tw Security
Healthcare Security & Privacy

Expertise you can trust

By the Numbers: As of Fourth Quarter 2020

Year-End Report

From 2009 to December 31, 2020, **3,387 breaches** that affected 500 or more patients were reported to the Department of Health and Human Services (HHS), for a total of **258,064,380 patients** affected.

The percentage of patients affected by hacking has remained steady at **78%**, reflecting the continuing efforts by cyber criminals to obtain valuable healthcare data.

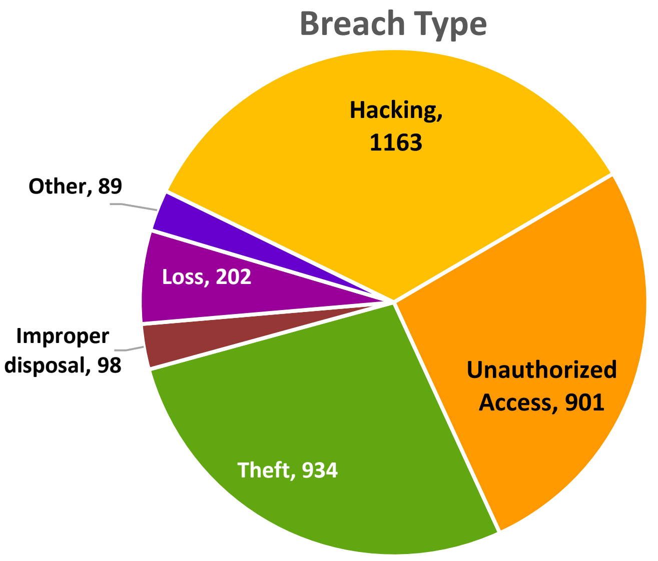
Hacking and **unauthorized access** continue to trend as highly significant figures in large reported cyber breaches this quarter. The "unauthorized access" category includes ransomware, social engineering/phishing attacks, and a variety of other exploits.

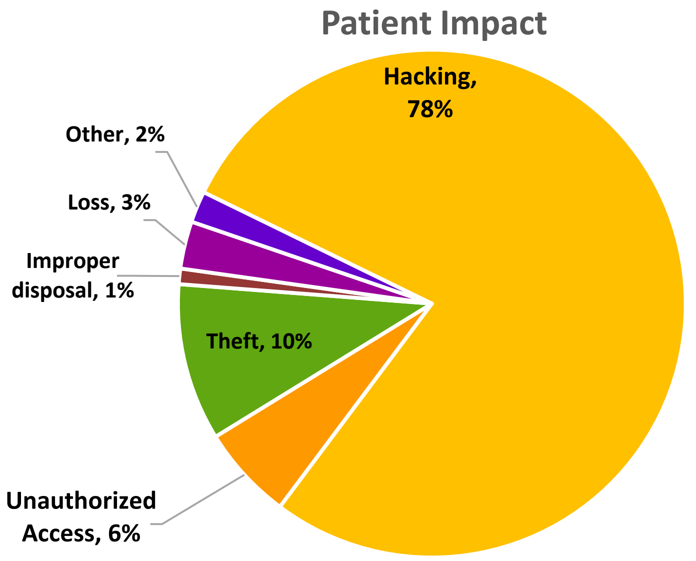
In the fourth quarter of 2020, **149 of the 166 reported breaches** were categorized as hacking and unauthorized access, representing approximately **90%** of all events reported and **98%** of all individuals whose data was compromised.

The FBI and others warn that **healthcare is being increasingly and imminently targeted by ransomware attacks**, in which cybercriminals use malicious software to encrypt vital data and then demand payment for a decryption key.

Cumulative Breach Type and Patient Impact

Exploit Type	Number of Incidents	% of Total Incidents	Number of Patients	% of Patients
Hacking	**1163**	**33%**	**202,135,541**	**78%**
Unauthorized Access	**901**	**27%**	**16,269,119**	**6%**
Improper Disposal	98	3%	1,922,771	1%
Loss	202	6%	8,281,870	3%
Other	89	3%	3,163,499	2%
Theft	934	28%	26,291.580	6%

