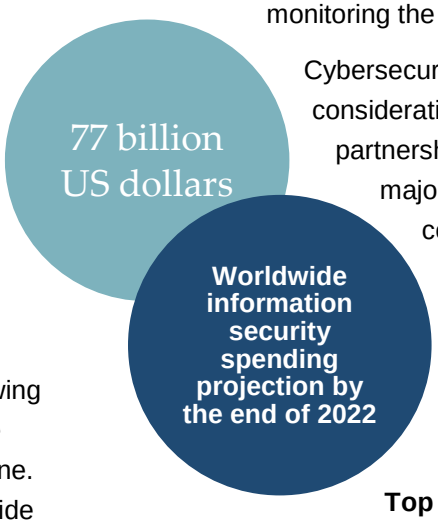
2Secure

MAIN CYBER TRENDS & THREATS IN 2022

MAIN CYBER TRENDS AND THREATS IN 2022

Worldwide information security services spending was 72.5 billion US dollars in 2021 and it is projected to reach 77 billion US dollars by the end of 2022. The global cybersecurity market size is forecast to grow to 345.4 billion US dollars by 2026.



The increase in cybersecurity spending is a result of the growing cyber threats mainly due to the pandemic and the war in Ukraine. However, the spending to provide cybersecurity remains insufficient due to the increasingly complex cyber threat landscape.

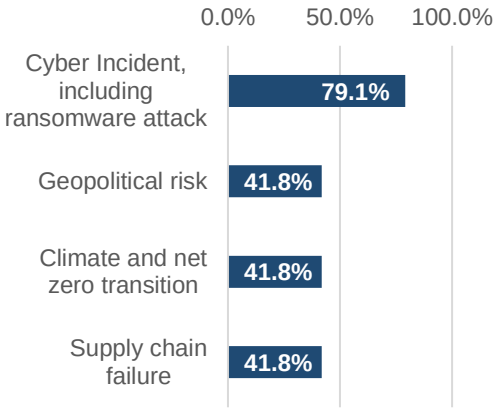
Since 2018, Europe has been bracing in response to a dramatic increase in cyberattacks. The risk from cyberattacks has increased between 300 and 400 percent since Russia's latest invasion of Ukraine on 24 February 2022.

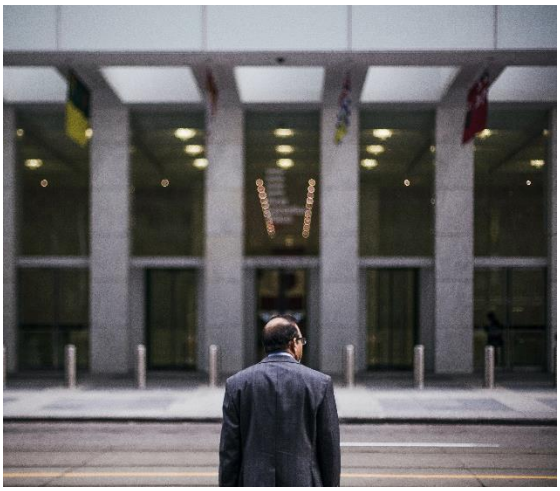
Russia based cyber-groups has been using cyberattacks as weapons targeting government agencies and businesses across Europe.

Business leaders are consistently rating cyberattacks as the biggest enterprise risk in 2022 followed by geopolitical, climate and supply chain-related risks. Even more so today, it is crucial for companies to establish a dynamic and continuous process of monitoring the evolving risk environment.

