ITBIZ system integrator

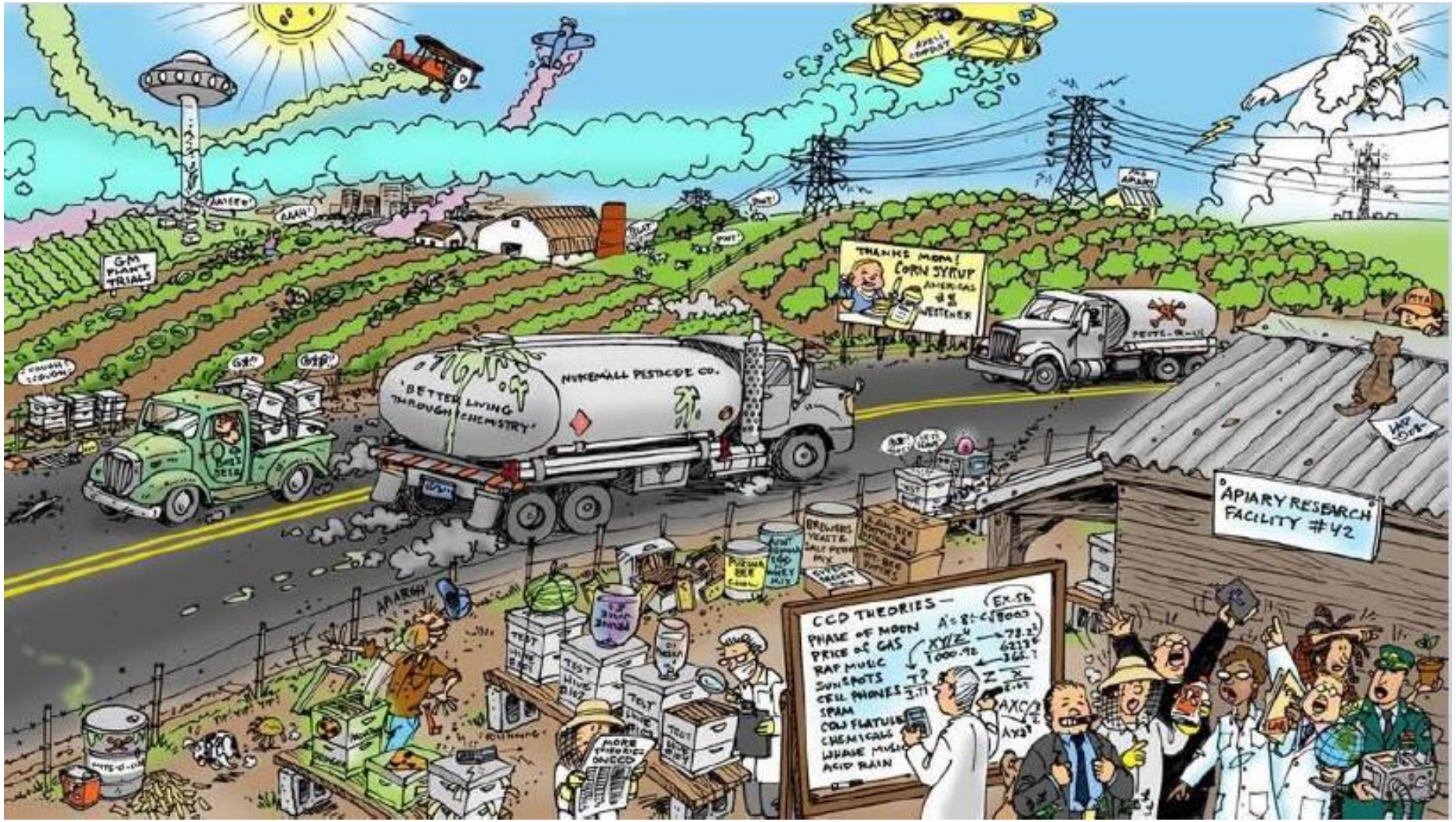
Ten Pertinent Cybersecurity Trends to Keep an Eye On

SERHII CHORNOUS

Head of Department
ITBIZ

ITBIZ system integrator

Our job as a system integrator is to replace chaos at the enterprise with information and intelligent systems



