According to the [Global Risks Report of 2020](http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf) by the World Economic Forum, risks associated with cyber-attacks stand at seventh and eighth number in terms of likelihood and impact respectively. Cyber threats are now the new norm across private and public sectors, and continue to grow in the year 2021. The [Targeting Scams report](https://www.accc.gov.au/publications/targeting-scams-report-on-scam-activity/targeting-scams-2019-a-review-of-scam-activity-since-2009) of 2019 by Australian Competition and Consumer Commission (ACCC) identified that Australians lost more than $634 million to scams in 2019 alone. While it’s hard to quantify the real cost of cybercrimes to the Australian economy, estimates indicate the annual cost to be as high as $29 billion.

The Australian Cyber Security Centre’s (ACSC) [Annual Cyber Threat Report](https://www.cyber.gov.au/sites/default/files/2020-09/ACSC-Annual-Cyber-Threat-Report-2019-20.pdf) of June-2019 to July 2020 for Cyber Security Australia shows two notable spikes in cyber security incidents during October 2019 and April 2020. Particularly at the start of COVID-19 pandemic, there was an increase of spear phishing campaigns and pandemic-themed malicious cyber activity. From 10th to 26th March 2020, ACSC received more than 45 COVID-related cybersecurity incident reports, as cybercriminals swiftly adapted phishing methods to take the coronavirus pandemic to their advantage.

To say the least, the pandemic affected all businesses – small and big. It also increased cybercrime ratio multiple times due to the manifold possibilities around remote working and uncertainty along with lack of knowledge of protecting businesses while following a work-from-home model. In the wake of the pandemic, nearly all industries had to adopt new solutions quickly in order to adapt to the changing threat landscape.

2020 was a year of uncertainty and sudden adjustments. Some organizations may have responded well to the new challenges – others, maybe not. However, the new normal is here to stay for a while now. So how can startups and businesses prepare themselves for data security in 2021 and beyond? To understand this better and make wiser decisions, let’s have a look at 10 must-know cyber-attack statistics and trends for the year 2021.

1. **Growth of Cybercrime Costs**

It is estimated that by 2025, cybercrime will cost [approximately $10.5 trillion](https://www.globenewswire.com/news-release/2020/11/18/2129432/0/en/Cybercrime-To-Cost-The-World-10-5-Trillion-Annually-By-2025.html#:~:text=Every%20U.S.%20business%20is%20under%20cyberattack&text=18%2C%202020%20(GLOBE%20NEWSWIRE),%243%20trillion%20USD%20in%202015.) annually around the world, up from $3 trillion in 2015. This amounts to a growth rate of 15 percent every year. Cyber crime inflicted damages are estimated to reach [6 trillion USD](https://cybersecurityventures.com/annual-cybercrime-report-2020/) in 2021. If we measure cyber crime as a country, it can be considered as the world’s third largest economy after USA and China. This is even larger than the damage caused annually as a result of [natural disasters](https://www.forbes.com/sites/rajindertumber/2019/01/05/cyber-attacks-igniting-the-next-recession), and even more profitable than the combined trade of [illegal drugs](https://blogs.cisco.com/financialservices/how-to-prevent-the-bank-robbery-no-one-can-see) globally.

This cost has been estimated by looking at historical cybercrime data that includes yearly growth and an increase in state-sponsored and organized cybercrime campaigns. The cybercrime costs include destruction and damage of data, productivity losses, stolen money, financial and personal data theft, embezzlement, theft of intellectual property, forensic investigation, fraud, reputational damage, disruption to the services, and restoration of data.

In Australia alone, cybercrime costs amount [to $29 billion](https://www.greenlight-itc.com/cyber-crime-security-statistics-australia/) every year. 53% of this cost is incurred on detection and recovery. The average cost incurred by a business on a single breach is $276,323.

[make an infographic for last paragraph]

https://www.greenlight-itc.com/cyber-crime-security-statistics-australia/

1. **Cyber Security for Small and Medium Business Australia**

Cyber-attacks are particularly becoming a threat for small and medium sized businesses, considering they are easier targets. According to a 2019 [Cost of Cybercrime](https://www.accenture.com/us-en/insights/security/cost-cybercrime-study) Study by Accenture, small businesses faced 43 percent of cyber-attacks, but only 14 percent were prepared for defense.

A cyber-attack not only interrupts with routine functions of the organization, it can also bring permanent harm to IT infrastructure and assets – making them irrecoverable in the absence of required resources or budget. Because of lack of resources and finances, small and medium businesses often ignore the need to invest in security, and become easier target for cyber criminals.

According to a [State of Cybersecurity Report](https://www.keepersecurity.com/ponemon2019.html) by Ponemon Institute, small and medium businesses all over the globe showed alarming statistics

* Attack Frequency – 71% of SMBs surveyed had faced a cyber-attack in their lifetime and 66% of them had suffered an attack in the last 12 months.
* Weak Security Measures – 45% believed that their security measures are not strong enough to mitigate cyber attacks
* Difficult to Detect – 69% of SMBs suffered attacks that evaded their intrusion detection systems and 82% reported evasion of their anti-virus programs.
* Employee Passwords – 68% of worldwide SMBs reported that their employee passwords were lost or stolen during the past year.

