flare

Executive Report

Clear Insights from a Deep Analysis of Dark Web Leaked Credentials

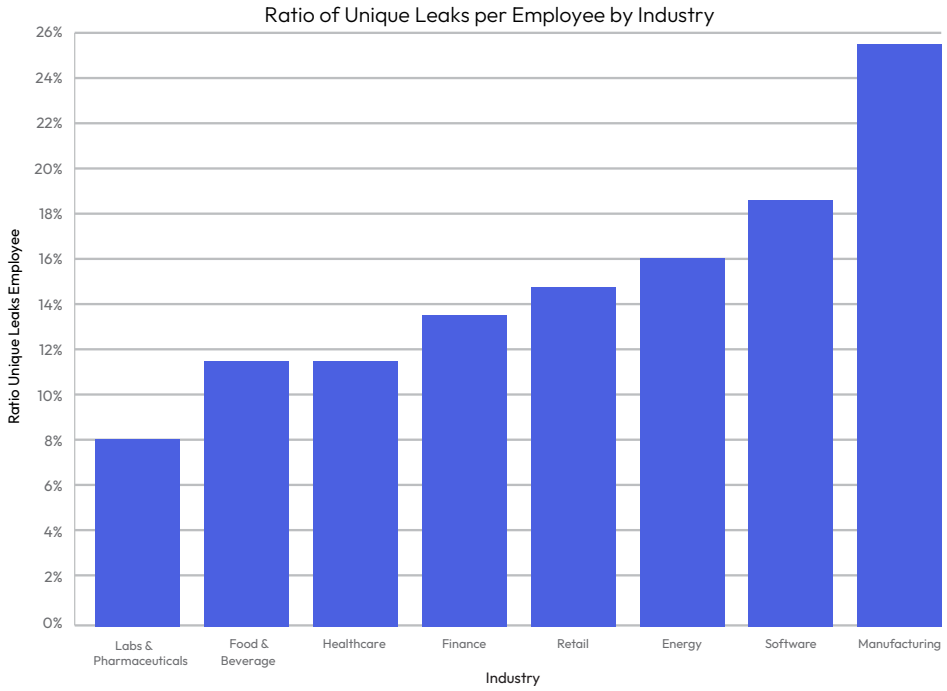
https://flare.systems

Executive Overview

Stolen credentials continue to represent the primary means of compromise for the majority of data breaches and cyberattacks. The number of leaked credentials on the dark web has also expanded considerably, approaching over 10 billion unique username password combinations once duplicates and combo lists have been removed. This report explores stolen credentials for sale on the dark web across 8 industries ranging from organizations we have defined as mid-sized (500-1,000 employees), large (1,000-5,000 employees), and enterprise (5,000+ employees).

Highlights

- Across almost all industries, the ratio of leaked credentials per employee **decreased as the size of the organization increased**. We believe this was likely due to improvements in security maturity for larger organizations and increasing separation of roles and responsibilities as organization size increased, resulting in fewer unique logins.
- The industry with the highest ratio of stolen credentials for sale on the dark web was Manufacturing, the lowest was Labs & Pharmaceuticals.
- On average, 43% of employees working at mid-sized companies had leaked credentials on the dark web, 19% of employees at large companies, and only 4% of employees at enterprise companies **with an average of 22% across all industries and sizes**.
- Password reuse discovered in 3 or more separate data breaches was common. An average of 2.3 employees per organization across all industries and sizes was discovered to have reused passwords that were discovered in 3 distinct data breaches.



The Anatomy of a Credential Leak

Before diving into the details of the methods and findings of this research, we'll explain how credentials (usernames and passwords) are stolen, and then how they are resold, shared, and used by malicious actors on the dark web and illicit communities more broadly.

Currently the most common way malicious actors steal credentials is through phishing emails targeting organizations which hold thousands, hundreds of thousands, or even millions of credentials. Threat actors attempt to gain access to sensitive networks and then move laterally through the organization to steal data, distribute ransomware, and escalate privileges. The data is then exfiltrated and either posted for free or sold on various marketplaces across the dark and clear web.

Another method for threat actors to steal credentials is through exfiltrating from the domain controller by **cracking**. This is less common compared to phishing attacks. Once they exfiltrate credentials, they can use them themselves in order to gain increased access, or sell them on a dark web marketplace, give them away on a forum, or even post them publicly on a file sharing site.