Telecommunications equipment and IT infrastructure

Servers for all types of tasks (Dell, Lenovo, Nutanix, Supermicro, Huawei);
Data storage systems (NetApp, Dell EMC, Lenovo, QNAP);
Backbone solutions based on spectral wave compression systems - DWDM.ME;
Networking equipment (Juniper Networks, Extreme Networks, Huawei, DELL);
Wi-Fi solutions (Aruba, Juniper Networks, Fortinet, Huawei)

Telecommunications equipment and IT infrastructure

BROCADE
JUNIPER NETWORKS
extreme networks
DWDM.ME
ERICSSON
riverbed Think fast
ekinops

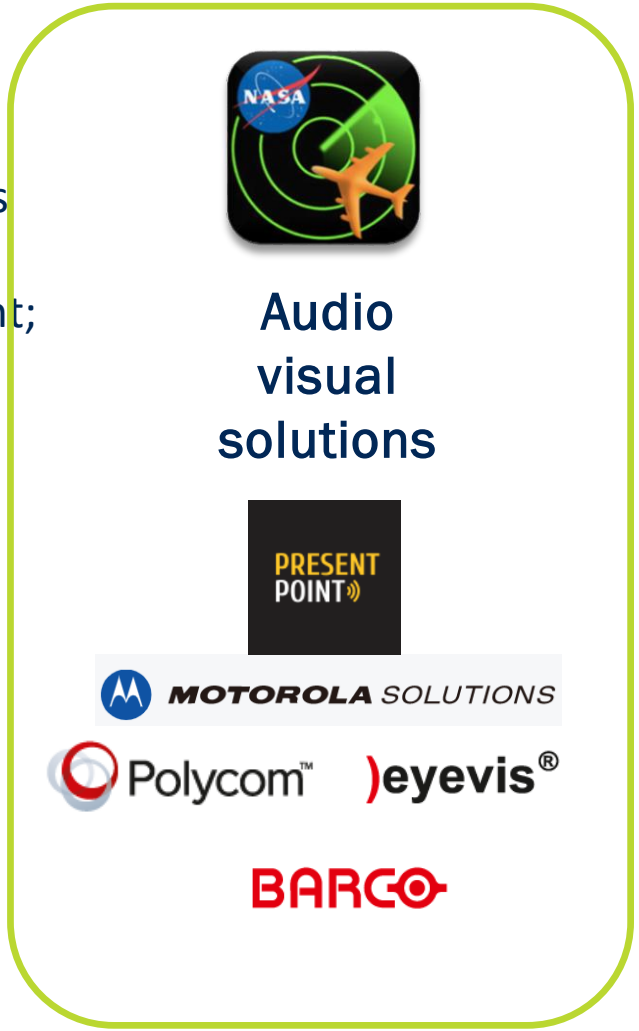
IT infrastructure security systems:

- Building an authentication and user authorization system in the IS (information system);
- Protection of the network perimeter;
- Protection of mail;
- Protection of WEB-resources and WEB-applications of the company;
- Protection of control points;
- Building a vulnerability control system;
- Control of administrators;
- Building a system against data leakage

IT infrastructure security systems

Audio visual solutions:

- Construction of control rooms and situation centers (Leyard Group: Planar / Eyevis);
- Video surveillance systems (Hikvision, Panasonic, Avigilon, Ahis, Tiandy), sales and implementation;
- Integrated solutions for mobile video recording based on Motorola equipment;
- IP telephony (Polycom, Grandstream, Cisco);
- Video conferencing (Polycom, Grandstream);
- Present Point wireless presentation systems



ITBIZ system integrator

1. Protection of confidential data
2. Risks to the Internet of Things (IoT) are increasing
3. Cyberhygiene training for employees
4. Fighting phishing
5. Passwordless access to systems
6. Ransomware
7. Protecting cybersecurity in supply chains
8. Mobile device security
9. Attacks on artificial intelligence systems
10. Increase in attacks using deepfake technology

1. Protection of confidential data

In 2022-23, companies and customers interacted digitally in almost 72% of cases. This means that consumers are increasingly trusting companies with their data, and therefore expecting greater efforts to ensure its protection. In the near future, personal data security will become a mandatory factor necessary to build customer trust in a brand.

Companies that can demonstrate a professional approach to managing confidential information will have a competitive advantage, strengthen their positioning, improve customer loyalty, and increase their profits.

