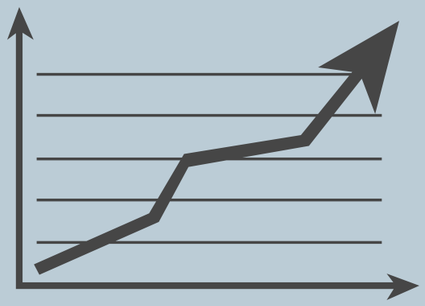
2020 Credential Breach Report

PREPARED BY
NORMSHIELD

INTRODUCTION

Credentials (usernames and passwords) are keys to an organization's confidential information and employees are the key holders. Often, employees use the same password for all logins associated with corporate email addresses.



Cybercriminals know about this lack of cyber awareness of employees. Threat actors attack well-known forums, IT tools, social network platforms, etc. to obtain user credentials and search for corporate email addresses.

We have seen billions of corporate-related credentials in several leaks* occur in 2019. We detected credentials related to the top 20 organizations in 20 industries for this research.

This report outlines breached credential trends in 2019, industry-specific insights, and best practices for protecting credentials and preventing future breaches.

BREACHED CREDENTIALS KEY FINDINGS

336
out of 400 organizations exposed

Among the 400 organizations investigated, for 84% (336) of them, there are at least 50 credentials that include their corporate email addresses.

Almost 3
billion breached credentials

NormShield investigated almost 3 billion breached credentials exposed in 2019 related to 400 organizations covered in this study.

845k
breached university credentials

The top 20 ranked universities had more than 800,000 credentials shared in 2019, the highest number among the 20 industries analyzed.

100%
of top 20 healthcare orgs exposed

Additionally, 95% of organizations in the higher education, technology, and law sectors had at least 50 breached credentials.

Weaponization of breached credentials

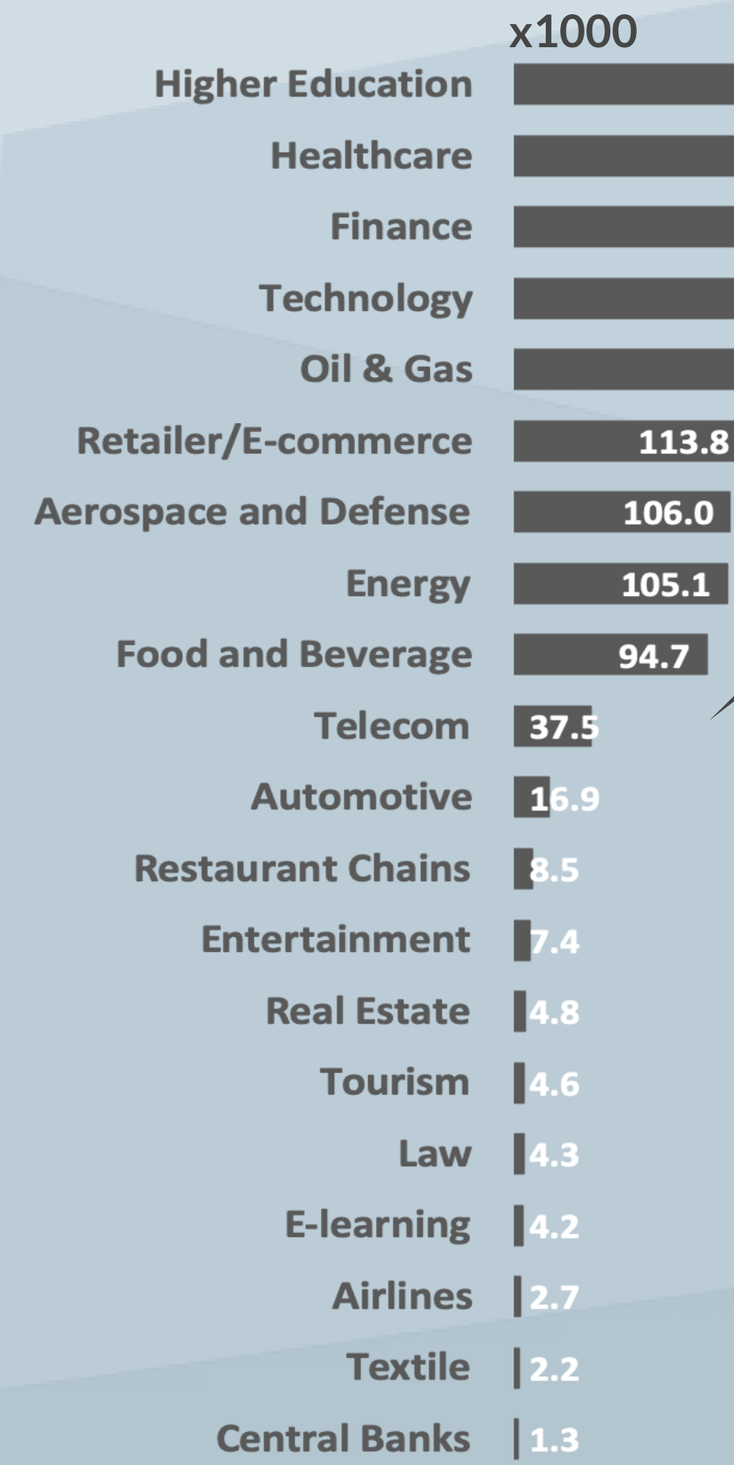
On January 25, 2019, the popular video-sharing platform DailyMotion shared news about a cyber attack that reads:

