Security **Report**

Health Care - Hospitals, Providers and more

This report covers the IT security traits of health care entities including hospitals, health systems, doctor's offices, consultants and more. These entities have been the target of **over two dozen** reported ransomware attacks in the past year, with numbers rising dramatically since mid-2019.

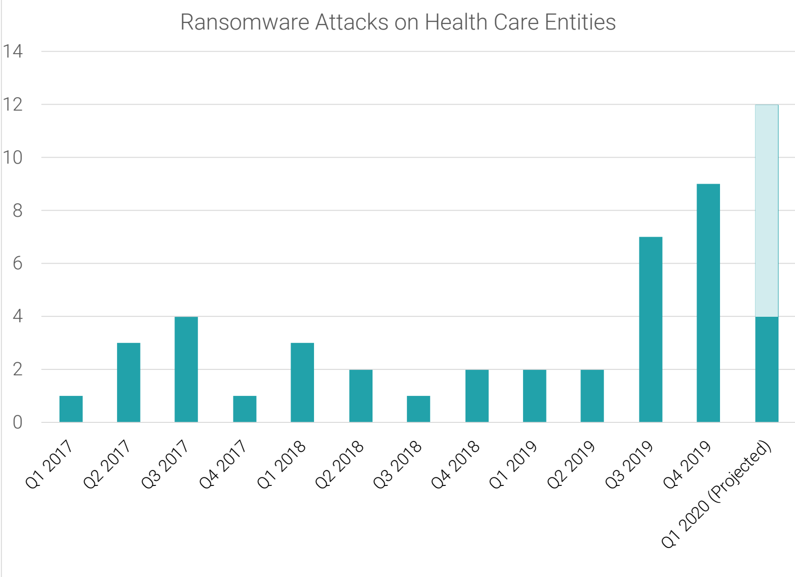
350%

Increase in ransomware attacks on health care entities in Q4 2019 vs. Q4 2018 (Corvus estimate)

Ransomware Activity

The rise of ransomware has been the most significant general trend in cybersecurity in the past year. Corvus's Data Science team studied reported attacks over time to get a view of this trend. Because of varying reporting standards across states, these numbers represent only a sample of the true number of attacks, but shows the dramatic rise in recent months.

4 health care entities reported attacks in January alone, according to a Corvus estimate: more than any *quarter* since Q3 2017. Our conservative projection of 12 for the quarter would continue a rapid rise in attacks that started in mid 2019.



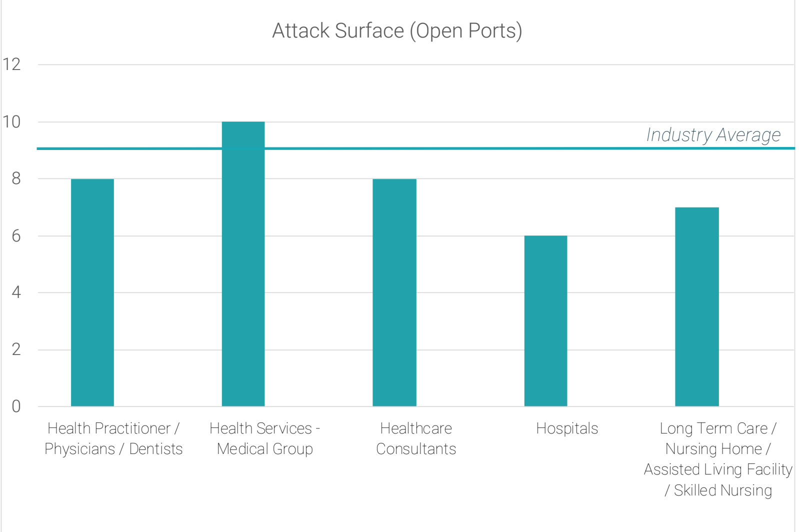
Industry Analysis: IT Security of Health Care Entities

Using data from the Corvus Scan, this section explores several key security factors for health care entities, including new analysis of likelihood of ransomware attacks.