2. Risks to the Internet of Things (IoT) are increasing

It is expected that by the end of 2023, there will be 43 billion Internet of Things (IoT) devices in the world, and by 2025, each person will interact with an IoT device every 18 seconds on average, which will require proper protection. Additionally, businesses need to regularly inventory their IoT-connected devices and monitor and maintain equipment more closely to secure endpoints, manage vulnerabilities, and respond to incidents. Each additional device connected to the company's network increases the number of potential "doors and windows" that can be used by attackers to gain access to confidential information. These can include computers, company cars, building alarm systems, industrial equipment, and more.

ITBIZ system integrator

3. Cyberhygiene training for employees

In 2023, companies around the world are focusing on developing a security culture among their employees. The human factor is becoming the most attractive component for criminals who carry out cyberattacks. Therefore, cybersecurity is now a concern for every employee, not just for security professionals. This requires the creation of clear instructions on how to process and protect data.
Consequently, training employees in the basics of cybersecurity and their ongoing development will become essential tasks for companies in 2023. This will help create a conscious security culture, reduce the risks of cyberattacks and ensure the protection of confidential information. Investing in employee training and implementing appropriate security policies will be a winning strategy for organizations seeking to maintain their reputation, customer trust, and operate successfully in the digital environment.

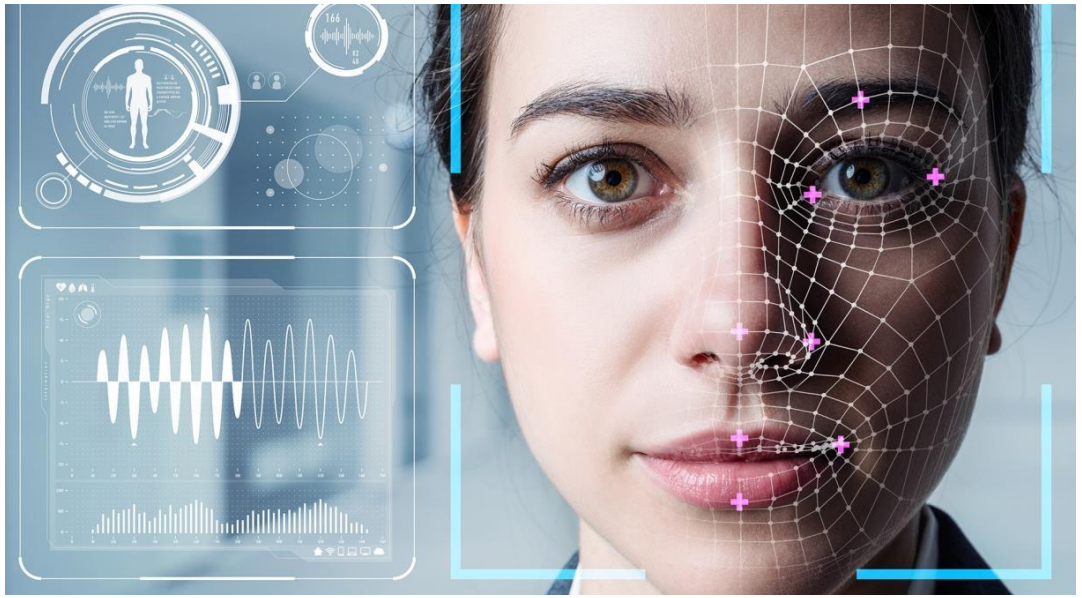
4. Fighting phishing

As phishing attacks become more sophisticated, companies need to stay ahead of the curve by improving technological security measures, providing employee education, and implementing strict policies on opening emails with questionable origins. Phishing protection is becoming a necessary element of every employee's daily work, as only by working together can we ensure the safety of the organization from phishing attacks.
Only through a combination of technological measures, effective staff training and a conscious approach to cybersecurity can a reliable defense be created and potential threats prevented.

ITBIZ system integrator

5. Passwordless access to systems

One of the most effective ways to combat phishing is to switch to a passwordless method of managing access to corporate networks and applications. This approach involves the use of a multi-factor authentication system that does not require a password or pin code. Instead, the user is prompted to provide a fingerprint or login confirmation via a smartphone or banking app. Passwordless systems offer a real opportunity to resist cyberattacks while providing improved privacy and convenience. Using a passwordless approach strengthens the security of organizations by eliminating the risk of account compromise and data alteration, and improving the user experience.



