INDUSTRY-FOCUSED DATA BREACH REPORT

2018

9% FINANCIAL

30% OTHER

8.9%

9% MEDIA AND ENTERTAINMENT

23% OIL, GAS, AND POWER

IT
The report is based on the major cybersecurity events that took place in 2017. However, not all the details on each event are publicly available, i.e., in some cases the data used for the statistics is presumable. Thus, it is quite easy to find the information about an attacked company and its business dimension. Nonetheless, the details regarding the losses and applied attack techniques are sometimes omitted or simply unknown.

This document or any of its fragments cannot be reproduced or distributed in whole or in part without prior written consent of ERPScan. Our SAP security surveys go beyond this whitepaper. You can find the latest statistics reports related to SAP services on the Internet and other endeavors of the ERPScan Research on ERPScan official blog.
<table>
<thead>
<tr>
<th>Contents</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>4</td>
</tr>
<tr>
<td>General results</td>
<td>4</td>
</tr>
<tr>
<td>Cyberthreats by industries</td>
<td>5</td>
</tr>
<tr>
<td>Risks</td>
<td>7</td>
</tr>
<tr>
<td>Attack techniques</td>
<td>9</td>
</tr>
<tr>
<td>Data breach risk zones</td>
<td>10</td>
</tr>
<tr>
<td>Attacked companies’ size</td>
<td>10</td>
</tr>
<tr>
<td>Cost of a security incident</td>
<td>11</td>
</tr>
<tr>
<td>Media and Entertainment</td>
<td>12</td>
</tr>
<tr>
<td>Government</td>
<td>14</td>
</tr>
<tr>
<td>Information Technology</td>
<td>15</td>
</tr>
<tr>
<td>Financial Institutions</td>
<td>16</td>
</tr>
<tr>
<td>Retail</td>
<td>18</td>
</tr>
<tr>
<td>Higher Education</td>
<td>20</td>
</tr>
<tr>
<td>Healthcare</td>
<td>21</td>
</tr>
<tr>
<td>Manufacture</td>
<td>23</td>
</tr>
<tr>
<td>Hotels</td>
<td>25</td>
</tr>
<tr>
<td>Oil, Gas, and Power</td>
<td>26</td>
</tr>
<tr>
<td>Others</td>
<td>27</td>
</tr>
<tr>
<td>Summary</td>
<td>28</td>
</tr>
<tr>
<td>Overall highlight</td>
<td>28</td>
</tr>
<tr>
<td>Industry highlights</td>
<td>28</td>
</tr>
<tr>
<td>Predictions</td>
<td>28</td>
</tr>
<tr>
<td>Conclusion</td>
<td>28</td>
</tr>
<tr>
<td>Reference materials</td>
<td>29</td>
</tr>
</tbody>
</table>
Introduction

As the number of cyberattacks and data breaches grows with time, the demand for information rapidly increases. The companies all over the globe strive to obtain actionable knowledge they can use to make themselves more protected.

With this report ERPScan Threat Intelligence team would like to share the most crucial and vital data collected during the analysis of all the data breaches of 2017. The report is intended to provide its readers with an insight into the specifics of attacks in every industry and, what is more important, to reveal what kind of companies’ assets has already become victims of cyberattacks and, consequently, show how to protect them.

► GENERAL RESULTS

The main principle of the analysis we decided to stick to was the classification of attack cases by the activity sphere of a victim company. Thus, it was possible to see main risks and soft spots in every field. We also paid attention to such features as the country a company operates in, size and staffing level of an enterprise.

After the data analyze had been analyzed, our primary aim was to illustrate starkly that there was an immense number of attacks launched on different enterprises every year. Finally, we concluded that there was no parameter to guaranty company’s security whatsoever.

We managed to collect data about the most known cyberattacks described in public sources and found over 200 incidents that took place in 2017. Unlike other advisories illustrating data breaches, which are privately reported or related to end users, we gathered the information about those incidents that were public and associated with a particular company. This can give us an understanding of targeted attacks.
The first and foremost question that definitely comes to one’s mind here is what industries are exposed most to onfalls of hackers. Considering the spheres these companies may specialize in, we decided to put them into 10 groups. The groups were formed according to the most susceptible spheres of activity.

- Higher Education
- Healthcare
- Public Transport
- Hotels
- Media and Entertainment
- IT
- Oil, Gas and Power
- Manufacture
- Retail
- Financial Institutions
- Government

There also was an additional 11th group comprised of those companies that did not suit any of the above groups. The overall information on the number of attacks launched in 2017 is presented below with a comparative chart (see Graph 1).
In 2017, the largest number of attacks was launched on Media and Entertainment companies. Governmental organizations were rated second according to the degree they were compromised. Enterprises in Financial Institutions, Retail, Healthcare and Higher Education got broken into medium with almost the same frequency. Manufacture, Hotels, Oil, Gas and Power companies rarely fell the victims of hackers; still, the compromises in these fields were widespread and had critical consequences.

