PHILIPS

Spotlight: getting to the source of risk

Where do your cybersecurity risks lie?

Cybersecurity is often a moving target. Health systems are under tremendous pressure to stay ahead of cyberattacks, but the inherent complexities, talent shortages and lack of a standardized playbook for keeping systems current also pave the way for vulnerabilities. Addressing those vulnerabilities requires the optimal mix of human and technical resources to achieve a full understanding, both granular and broad, of the challenges presented and potential impact. To put it simply, if you are not informed, you are at risk. In order to mitigate threats, healthcare leaders must not only recognize their level of risk but the cause of it. Philips understands the risks facing health systems today and can help identify and address those risks.

Potential outcomes of common organizational cybersecurity risks

Organizational risk	Potential outcome
Lack of embedded security requirements in application development as well as **lack of security parameters** in hosted websites	**Security breach** via abuse of vulnerabilities in software and websites
Lack of governance to handle the privacy of sensitive information collected during the course of business operations	**Loss of information from security breach** and violation of compliance requirements
Weak identity credential and access management (including failure to implement proper access, inconsistent review of user access and timely removal of access rights) and **failure to implement two-factor authentication**	**Unauthorized access** or leakage of critical information
Insecure decommissioning of IT assets/medical devices – including nonremoval of configuration, authentication and other information from assets prior to disposal	**Loss of organization's information assets**
Failure to incorporate minimum security requirements in information systems, such as password management hardening, vulnerability management and secure network zoning	**Security breach** on IT assets
Inadequate incident response infrastructure (e.g. plans, defined roles, training, communications and management oversight) for quickly discovering a cyberattack	**Delay in eradicating the attacker's presence, containing cyberattack damage and restoring integrity** of the network and systems
Inadequate backup of information from end-user devices and enterprise-grade servers/databases	**Failed continuity of business operations** during a crisis due to nonavailability of information

Philips can help organizations uncover cybersecurity vulnerabilities and implement best practices based on our extensive experience working with complex government agencies and health systems large and small. Our expertly trained and certified consultants can partner with your in-house staff to conduct organizational security assessments and provide actionable recommendations based on a globally recognized risk framework. We bring together the knowledge, resources and competencies to deliver a truly scalable approach to cybersecurity that helps empower our customers' digital transformation.

Learn about Philips Cybersecurity consulting services.