Types of Stolen Credentials

There are several types of credential leaks:

Named Leak: Named leaks are one of the most well known ways to group stolen credentials. This is the initial file or group of files that the malicious actor has stolen from an organization with username/passwords for each employee. So for instance, this could include all of the usernames and passwords stolen from an organization.

Collection: Often over time credentials quickly lose value after the initial compromise and essentially become free. In many cases, threat actors will build "collections" of leaks from multiple independent data breaches, then either give these away to build reputation or resell them.

Combo Lists: Combo lists are curated lists of victims that have had their usernames and passwords leaked from multiple sources. These lists are often only a few hundred to a few thousand sets of credentials. They are organized by groups like geographic region, industry, top-level domain (like .edu, .org), and more. This enables threat actors to take a very targeted approach to credential stuffing, often using open-source intelligence to augment data from breaches and identify applications and services that are most likely to be used by the victim.

Infected Device Marketplaces: These are marketplaces selling access to browser fingerprints where the victims computer was infected with stealer malware. These fingerprints often contain dozens to hundreds of logins that the victim has saved in their browser and if they come with cookies and active sessions, threat actors can potentially bypass MFA controls.

The Details

This research analyzed leaked credentials from various different angles including organization size, industry, country, and more.

Methodology:

Flare took a random sample of between 100 and 200 companies for each sector and divided them by size into medium-sized organizations (500-1,000 employees), large organizations (1,000-5,000 employees), and enterprise organizations (5,000+ employees). We then searched across dark web marketplaces, illicit Telegram channels, and illicit clear web sites to identify unique credentials for sale. We excluded collections and combo lists to ensure that we were counting unique instances and not identifying duplicates.

We then analyzed the data based on company size and industry as mentioned based on 3 primary criteria. We included the following industries: Energy, Manufacturing, Software, Retail, Finance, Food & Beverage, Healthcare, and Labs & Pharmaceuticals. We excluded the Education sector due to the prevalence of students using emails ending in their organization's domain.

The Ratio of Leaked Credentials Per Employee: We determined this metric by comparing the exact number of employees at a company to the number of users with identifiable leaked credentials for sale. For example if Acme Inc. has 10,000 employees, and we found 500 unique instances of credentials leaks with person@acmeinc.com, that ratio would be described as .05 or 5%.

Repeat Offenders: This metric describes the average number of employees at an organization that have 3 or more unique instances of credentials leaked. For example, we did not label someone a repeat offender who had 2 separate sets of credentials leaked, or whose credentials showed up in the same leak in 2 different instances.

Severe Repeat Offenders: This metric measures the average number of employees who were repeat offenders (their credentials were present in 3 or more distinct leaks) and used the same password across all accounts present in the leak (for plaintext leaks).

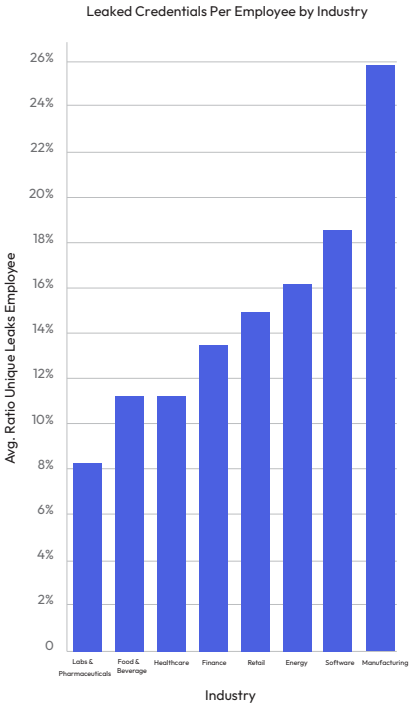
The Ratio of Leaked Credentials Per Employee by Country: This measure was the ratio of leaked credentials per employee divided by countries. We included over 650 companies across more than 40 countries in our large organization (500-5000) employee parameter.