Attack Surface

- Generally, health care entities have a smaller attack surface than the web average, making them easier to defend

Our take: *A larger attack surface is harder to defend. By reducing their overall exposure, hospitals are doing well to limit the risk of intrusion. One common type of exposure is RDP, or remote desktop protocol. According to a Corvus study,* ***the presence of an open port with RDP was associated with 37% greater likelihood of a ransomware attack.***



Contact **corvus@calibercorporate** for more information and interview requests.

CORVUS

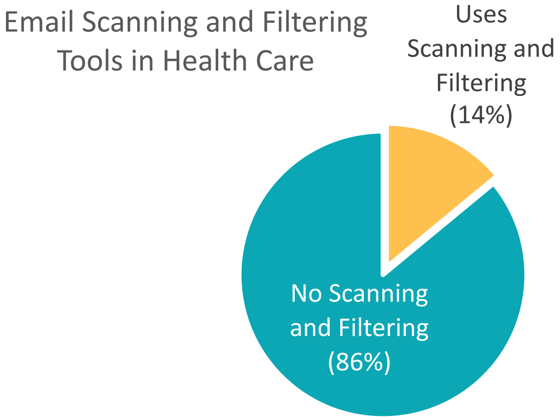
Security **Report**

Health Care - Hospitals, Providers and more

Email Security - not covering the basics

- Health care entities use email scanning and filtering tools at similar rates to the web average, which is low. Even among hospitals, which utilize those services at higher than average rates, **over 75% do not use email scanning and filtering tools**
- Health Practitioners like physicians and dentists are **14% less likely** than average to use the most basic forms of email authentication.

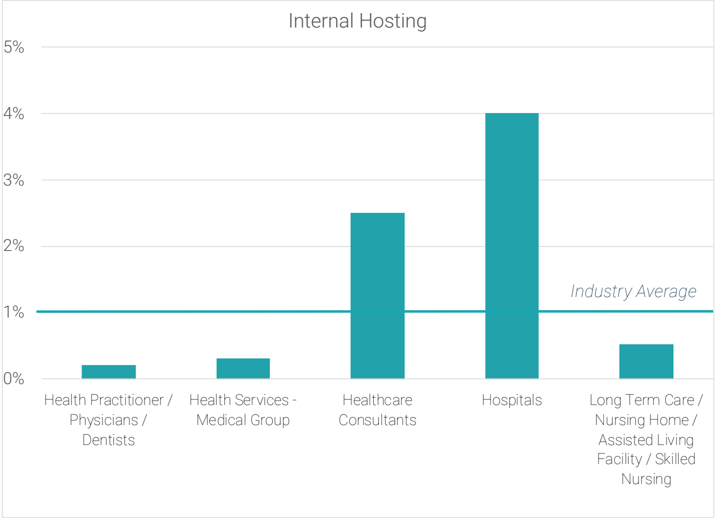
Our take: *Hospitals use email scanning and filtering tools more than average, but the average is low. According to Corvus research,* ***these services are associated with a 33% reduction in the likelihood of a ransomware attack****. All health care entities should strongly consider such services to help prevent phishing. Smaller organizations, like individual health practitioners, are less likely to use basic email authentication schemes that prevent suspicious emails.*



Hosting and Server Setup

- Hospitals are **far more likely (6x more)** to be internally hosted - rather than using a 3rd party hosting provider.

Our take: *Hospitals are a standout in rates of internal hosting over using a 3rd party vendor. For hospitals who choose that route, this puts the responsibility for maintaining some aspects of security in their court: keeping up with the ever-changing threats rather than handing it off.*



Security Not An Overwhelming Focus in Health Care, on Average

As commodity ransomware has become more readily available and examples of successful attacks on smaller organizations, like local governments, gain attention, attackers may well turn their attention to organizations like individual health practitioners or nursing/LTC facilities. Several examples of these kinds of attacks were seen in 2019, including a LTC/Rehab facility in Wyoming.

Based on this analysis, we can see that the security measures at these kinds of organizations are average at best, and in some areas worse. Health care organizations of all sizes are at risk, and given that 91% of ransomware attacks are the result of phishing exploits, they should be taking advantage of opportunities to improve email security. These include the use of scanning and filtering tools and basic authentication schemes to reduce the likelihood of a phishing attempt reaching their employees' inboxes.

Contact **corvus@calibercorporate** for more information and interview requests.