imperva

REPORT

Quantifying the Cost of API Insecurity

Contents

EXECUTIVE SUMMARY

Application Programming Interfaces (APIs) have emerged as useful tools that streamline business operations and enhance the digital experience for customers. As their use has proliferated, however, the importance of properly securing APIs is also becoming increasingly evident. API-related hacks and data breaches have impacted companies across nearly all sectors and geographies, resulting in skyrocketing remediation and legal costs for companies.

Just how high are these costs?

In order to quantify the cost of API insecurity, Imperva partnered with the Marsh McLennan Global Cyber Risk Analytics Center to analyze API-related incident data. Their research suggests that the lack of secure APIs could have the following impact:

USD 12-23 billion

Average annual API-related U.S. cyber loss

USD 41-75 billion

Average annual API-related total global cyber loss

USD 205-376 million

Average annual API-related global insured cyber loss

These estimates provide a view on losses that are entirely avoidable. If companies made an upfront investment in properly securing all of their APIs, their API-related losses could decrease significantly even as their API adoption continues to increase.

When comparing the number of reported API-related events to the non-API-related events identified in the database, Marsh McLennan discovered a positive correlation between company revenue and the API-related event frequency. Despite reporting the lowest number of API-related events over the analysis period, companies earning more than USD 100 billion in revenue attributed roughly 25% of the cyber events that they experienced to API insecurity. Similar elevated event frequencies were observed in companies with annual revenue over USD 1 billion as well. The analysis indicates that large firms face an elevated risk of experiencing an API-related incident. This is likely due to increased deployment and utilization of APIs in large companies, which could expose companies to more potential breaches.

The Growing Cost of API Adoption and Insecurity

In the last decade, API tools have become ubiquitous services within the corporate world, with the average company in 2018 operating an estimated 1,181 cloud apps across its entire organization, and most companies communicating intentions to substantially increase that number in the future.[1]

This trend has only accelerated. Decision-makers are currently lining up heavy investments into their digital transformation programs; 70% plan to heavily invest in new technology adoption, while 67% plan to secure their digital transformation efforts. The specific digital transformation initiatives for 2022 also line up with security priorities: The highest-ranking digital transformation initiative is to "improve security (e.g., for API, endpoint systems, web apps)" at 61%.[2]

As such, the number of companies, developers, and consumers using these tools has continued to grow at an exponential rate. In 2020 alone, API use by the Financial Services industry grew by an estimated 125%, while traffic from the Healthcare industry ballooned by more than 400%.[3] The following year, health monitoring API use increased an additional 941%, suggesting that the current API frenzy is not slowing down yet.[4]

Expanding API adoption comes with expanding risk, however—leading to rising costs. For example, in 2020 alone, Google's Apigee API recorded a 172% increase in malicious traffic.[5] The proliferation of API threats has continued to spread as API deployment expands. As such, in the past few years, multiple high-profile organizations have fallen prey to API breaches, exposing a plethora of personal and company records and costing companies millions of dollars. As the number of APIs continues to grow; data protection regulations expand; and malicious actors refine their tools; these trends will accelerate, underscoring the need to invest in robust and effective API protection strategies.

This report investigates recent API-related attacks; quantifies the proportion of cyber incidents that can be attributed to APIs; and estimates the potential reduction in financial losses to the cyber insurance industry, U.S. economy, and global economy if API security was improved.

In 2020...

Financial Services API use grew by

~125%

Healthcare API traffic ballooned by

400%+

In 2021...

Health monitoring API use increased an additional

941%[4]

[1] API Integration for Transportation & Logistics | eBook | Jitterbit

[2] Improve API Performance with a Sound API Security Strategy | Imperva.com

[3] Google Cloud State of APIs Report - Digital Transformation | Google Cloud Blog

[4] Importance of API Security in Healthcare Grows as Cyberattacks Increase (healthitsecurity.com)

[5] Apigee_StateOfAPIS_eBook_2020.pdf

The Rise of API Attacks

As API adoption has accelerated and API breaches have proliferated, attackers are targeting an increasingly diverse swath of organizations. In the last 5 years, API attacks have been reported in large financial firms, popular social media sites, health care groups, cryptocurrency trading platforms, consumer retailers, governmental organizations, and more. Consequently, the types of records impacted by these attacks and the financial costs of API breaches are also increasing, creating new headaches for companies already concerned by ransomware, phishing, and the myriad of other recent cybersecurity threats.

