



CYBERSECURITY REPORT 2020

2020 was a big year for us all but cybercriminals didn't rest! This paper presents an overview of the threats we faced in the last year as encountered by our partners and our in-house Security Operations Centre (SOC). It provides a useful backdrop when considering the changing threat landscape and evaluating your security priorities for 2021.

The extent of today's cyberthreat

The potential impact of a cyber breach

Key 2020 cyberthreats

Recommended steps and further reading

THE EXTENT OF TODAY'S CYBERTHREAT

“Cybersecurity threats are among the most significant concerns of IT managers and organisational executives alike because security incidents and data breaches can result in **reputational loss, direct economic loss, and regulatory sanctions.**”

IDC research shows that **93% of organisations have been attacked** within the past three years — and we believe, tongue in cheek, that the other 7% of organisations are simply unaware of it. Moreover, nearly half of organisations have suffered **at least one unrecoverable data event** within the past three years.”

From IDC White Paper: Addressing Cyber Protection and Data Protection Holistically

The TOP FIVE security numbers of 2020:

-  31% of global companies are attacked by cybercriminals at least once a day
-  Maze ransomware accounted for almost 50% of all known ransomware cases
-  More than 1000 companies had their data leaked after ransomware attacks
-  Microsoft patched close to 1,000 flaws in its products in just nine months
-  The average time for malware to be altered and redistributed is only 3.4 days

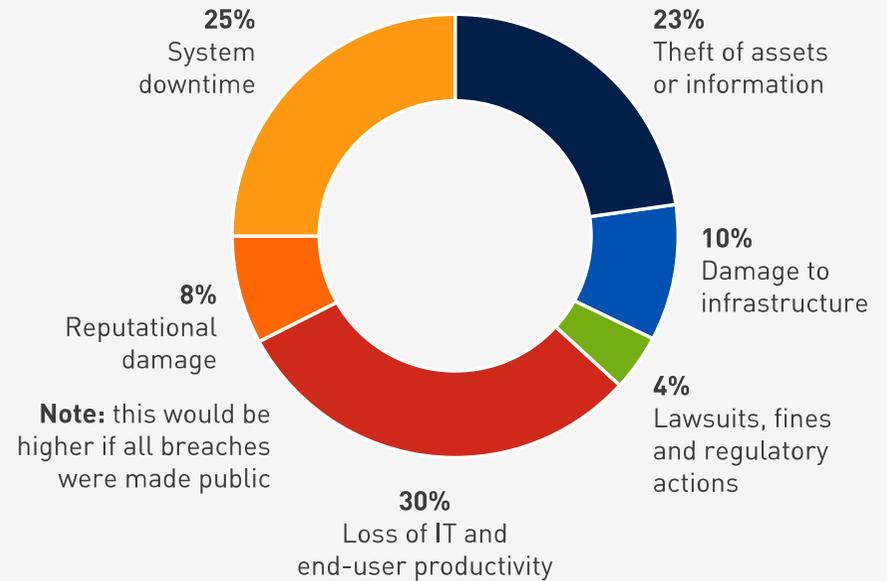
From Acronis Cyberthreats Report 2020

THE POTENTIAL IMPACT OF A CYBER BREACH

In addition to reputational damage, as well as direct and opportunity costs and regulatory sanctions, cyberattacks can result in **unplanned downtime, loss of competitive trade secrets, and permanent data loss**. IDC research has found that the average cost of downtime industrywide is **about £200k per hour**, Gartner puts this figure at **about £220K per hour**. Comparing the cost of attack prevention and recovery software with even one hour of downtime often more than justifies the price. In many cases, breaches now require public disclosure, ensuring reputational damage that is often long lasting, with no way to repair permanently lost customers or data. IDC research has found that reputational damage occurs in almost half of data breach situations, further increasing costs and justifying the costs of recovery,



Business impact of successful attacks:



Successful attacks cost large organisations **£5.3m** on average

44% of UK consumers claim they will stop spending with a business after a security breach, **41%** claim they will never return

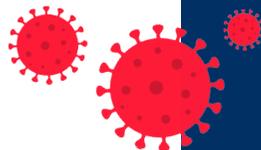
IBM and Ponemon

93% of organisations have been attacked within the past three years

IDC

*Sources: The State of Endpoint Security Risk, Emerson Network Power-sponsored study by the Ponemon Institute, PWC US CEO Survey, The Annual Study of the State of Endpoint Security Risk, Ponemon Institute, 2020

KEY 2020 CYBERTHREATS



1. COVID-19 themed exploitations

People rushed online to get information about the new pandemic this year. Seeking details on how to protect themselves, the latest news and so on. This interest resulted in a vast number of scams and other kinds of exploits.

