

Cybersecurity trends to watch in 2022 - blueAPACHE

Canonical: <https://www.blueapache.com/blog/cybersecurity-2022>

Details:

Published on 22 February 2022, this article reviews cybersecurity statistics and trends reported for 2021 and forecasts discussed at that time. The key trends we observed were the increasing cost of cybercrime, the most common exploits and loopholes, a growing awareness about cybersecurity, and some exciting advancements in cybersecurity tech.

Trend 1: The total cost of cybercrime is climbing faster than predicted

Cybercrime is getting expensive. In 2021, it was estimated to cost the world economy around 1 trillion (or over 1% of the global GDP), which is 50% higher than experts predicted in 2018. The Australian Institute of Criminology estimates that the total economic impact of Cybercrime to Australia was \$3.5 billion. In a 2021 survey by Cisco, 65% of Australian small and mid-sized businesses had suffered a cyber incident in the previous 12 months, and the average cost of the attack was over \$645,000 for two-thirds of impacted businesses. Although the average cost of a data breach has climbed, the data is not consistent across countries, industries or even organisations. One thing that is clear, the organisations that were prepared, having cybersecurity plans and trained incident response teams, were better positioned to mitigate financial loss and recover more quickly.

Trend 2: The most common loopholes and vulnerabilities in 2021

Some of the most notorious and large-scale data breaches from past years were also among the most common kinds of attacks. Through 2021, they tended to fall into the following three categories: Malware Any kind of malicious software designed to damage computer systems is considered malware. Malware is an umbrella term that includes trojans, viruses, worms, ransomware, spyware, botnets, and adware. Malware drove the greatest damage and costs for organisations. Ransomware A specialised form of malware, ransomware encrypts data in infected systems and often displays a message that instructs the recipient to pay a specific amount to restore the files. Ransomware can be downloaded when a user opens a malicious email attachment or file. Some highly sophisticated ransomware are self-propagating or even target dedicated data backups making it even more tricky to contain and remediate. A report from IDC found that Australian organisations were more likely to pay out in the event of a ransomware attack, making Australia an attractive target. Ransomware attacks increased by 60% in 2021 compared to the previous year, and the original article reported an average ransom paid of \$1.85 million without specifying the currency. Phishing More than a third of cyber attacks on companies involve phishing. To complicate this further, around 38% of end-users will fail phishing tests if they receive no cybersecurity awareness training.

Trend 3: Increased awareness and preparedness

While so many statistics and trends around cybersecurity can seem alarming, such as the increasing numbers of attacks and higher costs we've touched on already, there are some very encouraging trends taking shape. Despite the abysmal stats regarding security vulnerabilities, cyberattack preparedness — or the lack thereof — and the questionable effectiveness of implemented strategies, there are some positive trends on the horizon. In a recent survey from Cisco, 89% of company

executives place cybersecurity as a high priority. This is a positive trend because organisations that are well prepared for a cybersecurity incident are proven to recover better, faster, and with less financial loss.

Trend 4: Advances in security technology

Also in the good news category, advances in security technology, like artificial intelligence, improvements in Security Information and Event Management (SIEM), and network traffic analysis tools are helping organisations better protect themselves while they reduce administrative burdens. By 2023, Gartner predicts 40% of privacy compliance technology will rely on artificial intelligence to boost data privacy and security and reduce administrative burdens. With the rise in cybercrime and the high cost of a data breach, many organisations choose a cybersecurity partner to help them ensure they have a solid cybersecurity plan and security processes in place. If your organisation could use support with cybersecurity, we can help you assess where you are now and help you reach your security goals. To find out more, please contact us [here](#)

How much did cybercrime cost the world economy in 2021 according to the blueAPACHE article?

In 2021, cybercrime was estimated to cost the world economy around \$1 trillion, or over 1% of global GDP, which was 50% higher than experts predicted in 2018.

What was the estimated economic impact of cybercrime on Australia?

The Australian Institute of Criminology estimated that the total economic impact of cybercrime to Australia was \$3.5 billion.

What are the three most common categories of cyberattack vulnerabilities identified in the blueAPACHE 2022 blog post?

The three most common categories were malware, ransomware, and phishing.

How much did ransomware attacks increase in 2021, and what was the average ransom paid?

The February 2022 article reported a 60% rise in ransomware attacks in 2021 and an average ransom paid of \$1.85 million, without specifying the currency. It separately cited IDC on Australian organisations' propensity to pay; it did not attribute both figures jointly to IDC and HPE.

What proportion of cyberattacks on companies involve phishing, and how does lack of training affect phishing test results?

More than a third of cyberattacks on companies involve phishing, and around 38% of end-users will fail phishing tests if they receive no cybersecurity awareness training.

What technological advances does the blueAPACHE article highlight as helping organisations improve cybersecurity?

The article highlights artificial intelligence, improvements in Security Information and Event Management (SIEM), and network traffic analysis as technologies intended to improve protection and

reduce administrative work.

What does Gartner predict about the role of artificial intelligence in privacy compliance technology by 2023, as cited in the blog?

The 2022 article cited Gartner's forecast that, by 2023, 40% of privacy compliance technology would rely on artificial intelligence. This was a forecast, not a measured result for 2023.

How can organisations get help with cybersecurity according to this blueAPACHE blog post?

Organisations can contact blueAPACHE to discuss an assessment of their cybersecurity needs and available support.