As APIs are deployed in new industries, the types of data impacted continue to evolve. In 2021, insecure API in use by a credit monitoring company risked exposing the personally identifiable information of tens of millions of customers. In the health care industry, a recent hub of API adoption, experts are increasingly concerned about the potential loss of personal health information due to an API breach.[6] As such, the risks of operating an unprotected API will likely continue to rise, underscoring the importance of employing proper API protection solutions to mitigate the possibility of facing a highly damaging data breach.

[6] Importance of API Security in Healthcare Grows as Cyberattacks Increase (healthitsecurity.com)

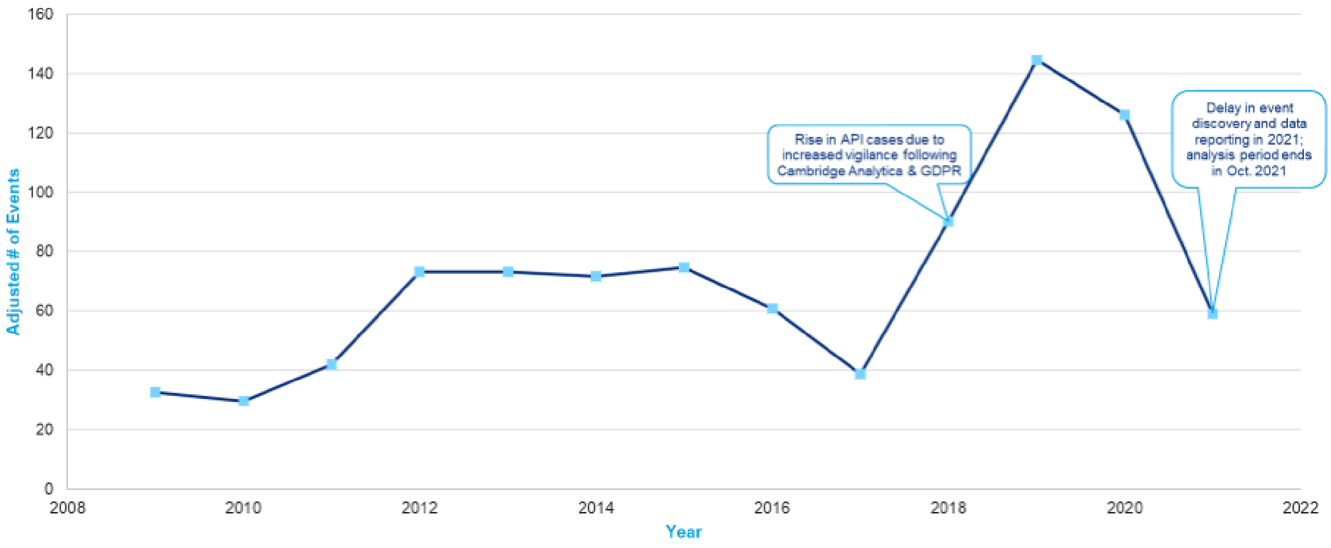
Marsh McLennan Global Cyber Risk Analytics Center Study

As an enterprise-wide resource for Marsh McLennan, the world's leading professional services firm in the areas of risk, strategy, and people, the Marsh McLennan Global Cyber Risk Analytics Center leverages Marsh McLennan's proprietary data, in addition to a suite of licensed models and data, to deliver insights on cybersecurity and the trends impacting the future of global cyber risk.

API-Related Incidents by Year

The API annual incidence between 2009 and 2017 represents a stable mean rate in API events, and the decrease in 2016 and 2017 remains within the statistical variability around that rate.

Figure 1: Adjusted API Event Count by Year
Source: Marsh McLennan Data



Rise in API cases due to increased vigilance following Cambridge Analytica & GDPR

Delay in event discovery and data reporting in 2021; analysis period ends in Oct. 2021

Between 2018 and 2020, however, the total event counts more than tripled over three years.

Following the 2018-2020 surge in API-related events, incident data displays a drop in reported API-related events in 2021. Due to delays in discovering API-related events and reporting cyber incidents, the total number of API-related events in 2021 is likely an underestimate, unrelated to any ongoing trends. Additionally, the data used to complete this analysis was as of October 2021. As companies continue to discover and report cyber breaches, this 2021 value is expected to increase above the currently recorded level.

