State of Cybersecurity Industry Exposure at Dark Web

Tuesday, September 8, 2020 By Application Security Series

97% of the leading cybersecurity companies have had their data exposed on the Dark Web in 2020, with over 160,000 high or critical incidents that may jeopardize their clients.

Table of Content

Introduction

Last year, we conducted and published several exploratory researches welcomed by international media and the global cybersecurity community:

- State of Cybersecurity at Top 100 Global Airports

- State of Stolen Credentials in the Dark Web from Fortune 500 Companies
- State of Application Security at S&P Global World's 100 Largest Banks

In light of the rapidly growing sophistication and quantity of cyber-attacks targeting trusted third-parties in the last 12 months, and following a number of requests and suggestions from our valued clients and partners, we decided to run exploratory research on the global cybersecurity industry to illuminate and measure its exposure on the Dark Web in 2020.

A survey by the Ponemon Institute says that 59% of companies had a data breach due to compromised third parties including cybersecurity vendors. Recent research, published in July 2020 by Digital Shadows, estimates that there are over 15 billion stolen records from over 100,000 data breaches currently available for sale.

A few weeks ago, a report from Malwarebytes suggested that Working From Home (WFH) causes a surge in security breaches. To better understand the multifaceted challenge, Forrester provides an insightful report on how insiders use the Dark Web to sell corporate data.

This research purports to help better understand the emerging risks and modern threat landscape both in qualitative and qualitative aspects, and to help cybersecurity companies better prioritize and address emerging cyber risks.

Key Findings

Below are the key findings about the leading global cybersecurity companies:

- 97% of companies have data leaks and other security incidents exposed on the Dark Web
- 631,512 security incidents were found whereas 160,529 are of a high or critical risk levels
- 29% of stolen passwords are weak, employees from 161 company reuse their passwords
- 5,121 records with professional emails come from hacked porn or adult dating websites
- 63% of the cybersecurity companies' websites do not comply with PCI DSS requirements
- 48% of the cybersecurity companies' websites do not comply with GDPR requirements
- 91 companies had exploitable website security vulnerabilities, 26% are still unfixed

Covered Cybersecurity Companies

We tried to make our sampling of global cybersecurity companies as representative, reasonably diversified and inclusive as possible to ensure generalizability of the findings.

For the purpose of this research, we compiled our list of the leading cybersecurity companies around the globe from the following independent sources:

- Crunchbase - Attendees of RSA Conference 2020 – 546 companies
- SecurityTrails - Top 100+ Best Security Companies in 2020 – 419 companies
- Cybersecurity Ventures - the Hot 150 Cybersecurity Companies – 150 companies
- The Manifest - Top 100 Cybersecurity Companies – 126 companies
- OWASP - Corporate Sponsors and Supporters – 78 companies

In total, we collected 1,319 cybersecurity companies and organizations. After the removal of duplicates from the list, we ended up with 1,040 entities.

Then we removed all entities that cannot be classified as a cybersecurity company (e.g. organizations like NIST or global companies like Panasonic whose involvement in cybersecurity business is insignificant).

We also removed all companies with an Alexa Rank above 500,000 to ensure that only sufficiently large companies remain in the research.

Finally, we ended up 398 cybersecurity companies headquartered in 26 countries. Unsurprisingly, most of them are domiciled in the US and Europe:

HQ Country	**Number of Companies**
USA	294
United Kingdom	20

HQ Country	Number of Companies
Israel	16
Canada	14
Japan	11
Germany	7
Ireland	5
India	4
Russia	3
Switzerland	3
Finland	2
Singapore	2
China	2
Romania	2
Taiwan	2
Belgium	2
France	2
Czech Republic	1
Slovakia	1
The Netherlands	1
Spain	1
Malta	1
Italy	1
Portugal	1

We used company size classification provided by LinkedIn. The following company sizes figure among the 398 cybersecurity companies:

