Prepared Testimony and
Statement for the Record of

Gary Horn
Vice President and CTO, Advocate Health Care

Hearing on:

"Federal Efforts to Improve Cybersecurity"

Before the

House Committee on Oversight and Government Reform
Subcommittee on Information Technology

Chairman Hurd, Ranking Member Kelly, and distinguished members, thank you for the opportunity to testify before the committee today.

My name is Gary Horn, and I am the Vice President of Technical Services and Chief Technology Officer of Advocate Health Care (Advocate). Advocate, a not-for-profit, mission-based health system, is the largest health system in Illinois and one of the largest health care providers in the Midwest. Advocate operates more than 350 sites of care, including 12 hospitals that encompass 11 acute care hospitals, one of the area's largest home health care companies, and one of the region's largest medical groups.

Advocate is proud to be a national leader in innovative payment and care delivery models, and we continually seek to enhance and expand such efforts to the benefit of more patients and communities. We have established one of the largest accountable care organizations (ACOs) in the country, which includes a commercial insurance contract, a Medicare Shared Savings Program (MSSP), and a Medicaid Managed Care Program. As the nation's health care system adopts new delivery system reform initiatives, we are eager to share our experiences and knowledge with the U.S. Congress to the benefit of providers and patients across the country.

Advocate on a monthly basis mitigates an average of 59,908 Endpoint Threats, and 200 Advanced Malware threats. With a daily internet usage of over 3.6 Terabytes, over 120 thousand known phishing, fraudulent, or spyware websites are blocked. Additionally, Advocate receives inbound requests from over 100 foreign countries in which we do not have a presence in.

My testimony today will focus on Cybersecurity and its importance in providing seamless data accessibility while providing a safe environment for the patients we serve.

The Trend Toward Digitization

In today's modern healthcare environment, a rapid shift from paper to the electronic medical record, in addition to the digitization of all facets of patient data has occurred. Data can be generated manually through data entry or automatically by medical devices, such as infusion pumps and electrocardiogram (EKG) systems. Given the rapid growth of the Internet of Things (IoT)[1], the amount of critical data is increasing exponentially. Much of this data is collected to support population health initiatives and hence originates outside the strictly controlled security walls of Advocate. As with the medical record, much of this electronic data is sensitive and must be protected per HIPAA regulations. Flexible high speed networks and the Internet play a key role in transporting data and supporting activities such as real-time analytics, decision support, machine intelligence, and seamless portability which is used to provide rapid, effective, and high-quality patient care. While the network infrastructure is a necessary and valuable asset, it is subject to cybersecurity attacks from both external and internal bad actors with malicious intent. Such attacks can range from outright theft, data leakage, data manipulation, and loss of accessibility, to being encrypted and held for ransom. Because any of these events can have a serious effect on patient safety, business operations, and community trust, it is paramount to have a proactive, well-structured cybersecurity program in place.

[1] The internet of things (IoT) is the network of physical devices, vehicles, buildings and other items—embedded with electronics, software, sensors, and network connectivity that enables these objects to collect and exchange data.

Cyber Measures and Risk Analysis

Advocate has taken a strong, proactive stance around the protection of both physical and electronic assets through the development of a cybersecurity framework. The pillars of the cybersecurity program include eight tenets: security and privacy assessments, electronic network security, enterprise device management, data breach insurance, business continuity, incident reporting, security awareness programs, and IT security metrics. Of particular interest are the areas of assessments and electronic network security. Security and privacy assessments allow Advocate to know where electronic protected health information (ePHI) is used and stored (including electronic medical devices) and to correct any anomalies proactively. The output of the assessments is used additionally in dashboards providing a complete view into the overall risk profile around ePHI.

Cyber Measures and Network Level Risk Reduction

While traditional perimeter security remains effective for inbound exploitation, modern threats are most often inside the protected network. To guard against these often complex and highly damaging threats, Advocate has made a significant investment in a multi-faceted, multi-layered approach that leverages Advanced Persistent Threat (APT) controls including an Enterprise Anomaly Detection System and Enterprise Vulnerability Scanning which allow for unsurpassed network visibility and real-time threat detection. This approach alerts network administrators of malware and associated operations where an unauthorized actor or group of actors has gained access to the network or other internal resource and has remained undetected for a long period of time with the goal of data exfiltration.