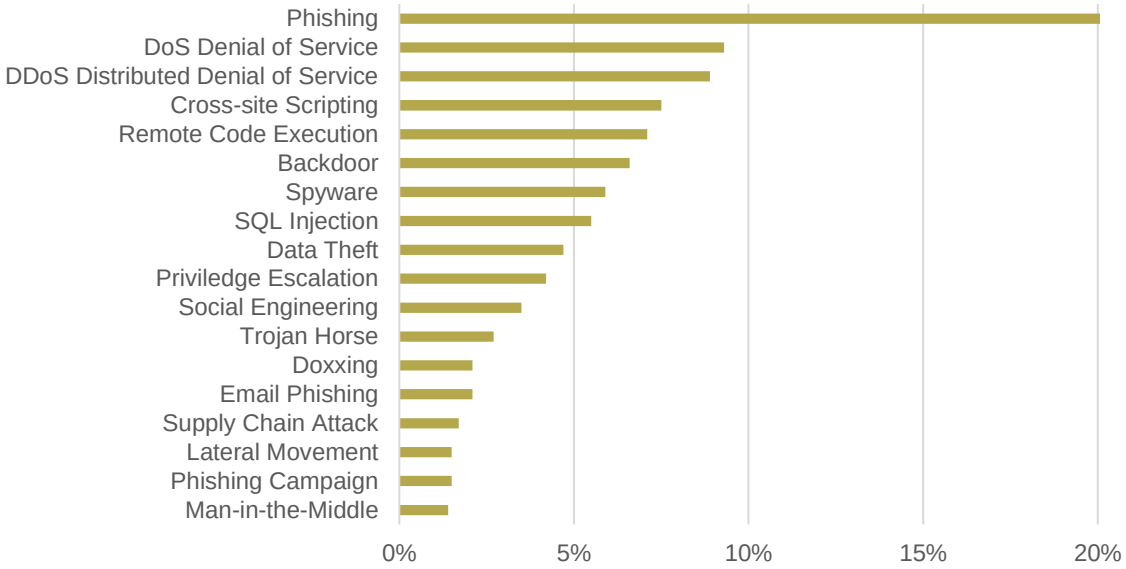
Cybersecurity is an important consideration when considering partnerships and third parties. The majority of business leaders consider cybersecurity risk as one of the primary considerations when choosing who to conduct business with.

Top risks for business 2022





Cyber trends 2022



According to cybercrime trends in 2022, phishing is the biggest trend in which scammers try to lure sensitive information or data from users by disguising themselves as a trustworthy source.

A fake e-mail asking the users to click a link and verify their account details is an example of phishing. As human error is still one of the primary reasons for data breach, insider threat may bring down a whole organisation with millions of stolen data.

Email is the primary entry point of 95 percent of malware attacks and human error is the biggest reason for information breaches.

Cyber-crime statistics show that almost quarter of the files and folders stored by a company are accessible to all employees.

More than half of companies have over 1,000 sensitive files open to every employee.

A study conducted among financial organisations, fuel and energy business, government bodies, and industrial companies showed that cybercriminals can penetrate 93 percent of company networks, where an external attacker can breach an organisation's network perimeter and gain access to local network resources.

In the first quarter of 2022 there were 1,025,968 total phishing attacks and it is the worst quarter for phishing observed to date.

Denial of Service (DOS) and Distributed Denial of Service (DDoS) have mainly similar result where the attack interrupts a computer, a server or any other device and makes it unavailable to users. For both, the attackers flood the targeted device with so many requests that its resources become insufficient for normal functioning.

The key difference between DoS and DDoS is the number of devices that are used for the attack. While a DoS attack uses only one system, a DDoS attack sends requests from multiple systems, so it is quicker. This makes harder to detect and mitigate DDoS attacks, while also producing greater damage.

Six Ransomware statistics

95%
of breaches caused by human error

$ 265B
Estimated annual cost of cyerattacks in 2031

32 %
Of cyberattack victims pay the ransom

57 %
Of businesses successully recover data using a backup

$ 1.85M
Average cost of recovery from a ransom attack in 2021

65%
The amount of data victims get back after a cyberattack

Ransomware incidents have become increasingly prevalent among organisations and government entities as well. Current ransomware trends are more coordinated, which means ransomware attacks are more frequent and severe.

Projections indicate that there is one ransomware attack every 11 seconds during 2022.

Ransomware is a form of malicious software or malware created by cybercriminals where:

- Access to data or IT systems on an organisation´s device is block.
- A ransom is demand in exchange to restore access.
- Demanding ransoms in a form of cryptocurrency to eliminate the risk of being uncovered is the trend.