Number of Employees	% of Companies
10,001+	11%
5,001-10,000	5%
1,001-5,000	9%
501-1,000	13%
251-500	17%

Number of Employees	% of Companies
101-250	21%
51-100	13%
11-50	11%

We also used annual income classification provided by CrunchBase. The following are estimated annual revenues figures among the 398 cybersecurity companies:

Estimated Annual Revenue	% of Companies
$10B+	1.7%
$1B to $10B	7.3%
$500M to $1B	2.8%
$100M to $500M	11.2%
$50M to $100M	12.4%
$10M to $50M	23.6%
$1M to $10M	27%
Less than $1M	14%

Data Sources and Methodology

For the purpose of this research, we unified the concepts of Dark Web, Deep Web and Surface Web and jointly refer them as Dark Web.

To search for and identify security incidents available on the Dark Web, we leveraged our free online test to discover and classify Dark Web exposure of the 398 cybersecurity companies described above.

The test is based on our proprietary OSINT technology enhanced with Machine Learning (see below). Here is a non-exhaustive list of various resources where we gather data about the incidents:

- Hacking Forums
- Underground Marketplaces
- IRC and Telegram Channels
- Public Code Repositories
- WhatsApp Groups
- Social Networks
- Paste Websites

The earliest security incident dates back to 2012, while the most recent one is of August 31, 2020.

Anomalies, such as surprisingly large or small number of incidents per company, were manually validated to ensure data consistency and accuracy.

It is important to mention the growing “noise” on the Dark Web, ranging from outdated or duplicative data leaks to overt fakes sold by scammers. To tackle this challenge, we leverage and continuously improve our proprietary Machine Learning (ML) models to distil the findings. For instance, we have a specially trained ML model capable of differentiating between humanly created and automatically generated passwords. We also have many other ML models that detect various “red flags” suggesting that the data, its advertised quality or date of breach, or the seller do lack basic trustworthiness and ascertainably. In this research, findings that did not trigger any red flags are referred to as **verified**, while others are labelled as **unverified**.

Below is the estimated risk scoring for the **verified incidents** used by our free test and in this research:

- **Critical Risk:** login credentials with plaintext passwords, or data leaks with highly sensitive data (e.g. PII, financial records, etc.) that are recent and/or unique
- **High Risk:** login credentials with plaintext passwords, or data leaks with highly sensitive data (e.g. PII, financial records, etc.)
- **Medium Risk:** login credentials encrypted passwords, or various data leaks with moderately sensitive data (e.g. source code, internal documents, etc.)

- **Low Risk:** mentions of organization, its IT assets or employees in data leaks, samples or dumps without accompanying sensitive or confidential information.

All incidents described and classified below are the verified ones.

How to Reproduce the Findings

The findings can be reproduced just by entering a company's main website URL into the free test and seeing the results.

The free test provides an exact number of security incidents with estimated risk scores but does not reveal technical details of the incidents for ethical and legal reasons.

Organizations looking to receive full details of the incident may consider using ImmuniWeb® Discovery to get the exposed data without these restrictions.

Incidents Overview

The total number of discovered incidents in the Dark Web for the 398 cybersecurity companies is 1,658,907 whereas 38% (631,512) are verified incidents (see above):

