

REPORT

2024 Cybersecurity Threat Report: S&P 500

An in-depth analysis of cybersecurity incidents, third-party cyber risk, and security ratings of the S&P 500

 **STRIKE**

SECURITYSCORECARD THREAT RESEARCH, INTELLIGENCE,
KNOWLEDGE AND ENGAGEMENT TEAM

Introduction

In fall 2023, the U.S. Securities and Exchange Commission (SEC) adopted landmark cybersecurity regulations requiring publicly traded companies to make cybersecurity disclosures – including publicly disclosing “material” cybersecurity incidents within four days. These new regulations marked a transition from the previous experience of having relatively few breach reporting requirements, which left the government and policymakers without key information on the current threat landscape.

Against this backdrop, SecurityScorecard analyzed the security ratings of the members of the S&P 500 U.S. stock market index.

This research set out to:

- Find ways to improve the security of key players in the U.S. economy
- Guide third-party risk management (TPRM) teams, particularly at organizations dependent on these companies

Our threat researchers analyzed these companies’ security ratings both as a whole and by industry, in search of industry-specific variations. We identify the general areas in which these companies have the lowest security ratings, as well as the specific issues that reduced their ratings the most. It also reviews security incidents reported at these companies in 2023, in search of trends and “lessons learned.”

BREACH LIKELIHOOD

Companies with an F rating have a

**13.8X
GREATER**

likelihood of a data breach than companies with an A.



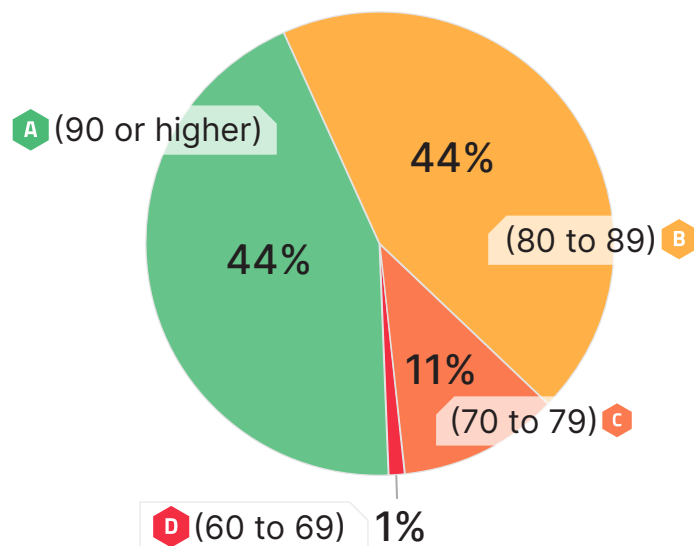
Key Findings:

- 1** 21% of S&P 500 companies experienced breaches in 2023.
- 2** 25% of S&P 500 breaches were at Financial Services & Insurance companies.
- 3** The average Social Engineering risk grade for the S&P 500 is an “F.”
- 4** Ransomware demands for S&P 500 victims are now often in the 8-figure range.
- 5** Average/median S&P 500 scores are 4-5% higher than our global sample.
- 6** Social Engineering is the most common risk factor (77%) for which S&P 500 companies receive their lowest scores. The exposure of employee information is a source of this vulnerability to social engineering attacks and was also the most common issue (52%) having the most negative impact on companies’ scores.
- 7** Comparison of security scores by industry revealed significant variations. Three industries have higher scores: Financial Services & Insurance; Government Services, Defense, and Aerospace; and Energy, Utilities, and Mining. Three industries have lower scores: Real Estate; Healthcare, Life Sciences, and Medical Supplies; and Technology, Telecommunications, and Media.
- 8** Breached S&P 500 members were disproportionately in three industries: Financial Services & Insurance; Healthcare, Life Sciences, and Medical Supplies; and Technology, Telecommunications, and Media. The higher rate of breaches in the latter two industries is consistent with their generally lower scores. The higher rate of Financial Services breaches is at odds with their typically high ratings and reflects the unique level of interest in this industry among criminals.
- 9** Many breaches affecting S&P 500 members occurred via third parties, rather than at the companies themselves. These vendors often provide software or other IT products and services. The most extreme example of this tendency is the mid-2023 campaign by the criminal group C10p, in which it exploited CVE-2023-34362, a zero-day vulnerability in the MOVEit file transfer software of Progress Software. This campaign affected multiple S&P 500 members directly, as actual users of MOVEit, as well as indirectly, via vendors using MOVEit.
- 10** Ransomware is a key threat for S&P 500 members due to the potential extortionate exposure of sensitive information and particularly the potential disruption of business operations, which may pose third-party supply chain risks for their customers. The amounts of ransom demands continue to trend upwards, and ransomware operators may retaliate for failed negotiations.

An Overview of S&P 500 Security Ratings

The average SecurityScorecard rating for all S&P 500 members is 88. The median rating is 89.

These average and median ratings compare favorably with the worldwide average rating of 84, and 88 and 89 are at the higher end of the “B” range. For example, a “B” rating means that the organization is 2.9 times more likely than one with an “A” rating to experience a breach. An organization with a “C” rating is 5.4 times more likely than one with an “A” rating to experience a breach, and so on. [Please consult this whitepaper](#) for a more detailed explanation of our current scoring methodology. The below pie chart illustrates the distribution of these scores across the whole S&P 500.