Such a gradation in attack frequency can be explained by quite an obvious fact: the companies from the first trine that suffered the biggest number of cybersecurity incidents are the most influential as well. Among them, there are Media, Governmental and IT. Moreover, IT companies are also drawn to Media (the importance of the platforms like Facebook for the society is immense).

The next category may be characterized by storage and process of financial and customer data, which makes it especially tempting for cyber criminals to launch attacks on the organizations of the kind. As a rule, these enterprises specialize in the Finance, Retail, and Healthcare spheres.

Finally, the third group of companies, which relate to critical infrastructure and manufacturing, faced relatively few incidents. But the active growth of attacks is yet to come. Manufacturing has come ever closer to such an important sphere as Healthcare while there were only a few incidents several years ago. The threat to such industries as Oil and Gas Utilities, Power, Energy, and others should not be underestimated either.
There are 3 types of cybersecurity risks organizations face on a regular basis:

- Espionage
- Sabotage
- Fraud

Espionage is the practice of obtaining critical data associated with a company. In this case, an attacker’s potential victims are those organizations that use large databases. Databases may be stolen and sold on the Black Market. An attack of the type can also be performed by a potential competitor in order to get the information about some special aspects of the workflows inside a company. In 2017, Espionage became the most spread (45% of cases).

All the attacks the purpose of which is to gain money straight from a victim or to manipulate company assets fall in the Fraud type.

Sabotage is usually performed either to halt work processes of an organization on purpose by reason of professional interest, or in terms of entertainment. Fraud and Sabotage are almost equally frequent with a little transcendence of the first.

See the statistics on the attack frequency on Graph 2.

Graph 2. Attack frequency

We can get even more interesting results if we take a look at the correlation between types of attacks and the spheres of industry (see Graph 3).
Graph 3. Frequency of attacks by different industrial spheres

<table>
<thead>
<tr>
<th>Industry</th>
<th>Sabotage</th>
<th>Espionage</th>
<th>Fraud</th>
</tr>
</thead>
<tbody>
<tr>
<td>OTHERS</td>
<td>2</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>PUBLIC TRANSPORT</td>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>OIL, GAS, AND POWER</td>
<td>1</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>HOTEL</td>
<td>1</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>MANUFACTURE</td>
<td>4</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>HEALTHCARE</td>
<td>7</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>HIGHER EDUCATION</td>
<td>6</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>RETAIL</td>
<td>12</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>FINANCIAL</td>
<td>10</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>IT</td>
<td>7</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>GOVERNMENT</td>
<td>14</td>
<td>7</td>
<td>1</td>
</tr>
<tr>
<td>MEDIA AND ENTERTAINMENT</td>
<td>20</td>
<td>9</td>
<td>2</td>
</tr>
</tbody>
</table>

The first notable point is that Sabotage is most frequent in Media and quite common for the Government group. It can be explained by the fact that these 2 spheres relate to the organizations that have most sway over the society.

Espionage occurs in cases of attacks on those organizations that obtain critical information. These are Government, IT, Retail, and Manufacturing.

Fraud is the most common in Financial and Healthcare industries and happens due to operating with significant sums of money in these spheres.
ATTACK TECHNIQUES

Usually, a type of threat correlates with a type of attack. For example, if a company suffers a Fraud attack, it is likely that the threat is some ransomware. Still, it is not an absolute rule as the previous data theft can be performed in different ways. It is especially relevant for Espionage and Sabotage attacks, where there is a rich abundance of both incidents and types of attacks (see Graph 4).

The first place among the attack techniques types is taken by Unauthorized Access cases and its variations (25%). These variations include Brute forcing as well. In this category, we put cases connected with data breaches that frequently happen in Espionage and sometimes in Fraud.

The next common type of attack techniques is Ransomware forming about 23%. DoS is at the third place with 15%. Phishing is performed quite often as well 13%. About 5% of attacks are done aiming Defacement in particular.

A significant percentage of cases, 19%, include various types of Malware that can be quite different depending on the attacked organization and hacker’s goals.

Talking about the distribution of spheres and attack techniques, the most common type is Unauthorized Access (see Graph 5).
In most cases, Unauthorized Access took place in Media, 46%, which is no surprise at all due to its high ratio of Espionage risks. After that, the risks are also high in IT, 24%, and Manufacturing spheres.

Unauthorized Access is the most common attack. It is more popular than Ransomware and Malware, which proves the special importance of various Behavior Analytics solutions, such as UEBA for user behavior analytics and SOD tools (check who has access and to what functions), and PAM solutions for privileged account management.

► DATA BREACH RISK ZONES

In terms of the geographical distribution, attacks took place in a large number of countries, including European and Asian ones, India, and others (see Graph 6).

Graph 6. Geography of risks

An overwhelming majority of cases happened on the territory of the USA; the UK was rated second. Most attacks were launched on the companies based in leading countries. The more offices of organizations there are in a country, the more vulnerable this country is. On the opposite, the countries with a weak business presence in the mentioned spheres of activity became victims relatively less often. In other words, the importance and high status of organizations bring its country a proportional part of cyber threats.