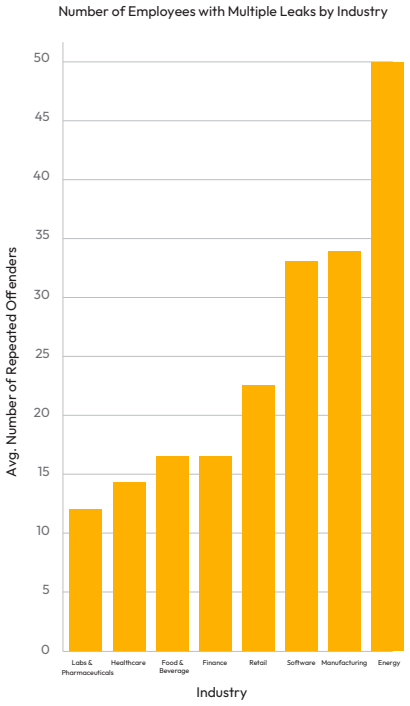
Repeat Offenders	
Industry	
Energy	149.6
Manufacturing	101.3
Software	98.5
Retail	67.6
Finance	49.2
Food & Beverage	49.1
Healthcare	43.0
Telecommunications	35.9
Labs & Pharmaceuticals	35.8

What We Found that Surprised Us

There were a few unexpected findings in our analysis of the data that are worth mentioning. We were surprised by the prevalence of credential leaks at software companies. Generally speaking, we found that the higher level of security maturity an organization had (measured by number of employees and industry security expenditure), the **less** credentials we would find for sale or leaked.

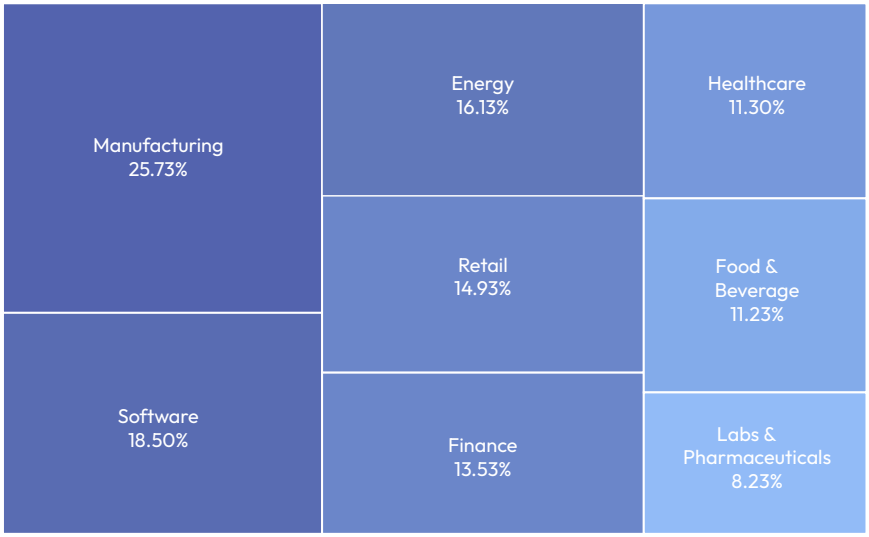
However, the Software category was a surprise. According to a 2020 report by Gartner, the category of "Software Publishing and Internet Services" commensurate with our category Software **had the highest security spend expressed as a percentage of total information technology budget**. We believe this is likely due to the prevalence of heavy IT/Technical users at software development companies. If an employee uses their credentials for dozens, or even hundreds of logins across third-party sites and software, the sheer prevalence of potential logins will outweigh the increased level of security maturity due to security spending.





We were also surprised that Energy led by average number of repeat offenders per organization followed by Manufacturing and Software. While Software companies still ranked in the top 3, the lower security maturity, security training, and general end-user security knowledge found in other industries likely outweighed the risks associated with the large number of accounts an average software company employee would use.

Software, Energy, and Retail eclipsed Manufacturing for the average number of Severe Repeat Offenders per organization. We theorize that this may be a result of the lower average number of third-party SaaS and website logins that employees in the Manufacturing sector may have compared to their counterparts in other industries.



Average Number of Leaked Credentials expressed as a percentage of employees by Industry Regardless of Size

What We Found that did not Surprise Us

Organization Size and Leaked Credentials

We expected that as organizational size increased that the ratio of leaked credentials per employee would decrease. The results of our study confirmed this hypothesis. We believe that there were several causes including:

- Individuals at smaller organizations likely have to "wear more hats" and perform a larger variety of work, leading to increased usage of SaaS applications and logins across more websites.
- Smaller organizations generally have lower security maturity than larger organizations and often lack third-party risk management programs. This could result in more smaller organizations having less rigorous security programs.
- Enterprise organizations often have lists of approved vendors and applications that employees can use, severely limiting the number of unique log-ins that an average enterprise user will have compared to a smaller organization user.