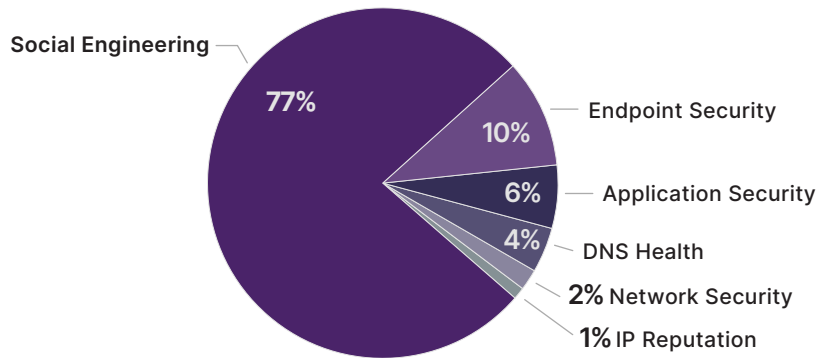
These generally favorable results do not come as a surprise to SecurityScorecard researchers. As we previously demonstrated in prior research, [there is a strong correlation between financial means and security hygiene](#). To put it simply: **security costs money**. Organizations with more resources are more able to afford the costs of security. It is thus not surprising that some of the largest companies in the world's largest economy would have somewhat above-average security ratings.

Distribution of Security Scores across the S&P 500

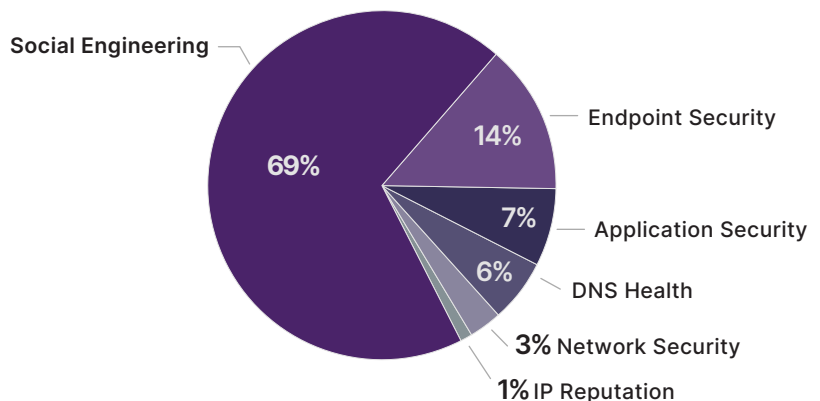
F Only one company had an F rating.

Problem Areas: Social Engineering

SecurityScorecard ratings reflect evaluations of an organization's observable security hygiene in 10 different factors or issue areas. Our researchers identified one of these 10 factors for which each S&P 500 member had its lowest score. Below are the percentages of S&P 500 members whose lowest scores were in the listed security factors. Of note, not a single S&P 500 member had its lowest score in any of the four other security factors by which SecurityScorecard evaluates organizations: Patching Cadence, Information Leak, Hacker Chatter, and Cubit Score.



We conducted further analysis along the above lines but limited its scope to those S&P 500 members whose scores were below the S&P 500 average of 88. The goal of limiting the analysis to organizations with below-average scores is to shed light on the factors that reduce scores for the whole sample. This more limited query revealed a similar but slightly more evenly distributed pattern of lowest-score factors. Indeed, the ranking of the six factors is the same as that of the broader sample. Social Engineering is still the most common area for organizations' lowest scores by a smaller margin that is nonetheless still enormous. Other problems of a more technical nature are somewhat more common as the lowest-scoring factor among these lower-scoring companies. We posit that less investment in security solutions by lower-scoring companies may account for this somewhat greater exposure to more security risks of a purely technical nature.



Distribution of Lowest-Scoring Security Factors among S&P 500 Members

Distribution of Lowest-Scoring Security Factors among S&P 500 Members with Below-Average Overall Scores

Average Social Engineering Score is an F

Both sets of figures suggest that vulnerability to social engineering attacks has the single-most negative impact on the security posture of S&P 500 member companies by an enormous margin, although this margin is somewhat less enormous for companies with lower overall scores. **The average Social Engineering score for S&P 500 members is 54, and the median is 53 - both of which are well within the “F” range.** For the more than three-quarters of S&P 500 members whose Social Engineering scores were the lowest component of their overall ratings, the average score was 48, and the median score was 50. In other words: social engineering poses a significant risk to many companies, even those with otherwise healthy risk profiles and good security.