► ATTACKED COMPANIES’ SIZE

The research comprises all the types of companies according to their size: both small ones (under 1000 employees) and big ones the workforce of which exceeds 5000 employees. There is no limit set for their origin (see Graph 7).
We can see that the most common victims of a data breach employ more than 5000 workers. Small companies are on the second place by attack frequency. Finally, mid-size companies (1000-5000 employees) form almost a half of the attacked enterprises.

**COST OF A SECURITY INCIDENT**

Though the majority of fraudulent attacks have been prevented, and the losses of some remain publicly disclosed, we can make a conclusion on the basis of the found details. In 18% of all the Fraud incidents, the losses are known and an average “price” of an attack is about 5.5 million dollars.

One of the biggest ransoms was gained from the cryptocurrency mining marketplace NiceHash when hackers got away with more than $62 million\(^1\). Another serious breach that took place in the sphere of Government was performed over the US Internal Revenue Service and amounted to $30 million\(^2\). Among the other huge losses, there are incidents happened to Canadian MacEwan University ($11.8 million lost CoinDash lost)\(^3\) and CoinDash platform ($7m in Ethereum currency lost)\(^4\).

The losses caused by a cyberattack may result not only in financial losses, but also in grave data breaches. Such breaches can be divided into several categories according to the type of stolen information (see Graph 8).

53% refers to clients’ personal data. In some cases the details of the leaked data are disclosed in terms of saving company’s reputation, but the cases where the loss of credit card data is confirmed form 30%. Employees’ data losses amount to only 11%. Other types of critical data stolen make 6%.

The average number of stolen credentials amounts to more than 14 million users or customers affected at a time. For example, one of the greatest breaches happened to Equifax\(^5\) and resulted in more than 143 million potentially affected consumers in the US.

Speaking of Sabotage, the average downtime was about 2 days. One of the longest service interruptions was the one of the Licking County government website that lasted more than 16 days.

Now, let’s turn our attention to the particular spheres of activity and discuss each of them in detail.
Forming 23% of the total incidents, Media became the most attacked sphere of 2017 (see Graph 9).

Graph 9. Data breaches in Media and Entertainment

<table>
<thead>
<tr>
<th>Sphere</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Journalism</td>
<td>41%</td>
</tr>
<tr>
<td>Social Services</td>
<td>28%</td>
</tr>
<tr>
<td>Broadcasting</td>
<td>13%</td>
</tr>
<tr>
<td>Gaming</td>
<td>11%</td>
</tr>
<tr>
<td>Casinos</td>
<td>7%</td>
</tr>
</tbody>
</table>

With their 40% inside the sphere, different journal companies and Internet services (such as online services, social and gaming websites) share the same frequency. Broadcasting companies and casinos that relate to Entertainment were also among the victims.

Most target companies employ under 1000 workers, as a great number of online services do not need a large team of specialists to be run and controlled (see Graph 10).

Graph 10. Attacked Media and Entertainment companies by number of employees

<table>
<thead>
<tr>
<th>Number of Employees</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>0-1000</td>
<td>57%</td>
</tr>
<tr>
<td>1000-5000</td>
<td>20%</td>
</tr>
<tr>
<td>5000+</td>
<td>23%</td>
</tr>
</tbody>
</table>

Still, among the victims there were such famous enterprises as New York Times, Facebook, HBO, YouTube, and others.

The chart below illustrates the preferences of attackers regarding attack techniques (see Graph 11).

Graph 11. Correlation of attacks on Media and Entertainment

<table>
<thead>
<tr>
<th>Attack Type</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sabotage</td>
<td>43%</td>
</tr>
<tr>
<td>Espionage</td>
<td>41%</td>
</tr>
<tr>
<td>Fraud</td>
<td>16%</td>
</tr>
</tbody>
</table>
The high ratio of Sabotage incidents can be explained with attempts of holding up some information from getting publicly available or even giving force to some other data with the help of a popular enlightener. Sabotage actions can also have no connection with a particular activity of some enterprise and use the resource as a place for the attraction of public attention to themselves, as in the case with over 300 popular Youtube accounts defacement by OurMine. This hacker group also had a hand in a number of attacks on media corporations, such as a breach of HBO Twitter, Vevo video hosting service, and WikiLeaks official website.

A lot of attacks in the sphere were also performed for Espionage purposes. A leak of yet unreleased materials with a further unauthorized distribution of them (e.g., theft of an episode of Game of Thrones from the 21st Century Fox) may serve as an example of it.

Another targets attackers were drawn to were user accounts and personal data. If stolen, these files may also be severe, which was the case of Equifax when hackers managed to steal more than 143 million of U.S. consumers’ data. It could probably be done due to a vulnerability in the CRM/Business Intelligence system.

Frauds are not that common in this field, however there was a number of fraudulent incidents.

Now, let’s turn our attention to the losses that took place in the most attacked sphere of the year and the types of leaked data (see Graph 12).

