SecurityScorecard

SecurityScorecard Big 500 Index:

A Cybersecurity Analysis of 500 Major Publicly-Traded U.S. Companies

securityscorecard.com [800] 682 1707

SecurityScorecard

Overview

With cyber crime-related costs to hit $6 trillion annually by 2021[1] and continued high-profile breaches in news headlines, more and more organizations fear that one cyber-attack can suddenly put a stop to the growth and profitability of the company–and large companies like those within the S&P 500 are no exception.

To take a look at some of the S&P's cybersecurity practices and to get a pulse on some pervasive cybersecurity threats, SecurityScorecard scanned 500 large companies representative of the S&P 500[2] from March to August 2017 and ran three kinds of analyses.

First, this "Big 500," viewed as its own industry, was compared to 18 U.S. industries to determine the group's relative cybersecurity performance, looking at overall scores and performance for specific risk factors. Second, we looked inside the Big 500, breaking the group down by industry to reveal cybersecurity insights. Third, we took a deep dive into the patching cadence behaviors of the Big 500, looking at the group's overall performance and then looked at performance by industry.

1 http://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics-for-2017.html
2 See Methodology Section for more information.

SecurityScorecard

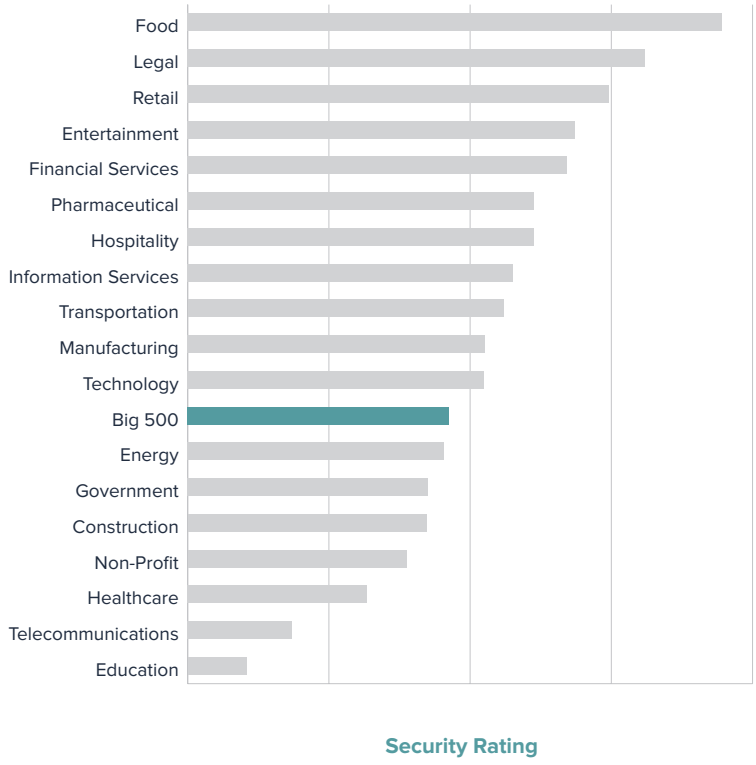
Key Insights from SecuurityScorecard:

- The Big 500 ranked 12th when compared to 18 other U.S. industries in overall cybersecurity performance.
- Seventy percent of top performers exhibited a lack of due diligence regarding patching cadence.
- There were more than 100 million issues related to patching cadence found in the Big 500 in a span of just five months in 2017.
- Within the group, pharmaceutical companies, financial services companies, and construction companies were the worst patching practice offenders.
- The three most common patching issues found within the group were:
    - Medium risk Common Vulnerability Exposures (CVE)s detected within attributed corporate IP space
    - Services that had reached End of Life date detected within attributed corporate IP space
    - Products that had reached End of Service dates detected within attributed corporate IP space

SecurityScorecard

The Big 500's Cybersecurity Performance Overall Based on SecurityScorecard's Analysis