The attacks faced by small businesses most commonly included:

* 57% Phishing and Social Engineering attacks
* 33% Compromised or stolen devices
* 30% of credential theft

If you understand the target and consequences of each of these attacks as a business leader, you can not only minimize the potential but also prevent future threats altogether.

The ACSC conducted a [cybersecurity survey for small business](https://www.cyber.gov.au/acsc/small-and-medium-businesses/small-business-survey-results) in November 2020. This survey concluded that 62% of the respondents, which included small and medium businesses, had experienced a cyber security incident. Moreover, 1 in 5 SMEs were unaware of the term “phishing”. Almost half of the respondents agreed on having a low level understanding of cyber security, rating themselves as ‘average’ or ‘below average’ with poor cyber security practices. Again, almost half of them reported that they spent less than $500 on cyber security every year.

[infographic for the paragraph]

https://www.cyber.gov.au/acsc/small-and-medium-businesses/small-business-survey-results

The report states that the biggest barriers to effective cyber security practices are the failure to identify weaknesses, not knowing where to begin, inability to understand the risk and impact of cyber threats, a lack of dedicated IT staff, and inefficient planning to respond to cyber-attacks.

The long-term costs of data breaches can go as far as months to even years. These are usually costs that are unanticipated during the planning process and can have a significant impact. These include disruption in business processes, data loss, notification costs, revenue loss resulting from downtime, and even the brand’s reputational damage.

1. **Remote Work Challenges**

A 2020 Global Risk Report on [Cybersecurity in the Remote Work Era](https://www.keeper.io/hubfs/PDF/Cybersecurity%20in%20the%20Remote%20Work%20Era%20-%20A%20Global%20Risk%20Report.pdf) by Ponemon Institute surveyed 2215 IT and security employees in the USA, UK, Scandinavia, Australia and New Zealand. All these respondents belonged to organizations that directed their employees to work from home during COVID-19 pandemic.

This study found out that the security effectiveness of the organizations was significantly reduced due to the remote workforce model. It showed that prior to the pandemic 71% of respondents believed their organizations to be effective at mitigating vulnerabilities, risks and attacks across their organization. However, for post-covid times, only 44% of respondents believed the same.

Furthermore, the time to respond to cyberattacks has also increased according to 56% of respondents and only 27% believe that it takes the same amount of time as pre-covid time.

Customer records are most vulnerable during remote working according to 55% of respondents. This is followed by financial loss, which is at risk according to 48% of respondents.

In terms of authentication, many organizations still don’t require their remote workers to use any form of authentication. Around 31% (one-third) of respondents said their organizations don’t require any authentication method. Out of the 69 percent respondents who said their organization uses authentication methods, 40% had organizations with two-factor authentication and only 35% had multi-factor authentication for improving remote access security.

[Infographic]  
https://www.keeper.io/hubfs/PDF/Cybersecurity%20in%20the%20Remote%20Work%20Era%20-%20A%20Global%20Risk%20Report.pdf

1. **Severity and Impact of Cyber Attacks**

A cyber attack can impact any organization in numerous ways. It can be of low or very high severity, and consequently result in low or high impact – from a minor disruption to a major financial loss. Regardless of the severity of the attack, it will always have a consequence – whether financial or otherwise. Organizations are usually impacted as a result of cyber attacks in the form of financial losses, reputational damage, loss of productivity, business continuity or legal liability problems.

Another high-impact threat is ransomware. Ransomware attacks have increased [25%](https://www.keeper.io/hubfs/PDF/Cybersecurity%20in%20the%20Remote%20Work%20Era%20-%20A%20Global%20Risk%20Report.pdf) in the past year, whereas phishing and social engineering attacks increased by [62%](https://www.keeper.io/hubfs/PDF/Cybersecurity%20in%20the%20Remote%20Work%20Era%20-%20A%20Global%20Risk%20Report.pdf). According to a report by Cybersecurity Ventures, a business falls victim to a ransomware attack [every 11 seconds](https://cybersecurityventures.com/ransomware-damage-report-2017-5-billion/).

CrowdStrike, an IT security company revealed in its Global Security Attitude Survey of 2020 that one of the world’s hottest ransomware targets of the world is Australia, with 67% survey respondents claiming their organization to have suffered a ransomware attack in 2020. This figure shows Australia at the second position among the surveyed countries, while India stood in the first place.

