Guidehouse

Cybersecurity: Equip Your organization to Defend, Detect, and Respond to Cyber Threats

Cybersecurity: Equip Your Organization to Defend, Detect, and Respond to Cyber Threats

Without such a program in place, organizations take serious risks, including:

- Regulatory fines for breaches/lack of notification (General Data Protection Regulation, Health Insurance Portability and Accountability Act, California Consumer Privacy Act, etc.).
- Reputational harm from negative news surrounding breach and loss of consumer trust.
- Financial harm from interruption of business systems or product recalls.
- Costly support for breach response and ensuing investigation.
- Shareholder lawsuits for insufficient data protection programs.

From early-stage companies preparing for a first product launch, to organizations completing clinical trials, to longstanding global manufacturers, no company anywhere in the world can avoid cyber threats without implementing and institutionalizing information security management best practices.

Employee, customer, patient, and company confidential data is collected, processed, and stored for a multitude of purposes, both within organizations and externally through the third parties that provide support and services, as well as the connected nature of products or other patient interactions. All of this information must be protected from the potential of unwanted or unlawful access, theft, or modification.

A robust cybersecurity management program will align with local or international security frameworks, including the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC) and the National Institute of Standards and Technology (NIST), to prevent, detect, and respond to suspected cyberattacks.

An established security program will be able to track and detect suspected incidents, and have communication channels in place to evaluate and respond to those risks.

In practice, especially for early-stage organizations, information security management programs often miss key components or get folded into another related but separate discipline, such as privacy or information architecture. It is important to recognize that privacy and security are separate functions. Data privacy focuses on how a company uses, protects, and shares an individual's personal information, whereas data security safeguards data from malicious attacks and unauthorized access.

Likewise, information security also should be delineated from the information architecture, which focuses on the structural design and use of data, not how to protect it.

A thorough cybersecurity risk assessment will review existing policies and procedures to 1) identify potential risks and critical gaps, 2) prioritize how and when to address each, and 3) develop a strategic road map for future enhancements. The assessment will also help to describe the types of measures to implement, which may include:

Initiating employee awareness training on best practices and measures.

Establishing responsibilities and assigning owners for information security within your organization.

Creating an Information Security Policy to emphasize to employees the importance of protecting personal and confidential data.

Implementing an Incident Response Plan so you can receive, evaluate, and respond to suspected incidents, as well as meet obligations for data subject and regulator notification.

Developing a strategic road map for future framework enhancements.

How Guidehouse Can Help

Whether you need an assessment of a more mature information security program or help with developing an initial framework to start a program, Guidehouse supports clients in assessing and implementing cybersecurity programs based on international standards through our collaborative expertise in compliance, data management, and security.

Guidehouse works with clients to develop best-practice frameworks, providing an understanding and appreciation for identifying and managing cybersecurity risks, and creating policies and procedures that serve as the foundation on which information security programs can grow and scale in the future.

Cybersecurity: Internationally Recognized Standards

- The global standard ISO/IEC 27001:2013 specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization.
- The Cybersecurity Framework from NIST provides best practices for computer security, including information security measures and controls to identify, assess, and manage cyber risk. Currently, organizations in more than 30 countries voluntarily follow NIST.

Contacts

J. Mark Farrar, MSJ, CPA, CFE, CFF
Managing Director, Life Sciences
M +1-404-575-3800
E mark.farrar@guidehouse.com

Stephanie M. Lewko, CFE
Director, Life Sciences
M +1-202-973-2458
E slewko@guidehouse.com

Thomas Hauser, MSJ, CIPM, CIPP/E, IPMA Level A
Director, Life Sciences
M +44-20-7661-7750
E thomas.hauser@guidehouse.com

linkedin.com/company/guidehouse

twitter.com/guidehouse

guidehouse.com

About Guidehouse

Guidehouse is a leading global provider of consulting services to the public and commercial markets with broad capabilities in management, technology, and risk consulting. We help clients address their toughest challenges with a focus on markets and clients facing transformational change, technology-driven innovation and significant regulatory pressure. Across a range of advisory, consulting, outsourcing, and technology/analytics services, we help clients create scalable, innovative solutions that prepare them for future growth and success. Headquartered in Washington DC, the company has more than 7,000 professionals in more than 50 locations. Guidehouse is a Veritas Capital portfolio company, led by seasoned professionals with proven and diverse expertise in traditional and emerging technologies, markets, and agenda-setting issues driving national and global economies. For more information, please visit: www.guidehouse.com.

Guidehouse Inc. f/k/a Navigant Consulting, Inc. ("Guidehouse" or "Navigant") is not a certified public accounting or audit firm. Navigant does not provide audit, attest, or public accounting services. See navigant.com/about/legal for a complete listing of private investigator licenses.

This publication is provided by Navigant for informational purposes only and does not constitute consulting services or tax or legal advice. This publication may be used only as expressly permitted by license from Navigant and may not otherwise be reproduced, recorded, photocopied, distributed, displayed, modified, extracted, accessed, or used without the express written permission of Navigant.

Guidehouse