"The attack consists of “guessing” the passwords of some DailyMotion accounts by automatically trying a large number of combinations, or by using passwords that have been previously stolen from web sites unrelated to DailyMotion.”

This is the very definition of a **credential-stuffing attack**. Besides Daily Motion, Sky (a British telecom company), Dunkin' Donuts, and the insurance company State Farm also experienced credential-stuffing attacks in 2019.

With such attacks, cybercriminals can get into web applications and crack open databases that include sensitive information. Disastrous effects of credential-stuffing attacks include increased security cost, loss revenue downtime, remediation costs and fees, as well as customer mistrust and churn.

Number of breached credentials by industry



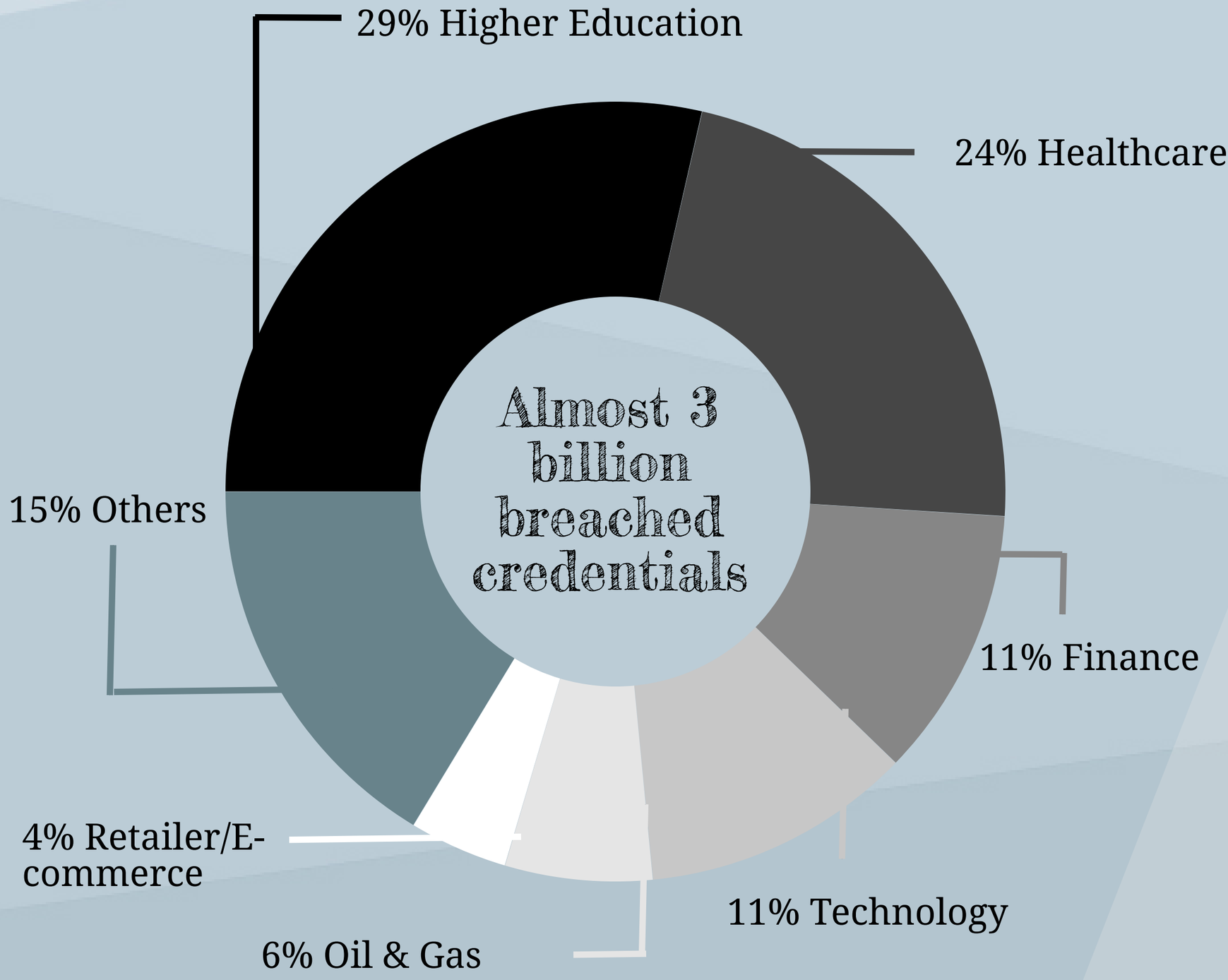
It is expected that universities would experience the highest number of breached credentials, considering that they provide university e-mail addresses to their students.

