Hologic Enterprise Information and Cybersecurity

INTRODUCTION

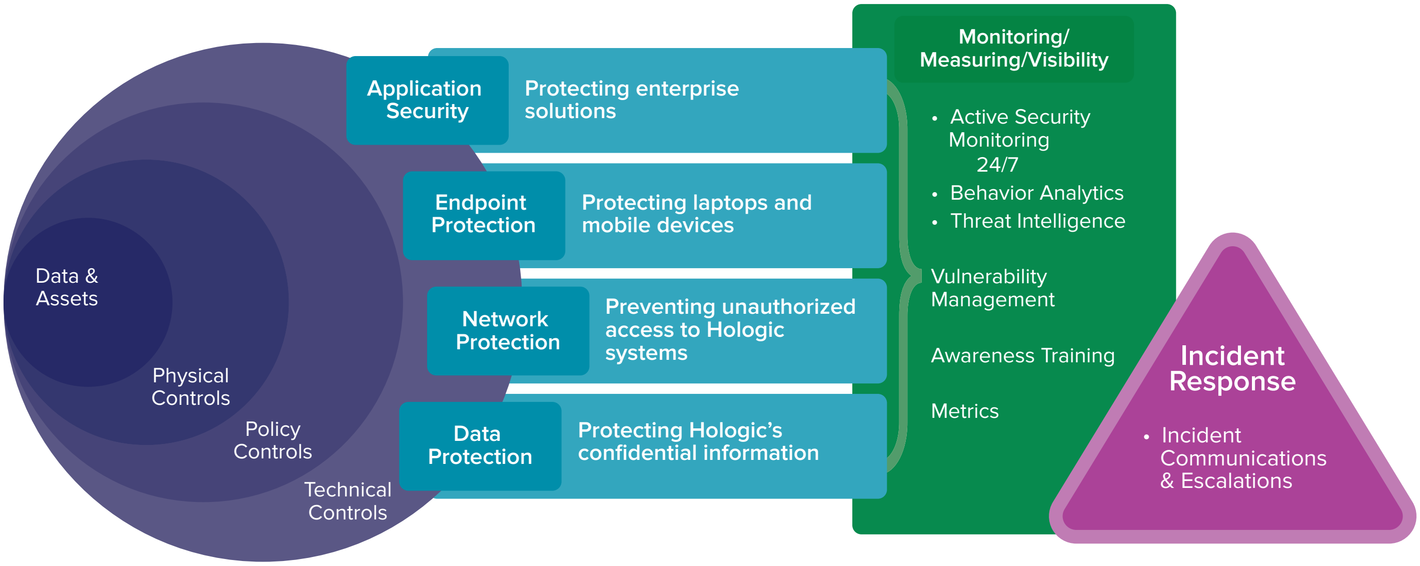
Hologic is a global medical technology company specializing in women's health and wellbeing. We offer innovative solutions for screening, detecting and treating conditions and diseases that affect women throughout their lives, including breast, gynecological and skeletal issues; cervical cancer testing; and sexually transmitted diseases. As a science-driven company, our products are backed by clinical evidence, ensuring that they perform as intended, so healthcare professionals can have greater certainty in their decisions and patients, greater peace of mind.

In recognition of this mission, it is critically important that the Hologic enterprise systems, applications and infrastructure our employees leverage to deliver solutions to our customers and the marketplace are secure. It is also equally important that any information we maintain about our customers, partners and employees is secure. It is for this reason Hologic has implemented a robust, multi-layered Enterprise Information and Cybersecurity Program.

The Cybersecurity Program is aligned with the *National Institute of Technology (NIST) Cybersecurity Framework (CSF).* The NIST CSF offers a simple, yet effective construct whose core represents a set of cybersecurity practices, outcomes and technical, operational and managerial security controls (referred to as Informative References) that support the five risk management functions: Identify, Protect, Detect, Respond and Recover.

