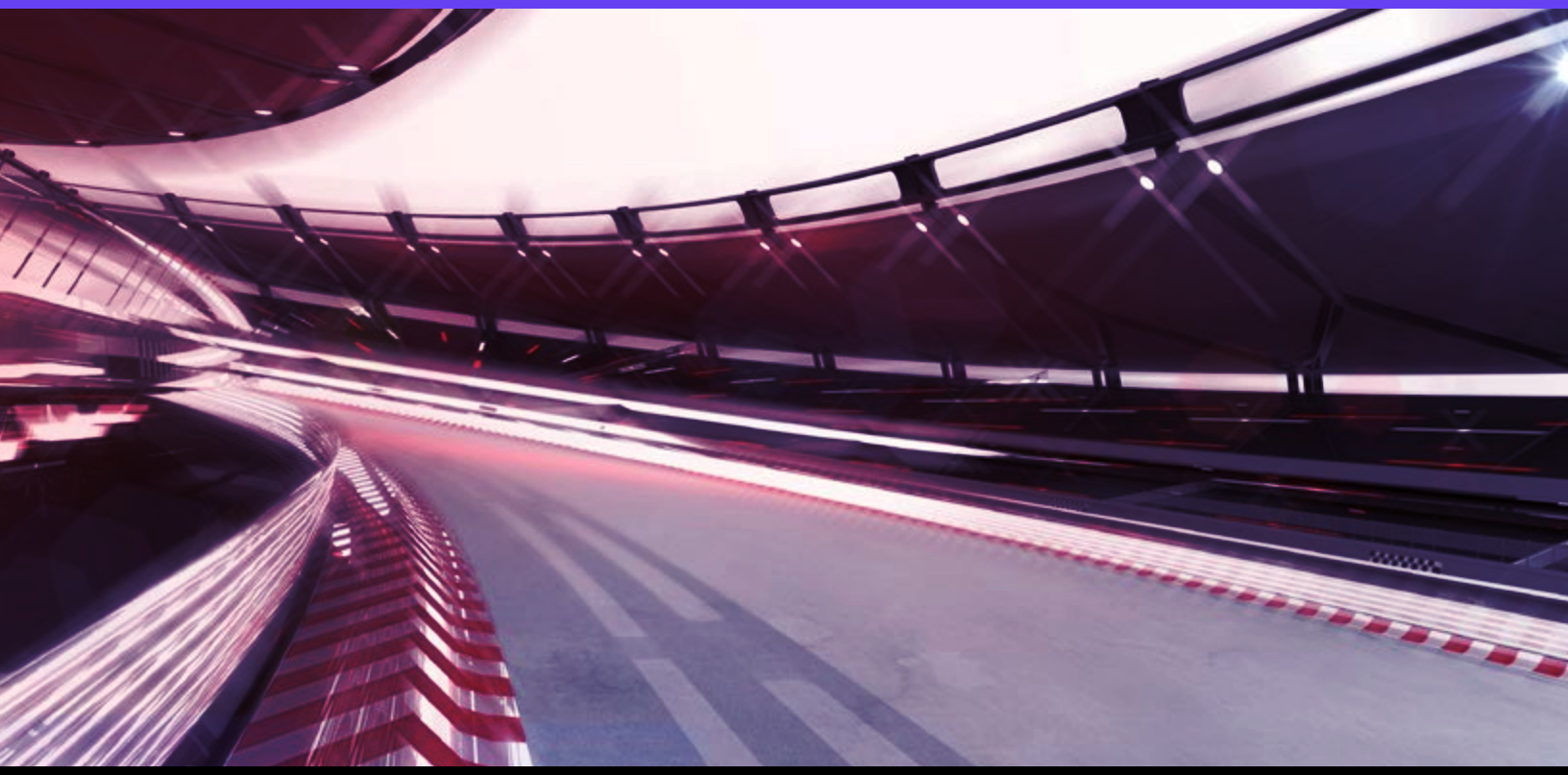
The Fast and the Frivolous

The Financial Industry Sector Snapshot



a collaboration between

SecurityScorecard | Cyentia Institute

The Financial Industry

In our first volume of a new report with SecurityScorecard, "The Fast and the Frivolous," we examine the pacing remediation of Internet-facing vulnerabilities, and how organizations tackle threats that come their way. The data examined in this report looks at vulnerabilities scanned over a three-year period (early 2019 - early 2022) by over 1.6 million organizations. All said and seen, 53% of those 1.6 million organizations had at least one open vulnerability exposed to the Internet, and 22% of them had over 1,000 vulnerabilities each.