The high number of breached credentials may give hackers access to patient information and healthcare providers may face serious fines regulated by HIPAA.

Even though both financial institutions and technology companies invest heavily in cybersecurity, these numbers show that a serious number of employees still use corporate e-mail addresses in non-business places, an act which jeopardizes their companies' security.

The companies in these categories are also at great risk of credential-stuffing attacks due to high number of berached credentials.

Half of breached credentials in 2019 belonged to universities and healthcare providers

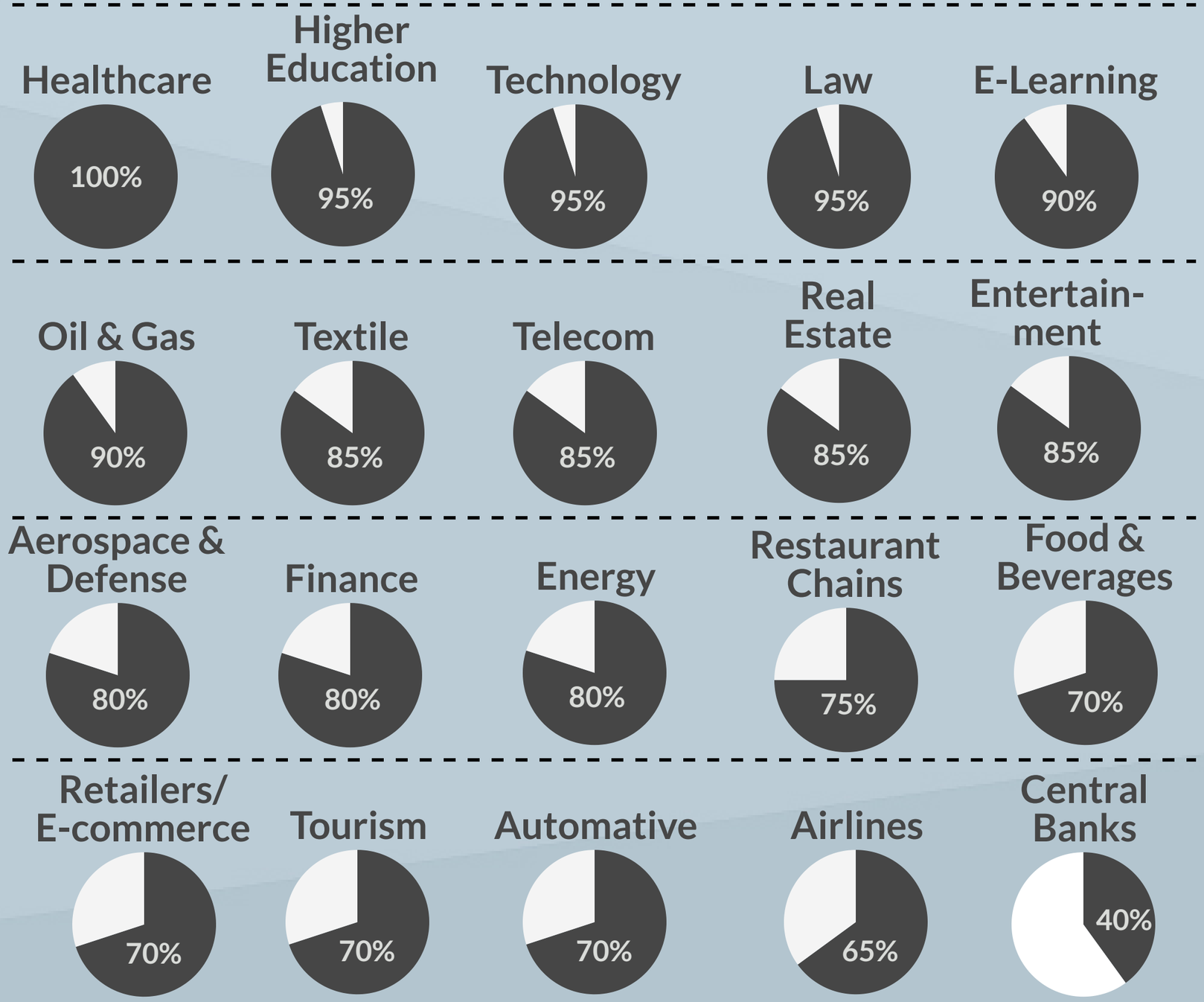


84% of organizations have at least 50 breached credentials per organization