Cybercriminals continued to use old tricks to exploit the COVID-19 theme tricking victims into entering their credentials or personal information on a phishing web page, or loading malicious payloads into documents that pretend to contain essential information related to the pandemic. There were other notable approaches, and the following examples are some of the COVID-19 themed scams that have emerged over the last year:

Fake financial support

The state of North Rhine-Westphalia (NRW) in Germany fell victim to a phishing campaign. Attackers created rogue copies of the NRW Ministry of Economic Affairs' website for requesting COVID-19 financial aid. The fraudsters collected the personal data submitted by victims and then presented their own requests to the legitimate website using the victims' information but the criminals' bank account. NRW officials reported that up to 4,000 fake requests were granted, resulting in up to \$109 million being sent to the scammers.

Fake free testing

The latest version of Trickbot/Qakbot/Qbot malware was spread in numerous phishing emails that offered free COVID-19 testing. Victims were asked to fill out an attached form, which turned out to be a fake document embedded with a malicious script.

Scams around remote education

A new pandemic-themed phishing email delivered a Formbook Trojan embedded into a bogus grading application for school teachers. Formbook is a type of infostealer malware capable of stealing login credentials from Internet browsers.

A new type of sextortion

A new variation of so-called sextortion scams sees cybercriminals threatening the life of the user rather than threatening to release a recorded video. The cybercriminals claim to know the exact location and daily routines of the victim and declare that they "could even infect your whole family with the coronavirus", demanding £3,000 in Bitcoin be transferred to stop them from doing so.

COVID-19 secrets

Certain valuable data related to the COVID-19 pandemic and suspected by some analysts to have been kept secret by the Chinese government is attracting hackers from around the world. For example, the Vietnamese state-sponsored hacking group APT32 (also known as the OceanLotus Group) reportedly attacked Chinese state organisations hoping to steal virus control measures, medical research and statistics revealing the number of infections that allegedly have not been disclosed by China.



KEY 2020 CYBERTHREATS

2. Remote workers under attack

The COVID-19 pandemic has significantly changed the threat landscape, highlighting numerous security and privacy risks associated with remote work operations – including remote access to internal company servers, virtual conferencing and security training among employees.

Our partners Acronis surveyed 3,400 companies from around the world in June and July 2020 and the results were alarming:

Nearly half of all IT managers struggled to instruct and secure remote workers

31% of global companies are attacked by cybercriminals **at least once a day**.
The most common attack types were phishing attempts, DDoS attacks, and videoconferencing attacks.

92% of global organisations had to adopt new technologies to complete the switch to remote working



As a result, **72%** of global organisations saw their IT costs increase during the pandemic

Successful attacks remain frequent, despite increased tech spending, because organisations aren't prioritising defensive capabilities properly

39% of all companies reported video conferencing attacks during the pandemic



Now that many people are having to work from home on their own computers, security threats are rampant. Not only do these home machines often lack adequate cyber protection, but many users also don't regularly apply the latest security patches for their operating system and popular third-party software, leaving their machines vulnerable.

