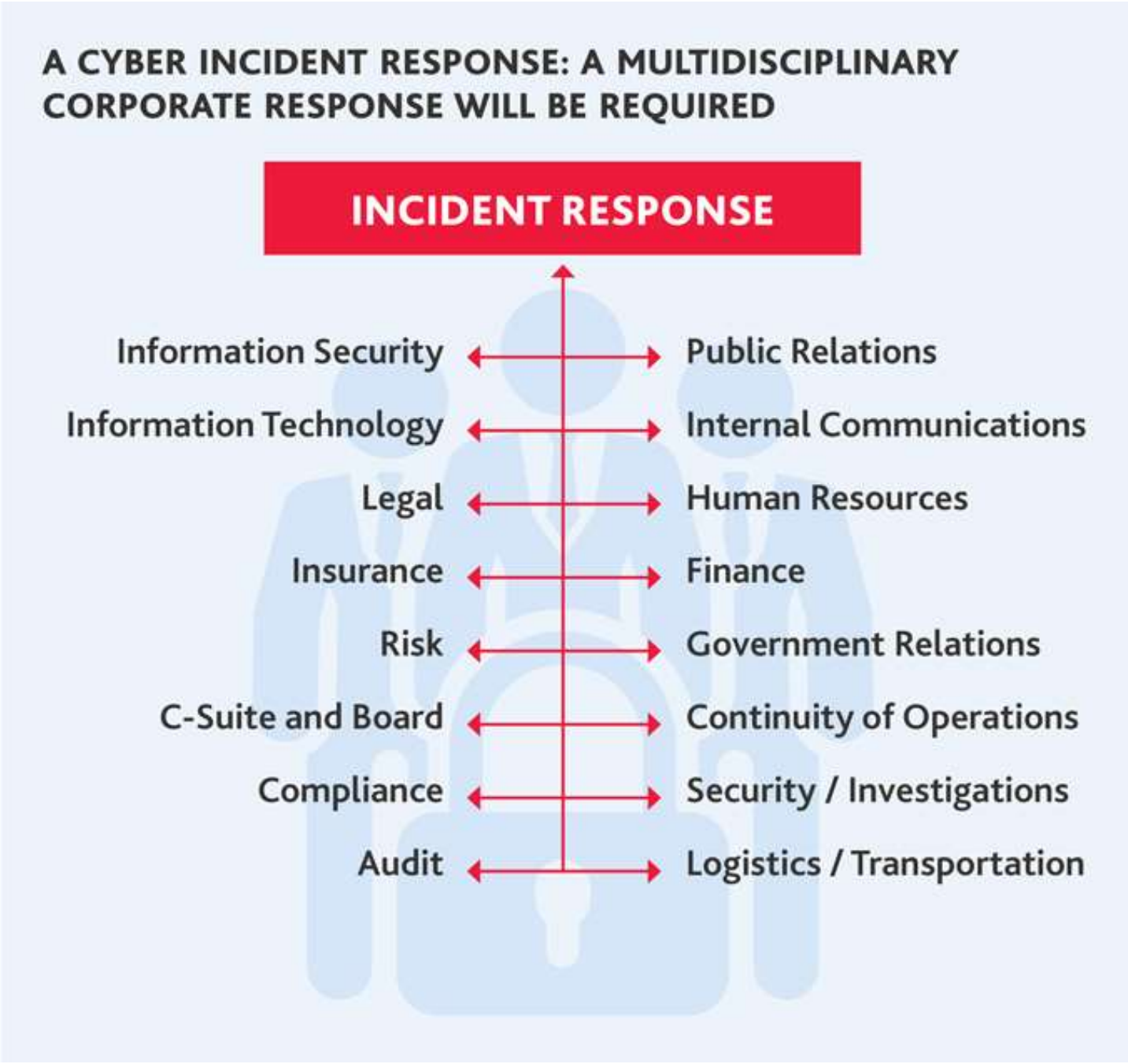
How Hospitals Can Improve Cyber-Response by Forging a Stronger Relationship Between Counsel & IT

by George Socha and Ian Lewis

This article originally appeared in the of *BDO Knows Healthcare* Spring 2017 newsletter. Reprinted with permission.