Graph 12. Types of leaked data

<table>
<thead>
<tr>
<th>Type of Data</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users’ details</td>
<td>53%</td>
</tr>
<tr>
<td>Accounts</td>
<td>27%</td>
</tr>
<tr>
<td>Professional materials</td>
<td>20%</td>
</tr>
</tbody>
</table>

The main part of the leaked data was comprised by users’ email and personal details (53%). Account databases attracted hackers a bit less, still they also became subjects of theft (27%). Finally, there also were cases of a company’s professional materials being stolen, 20%, as in the case with the mentioned episode of Game of Thrones.

The sphere of Media and Entertainment proves that there is no correlation between company’s sizes and its security. Probably, the situation is even opposite, as the more attention of users and clients the corporation has, the more attackers get drawn to it.

The most important type of data for Media and Entertainment companies is that of their users. Such data is usually stored in databases including custom ones (especially when social networks are considered). We would suggest paying extra attention to application vulnerabilities of such custom solutions, as well as password storing algorithms, so that even if an attack is performed, and user data is compromised, there will be no easy way to decrypt passwords.
The cases included in the Government group are associated with the governmental or state organizations, administration or military services. While not being private, they are still of interest to us as they demonstrate the weakness and vulnerability of the systems once again – even on the level of governmental institutions.

Almost 50% of the compromises happened in the USA. Breaches were also performed in Russia, Ukraine and a number of European countries (see Graph 13).

Graph 13. Correlation of attacks on Government

- ESPIONAGE: 41%
- SABOTAGE: 35%
- FRAUD: 24%

The main part of threats was espionage-related, 41%. Among the victims of Espionage, there are such organizations as the Vermont Department of Labor, National Security Agency, and the Parliament of the UK. A breach performed on the Internal Revenue Service (presumably with a loophole in the CRM system) resulted in 100,000 taxpayers’ data stolen.

Sabotage was also quite common (35%). Sabotage may be used to cause disruptions in work processes. For example, there was an incident with National postal service of Ukraine resulted in a 48-hour downtime.

Some attacks, while not being connected with any information or financial losses or service interruption in the usual sense, may bring quite serious consequences in a different way. In the case that can be referred to Sabotage, a man from Michigan managed to modify the data about some inmates in the Washtenaw County Jail. To launch an attack, a cybercriminal used spare phishing to reduce their terms. The hacker was pleaded guilty and remains in custody. The prison officials claim to have paid $235,488 to deal with the breach.

Frauds turned out to be less frequent here, 24%. Still, as a result of one of the major incidents the US Internal Revenue Service lost $30 million.

Governmental organizations usually store valuable customers’ information. They also have subcontractors from private sector responsible for collecting this data. For example, a last-year incident in the USIS with the leakage of thousands’ of US workers data happened due to a subcontractor’s vulnerability in SAP systems. Such systems as ERP’s HRs and others from vendors like SAP and Oracle are implemented in many governmental organizations. Over 4000 vulnerabilities were found in SAP applications, and about the same number was found in Oracle business applications including EBS, JD Edwards and PeopleSoft and the list of them is steadily growing. So, it is essential to be sure that those applications are safe.
The Information Technology is the third by the breaches frequency (see Graph 1, p.5). In this group, there are Internet services, software, hostings, search engines and others. Approximate distribution of attacks among the subspheres can be seen below (Graph 14).

Graph 14. Correlation of attacks on IT

<table>
<thead>
<tr>
<th>Category</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Espionage</td>
<td>48%</td>
</tr>
<tr>
<td>Sabotage</td>
<td>26%</td>
</tr>
<tr>
<td>Fraud</td>
<td>26%</td>
</tr>
</tbody>
</table>

As in case of Media and Entertainment, more than a half of the breaches were performed on the American companies due to the fact that a great part of the IT world is located on the territory of the USA. Among the victims, there also were Canada, European and South American countries.

Half of the breaches were Espionage cases. As there is a number of companies in this sphere that work with personal data of its clients directly, it is essential that the data is secured properly. Still, the results showed that some organizations might have serious vulnerabilities in their Customer Services systems, for example, such as Indian Reliance Jio, or Bell Canada where 1.9 million email addresses, 1,700 names, and phone numbers of Canadian customers were compromised.

Fraudulent and Sabotage actions were almost similarly frequent here making approximately a quarter of cases. Despite not being the most common type of threat, Sabotage still can put a strain both on the company and its customers as it happened in case with an attack on the Grapher Communications Internet service company. As a result, thousands of New Yorkers suffered the Internet cutoff.

Losses caused by frauds may sometimes be prevented just like with a ransomware attack on the Kenian Internet service provider Safaricom. However, from time to time, malefactors also reach their goal as they did by receiving $200,000 ransom from IBMi in April 2017.

IT and Telecom providers usually fall victims to Sabotage attacks. With their sizes and influence on economy and information, the security of these companies is essential. They mostly use custom solutions for asset management. Most of those solutions are developed inhouse, so they have to focus on secure development lifecycle and check their applications against common vulnerabilities in the source code. Another area is password storage. Since those systems store significant amounts of user accounts, in case of a compromise, all their encrypted passwords may be stolen, so it is important to store them securely using the latest hash algorithms.
Financial companies made a pay-off for hackers and got broken into quite frequently taking the 4th place in our list (9% of the cases). About a half of the attacks in this sphere were performed on banks, another half covered such projects as ATMs, currency exchanges and loan companies (Graph 15).