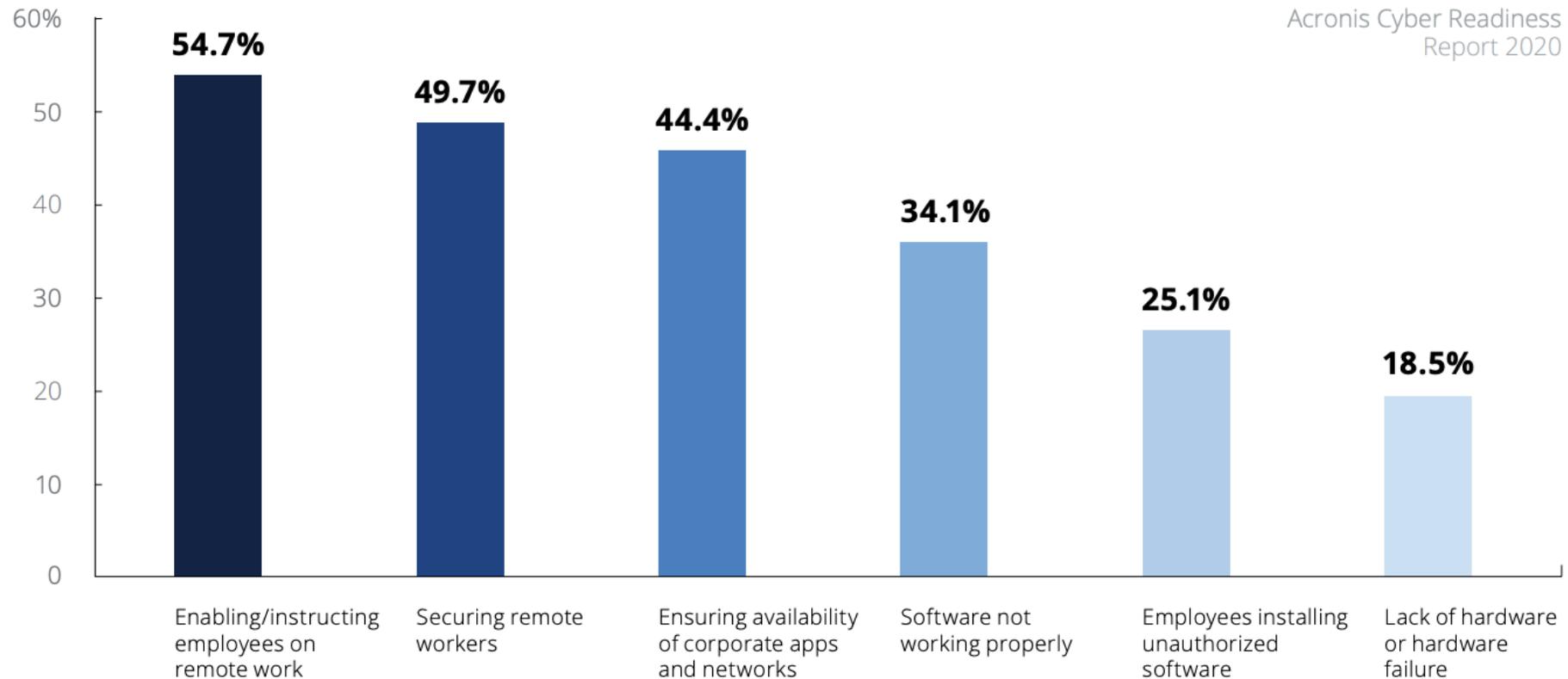
Many of these private machines are not managed by the IT department, and therefore no company policies are applied to them. Covering these vulnerabilities and patch management issues on the edge became a headache for administrators and technicians that provide the IT support to help small businesses survive during this emergency. In addition to this, home networks are often exposed to other unprotected devices, often from children and other members of the family.



KEY 2020 CYBERTHREATS

IT managers struggling the most with instructing employees on remote work

What were the top tech challenges you encountered when managing the surge in employees working remotely due to the pandemic?



KEY 2020 CYBERTHREATS

3. Ransomware is still the number one threat

2020 has been a year of ransomware with more attacks, higher losses and new extortion techniques being implemented by cybercriminals. Big cases become public practically every week. According to a report published by Coalition, one of the largest providers of cyber insurance services in North America, ransomware cases have accounted for 41% of cyber insurance claims filed in the first half of 2020. “Ransomware doesn’t discriminate by industry. We’ve seen an increase in ransom attacks across almost every industry we serve,” reports Coalition.

Some examples:

[Argentina’s largest telecom provider](#) - Ransomware allegedly infected more than 18,000 workstations including terminals with highly-sensitive data and demanded a \$7.5 million ransom which was set to double if not paid within 48 hours.

[Garmin](#), one of the world’s largest wearable device companies, confirmed that the major outage that began on 24 July was due to a WastedLocker ransomware attack. This attack forced Garmin to halt its contact centre operations, Garmin Connect, as well as production lines in Taiwan. The requested ransom amount is believed to be \$10 million.



[Brown-Forman \(Jack Daniels, Old Forester, The Glendronach etc.\)](#) Allegedly had 1TB of data stolen, including confidential employee information, financial data, internal communications, and company agreements. Images posted on the attacker’s leak site indicate that they possess data dating back to at least as far as 2009.