So, what happens when we take a deeper look at how organizations in each sector fares?

This snapshot provides a view of pacing remediation in the Financial Services sector. We hope that this brings the findings a little closer to home, so you can better refine your organization's remediation program based on data that is most relevant to you.

In the main report, we noted that the Financial Services industry had the one of the slowest remediation rates, with the median being 426 days.

In Figure 1, we're able to see how organizations in the Financial Services world stack up to those in Healthcare, Manufacturing, and Public.

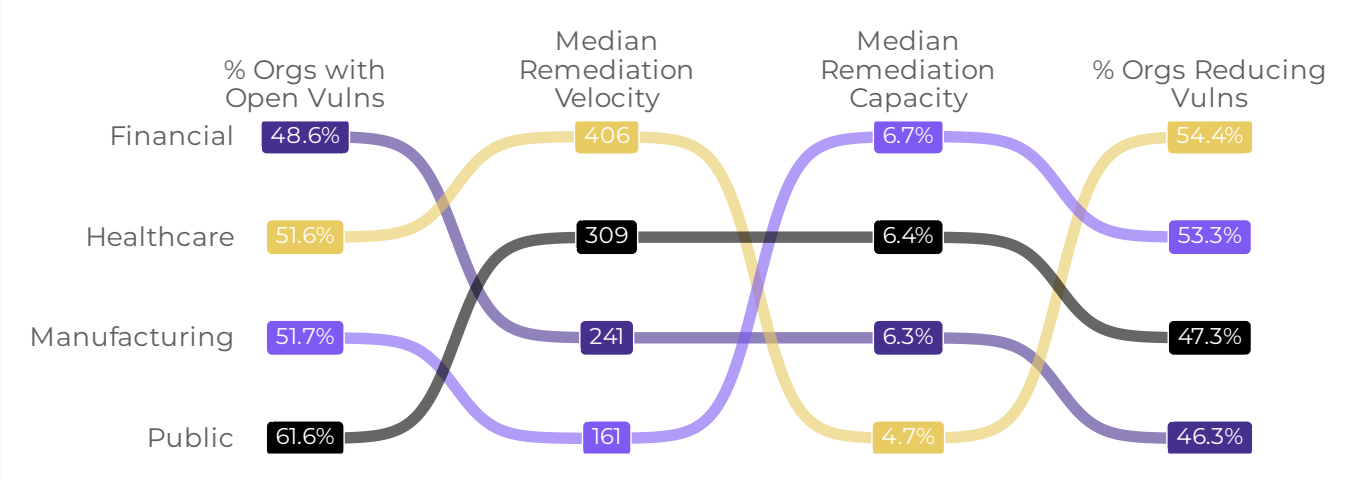


Figure 1

Taking a quick glance here, we can follow each path per industry. In the Finance world, 48.6% of organizations have open vulnerabilities, with a median remediation velocity of 241. Finance also has a 6.3% median remediation capacity (aka, how many are closed per month), but falls behind the pack with just 46.3% of organizations actually reducing vulnerabilities.

To measure the speed at which those vulnerabilities are remediated, we'll use a statistical technique known as survival analysis. In a nutshell, it measures the duration of time to some event of interest. In our case, that's the time required to remediate vulnerabilities. For example, if an organization has 100 open vulnerabilities across its systems and manages to fix 15 of them today, that means 85 vulnerabilities remain open—an 85% survival rate. If they fix 10 the next day, survivability drops to 75%, and so on over time.

So, let's take a deeper look at all the different sub sectors within the financial world, especially when it comes to remediation velocity, in Figure 2.