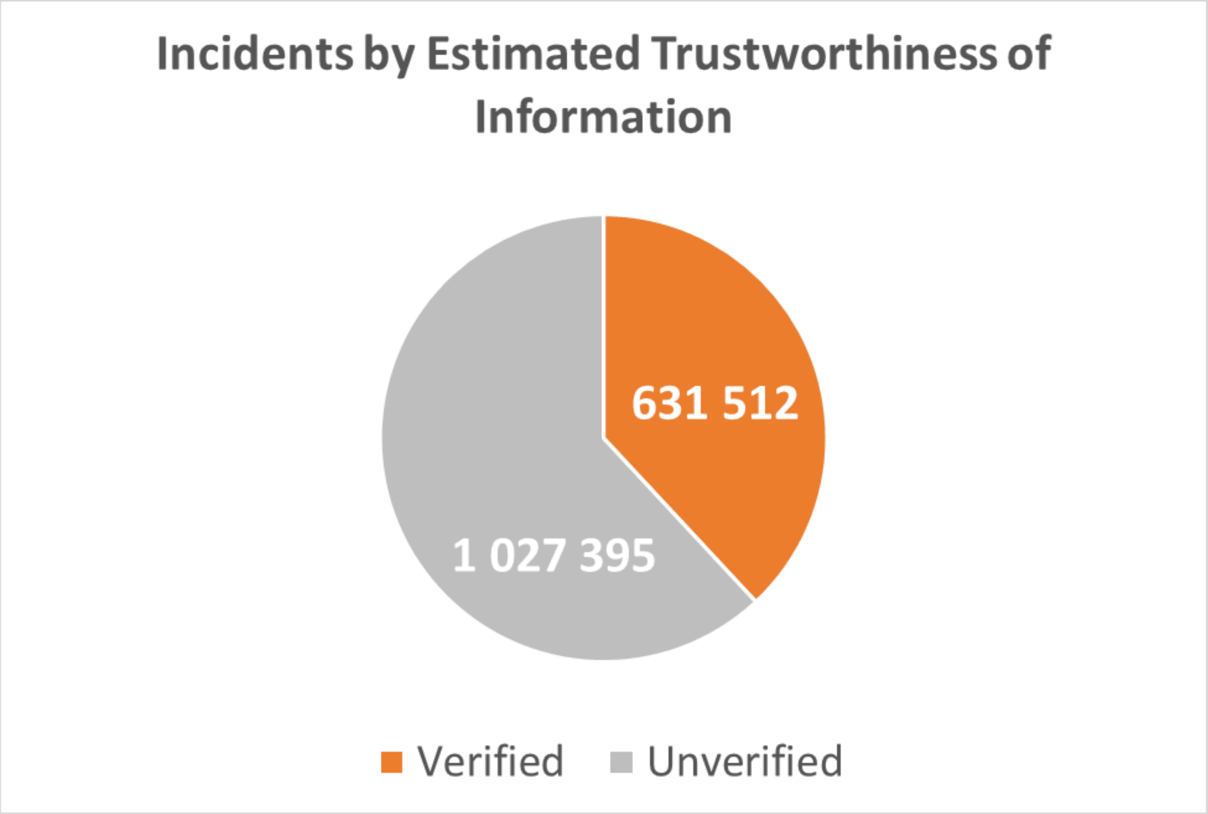

Diagram 1: Incidents by Estimated Trustworthiness of Information

Incidents by Estimated Risk Level

The graph below illustrates the allocation of incidents by the estimated risk level (see above). Among the verified incidents, almost 17% (109,019) have estimated critical risk, 8% have estimated high risk (51,510), 49% are of estimated medium risk (311,521) and 25% have estimated low risk (159,462):