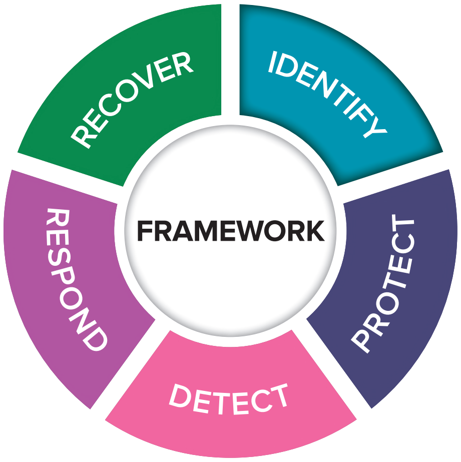
Hologic leverages best-of-breed technologies monitored and implemented by qualified information security professionals and world-class partners to ensure a secure environment. Implemented technologies include strategic placement and monitoring of firewalls, network and host-based IPS; data loss prevention (DLP) tools; Internet access monitoring; enterprise antivirus; hardened hosts; electronic media forensics; vulnerability management; role-based access controls (RBAC) for internal or external access to Hologic applications and networks; Secure Authentication, including Multi-Factor authentication (MFA); and security information event monitoring (SIEM), among others.

Figure 1:


Data & Assets
Physical Controls
Policy Controls
Technical Controls
Application Security
Protecting enterprise solutions
Endpoint Protection
Protecting laptops and mobile devices
Network Protection
Preventing unauthorized access to Hologic systems
Data Protection
Protecting Hologic's confidential information
Monitoring/ Measuring/Visibility
• Active Security Monitoring 24/7
• Behavior Analytics
• Threat Intelligence
Vulnerability Management
Awareness Training
Metrics
Incident Response
• Incident Communications & Escalations

Independent assurance through annual external audits and dedicated internal audit and compliance group

As a public company, Hologic complies with the *Sarbanes-Oxley Act of 2002 (SOX)* regulations of financial systems. This means that independent external auditors annually audit and report on Hologic's Information Technology General Controls (ITGC). Furthermore, Hologic's Quality Management System (QMS) complies with international regulations and standards, including Good Manufacturing Practices (GxP), ISO 13755 and others, as applicable. As part of these regulations, Hologic is regularly inspected by auditors and certifying agents. Hologic also relies on our Management, Board of Directors, Internal Audit, Quality and Regulatory teams to provide an additional layer of internal oversight, governance, inspection and quality. Hologic's dedicated internal audit group reviews compliance and security laws, regulations and standards, and recommends controls and processes that need to be implemented to meet them. Similar to the NIST CSF, Hologic organized its Cybersecurity Program around the framework's five concurrent and continuous functions: **Identify, Protect, Detect, Respond, Recover.**



IDENTIFY

The Identify function assists Hologic in managing cybersecurity risks to systems, people, assets, data and capabilities. Understanding the business context, the resources that support critical functions and the related cybersecurity risks enables Hologic to focus and prioritize its efforts consistent with our risk management strategy and business needs.

ASSET MANAGEMENT

Hologic identifies and maintains an inventory of hardware and software assets. Hologic established its Information Protection Program, which is designed to educate associates on the methods to classify, label, handle and dispose of confidential information and all types of media. A matrix was developed to instruct employees on the appropriate methods of handling information, such as distribution, discussion, mailing, emailing, copying, storage and destruction. This matrix includes how each type of information classification should be handled in each of the above methods. Hologic employees are required to undergo and successfully pass Information Protection training to confirm their understanding of the Information Protection Program.

INFORMATION SECURITY POLICIES

Hologic established comprehensive protection and clear accountability for Hologic personal data and confidential business information assets through an extensive system of policies, procedures and standards. This includes information assets that are confidential and proprietary to Hologic, personal to our clients and

Figure 2. NIST CSF Five Functions

Identify	Protect	Detect	Respond	Recover
Identify the right strategy that removes risk and enables best-in-class service: ✓ Asset Management ✓ Information Security Policies ✓ Organization of Information Security ✓ Technology Risk Management ✓ Human Resources Security ✓ Compliance	Develop preventive processes and technologies to protect critical assets: ✓ Access Control ✓ Cryptography ✓ Physical and Environmental Security ✓ Communications Security ✓ Malware Protection ✓ System Acquisition, Development and Maintenance ✓ Supplier Relationships	Run capabilities to detect and respond to cyber events: ✓ Security Operations Center ✓ Operations Security	Rapid response through Incident Management protocols: ✓ Incident Management	Regularly tested Resiliency and Recovery programs: ✓ Business Resiliency

all other personal and confidential business information assets and resources subject to legal, regulatory and compliance protection. Hologic also has a mature Information Security Awareness and Training Program, including mandatory training, to ensure that all Hologic associates are aware of, and comply with, the provisions of these policies.