Out of 400 organizations analyzed in this study, **336 organizations** had at least 50 credentials breached in 2019.

Not all the top organizations had credentials breached

Ratio of organizations with at least 50 breached credentials shared in 2019



For each industry, we explored the number of organizations that had breached credentials.

For the top 20 organizations in all industries except Central Banks, more than two-thirds had breached credentials.

In some industries, such as healthcare, higher education, technology, law, and oil & gas, the ratio of top organizations with breached credentials was more than 90%.

Simple steps to prevent credential breaches

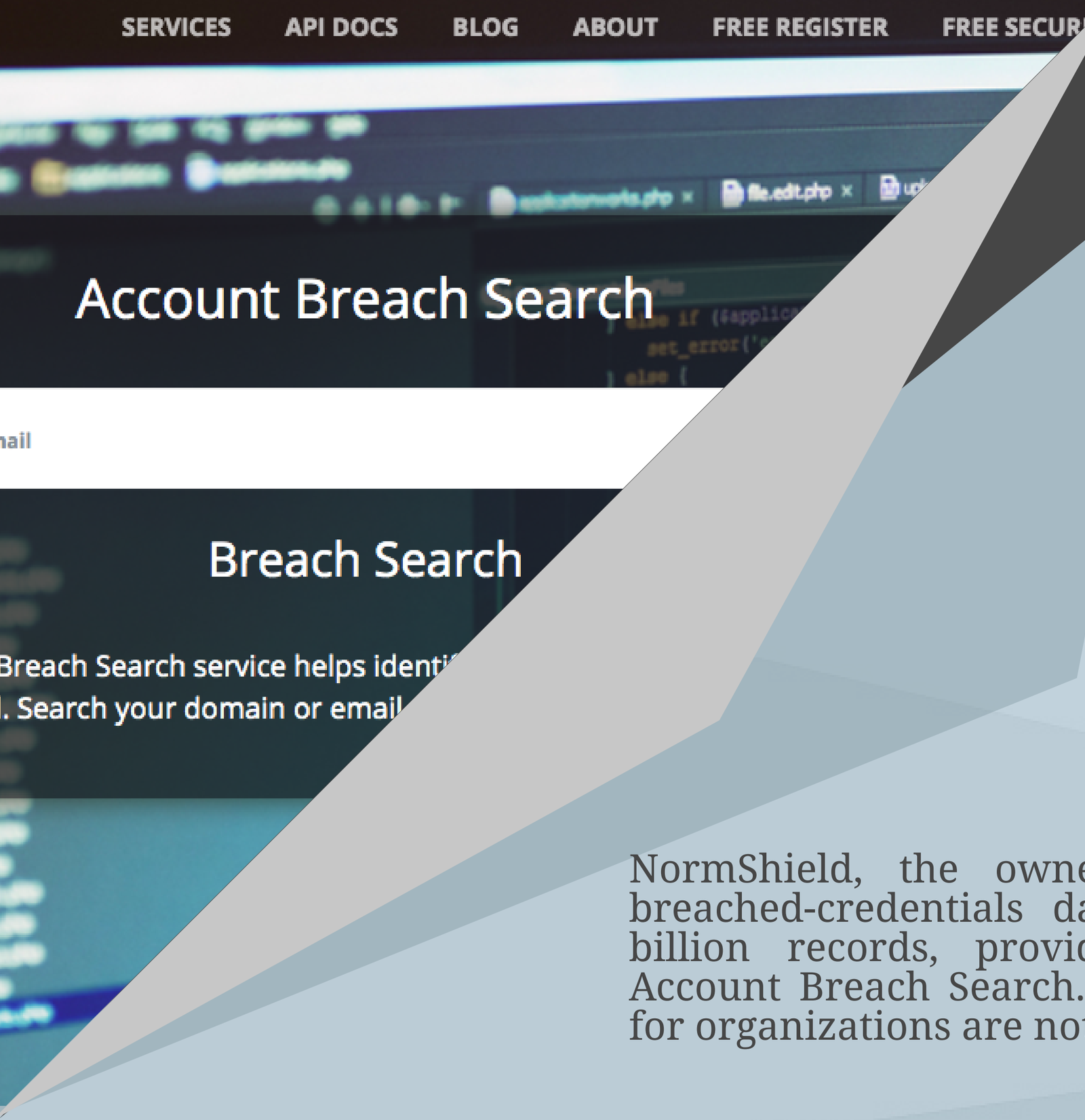
1. **Your organization's password security policy should include two-factor or multi-factor authentication**

