50 Noteworthy Cybercrime Statistics in 2019

Andrew Zangre | April 1, 2019

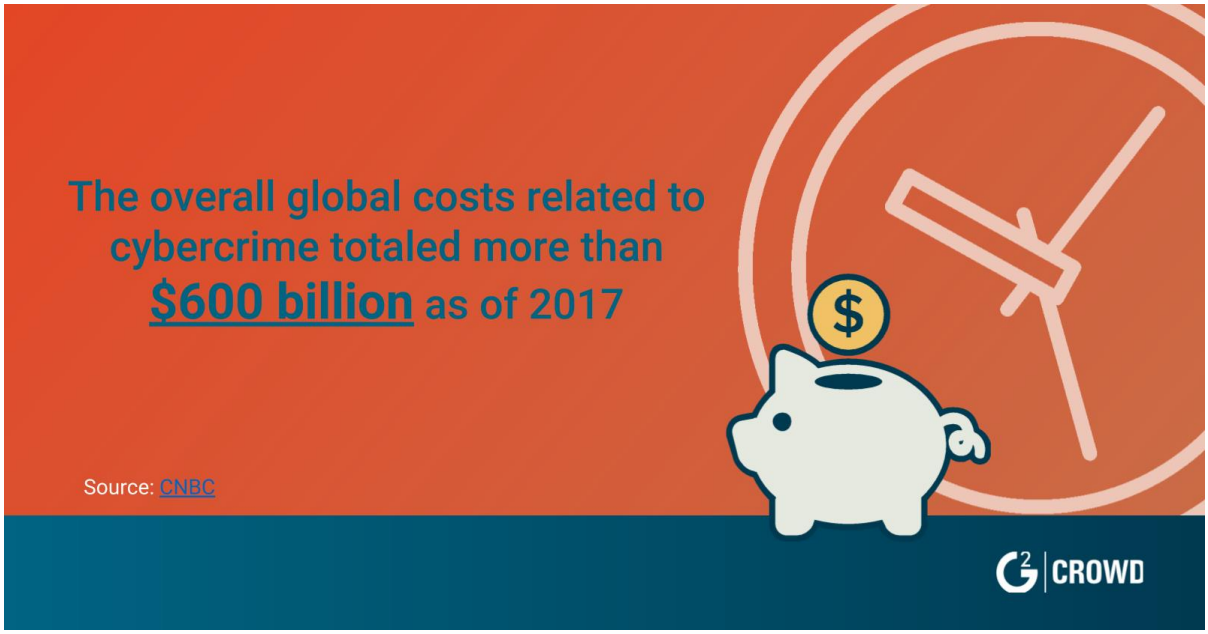
https://learn.g2.com/cybercrime-statistics

Due to the ballooning urgency and prevalence of cybercrime, with companies losing billions and — more importantly — individual lives being ruined, the cybersecurity industry is one of the hottest in the world. Experts estimate that **the cybersecurity software industry will be worth nearly $250 billion by 2023**.

It's a real bummer about cybercrime that it's forcing family-run businesses and enterprises alike to shell out big-time funds and always be on alert. But on the bright side, the resources pouring into the industry have allowed for fascinating developments. **Cybersecurity trends in 2019** show the fast-moving evolution of cyberdefense to greet the rising demand. And business owners are becoming more proactive and honest about these threats, working together to fight the good fight.To help illustrate the dangers of cybercrime and reinforce the need for a proper defense, we've compiled some recent cybercrime statistics. Read on to get a better sense of cybercrime today and how your business might be affected so you can plan and/or respond accordingly.

General cybercrime statistics

- The overall global cost of cybercrime has exceeded $600 billion. (CNBC, 2018)
- 23 percent of Americans say that they or someone in their household had their personal, credit card or financial information stolen by hackers in 2018. (Gallup, 2018)
- 16 percent of Americans say that they or someone in their household was a victim of identity theft in 2018. (Gallup, 2018)



- Experiences with identity theft increased fourfold between 2017 and 2018. (Norton, 2018)
- More than $15 billion was stolen in incidents related to identity theft in 2017. (Norton, 2018)
- 71 percent of Americans say they worry about cybercrime. (Gallup, 2018)
- 30 percent of U.S. consumers were affected by data breaches in 2018. (Gallup, 2018)
- Individual victim losses due to internet crime were greater than $1.4 billion in 2017. (FBI, 2018)
- The Internet Crimes Complaint Center (IC3) received more than 300,000 complaints related to cybercrime in 2017. (FBI, 2018)

- The U.S. economy loses between $57 billion and $109 billion per year due to cybercrime. (Nextgov, 2018)
- The U.S. government plans to spend $15 billion on cybersecurity-related activities in 2019. (Norton, 2018)