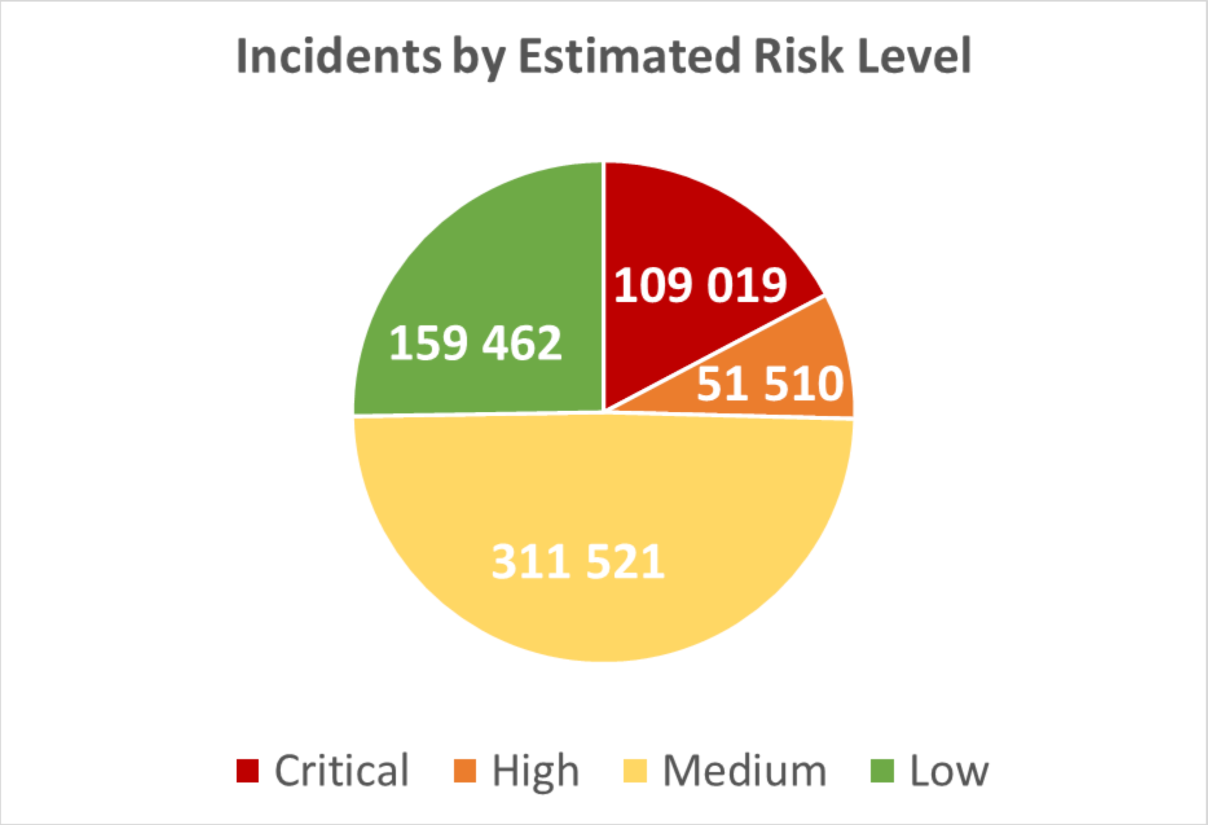

Diagram 2: Incidents by Estimated Risk Level

Incidents by Exposed Data Types

631,512 records contain highly sensitive information such as plaintext credentials or PII including financial or similar data. Hence, on average, there are 1,586 stolen credentials and other sensitive data exposed per cybersecurity company. Generalized classification of leaked data from the incidents is illustrated in the graph below:

