PROTECTING YOUR ASS-ETS FROM RANSOMWARE

André Gignac, Senior Country Solutions Architect

Enterprise Data Protection Solutions / Media & Enterprise Solutions / Government Solutions

Agenda

- Introduction
- Timeline of an attack
- Cost of the attack
- What can you do / Best practices
- Summary

Quantum Overview – Who We Are

WHO WE ARE

Quantum technology and services help customers capture, create and share digital content – and preserve and protect it for decades.

WHAT WE DO

We deliver solutions built for every stage of the data lifecycle - Quantum's platforms provide the fastest performance for high-resolution video, images, and industrial IoT, and the lowest cost long-term storage for archiving and preservation.

WHO WE WORK WITH

The world's leading entertainment companies, sports franchises, researchers, government agencies, enterprises, and cloud providers are making the world happier, safer, and smarter on Quantum.

QUANTUM. MAKING THE WORLD…

HAPPIER

SAFER

SMARTER

Bad people are out there

- And they want your data
- And your money
- Remember pop-ups? I'll take those again.
- Evolution
  - Viruses
  - Adware
  - Spyware
  - Malware
  - **Ransomware**

What is Ransomware?

- **ran·som·ware**
  - **/ˈransəmˌwer/**
  - **noun**
- **A type of malicious software designed to block access to a computer or system until a sum of money is paid.**
- More modern ransomware families, collectively categorized as crypto-ransomware, encrypt certain file types on infected systems and forces users to pay the ransom through certain online payment methods to get a decrypt key.

