Theme: Cybersecurity
A topic we cannot ignore

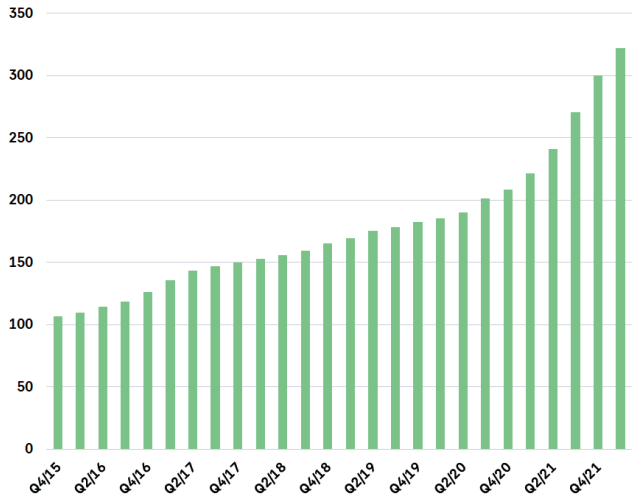
Economic crime has moved out into cyberspace and into our computers. Private individuals, businesses and government agencies are more and more frequently subjected to cyberattacks. Cybercriminals, who are often untraceable, are among our biggest security threats. The already high costs of cybercrime are soaring. This has turned internet security – or cybersecurity – into a sector that is growing at record speed.

Today a large percentage of the world's population is already connected to the internet 24/7 through mobile phones, tablets and computers, while new kinds of connected devices are growing exponentially. More and more systems are digitally connected, and the internet of things (IoT) – which links together various smart devices online – is a fast-growing trend that includes everything from self-driving cars and smart refrigerators to clothing that can control electronic devices. According to the organisation iPropertyManagement, the number of IoT devices surpassed 14.2 billion in 2019, up from 12 billion in 2018. The number of IoT devices is expected to exceed 75 billion by 2025.

This technology is gaining ground not only at the consumer level but also the industrial level, for example, in the development of smart city solutions. Traffic planning is another area where IoT is expected to make a breakthrough. The list of applications is long and growing.

The rising number of connected devices is also reflected in the growth of a telecom operator like Swedish-based Telia. The company has seen accelerating growth in mobile subscriptions for machine-to-machine communication. At the end of Q1 2022, this kind of subscription had increased by 45 per cent compared to the same date in 2021, and by 7 per cent since year-end 2021.

Accelerating growth in subscriptions for machine-to-machine communication



Source: Telia

The chart shows how the number of Telia machine-to-machine communication subscriptions for connected devices has grown since Q1 2015 (index 100). The number of subscriptions is now at 4.2 million. As indicated, growth has accelerated in recent years.

Cybercrime – our fastest growing security threat

As our society continues to digitise, there is greater incentive for criminals to move into the digital world. Cyberattacks are among our fastest growing security threats, and there is no sign that this growth is slowing, despite the record amounts being spent on cybersecurity. The first cyberattack to attract widespread attention, which came to be known as the Morris Worm, took place in 1988. The worm destroyed some 6,000 computers, which at the time represented 10 per cent of the entire internet. Since then, the trend has unfortunately accelerated, both in terms of the frequency of attacks and their degree of sophistication. According to recent statistics, a ransomware attack – using a virus programme that encrypts data – is carried out every ten seconds. According to Cybersecurity Ventures, by 2031 we can expect a new attack on an individual or organisation every three seconds. An FBI agent who works with cyber intrusions told *The Wall Street Journal* as early as 2018 that every US citizen can assume that their personal data have been stolen and are available on the dark web, a well-concealed part of the internet.

More than 70 per cent of all attacks are for economic motives. A report from as far back as 2013 noted that cybercrime had a turnover greater than the global trade in marijuana, cocaine and heroin combined. Intellectual property rights theft and espionage account for most other cyberattacks.