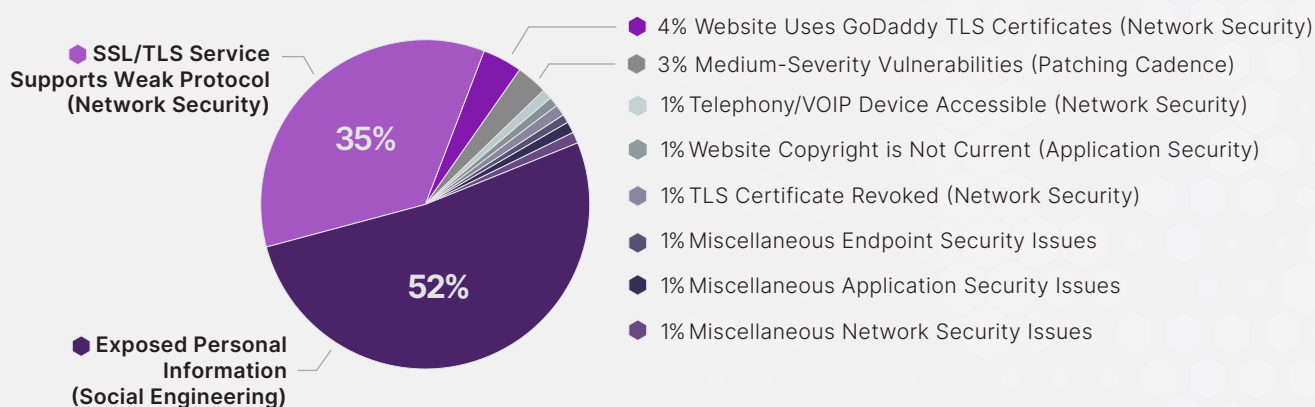
We noted above that investment in security solutions is a key factor in determining a company’s security posture. The somewhat greater prevalence of technical issues as lowest-scoring risk factors among those companies with below-average overall scores probably reflects this point. With that said, many if not most of these security solutions are technical in nature but might not solve human security problems, such as the tendency of so many users to fall victim to social engineering attacks that compromise their organizations. **Indeed, many threat actors use social engineering attack vectors precisely because they enable attackers to circumvent technical security solutions by manipulating human users.** In this case, the relatively low Social Engineering score factors of many otherwise high-scoring S&P 500 members serves as a reminder that investments in technical security solutions can only achieve so much without robust human defenses. Money can buy technology, but changing human behavior is more complex. Training employees to defend against social engineering attacks is an excellent security investment, but even that can only accomplish so much.

We will revisit the issue of social engineering in a subsequent discussion of breaches affecting S&P 500 members in 2023. Some of the most high-profile incidents at these companies last year lend credence to our finding that social engineering is the greatest weakness in the defenses of companies with otherwise strong security postures.

Problem Areas: Exposed Personal Information

Our researchers delved deeper into the specific issues within the various score factors that had the single-most negative impacts on the ratings of S&P 500 member companies. This pie chart illustrates the respective percentages of S&P 500 member companies whose ratings had the most negative impact from these issues. Within the parentheses are the broader score factors under which these specific issues fall.

Distribution of Most Negative Score Impact among S&P 500 Members



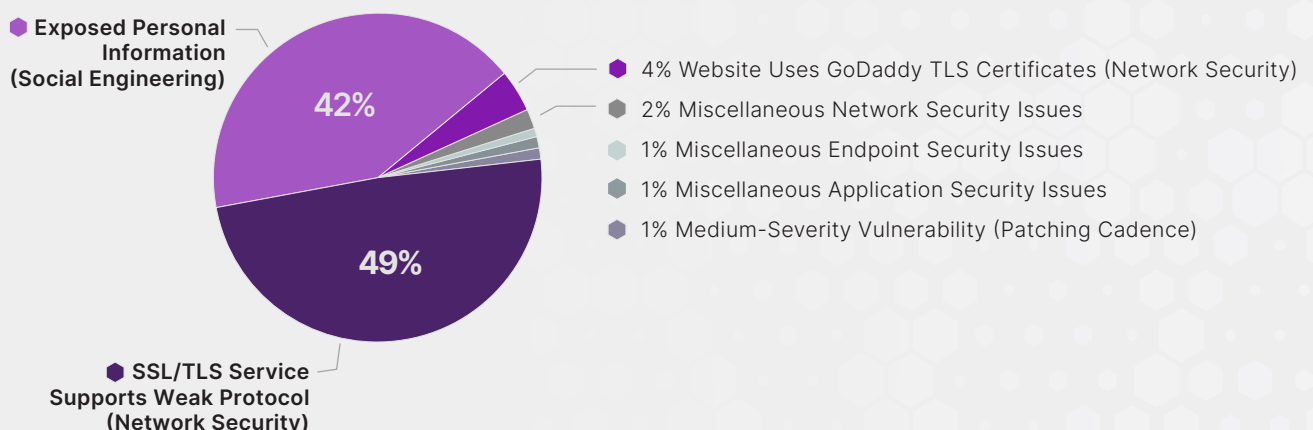
Exposure of Personal Information Facilitates Social Engineering Attacks

These results shed light on the above finding that Social Engineering is the area in which more than three-quarters of S&P 500 members had their lowest ratings. The exposure of personal information on employees greatly facilitates social engineering attacks on their employers. Skilled threat actors conduct reconnaissance on targeted organizations, including their employees, combing through a variety of sources in search of information to tailor their social engineering attacks for maximum effectiveness, or to impersonate employees to gain access. Contact information, such as email addresses and phone numbers, gives threat actors targets to which they can send their malicious email, voice, and SMS messages. LinkedIn and other social networking platforms also provide useful entry points and venues in which to engage employees as social engineering targets. Additionally, the availability of personal details such as dates of birth and mother's maiden names are useful in bypassing PII-based help desk authentication procedures.

Beyond the exposure of personal information facilitating social engineering attacks, three of the specific issues that most frequently had the most negative impact on scores pertained to SSL/TLS. The bulk of those encryption issues involved the use of weak TLS protocols in the organizations' websites that could be vulnerable to decryption.

Further analysis of the specific issues with the most negative impact on the subset of S&P 500 members with below-average scores reinforced one of the findings from above. We noted above that companies with below-average overall scores still have Social Engineering as their top problem, but by a less enormous margin than their higher-scoring counterparts; the lower-scoring companies also have greater exposure to a wider range of technical risks. That pattern changes only somewhat at this more granular level of analysis. The Social Engineering risk of Exposed Personal Information is still a pervasive problem, with 42% of below-average S&P 500 members having the most negative impact on their scores from this issue, but it is no longer the most common one. Weak SSL/TLS protocols were instead the leading negative issue at 49%. Other Network Security issues had the most negative impact on scores for another 6% of the below-average subset of the S&P 500. These figures suggest, as noted above, that organizations with weaker security in general face a more diverse range of risks.