API-Related Events by Industry

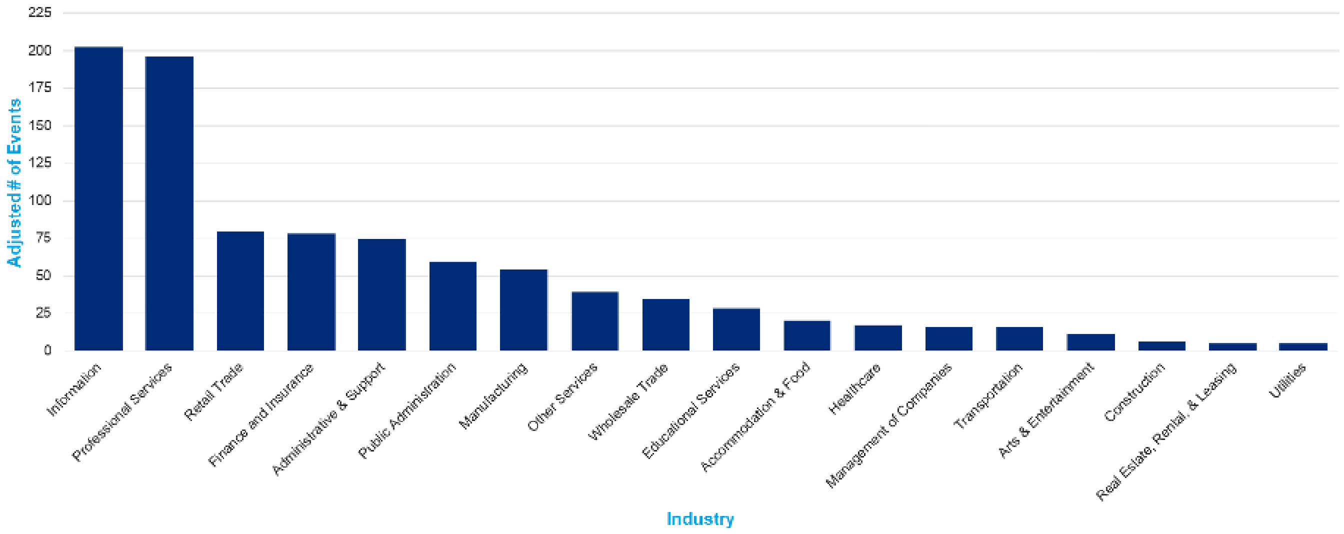
Despite the recent expansion of API deployment in industries such as Healthcare, technology-dependent industries operate far greater numbers of APIs than traditional industries and, by extension, face a greater risk of experiencing an API-related event.

As expected, the analysis reveals a heavy concentration of events in technology-dependent industries, with the vast majority occurring in the Information, Professional Services, Retail, and Finance industries.

Top Industries Affected by API-Related Events:

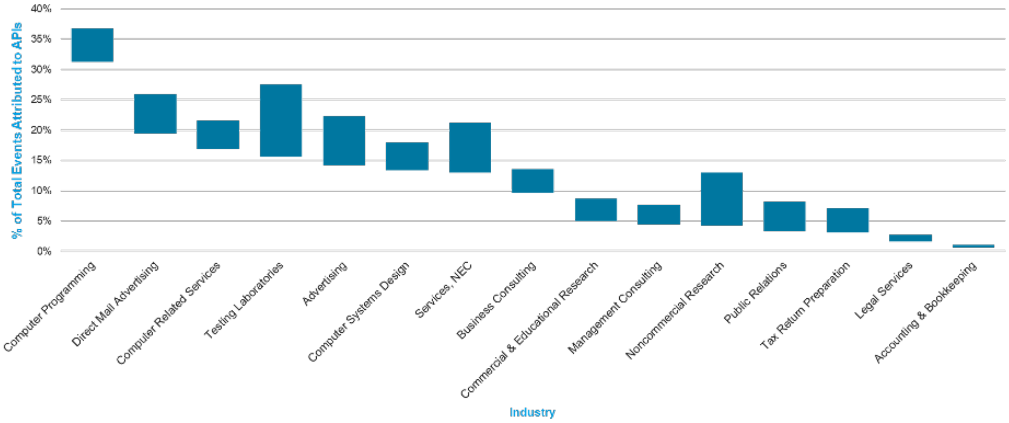
- **Information**
- **Professional Services**
- **Retail**
- **Finance**

Figure 3: Adjusted API Event Count by Industry
Source: Marsh McLennan Data



While technology-dependent industries tend to experience higher API-related event frequencies, this is not uniformly true for all sectors. Notably, despite recording the fourth-highest number of API-related events during the analysis period, the Finance & Insurance industry recorded the third-lowest percent of cyber incidents attributed to API insecurity. Similarly, the Healthcare sector reported the lowest event frequency, despite experiencing a higher event volume than six other sectors. While some of these discrepancies may be attributed to higher API security standards, it is also likely that the elevated incidence of other cyberattacks, such as lost or stolen data and ransomware in the Healthcare industry, depresses their sector's API-related event frequency.