Fostering a better working relationship between corporate counsel and information technology staff can be a tricky dance, but it's one that's essential in today's digital world—where a cyber incident can put a major dent in a hospital's reputation and assets with a single keystroke.



Hospitals should keep several key components in mind.

There are three "must haves" for hospitals before an incident occurs.

Too often, hospitals may have basic cyber defenses in place but don't prepare a coordinated response plan until after an incident occurs, leaving their assets—and their patients—at risk. Prior to an attack, hospitals should review internal controls, and legal and insurance considerations. They should also instate a comprehensive cyber risk management strategy that outlines the response structure, governance, policies and procedures, and training, as well as:

- **A crisis communications plan** that includes both internal and external communications and is aligned with an existing enterprise risk management (ERM) framework;
- **A comprehensive coordinated incident response plan** that is regularly tested and takes into consideration hospital network processes and responsibilities of individuals; and
- **Post-breach digital forensics and cyber investigations** to identify the cause of the breach and implement remediation measures for affected areas of the hospital's system. Other post-breach activities should include system repair and data recovery.

To execute these components successfully, responsible team members should be designated for each, ensuring lateral communication and coordinated action. Tabletop exercises should also be conducted with all key stakeholders so everyone knows their individual role in the event of an incident.

Communication between all enterprise stakeholders is key both in advance of and in response to a cyber-attack. And a multidisciplinary corporate response is crucial to best avoid and quickly recover from a cyber-attack. To effectively respond to a potential incident, relevant stakeholders should have a defined process in place to act swiftly. In most cases, stakeholders should include those responsible for information technology, legal, risk, insurance, compliance, audit, communications, human resources, finance and government relations, along with the C-suite and the board of directors.

While timely data breach notification is critical to preserving relationships with patients and network partners, hospitals should be cautious about launching external communications too quickly after a breach to avoid spreading misinformation. Response teams should first work with their IT and security professionals to pinpoint the source of the incident so vulnerabilities can be patched, internal controls strengthened and messages aligned.

A good in-house lawyer should bridge the divide between the IT and business worlds.

Many people look to the general counsel or legal team to be the voice of reason. However, to be that voice in the wake of a cyber incident, an in-house lawyer must know enough about the technology involved to not only understand industry language, but also to communicate about it to the relevant stakeholders. One emerging practice is to add an IT professional to a hospital's legal department to serve as a dedicated liaison between the two. However, the best way to bridge the divide between IT and legal is to be the lawyer who already knows and is trusted by the IT security team.

The cost of a cyber incident is two-fold.

In the immediate aftermath of an incident, hospitals suffer from reputational and financial fallout due to the loss of intellectual property or records fundamental to viability, interruption costs and a loss of revenue. Additionally, several sustained opportunity costs come into play, including: higher cyber insurance premiums, IT infrastructure restoration costs, cybersecurity costs related to securing the network and its data, and regulatory scrutiny or litigation.

Lagging data governance is sometimes the greatest threat to cybersecurity.

One of the greatest risks to a hospital's cybersecurity is poor data management hygiene. Often it is enterprise insiders with permissions to access key information who steal from their employers. It's important to clearly delineate who has permissions to what information—and to regularly update those permissions as the hospital and its employees change, applying the principle of least privilege.

There are two types of hospitals—those who have been hacked and those who are going to be hacked.

This reality underscores the importance of cybersecurity controls.

While IT security professionals help to thwart would-be attackers, potential red flags can quickly multiply, and

potential breaches can be missed. A hospital's legal team should approach cybersecurity knowing there are vulnerabilities that will fall through the cracks. Even with the best preventive measures in place, social engineering alone can take down an entire firewall. It is for this reason, among others, that early detection and a well-planned, rapid response may ultimately prove most valuable when it comes to a hospital's cybersecurity.

George Socha is a managing director in BDO Consulting's Forensic Technology Services practice and co-founder of the Electronic Discovery and Information Governance Reference Models. He can be reached at gsocha@bdo.com.

Ian Lewis is a director in BDO Consulting's Technology Advisory Services practice. He can be reached at ilewis@bdo.com.