Distribution of Most Negative Score Impact among S&P 500 Members with Below-Average Overall Scores



Statistics by Industry

Average and Median Security Scores for S&P 500 Members, by Industry with average and median scores paired together for each industry.

■ Average ■ Median



Real Estate
85 / 86



Healthcare, Life Sciences, and Medical Supplies
86 / 87



Technology, Telecommunications, and Media
86 / 87



Transportation & Logistics
87 / 88



Manufacturing & Construction
87 / 88



Professional Services
88 / 88



Retail & Hospitality
88 / 89



Consumer Goods & Services
89 / 90



Government Services, Defense, and Aerospace
90 / 90



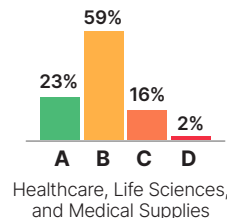
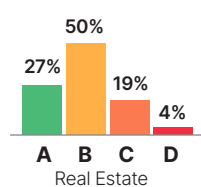
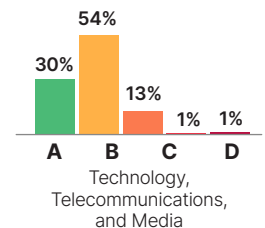
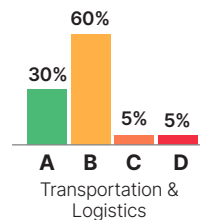
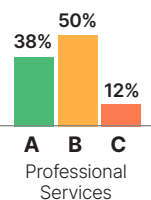
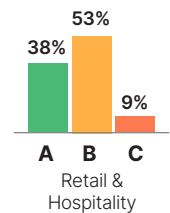
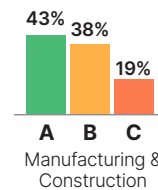
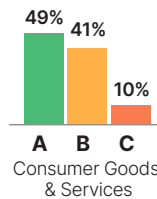
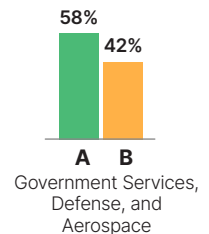
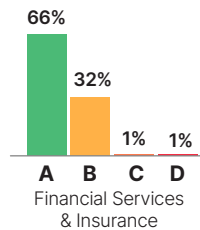
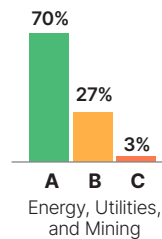
Energy, Utilities, & Mining
91 / 92



Financial Services & Insurance
91 / 92

SecurityScorecard researchers asked the same questions of our data again, but this time by industry, in search of variations between the different verticals.

The distribution of scores within each industry was as follows. We have ranked these industries roughly according to the distribution of their letter grades.



Comparing the various industries by both average scores and by the distribution of scores within them, three industries stand out at the top of the pack, while another three stand out at the bottom.

An examination of the factors and specific issues responsible for these scores may shed further light on the variations between industries. Within each industry, Social Engineering remains the most common lowest-scoring factor across the board, as it is in the general sample. The degree to which Social Engineering is the most common lowest-scoring factor nonetheless varies considerably from one industry to another.

Financial Services & Insurance

It should not come as a surprise for Financial Services & Insurance to be in the top three. Financial institutions tend to have some of the most robust security programs in the private sector due to extensive criminal targeting of them and the significant funds that they hold. By the same token, government contractors and manufacturers of aircraft and military hardware often have tighter security because they possess highly sensitive information of great value to both criminals and other actors operating on behalf of foreign governments. It is thus not surprising that this was the only industry whose S&P 500 members had only “A” or “B” ratings and nothing in the “C” range or lower. The strong performance of the Energy, Utilities, and Mining vertical may not be as obvious, although oil & gas exploration does generate some extremely valuable intellectual property of a geological nature that would be extremely valuable to competitors.

Healthcare

Healthcare organizations have a reputation for security challenges, so it is not surprising that this industry’s scores are toward the lower ends of both lists. More surprising was Real Estate. Security researchers often include Real Estate under the broader rubric of Financial Services, so perhaps our treatment of it as its own industry has revealed an issue that has gone unnoticed as of yet. Technology, Telecommunications, and Media organizations are also toward the lower end of the list. We attribute this ranking to: the often larger and more complex attack surfaces of technology and telecommunications organizations, which gives them more potential points of failure; and the greater third-party risk of organizations in this industry, as both primary targets themselves and also as attack vectors to use against other targets. Please read [this paper on third-party breaches](#) for more information on this vertical’s distinctive third-party risk profile.

Percentages of S&P 500 Members in Each Industry with Social Engineering as Their Lowest Score Factor

Professional Services	100%
Financial Services & Insurance:	91%
Government Services, Defense, and Aerospace	83%
Manufacturing & Construction	80%
Technology, Telecommunications, and Media	80%
Consumer Goods & Services	79%
Energy, Utilities, and Mining	79%
Technology, Telecommunications, and Media	70%
Healthcare, Life Sciences, and Medical Supplies	69%
Real Estate	65%
Retail & Hospitality	60%

Percentages of S&P 500 members with Most Negative Impact from Specific Issues

Of note, the percentage of organizations for which Social Engineering is the lowest-scoring factor is higher in some industries that have higher scores in general, such as Financial Services & Insurance and Government Services, Defense, and Aerospace. By the same token, organizations tend to have a greater diversity of technical security issues other than Social Engineering in industries that tend to have lower scores in general, such as Real Estate, Healthcare, and Technology. As mentioned above, we posit that Social Engineering remains a key vulnerability for organizations that have otherwise robust security programs from a purely technical perspective. Social Engineering attacks can often easily circumvent expensive technical security solutions. In contrast, organizations that have not invested as much in security remain exposed to a wider range and greater diversity of risks, technical or otherwise.