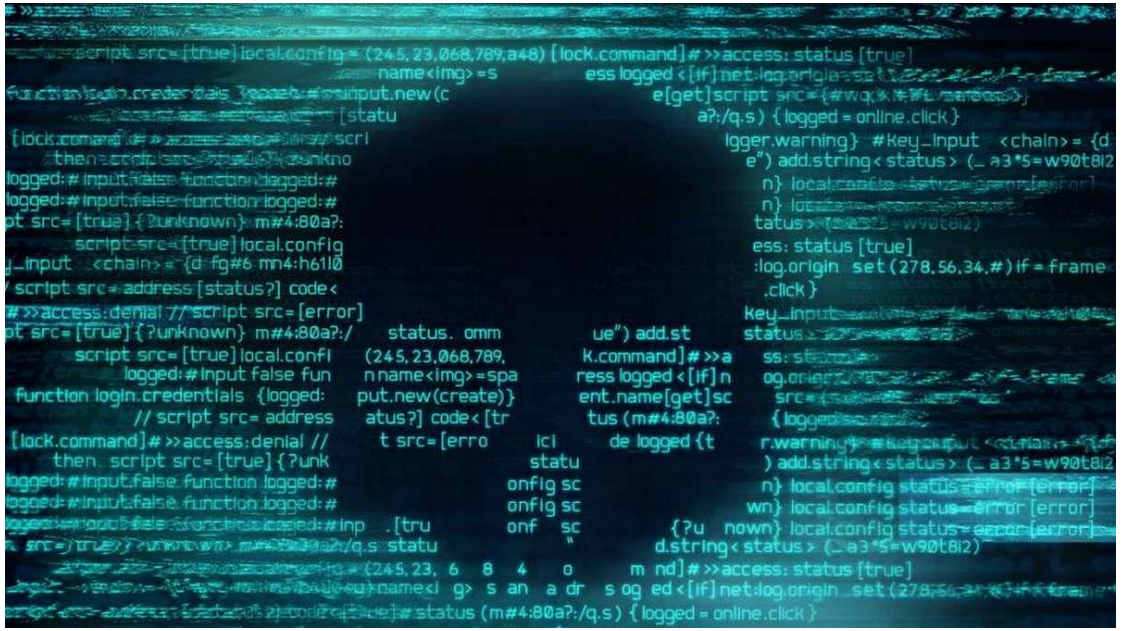
ITBIZ system integrator

6. Ransomware

Ransomware poses a serious threat to corporate networks because it can infiltrate systems and conduct reconnaissance without being noticed. What's particularly alarming is that every year these malicious programs take less and less time to explore companies' resources. According to Cybereason's research, the number of ransomware attacks on businesses worldwide increased by 33% year-on-year.

Almost half of the organizations (49%) fell victim to these attacks and paid the ransom, but 80% of them were attacked again.

According to Cybersecurity Ventures, by 2031, the fight against ransomware will cost organizations approximately $265 billion annually, and new attacks will occur every 2 seconds. In 82% of cases, hackers successfully achieve their goals due to the human factor, i.e., due to employee inattention.



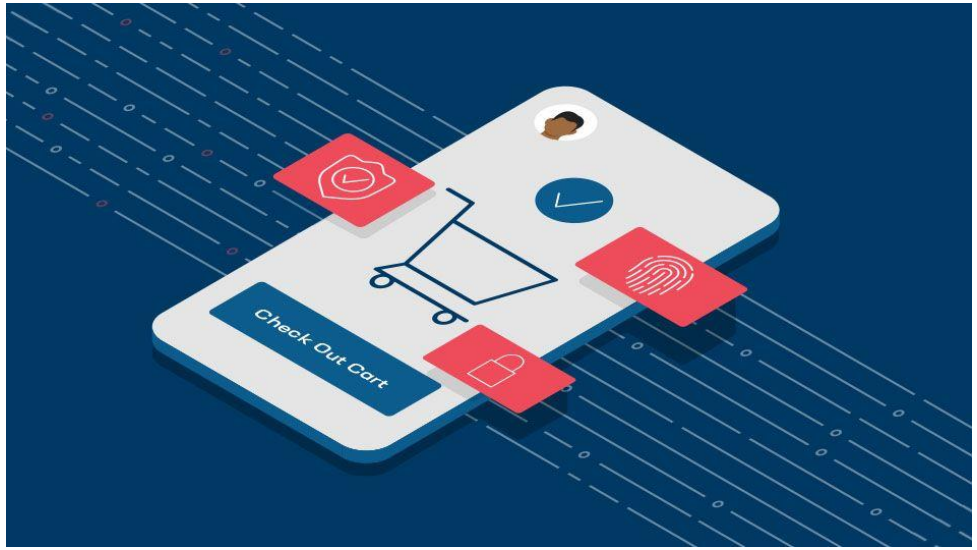
ITBIZ system integrator

7. Protecting cybersecurity in supply chains

Even companies that take care of the security of their own IT infrastructure cannot guarantee 100% protection against hacker attacks aimed at the supply chain. We mean intrusions into corporate networks through compromised third-party software used by the organization. For example, attackers can hack into a supplier's warehouse inventory system, and a virus will enter the customer's network through regular updates of this software.