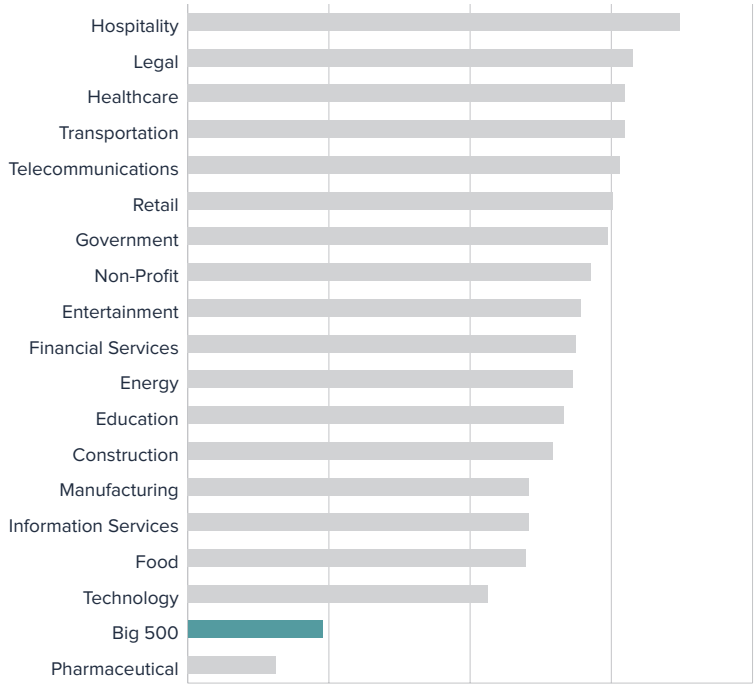
When viewing the 500 large companies as their own group and comparing it to 18 major U.S. industries, the Big 500 ranked 12th.



On a factor level, companies within the Big 500 scored poorly in Password Exposure, Hacker Chatter, and Social Engineering.

SecurityScorecard

A Closer Look at Password Exposure



Password Exposure scores are a reflection of the degree to which employees at companies within the Big 500 have had their email:password combinations exposed and circulated within the hacker underground. Furthermore, the ISC-CERT released an advisory earlier this year that identified compromised administrative credentials as a top vector of attack across all industries.[3] This score is in part based on the user credential data discovered in hacker chatter and from identified credential sets within publicly released archives. A low password exposure score can indicate a user's credentials have been leaked via a third-party breach and are actively being circulated within the hacker underground. This can leave these credentials at risk for unauthorized use and thus poses a massive threat to the cybersecurity of the organization–81 percent of data breaches are caused by a hacked password.[4]

Furthermore, this risk is magnified by the fact that a significant number of individuals will use the same "secure and complicated" password for all their services, unaware that a single breach of a third-party plaintext database will open the door to all of their resources. The situation is further exacerbated given that less than 1% of users will change their passwords or password management behavior even *after* they have been notified of a data breach.[5]

3 https://www.us-cert.gov/ncas/alerts/TA17-117A
4 2017 Verizon Data Breach Investigations Report (DBIR)
5 https://www.defcon.org/images/defcon-17/dc-17-presentations/defcon-17-matt_weir-sudhir_aggarwal-cracking_passwords.pdf

SecurityScorecard

A Closer Look at Social Engineering

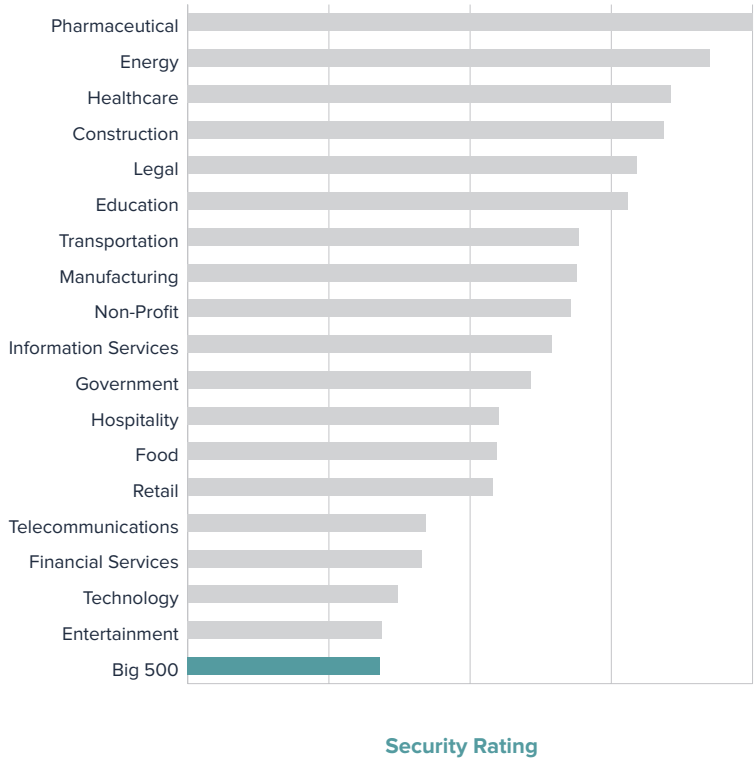
When compared to 18 major U.S. industries, the Big 500 scored the lowest in social engineering. This data point is calculated through cross referencing all discovered email addresses from corporate entities with social networks to discover active accounts that may exist using corporate assets. For example, if someone creates a Facebook, LinkedIn, Flickr or Amazon account with their corporate email address, they are at a higher risk for an out-of-band spear phishing attack that may originate through these third-party networks. Additionally, all discovered email addresses are compared against circulating bulk email marketing lists to determine the likelihood of incoming unsolicited mail/spam attempts.