Industry and Leaked Credentials

We were also not surprised to see Energy, Retail, and Manufacturing towards the top of our list of industries with the highest proportion of leaked credentials per employee. According to Gartner, those industries on average have a lower ratio of security spend when compared to industries such as Healthcare and Financial Services.

English and Leaked Credentials

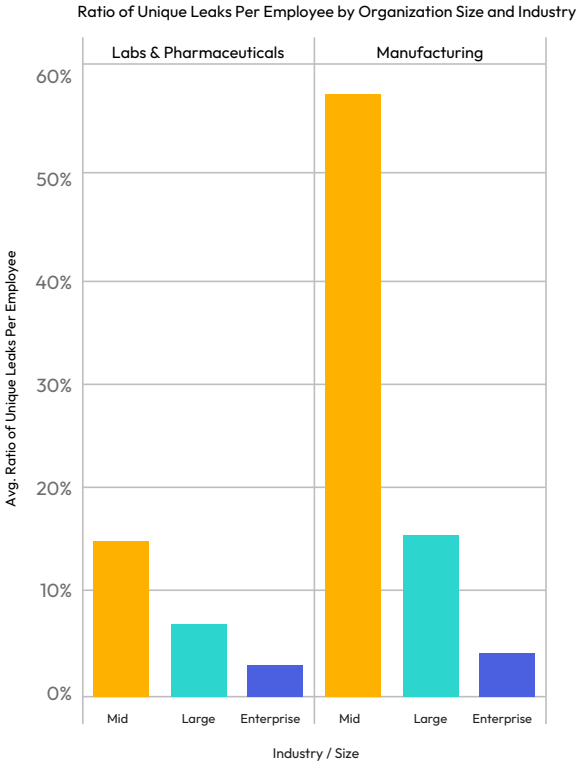
We were also not surprised to find that predominantly English speaking countries tended to have some of the highest ratios of leaked credentials per employee. We theorize that this may be the result of English being one of the most spoken languages in the world, enabling threat actors who also speak English to launch campaigns against predominantly English speaking countries.

We also suspect that the market for credentials and information in English is likely to be more lucrative, since there is a larger "target market" for threat actors to sell credentials to, compared to a set of credentials for a platform in a less spoken language. We theorize that credentials to a Japanese platform may be, on average, less valuable since there are fewer threat actors who could use this language efficiently.

Also, the U.S. led amongst developed countries in the percentage of employees with leaked credentials on the dark web. This did not surprise us, as American organizations are often targeted because of state sponsored motives and financial reasons.

Stolen Credentials and Healthcare - An Interesting Case

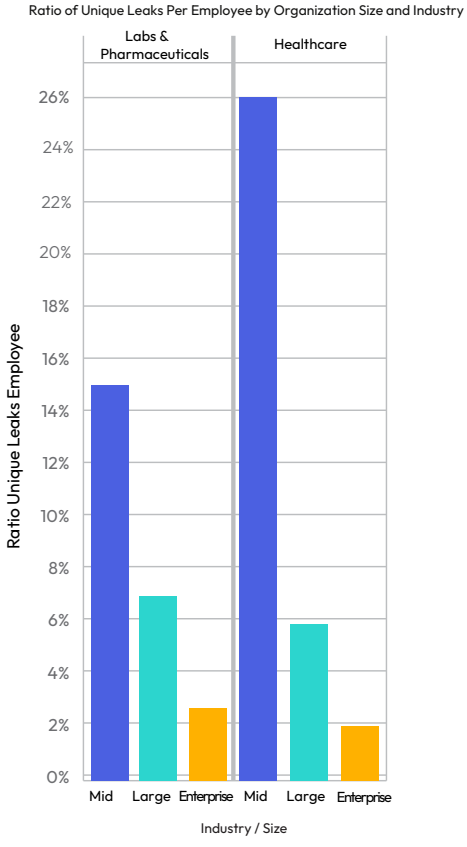
This chart provides another compelling view of just how stark the differences between industries is. Here we compare Labs & Pharmaceuticals with Manufacturing, the industry with the **lowest proportion of employees that have leaked credentials on the dark web**, with Manufacturing on the right is the industry that has the **highest proportion of leaked credentials on the dark web**. There are a few things that stand out here, such as the incredible difference between mid-sized Manufacturing organizations and mid-sized Labs & Pharmaceuticals.