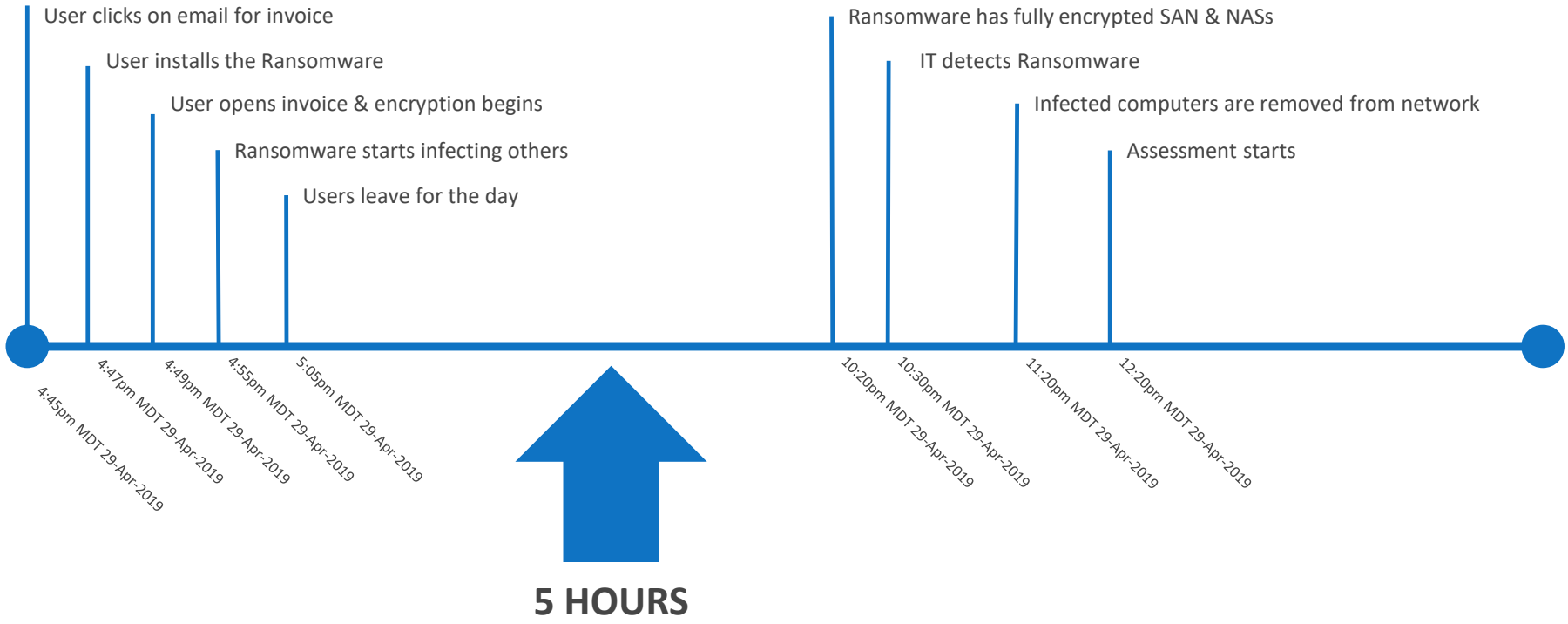
Trends

- In 2018, the tech industry saw a shift from the usual ransomware techniques.
- The preferred victims are now companies, and not consumers.
  - Current ransomware attacks are becoming more targeted, and they require more research and strategic planning.
  - All industries were susceptible to attacks, especially the healthcare, gaming, and retail sectors.
- Severe damages companies suffer in the downtime, along with the data theft and missed business opportunities, make reporting this type of cybercrime a challenge.
- Paying the ransom will likely make your business more vulnerable to future attacks.
- Success encourages the continued global growth of ransomware as a criminal act.

Key Ransomware Stats

- Ransomware cost businesses more than $8 billion in the past year
- The average cost of a ransomware attack on businesses is $133,000
- The estimated losses in 2019 for the healthcare industry are $25 billion
- The global spending on cybersecurity is over $14 billion
- Ransomware is behind 56% of malware attacks
- 95% of ransomware profits went through the cryptocurrency trading platform BTC-e

