Power-supply enterprises cyber security and IT-immunity in the Customs Union countries

Dmitri Pletnev[1*], *Sergey* Vikulin[2], *Pavel* Shchelkanogov[2], and *Alexandr* Pletnev[3]

[1] Chelyabinsk State University, 454001, Br. Kashirinykh str., 129, Chelyabinsk, Russia
[2] Defender of Sites LLC, 143345, Promyshlennaya VL 1, Selyatino work settlement, Russia
[3] ITMO University, 197101, Kronverksky Pr. 49, bldg. A, St. Petersburg, Russia

Abstract. It is important for power supply firms to remain immune to rapidly emerging cybersecurity threats. These can be acts of a hooligan nature, and an attempt to steal data and money, and even cases of electronic terrorism. To counter these threats, power supply companies must take care of their cyber security and prevent possible threats. The paper aims to assess the main cyber security risks and consider their relevance to the cases of specific energy sales companies of the companies of the Customs Union countries. The paper analyzes the trends and the current structure of cyber threats, on the example of power supply companies of the countries of the Customs Union, using the original methodology, assessed IT immunity, and the main vectors of threats. The directions for further research aimed at preventing cyber threats for energy sales companies are formulated.

1 Introduction

As industrial and manufacturing companies increasingly rely on digital technologies, the risk of cyberattacks has become a major concern. The potential consequences of a successful attack can be significant, including theft of sensitive data, disruption of operations, and damage to equipment or infrastructure.

The main threats to information security for industrial, manufacturing, energy and energy retail companies are internal threats, external attacks and supply chain vulnerabilities.

- Insider (internal) threats are one of the most significant and complex aspects that must be managed in terms of information security. Such threats come from individuals within an organization who have authorized access to sensitive information, systems, and resources. These threats can be intentional or unintentional, such as employees stealing data or accidentally revealing sensitive information. Examples of insider threats include employees who steal data to sell on special sites or use company resources for personal gain, such as running cryptocurrency mining software on company servers. Insider threats can also arise from unintentional activities, such as employees falling victim to phishing attacks or inadvertently transmitting sensitive data through misconfigured or unsecured systems.

*Corresponding author: pletnev@csu.ru

- External attacks - external attacks refer to cyber attacks that are carried out from outside the organization's network or systems. These attacks can come from a variety of sources, including cyber criminals, hackers, government actors, and even disgruntled customers or partners. Common external attacks include phishing attempts, where attackers use social engineering techniques to trick users into divulging sensitive information such as passwords or account information. Other common types of external attacks include malware, ransomware, and DDoS attacks.
- Malicious software is software that is installed on a system without the knowledge or consent of the user and can be used to steal data or damage systems.
- Ransomware is a type of malware that encrypts the victim's data and requires payment in exchange for a decryption key.
- DDoS attacks involve flooding a network or website with traffic to make it inaccessible to legitimate users.
- Vulnerabilities in an organization's supply chain are risks associated with external providers that provide goods or services to the organization. These risks can be caused by a number of variables, such as a vendor's lack of adequate security controls or vulnerabilities introduced into an organization's systems through third-party software or hardware. Consider this case, a company may be using third-party software that has flaws that attackers can use against it. Also, the provider may have insufficient security measures, such as weak passwords or unsecured networks, which open the organization's systems to attacks.

Given the potential impact of information security breaches on industrial and manufacturing companies, it is essential to conduct risk assessments on a regular basis to identify and mitigate these threats. In this article, we will look at the key aspects of conducting a thorough information security risk assessment in the context of industrial and manufacturing companies, including identifying threats, assessing risks, and developing effective risk management strategies [1].

Separately, the concept of IT-immunity stands out in the literature, which characterizes not so much the absence of threats to a particular company as the ability to withstand emerging threats. For modern companies, it is important to have IT-immunity [2].

The energy supply industry is becoming more and more competitive today, there are small companies that are not ready to spend money on complex cybersecurity systems and maintain a large staff of relevant specialists. On the other hand, the stable operation of power supply companies is very important for the smooth operation of the entire economy, as well as for maintaining a high quality of life for the population [3-5]. This makes the issues of studying the features of cybersecurity and IT immunity relevant.

The paper aims to assess the main cyber security risks and consider their relevance to the cases of specific energy sales companies of the companies of the Customs Union countries.