8. Mobile device security

The number of cyberattacks on mobile devices globally increased by 500% in the first months of 2022, with Android devices being particularly targeted. Malware is being actively developed for different types of mobile devices, such as smartphones, tablets, and laptops.
In particular, smartphones are particularly attractive targets for hackers because attacks on them are less visible. Malicious apps, websites, ransomware, phishing, Man-in-the-Middle (MitM) attacks, sophisticated hacking techniques, and device and operating system flaws are the main sources of threats to mobile devices.



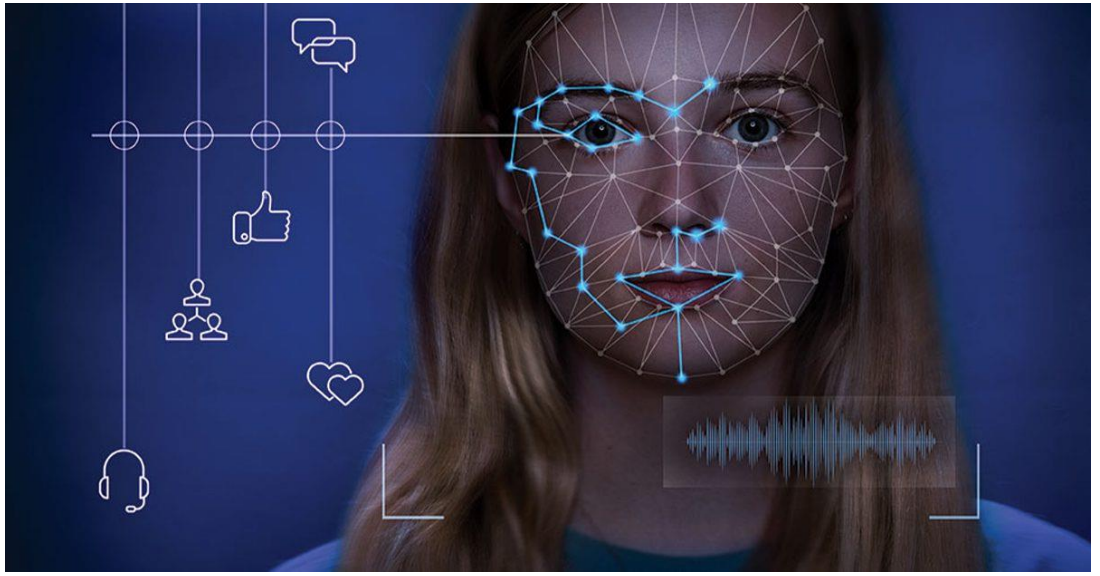
9. Attacks on artificial intelligence systems

A study conducted by IBM in 2022 showed that 35% of businesses are already using artificial intelligence (AI) in their business processes, and another 42% are exploring its potential. The number of cyberattacks on AI systems is expected to increase, which can lead to "poisoned" data that is entered into the system by an attacker. This distorts the process of processing AI queries, potentially leading to incorrect results that affect decision-making in the company. It is predicted that such an impact on AI algorithms will be observed in systems with a weak level of protection or those that contain important data among many computers connected to the Internet. In addition, attackers can use this method to create a large number of personalized phishing emails, artificially imitate the voice of executives and abuse fraudulent authorization and transactions.

ITBIZ system integrator

10. Increase in attacks using deepfake technology

Deepfakes are realistic audio and video materials created with the help of artificial intelligence and deep learning using generative adversarial networks (GANs). Using GANs, a deepfake can copy the face, facial expressions, and voice of one person and transfer them to other images or videos. This type of attack is used to distort trust by making us perceive fake videos or audio recordings as real.



ITBIZ system integrator

https://itbiz.ua

https://presentpoint.com.ua

https://dwdm.me

Serhii CHORNOUS

Mobile phone: +380 97 787 77 26
e-mail: stc@itbiz.com.ua