Organizations are already spending large amounts of time to cope with and prevent social engineering attacks. In fact, a recent presentation at Black Hat revealed that 34 percent of IT security personnel surveyed spent the greatest amount of time dealing with issues like phishing, social network exploits, or other forms of social engineering.[6] With the attack surface estimated to reach four billion people by 2020[7], improving employee cybersecurity awareness to help foster early identification of social engineering attacks will only become increasingly important.

6 Black Hat Europe. Dark Reading Session. "Effects of Compliance and GDPR on IT Security Department." 5 Dec 2017.
7 http://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics-for-2017.html

SecurityScorecard

A Closer Look at Hacker Chatter



A hacker chatter score is based on the frequency with which companies in the Big 500 have had their domains, company names, or IP addresses mentioned within underground hacking forums. A low score in hacker chatter in this case indicates that the organizations within this group are mentioned more frequently than when compared to the other U.S. major industries.

SecurityScorecard

S&P Highlights Potential Ramifications of Poor Cybersecurity Health

Earlier this year, the S&P[8] acknowledged that cybersecurity attacks can have a negative impact on a business by introducing credit risk–citing the loss of future revenue as just one example of how these attacks can have negative impacts on the management, liquidity, or operations criteria of credit risk.

With this acknowledgment of cybersecurity risk, the S&P also advocated four risk management practices:

1. the hardening of systems and backups,
2. identifying vulnerabilities,
3. establishing policies and training employees on them, and
4. testing the policies and the systems for weaknesses.

While these action items will go a long way to mitigate a significant portion of risk, the importance of **continuous security monitoring** across all four domains is critical to success.

Hardening, backups, vulnerability research, employee training, and security testing must be continuous to keep up with the ever-changing landscape of modern emerging threats and identify vectors of risk before they are exploited.

8 http://www.pionline.com/article/20170320/PRINT/303209989/sampp-warns-institutions-on-cybersecurity

SecurityScorecard

SecurityScorecard's Look at the Top 20 Cybersecurity Performers

The top performers in terms of cybersecurity health were as follows:

Company	Total Score	Application Sec	Cubit Score	DNS Health	Endpoint Security	Hacker Chatter	IP Reputation	Network Security	Password Exposure	Patching Cadence	Social Engineering
Aerospace and Defense Company	A	A	A	A	A	A	A	A	A	B	A
Healthcare Provider	A	A	A	A	A	A	A	A	A	B	A
Professional Services Company	A	A	A	A	A	A	A	A	A	A	A
Healthcare Provider	A	A	A	A	A	A	A	A	A	B	A
Energy Company	A	A	A	C	A	A	A	A	A	A	B
Aerospace and Defense Company	A	A	A	B	A	A	A	A	A	A	A
Energy Company	A	A	A	B	A	A	A	A	A	B	A
Food Manufacturer	A	B	A	B	A	A	A	A	A	A	A
Retailer	A	A	A	C	A	A	A	A	A	A	A
Drink Manufacturer	A	A	A	C	A	A	A	A	A	A	A
Real Estate	A	B	A	B	A	A	A	A	A	A	A
Mining Company	A	B	A	B	A	A	A	A	A	A	A
Manufacturer	A	A	A	B	A	A	A	A	A	A	B
Energy Company	A	A	A	A	B	A	A	A	A	A	A
Brewing Company	A	A	A	C	A	A	A	A	A	A	A
Energy Company	A	A	A	B	B	A	A	A	A	A	B
Gas Corporation	A	A	A	A	A	A	B	A	A	A	A
Insurance Company	A	A	A	C	A	A	A	A	A	A	C
Real Estate	A	A	A	B	A	A	A	B	A	B	A
Energy Company	A	A	A	B	A	A	A	B	A	A	A