Figure 5: Percent of Cyber Incidents Attributed to API for Professional Services Industry
Source: Marsh McLennan Data



In general, API-related events remain concentrated in technology-dependent industries, such as the Information sector. Nonetheless, as API adoption continues to expand, similar trends could impact additional industries, underscoring the importance that companies—regardless of the current API-related event frequency observed in their industry—invest in proper API protection tools and techniques.

Most API-related events occurred in companies with

< $50 million

in annual revenue.

However, companies generating

> $100 billion

saw a 25% increase in API-related cyber events.

Large firms face an elevated risk of experiencing an API-related incident.

API-Related Events by Company Revenue

In its analysis, the Marsh McLennan Global Cyber Risk Analytics Center also partitioned the data into nine distinct revenue bands to view how companies of different sizes are impacted by API-related events. Due to the considerable number of small firms within the incident database, most API-related events were witnessed in companies generating less than $50 million in revenue per year.

Figure 6: Adjusted API Event Count by Company Revenue
Source: Marsh McLennan Data

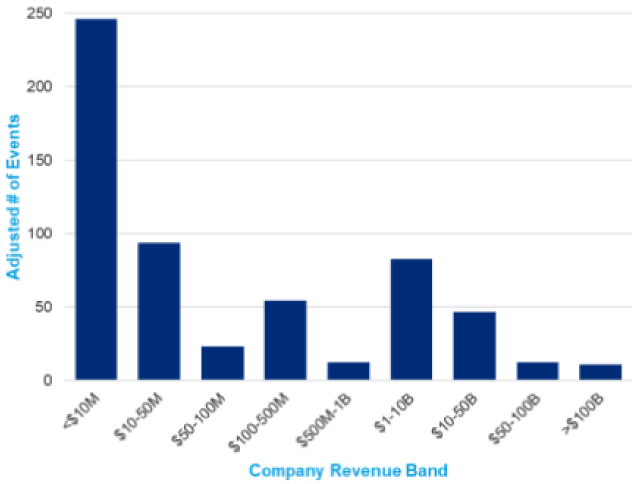
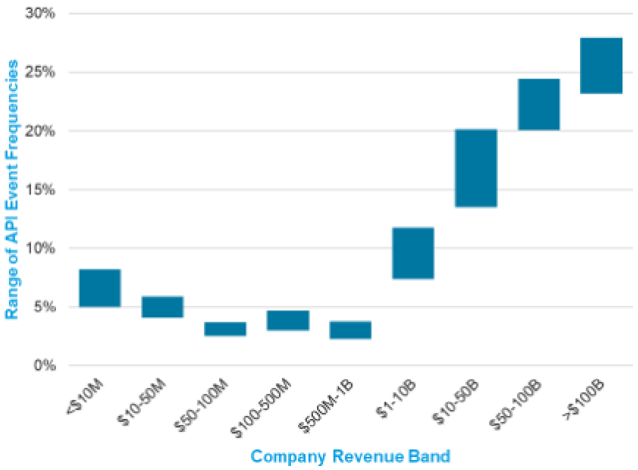


Figure 7: Percent of Events Attributed to APIs by Company Revenue
Source: Marsh McLennan Data



When comparing the number of reported API-related events to the non-API-related events identified in the database, Marsh McLennan discovered a positive correlation between company revenue and the API-related event frequency. Despite reporting the lowest number of API-related events over the analysis period, companies earning more than USD 100 billion in revenue attributed roughly 25% of the cyber events that they experienced to API insecurity. Similar elevated event frequencies were observed in companies with annual revenue over USD 1 billion as well. The analysis indicates that large firms face an elevated risk of experiencing an API-related incident. This is likely due to increased deployment and utilization of APIs in large companies, which could expose companies to more potential breaches.

API-Related Events by Geography

Finally, the incident data was partitioned by geography to determine potential geographic signals in API-related events.

Due to the high volume of ransomware and other cyber events in North America, the percent of events attributed to API in the region is remarkably low, with API-related events accounting for between 3.1-5.9% of all observed cyber incidents. European companies also reported more API-related events than Asia, Africa, and Latin America combined; however, elevated levels of other cyberattacks on the continent also resulted in a lower API-related event frequency of between 8.5-12.9%.