Comparison of Remediation Velocity

Figure 2

Here in Figure 2, we can see that there is a difference between subsectors: Funds, Trusts, and Other Financial Vehicles have the quickest time of remediation, with the half life being just about 241 days. Insurance Carriers, on the other hand, have a half life of 560 days - a little over a year and a half. What's interesting to note here is the length of time between each marker - quarter life, half life, and three quarters life. When you look at Insurance Carriers for instance, even though it takes 560 days to get to remediation half life, the jump to 75% is just another 100 days. However, when looking at Monetary Authorities, the difference between half life and 75% is 463 days!

There must be some reason to explain the difference between each subsector, whether it's the systems and processes in place, the vulnerabilities faced, or maybe even the amount of bandwidth the teams have. So, let's go ahead and look at the remediation capacity next.

Comparison of Remediation Capacity

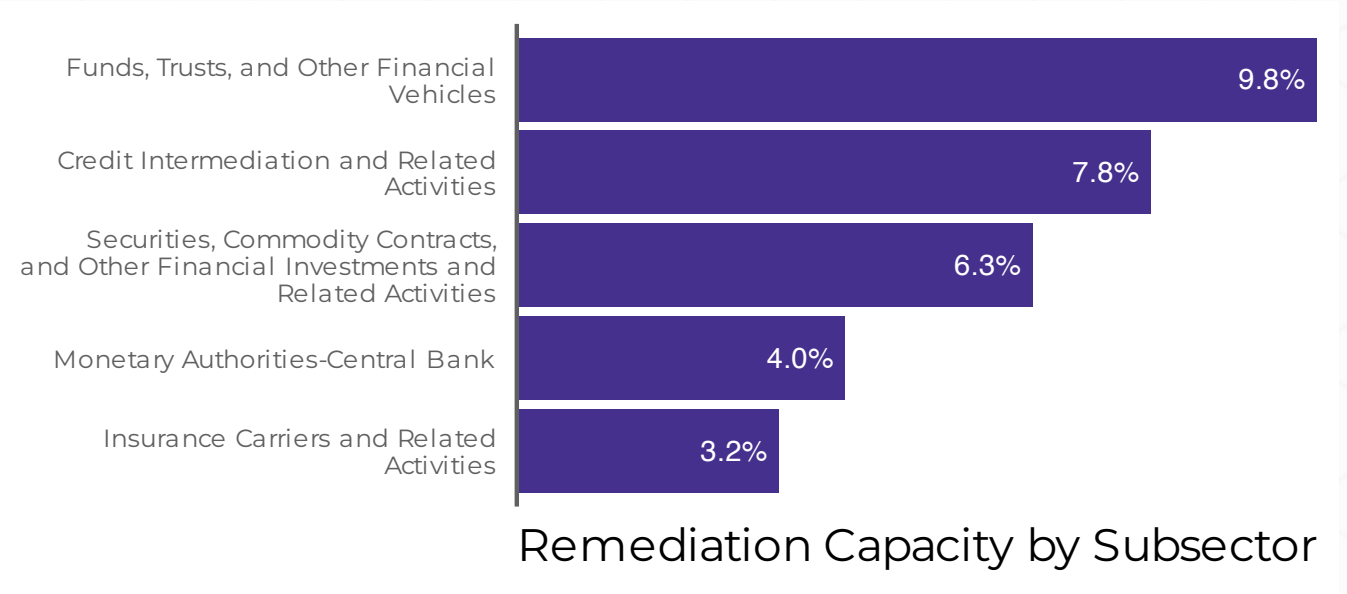


Figure 3

Here in Figure 3, we take a look at the ratio of open to closed vulnerabilities in a given timeframe, also known as remediation capacity. In the main report, we noted that across industries, we saw that organizations generally are able to remediate about 10% of vulnerabilities each month. If we take 10% as our general capacity, then anything below that capacity illustrates that organizations can't keep up with new vulnerabilities and anything above 10% illustrates that organizations are able to close enough vulnerabilities to offset new ones.

