# 5 Ways Health Cos. Can Reduce Pandemic Cybersecurity Risk

By **Elliot Golding and Kristin Bryan** (June 9, 2020)

Elliot Golding

Kristin Bryan

Robust cybersecurity continues to be of paramount importance as the COVID-19 outbreak develops and cybercriminals seek to exploit a remote workforce.

The Cybersecurity and Infrastructure Security Agency at the U.S. Department of Homeland Security recently issued an alert identifying the top 10 cybersecurity vulnerabilities routinely exploited by foreign malicious actors.[1]

The U.S. Department of Health and Human Services Office for Civil Rights shared the alert so health care organizations can likewise take appropriate action to reduce the potential risk of exploitation, as entities in this field are increasingly the target of cyberattacks.

This article provides a summary of the most common vulnerabilities and practical steps companies can take to reduce their risk today.

**Cybersecurity Issues Remain Federal Government Priority in 2020**

The alert reinforces that cybersecurity continues to be top of mind for regulators, particularly in the health sector. Other developments include the Federal Trade Commission seeking comments on whether revisions should be implemented to its breach notification rule. The rule currently requires personal health record vendors not covered by the Health Insurance Portability and Accountability Act to inform consumers and the FTC of breaches within 60 days.[2]

In March, the FTC separately issued cybersecurity advice regarding best practices for working remotely during the COVID-19 outbreak.[3] Other well-regarded organizations like the Health Information Sharing and Analysis Center have also issued detailed cyber guidance.[4]

A consistent theme in these documents — including the alert — is that malicious actors continue to exploit well-known software vulnerabilities against targets. This is because "exploitation of these vulnerabilities often requires fewer resources," particularly "compared with zero-day exploits for which no patches are available."[5] The alert urges U.S.-based entities to mitigate foreign cyberthreats through increased system patching and maintain comprehensive cyber programs.

To assist, the alert identifies the top 10 most exploited vulnerabilities by state, nonstate and unattributed cyberactors historically (from 2016 to 2019) and currently in 2020 using the common vulnerabilities and exposures classification system. In one case, a vulnerability first discovered in 2012 and publicly identified in 2015 continues to make the top 10 list years later. This suggests that companies are not addressing critical patches (in this case, a buffer overflow vulnerability that typically is exploited in connection with email phishing campaigns).

In addition to the top vulnerabilities from 2016-2019, the alert notes several trends the government already has observed in 2020 that companies should address immediately:

- Cyberactors are increasingly targeting unpatched virtual private network vulnerabilities;

- Organizations face heightened risk where rapid deployment of cloud collaboration services led to oversights in security configurations and greater vulnerabilities, e.g., companies failing to properly configure new Microsoft Corp. Office 365 deployments; and

- Preexisting cybersecurity weaknesses — such as poor employee education on social engineering attacks and a lack of system recovery and contingency plans — continue to make organizations susceptible to ransomware and phishing attacks, which have only increased in 2020.

The alert provides technical mitigation measures for each of the top 10 vulnerabilities. It also recommends that organizations transition away from any end-of-life software to improve cybersecurity.

**Best Practices for Reducing Cyber Risks**

Technical cybersecurity safeguards, such as patching, are obviously critical to an effective cybersecurity program. However, many of the most common vulnerabilities can be addressed without complex technical solutions. A top five list of practical recommendations to reduce risk is below.

***1. Preparing for a Breach***

Cybersecurity incidents do not need to be a crisis. Indeed, companies often are judged more by their response to an incident than the fact that one occurred. Organizations should take time to prepare for an incident in order to respond effectively and efficiently.

For example, organizations should develop and implement robust incident response plans, or IRPs, that cover how incidents are detected and reported internally, triaging, escalation, remediation and external notification if necessary. IRPs should be readily usable and practical, not tomes that sit on a shelf unused.

Companies should prepare for breaches and test their IRPs by engaging counsel to conduct a privileged tabletop exercise that simulates an actual data breach. Tabletops are a phenomenal way to check if employees know roles and responsibilities as well as to practice the process of investigating and responding to an incident. It is much better to identify and address weaknesses during a simulation than during a real incident.

***2. Vendor Management/Contracting***

Vendors continue to be a major source of risk. Companies should seek to reduce these risks by carefully vetting vendors and undertaking periodic oversight where feasible. For most companies, resource limitations prevent detailed reviews of every vendor, but a risk-based approach to vetting at least some vendors can pay big dividends in risk reduction.

For example, companies should consider using questionnaires to weed out less sophisticated vendors and prioritizing reviews based on the amount and sensitivity of personal information and technical access a vendor has. Companies should also seek contractual protections — particularly regarding breach issues — wherever possible.

Contracting playbooks can be enormously helpful to predetermine which clauses a company is willing to accept and what risks it is willing to take. Savvy counsel can provide industry benchmarking around market terms to identify which risks need to be addressed contractually.

### *3. Training*

Employees continue to cause many security incidents, whether the result of negligent conduct or intentional wrongdoing.[6] Even the best technical security cannot prevent all cyber risks, so companies should focus on the weakest links.

Companies should train employees regarding the company's cybersecurity policies, how to identify and avoid phishing attempts, and other common exploits. Then, train them again. Counsel can provide such training in addition to help companies develop insider threat monitoring programs to detect and prevent malicious conduct.

### *4. Policies and Procedures*

As part of a comprehensive cybersecurity plan, companies should document customized policies and procedures to reduce risk. Although writing down policies might not seem like the most important thing in the world, it helps formalize requirements, provide a yardstick to measure against, and foster a culture of compliance.

Key documents, beyond an IRP, include an acceptable use policy that provides guidance to employees about permissible use of data, networks, systems and other resources; VPN usage policies — particularly given the significant move to remote work — data backup and business continuity plans; and many others.

### *5. Cyber Insurance*

Finally, an organization should assess whether it has adequate cyber liability insurance. At a minimum, policyholders should review their commercial general liability policies and any standalone cyber policies with counsel to determine whether there is a gap in their coverage.

To the extent a deficit in coverage is identified, additional coverage options should be explored. With cyberthreats and data breaches increasing by the day, insurance, combined with a robust cybersecurity program, is a useful tool to manage those risks.

## Conclusion

The importance of a good cyber program is not new, but the COVID-19 pandemic has highlighted more cracks in the armor for companies than any other event in recent memory. As the alert noted, "March 2020 brought an abrupt shift to work-from-home that necessitated, for many organizations, rapid deployment of cloud collaboration services."[7]

Cybercriminals know those rapid changes likely mean more vulnerabilities to exploit.

Companies should take steps now to reduce their risk exposure by not only implementing the alert's patching recommendations, but also taking this opportunity to shore up privacy and cyber programs more generally. The recommendations listed above will go a long way toward helping any organization reduce risks and be better prepared to address any incidents that do occur.

---

*Elliot Golding is a partner and Kristin Bryan is a senior associate at Squire Patton Boggs LLP.*



[1] https://www.us-cert.gov/ncas/alerts/aa20-133a.

[2] https://www.ftc.gov/news-events/press-releases/2020/05/ftc-seeks-comment-part-review-health-breach-notification-rule.

[3] https://www.consumer.ftc.gov/blog/2020/03/online-security-tips-working-home.

[4] See https://healthsectorcouncil.org/hic-tcr/.

[5] https://www.us-cert.gov/ncas/alerts/aa20-133a.

[6] See https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf.

[7] https://www.us-cert.gov/ncas/alerts/aa20-133a.