2 Materials and methods

The logic of the study involves the consistent solution of the following tasks. First, an analysis of the dynamics and structure of cyber threats that are typical for modern companies, identifying their trends. Secondly, an assessment of the IT immunity of a sample of energy sales companies from countries that are members of the Customs Union (Russia, Kazakhstan and Belarus). Thirdly, an analysis of the main risks specific to such companies.

In the analysis of IT immunity and structural risk analysis, the online service Vulndetector (https://vulndetector.ru/) was used, which allows to identify 11 risk groups, such as Websites, Mail, Telephony, Gateways, Domains, Network, Development, Backend,

Data, Finance, Common, and also calculate the IT immunity index for each analyzed company. It allows to classify and measure objects of any complexity, as well as visualize the results. Vectors of classification of business systems are used to determine IT immunity with high accuracy. A detailed description of each risk group (threat vector) is presented in Table 1.

Table 1. Vectors of threat of IT immunity of energy supply companies.

Vector of threat	Description
Websites	Web servers, for example, Apache, Nginx, HAProxy, are responsible for the operation of the Website.
Mail	Various mail systems and programs, including Exchange, Postfix, Exim and Mail.
Telephony	IP telephony uses Asterisk, Avaya, CommuniGate, Cisco and H323 protocols, as well as FreeSWITCH. This is a unique list, collected empirically.
Gateways	All entry points to the company: SSH, Internet, Wi-Fi and VPN
Domains	Domain Name management systems, various address resolution services, DNS, BIND, PowerDNS, Unbound Servers, Windows Active Directory domain management
Network	Various routers, OSPF, BGP, Microtics, Cisco, Huawei, Juniper, Proxy servers, D-Link, BRAS
Development	Build systems (Jenkins, GitLab), code storage (Git, SVN, CVS), repositories (docker, helm) and development management (Jira).
Backend	Information about the production environment, including Kubernetes clusters, Hadoop clusters, private APIs, authorization systems and application servers.
Data	Various archives, databases, Wiki information storage systems, shared disks, Logs.
Finance	Accounting systems (1C and Galaxy ERP) Payment systems, gateways and aggregators that manage the financial flow.
Common	Internal projects/clusters of the company, common names are used, such as the names of planets, star systems, mountains on the Earth/Moon/Mars, the names of famous characters from TV series or popular animals.

The study analyzed 8 companies from countries of Customs Union (Russia, Belarus and Kazakhstan). Analysis results will be presented anonymously, in graphs. The use of graphic results allows for the prompt identification of risks that may lead to unacceptable events. A quick response to new entry points can protect your business from targeted cyber attacks and determine what measures need to be taken to ensure its reliable protection.

3 Results

In today's world, cybercrimes are becoming more and more commonplace. The number and losses from such an increase in crimes are growing intensively, while the growth rate of losses fluctuates quite strongly from year to year (Table 2)

Table 2. Growth Dynamics of Losses from Cybercrimes.

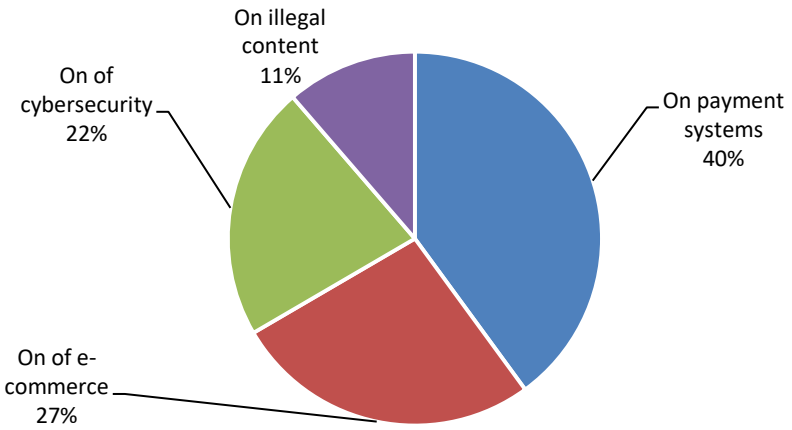
Year	Losses, mln. $	Losses Growth ratio
2001	17.8	-

2002	54	3.034
2003	125.6	2.326
2004	68.1	0.542
2005	183.1	2.689
2006	198.4	1.084
2007	239.1	1.205
2008	264.6	1.107
2009	559.7	2.115
2010	563.2	1.006
2011	485.2	0.862
2012	581.4	1.198
2013	781.8	1.345
2014	800.4	1.024
2015	1070.7	1.338
2016	1450.7	1.355
2017	1418.7	0.978
2018	2710	1.910
2019	3500	1.292