[CWT](#), one of the world’s largest travel and event management companies, was compromised by the Ragnar Locker ransomware. The attackers allegedly stole 2TB of sensitive corporate data and claim to have compromised more than 30,000 systems. While the attackers initially demanded \$10 million for the safe return of stolen data, CWT eventually agreed to pay a ransom of more than \$4 million.

[Canon](#), the multinational corporation specialising in optical and imaging products, fell victim to a Maze ransomware attack that impacted its email system, Microsoft Teams, its U.S. website, and other internal applications. The Maze ransomware operators stated that they stole more than 10TB of data from Canon, including private databases. Canon acknowledged the attack in an internal message sent to employees.

KEY 2020 CYBERTHREATS



4. Simple backup and security are not enough anymore

A key concept in the past has been that if you have a backup, you don't need to pay a ransom, since you can restore from it. However, this is no longer the case, practically every ransomware now attempts to delete or disable Windows volume shadow copies and tries to sabotage traditional backup solutions, leaving this approach outdated.

Some examples from recent ransomware, as detected by Acronis:

Conti Ransomware

- The average demand for this ransomware is under \$100,000
- Uses Windows Restart Manager to close any open or unsaved files before encryption
- Contains more than 250 strings decryption routines and about 150 services to be terminated
- Performs fast file encryption in 32 simultaneous threads using Windows I/O Completion Ports
- Follows the trend and recently has launched the 'Conti.News' data leak site
- Stops services that belong to SQL, antivirus, cybersecurity, and backup solutions such as BackupExec and Veeam

Netwalker Ransomware

- Discovered in August 2019
- Implements the Ransomware as a Service (RaaS) model and targets organisations as well as individual users
- Has managed to extort approximately \$25m since March 2020
- Uses a heavily obfuscated PowerShell loader to start ransomware on an infected system
- Deletes Windows shadow copies of the Netwalker files
- Attempts to stop backup services in order to prevent restoration

Both Ransomwares also attempt to terminate the Acronis Cyber Protect solution but fails due to the self-protection feature.

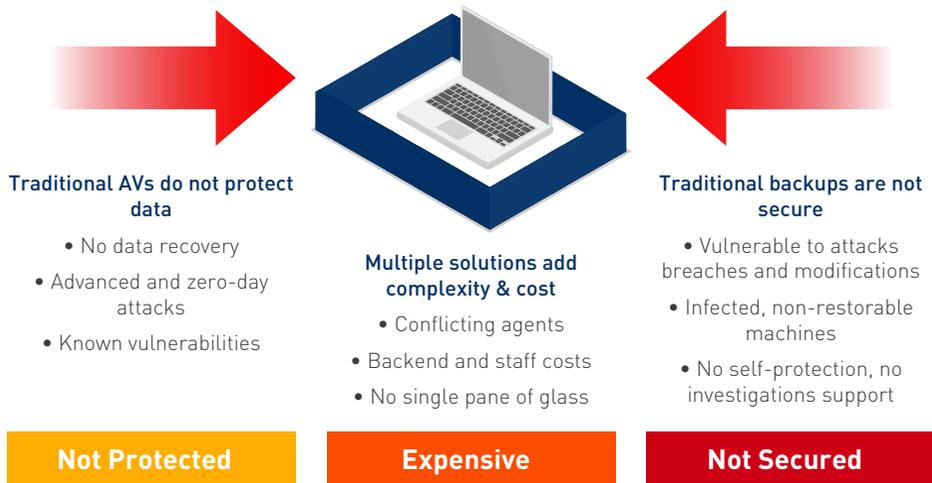
RECOMMENDATIONS AND FURTHER READING



Traditional data protection and recovery have been found to be vulnerable, and conventional antivirus solutions do not protect everything. To address today's security requirements and solve the shortcomings of yesterday's solutions, we are offering an integrated solution Acronis by Daisy, that cuts through the complexity of these solutions by combining security with backup and also device management.

Why?

Traditional tools are no longer adequate



Acronis by Daisy

Backup & DR

Fast and reliable recovery of your apps, systems and data

Mobiles and tablets
Desktops and laptops
Virtual machines and servers
Cloud productivity suites

Security

Next-generation AI and machine learning based security

Antivirus
Anti-malware
Ransomware protection
Vulnerability assessment

Management

Group management, reporting and patching of devices

Remote assistance
Automated patching
Hard drive health
Dashboard and reports

What is Acronis? [Read the article](#)

For more information, visit: dcs.tech/acronis

0344 863 3000

enquiries.dcs@dcs.tech