We explain this as largely a result of the differences in security maturity for mid-sized Labs & Pharmaceuticals companies when compared to mid-sized Manufacturing companies. By default, healthcare organizations dealing with PHI (Personal Health Information) are required under the HIPAA Security Rule to take certain measures to safeguard patient data, likely beyond the security controls that the average mid-sized manufacturing organization would employ. In addition, Labs & Pharmaceuticals companies are also likely to have extremely valuable intellectual property to protect that mid-sized Manufacturing companies may lack.

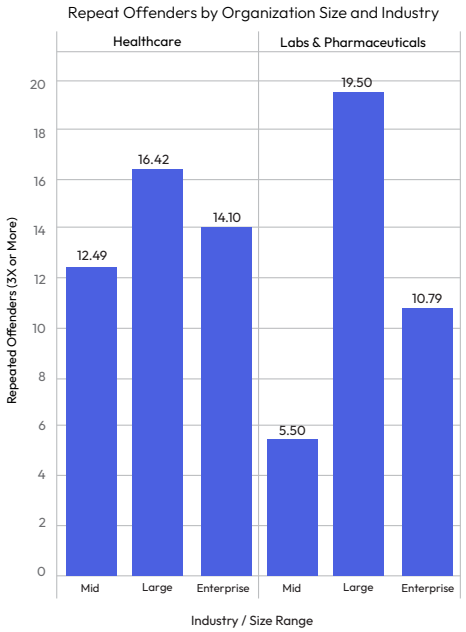
Labs & Pharmaceuticals	Mid	15.00%
	Large	7.00%
	Enterprise	2.70%
Manufacturing	Mid	57.70%
	Large	15.40%
	Enterprise	4.10%

One of the most interesting pieces of data is how the gap in average unique credentials leaked per employee narrows between the 2 industries as the organizations increase in size. The average mid-sized Manufacturing organization has 284% more leaked credentials per employee than the average mid-sized Labs & Pharmaceuticals company. However, the difference narrows when we compare large Manufacturing companies to large Labs & Pharmaceuticals companies. Compared to their mid-sized counterparts, Manufacturing organizations categorized as large only have 120% more credentials for sale than their Labs and Pharmaceuticals counterparts, while enterprise Manufacturing companies only have a 34% decrease compared to their Healthcare peers.



Another interesting data point emerges when we compare Labs & Pharmaceuticals, to Healthcare, which includes hospitals and elderly care facilities. Mid-sized Healthcare providers suffer disproportionately higher numbers of stolen credentials for sale compared to their Labs & Pharmaceuticals counterparts. However as the size of the organization increases, this trend reverses with enterprise Labs & Pharmaceuticals companies suffering comparatively higher ratios of leaked credentials when compared to Healthcare provider organizations. We thought it would be interesting to see if this trend held true across 2 of our other variables, Repeat Offenders and Severe Repeat Offenders.

The results of this analysis were quite surprising. In line with our expectations, we found that the average Healthcare organization has more credential leaks than the average Labs & Pharmaceuticals organization.



However, contrary to our expectations, we found that enterprise Labs & Pharmaceuticals organizations had 3 times as many data breach appearances for the average employee than in Healthcare organizations.

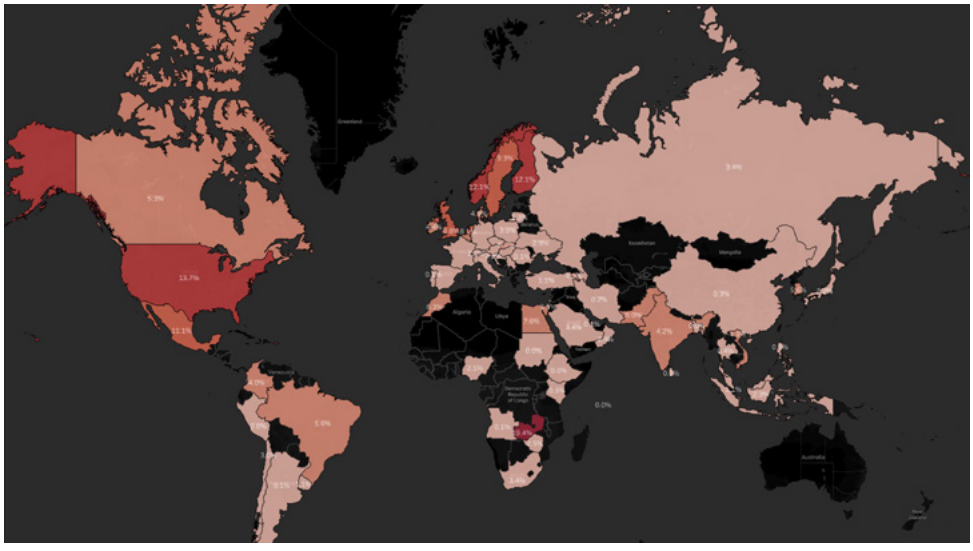
While mid-sized and large Healthcare companies had significantly more instances of triple credential leaks than their Labs & Pharmaceuticals counterparts, this trend was flipped on its head for enterprise organizations. Enterprise Labs & Pharmaceuticals companies had significantly more employees with instances of triple credential exposures on average.