Funds, Trusts, and Other Financial Vehicles have the best remediation capacity at 9.8%, while Insurance Carriers and Related Activities are at just 3.2%. When we see this number, along with taking a look back at Figure 2, we can see that it takes almost a year for a vulnerability to hit 25% remediation - which could be an indicator of a sub sector wide pace of remediation. It's important to realize the potential impact that a backlog of vulnerabilities can have on an organization.

So what does that mean in terms of gaining ground on vulnerability management?

Gaining vs Losing in Vulnerability Management

Everyone loves a battle of good versus evil, and the battle of gaining and losing in vulnerability management is almost just as classic. Broken out by the subsector, Monetary Authorities- Central Bank is gaining ground on their vulnerabilities. However, the bottom two, Securities and Insurance Carriers are right around the halfway point - with only a couple percentage difference in either direction.

Taking a moment to zoom out, in the main report, we found that about 4 in 10 organizations are losing ground when it comes to managing their vulnerabilities. In Figure 5, we take a look at financial organizations gaining and losing ground in vulnerability management over time.

Remediation Capacity

Measures the ratio of open vs. closed vulnerabilities over time.

Below capacity indicates that organizations can't keep up with newly discovered vulnerabilities over time.

Above capacity means the program is generally able to close enough vulnerabilities to offset the new ones.