The above analysis revealed that:

- One of four companies in the Top 20 Cybersecurity Performers are energy companies.
- Seventy percent of top performers show poor patching cadence.
- Only 10 percent of the top providers were healthcare companies.

SecurityScorecard

SecurityScorecard Analysis Reveals Poor Patching Practices Across the Big 500

After software is deployed, vulnerabilities are often found and publicly disclosed. To fix these issues or bugs (or, in other cases, to improve functionality), software vendors release patches regularly. Patching cadence is a measure of how quickly organizations apply available security patches over the period of the scan.[9] The longer it takes for an organization to implement security patches, the longer window of time an attacker has to successfully leverage an attack from the time of vulnerability disclosure.

On average, companies within the Big 500 received a factor grade of C in patching cadence, indicating room for improvement in patching practices and threat management programs of most companies. There were 117,653,451 unique issues related to patching cadence impacting the Big 500.

Companies are frequently slow to implement updates, whether for improved function or security controls, as the updates are considered untested code releases that may impact the production environment. In other words, sometimes updates break things - and large companies can be very cautious and slow to implement a patch. Attackers take this opportunity and try to exploit as much as possible, knowing the enterprises can be slow to apply security patches.

Slow patching cadence is generally an indicator of a lack of engineering resources to implement an available fix, a lack of engineering resources to deal with the overhead of additional efforts that may emerge as a byproduct of the fix, a lack of awareness regarding the existence of the vulnerability and patches, or a combination of all of the above.

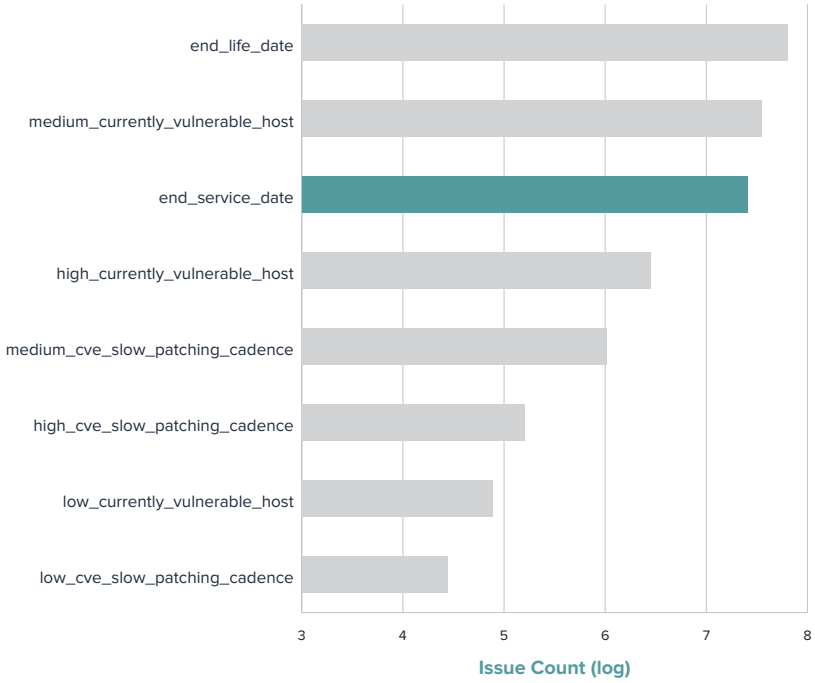
In addition to maintaining a frequent patching schedule for critical assets, it is equally important to monitor the emergence of newly released vulnerabilities and CVE vectors. Considering that 80 percent of attacks use vulnerabilities for which patches already exist[10], staying on top of emerging CVEs is a needed step for success. CVEDetails.com is a trusted, public, and free repository of continuously updated CVE information that can be used as a resource to facilitate these efforts.