Timeline of an attack – Day 1

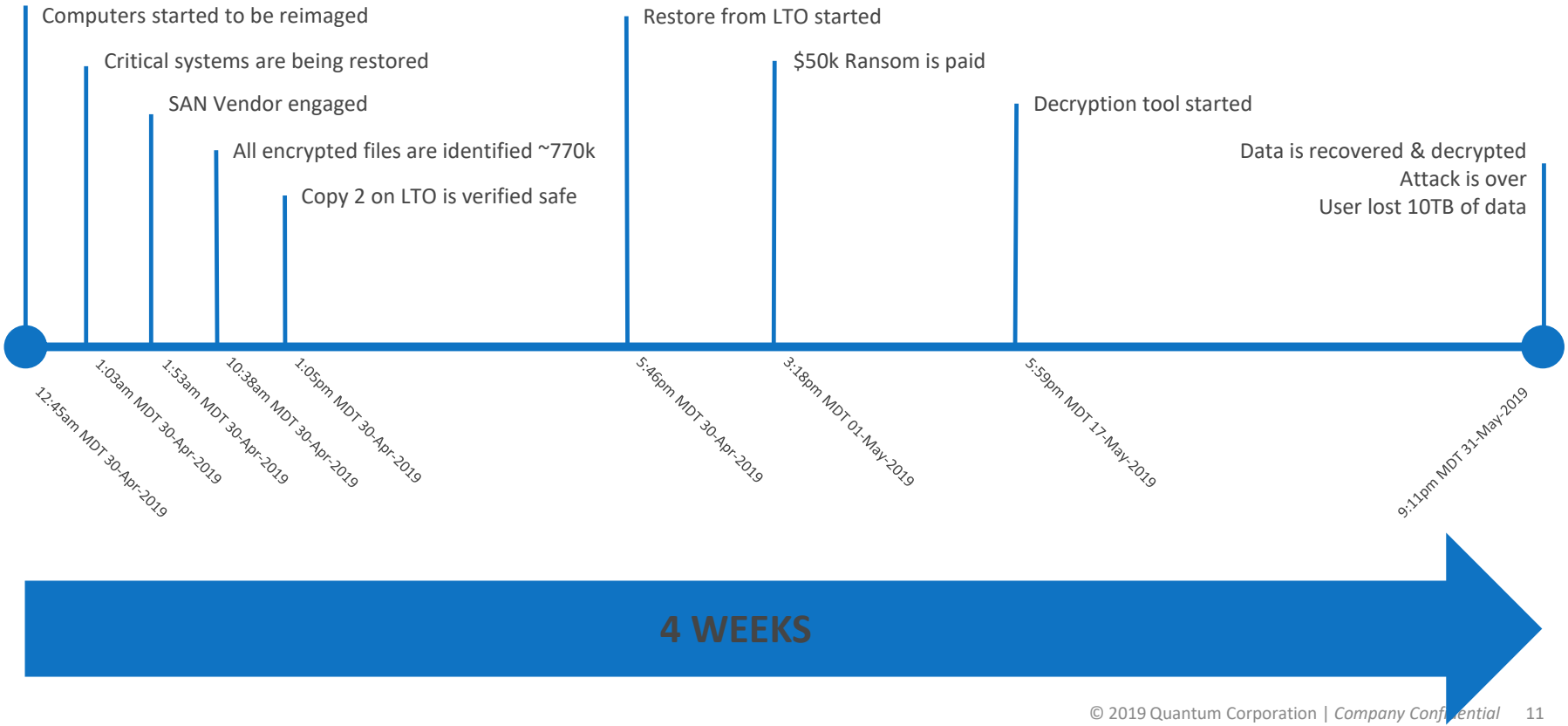


No data is safe

- Summation of attack:
  - Faster networks, CPUs, systems made this attack happen faster
  - Human at fault
  - Bad practices made them an easy target:
    - No A/V on critical computers
    - No air-gap
    - No permissions

- Smart decisions were made:
  - Automated backup on LTO
  - Started engagement with vendors right away

Cleanup of an attack – Day 2 through week 4



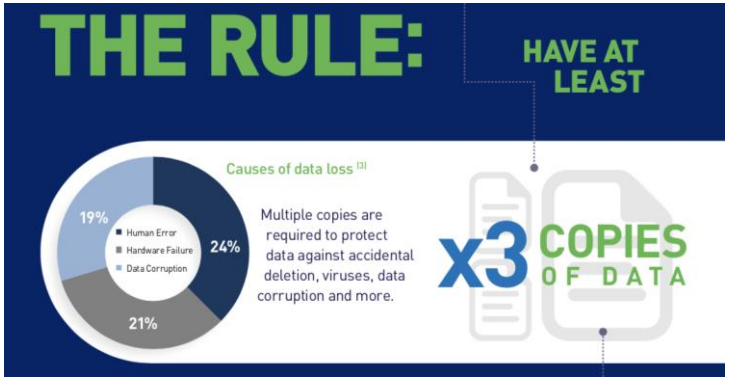
What did this cost?

- Time
- Lost production time
- 5 employees
- $50,000 in bitcoin
- 3 contracts
- $$$$$ in overtime
- $$$$$$$$$ in future business

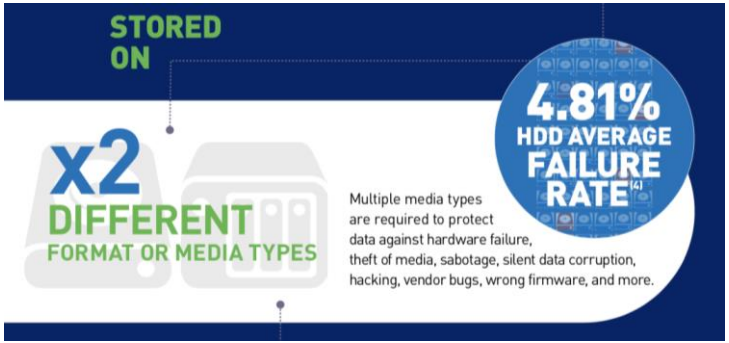
What can you do / Best practices

- Remember that you are a target
- Train employees
- Firewalls/AntiVirus
- Isolation – Air gap
  - Editing systems don’t touch Internet
  - Financial systems don’t touch Storage environments
  - Networks are separate
  - Permissions
- Automated 3-2-1-1 data protection model