One of the very largest attacks to date was the 2017 WannaCry ransomware attack, in which 230,000 computers in 150 countries were infected with a virus. Last year, one trend was to attack different kinds of platforms, such as firms that supply software to other companies. These companies were then infected by a computer virus when they updated their software. One such attack targeted the software company Kaseya and led to a majority of the Swedish-based Coop's 800 supermarkets being forced to close since their point-of-sale tills stopped working. According to a survey carried out by the audit firm PWC, an increased number of attacks on so-called cloud services is expected in 2022.

A selection of attacks over the past year

Meta (Facebook)	April 2021 – data from more than 530 million users were stolen and published online
Colonial Pipeline	May 2021 – the oil pipeline operator was hit by a ransomware attack carried out by the DarkSide hacking group, which led to production shutdowns and panic buying in the US.
T-Mobile	August 2021 – data from 50 million customers were stolen by a 21-year-old.
AP-HP	September 2021 – personal data from 1.4 million people were stolen from a hospital in Paris.
Poly Network	August 2021 – cryptocurrency worth more than 600 million dollars was stolen.

Source: Fortinet

Some common types of cyberattacks	
Malware	Harmful software, such as a computer virus, spyware or Trojan horse.
Ransomware	Malware that locks or encrypts data until a ransom is paid.
Phishing attacks	Measures to obtain sensitive information (such as passwords or credit card information) through a disguised email, phone call or text message.
Social Engineering	Psychological manipulation of an individual to obtain confidential information; often overlaps with phishing.
DDoS (distributed or denial of service) attacks	Overload of a website, for example, thus preventing users from accessing it.
Wiper attack	Attacks aimed at erasing important data.

Hacker groups are often behind attacks

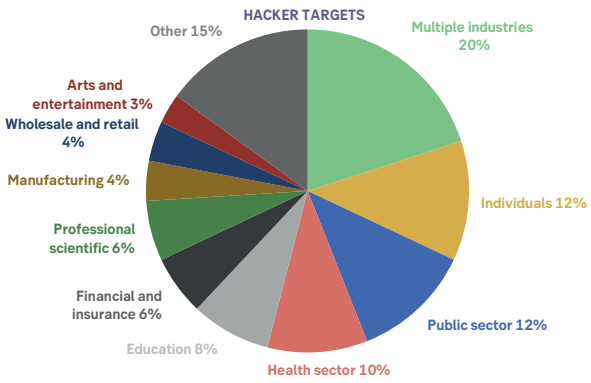
While individuals do carry out cyberattacks, most known large-scale attacks have been carried out by well-organised hacker groups. For example, the work of the group known as Shadow Brokers is behind two of the biggest attacks in history – NotPetya and WannaCry – with the latter probably carried out by the North Korean-based Lazarus Group. The attacks were based on software vulnerabilities that the group managed to steal from the US National Security Agency (NSA). A third example is the cybergroup Anonymous, which is considered the first hacker group to have played a revolutionary role in society. The group was behind an attack on PayPal that cost the company USD 5.36 million. It has also gone on the attack against Russia since it invaded Ukraine, including Russian state television.

A weapon in warfare

Technological advances have improved the efficiency of public sector activities and essential services, with the result being that large parts of society today are totally dependent on IT and the surrounding infrastructure. Attacks are generally not expensive to carry out but may cause enormous damage and have a devastating impact on the functioning of society, while the risk of getting caught is relatively low, at least so far. As a result, there is a significantly growing risk of cyberattacks that can have consequences for the supply of drinking water and the distribution of electricity, as well as the functioning of electronic payment systems and healthcare facilities.

In the ongoing conflict between Russia and Ukraine, Russian or Russian-backed cyberattacks on Ukraine have been regarded as part of Russia's hybrid warfare strategy. The objective, according to Microsoft, which identified 237 cyberattacks on Ukraine just before war broke out, is to destroy, disrupt and infiltrate. The day before the invasion, hundreds of targets in Ukraine's government agencies and IT, energy and financial sectors were attacked. These attacks, aimed at erasing data, are known as wiper attacks. According to Microsoft, the Russian intelligence agency GRU was closely affiliated with those carrying out the attacks.

