CYBERSECURITY CHALLENGES TO HEALTHCARE SECTOR

Independent Of and Due To COVID-19

RAPIDLY GROWING (AND EVOLVING) TECHNICAL LANDSCAPE
- Internet-connected medical devices have been developed and widely deployed, without proper privacy and security measures in place
- Proliferation of unregulated mobile apps that leverage PHI/PII but do not secure it

OVERWORKED AND UNDERTRAINED STAFF
- Many healthcare personnel are undertrained on cybersecurity
- Even with good training, environmental factors affect practitioners’ security-related behaviors more than intention

COMPETING OPERATIONAL PRIORITIES
- Operational needs often prioritize speed and information sharing over information security
- Business and compliance requirements result in large-scale data portability needs

INCONSISTENT CYBER HYGIENE
- Stand-alone technologies are being digitized and integrated with other systems, creating interoperability dependencies, network segmentation risks, and other cybersecurity challenges
- Legacy systems, no longer supported by their manufacturers, cannot incorporate the latest security updates, thereby introducing permanent vulnerabilities into organizations’ networks

HIGHLY VALUABLE TARGET DATA
- PHI is estimated to be worth 10-20 times the value of credit card data on the Dark Web, and is sought after by criminals and nation-states alike
- Credentials enable repeated, and continuous expansion across targeted systems, providing multiple avenues for malicious actors to inflict damage
- Biomedical and pharmaceutical research and development data is the backbone of a nearly $160 billion industry

BUDGETARY CONSTRAINTS
- Organizations are spending a vast majority of limited IT budgets on acquisition, implementation, and adoption of technical solutions with few resources left to secure and maintain their networks
- Many HPH organizations don’t have internal IT or security teams and outsource the capabilities or conduct activities ad hoc without having anyone internal who is accountable for security
- Minimal training for remote workers
- Lack of distributed/remote system recovery plans
- Lack of endpoint protection due to overreliance on network security

RAPID PROCUREMENT AND IMPLEMENTATION OF SECURITY TOOLS FOR NEW WORK ENVIRONMENT
- Increased likelihood of misconfiguration or botched security tool deployments
- Lack of maintenance and sustainment plan for new technology

GLOBAL SCOPE OF CRISIS
- Effective response requires coordinating with other nation states—including geopolitical adversaries and nontraditional partners
- Risks and consequences evolve over time through chain reactions
- Fewer options for aid or support

PROTRACTED DURATION OF CRISIS
- Continued uncertainty of long-term crisis compounds societal and individual stressors, increasing susceptibility to social engineering
- Economic consequences increase individual financial need

2 A literature review of the state of cybersecurity in healthcare found that organizations were spending up to 95% of their budgets on implementation and adoption and less than 5% on security | Eric Decker and Julie Chua, “Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients,” Health and Human Services, Department of Homeland Security, and National Institute of Standards and Technology (2018).