Both Security Incident Event Monitoring and a Managed Service arrangement are utilized to determine if security threats need to be investigated and/or mitigated. The latter provides not only critical monitoring but also correlates events from all of its customers regardless of sector to provide alerts around zero day

vulnerabilities[2]. One of the most important components of the infrastructure are the Authentication Provider Services[3]. If these services are compromised, an attacker can gain access to essentially all digital assets and has full control of the network and user access policies. Advocate has gone to great lengths to harden these services through the addition of a trusted and known good architecture including a highly secure administrative environment. This modernization effort is seen as a critical component in ensuring the digital environment is safe and protected.

Advocate is in the process of addressing a component often overlooked in network security design - the software internal to the network and routing components. Should this software be compromised in any way through malicious code or a back door, the entire network and associated assets are at risk. To mitigate this risk, the installed software is hardened through a combination of independent verification and validation, diversification to prevent exploitation, and secure software delivery.

Cyber Measures at the User Level

In most instances, a malicious payload[4] is delivered unknowingly through an end-user action such as web browsing or opening an email attachment. While network level detection and protections are vitally important, preventing an exploit from entering the network is the most beneficial defense; Advocate has invested heavily in multiple controls to help afford the required protections:

- All systems are electronically inventoried and patched on a monthly basis.
- Locally installed applications allow monitoring of the environment to ensure all machines are in compliance.
- Endpoint tools provide both traditional malware protection along with intrusion prevention services as a primary line of defense; the associated

[2] The term is derived from the age of the exploit, which takes place before or on the first (or "zeroth") day of a developer's awareness of the exploit or bug. This means that there is no known security fix because developers are oblivious to the vulnerability or threat.

[3] A centralized and standardized system that automates network management of user data, security, and distributed resources, and enables interoperation with other directories.

[4] Software carried by a delivery mechanism such as a Trojan horse, often intended to do harm to a computer system

malware signatures are refreshed twice daily however; a manual push can be performed if necessary.

- Advanced Threat Protection has been added to further protect against unknown malware by providing robust zero-day protection, and includes features to safeguard the organization from harmful links in real-time.
- Privileged User Management is employed through the removal of all administrative rights while allowing the user to safely perform their duties; this scheme prevents malware from exploiting privilege access rights and executing their payload.
- In the near future Data Loss Prevention (DLP) strategy will be deployed to prevent the inadvertent or malicious dissemination of confidential data outside the organization. DLP will reside both at the workstation and as a man-in-the-middle deployment, the latter to guard against the same risks at an application/server level. Should a device be physically removed from the organization, the local storage device is encrypted preventing the contained data from being read; in addition, the stolen device can be remotely disabled.
- Finally, automatic encryption of removable medium such as memory sticks and portable hard disk drives is also included with the encryption tools.
- Email classification and encryption.

Clinical equipment that cannot be patched and provided malware protection due to FDA regulations is containerized via advanced firewall technologies that include network level malware protection as well as intrusion detection and prevention systems.

A key pillar of the cyber security program is end-user awareness training. It is well known by the cybersecurity community that people are the weakest link in the security chain and hence Advocate provides to all associates both mandatory training around HIPAA and other related topics as well as regular cybersecurity awareness campaigns through various forms of media. The training and informational programs are designed to build and maintain a strong organizational culture of safety.

While the cost of all of the aforementioned security components is significant and requires a considerable number of skilled cybersecurity associates to build, maintain and monitor, each technology is considered mandatory in ensuring the delivery of safe and effective patient care, and is a key component in the delivery of population health management services.

Role of Government

While I applaud the President's Cybersecurity National Action Plan (CNAP), which outlines strategies to improve cybersecurity and protect the national interest, I believe the CNAP does little to enhance privacy or preserve public safety as it does not provide a concise plan around an overarching cybersecurity ecosystem. The establishment of cybersecurity public awareness campaigns and the creation of the Federal Chief Information Security Officer (CISO) are steps in the right direction. While it is unclear whether the CISO will play a significant role in the development of cybersecurity programs, I believe it is imperative that the CISO be afforded the opportunity to be an agent for change.

Federal IT infrastructure requires modernization. It is important to recognize, however, that improving IT infrastructure cannot focus solely on cybersecurity. Instead, modernization should take into account the needs of the business community and must take the utmost care to not impede private enterprise. With a growing shortage of professionals with strong cybersecurity skills and understaffed organizations, the development of a fully comprehensive strategy around training and education in addition to a well-designed core cybersecurity curriculum is critical. In my opinion, the shortage of professionals with cybersecurity training is a national security issue.