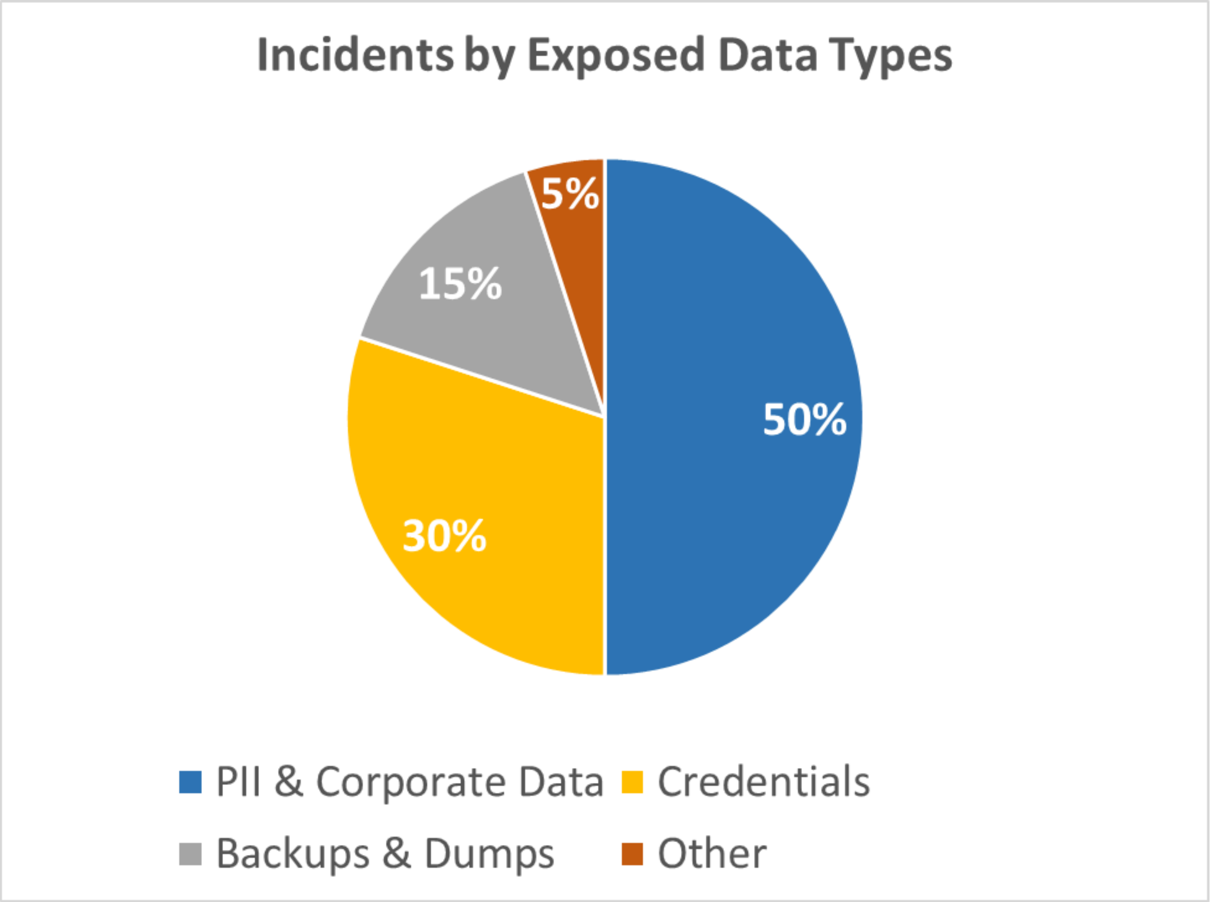

Diagram 3: Incidents by Exposed Data Types

Incidents by Leaked Passwords Strength

We automatically analyzed the strength of leaked passwords for the Credential Theft incident types described above. 29% of the passwords were weak (i.e. less than 8 characters, no uppercase, no numbers and no special characters):