CRITICAL ACTORS

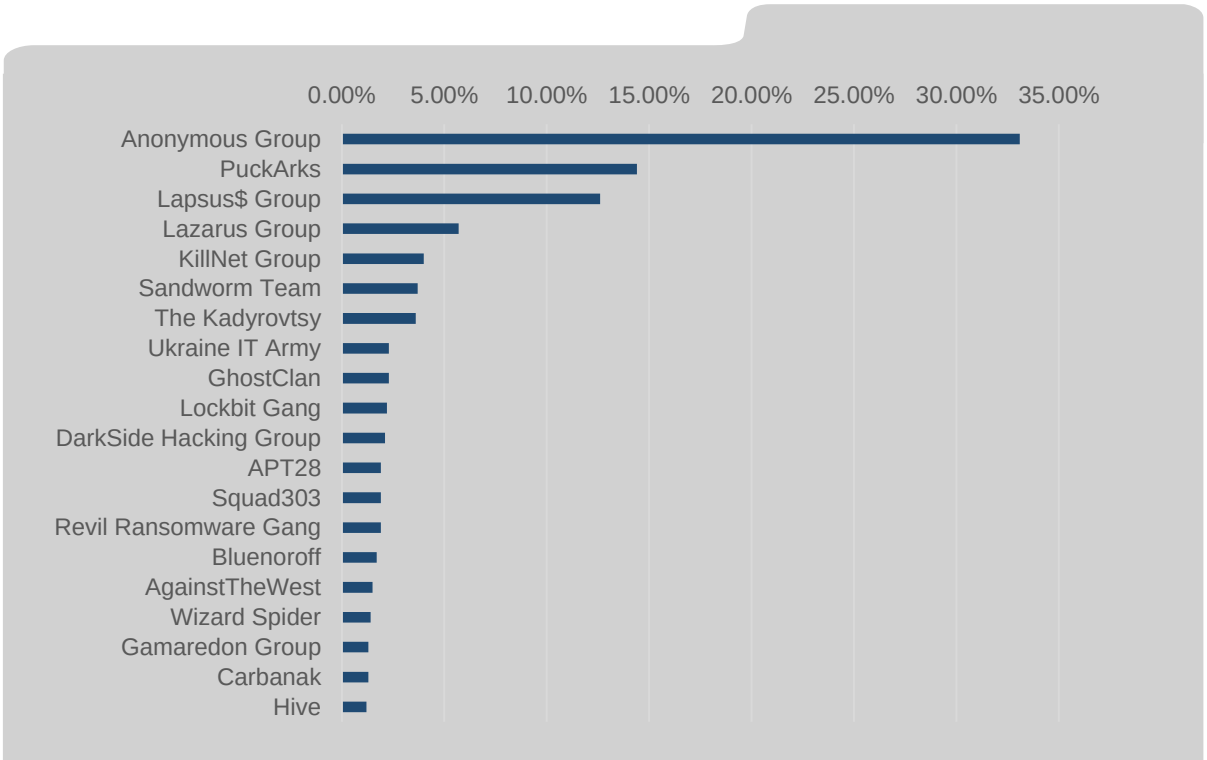
Since Russia's invasion of Ukraine on 24 February 2022, 2Secure have monitored changes in the main actors involved in cyberattacks. Various groups of cyber activists have targeted different organisations motivated by both pro-Ukrainian and pro-Russian sentiment. Several profiles have emerged during the war, some of them already existing before the beginning of the military operations, e.g., Conti and SandWorm on the Russian side, or Anonymous on the Ukrainian side. Some other groups were born during the conflict itself, such as the Ukraine IT Army, a volunteer hacker group.

Cyberattacks launched by pro-Russian hacker groups have targeted Western entities supporting Ukraine like companies, government agencies and other public bodies linked to critical national infrastructure.

Several countries such as the United States, the United Kingdom, Canada and Germany have experienced an increase in ransomware incidents after the start of the war in Ukraine, as they are perceived as leaders in the punitive response against Russia.

Government agencies and private entities need to ensure adequate cyber security processes within their organisation and supply chain; first by identifying vulnerabilities, reviewing current policies and incident response plans, improving cyber security training and building a robust cyber security posture.