1. **Industry-wise Cyber Attacks**

Due to the different business nature of every industry, some are more vulnerable to cyber attacks than others. Although any industry can suffer a data breach, it is the ones that deal closely with people and customers that are the riskiest. These companies hold Personally Identifiable Information or sensitive customer data and are desirable targets of hackers. Some industries or organizations vulnerable to cyber attacks are:

* Financial Institutions and Banks: They have sensitive customer information such as bank account details or credit card data.
* Healthcare Industry: these have health record repositories, research data and patient record such as billing information, insurance claims and social security number.
* Educational Institutions: Hold student data such as enrollment details, financial record, research, names and address
* Enterprises: Data that can benefit competitors such as intellectual property, product concept, marketing plans, employee and client details and contract deals

In Australia, the [sectors most affected by cyber security incidents](https://www.cyber.gov.au/sites/default/files/2020-09/ACSC-Annual-Cyber-Threat-Report-2019-20.pdf) from July 2019 to June 2020 were Government- Commonwealth (436 incidents), State Government (367 incidents), followed by Health(164), Education(122) and other sectors.

[Insert Infographic]

Refer to Page7 of

<https://www.cyber.gov.au/sites/default/files/2020-09/ACSC-Annual-Cyber-Threat-Report-2019-20.pdf>

1. **Data Breaches**

According to a [report by IBM](https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/), an organization becomes aware of a breach incident after 197 days and is able to contain it in 69 days. Organizations that were able to contain a breach within 30 days were able to save more than [$1 million](https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/) as compared to those that took more time than 30 days. This statistic shows that a slow response to data breach can cause more loss to your organization in the form of loss of productivity, customer distrust and fines.

To deal proactively with a breach incident, it’s imperative to design an incident response plan. It provides guidance and allows you to be prepared in the event of a breach and respond quickly during all the phases of detecting containing, investigating, remediating and recovering.

In Australia, there were 33 data breaches resulting from ransomware in the first half of 2020, which was 20 more than the previous six months.

1. **Information Security Expenditure**

Expenditure on IT security related products and services will predictively exceed $1 trillion in 2021. According to [AustCyber Digital Census of 2020](https://itbrief.com.au/story/gartner-spending-on-information-security-and-risk-management-to-continue-to-grow-in-2020), Australians spent approximately $5.6 billion on cyber security. This figure is predicted to increase to $7.6 billion by the year 2024. Since 2017, the revenue of local sector grew by $800 million.

As of now, there are more information security providers in Australia than ever before. The domestic sector has approximately 350 security providers.

[Infographic]

https://itbrief.com.au/story/gartner-spending-on-information-security-and-risk-management-to-continue-to-grow-in-2020

1. **Phishing Emails and Email Security**

According to [Verizon](https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf), the biggest type of social engineering attack in 2020 was phishing, accounting for more than 80 percent of all reported cyber incidents.

According to Scamwatch, in 2020, [phishing was one of the most reported](https://channellife.com.au/story/country-wide-phishing-reports-up-75-in-2020) scams in Australia like previous years, but with larger numbers than in 2019. There were 44,084 reported phishing attacks, which were 75% more than 25,168 incidents reported in 2019.

Moreover, the most profitable method that scammers used was via emails and phone calls. Phone calls were the most popular delivery method in 2020, with a total of 103,153 attacks. Email attacks also increased from 40,277 in 2019 to 47,502 reported attacks in 2020. Money that was stolen with the help of emails increased from $28.36 million to $34.28 million from 2019 to 2020 respectively.

1. **Malware Attacks**

With more than [11,000 exploitable vulnerabilities](https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html) found in used software and systems by mid 2019 – with 34 percent of them without any available patches – there was plenty of malware to exploit them. According to Kaspersky, about 20 percent of users fell victim to some kind of a malware attack. However, the attacks were not equally distributed, with the attackers preferring to attack richer targets. Malware Bytes [reports](https://resources.malwarebytes.com/files/2020/02/2020_State-of-Malware-Report.pdf) that malware attacks dropped 2% on consumers, but businesses were the main targets with threats increasing at a rate of 13 percent.

The 2020 [report of ACSC](https://www.cyber.gov.au/sites/default/files/2020-10/Ransomware%20in%20Australia%20%28October%202020%29.pdf) shows ransomware to be a prevalent threat all over the world. Most of these attacks occur after a malicious activity such as phishing campaign is conducted. The report also states that ransomware across Australia will continue to be a threat due to its higher success rate. However, ACSC is against the practice of paying ransom to the hackers. According to them, paying ransom will increase an organization’s vulnerability and make them more prone to future incidents. Additionally, paying the ransom does not guarantee that the damage will be undone.

1. **Online Payment Fraud**

According to a [new study](https://www.juniperresearch.com/press/press-releases/ecommerce-losses-to-online-payment-fraud-to-exceed) by Juniper Research, Ecommerce losses due to online payment fraud will exceed $25 billion annually by 2024. The increased dependency on online shopping and popularity of Ecommerce has made it an attractive target for cyber criminals. Hence, merchants must adopt measures such as multi-factor authentication along with secure payment gateways to ensure that all requirements are effectively implemented.

**Wrapping up …**

Looking at the data, it is evident that cyber criminals are an imminent threat to governments, businesses and consumers alike. Not only are these threats external, but also internal ones such as a lack of asset management and network security, cybersecurity defenses, employee cyber awareness and cyber security policies and procedures. Thankfully, following industry best practices, implementing defense technologies from reputable vendors and conducting employee awareness trainings can help protect your organization against many of these growing threats.