Despite reporting a relatively sparse number of API-related events, companies in Asia experienced an API-related event percentage approximately four times higher than the North American estimate. Several factors could contribute to the high percentage of events attributed to API insecurity, including the scarcity of reported ransomware attacks in the region or relaxed reporting requirements in some countries.

Figure 8: Adjusted API Event Count by Continent[7]
Source: Marsh McLennan Data

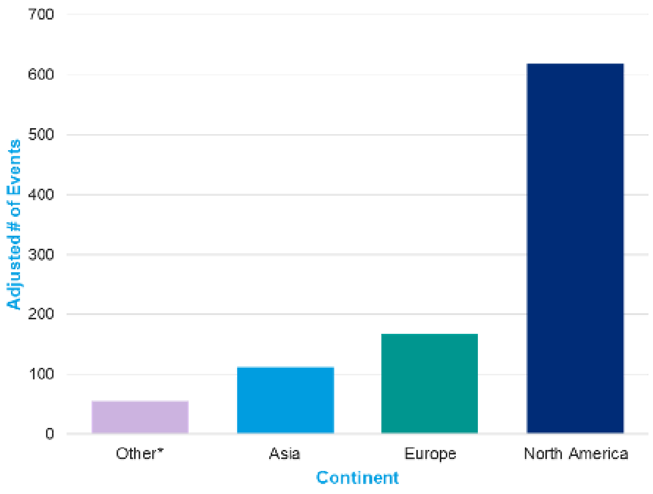
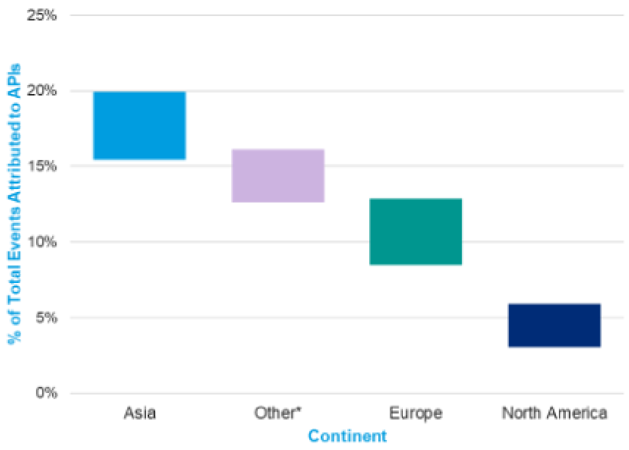


Figure 9: Percent of Total Events Attributed to API Insecurity by Continent
Source: Marsh McLennan Data



[7] Data for Africa, South America, and Oceania were combined in the Other* category due to low incident volume

When looking at the data by country, the exceptionally high event volume in the United States becomes increasingly clear, with more than 57% of all reported API-related events occurring in the United States. As a result, when compared to the number of total observed cyber events, the frequency of API-related events falls to between 3.2-5.9%. Of the 10 countries examined, only Canada experienced a lower estimated event frequency, of between 2.1-6.7%.

By examining API-related events on a country level, the analysis highlights specific markets that may benefit from increased API protections. For instance, although the percentage of total events attributed to API in the United States is relatively low, the high raw number of events observed over the analysis period suggests a large number of companies in need of greater protections. Additionally, despite a relatively low total event count in the Netherlands, between 17.9-24.2% of all events there were attributed to API insecurity, signaling that Dutch companies could benefit from greater API security.

57% of all reported API-related events occurred in the U.S.

Most countries experienced a higher estimated API-related event frequency of **3–6%** compared to the number of total cyber events.

The Netherlands experienced the highest percentage of API-related events at **18–24%**.