Source [10] and authors calculations

In subsequent periods, especially given the accelerated digitalization of society and business in 2020-21, as well as the violation of the integrity of the global security loop, the number and losses from cybercrime increase even more rapidly. In addition to objective trends, this is also facilitated by a change in the legislative framework, as well as the improvement of methods for detecting cybercrime. On the other hand, the improvement of cybersecurity methods hinders the growth of these indicators (an annual increase of 2-3 times is observed only until 2005).

In the structure of cybercrime, it is useful to distinguish four main groups (fig. 1): disruption of payment systems, interference with e-commerce, general cybersecurity problems and illegal use of content. The main damage from cybercrime is direct losses from the theft of funds in various ways. This makes cybercrime even more important to the attention of business executives and security officials.



Source [11], authors calculations

Fig. 1 Structure of cybercrimes in 2020 (worldwide).

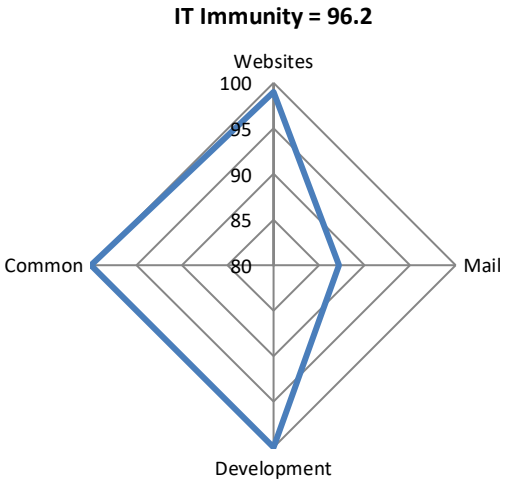
An analysis of power supply companies in the countries of the Customs Union showed that, in general, IT immunity is at a high level. Many threat vectors are not implemented due to the lack of appropriate functions from the company, and those that are relevant are usually reliably protected. However, sometimes the analysis showed the presence of "holes" in security, which attackers can use to commit cybercrimes. And two companies out of 8 turned out to be practically defenseless against potential cyber threats (table 3). We hypnotize that these companies are zombies-firms that on the way to bankruptcy and reorganization.

Table 3. IT immunity and treats types for selected energy supply companies.

	Company number							
Indicators	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
IT immunity	96.2	99	0	99.2	90.8	46.2	99.75	95
Critical threats	0	0	10	0	0	23	0	0
High threats	0	0	6	0	0	0	0	0
Average threats	9	0	26	0	9	7	0	0
Low threats	2	2	6	4	12	3	2	5

Source: authors calculations based on vulndetector.ru

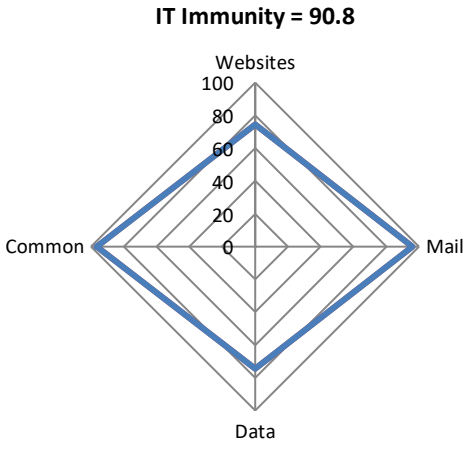
The profile of threat vectors for specific power supply companies turned out to be different (see Fig. 2-4). The figures show only those vectors that can potentially be implemented in this company, with the available equipment and connections. Company 1 profile shows that overall the level of immunity is quite high, but non-urgent updates to the mail server should be done. If this is not done, there will be risks of email hacking or the server will start sending spam. This risk is not critical and, as a rule, does not lead to significant financial losses for the company (fig. 2).



Source: authors calculations based on vulndetector.ru

Fig. 2. IT immunity profile for Company 1.

The Company 5 also demonstrates a fairly high level of immunity. It is necessary to properly configure the firewall on Windows shares, reduce the risk of leakage. For this case, it is time for some updates to the web server. Other vectors are safe (fig. 3).