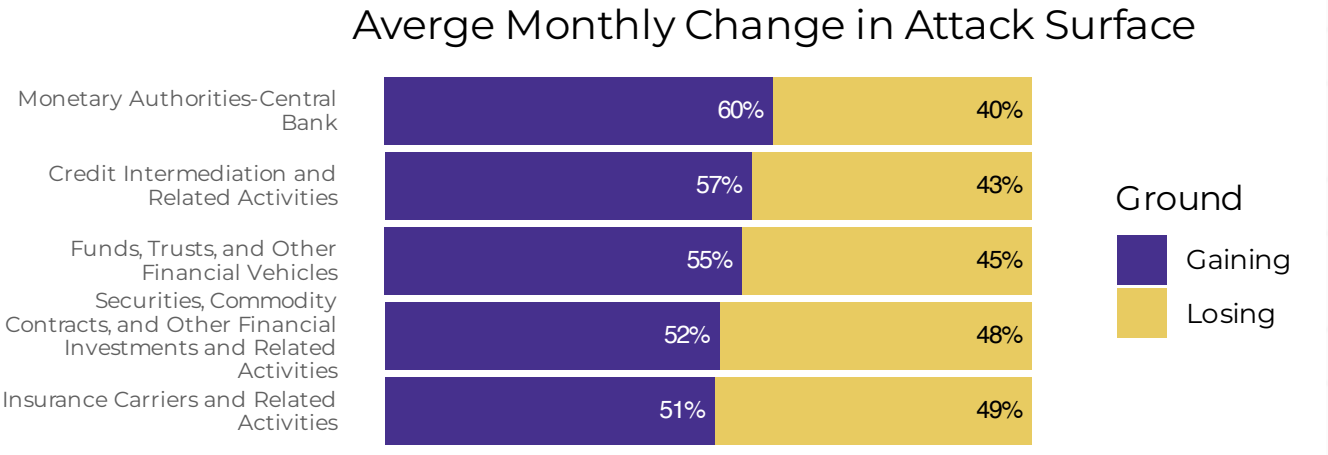


Figure 4

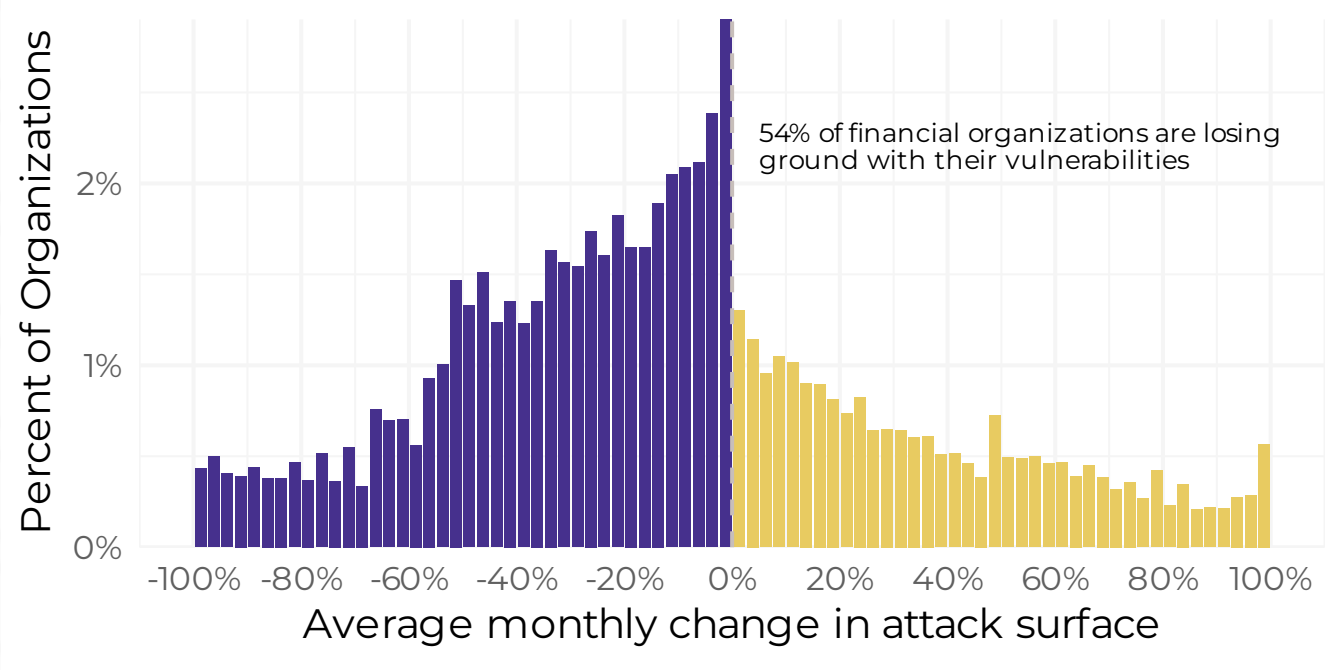


Figure 5

We can see that 54% of financial organizations are actually losing ground when managing their vulnerabilities. So, what does this mean? The data doesn't mean it's all gloom and doom. Taking a look at the systems currently in place at your organization is a great place to start, when you are looking to improve vulnerability management.

TO READ THE FULL REPORT, AND LEARN MORE ABOUT VULNERABILITY MANAGEMENT, VISIT SECURITYSCORECARD.COM

SecurityScorecard

Funded by world-class investors including Evolution Equity Partners, Silver Lake Waterman, Sequoia Capital, GV, Riverwood Capital, and others, SecurityScorecard is the global leader in cybersecurity ratings with more than 12 million companies continuously rated. Founded in 2013 by security and risk experts Dr. Aleksandr Yampolskiy and Sam Kassoumeh, SecurityScorecard's patented rating technology is used by over 30,000 organizations for enterprise risk management, third-party risk management, board reporting, due diligence, cyber insurance underwriting, and regulatory oversight. SecurityScorecard is the first cybersecurity ratings company to offer digital forensics and incident response services, providing a 360-degree approach to security prevention and response for its worldwide customer and partner base.

SecurityScorecard continues to make the world a safer place by transforming the way companies understand, improve and communicate cybersecurity risk to their boards, employees and vendors. Every organization has the universal right to their trusted and transparent Instant SecurityScorecard rating. For more information, visit securityscorecard.com or connect with us on LinkedIn.

Gain continuous visibility into your digital footprint, vulnerabilities, and clear steps to remediate them with SecurityScorecard. Claim your free account now and take control of your cybersecurity risk.

Cyentia Institute

The Cyentia Institute is a research and data science firm working to advance cybersecurity knowledge and practice. Cyentia pursues this goal through data-driven research publications like this one and through a growing portfolio of analytic services. Learn more at www.cyentia.com.