Figure 10: Adjusted API Event Count by Country
Source: Marsh McLennan Data

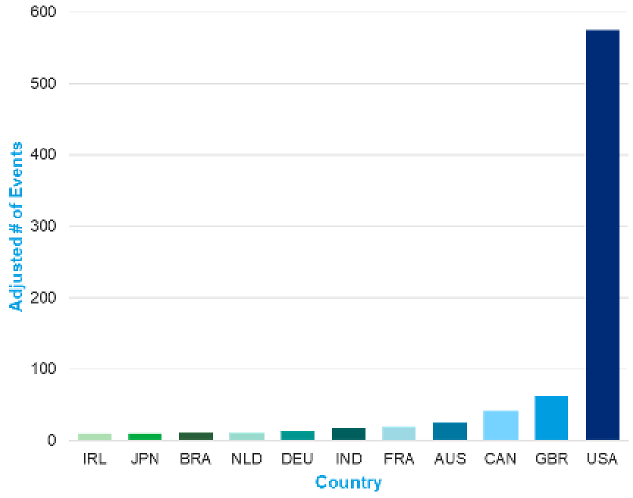
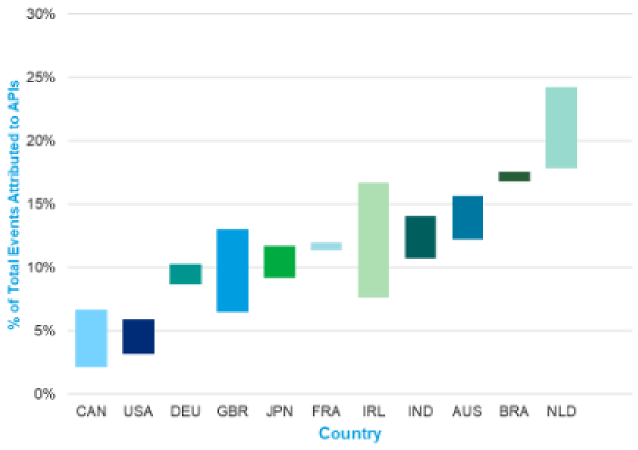


Figure 11: Percent of Total Events Attributed to API Insecurity by Country
Source: Marsh McLennan Data



Technographic Indicator Analysis

In addition to analyzing reported API-related events, the Marsh McLennan Global Cyber Risk Analytics Center examined key technographic indicators of API security to identify changes in protections against API breaches over time and by industry. In coordination with Imperva, Marsh McLennan identified four technographic indicators relevant to API security:

1. Web application headers, which analyzes the security-related fields in the header section of web applications
2. Patching cadence, which identifies software vulnerabilities and measures the speed at which vulnerabilities are addressed
3. Security incidents, which identifies events involving the unauthorized access of a company's data
4. Server software, which tracks issues relating to unsupported server software.

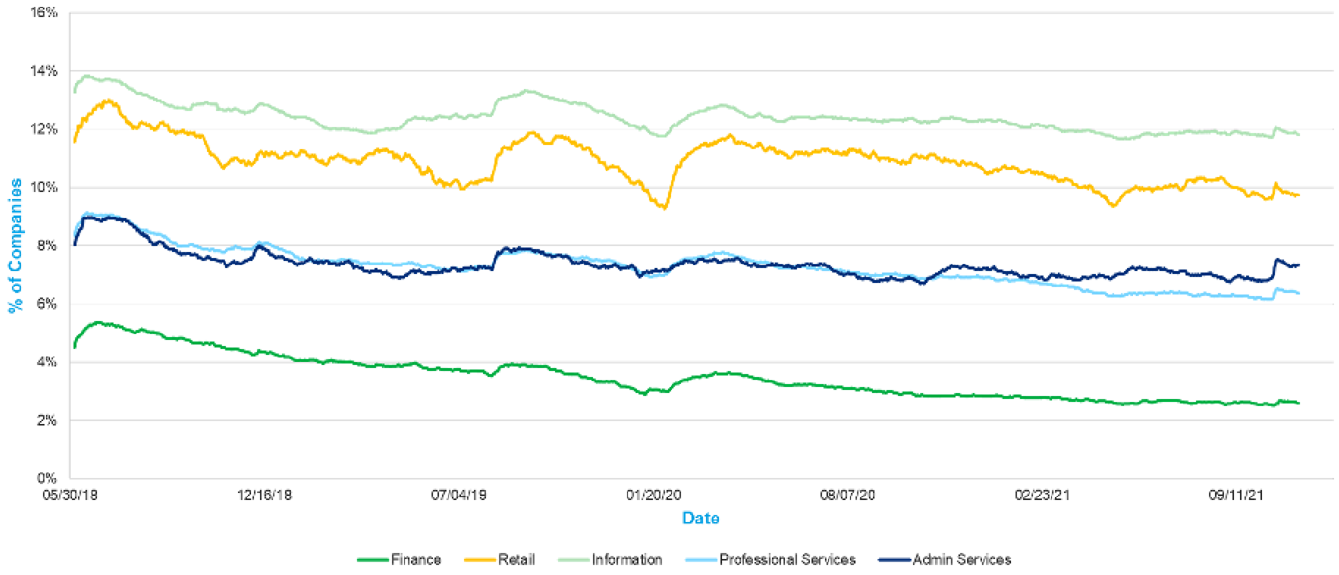
While these technographic indicators do not necessarily directly measure API security, they are a useful proxy indicator for a company's overall cybersecurity posture, including API security. Researchers then developed an API-Specific Cyber Control score by averaging the above indicators.