Not unlike the cross-industry sample of S&P 500 members, the exposure of employee information remains the single-most common issue having the most negative impact on organizations' ratings in all but three industries, under the broader rubric of Social Engineering exposure. In the three other industries, the use of weak TLS protocols was the most common issue with the most negative impact on organizations' ratings.

Exposure of Personal Information

Professional Services	88%
Financial Services & Insurance	69%
Healthcare, Life Sciences, and Medical Supplies	61%
Consumer Goods & Services	56%
Transportation & Logistics	55%
Manufacturing & Construction	53%
Government Services, Defense, and Aerospace	50%
Retail & Hospitality	49%

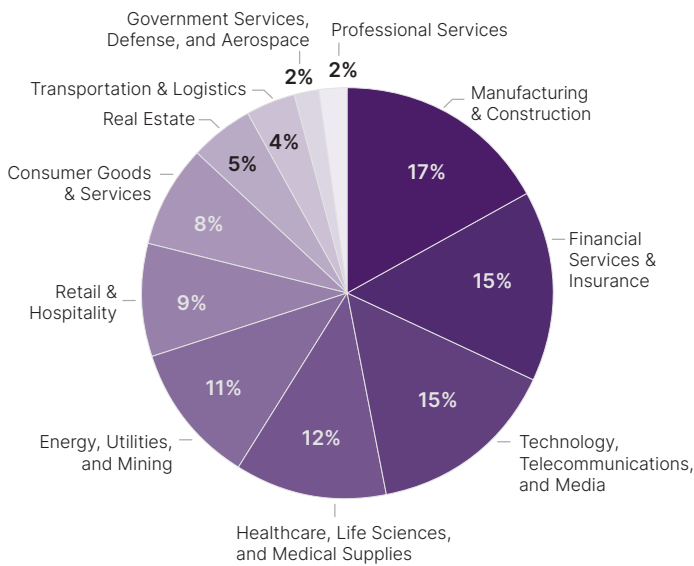
Weak TLS Protocol

Real Estate	54%
Energy, Utilities, and Mining	52%
Technology, Telecommunications, and Media	52%

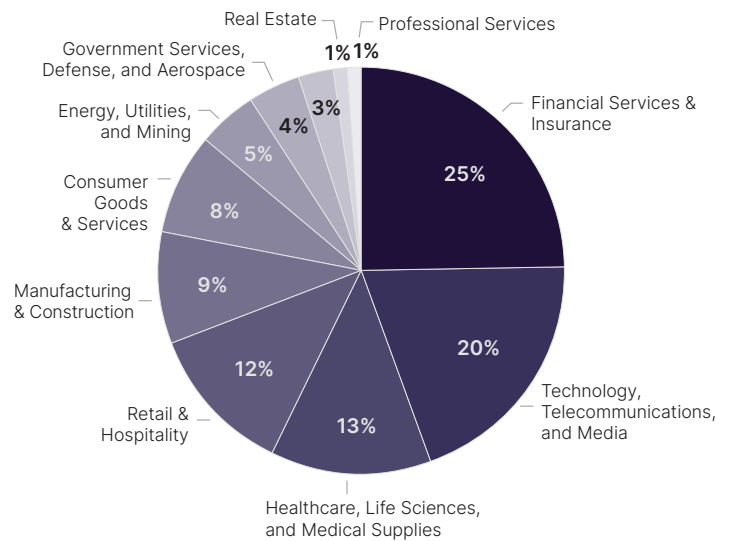
Incidents

21% of S&P 500 members experienced network or data breaches last year, according to reporting that our tools collected. Both the average and median scores of those S&P 500 members that reportedly experienced breaches was 88 - the same as the overall average, but slightly lower than the median score of the whole sample.

Below is a comparison of the distribution of S&P 500 members by industry, compared to a distribution by industry of that subset of 21% of S&P 500 members that reportedly experienced a breach.




Overall Distribution by Industry of S&P 500 Member Companies



Distribution by Industry of Reportedly Breached S&P 500 Member Companies

The distribution of breached companies by industry has marked differences from the overall sample. More than half of all breached companies (58%) were in just three industries: Financial Services & Insurance; Technology, Telecommunications, and Media; and Healthcare, Life Sciences, and Medical Supplies (13%). In contrast, it took the top four industries to make up a similar percentage (59%) of the overall S&P 500.



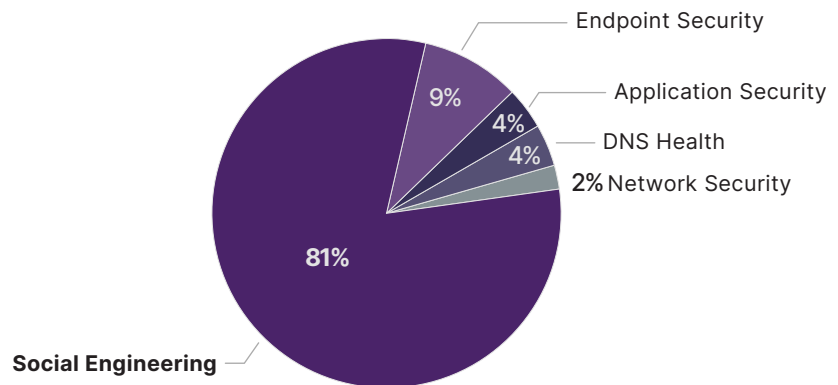
More importantly, the top three industries in the subset of breached S&P 500 member companies are an unusual combination. As we have seen above, Healthcare and Technology companies are often at the lower end of the score range, so it is not a surprise to see that they constitute larger shares of the subset of reportedly breached S&P 500 companies. Technology in particular stands out in this regard, as it represents only 15% of the broader S&P but 20% of the reportedly breached subset.