No one is spared



Source: hackmageddon.com

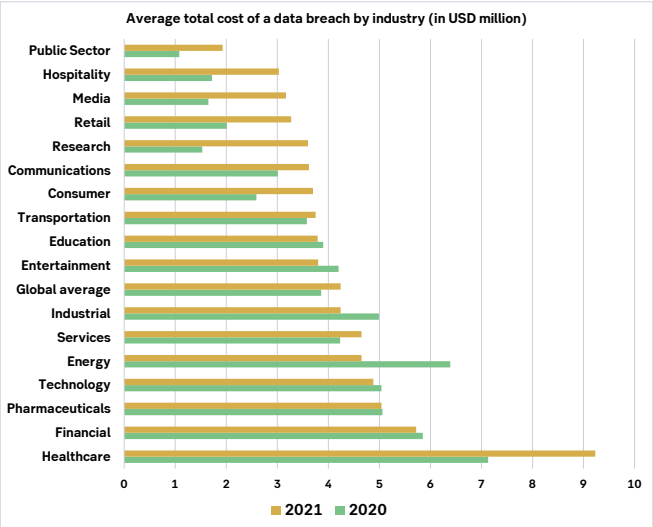
The chart shows that no particular target stands out. Instead, individuals as well as all kinds of activities have been subject to cyberattacks.

Devastating consequences and soaring costs

According to a report by Cybersecurity Ventures published in early 2021, cybercrime costs globally are expected to rise 15 per cent annually in the years ahead. By 2025, costs are expected to have reached USD 10.5 billion annually, an increase of USD 7.5 billion since 2015. In comparison, costs for natural disasters totalled USD 300 billion in 2017, a record year, according to the World Economic Forum.

The average total cost for a company affected by a data breach is rising and is currently estimated at USD 4.2 million, according to IBM Security. In addition to the direct cost of restoring functionality etc., an attack also often leads to a halt in production and decreased trust in the company. This in turn may cause difficulties in attracting new customers and securing new financing. For small businesses, the consequences are often devastating. More than half of all cyberattacks have targeted small and mid-sized firms, and 60 per cent of companies that have fallen victim to an attack are no longer in business six months after the incident, according to statistics from Mastercard.

The costs associated with an attack are clearly rising



Source: IBM Security

In the chart above, we can clearly see that the costs associated with an attack have risen for most sectors, with the healthcare sector standing out by a wide margin.

Large-scale cybersecurity investments create opportunities

Since the number of victims is growing and the cost of an incident is high and rising, more and more companies and other organisations around the world are investing in preventive measures to reduce the risk of cyberattacks. The future of companies that provide products and services in this field certainly looks bright. Cybersecurity includes protecting computers, networks, software and data from unauthorised access. According to an analysis by Bloomberg Intelligence, cybersecurity investments may exceed USD 200 billion by 2024, up from about USD 134 billion in 2020. This is an enormous amount in absolute terms, but the figure actually looks low relative to expected costs associated with cybercrime.

The cybersecurity industry has historically provided services to enable compliance with various standards. It is now also increasingly common to help organisations raise their awareness of various security risks, as well as contribute know-how and thereby improve the ability of these organisations to protect their assets.