As a result, the higher percentage in Figure 12 indicates a higher proportion of companies within a given industry underperforming against the API-related technographic controls. Figure 12 charts the performance of five key industries: Finance, Retail, Information, Professional Services, and Administrative Services.

The analysis of API-related technographic indicators reveals a substantial difference in API-related controls by industry, with less than 4% of Finance firms scoring below the Controls Threshold. Due to the Finance industry's strong API-related controls, the industry consistently attributes a relatively low percent of cyberattacks to API insecurity. Conversely, 12% or more of companies in the Information industry score below the Controls Threshold, indicating a larger proportion of Information industry companies with poor API-related security.

The Finance industry had the strongest API-related controls and therefore experiences a relatively low percent of API attacks, compared to the Information industry companies with poor API-related security.

Figure 12: Percent of Companies below API-Specific Cybersecurity Threshold
Source: Marsh McLennan Data



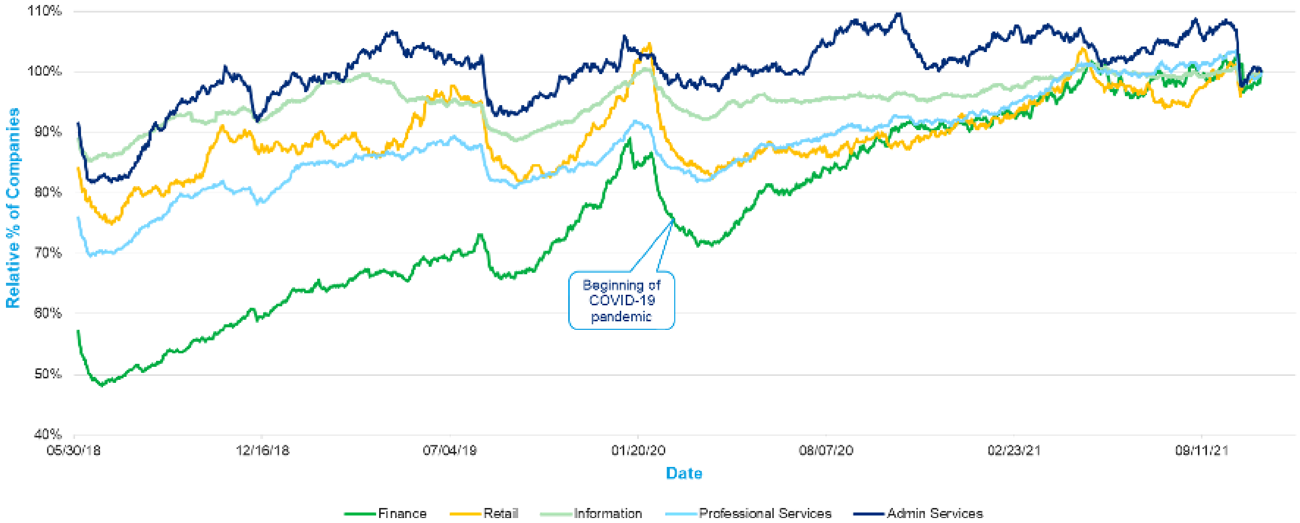
Researchers also found a substantial improvement in the Finance industry's performance against the API-related technographic indicators during the analysis period. Between June 2018 and September 2021, a larger percentage of companies in the Finance industry improved their API-specific cyber security posture as compared to other industries over the same period. Although the Finance industry experienced the greatest percentage of companies with an improved API-specific cyber security controls score, industry performance against the API-related technographic indicators increased across all key industries between June 2018 and November 2021.

Additionally, the trends analysis highlights the substantial impact of the Covid-19 pandemic on API-related cyber controls, with some industries experiencing up to a 20-point drop in their normalized performance score. The sudden shift to work-from-home arrangements caused companies to rapidly decentralize business operations and vastly increase the number of remote work systems. Consequently, companies sacrificed API-related cyber controls in order to rapidly accommodate for new health-conscious work requirements. While some industries, such as the Professional Services sector, were able to quickly rebound from the pandemic, other sectors, including Retail, took more than a year to revert to their January 2020 benchmark. The inconsistent recovery rate following March 2020 reveals the divergent impacts of the Covid-19 pandemic across industry API-related cyber controls.