Leaked Credentials and Geography

One of our most surprising findings was that the ratio of leaked credentials by employee **per country** did not seem to correspond at all to security maturity. While we found that the by-industry and by-size comparisons generally corresponded with security maturity, we found that by-country did not. We generally expected countries with lower levels of security maturity would experience higher ratios of leaked credentials, but this was not the result. When excluding outliers, the United States and Nordic countries ranked in the top 5 for leaked credentials per employee, while countries that spend far less on cybersecurity both nominally and as a percentage of GDP came in far lower.

We theorize that English speaking countries, and those that use English as a common business language are more targeted by malicious actors. English is spoken and understood by over 1 billion people worldwide and is by far the most commonly studied language in the world.

The reason for the exceptionally high percentage of leaked credentials may occur in countries that often use English for business purposes is that those companies have relatively high levels of GDP per capita and numerous multinational companies. The United States, Norway, Sweden, and the U.K. are homes to several multinational conglomerates worth hundreds of billions of dollars. The larger and more established the organization, the more likely it is considered valuable enough to try and break into.



United States	13.67%
Finland	12.11%
Norway	12.10%
Mexico	11.10%
Sweden	9.27%
United Kingdom	8.80%
Netherlands	8.14%
Egypt	7.57%
Morocco	6.25%
Slovakia	6.22%
Brazil	5.59%
Korea, Republic of	5.59%
Canada	5.29%
Pakistan	4.97%
Denmark	4.92%
Armenia	4.87%
Belgium	4.70%
Ireland	4.43%
Viet Nam	4.27%
India	4.22%
Colombia	4.00%
Poland	3.54%
Israel	3.50%
South Africa	3.44%
Russian Federation	3.42%
Germany	3.39%
Saudi Arabia	3.36%
Bahrain	2.95%

How Serious are Leaked Credentials?

When discussing leaked credentials, phishing attacks, and other forms of potential compromise on the dark web, many CISOs and other security practitioners will respond that while no program is perfect, they feel comfortable with their existing controls. This is typical for those who have a suite of security platforms set up and have implemented MFA across all corporate accounts. Leaked and stolen credentials are a huge issue, causing up to 50% of data breaches and costing companies hundreds of millions of dollars per year.

Unfortunately, malicious actors already have numerous means to bypass 2FA and MFA controls. Having MFA is **certainly better than not**, but counting on it as the catchall for when other controls fail is not a sound plan.

For information on your organizations leaked credentials on the dark web, and how they compare to others, use our leaked credential monitoring tool.

Recommendations

Leaked credentials can be costly and dangerous, but there are ways to improve your organization's password hygiene and security practices. Being informed is the first step to stronger cybersecurity.

1. **Compare your organization's ratio of leaked credentials to your industry average**.
   If your ratio is higher than the average, review your current security practices to improve your employees' password hygiene. Make sure to implement MFA. If your ratio is lower than the industry average, keep tracking it to see how it evolves.

2. **Provide additional training to Repeat Offenders**.
   Cybersecurity is a collaboration, so take a constructive approach rather than a penalizing one.

3. **For Software organizations, be aware that there are more potential exposures with your digital footprint than others**.
   Take precautions to adjust your organization's level of protection to match this increased level of risk. When comparing with peers in other industries, keep in mind that MFA is critical since your employees can have a bigger digital footprint.

4. **For Energy or Manufacturing organizations, be aware that your employees may be significantly reusing passwords**.
   Provide training and awareness on safe password management practices.

About Flare Systems

Flare is the proactive external cyber threat detection solution for organizations. Our AI-driven technology constantly scans the online world, including the dark and clear web, to discover unknown events, automatically prioritize risks and deliver actionable intelligence you can use instantly to improve security.

Want to learn about how Flare can support dark web monitoring for leaked credentials?

Free Trial **Book a Demo**

flare.systems
hello@flare.systems