However, the biggest increase in “market share” was for Financial Services, which represents only 15% of the broader S&P 500 but a whopping 25% of the breached subset - a 10% increase. It is even more surprising because Financial Services organizations tend to have some of the highest security scores in general. The simple answer to this ostensible anomaly is that the willingness of many criminals to pursue harder targets in the hopes of greater profits is a threat that even the best security measures cannot always defeat. Indeed, Financial Services organizations tend to have some of the best security in the private sector precisely because they are such a uniquely desirable target for criminals. Someone once asked the famous bank robber Willie Sutton why he robbed banks, to which he responded: “because that’s where the money is.” In contrast, the Energy vertical displayed a pattern that one would expect of an industry whose organizations tend to have higher security ratings. It represented 11% of the overall sample but only 4% of the breached subset of that sample.

The biggest increase in “market share” was for Financial Services, which represents only 15% of the broader S&P 500 but a whopping 25% of the breached subset - a 10% increase.

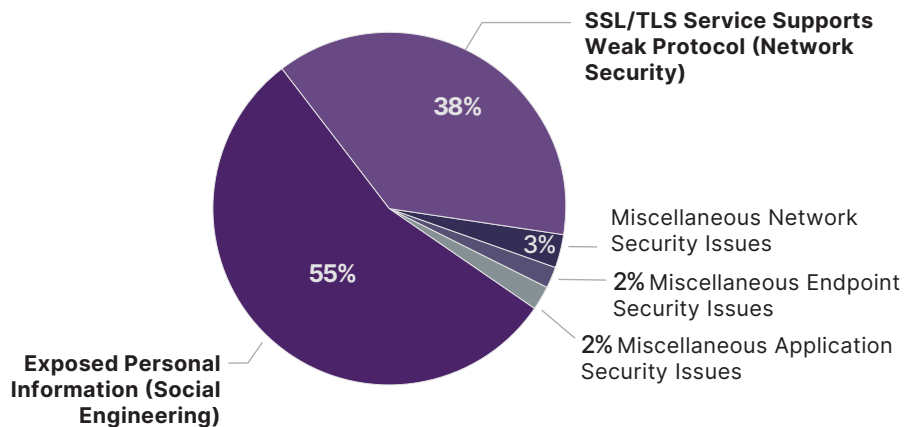
Distribution of Lowest-Scoring Security Factors among Breached S&P 500 Members

An analysis of the lowest-scoring factors of the subset of S&P 500 companies affected by breaches in 2023 suggested that Social Engineering is a bigger risk area for them than it was for the whole sample. Below are the percentages of breach-affected S&P 500 members whose lowest scores were in the respective areas. At 81%, the “market share” of Social Engineering as the lowest-scoring area is somewhat higher than in the overall S&P 500 sample (77%). As with the overall sample, Endpoint Security and Application Security come in a distant second and a distant third, respectively.



The distribution of individual issues with the single-most negative impact on scores among breach-affected S&P 500 members was similar to that of the overall sample, but with a somewhat greater prevalence of Exposed Personal Information as a Social Engineering issue (55% vs. 52%), as well as weak TLS protocols (38% vs. 35%).

Distribution of Most Negative Score Impact among Breached S&P 500 Members



The above figures suggest that Social Engineering, particularly via the exposure of employee information, has been an even more significant issue for breached S&P 500 members than it has been for the overall sample of companies, for which it also appears to be the dominant concern. The greater prevalence of Social Engineering issues among companies that actually were affected by incidents thus raises the question of what if any role actual social engineering tactics may have played in those incidents.

Qualitative Analysis of Incidents

Below are examples of incidents that affected S&P 500 members in 2023. We have selected those incidents that illustrate the above points or other lessons to learn about the current threat landscape and recent trends for such companies.

Social Engineering

The above quantitative analyses indicated that exposure of employee information was a key source of vulnerability to social engineering attacks. Previous compromises of companies are a potential source of employee PII for attackers to use for future social engineering purposes. For example, the food distributor [Sysco](#) experienced a compromise of employee PII in 2023. Another U.S. food distributor experienced [a phishing compromise](#) of employee email accounts that [exposed employee PII](#). Many of the other incidents below also involved the exposure of employee PII, so those companies may be more vulnerable to social engineering attacks in the future.

Websites and other public-facing infrastructure can become a source of information for use in social engineering attacks on employees and customers. For example, as of April 2023, attackers [had been abusing access to the publicly accessible shipment tracking service of UPS](#) to obtain contact information and other details for customers. The goal of obtaining this information (which UPS later prevented) was to find ways to contact potential targets and context with which to craft more credible phishing messages. One does not necessarily need to abuse access like that to obtain useful reconnaissance data. LinkedIn and other social media platforms are also useful sources of such data.