Source: authors calculations based on vulndetector.ru

Fig. 3. IT immunity profile for Company 5.

Company 7, based on its profile, demonstrates a fairly high level of immunity. However, to achieve a perfect result of 100%, you can replace the VPN server and reduce the risks of managing Windows Active Directory. It is important to bear in mind that all the risks listed above are not critical and, as a rule, do not lead to significant financial losses for the company (fig.4).

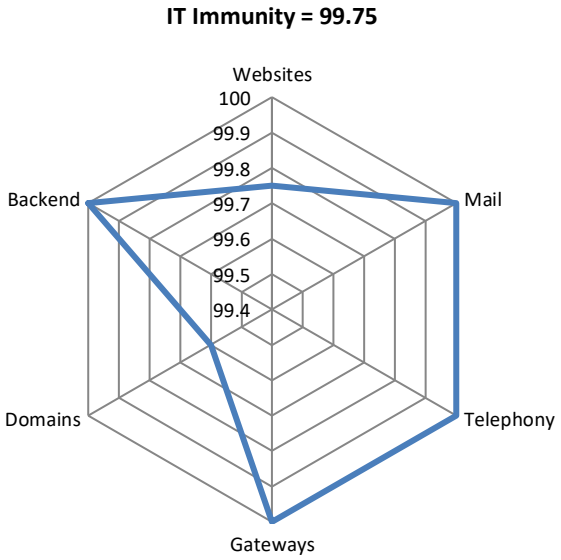


Fig. 4. IT immunity profile for Company 7.

Visualization of this kind allows visually comparing the vectors of urgent problems, evaluating their dynamics and the relationship between companies. This kind of analysis is still rarely used by energy retail companies, and in this they have development potential.

4 Conclusion

Thus, the issues of cybersecurity and IT immunity of modern enterprises in the field of electricity sales are important, and organizations themselves are most often aware of the importance of these aspects of their activities. At the same time, it is necessary to understand that new cybersecurity risks appear very quickly, and there is no time to enjoy success, companies should regularly update their security systems, use reliable companies that test its information "security perimeter" and ensure their owners have a restful sleep. The approach presented in this article can be developed in subsequent publications by expanding the geography of companies, their industry composition, analyzing the dynamics of IT immunity of specific companies and their groups. In the age of information, informational immunity is no less important than biological immunity, and its support is the responsibility of everyone.

References

1. E. Akinfeeva, Bulletin of MIRBIS **4(20)**, 79-88 (2019) DOI: 10.25634/MIRBIS.2019.4.9
2. D. Pletnev, S. Vikulin, P. Shchelkanogov, A. Pletnev, Bulletin of Chelyabinsk State University **11(469)**, 177-181 (2022) DOI: 10.47475/1994-2796-2022-11119
3. M. Ricardo Saavedra M., Cristiano Hora de O. Fontes, Francisco Gaudêncio M. Freires, Renewable and Sustainable Energy Reviews **82(1)**, 247-259 (2018) DOI:10.1016/j.rser.2017.09.033

4. S. Emenike, G. Falcone, Renewable and Sustainable Energy Reviews **134**, 110088 (2020) DOI: 10.1016/j.rser.2020.110088
5. D. Pletnev, V. Barkhatov, M. Kazadaev, E3S Web of Conf. **157**, 04028 (2020)
6. B. Obotivere, A. Nwaezeigwe, Internat. J. of Adv. Res. in Computer and Communication Eng. **9(9)**, 92-97 (2020) DOI: 10.17148/IJARCCE.2020.9913
7. Z. King, D. Henshel, L. Flora, M. Cains, B. Hoffman, C. Sample, Frontiers in Psychology **9(39)** (2018) DOI: 10.3389/fpsyg.2018.00039
8. D. Henshel, C. Sample, M. Cains, B. Hoffman, Advances in human factors in cybersecurity, 123-137 (2016) DOI: 10.1007/978-3-319-41932-9_11
9. A. Oltramari, D. Henshel, M. Cains, B. Hoffman, Semantic Technology for Intelligence, Defense, and Security, 26–33 (2015)
10. I. Nikolina, I. Hulivata, K. Kopniak, East European Scientific Journal **3(55)**, 17-23 (2020)
11. S. Tkalichenko, V. Khotskina, Zh. Tsymbal, V. Solovieva, O. Burunova, SHS Web of Conf. **100**, 01014 (2021) DOI: 10.1051/shsconf/202110001014