Graph 15. Attacked financial institutions

<table>
<thead>
<tr>
<th>Category</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Banks</td>
<td>47%</td>
</tr>
<tr>
<td>Cryptocurrency projects</td>
<td>21%</td>
</tr>
<tr>
<td>Loan companies</td>
<td>11%</td>
</tr>
<tr>
<td>Others</td>
<td>21%</td>
</tr>
</tbody>
</table>

Financial organizations normally tend to conceal financial information regarding their losses and employee data, which lets us assume, presume the scopes of harm done by hackers.

Presumably, due to the current financial situation in the world, most breaches took place in the UK, South Korea, and the USA. Among other victims there were also India, Brazil, Hungary, and Russia.

Although banks still stand on the first place in the list of victims, one of the special features of the attacks in this sphere in 2017 was connected with the growing popularity of cryptocurrency. As distinct from the state currency, this one is much easier to manipulate with anonymously, without any official authorization. Another difference is that crypto money as well as crypto tokens do not amount to legal currency, so that the rules and measures for such incidents are quite vague. In other words, this year there were many cases of attacking cryptocurrency exchange services, s.a. Yapizon and Bithumb (both in South Korea). A number of incidents with cryptocurrency exchanges coincided with the increase in bitcoin price.

These days, a number of emerging financial projects that are rather popular but not yet fully approved or legalized are facing the growing risks of attacks on them. A Fraud of Zcoin project may serve as an example of such an attack. This year, Zcoin losses amounted to 370,000 Zerocoin, which is $592,000.

Regular banks also get attacked by hackers, still the majority of their names are omitted in the media due to reputational issues. One of the mentioned banks was the Bank of America, which suffered a phishing attack. Fortunately, the losses were prevented.

All in all, classic bank and ATM attacks remain in the list of incidents, but the attackers now tend to move on to crypto thefts.

For banks and traditional financial systems, there is a number of well-known recommendations from GLBA and PCIDSS. Strict fulfillment of these recommendations may enhance the overall security. Another suggestion will be to focus on security of core banking systems. In such systems, we see a shift from attacks on users to attacks on systems that are closer and closer to the core of banking infrastructure. While years ago the main type of attack had been phishing, in 2017 we saw many attacks on ATMs.
With more security on the user side, such as 3-D Secure, there will be more attacks on ATMs as well as on the core banking systems, as the amount that is possible to steal from bank is much bigger than from a customer, even if there are multiple customers. However, another thing that can change is the implementation of machine learning techniques for phishing. The latest Deep Learning algorithms can generate text, pictures and even videos which are extremely hard to differ from the real ones. If hackers incorporate the latest ML techniques to their jobs, it can significantly improve their gain.
The Graph 16 illustrates the distribution of attacks on Retail companies by the subspheres they belong to.

Graph 16. Attacked Retail companies by subspheres

<table>
<thead>
<tr>
<th>Subsphere</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Food Services</td>
<td>60%</td>
</tr>
<tr>
<td>Trading Companies</td>
<td>27%</td>
</tr>
<tr>
<td>Travelling</td>
<td>13%</td>
</tr>
</tbody>
</table>

Retail companies are situated in the middle of the victim organizations list counting to 8% of the total number of all the incidents. Up to 60% of the breaches are performed on the representatives of the food services. Among other affected, there are different trading enterprises and companies of travel industry.

World leadership draws not only the attention of customers but also that of malefactors: this consequence was once again experienced by the USA this year with its more than 55% of all the cases in Retail sector. the UK, Germany, Japan, and China were also affected.

Every fisher dreams of catching a big fish, probably that is also actual for this case (see Graph 17).

Graph 17. Attacked Retail companies by number of employees

<table>
<thead>
<tr>
<th>Employee Range</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>0-1000</td>
<td>19%</td>
</tr>
<tr>
<td>1000-5000</td>
<td>12%</td>
</tr>
<tr>
<td>5000+</td>
<td>69%</td>
</tr>
</tbody>
</table>

The biggest number of affected corporations (69%) had more than 5000 members. 1000-5000 and 1-1000 employee companies got 12% and 19% of attacks respectively.

Graph 18 shows the distribution of attacks on Retail according to the type of a launched attack.

Graph 18. Correlation of attacks on Retail

<table>
<thead>
<tr>
<th>Type</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Espionage</td>
<td>73%</td>
</tr>
<tr>
<td>Sabotage</td>
<td>14%</td>
</tr>
<tr>
<td>Fraud</td>
<td>13%</td>
</tr>
</tbody>
</table>
Retail is probably the leader in Espionage attacks in comparison with other industries with its 73% of Espionage occasions within the sphere. It is not surprising, as nowadays Internet commerce forms a giant part of the retail sector, which means that most companies obtain their customers’ databases with all the personal and credit card information. In several cases, the leakages were prevented, but there is a number of occasions when the corporations lost great amounts of their clients’ data as it happened, for example, with Sonic Drive-In food service chain breach that resulted in 5 million stolen credit and debit card accounts\(^\text{30}\). In another breach that was performed on Debenhams Flowers retailer, there was data of more than 26,000 customers compromised\(^\text{31}\).

