“Examining Health Sector Cybersecurity in the Wake of the Change Healthcare Attack”

Questions for the Record - Robert Sheldon

The Honorable Earl “Buddy” Carter

As these challenges have persisted for weeks, pharmacies continue to encounter challenges with delayed reimbursement and processing manufacturer coupons and copay assistance programs that some of their patients rely on to access essential medications. Given this ongoing impact, what preventative steps can be taken to expedite restoration for pharmacies and their patients amid future incidents and to help mitigate the impact on pharmacies and patients?

Response

Thank you for the question. Unfortunately, I’m unable to comment specifically on reimbursement challenges. However, based on recent threat activity, it is likely that pharmacies and other healthcare entities large and small will continue to be targeted by cyber threat actors due to their access to sensitive medical information and their demanding operational requirements. Therefore, it's important that entities proactively deploy cybersecurity measures to protect themselves.

Additionally, as I outlined in my testimony, policymakers can support stronger cybersecurity defenses by:

- Leveraging tax mechanisms (e.g., credits) to promote adoption of cybersecurity measures. These measures could be prescribed and/or targeted to selected beneficiaries (e.g., small providers, rural providers, etc).
- Enabling harmonization of regulatory obligations to report cyberattacks. This will ensure that small entities in particular are not distracted from breach response by duplicative compliance requirements.

The Honorable Nanette Barragán

There is a significant risk of cybercriminals who seek to steal data for financial gain. With the increasing frequency of cyberattacks on healthcare systems, what strategies do you propose to bolster cybersecurity measures specifically tailored to safeguard patient Data?

Response

Thank you for the question. As I highlighted in my submitted testimony, there are a few things that all entities should be doing in order to protect themselves and their sensitive data.

First, small- and medium- sized entities in particular, including those with resource constraints, should strongly consider leveraging a trusted Managed Security Services Provider (MSSP). The focus should be increasing speed and efficiency in dealing with threats. At best, this type of partnership enables MSSPs to focus on security and healthcare providers focus on healthcare. Resident security talent within user organizations also saves time and can focus on esoteric security challenges (like those presented by integrating new IOMT solutions); broad security program maturity enhancements; and leadership communication.

Entities in the sector that already have sophisticated security programs should focus on the frontiers. These include:

- Leveraging Artificial Intelligence for security-related tasks;
- Implementing robust identity threat protection solutions;
- Driving enterprise-wide operational efficiency through the use of Next-Generation Security Incident and Event and Management (Next-Gen SIEM) solutions;
- Adopting a “shared services” architecture where appropriate to enforce security measures across federated or multiple associated entities;
- Addressing concentration risks from overreliance on one vendor across multiple parts of the enterprise IT environment.