ORGANIZATION OF INFORMATION SECURITY

Information Security is an independent function of the organization, with the Chief Information Security Officer (CISO) reporting directly to the Chief Information Officer (CIO). Periodic interactions on the status of security within Hologic are scheduled with the Global Leadership Team and the Audit Committee of the Board of Directors to align with the company's business strategy and risk tolerance. The team is responsible for the alignment of Hologic's enterprise security to support business goals through strategic governance and continuous assurance programs.

TECHNOLOGY RISK MANAGEMENT

Hologic's Technology Risk Management Program is supported by the CISO and a dedicated staff of security professionals. The Technology Risk Management Program is tailored to the protection of applications, systems, network and data across Hologic applications, databases, systems and processes.

HUMAN RESOURCES SECURITY

Hologic executes a multi-layer Human Resources Security Program. Individuals employed by Hologic are required to have an identification badge and sign a Non-Disclosure, Confidentiality Agreement and Code of Ethics acknowledgment. Individuals are also required to complete a comprehensive background check that may include fingerprinting, criminal record, credit history and reference background checks, as permitted by law. Hologic developed a Security Awareness Program that is disseminated through multiple communication channels and security awareness training sessions. This approach ensures deeper understanding of the culture of security, while helping associates adhere to it through multiple channels of communication. Channels include corporate security newsletters, simulated social engineering and phishing exercises, classroom-based trainings, bulletins and security videos, among other practices.

COMPLIANCE

Hologic conducts business in a highly regulated environment, adopting corporate-level policies and procedures that promote awareness of applicable privacy laws and regulations, ensure compliance with all requirements, and align internal programs with appropriate action. Hologic proactively monitors the cyber regulatory environment and implements practices consistent with direction from regulatory authorities. Hologic's Privacy Policy can be found on Hologic's corporate website: https://www.hologic.com/privacy-policy

PROTECT

The Protect function outlines appropriate safeguards for Hologic to ensure delivery of critical infrastructure services. The Protect function supports the ability to limit or contain the impact of a potential cybersecurity event.

ACCESS CONTROL

Hologic implements a multi-layered Access Management Program that includes documented approved job roles; access appropriate to role reviews; and is supported by mature authentication, authorization and accounting standards. Access policies, procedures and controls ensure that only authorized personnel are granted access to data. Access is authorized and granted based on the concept of least privilege and limited to those having a business need for such access. Access requests are authorized and tracked through a formal access management system, and appropriate management approvals are required to enable system access. Associate access is reviewed periodically, and access is removed upon termination or transfer out of appropriate job roles. Hologic also established and maintains appropriate authentication credentials for access to Hologic information systems. The strength and sophistication of these credentials is commensurate with the inherent risk and/or value of the information or the resource. The IS Access Control standard mandates the length and complexity of credentials, how often passwords are changed, and the number of invalid attempts before account lockout.

CRYPTOGRAPHY

Hologic established a cryptography standard and techniques used to protect Hologic information and information with which Hologic has been entrusted. This includes approved algorithms and key lengths. Additionally, Hologic established processes and technologies to encrypt confidential customer data during external transmission, removable media and record-keeping systems where customer data is stored.

PHYSICAL AND ENVIRONMENTAL SECURITY

Hologic implemented a comprehensive Physical Security Program that employs a variety of techniques and strategies to secure company assets, including people, property, systems and information. The application of specific physical security controls is based on a risk assessment process that evaluates the criticality of an asset and the threats against which it must be protected. Security controls may include, but are not limited to, 24/7 security officer presence on site, electronic access control (including two-factor authentication for highly sensitive areas such as data centers), intrusion detection systems, closed circuit television (CCTV) and physical locking devices. Education and awareness programs are specifically targeted to ensure that employees understand their personal responsibility for security. Hologic facilities are also equipped with appropriate systems and procedures for monitoring of the environment to include temperature, fire, smoke and power failure.

COMMUNICATIONS SECURITY

Hologic established network security and information transfer controls that ensure the protection of information and information assets. These controls include, but are not limited to, firewalls, intrusion detection and prevention systems, Distributed Denial of Service (DDoS) mitigation, multiple layers of threat detection and advanced malware prevention, proxy servers, and secure file transfer technologies.

