comes to assessing supply chain risk, market intelligence or competitor analysis. Up-to-date industry data ensures your organization has more precise gauges through which to evaluate your risk mitigation efforts. And employing robust enterprise intelligence platforms that can aggregate and analyze information across a varied set of metrics provides actionable insights not possible through manual searches and surveys alone.