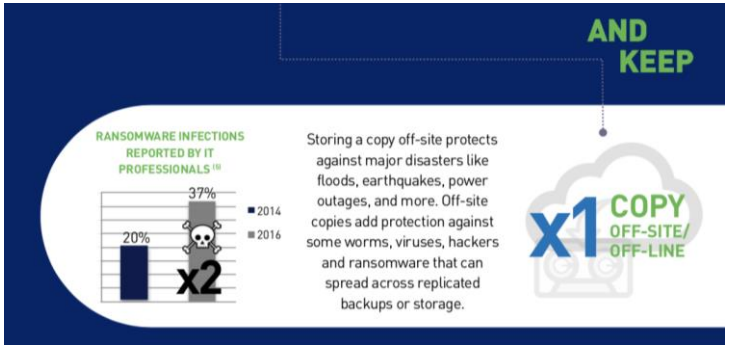
3-2-1-1 data protection???



- 3 - At least 3 copies of the data or asset



- 2 – Stored on 2 different format or media types



- 1 – 1 copy off-site
- 1 – 1 copy off-line

Quantum Technology and Services

For high-performance video editing and large unstructured data sets

StorNext Products
The # 1 choice of leading broadcast, post-production, sports production, and corporate video entities around the world.

For surveillance and industrial IoT

VS-Series
Retain more surveillance footage at the lowest cost, and converge and run entire building operations on a single box.

For archive and long-term storage

Scalar Series
The lowest-cost long-term storage used by the biggest clouds and leading enterprises to preserve digital content for decades.

For remote data capture

R-Series
Ruggedized removable storage designed for fast ingest and easy upload/offload.

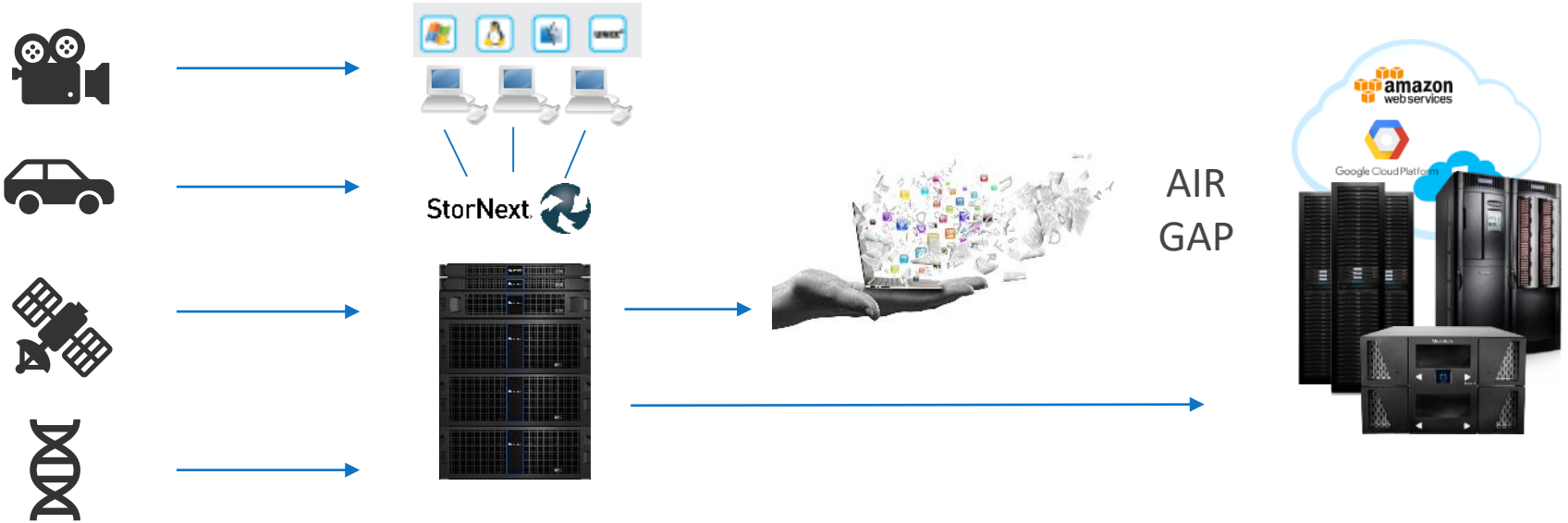
For enterprise backup and DR

DXi-Series
The most efficient solution for protecting business-critical applications.