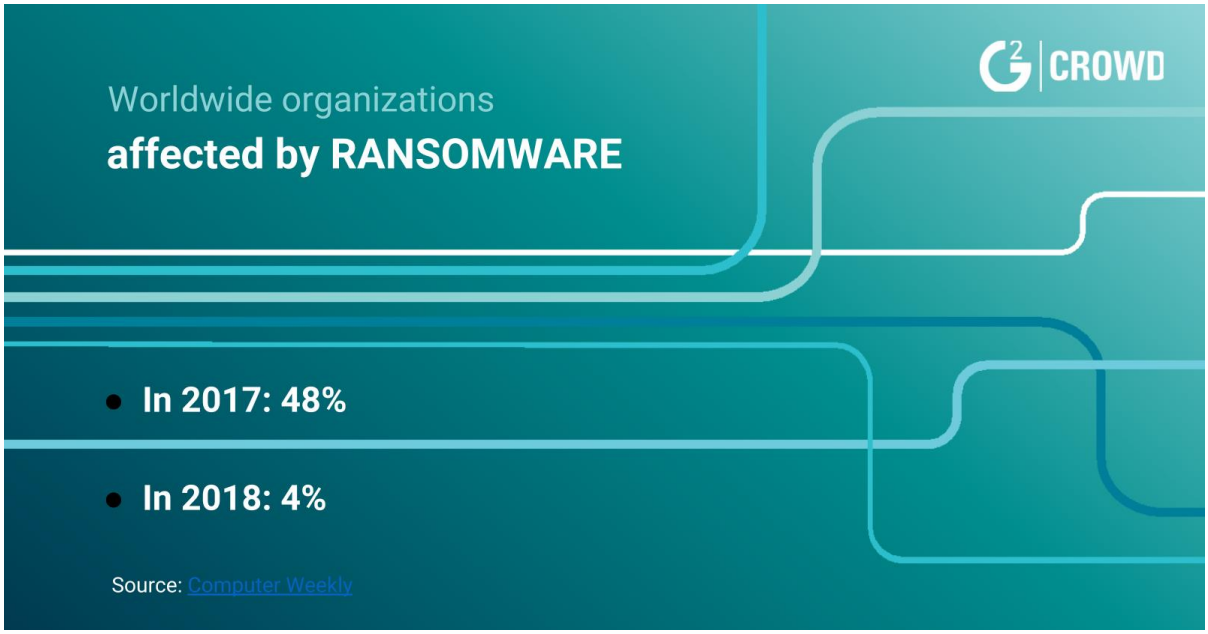
Cybercrime and business

- 30 percent of company cybersecurity incidents are performed by current employees within the organization. (PwC, 2018)
- 26 percent of company cybersecurity incidents are performed by former employees of the organization. (PwC, 2018)
- 23 percent of company cybersecurity incidents are performed by unknown hackers. (PwC, 2018)
- 29 percent of businesses report loss or damage of internal records as a result of a security incident. (PwC, 2018)
- 35 percent of businesses report that customer records were compromised at some point due to a security incident. (PwC, 2018)

- 30 percent of businesses report that employee records were compromised at some point due to a security incident. (PwC, 2018)
- 53 percent of cyberattacks on business systems resulted in damages of $500,000 or more. (Cisco, 2018)
- The total volume of cyberevents among businesses increased nearly fourfold between January 2016 and October 2017. (Cisco, 2018)
- In 2018, 18 percent of organizations were hit by bots or botlets used to launch distributed denial of service (DDoS) attacks in addition to other malware. (Computer Weekly, 2019)
- Bot infections played a role in 49 percent of organizations experiencing a DDoS attack in 2018. (Computer Weekly, 2019)

Ransomware statistics

- Spam and phishing emails are responsible for 66 percent of ransomware infections. (PCMag, 2018)
- 33 percent of businesses believe a lack of end user cybersecurity training was a cause of ransomware infection. (PCMag, 2018)
- In 2017, 48 percent of organizations were affected by ransomware. (Computer Weekly, 2019)
- In 2018, around 4 percent of organizations were affected by ransomware. (Computer Weekly, 2019)



Facebook data breach

- 30 million Facebook users were affected by the site's data breach in 2018. (Consumer Reports, 2018)
- Around 14 million of those users had sensitive information exposed, such as their username and recent Facebook searches. (Consumer Reports, 2018)
- 7 out of 10 Facebook users altered the way they use the platform because of privacy concerns after the site's 2018 data breach. (Consumer Reports, 2018)

Cryptocurrency and cryptomining

- In 2018, cybercriminals stole around $1.7 billion in cryptocurrency. (Bitcoinist, 2019)
- There were 3.6 times more hacks on cryptocurrency exchanges in 2018 than in 2017. (Bitcoinist, 2019)
- Over 60 percent of cryptocurrency exchange hacks were carried out by just two professional groups. (Bitcoinist, 2019)
- In 2018, $725 million in stolen cryptocurrency was due to "inside jobs." (Bitcoinist, 2019)
- Cryptominers infected 10 times more organizations than ransomware in 2018. (GlobeNewswire, 2019)
- The top four most prevalent malware types in 2018 were designed to hijack computers and mine cryptocurrency. (Computer Weekly, 2019)