Advocate is an individual actor investing heavily in cybersecurity measures to provide a secure environment, however much of this work is performed in a silo. I feel that the Information Technology-Information Sharing and Analysis Center (IT-ISAC) has an excellent model that demonstrates significant value in enhancing cybersecurity through both collaboration and the sharing of threat information; it is a good example of a critical tenet of the cybersecurity ecosystem. Too often, other means of sharing information around cybersecurity incidents is

overshadowed by legal, and regulatory concerns, and is general in nature, lacking sources of truth resulting in limited effectiveness. The knowledge and processes around the rapid dissemination of events can go a long way in supporting the proactive cybersecurity stance required by data critical organizations such as Advocate, its cybersecurity continuum, and the public interest.

However, as a nation, we must be bolster the security of our ecosystem, not just place the burden on individual institutions. The bad actors targeting all sectors include foreign and domestic criminals, as well as nation states. The Cybersecurity Act of 2015 took important steps to improve our cybersecurity defenses, which are just now being implemented. Among other things, the Act promotes information sharing across public and private sectors, and also contains specific provisions related to health care. Among those is creation of the recently formed Health Care Industry Cybersecurity Task Force, which is charged with better understanding the needs of the health care field and identifying helpful resources. The Cybersecurity Act of 2015 also directs federal agencies to establish, in coordination with the private sector, voluntary, consensus-based guidelines and best practices that are consistent with existing requirements. These resources will be tremendously helpful to health care systems such as Advocate, but also must address the needs of small hospitals and individual practitioners. Given that information is shared across health care organizations, even the smallest provider must be secure. To provide the most benefit, they will also need to be actionable, and specific. While these steps are critically important, we also need to ensure that the federal government is doing everything it can to identify, disrupt and apprehend the bad actors

An area of particular concern are the OCR and HHS policies around cybersecurity incidents. Healthcare takes cybersecurity seriously and invests heavily in people, policies, procedures, and infrastructure to prevent bad actors from compromising their network environments, however there is never a guarantee that a cybersecurity event cannot occur. New threats emerge constantly and it is unlikely that any healthcare entity can always be a step ahead of the emerging threats. When an incident does occur, the reporting entity is viewed as negligent or incompetent rather than a victim of a crime and a stiff penalty levied. Because healthcare is being asked to reduce cost and improve its cybersecurity measures,

it would be in the public interest that rather than a monetary fine, the monies be applied to that entities cybersecurity continuum allowing it to swiftly and effectively address the cause of the event and enhance its cybersecurity profile.

The importance of all aspects of cybersecurity are front and center at Advocate and is part of its corporate culture. At stake is the safety of the patients we serve, the trust of the community, and the integrity of our business relationships. It is well understood that no matter the size of the investment and the breadth of solution, the risk of an attack is always present. Advocate is committed to ensuring cybersecurity remains a top priority.

Thank you again for the opportunity to testify before you today. I look forward to your questions.

GARY HORN

210 Amherst Avenue
Des Plaines, Illinois 60016
(847) 699-4093

SUMMARY:

An executive visionary with extensive leadership experience and proven ability focused on planning, engineering, business process improvement, budget development and cost control, safe culture, collaborative tools, team management, and staff education to provide leading technical services and infrastructure to a large integrated health care system.

RECENT PROFESSIONAL HIGHLIGHTS:

- Innovation leader and consultant involved in many major corporate engineering and service improvement initiatives.
- Thought leader in the development and evangelism of the corporate culture of safety and network security.
- Collaborated in the authoring and publication of several industry related white-papers and text books.
- Leadership role in the engineering and implementation of the Advocate Health Care call centers utilized enterprise-wide for patient scheduling and collaboration.
- Responsible for the technical integration and optimization of merged or acquired entities into Advocate Health Care.
- Responsible for the restructuring of partner relationships to optimize purchasing leverage and contract structure to provide continual operating and capital cost reductions.
- Leadership role in the construction of a comprehensive regulatory compliance program focused around HIPAA, HITECH, and PCI guidelines.
- Redesigned processes and procedures, optimized staffing models, and focused responsibilities to optimize the operation of the Technical Services area while providing comprehensive training and development of associated team members.
- Developed and managed the deployment of a comprehensive network security program comprised of both technical infrastructure and regulatory compliance tenets.
- Responsible for developing methodologies to integrate clinical technologies such as patient monitoring within a standard enterprise network environment.
- Engineered and managed the deployment of the enterprise-wide software defined and unified services aware, local area, wireless, and wide area networks.
- Developed and managed the deployment and maintenance of a carrier-grade Metropolitan Area Network employing dark fiber and MPLS services providing significant operational flexibility, high availability, and significant cost savings.
- Engineered and managed implementation of a hybrid cloud compute infrastructure leveraging the Metropolitan Area Network to provide maximum flexibility, applications availability, and business continuity while reducing operational costs.
- Designed and managed implementation of a carrier-grade, highly available and secure Internet infrastructure leveraging the Metropolitan Area Network.
- Designed and managed optimization of the data center SAN architecture to support a hybrid cloud strategy resulting in maximum flexibility, high-availability, and overall operational cost savings.