Quantum Distributed Cloud Services
We'll handle the technology, so you can focus on what you do best.

Video and IoT Data Sets Have a Common Workflow

1. CONTENT IS CAPTURED, CREATED, UPLOADED
2. CONTENT IS CATALOGED, WORKED ON, ANALYZED
3. CONTENT IS FINISHED AND DISTRIBUTED
4. CONTENT IS STORED AND PROTECTED FOR FUTURE USE



Deliver a Portfolio for All Phases

1. **CONTENT IS CAPTURED, CREATED, UPLOADED**
2. **CONTENT IS CATALOGED, WORKED ON, & ANALYZED**
3. **CONTENT IS FINISHED AND DISTRIBUTED**
4. **CONTENT IS PRESERVED AND PROTECTED FOR FUTURE USE**

Mobile Storage

Ruggedized removable storage designed for fast ingest and easy upload/offload.

Use Cases: Autonomous vehicle design, rolling stock surveillance capture, on-site production, military.

High-Performance Video Platforms

Fastest streaming performance on the planet, IP and SAN support, specifically designed for video and rich media use cases.

Use Cases: High-performance storage for video and rich media workflows, hyperconverged surveillance systems.

Archive Storage and Cloud Managed Services

Lowest-cost, massively scalable long-term storage of video and rich media content and assets, on prem and in the cloud.

Use Cases: Digital media archives for broadcast and post, PB-scale archives for HPC/research rich media, exa-scale cloud archives.

Tape is Secure “Offline” Storage

Tapes stored in libraries, are “offline”
and “air-gapped” from the network.

Quantum®

Supporting statements

- **Ransomware's minimum annual global revenue is $1 billion**
  - This number is actually impossible to know or calculate, and that number is a large sum. Based on a 2018 study from Bromium suggests, cybercrime brings in more revenue than working in a legitimate company. This figure includes both of the types of ransomware, as in, encryption and screen-locking ransomware.
- **Ransomware cost businesses more than $8 billion per year in 2018**
  - How much does ransomware cost? This is an incredibly high surge compared to 2016, when the annual cost of ransomware was estimated at $1 billion. It's also important to note that the money is only a part of what a company loses. The company's reputation, the downtime, and other factors all amount to disastrous consequences behind these ransomware statistics.
- **There was a 79% overall increase in malware-targeted businesses in 2018**
  - Attackers have realized that businesses will bring them a higher revenue than an individual person. Even though the use of ransomware has decreased, the attacks are now more targeted manual attacks, according to a 2019 report on the state of malware from Malwarebytes.
- **25% of cyber insurance claims in 2017 were related to ransomware attacks (AIG, 2018)**
  - This did not prove too effective, as most businesses seek help in vain. The amount of time businesses spend unable to access their data, as well as the costs of rebuilding, well surpass the ransom demand.
- **The average ransom demand was cut in half in 2018, dropping from $1,077 to $522**
  - This mostly goes for small business ransomware attacks. The 2017 prices increased threefold when compared to 2016. Conversely, the average ransomware demand in 2018 is larger for enterprises.
- **GandCab Version 5 requires its victim to pay $2,499 for the decryption key**
  - Some individual new versions of file-encrypting ransomware require quite a bit more money than the yearly average, as stated in the McAfee ransomware report from December 2018. Past versions asked for $1,000.
- **Fewer than a third of the businesses that pay the ransom retrieve all of their money**
  - So much for the efficacy of the legal system and their ability to make up for the companies' losses caused by cybercrime. Most businesses need to understand that, when it comes to ransomware.
- **The number of new ransomware variants has increased by 46%**
  - Bigger, better, and more sophisticated ransomware strains are popping up on a daily basis. Some of the most profitable ransomware families are SamSam, Crypt XXX, GandCab, and Locky. The ever-evolving ransomware industry is not easy to tackle, and cybersecurity companies are struggling to keep up against new advancements.
- **The average cost of a ransomware attack on businesses was $133,000**
  - This figure covers the ransom demanded, along with the price of downtime, the network costs, and manpower. Assessing the ransomware losses for businesses requires a multifactor analysis—it's never just the ransom itself.
- **Less than one-quarter of SMBs report their ransomware attacks**
  - According to a Datto report in 2018, one of the biggest problems is that most small to midsized businesses don't bother to report this type of attack. This might be due to the low probability of getting their money back.
  - If you want to know how to report a ransomware attack to law enforcement, pay attention to the date of infection, the ransomware variant, how the infection occurred, and the actor's cryptocurrency wallet address. It would also be useful to mention your business type, industry, and number of employees, along with your estimated overall losses.

