HealthManagement.org
Promoting Management and Leadership

Do you do these 7 things to get C-suite behind cyber-security?

As the **healthcare C-suite** reshuffles its priorities and the responsibilities of its members, technology chiefs in a healthcare organisation can have a hard time getting their voice heard.

While the role of the CIO and CISO continues to take a more central position in decision-making, there can still sometimes be gaps in understanding about the importance of their contribution from the people who hold the purse strings.

You might also like: ***Fighting cyber threats with a global community***

One area where technology heads struggle to convince C-suite colleagues of the need for **investment and action** is that of cyber security.

This is in spite of the growing number of cyber attacks on healthcare systems where patient data, a precious digital commodity, is threatened.

Both the **financial and reputational cost** of such incidents can be high and have a severe impact on operations.

With so many pressures and priorities on the table, many C-suite leaders overlook the importance of cyber security largely because of a **lack of tech savvy.**

Deloitte Insights has released a report homing in on how CIOs and CISOs can impress upon C-suite executives the necessity of investing in cyber security.

The global business advisory service interviewed 18 biopharma, health plans, medical device manufacturers, and health systems C-level executives for an overview on what communication strategies are working and where the challenges lie.

Deloitte pinpointed the following seven strategies that **CIOs/ CISOs can leverage to communicate their message on cyber security:**

Engage leadership and build trust through dialogue: provide cyber threats and vulnerabilities facts and figures on which executives can make solid decisions.

Make it relatable through storytelling: use face-to-face time effectively by illustrating the situation in a way that's engaging, crisp and clear.

Underline the "cyber-everywhere" mentality: drive home that expansion on the cloud with patient apps means cyber security is more critical.

Emphasise cooperation amongst healthcare organisations on cyber security: describe how cyber threat cultivates cooperation, not competition.

Use metrics to illustrate risks and how they link back to organisation: stipulate that cyber security is a business decision and not solely a technical move.

Be ready to defend cyber security investment: not all cyber threats come with an immediate tangible financial cost so be prepared to explain secondary impact on data destruction, credit-rating and loss of intellectual property.

Champion innovation in recruitment models: being open to unorthodox cyber security hiring can mean a stronger, more versatile team.

Source: Deloitte Insights

Image credit: Pixabay

Published on : Thu, 30 May 2019