9 https://arstechnica.com/information-technology/2015/09/mit-is-tops-in-bad-security-at-major-universities/
10 http://www.computerweekly.com/news/450421649/Security-Think-Tank-Patching-is-vital-and-essentially-a-risk-management-exercise

SecurityScorecard

Most Common Patching Cadence Issues

SecurityScorecard broke down all the patching cadence issues by type and found that the two most common patching issues in the Big 500 were:



- Medium risk Common Vulnerability Exposures (CVE)s detected within attributed corporate IP space. The risk definition is based on the NIST CVSSv2 calculation of the identified CVE, which consider ratings of 4.0 - 6.9 in the "Medium" risk range.[11] [12]
- Services that had reached "End of Life or End of Service" dates detected within attributed corporate IP space. End of life or end of service means that the software or hardware is no longer being supported by manufacturers.[13] In the case of hardware, this means components will no longer be replaced, and in the case of software, this means no further patches will be released for public vulnerabilities or for functionality improvements.[14] Common examples include: Windows XP, Office 10, and Blackberry OS.[15]

11 https://nvd.nist.gov/vuln-metrics
12 https://nvd.nist.gov/vuln-metrics/cvss/v2-calculator
13 http://www.zoginc.com/old-computers-are-security-risks/
14 https://its.ny.gov/sites/default/files/documents/russel_kiernan_compatibility_mode.pdf
15 https://securityscorecard.com/blog/end-of-life-cybersecurity-infographic/

Both pose an increased risk to an organization's cybersecurity posture. The prolific availability of medium risk CVEs indicates to attackers that not only is the enterprise slow to implement available security fixes - The EOL/EOS allows hackers to more easily develop exploits for these assets, as they operate with the knowledge that patches will not be released.[16] In fact, over half of breached organizations have EOL/EOS devices–a proofpoint of how much of a risk EOL/EOS assets can cause.[17]

Being continuously aware of the assets within an organization and the end of life or end of service dates of those assets is an important step in proactive risk mitigation, not to mention compliance against standards, such as PCI DSS.

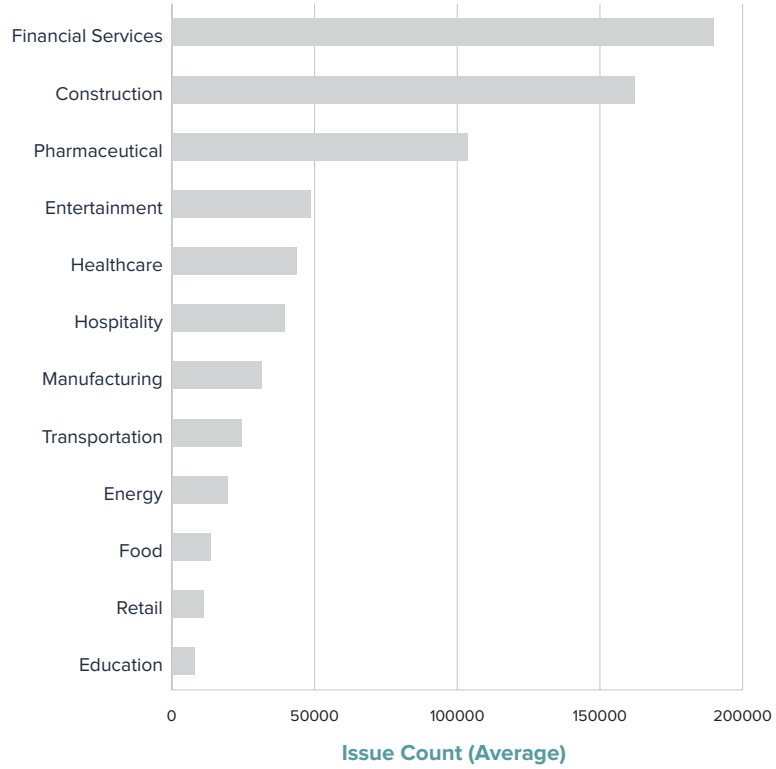
16 https://its.ny.gov/sites/default/files/documents/russel_kiernan_compatibility_mode.pdf
17 https://securityscorecard.com/blog/end-of-life-cybersecurity-infographic/

SecurityScorecard

Spotlight on Patching Issues Within the Big 500

Taking a closer look within the Big 500, pharmaceutical companies, financial services companies, and construction companies were the worst patching practice offenders.*

Overall Number of Patching Issues by Industry Within the Big 500



*Technology, telecommunications, and information services were excluded from this graph, because these types of companies can contain the IP addresses of their customers in some instances.