Supporting statements

- **Malicious activity from exploit kits dropped by 60% in 2016**
  - This answers the question, How is ransomware delivered? Email is the preferred ransomware method with hackers all over the world to this day. It turns out that humans are once again the weak link criminals enjoy targeting.
- **A business will fall victim to a ransomware attack every 14 seconds by 2019, and every 11 seconds by 2021**
  - A report that Cybersecurity Ventures released in 2019 shows the towering volume of cyberattacks companies have to face on a daily basis. In these rather bleak ransomware predictions, it's clear the number of attacks is expected to grow.
- **The estimated losses in 2019 for the healthcare industry should be around $25 billion**
  - A 2019 report from Singapore-based Cyber Risk Management (CyRiM) states that healthcare will be one of the most affected industries out there.
- **After an attack in 2018, the US hospital Hancock Health paid a $55,000 ransom to hackers**
  - Hancock Health's systems were infected by SamSam, the most successful ransomware in 2018. Despite having made backups, the prospect of spending days, even weeks fixing the damages this hospital ransomware caused was too much.
- **2019's global spending on cybersecurity is estimated to be over $14 billion**
  - In 2018, the global spending on information security will see an increase of 12.4% from 2018. In 2019, the security market is estimated to grow by 8.7%.
- **Microsoft Security Essentials and Avast Free make up 30% of the security market**
  - Popular options like Avast Bitdefender and Avira can fend off most of the threats and still run in the background. Online encryption tools as well as a ransomware antivirus are a must, but they might not protect you completely.
- **In 2018, more than 77% of the businesses affected by ransomware were using up-to-date protection**
  - This just goes to show that run-of-the-mill endpoint security doesn't do enough to protect businesses from the latest ransomware threat. The targeted, well-thought-out, and sophisticated attacks are often more difficult to fend off.
- **Over a quarter of all companies would pay between $20,000 and $50,000 to hackers to recover their data**
  - An IBM study suggests that most businesses are willing to pay up when under attack, especially when they store important, confidential data. The type of data that's threatened can range from confidential customer data, financial records, business plans, and high-value intellectual property.
- **67% of Indian organizations said they were victims of ransomware, and 38% faced this threat twice**
  - The number of reports of ransomware in India is increasing. India is one of the six countries in the world most targeted by ransomware. As we saw earlier, hospitals are also common targets.
- **60% of cryptocurrency transactions can be traced back to individuals**
  - As recent studies have shown, cryptocurrencies aren't nearly as anonymous as they used to be. Obscuring your purchases or your transaction activities is becoming more and more difficult, especially with Bitcoin. More and more people are considering Monero or Zcash. But how does a ransomware attack work, then? Even with this high transparency, a significant percentage of cybercrimes manage to go unpunished.
- **95% of ransomware profits went through the cryptocurrency trading platform BTC-e.**
  - This cryptocurrency trading platform was founded in 2011, and it was then seized by the US government in 2017. This stat covers the period from 2014 to 2017.

