The pandemic has led to many digital shifts and advancements in IT, especially in healthcare with the rise of telehealth and virtual visits. However, the security of these systems remains a concern. In Oct. 2020, the FBI, Department of Health and Human Services and the Cybersecurity and Infrastructure Security Agency alerted the healthcare industry and public health sector about the increased threat of ransomware targeting their networks and devices.

Government healthcare and industry leaders spoke at a recent FedInsider webinar about the security needs of the healthcare industry and the importance of health data protection. The following are some of the most important aspects of their discussion.

The Influx of Health Data
Health agencies are often users, custodians, owners and overseeing entities of personal identifiable information - which is data produced in structured and unstructured formats. Their complex systems must protect various types of health data with the right compliance and rules in place, especially as more data becomes digitized.

This rings true for the California Health and Human Services Agency, according to its Agency Information Security Officer Lloyd Indig. Indig said the quantity of health data has drastically increased, especially with COVID-related vaccine and testing results being added to the normal day to day collections.

“We went from zero records for COVID, of course, to now, having a record or multiple records for each citizen or resident of the state of California,” Indig said. “It’s been a drastic increase in what we’re receiving and trying to build and manage systems for.”

In addition to regular cybersecurity concerns, with healthcare data, there’s also the layering in of various federal restrictions and compliance requirements on top of everything else. And in California, there can be even more considerations depending on which department is collecting the information and what it contains. According to Tony Lauro, director of technology security and strategy at Akamai, looking across all health systems in the country, when you include every hospital and provider, there’s around 630 discrete regulatory requirements across nine domains.

This only gets more complex when it comes to flagging, archiving and storing data and medical imaging data. “All of that has to be thought about in terms of how it’s shared, who it’s shared with and making sure you keep all of that data,” Lauro said.

Managing the Complexity of Healthcare Infrastructures
Skilled attackers know that healthcare infrastructures are complex, and are starting to use that complexity as cover for some attacks. For example, in California, each health department has its own infrastructure, sets of tools and technologies. “There’s not one Health and Human Services infrastructure,” Indig said. “It’s a complex model and there’s not one solid network supporting me and my 13 departments.”

Featured Experts

Lloyd Indig
Agency Information Security Officer, California Health & Human Services

Tony Lauro
Director, Security Technology & Strategy, Akamai
Indig said they do have common tools and ways of sharing knowledge, resources and mitigation techniques to bring together and protect the disparate networks. Still, the department experiences phishing attempts, and its third-party partners have experienced ransomware attacks that can filter upstream.

The California Health and Human Services Agency has never directly experienced a ransomware attack, but is alerted when third-party partners do and must prepare to take preventative actions. “We do have some insider threats that have caused disruption too,” Indig added. These have largely resulted in unauthorized access to data, a worrisome cybersecurity breach in the health space.

**Securing Health Data and Public-Facing Services**

Akamai worked with Salesforce to set up a health-focused cloud for a patient portal so that citizens can better manage relationships and connect to the medical care they need. The goal, Lauro said, was to do this for the entire country as part of the COVID vaccine effort. Akamai was in a unique position to help with this effort considering the size and scale of Akamai’s distributed platform and geographically dispersed servers.

“We had 341 or 342 million people trying to go to the same website at the same time, and we were able to front that website and protect it from going offline,” Lauro said of the portal. Using bot management, login detection and web application firewall technology, Akamai successfully protected the security, privacy and login process of the portal from attacks.

In California, Indig is beefing up the state’s cybersecurity within healthcare using incident response planning, which adds resiliency to their already advanced protections. The California Health and Human Services Agency is also in the process of a strategic information security assessment with a third-party consultant to try and better understand where they should focus their security priorities and how to improve incident response should an attack successfully land.

“We are making sure that the technology recovery plans and the business continuity plans are all synced and tied,” Indig said.

The results from high-level exercises to assess the readiness of agencies in the event of a major cybersecurity attack and the role each department would play are also being put into playbooks so that everyone knows their role in an emergency. Now, the California Health and Human Services Agency is in the process of fine tuning those playbooks and communication plans that will become the baseline for policies regarding incident response.

**Investing in the Protection of Health Data**

Administratively, with the evolution of health technology and increase of public-facing portals, having a web application firewall to prevent account breaches is key. Also, Lauro recommended an investment in bot management to prevent fake user account creations, especially as attackers increasingly rely on bot nets to do a lot of their initial legwork.

Also, considering the rise in device usage from home that connects back to the enterprise network, Lauro advised installing proper malware protection and the ability to validate a remote connection using various components of zero trust.

“By validating the user and doing a device posture assessment, you can make sure that a device isn’t infected before it comes in,” Lauro said. “How you manage those remote connections is more important now than ever.”

A recursive Domain Name System lookup can also help prevent a health organization from a cyberattack or mass exploitation campaign. This method allows a single DNS server to watch all devices and servers connected to the enterprise network regardless of where they are located. If one device falls victim to a malicious phishing attempt, and others begin downloading the same malware, the potential threat is assessed and flagged to prevent other devices from also falling victim.

And finally, to prepare for the threat of increased ransomware attacks, Lauro said that investing in secure, offline backups that can’t be accessed, erased, infected or changed is a key to better cyber resilience. It’s almost a necessity today in the face of an increasingly dangerous threat landscape.