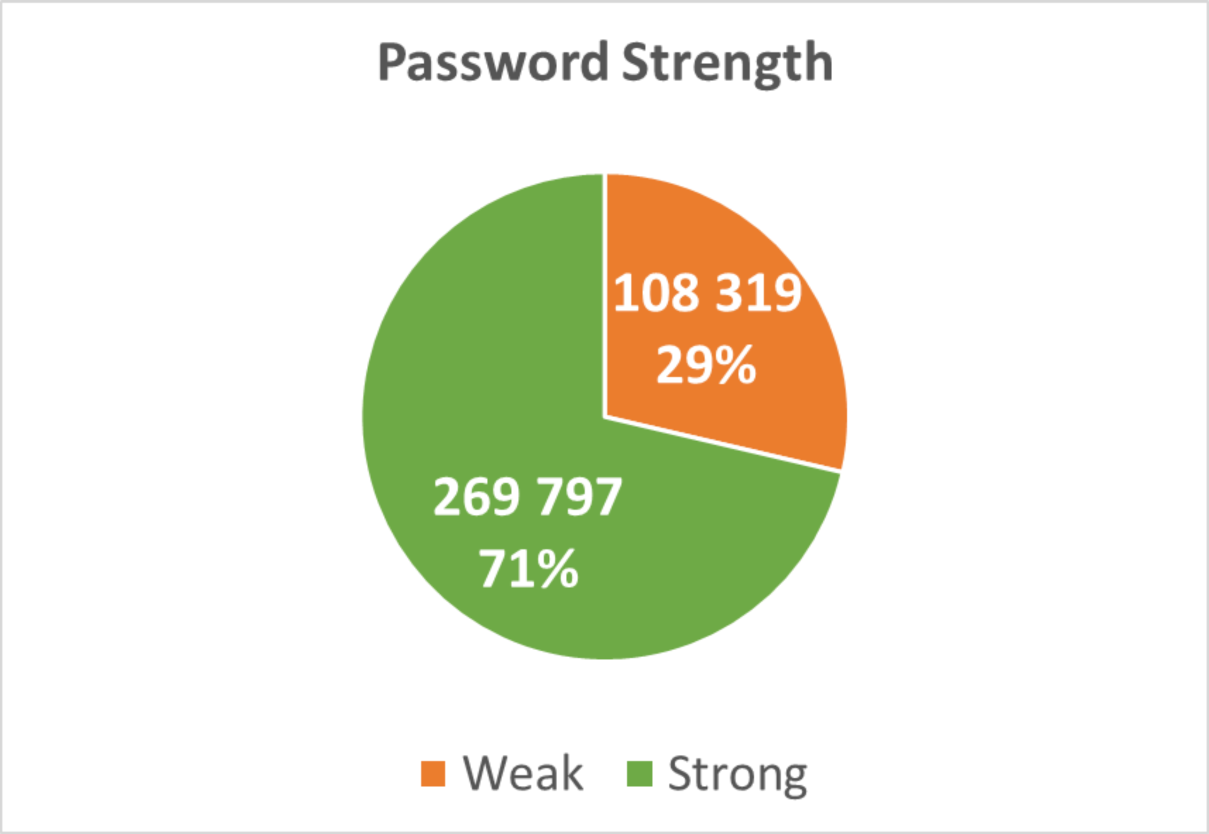

Diagram 4: Password Strength

162 out of 398 companies have incidents where their employees reuse identical passwords on different breached systems. This boosts the risk of password re-use attacks by cybercriminals.

Below is a table with the most popular passwords that clearly evidences poor password hygiene and practice even among employees of the leading cybersecurity companies:

Password	Number of Uses
password	1,186
123456	1,137
aaron431	1,109
12345678	344
123456789	271
Password	258
EvoPassword	254
12345	250
old123ma	237
1234	207
career121	190
none	182
welcome	163

Password	Number of Uses
password1	158
zaq12wsx	151
qwerty	148
micros1	144
1qaz2wsx	132
passw0rd	120
111111	120
blackberry	112
Password1	107
1234567890	92
abc123	90

Incidents by Country and Company Size

The table below show distribution of the incidents by country of the 398 cybersecurity companies:

HQ Country	Total Incidents	Verified Incidents	High & Critical Risk
USA	991,387	362,054	90,959
United Kingdom	285,656	117,559	29,226
Canada	147,866	61,447	20,902
Ireland	99,701	42,175	10,965
Japan	70,717	29,178	7,007
Germany	14,407	4,935	371
Israel	9,395	3,388	151
Czech Republic	9,097	2,932	112
Russia	5,460	1,746	98
Slovakia	5,187	1,006	257
The Netherlands	5,143	920	111
Finland	4,890	1,348	246