PROFESSIONAL EXPERIENCE:

Advocate Health Care ***(formally EHS Health Care and Lutheran General HealthSystem)***

A forward thinking organization focused on providing cutting edge solutions in the delivery of safe, high-quality health care.

Vice President, Technical Services and CTO **2009-Present**

Responsible for the innovation, vision, direction, and overall management of the technical infrastructure required to support the business and strategic needs of a complex, rapidly changing and dynamic healthcare delivery network. Responsibilities include but not limited to the oversight of network security and regulatory compliance, voice, data, and storage area networks, compute infrastructure data centers, business continuance operations, call centers, budgeting and, cost containment. 130 FTE's with a budget exceeding $100 million dollars.

Director, Enterprise Architecture and Network Security **1995-2009**

Responsible for the design, configuration, installation, and maintenance of large and complex voice and data network system implementations to support the business and strategic needs of the enterprise. Responsible for network security and business continuity operations. 32 FTE's with a budget exceeding 25 million dollars.

Regional Team Leader, Information Systems **1994-1995**

Manage the selection, design, installation, configuration, and support of complex systems to support the business needs of the organization and regional sites.
7 FTE's with a budget exceeding 5 million dollars

Lutheran General Hospital and HealthSystem

A leading health care organization in the Midwest, providing a vast range of services to the community.

Director, Technical Engineering **1991-1994**

Administratively responsible for the daily operations of Communications Engineering, Switchboard, Answering Service, and Clinical Engineering.
45 FTE's with a budget exceeding 10 million dollars.

Director, Telecommunications **1988-1991**

Managed Communications Engineering, Switchboard and Answering Service. 30 FTE's

Manager, Telecommunications **1985-1988**

Managed Communications Engineering Department. 5 FTE's

Supervisor, Telecommunications **1983-1985**

Developed and supervised the area of Communications Engineering.
4 FTE's

Biomedical Engineer, Clinical Engineering **1981-1983**

Responsible for design and development of custom medical electronics required by the hospital and its research programs. Coordinated departmental operations and provided technical training sessions.

WCBR-FM
Arlington Heights, Illinois

Director of Engineering **1983-1998**
Responsible for the design, installation, and maintenance of audio and R.F. systems. Insure broadcast and administrative operations are in compliance with FCC rules and regulations. Manage on-air operations staff. 10 FTE's.

Maine Township High School District 207 **1981-Present**
Park Ridge, Illinois

Chief Engineer - Broadcast Facilities
Provide consulting, implementation, and technical support for school district on-air broadcast facilities. Provide classroom instruction to students as needed.

Hamilton Electronics Corporation
Chicago, Illinois

Chief Design Engineer

1978-1997
Responsible for the design, development, and documentation of professional audio products and custom instrumentation. Directed production and testing of product manufacturing and associated build team. 8 FTE's

---

EDUCATION:

University of Illinois, Chicago, Illinois **2007-Present**
Ph.D. Program – Electrical Engineering

Southern Illinois University, Carbondale, Illinois **1977-1981**
Masters of Science in Electrical Engineering
Bachelor of Science in Electrical Engineering
Associate of Science in Electronics Technology

ACCREDITATION AND MEMBERSHIPS:

General Class FCC Radio Telephone License
Member of the Institute of Electrical and Electronics Engineers
AOPA

INDUSTRY LEADERSHIP AFFILIATIONS:

Chair, Alcatel-Lucent Health Care Technical Advisory Board
Philips Technical Advisory Board
Palo Alto Networks Technical Advisory Board
AT&T Healthcare Services core design team
Sun Microsystems product steering committee
Cisco strategic product development committee

INDUSTRY SPEAKER:

Gartner Health Care Symposium
Cerner Health Conference
VoiceCon
HIMSS
Keynote, Alcatel-Lucent Forum
Keynote, Alcatel-Lucent Engagement Tour, 2015, 2016
Alcatel-Lucent Engagement Tour 2010-2014
Alcatel-Lucent SReXperts
Philips Healthcare User Summit