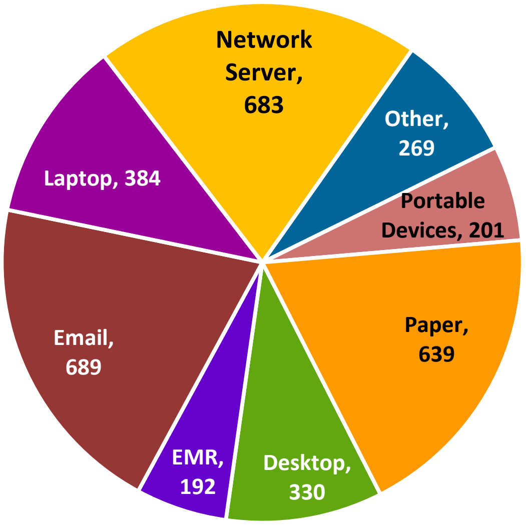




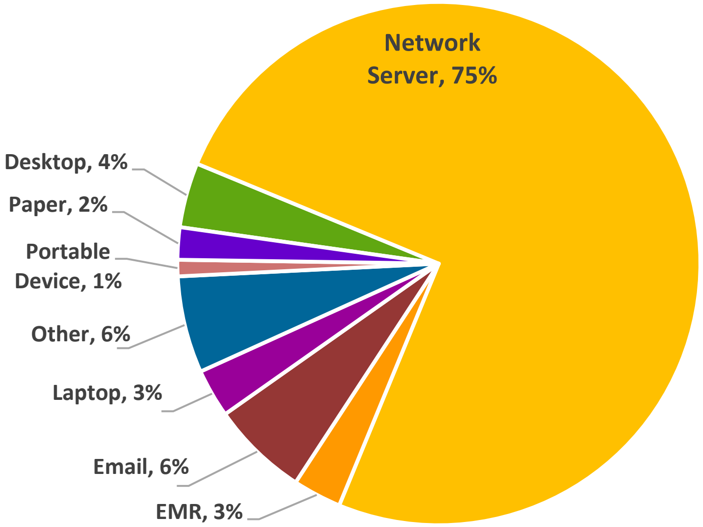
Cumulative Data Location Breakdown

Data Location	Number of Incidents	% of Total Incidents	Number of Patients	% of Patients
Network Server	**683**	**20%**	**194,627,852**	**75%**
Desktop	330	10%	11,482,989	4%
EMR	192	6%	8,078,950	3%
Email	689	20%	14,753,107	6%
Laptop	384	11%	7,158,767	3%
Other	269	8%	14,400,594	6%
Portable Device	201	6%	2,515,465	1%
Paper	639	19%	5,046,656	2%

Data Location



Patient Impact by Location



Source: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

Note: The data analyzed is a snapshot in time of the data available when we create the report.

Business Associates/Business Partners

Since reporting began, business associates and business partners have reported **858 incidents**, or **25% of all breaches**. **87,494,092 patients**, or **34% of the total** have been impacted.

This past quarter, business associates/business partners were the target of **43% of all breaches reported**, impacting **75% of the total**.

Growing Threat

Email continues to grow as a vector for attack, and was the #2 source for data breaches, impacting over **2.5 million individuals.**

High-Value Target

Network servers continue to be the most attractive hacking targets, offering the greatest concentration of valuable data. Attacks on networks had the highest impact on patients this quarter **(194 million, or 75% of the total)**.

2020 Year-End Highlights

2020 has been a challenging year in healthcare. The pandemic created additional stress on healthcare systems and their workforce. Many employees were forced to work from home, introducing new security challenges. Cybercriminals showed no mercy. They exploited people who were seeking answers to their many questions or looking for ways to help. The recent SolarWinds attack was a prime example of how much time it takes and how difficult it is to detect when a system has been compromised.

2020 registered some alarming trends and high breach numbers in healthcare with 534 large data breaches, more than have ever been reported in a single year. Considering the investments made in technologies to enhance security, the increases in information security staffing, and the other deployed resources, we had hoped for a different result.

There is a small measure of good news in this accounting. The number of individuals impacted this year decreased from the previous year by almost 50%. Possible causes of this improvement include increased vigilance, effective technology improvements, and faster incident response time. We hope to help our customers continue to see these improvements through strengthened security practices and enhanced technical controls.

For business associates, the news is not as good. Data breaches targeting business associates appear to be increasing. In 2020, a total of 204 breaches were recorded that impacted 12,862,878 individuals. This means that business associates or third-party vendors experienced 38% of all data breaches in 2020. 60% of individuals in the healthcare system were impacted this year, with business associates contributing a significant portion of that number.

The healthcare industry must identify ways to ensure that business associates can provide the same data protection level as the covered entities do. That is why covered entities are stepping up their due diligence efforts—creating security agreements with their business associates and vendors, asking the right questions through questionnaires, and, in some cases, outsourcing the vendor vetting process to third parties.

Looking Ahead

The pandemic forced us to change our behavior and operations. Now is the time to acknowledge the “new normal” and address new and evolving data privacy and security challenges. Let’s put data privacy and security strategy at the top of the 2021 to-do list.

- Take a fresh look at workforce training. Ensure that we are addressing the hot topics: phishing, ransomware, and telecommuting. Provide real-life examples of recent breaches to make security and data privacy training more exciting and reminders more effective.
- Update incident response playbooks, data backup plans, disaster recovery plans, and policies and procedures. Conduct tabletop exercises to assess readiness and incident response capability.
- Working from home is a trend that is likely to continue for the foreseeable future. Conduct risk analysis on telehealth/telemedicine and telecommuting/remote access to identify vulnerabilities and implement risk mitigation strategies. The Office for Civil Rights (OCR) stated that it would exercise its enforcement discretion and waive potential penalties for HIPAA violations that might occur when widely available communications apps are used in good faith for any telehealth treatment or diagnostic purpose. The OCR further clarified that acting “in good faith” is equivalent to conducting a risk analysis on the telecommunication systems.

As we work to keep ourselves, and those we care for safe this year, let’s also keep our data’s safety and the data’s security top of mind.