The number of fraudulent and sabotage actions is surprisingly low this year, reaching 13% of the incidents in retail. The information on financial losses mostly remains unknown. Sabotage actions led to service interruptions on the websites of such organizations as Lotte Group\(^\text{32}\) and McDonald’s Corporation\(^\text{33}\).

Taking into account that the majority of incidents in the Retail industry is related to Espionage and the main types of the stolen information are customer and credit card data, it is no secret that the core systems that should be protected in Retail organizations are CRMs as well as billing and POS/POS\(^\text{34}\) systems. Last year there was a number of critical vulnerabilities found in CRM and POS systems by major vendors, such as Oracle and SAP. Those vulnerabilities are the keys to cyberattacks. We will probably get the information about them in 2018, since it usually takes 1 year for an attack to be detected. This year, an example of a vulnerability in such systems was an incident with a leader in credit and debit card payments, Verifone. It resulted in a number of companies that use point-of-sale solutions suffering a severe impact\(^\text{35}\).

As for the future, we should not forget that the key business application for the Retail sector is SCM, supply chain management system responsible for all business processes. If somebody conducts a Denial of Service attack on these systems, imagine what the consequences can be. A halt of operations of a big retailer even for a few hours can cause millions in losses.
Attacks in the sphere of Higher Education happened with medium frequency and amounted to some 7% of all the incidents last year. There is little publicly available information on the number of employees of the attacked Higher Education organizations. Still, the main attention of the attackers was mostly attracted to the universities with world-known names.

Almost a half of the victim universities are located in the USA and Canada, several of them are British, which is no surprise, as these countries are supposed to be global leaders in the field of educational institutions.

Most malicious actions are fraudulent. They make 40% of all the attacks on the Organizations in this sphere. One of the most significant known losses amounts to $11.8 million. Canadian MacEwan University in Edmonton, Alberta, was one of those that financially suffered the most due to business email compromise (BEC) scam\textsuperscript{36}.

Graph 19 describes the proportion of the attacks launched on Higher Education.

Graph 19. Correlation of attacks on Higher Education

Espionage occupies the second place with its 33 %, which makes one-third of the total number. In the majority of cases, data leaks were prevented. The stolen information mostly consisted of students' personal data.

The notable Espionage incident was detected in over 60 universities where the hacker Rasputin used an SQL Injection to hack into their systems\textsuperscript{37}.

While Espionage and Fraud attacks usually stick to the same scenario, Sabotage actions may sometimes be unpredictable and quite surprising. For example, during an attack on the American University, more than 5000 Internet-connected devices started to search for seafood, which caused interruptions in work processes\textsuperscript{38}. The breach could presumably take place in the corporate performance and governance system.

The majority of incidents in the Education sphere were associated with Fraud and many of them are focused on financial manipulations. Universities use various Student Information Systems (SIS) that store and process most of the critical data. They can be described as “ERP for universities”. These solutions may also have vulnerabilities. There was a number of notable issues found in the SIS systems by different vendors, such as Oracle, PeopleSoft, and Campus Solutions\textsuperscript{39}.
Healthcare-related cyberattacks may be the most harmful ones, as this sphere is directly responsible for human health. These organizations got broken into almost as frequently as educational institutions this year (about 7%).

About 44% of cases happened on the territory the UK, 25% in the USA. Among the victim countries there are also Russia, Lithuania, and Israel.

The precise figure on the size of attacked companies is presented below (see Graph 20).

Graph 20. Attacked Healthcare organizations by number of employees

<table>
<thead>
<tr>
<th>Number of Employees</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>0-1000</td>
<td>34%</td>
</tr>
<tr>
<td>1000-5000</td>
<td>13%</td>
</tr>
<tr>
<td>5000+</td>
<td>53%</td>
</tr>
</tbody>
</table>

Over a half of the attacked healthcare companies had 5000+ employees. Such a big number of large medical companies being affected means that the damage inside every organization can potentially put at risk a considerable number of patients. For example, in case of an attack on Bupa international healthcare group 547,000 customers contact data was stolen\(^{40}\).

The Graph 21 describes the distribution among the types of attacks on Healthcare.

Graph 21. Correlation of attacks on Healthcare

Almost a half of the incidents were Frauds. Still, the real financial losses remain publicly unknown. Some blackmailing attempts ended up in data leakage: the breach took place on the servers of Grozio Chirurgija, and though hackers did not manage to get the ransom, over 25,000 of the private photos and critical personal data was stolen\(^{41}\).