MALWARE PROTECTION

Hologic employs a suite of endpoint protection solutions, including Next-Gen Antivirus (NGAV), Endpoint Detection and Response (EDR) that give real-time protection, as well as threat hunting capabilities.

SYSTEM ACQUISITION, DEVELOPMENT, AND MAINTENANCE

Hologic's procedures and development methodologies incorporate security into the systems development life cycle. This includes, but is not limited to, security training of application developers, and secure code reviews and penetration tests of externally facing applications.

SUPPLIER RELATIONSHIPS

Hologic's Partner Risk Management Program includes technology risk reviews of Hologic partners that process sensitive information, including those that process or store data. These reviews are conducted on a regular basis and follow a comprehensive risk questionnaire derived from Hologic security policies, ISO 27001 and other industry best practices. Contract language is drafted to include information security and privacy provisions in addition to the standard business agreements.

DETECT

The Detect function defines the appropriate activities for Hologic to identify the occurrence of a cybersecurity event. The Detect function enables timely discovery of cybersecurity events.

SECURITY OPERATIONS CENTER

Hologic leverages a highly rated global Managed Security Service Provider (MSSP) to augment its Security Operations group, adding additional threat intelligence for higher fidelity and to have 24/7/365 coverage for reviewing and detecting security events.

OPERATIONS SECURITY

Hologic executes a mature suite of controls and procedures that include change control, protection from malware, information backup, vulnerability management, data leakage prevention, hardened perimeter and infrastructure, backups, and logging and monitoring of numerous defense-in-depth security and risk mitigation technologies. Periodic vulnerability and penetration tests are performed by independent world-class security consultants.

RESPOND

The Respond function includes appropriate activities for Hologic to take action regarding a detected cybersecurity incident. The Respond function supports Hologic's ability to contain the impact of a potential cybersecurity incident.

INCIDENT MANAGEMENT

Hologic established comprehensive information security incident management processes that include documented and tested cyber playbooks to address cyber events. Hologic defined processes to identify potential threats, assess any risk exposure, report risks to management and protect business operations. Where deemed appropriate, personnel will preserve the necessary evidence, inform legal authorities and perform forensic analyses.

RECOVER

The Recover function identifies appropriate activities for Hologic to maintain plans for resilience and to restore any capabilities or services impaired due to a cybersecurity incident. The Recover function supports Hologic's timely recovery to normal operations to reduce the impact from a cybersecurity incident.

BUSINESS RESILIENCY

Hologic has a comprehensive Business Resiliency Program, including both disaster recovery and business continuity. Hologic focuses on both preventing outages through redundancy of telecommunications, systems and business operations, as well as recovery strategies in the event of a loss. The business resiliency process includes business resiliency and disaster recovery planning, testing and ongoing training.

CONCLUSION

As global champions of women's health, Hologic is driven to enable healthier lives everywhere, every day. Toward this end, we are committed to helping healthcare professionals minimize doubt and maximize the confidence they have in their decisions and diagnoses. They must be able to count on our products to perform as we say they will, when lives and livelihood are at stake. A significant aspect of building this trust—a promise we call The Science of Sure®—comes from our creating and implementing a robust, multi-layered Enterprise Information and Cybersecurity Program. Within this highly secure environment, Hologic is able to manage today's evolving threats, adapt to securely meet changing organizational needs and protect all information we maintain about our customers, partners and employees.

If you have questions about Hologic's Enterprise Information and Cybersecurity Program, or this whitepaper, please contact Hologic at ecommerce@hologic.com or CustomerSupport@hologic.com

Appendix A

NIST Reference:

https://www.nist.gov/cyberframework/new-framework#background

Recognizing the national and economic security of the United States depends on the reliable function of critical infrastructure, President Barack Obama issued Executive Order (EO) 13636, Improving Critical Infrastructure Cybersecurity, in February 2013. The EO directed NIST to work with stakeholders to develop a voluntary framework, based on existing standards, guidelines and practices, for reducing cyber risks to critical infrastructure. The Cybersecurity Enhancement Act of 2014 reinforced NIST's EO 13636 role.

Created through collaboration between industry and government, the voluntary framework consists of standards, guidelines and practices to promote the protection of critical infrastructure. The prioritized flexible, repeatable and cost-effective approach of the framework helps owners and operators of critical infrastructure manage cybersecurity-related risk.

United States / Latin America
250 Campus Drive
Marlborough, MA 01730
Tel: +1.508.263.2900
www.hologic.com