Optum

Keeping hackers out and vital data in

At Optum, protecting your data is our priority.

Hacking is real — and dangerous

Cyberattacks and data breaches continue to be pervasive across many industries, including health care. The associated cost for each data breach is staggering. The average cost of a healthcare data breach in the U.S. reached $10.1 million in 2022. That's up more than 41% just since 2020.[1]

Ransomware has become the most lucrative form of malware globally, generating $1.3B in profit for criminals in 2021. Meanwhile, the resulting business disruptions caused a disproportionately large impact: over $159B in damages and downtime in that same year.[2]

As the graphic illustrates, the actual amount of ransom paid is really the smallest part of the problem:

[alt text: Graphic shows an iceberg. The small, exposed tip represents to actual amount of ransom collected by criminals: $1.3 billion in 2021. The larger, hidden portion represents the cost of damages and disruption: $159 billion in 2021.]

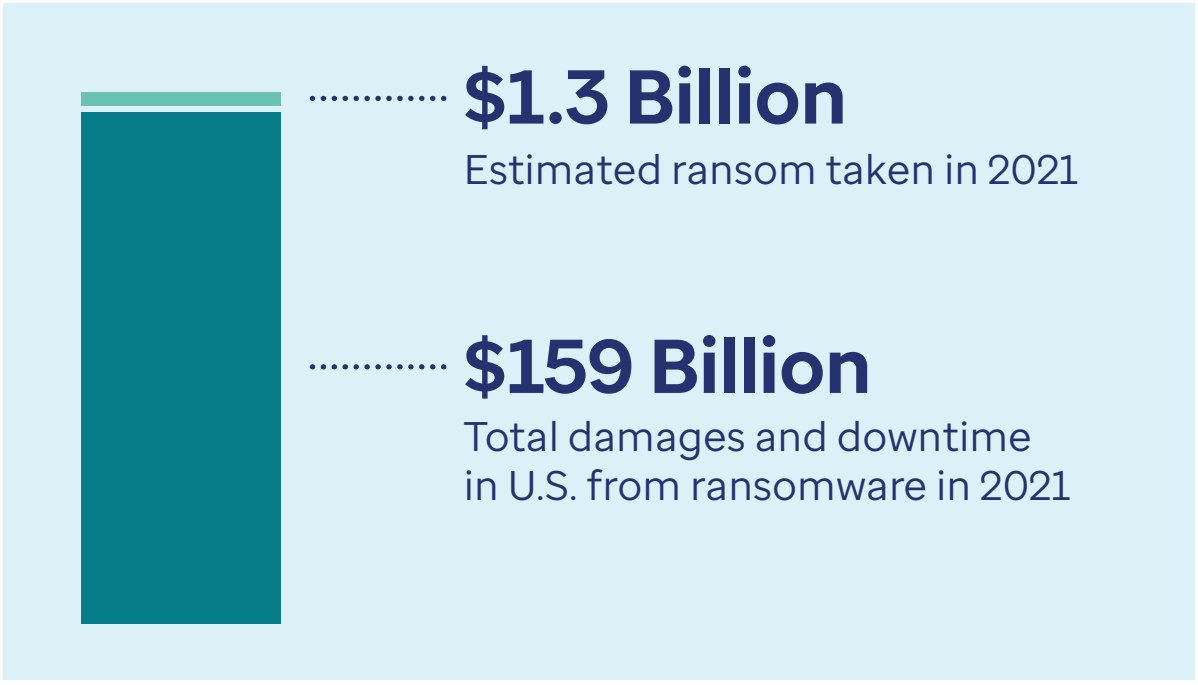

Image source: Comparitech. Ransomware attacks cost the US $159.4bn in downtime alone in 2021. Published July 19, 2022.

Continued

Cost is more than just dollars

In addition to the financial cost, there are also vital personal privacy concerns The data used in health care covers everything from doctor's notes, diagnoses, x-ray images, medication usage and highly detailed financial records. Optum® understands that people, and their associated data, are at the heart of our unique position in health care. That makes protecting data an essential task.

Given our healthcare perspective, Optum employs a preventative mindset. Being proactive is the best way to protect our clients' health, financial and other vital information from harmful cyberattacks.

We put that core responsibility into practice with strong cybersecurity defensive tactics:

> At Optum, we are on a mission to make health care work better for everyone. Defending health care from cyberattacks is a critical part of this mission.
>
> **Allison Miller,** chief information security officer at Optum

Internal data security protocols

- Control practices, monitoring, auditing and quality assurance processes are dedicated to assessing our organization's ongoing compliance
- Performing an in-depth data risk assessment before any new business entity is integrated into our company
- Compliance with best-practice industry certifications and applicable regulatory obligations. These include the Health Insurance Portability and Accountability Act (HIPAA), General Data Protection Regulation (GDPR), and other requirements by state, federal and international authorities

Global cyber threat inoculation

- Global 24/7 security command center to proactively monitor emerging cyber threats with the ability to respond quickly
- Partnering with information security experts worldwide to deliver protection and compliance with local, national and international health regulations

Optum is committed to building and maintaining the trust and confidence of our customers and stakeholders. We take seriously our responsibility to protect the information of those we serve in health care.

1. HIPAA Journal. IBM: Average Cost of a Healthcare Data Breach Reaches Record High of $10.1 Million. Published July 28, 2022. Accessed December 7, 2022.
2. Comparitech. Ransomware attacks cost the US $159.4bn in downtime alone in 2021. Published July 19, 2022. Accessed December 12, 2022.

Optum

optum.com