Espionage was also quite frequent with its 40%. In this case, the main part of the stolen data included personal patients’ and workers’ information. The level of Sabotage was relatively low this year, 13%. However, the damages and risks caused by this type of threat are especially dangerous. Still, a strident attack was performed on the NHS websites by Isis-linked hackers when Syrian ISIS-linked hackers when images related to Syrian Civil War were placed on the defaced web pages. The attack caused service interruption and psychological threat\(^{42}\).
Being among the most unprotected ones, Healthcare companies are tempting targets for cybercriminals. On the one hand, they store significantly important data about patients and, on the other hand, they do not have so much awareness comparing to IT, Banks or Government that have been victims for years and now have more or less developed processes. As for the practical takeaways, Healthcare companies’ heart is the EMR and EHR systems that store and process all the information about patients. Protection of those systems should be the main priority for Healthcare organizations.
The frequency of incidents in this sphere amounts to 6% of all the attacks. Most cases are presented by breaches of the companies in technology, 46%, and food-manufacturing companies. As for the size of the attacked companies, the statistics look similar to those of the Retail and Hotel industries (see Graph 22).

The consistent part of the affected companies had 5000+ employees, as it is more profitable for attackers to break into systems of big corporations. 25% of cases happened in the USA, among the affected countries there are also Japan, the UK, Australia, South Korea, and India.

The correlation of types of the attacks on the sphere is presented with the graph below (see Graph 23).

Espionage (59%) predominated in the sphere; though in a number of cases the losses were prevented. Spiral Toys toy maker (CloudPets) experienced a serious data breach when more than 800,000 user accounts were allegedly affected.

Fraud formed about 33% of attacks in the sphere. Several cases were caused by WannaCry ransomware, for instance, LG Electronics and Honda were among the affected, in both cases financial losses were avoided. The information on the other monetary losses remains unknown. Such huge corporations as Apple also fell victims to fraud this year. Attackers claimed to have about 559 million accounts stolen; still, this information was not confirmed.

Among the notable Sabotage attacks, we can mention the breach of PlayStation’s social media accounts by OurMine – just right after their attack on the HBO. The company’s database was breached too, and the accounts were defaced with the post left: “We choose the people who have bad security to hack them and notify them about their security.”
In manufacturing companies, even the tiniest fluctuations in performance of operational technology may cause process disruptions, leading to defective products (meaning recalls and reputational losses), production downtime, physical damage, and even injuries and deaths. To give you another example: a hacker can slightly change welding conditions (e.g., lower temperature and time) in any part of a car manufacturing process so that two pieces will be joined not as firmly as they are required to. A number of systems is responsible for these operations, from robots on the plant floor to MES systems, PLMs and ERPs for storing and processing the data. Those systems, especially ERPs, are big targets for cyberattacks. As it was mentioned in ERP Cybersecurity Survey, an average cost of a security breach in SAP is estimated at $5m with Fraud considered as the costliest risk. A third of organizations assess the damage of fraudulent actions at more than $10 million. At the moment, the number of vulnerabilities in these systems from such top vendors as SAP and Oracle is skyrocketing.
Hotel business was rated 9th according to the frequency of breaches and got about 3% of all the incidents. As it is more profitable to break into the corporate-level system and get the control over a number of hotels inside one organization, the main part has occasion to hotel chains with several campuses affected at a time. In rare cases, single unit hotels get affected. That is also an explanation to the fact that about 84% of hotel victims had more than 5000 workers.

More than 60% of the hotels are located on the territory of the USA. Among the most compromised countries there are also the UK (22%) and Austria.

The statistics on the types of the attacks on Hotels conducted in 2017 can be found below (see Graph 24)

Graph 24. Correlation of attacks on Hotels

- Espionage: 83%
- Fraud: 17%

In the list of the most important 2017 incidents, there are more than 80% cases of Espionage resulted in clients’ personal data leakage. Fraud also took place among the breaches but, fortunately, rarely led to major financial losses. The biggest monetary loss was caused by the ransomware being applied to the system of Romantik Seehotel Jägerwirt, Austria, when the owners were forced to pay 1,500 euros (1800 $).

Sabotage was not common for the industry, as the main goal of attackers was either to get the access to databases with the further inappropriate implementation of the stolen data or to perform financial extortion.

The security of business applications that control multiple hotels is especially important in the Hotel industry as the attacks were mostly performed on hotel chains, which means that one major breach could develop on many hotels.
We decided to combine these three industries into one group. The attacks in these spheres last year were rare occurrences. Still, they might cause serious consequences.

About 40% of attacks were performed in the USA, Ukraine, China, and Ireland. Due to the fact that the losses caused by the incidents may lead to huge losses, the major part of them is supposed to be state-sponsored, there are several examples of such cases. One incident took place in Ireland; the attack was performed on the power provider EirGrid with the use of a man-in-the-middle attack scheme.

The breaches can potentially cause different consequences that mostly depend on the purpose attackers pursue. For example, state-sponsored attacks are usually performed with the aim of stealing sensitive information. In their turn, hacktivist groups tend to carry out Sabotage attacks.

Enterprise applications, such as Enterprise Resource Planning (ERP) or Business Intelligence (BI) systems, are typically connected with numerous plant devices with the help of various integration technologies, for example, to transfer collected data to a corporate network for further analysis. Unsecured connections between IT and OT environments can lead to vulnerabilities.