Recent Ransomware Attacks

- **$400,000 was paid by Jackson County, Georgia, after a ransomware attack in 2019**
  - This latest ransomware attack locked the sheriff's office and numerous agencies out of their systems. Right after paying the ransom, everyone successfully gained access to their data. The decision to pay up after this new ransomware attack in 2019 might be for fear of severe losses suffered by the city of Atlanta—proof once more that towns and cities are profitable targets.
- **$51,000: the unpaid ransomware demand for the city of Atlanta, GA; $17 million: the recovery costs**
  - In March 2018, the SamSam ransomware attacked Atlanta's infrastructure. Many essential functions were affected, including citizens' abilities to pay water bills and parking tickets. The money the attackers demanded was way above the average ransomware demand. The recovery costs, as you can see, exceeded the ransom by far. So, if you want a simple answer to the question, "Does paying ransomware work?" think about your priorities—public safety should be high up on the list, because paying the ransom only breeds more crime. Atlanta spent over $5 million on rebuilding their computer network and $3 million on crisis managers and emergency consultants.
- **The total damages from NotPetya, a worldwide ransomware attack that wreaked havoc in 2017, were $10 billion**
  - The White House estimated the global damages. Once released, this malware raced through Ukraine and infected various machines all over the world. Various institutions were affected, from healthcare institutions in Pennsylvania to a chocolate factory in Tasmania.
- **The international shipping company FedEx suffered $400 million in damages from NotPetya attacks**
  - It took the Ukrainian company around three months to fully restore itself after the file-scrambling mess that ravaged its networks. Ukrainian companies were among the first to state they were under attack and suffering the effects of ransomware.
- **French construction company Saint-Gobain's losses to NotPetya's attack were $384,000,000**
  - The attack cost one of Europe's most prolific building supply companies 1% of their first-half sales. In 2016, Saint-Gobain made €39.1 billion in sales, which means the company probably lost around €200 million in turnover in this global ransomware attack.
- **Pharmaceutical company Merck lost $870,000,000 after the NotPetya attack**
  - Millions of dollars are lost through technology cleanup, lost sales, and disrupted business. Merck CFO Robert Davis stated that NotPetya had "negatively impacted third-quarter results, including an unfavorable revenue impact of approximately $135 million from lost sales and approximately $175 million in costs, spread across the cost of goods sold and the operating expense lines."
- **As far as WannaCry statistics go, $255 million was the cost for TSMC, a chipmaker company, due to WannaCry's ransomware**
  - Taiwan Semiconductor Manufacturing Company (TSMC), an Apple iPhone supplier, was temporarily shut down in August of 2018 after the virus spread to 10,000 of their machines. This was one of the worst recent attacks.
- **A Massachusetts school district paid $10,000 in Bitcoin after a ransomware attack in April 2018**
  - Against the FBI's advice, the school district decided to pay the ransomware attackers and got most of their computers back. The complete lack of offsite backup was one of the main reasons.

Ransomware Stats 2018–2019

- **Ransomware is behind 56% of malware attacks**
  - Out of 1,379 malware incidents, the above-mentioned percentage is the majority. A malware attack is still a popular way to dump ransom malware onto a target's computer.
- **Barracuda found that 47% of businesses in the US have been affected by ransomware**
  - This is what we know from the most recent 2019 studies of ransomware attacks in the USA. Out of these infections, 59% of the ransomware was delivered via phishing emails. Phishing and ransomware are a match made in heaven.
- **The number of mobile miners has increased by almost 44.5% from 2016–2017 to 2017–2018**
  - According to a Kaspersky ransomware report, ransomware is decreasing in popularity. Malicious cryptocurrency miners are capitalizing on the power of other people's hijacked computers and devices without their knowledge. The amount, which used to be over 1,800,000, reached over 2,700,000 in 2018.
- **The number of ransomware Mac OS/iOS attacks surged by 500%**
  - During the first half of 2018, according to Datto's Global State of the Channel Ransomware Report, ransomware iOS and Mac attacks saw an insane increase, proving that safety is an issue, even for Apple devices.
- **The number of users plagued by ransomware dropped by almost 30% in 2018**
  - The number of ransomware victims worldwide was 2,581,026 from 2016 to 2017. This significant decrease is definitely a sign that ransomware is becoming less popular as a type of cybercrime, but it's unclear whether this is happening because the targeting has simply gotten more sophisticated.