HQ Country	Total Incidents	Verified Incidents	High & Critical Risk
Singapore	3,628	401	8
Spain	1,749	692	18
China	1,514	542	58
Romania	1,028	371	19
Malta	499	86	3
India	331	107	9
Taiwan	169	144	2
Switzerland	149	66	0
Italy	78	68	0
Belgium	23	3	2
France	16	13	5
Portugal	13	4	0

The next table demonstrates distribution of incidents by company size:

Number of Employees	% of Affected Companies	High & Critical Risk Incidents
10,001+	92%	54,384
5,001-10,000	100%	3,545
1,001-5,000	100%	756
501-1,000	97%	533
251-500	95%	4,498
101-250	98%	949
51-100	97%	239
11-50	100%	102

Incidents Involving Third-Party Resources

A considerable number of the incidents stem from silently breached trusted third parties, such as suppliers or other subcontractors of the cybersecurity companies, mostly represented by stolen website databases and backups.

A large number of stolen credentials with plaintext passwords likewise come from incidents involving unrelated third parties including dating or even adult-oriented websites where victims were using their professional email addresses to sign in. We found at least 5,121 stolen credentials in pornographic and adult dating websites.

Below is the table with the most popular types of the breached third parties that presumably have no direct relation to the cybersecurity company whose employees were using its services:

Breached Third Parties	Number of Credentials
Personal services	24,526
Shopping	16,676
Games	11,119
Business	8,030
Services	5,776
Dating	5,121
Messengers and Social Media	4,966
Media	4,076

PCI DSS & GDPR Compliance

Furthermore, to paint an even a broader picture, go beyond the Dark Web exposure perimeter and indirectly cross-validate the findings, we used our free online website security test to check compliance of the main websites belonging to the 398 cybersecurity companies.
The test uses a non-intrusive and production-safe methodology to check PCI DSS and GDPR requirements specific to a website and web server security:

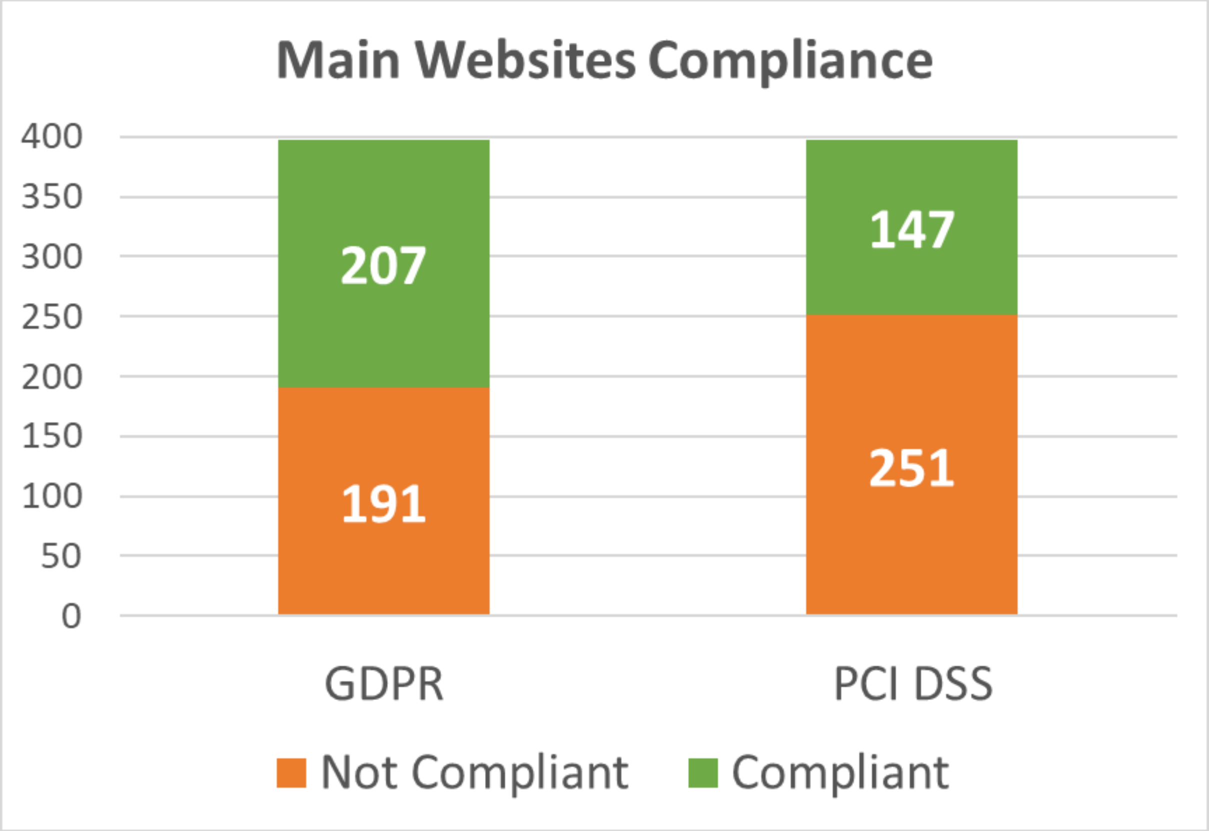

Diagram 5: Main Websites Compliance

As illustrated in the graph above, the main websites of more than half of all companies (63%) fail to meet these PCI DSS requirements, which means that they use vulnerable or outdated software (including JS libraries and frameworks), or have no Web Application Firewall (WAF) in blocking mode.
191 websites (48%) do not comply with these GDPR requirements because of vulnerable software, absent of a conspicuously visible privacy policy, or a missing cookie disclaimer when cookies contain PII or traceable identifiers.

Finally, we referred to data openly available at the Open Bug Bounty project to shed more light on web application (in)security of the 398 cybersecurity companies. 279 XSS vulnerabilities were reported there for 91 companies, wherein 26% of the reported vulnerabilities were still unpatched as of this research publication date.

Conclusion

Ilia N. Kolochenko, ImmuniWeb Chief Architect & Founder, says: "*The modern threat landscape has become a highly sophisticated, multidimensional and convoluted challenge for all industries. Human risk, IT outsourcing and reliance on third parties for data processing - gradually exacerbate the situation and complicate continuous security monitoring.*

Worse, mushrooming national and transnational compliance requirements start overconsuming a substantial part of shrinking cybersecurity budgets. Even the cybersecurity industry itself is not immune to those problems as demonstrated in this alarming research. Covid-19 bolstered international cybercrime, and compelled millions of unprepared organizations around the globe to urgently digitalize their business processes without requisite security and data protection. In this context, cybersecurity companies are, however, doing fairly well compared to many other industries in 2020, also because of generous venture funding and access to internal talents to tackle security and compliance.

Today, cybercriminals endeavor to maximize their profits and minimize their risks of being apprehended by targeting trusted third parties instead of going after the ultimate victims. For instance, large financial institutions commonly have formidable technical, forensic and legal resources to timely detect, investigate and vigorously prosecute most of the intrusions, often successfully. Contrariwise, their third parties, ranging from law firms to IT companies, usually lack internal expertise and budget required to react quickly to the growing spectrum of targeted attacks and APTs. Eventually, they become low-hanging fruit for pragmatic attackers who also enjoy virtual impunity. In 2020, one need not spend on costly 0days but rather find several unprotected third parties with privileged access to the 'Crown Jewels' and swiftly crack the weakest link.

Holistic visibility and inventory of your data, IT and digital assets is essential for any cybersecurity and compliance program today. Modern technologies, such as Machine Learning and AI, can significantly simplify and accelerate a considerable number of laborious tasks spanning from anomaly detection to false positive reduction. This picture is, however, to be complemented with a continuous monitoring of Deep and Dark Web, and countless resources in the Surface Web, including public code repositories and paste websites. You cannot protect your organization in isolation from the surrounding landscape that will likely become even more intricate in the near future."