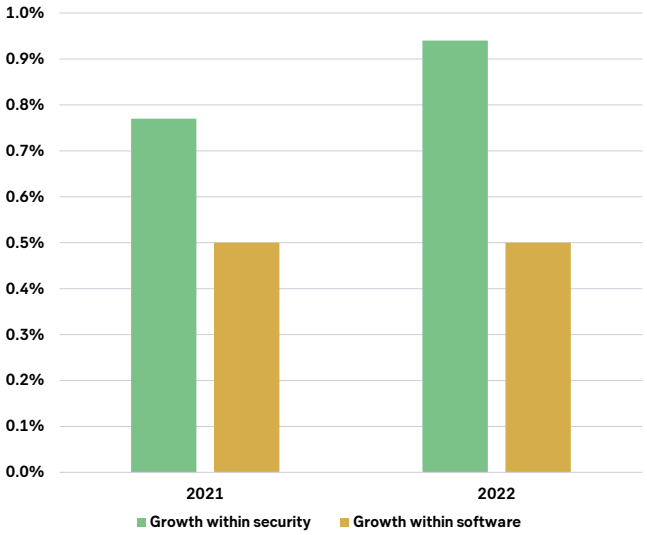
As noted, cyberattacks have become increasingly sophisticated, but fortunately so have the tools to avoid, prevent and mitigate their effects. New companies and new products and services are continuously being launched. One example is artificial intelligence (AI). According to a survey carried out by IBM Security, the cost of a data breach is 30 per cent lower for companies with a well-developed AI platform.

Regulations are driving industry growth

In recent years, a number of new regulatory measures have been implemented. In Europe, the EU General Data Protection Regulation (GDPR), adopted in 2018, plays an important part in making the internet more secure for private individuals. The directive regulates how companies collect and manage their customers' personal data. Companies that fail to comply with these requirements may be ordered to pay heavy fines.

The NIS Directive (directive on security of network and information systems) is aimed at fostering security measures and increasing the level of protection for critical infrastructure in EU member countries. Furthermore, the EU's new cybersecurity guidelines for banks entered into force in 2020. It is now clearer how various financial services should be able to manage internal and external risks associated with IT and security. There is even more proposed legislation in the works related to improved IT security.

A larger share of expenditure will go towards security



Source: Morgan Stanley

The chart shows the rate of growth in expenditure for security and for software generally in 2021 in per cent for 60 US organisations, as well as their forecasts for 2022.

Cybersecurity – high on the list of priorities

A survey by Morgan Stanley early this year of 60 US-based IT executives indicates that investments in information security will accelerate in 2022. In contrast, investments in software generally are expected to grow at about the same rate as in 2021.

According to the survey, a heightened threat environment is the main reason for the increased demand. Upgrading and updating existing technology is another driver, as are the growing points of attack for cyberthreats. More stringent regulations and regulatory compliance were also mentioned as reasons for the companies' investments.

The strongest growth is expected in the field of enhanced protection of company networks. Many companies build their network architecture on the basis of cloud services. This is also true of IT security, which increasingly consists of cloud-based services instead of – or in addition to – the company's own personnel and software.

One fast-growing technology or security concept is Secure Access Service Edge (SASE). A number of local networks are connected and combined with security services in a cloud-based model. The model identifies the user and the device being used, applies customised security and provides secure access to the application or data intended. Organisations can thus allow access regardless of where the user is located. Since the number of connected products is growing rapidly, there is increasing demand for this service.

Software that provides protection for an increased number of new interfaces is another area that is growing rapidly. This software is used for everything from mobile phones and computers to IoT devices, since they are frequently the target of attacks aimed at gaining access to valuable assets within networks. This area includes, for example, virtual private networks or VPNs (commonly used for remote work, which has increased due to the pandemic) and regular updates of antivirus programmes.

A third fast growing area is identification and asset management software, a framework of policies and technologies aimed at allowing only authorised people access to certain data. The software is centralised, and one example is to approve access for employees connected to a virtual network so they can work outside the office.

Conclusion

As society becomes increasingly digitised, there are also growing incentives for criminals to go digital. Unfortunately, the number of cyberattacks continues to climb, and so do the costs for those who are affected. It is easy to get the feeling that criminals have a head start in this field compared to the products and services available to prevent cyberattacks, but advances are rapidly being made. More and more resources are being invested in cybersecurity, and a growing number of companies want a piece of this fast growing market. There are many indications that plenty of attractive investment opportunities exist in this field and that this will be the case for a long time to come.