Third-Party Breaches and MOVEit

Many incidents affecting S&P 500 members in 2023 were third-party data breaches, rather than breaches of the companies themselves. The exact percentage of S&P 500 breaches attributable to third-party attack vectors was unclear, as many of the reports were ambiguous on this point. The reports with clearer details nonetheless provide qualitative insights into the circumstances that cause third-party breaches.

For example, [a data breach at law firm Bryan Cave Leighton Paisner LLP](#) compromised the PII of former and current employees of Mondelez Global, a client of that law firm. Charles Schwab informed some customers in June 2023 that [a third-party vendor whose services it had retained for customer service calls had gained unauthorized access to customer accounts](#).

Third-party breaches often involve providers of IT products and services, particularly software. SecurityScorecard researchers determined in recent research that **as many as three-quarters of all third-party breaches involved such technical vendors**; the other quarter of third-party breaches involved non-technical vendors, such as professional services firms. For example, Massachusetts **gas & electric utility Eversource** experienced a customer data breach via an unidentified vulnerability in software from CLEAResult, which provides software for utilities to monitor consumer energy efficiency. Similarly, **pilots for Southwest and another U.S. airline** experienced compromises of their personal information via a third-party pilot recruitment website in April 2023.

The **healthcare platform of a subsidiary of a major U.S. pharmaceutical company**, with over 1 million users as of 2022, had experienced a compromise of user/patient information via an unidentified technology vendor as of August 2023. The compromised data included PHI, such as conditions, medications, and health insurance details, as well as regular PII. It was not clear how the attackers compromised the unnamed third-party vendor, but the investigation suggested that they may have exploited a vulnerability or security misconfiguration.

A major U.S. bank experienced three separate third-party data breaches affecting its customers in 2023. A February 2023 compromise at **NCB Management services**, which manages accounts receivable, exposed information for some of that bank's credit card holders. **A separate November 2023 LockBit** ransomware attack on Infosys McCamish Systems exposed PII and financial details on approximately 57,000 customers of this bank.

One of the most prolific causes of third-party breaches last year was the exploitation of a zero-day vulnerability in MOVEit file transfer software (CVE-2023-34362), a product of Progress Software, by the criminal group C10p in May 2023. The above-mentioned major U.S. bank received services from tax, advisory, and consulting firm **Ernst & Young, one of the numerous direct victims of the MOVEit campaign**. The compromise of Ernst & Young exposed PII and financial details on approximately 30,000 customers of the above-mentioned U.S. bank.

Direct victims of the MOVEit campaign included other S&P 500 members, such as: **M&T Bank**, whose customer information was compromised; pharmaceutical company Bristol Myers Squibb, whose **employee PII was compromised**; **a major U.S. steel producer** whose employee PII and direct deposit details were compromised; **AutoZone**, an automotive parts retailer and distributor whose business details and employee PII were compromised; and **Gen, the owner of cybersecurity brands** like Norton, LifeLock, Avast, Avira, and AVG, whose employee information was compromised.

Another direct victim of the MOVEit campaign, **Pension Benefit Information (PBI Research)**, provides pension and other employee beneficiary monitoring services for other companies, including at least one S&P 500 member, to determine when beneficiaries have died and should stop receiving benefits. The MOVEit

compromise of PBI research exposed the PII of people receiving pension and other employee benefits from that S&P 500 member and other plan sponsors. [Yet another benefits-related victim of the MOVEit campaign, healthcare software provider Welltok](#), resulted in third-party breaches for its many customers. Welltok provided a platform for an S&P 500 company's employee benefits program, thus exposing the PII of its employee participants when the MOVEit campaign hit Welltok. In another healthcare-related third-party MOVEit breach, [the Colorado Department of Health Care Policy and Financing \(HCPF\)](#), which runs Medicaid in that state for 4 million patients, experienced a third-party breach via IBM. IBM had been using MOVEit to manage files for its HCPF customer.

Similarly, in June 2023, a [major U.S. healthcare organization](#) experienced a breach of patient data from an unspecified external storage location for lists that manage the automation of communications with patients, such as reminders to make appointments. The incident exposed patients' PII but not more sensitive details, like clinical, insurance, or payment information. The company's statement did not specify a third-party vendor for the compromised external storage location that the attackers compromised.

Third-party breaches can have U.S. national security implications if a compromised company does sensitive work for the U.S. Government. For example, a November 2023 compromise of [General Electric \(GE\) reportedly included files on the company's work for the Defense Advanced Research Projects Agency \(DARPA\)](#). The actor "IntelBroker" offered to sell these files for relatively cheap prices.

Ransomware

Ransomware attacks nowadays frequently include a threat to expose data to extort payment, in addition to or instead of the traditional encryption of files for ransom. S&P 500 Defense & aerospace company [Boeing was the target of such an attack by LockBit ransomware operators](#) in fall 2023. The sensitivity and U.S. national security implications of Boeing's defense and aerospace work makes companies like it more vulnerable to such extortion, if and when a compromise occurs.

It is nonetheless the disruptive potential of ransomware, both on targets themselves and their customers, that often has the greatest impact. Ransomware thus poses a significant supply chain risk. For example, [clothing manufacturer VF Corp.](#) predicted that its December 2023 ransomware attack would disrupt its ability to fulfill orders of its various clothing brands from retailers and wholesalers. Hard drive manufacturer [Western Digital](#) took its network offline in March 2023 in response to an incident, disrupting its regular business operations. Similarly, [a January 2023 ransomware attack on Yum! Brands](#), which owns restaurant franchise chains like KFC, Taco Bell, and Pizza Hut, forced the closure of some 300 branded restaurant locations in the U.K.