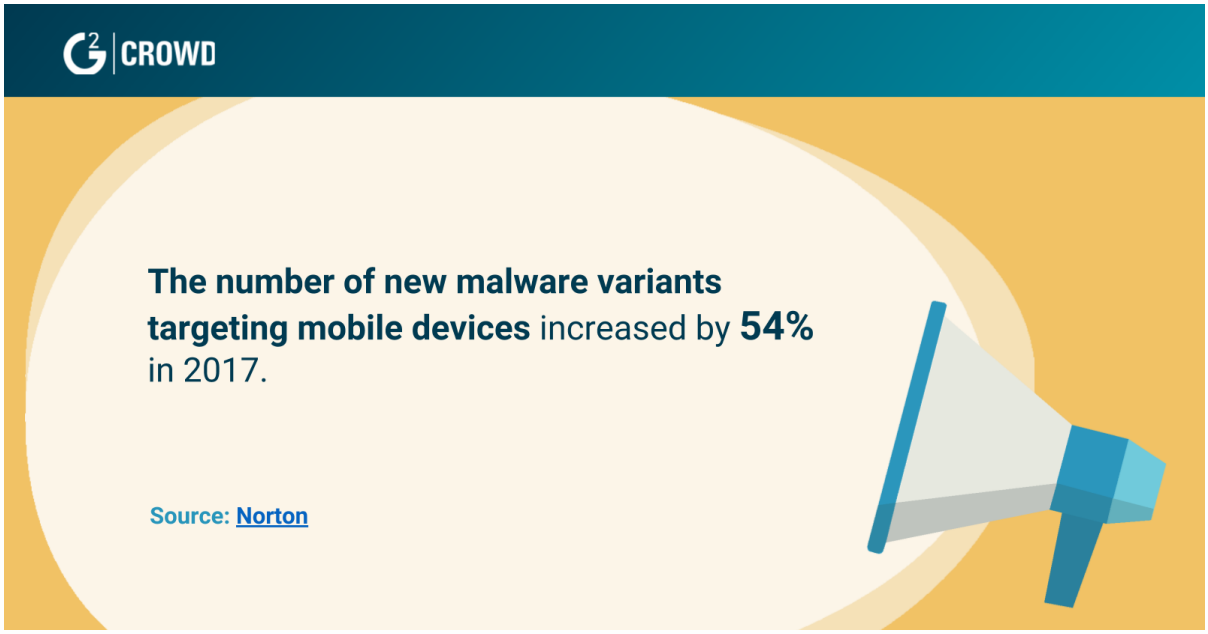
- 37 percent of organizations worldwide were affected by these top four crypto-related malware types in 2018, making it the most prevalent malware type. (Computer Weekly, 2019)
- 20 percent of companies are hit by cryptomining each week. (Computer Weekly, 2019)

Internet of things (IoT)

- 67 percent of businesses have an IoT security strategy in place or are currently implementing one. (PwC, 2018)
- 36 percent of businesses have uniform cybersecurity standards and policies for IoT devices and systems. (PwC, 2018)
- 34 percent of businesses have new data collection, retention and destruction policies. (PwC, 2018)
- 24 percent of businesses assess device and system interconnectivity and vulnerability across the business ecosystem. (PwC, 2018)
- 40 percent of businesses believe loss of operations is the most critical risk of a cyberattack on automation or robotics systems. (PwC, 2018)
- 39 percent of businesses believe lost or compromised sensitive data is the most critical risk of a cyberattack on automation or robotics systems. (PwC, 2018)
- 32 percent of businesses believe that harm to the quality of products produced is the most critical risk of a cyberattack on automation or robotics systems. (PwC, 2018)

Mobile threats

- After cryptomining software (cryptominers), mobile malware is the most prevalent malware type, affecting 33 percent of organizations worldwide. (Computer Weekly, 2019)
- The top three mobile malware types in 2018 targeted the Android operating system. (Computer Weekly, 2019)
- The number of new mobile malware variants targeting mobile devices increased by 54 percent in 2017. (Norton, 2018)



- In 2017, 27 percent of malicious mobile apps were found in the Lifestyle category. (Norton, 2018)
- In 2017, 20 percent of malicious mobile apps were found in the Music & Audio category. (Norton, 2018)
- In 2017, 10 percent of malicious mobile apps were found in the Books & Reference category. (Norton, 2018)
- Third-party app stores host 99.9 percent of discovered mobile malware. (Norton, 2018)