There is no gap between IT and OT systems, and there are business applications that exchange information with critical devices. So, consider the secure settings of these connections and business applications themselves, such as ERP’s and BI systems, because they form the first line of defense against attacks.
Above, we have covered 10 main spheres, that trace among the analyzed attacks. Still, there are cases that hardly fit the stated categories.

For example, there was a number of incidents happened in the sphere of Public Transport. The majority of breaches took place in the USA and were fraudulent. Most losses were prevented. However, Frauds can potentially target not only the workers and owners of a company. In case of Delta Air Lines, a phishing attack, when fake confirmation emails were sent to the company’s clients, the enterprise suffered reputational risks. This could happen due to the vulnerability in the CRM system of the company.

Among other notable cases, we can name the breach in Deloitte, one of the most influent accountancy firms, with more than 400,000 customers’ personal data compromised.

Also, there were several sports organizations compromised, including The International Association of Athletics Federations (athletes’ personal data stolen) and Boa Esporte football club website (service interruption).
OVERALL HIGHLIGHTS

• The average data breach costs were estimated at $5m in case of Fraud. An average of 14 million user accounts were affected by Espionage, and Sabotage resulted in 2 days of downtime.
• Unauthorized Access is the most common attack type. It is more popular than ransomware and malware, which proves the special importance of various Behavior Analytics solutions.
• Cyberattacks became much goal-oriented and did not only end up with credit card data theft, people hacking prisons to free friends, but also with breaching such applications as terminal management systems.

INDUSTRY HIGHLIGHTS

• It is more profitable to hack crypto-projects than financial institutions. Moreover, 20% of all financial incidents related to crypto-projects, and it is only the public data.
• Media companies are the most common attack victims and the only where the Sabotage was performed in 45% of all incidents.
• Retailers are subjects of espionage attacks via insecure CRM or POS systems. Retailers are in the 4th place by the number of data breaches.
• The UK is the biggest victim of Healthcare data breaches, and the number of attacks on the sphere is growing all around the world.

PREDICTIONS

• The number of target attacks on companies with the help of industry systems and specific business applications, such as ERP (Manufacturing) or EMR (Healthcare) and CRM (Retail), will grow.
• Hackers will use Machine Learning and Artificial Intelligence for phishing and malware cyberattacks, especially against clients.
• We will definitely see attacks not only on Crypto Exchanges but also on Blockchain smart contracts when these systems will become more efficient and publicly adopted.

CONCLUSION

We got the results of our attack statistic analysis, and they are not gleeful at all. We can see that the organizations that possess enough finances should be secure enough, but in reality, they are not. In the list of the victims, you can see famous names that belong to the world-known companies that turned out to be naked to hackers.

We hope that now, as you have the overview of the biggest and most important data breaches, you will not doubt the importance of your system’s security. It does not matter how influent and famous your company is, it will always attract the attacker.
Below you can find the list of reference materials. The entries are clickable.

2. Zeljka Zorz. How fraudsters stole millions with the help of a legitimate online tool.
5. Ines Gutzmer. Equifax Announces Cybersecurity Incident Involving Consumer Information.
7. Waqas Amir. Indian hackers hack Facebook groups for posting teen, revenge porn images.
17. Joshua Roberts. 100,000 federal student aid applicants at risk of identity theft after IRS breach.
18. Ukrainian postal service hit by 48-hour cyber-attack. BBC News.
21. Zeljka Zorz. 1.9 million Bell Canada customer account details stolen, leaked.
22. Samantha Cole. VILLAIN or HERO? A Vandal Cuts Off Internet for Thousands of New Yorkers.
27. Zeljka Zorz. DDoS attackers increasingly targeting cryptocurrency exchanges.
30. Brian Krebs. Breach at Sonic Drive-In May Have Impacted Millions of Credit, Debit Cards.
31. Cara McGoogan. Debenhams Flowers hacked: Credit card details of 26,000 people stolen.
33. Samantha Boonkamp. McDonald’s got Twitter bump after hacked account insulted Trump, expert says.
34. Alexander Polyakov. The Vulnerabilities Of A POS System.
37. Charlie Osborne. Lone hacker Rasputin breaches 60 universities, federal agencies.
38. University’s internet brought down by cyber-attack making vending machines search for seafood. Irish Examiner.
42. Kim Sengupta. Isis-linked hackers attack NHS websites to show gruesome Syrian civil war images.
43. Michael Kan. Smart teddy bears involved in a contentious data breach.
44. Waqas Amir. LG service centers in S.Korea Possibly Hit By WannaCry ransomware.
45. Peter Lyon. Cyber Attack At Honda Stops Production After WannaCry Worm Strikes.
46. Leo Kelion. Apple suffers ‘major iPhone X leak’.
47. Alexander Polyakov. Why Manufacturers Should Be Mindful Of Cybersecurity.
49. Bitcoin hotel hack victim speaks out. The Local.
50. Graham Cluley. Attack on Ireland’s state-owned power provider blamed on state-sponsored hackers.
53. Brian Homewood. IAAF says medical records compromised by Fancy Bear hacking group.