Covid-19 and the sudden shift to work-from-home arrangements impacted industries and their API-related cyber controls differently, with inconsistent recovery rates.

Professional Services quickly rebounded, while Retail took over a year to return to its January 2020 benchmark.

Figure 13: Relative Proportion of Companies at or above Controls Threshold, compared to November 2021
Source: Marsh McLennan Data



Overall, Marsh McLennan's technographic indicator analysis closely aligns with the event analysis by industry, with other low performing industries, such as the Information and Retail sectors, recording elevated API-related event frequencies.

Total API Cost Estimates

Finally, Marsh McLennan developed benchmark loss estimates on the cost of cyber incidents in the United States, across the globe, and globally paid by insurers, identifying the following loss estimates:

USD 300 billion

Average annual API-related U.S. cyber loss

USD 1,000 billion

Average annual API-related total global cyber loss

USD 5 billion

Average annual API-related global insured cyber loss

In order to develop the estimated amount of loss attributed to API-related events, researchers combined the Marsh McLennan incident data, the raw API-related incident proportion, and the underreporting factor to develop an estimated API-related frequency range of 4.1-7.5%. Researchers then applied the percentage range of events from API issues to develop the following annual API-related loss estimates:

USD 12-23 billion[8]

Average annual API-related U.S. cyber loss

USD 41-75 billion

Average annual API-related total global cyber loss

USD 205-376 million[9]

Average annual API-related global insured cyber loss

These estimates provide a view on the potential losses that could be avoided if all companies properly secured all of their APIs and suffered no incidents related to APIs going forward.

[8] The "average annual total US loss" includes losses that may or may not covered by insurance (the bulk of losses, in fact, are not covered by cyber insurance). This is because cyber insurance limits are not sufficient in today's market, and many companies, especially small ones, don't purchase cyber insurance at all. An example conclusion here is that up to USD 23 billion of loss to US companies in total can be eliminated if companies maintained perfect API security.

[9] The "average annual insured loss" is the loss that cyber insurers pay out to (all their) clients during an average year. So, an example conclusion of this finding is that cyber insurers could reduce up to USD 376 million of their claims per year if they required their insured clients to have better API security.

Conclusion

Since 2017, API-related events have become increasingly common, impacting a plethora of companies across disparate industries, revenue bands, and geographies. This rise—coinciding with a meteoric increase in competing cyber threats, such as ransomware attacks—threatens to compound the already spiraling costs impacting both businesses and insurers.

In its investigation of API-related incidents and technographic controls, the Marsh McLennan Global Cyber Risk Analytics Center estimates that API insecurity costs insurers around the globe **USD 205-376 million per year**—a value that has risen in recent years as the total volume of attacks has increased. Additionally, the threat of API-related events amounts to an estimated **USD 41–75 billion** of global cyber losses each year.

As evidenced by the API-related technographic indicators analysis, robust performance against API-related cyber controls is essential to limiting the threat of experiencing a costly API-related event. As API development and deployment continues to expand in companies, industries, and geographies, employing proper controls will remain paramount to controlling the costs of API insecurity. Barring any substantial changes to the current cybersecurity landscape, insurers and businesses will continue to see increasing API-related costs, compounding an already concerning cybersecurity landscape.

Appendix

The Marsh McLennan research suggests that between 4.1-7.5% of cyber events are attributed to API insecurity. They further partitioned the data by industry, company revenue, and geography.

INDUSTRY. By partitioning the data by industry, researchers discovered significantly higher frequencies of API-related incidents in the Information and Professional Services sectors.

COMPANY REVENUE. By analyzing events by company revenue, researchers highlighted higher proportions of API-related events for companies earning over $1 billion in annual revenue. Both the industry and revenue findings suggest that industries and organizations that tend to employ more APIs attribute a greater percentage of cyber events to API insecurity.

GEOGRAPHY. By partitioning the data by geography, researchers illustrate that, despite the United States witnessing the highest number of total API-related events, the proportion of cyber events attributed to API insecurity is higher abroad, with the Netherlands, Brazil, and Australia reporting the highest percentages.

In addition to the cyber incident analysis, researchers also examined key API-related technographic indicators to identify how API-related security practices differ by industry. The results suggest that companies in the Finance and Professional Services industry are best protected against API-related threats, while companies in the Administrative Services and Information sectors lag behind.