Main threat actors in 2022



CRITICAL SECTORS

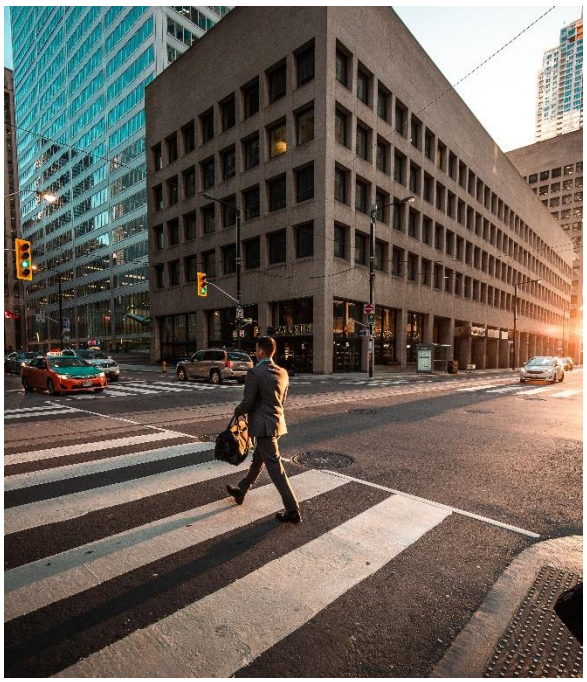
The biggest targets for cybercriminals are industries and business that store valuable information, such as:

- Healthcare
- Finance
- Governments and public administrations

Since the war in Ukraine started, 2Secure have observed an increase in targeting of critical national infrastructure and strategic sectors like:

- Energy
- Telecommunication
- Transport
- Oil and gas companies
- Renewable energy

Another trend 2Secure has observed in 2022 is an increase in the number of disruptive attacks targeting supply chain companies, due to the large domino effects that an attack against a physical or IT supply chain company can have on both the targeted organisation and its customers.



Case study

As the world is becoming increasingly connected with millions of networks interconnected with one another, the risk of being subject to a cyberattack, and indeed the extent of one's loss, is increasing rapidly. In a report released in March 2022, almost 40 percent of businesses in Britain stated that they had been subject to cyberattacks during the past year, with 82 percent of business leaders regarding cyber threats as a very high priority.

However, cyberattacks should, indeed, be regarded as a palpable threat to private individuals as well. In November 2021, the data on celebrities, politicians, and other high-net individuals was accessed by the ransomware group Conti, who accessed the data via Graff – a high-end jewellery company based in London. Thousands of documents were released on the dark web, with plenty more documents used as ransom against the firm. Conti asked a significant amount of ransom fee from Graff. What this demonstrates, however, is that anyone can be a victim of a cyberattack, regardless how safe one's internal systems are. Individuals, especially high-net individuals, ought to exercise caution when sharing information with third parties, thus minimising one's exposure in the millions of interconnected networks.

RECOMMENDATIONS

As the supply chains and networks are globalised and interconnected, the cyber risk exposure is increasing in an unstoppable way. The total cost of all cybercrime damages in 2021 was approximately US$6 trillion worldwide, compared to US$2 trillion in 2020. Organisations must ensure robust cyber security processes both within the organisations and third-party suppliers.

2Secure recommend:

Plan: as with all risks, the best way to prevent or minimise potential damages is to try to avoid them. Start by identifying your organisation vulnerabilities. It is also important you establish or review current policies and incident response plans, and conduct cybersecurity training within your employees. Train your employees in information security awareness and hire information security experts, who play an essential role in cyber preparedness and information security awareness.

Establish proper routines and processes: when a cyberattack occurs, having planned and established proper procedures beforehand is key. Ensuring that your organisation has implemented robust incident response plans and recovery capabilities will help mitigating the risk as well as speed up the recovery process if a cyberattack occurs. This extends to supply chain partners as well. Ensure proper cybersecurity processes before on boarding any new business or individual in your ecosystem and monitor to guarantee compliance of processes by all partners.

A proper response: before an incident occurs, make sure you are aware of the process and have tested all elements of your plan. Assess the incident and implement the protective response measures. Consider the option of not paying the ransom and the need to preserve evidence for authorities. Only turn off devices if they cannot be disconnected from the network. Contact 2Secure and we will help you with essential crisis management activities.

Seek guidance: make use of professionals to guide you through the proactive and reactive processes if your organisation is unsure about proper measures or responses. Seeking outside help is also a good way to ensure an impartial third-party review of current cyber routines and planning.

+46 101 740 310

Visit our website for more information on how 2Secure can support you with your international security and risk management needs.

We provide bespoke and tailored analysis, trend monitoring, enterprise risk management support, training, global support, and risk assessments on a variety of issues and locations around the world.

Email or call our experts for an obligation free discussion today.

2Secure

Box 34037 • 10026 Stockholm • www.2secure.se