2. **Based on these policies, passwords should be changed at least quarterly**

3. **Employee training**

   - **Do not use corporate credentials for personal use, such as social media, online purchasing, etc.**
   - **Use different, distinct passwords for business, personal, and banking**

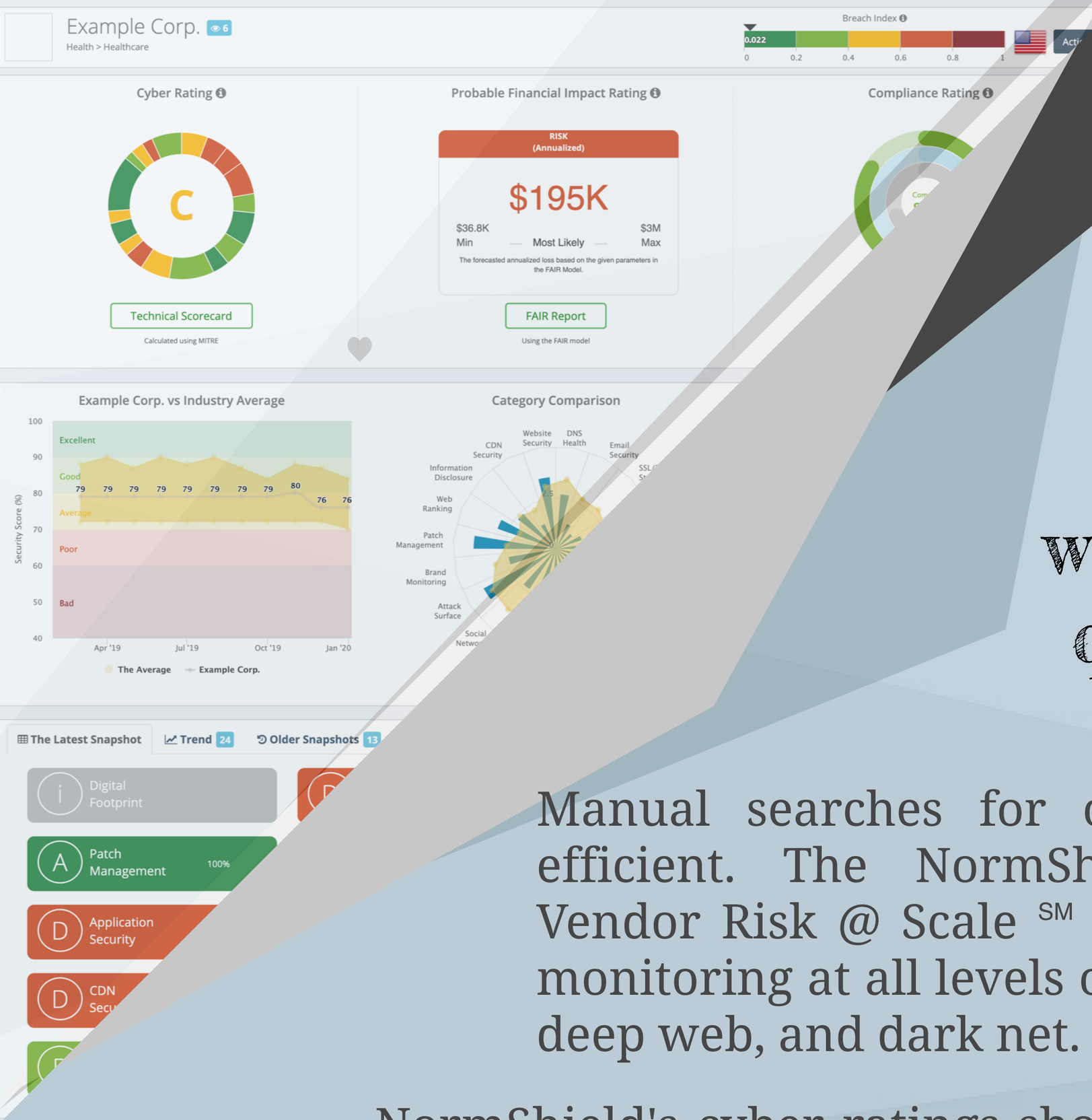
4. **Monitor credential breaches**



How to monitor breached credentials

NormShield, the owner of one of the largest breached-credentials database with more than 7 billion records, provides a free service called Account Breach Search. However, manual searches for organizations are not efficient.

Organizations need more effective monitoring in a broader sense.

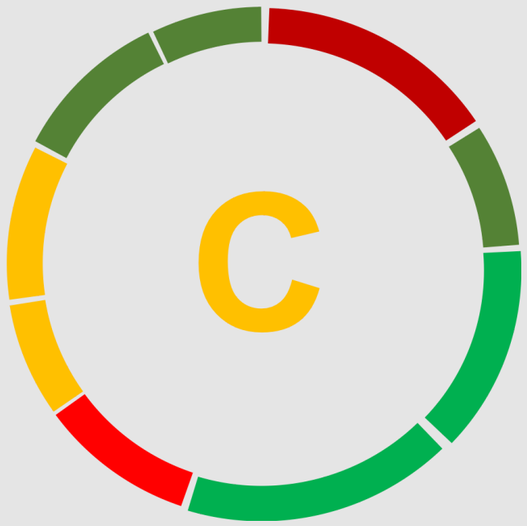


Effective monitoring with cyber risk quantification

Manual searches for organizations are not efficient. The NormShield provides a 3D Vendor Risk @ Scale [SM] approach that enables monitoring at all levels of the internet: surface, deep web, and dark net.

NormShield's cyber ratings show the leaked or hacked credentials that were discovered and provide a cyber risk quantification for a company and its vendors.

3D Vendor Risk @ Scale SM



Cyber Rating

Perform non-intrusive cyber risk assessments of any third party. Get technical score with easy-to-understand letter grades and drill down into technical details in each risk category.

Probable Financial Impact Rating