Across all industries, on an issue level, areas of cybersecurity weakness were distributed as displayed in the table below:

Top Three Patching Cadence Issue Types by Industry Within the Big 500

Industry	End of Life	End of Service	Medium Currently Vulnerable Host	High Currently Vulnerable Host	Medium CVE Slow Patching
Construction	2	3	1		
Education		3	1		2
Energy	2		1		3
Entertainment			1	2	3
Financial	1	2			3
Food	2		1		3
Healthcare	2	3	1		
Hospitality	2		1		3
Information Services	1	3	2		
Manufacturing	2		1		3
Pharmaceutical	2	3	1		
Retail	3		1		2
Telecommunication	1	2			3
Technology	1	3			2

Our research demonstrates that while there may be some variation in how patching issues present themselves across industries within the Big 500, the threat of an inattentive approach to patching is pervasive across industry types.

The same is true of the impact: While energy or infrastructure companies face more acute risk associated with business interruption and financial service companies may face a greater fallout from loss of customer trust or brand, cyberattacks pose a multifaceted threat to a company's earnings regardless of industry.[18] This explains why companies–within and outside of the Big 500–are investing more time, budget, and resources into combating cyberthreats.

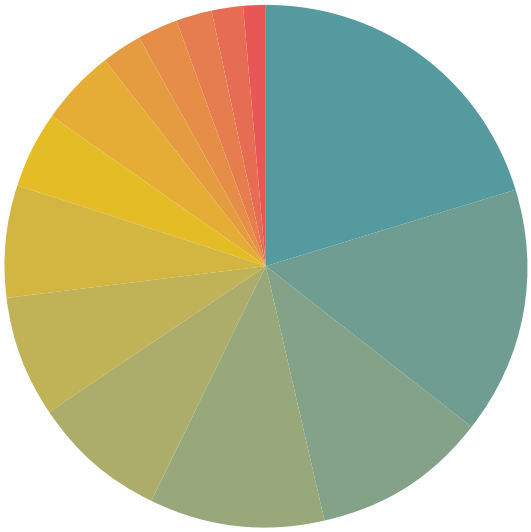
18 https://www.thestreet.com/story/14215631/1/it-s-time-companies-start-spending-big-on-cybersecurity-jim-cramer-reveals-top-trades.html

SecurityScorecard

Methodology of SecurityScorecard's Analysis

The Sample

SecurityScorecard evaluated 500 companies between March and August 2017. The companies evaluated for this "Big 500" cohort were representative of companies that are, have been, or are similar to companies in the S&P 500 (referred to as the "Big 500"). The distribution of companies is as follows:



Industry Composition of the Big 500 Sample

- Manufacturing 20.2%
- Finance Services 15.1%
- Energy 11.1%
- Retail 10.7%
- Technology 8.5%
- Information Service 7.5%
- Healthcare 6.9%
- Food 4.8%
- Pharmaceutical 4.6%
- Transportation 2.6%
- Construction 2.4%
- Entertainment 2.2%
- Telecommunications 1.8%
- Hospitality 1.4%
- Education 0.2%

Important Definitions and Explanations

Throughout the report the term "Big 500" throughout the report is solely intended to refer to the group described in the Sample section above. S&P has made no representations or been involved in any way in the production of this report.

For a detailed explanation on "issues," "factors," and "overall score," please download our Scoring Whitepaper.

SecurityScorecard

About SecurityScorecard

SecurityScorecard helps enterprises gain operational command of their security posture and the security posture of their third-parties through continuous, non-intrusive monitoring. The company's approach to security focuses on identifying vulnerabilities from an outside perspective, the same way a hacker would. SecurityScorecard's proprietary SaaS platform offers an unmatched breadth and depth of critical data points including a broad range of risk categories such as Application Security, Malware, Patching Cadence, Network Security, Hacker Chatter, Social Engineering, and Leaked Information.

To receive an email with your company's current score, please visit instant.securityscorecard.com.

www.securityscorecard.com

1 (800) 682-1707

info@securityscorecard.com

@security_score

SecurityScorecard HQ

214 West 29th St

5th Floor

New York City, NY 10001