The disruptive potential of ransomware was clearer in two successive AlphV/BlackCat attacks on [a major U.S. medical supplier](#). The original October 2023 incident compromised the PII and PHI of approximately 29,000 employees and their dependents. Third-party compromises often expose a vendor's customers, but in this case, the breach exposed the bank account details of the companies' suppliers as well, which the attackers evidently tried to use for fraudulent purposes. The company indicated that [the downtime resulting from the incident would likely disrupt projected sales](#), leading the company to offer discounts to inconvenienced customers. The threat group [re-encrypted this company's files](#) in November 2023, just as the company had almost finished restoring them, due to a breakdown in ransom negotiations.

Ransom amounts have been trending upward for years. Ransomware operators often base their ransom demands in part on a company's size, in terms of both the number of employees and its monetary value (e.g. market capitalization or annual revenue). S&P 500 members should thus be prepared for high ransom demands. For example, ransomware operators demanded [\\$51 million USD](#) from manufacturer Johnson Controls. A major U.S. technology company tried to negotiate LockBit ransomware actors down from their initial demand of [\\$80 million USD](#). The actors offered a discount of as much as 50%, but negotiations nonetheless failed, as [the actors took offense at the technology company's much lower counter offer of \\$1.1 million](#), resulting in the leakage of data from the breached company.

Recommendations

Social Engineering

Security costs money; large security investments are a necessary but not sufficient condition of a strong security posture. Even those organizations that have invested vast sums in technical security solutions remain vulnerable to social engineering attacks that exploit human vulnerabilities to circumvent those technical defenses. Organizations that have already invested heavily in technical security measures may see better returns on future security investments by focusing more on their human vulnerability to social engineering. More extensive security awareness training for employees should be a high priority for organizations with already robust security programs. More specific measures should aim to mitigate the exposure of employee information, such as by monitoring for dark web data disclosures and by encouraging discretion and caution in the use of professional networking services and other social media.

Third-Party Cyber Risk Management

TPRM is a key component of a robust security program, as the third-party breaches affecting S&P 500 members last year illustrated. Providers of software and other IT products and services should be high priorities for such a program, but also consider other vendors with access to your data, such as law firms and other professional services providers. Your organization should immediately establish a TPRM program if it does not already have one, as the vetting and continuous monitoring of vendors can go a long way toward preventing third-party breaches. Many organizations may find it more cost-effective, or simply more effective in general, to outsource their TPRM to a managed service, such as SecurityScorecard's new **MAX** offering. In-house TPRM teams can also use SecurityScorecard's platform to evaluate prospective vendors and monitor existing ones for security issues that could enable third-party breaches.

Avoid the "One Size Fits All" Approach

In-house security programs, including any TPRM components, should be tailored to fit the distinctive challenges of their respective industries - which may vary considerably from one industry to another, as the above findings illustrated. For example, the relatively high frequency of breaches at S&P 500 Financial Services & Insurance companies, despite their relatively strong security measures, would benefit from a more mature threat intelligence program enabling them to stay one step ahead of more determined and resourceful adversaries willing to pursue harder targets. In contrast, organizations in more security-challenged industries, such as Healthcare, Life Sciences, and Medical Supplies, might benefit from more basic measures, such as establishing TPRM programs. Previous SecurityScorecard research indicated that organizations in this vertical suffer from **a uniquely complex and severe third-party risk environment** that accounts for many of the numerous incidents affecting this industry.

The Risks of Paying Ransoms

Ransomware is a top threat for S&P 500 members and can pose supply chain disruption risks for partners of those companies as well. Ransomware operators may view S&P 500 members as particularly valuable targets on the basis of their stocks' market value and demand accordingly high ransoms. Negotiating a ransom payment poses significant risks for victims, who should resist the temptation to simply make the problem go away faster by paying. The contrast in results between the ransomware attacks on MGM and Caesar's, the latter of which suffered less disruption as a result of its payment, may make this option seem logical. Nonetheless, paying ransoms does not guarantee a prompt resolution of the incident. Coding errors in ransomware may prevent file decryption. Unscrupulous ransomware operators might simply not bother to decrypt files, or they might sell compromised data despite promises to the contrary. Paying ransom marks victims as vulnerable to extortion and thus more desirable targets for future attacks. Breakdowns in negotiations, in which victims willing to pay in principle nonetheless balk at high ransom amounts, can also prompt retaliation by attackers. Ransom payments may also have legal implications, depending on your jurisdiction and other factors. Consult with an attorney before you consider negotiating.

To learn more and create
your free account, visit
SecurityScorecard.com

ABOUT SECURITYSCORECARD

Funded by world-class investors, including Evolution Equity Partners, Silver Lake Partners, Sequoia Capital, GV, Riverwood Capital, and others, SecurityScorecard is the global leader in cybersecurity ratings, response, and resilience, 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 25,000 organizations for enterprise risk management, third-party risk management, board reporting, due diligence, cyber insurance underwriting, and regulatory oversight.

SecurityScorecard makes the world safer by transforming how companies understand, improve, and communicate cybersecurity risk to their boards, employees, and vendors. SecurityScorecard achieved the Federal Risk and Authorization Management Program (FedRAMP) Ready designation, highlighting the company's robust security standards to protect customer information, and is listed as a free cyber tool and service by the U.S. Cybersecurity & Infrastructure Security Agency (CISA). Every organization has the universal right to its trusted and transparent Instant SecurityScorecard rating. For more information, visit securityscorecard.com or connect with us on [LinkedIn](#).



SecurityScorecard.com
info@securityscorecard.io