Use the FAIR model to calculate the probable financial impact if a cyber event were to occur at a third party in order to cost-effectively achieve and maintain an acceptable level of loss exposure.

Compliance Rating

Correlate findings to industry standards and best practices. Measure any third party's compliance with regulations like NIST 800-53, ISO27001, PCI-DSS, HIPAA, GDPR, and Shared Assessments.

Request a free Cyber Risk Assessment

www.normshield.com

info@normshield.com

8609 Westwood Center Dr.
Ste 110, Vienna, VA 22182

+1 (571) 335-0222

@normshield

/company/normshield

References

(*) The breaches analyzed in this study are gathered from public sources, hacker forums, and deep web sites; and they have been obtained via propriety methods that include automatic crawlers and manual gathering. The breaches include massive breaches such as Collection #1 - #5, Pastebin Leaks, Zynga breach, Canva breach, and big data dumps of hundreds of online services.

To see the references for selection of Top 20 organizations for each industry, click on the industry name:

Healthcare	Oil & Gas	Finance	Tourism
Higher Education	Entertainment	Aerospace and Defense	Retailer/E-commerce
Technology	Telecom	Energy	Automative
Law	Real Estate	Restaurant Chains	Central Banks
E-Learning	Textile	Food & Beverages	Airlines

Notes:

(1) Universities are selected by academic rankings.

(2) Central banks are selected from G20 countries.

(3) All the other categories are selected by market value.