COSMOS
Navigate the Compliance Universe

Compliance Today - May 2021
How effective information governance can help mitigate damages from an information breach

By Brian D. Annulis, Joseph Shepley, and Samir B. Almhiemid

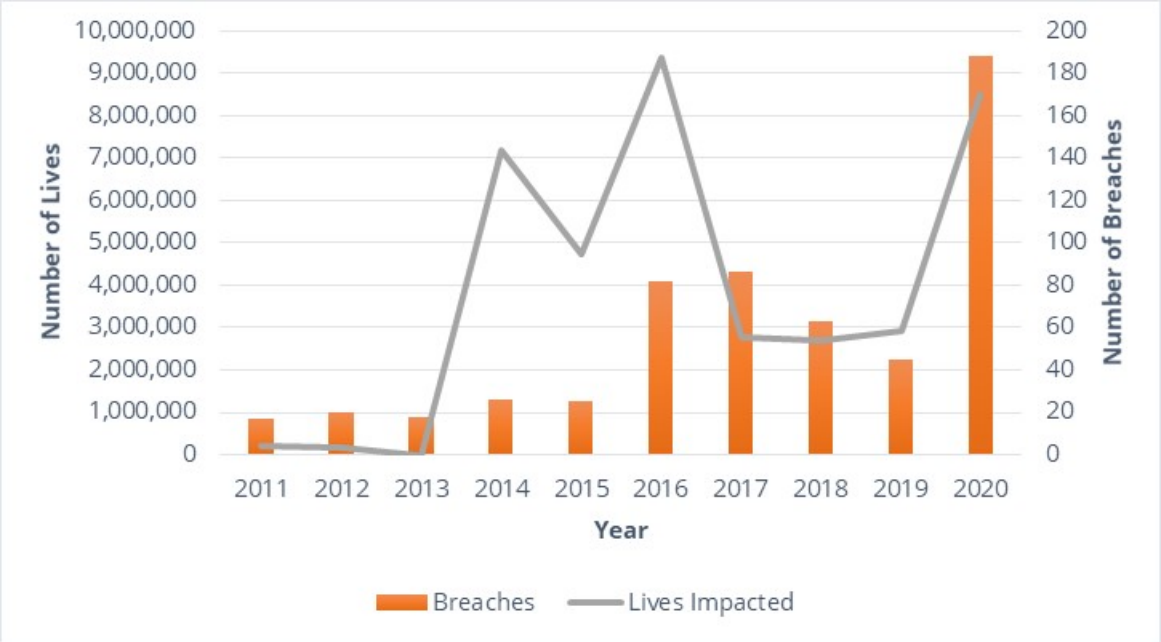
Brian D. Annulis (brian.annulis@ankura.com) is Senior Managing Director, **Joseph Shepley** (joseph.shepley@ankura.com) is Managing Director, and **Samir B. Almhiemid** (samir.almhiemid@ankura.com) is an Associate at Ankura Consulting Group LLC Chicago, IL.

- linkedin.com/in/brian-annulis-71195b1/
- linkedin.com/in/joeshepley/
- linkedin.com/in/samir-almhiemid-aa8337157/

Healthcare organizations today face unprecedented challenges managing and protecting their sensitive electronic information—not only electronic protected health information (ePHI) but other high-value, high-risk data such as personally identifiable information (PII), payment card industry (PCI), network access credentials, and financial data. Prior to 2020, cyberattacks had been on a steady year-over-year increase, but in 2020, this steady increase turned into explosive growth.

Healthcare experienced a more than 9,000% increase in endpoint attacks compared to 2019, which led to approximately 1 million patient records breached per month.[1] The U.S. Department of Health & Human Services Office for Civil Rights (OCR) breach data[2] shown in Figure 1 tells a similarly alarming story: in 2020, there were 188 reported breaches of network servers[3] involving 500 or more individuals—a more than 400% increase compared to 2019 and a more than 200% increase compared to 2017, which was the previous high-water mark for reported network server breaches. Beyond the typical impacts of these attacks, such as regulatory fines, sanctions, and mandated corrective action plans, 2020 also saw the first-ever reported loss of life due to a cyberattack: in September, a German patient died during a ransomware attack when being rerouted to another healthcare facility to receive care.[4]

Figure 1: Number of breaches and lives affected 2011–2020



Cybersecurity is not enough

In response to the increase in cyberthreats, healthcare organizations have quite rightly focused on their cyber defenses: hardening their endpoints (e.g., laptops, mobile devices, and web applications); strengthening their network access credentials (by introducing two-factor authentication, requiring more frequent password updates, and removing outdated or expired credentials); and more actively and closely scrutinizing the security posture of third parties (such as vendors, contractors, and other partners).

Yet, as important as these cybersecurity-focused efforts are, the reality is that no organization can prevent all breaches; no matter how much time or money is applied to cybersecurity, there will inevitably be breaches. Regrettably, when it comes to being a victim of a cyberattack, it is a matter of when, not if.

This somber reality means that healthcare organizations, to better address the heightened levels of risk in our new normal, need to complement their cybersecurity-focused efforts with information governance (IG) efforts to help them better manage the information (sensitive or otherwise) behind their firewall. When done properly, IG will help ensure that when the next breach happens—which it will—the attackers will find less sensitive information to compromise, and the organization affected will have better (and more rapid) visibility into what information was in fact compromised.