HealthManagement
Promoting Management and Leadership

5 steps to prepare for a cyber-attack

"Being prepared is preventive medicine." Putting this principle in practice can help you stay calm and composed even during times of crisis, such as a cyber emergency.

Cyberattacks have become more common and pernicious. It would be wise for healthcare organisations to prepare for one in advance so they aren't scrambling last minute and make matters worse. A cyber emergency management plan need not come in thick three-ring binders. They pretend to be comprehensive but are usually ineffective because no one reads them, says Eden Gillott, president of a strategic communications and reputation management firm. She is the author of A Board Member's Guide to Crisis PR.

Gillott says a concise plan based on these "simple concepts" could help make a cyber crisis less terrifying.

1) Build a team. Select people who are good at dealing with a crisis. It only gets worse during an actual crisis, and you need your strongest people watching your back. Besides in-house staff, you'll need: an outside attorney who specialises in privacy and cybersecurity (laws and requirements are constantly evolving); an IT security consultant (your own IT department may not be as familiar or comfortable dealing with such matters); and an insurance agent who's familiar with your cyber insurance policy.

2) Create an action plan. You really can't know what to say until an event happens. But you can understand the broad rules and messaging: Reassure. Don't alarm. Never let the public see you're nervous. Demonstrate you're in control by avoiding cookie-cutter statements – which are perceived as insincere and weak.

3) Practise, practise, practise. Don't create a plan, then forget about it. To stay fresh and effective, you must rehearse. Periodic tabletop exercises are best, Gillott says, but they too often slip by the wayside. At the very least, plans should be reviewed as team members come and go and when major operational changes occur.

4) Communicate with purpose. Before taking any actions or making any comments, you must know what you want to achieve. Where you want to go. Remember that the sooner you communicate, the better – even if the scope of the breach doesn't mandate disclosure. If the media breaks the story and you've said nothing, it'll look like you were covering up. If you're hit with ransomware that causes your hospital's operations to go down, the media will be all over the chaos. Reporters love sound bites. So be concise. Stick to two or three talking points that are most important to you. Don't stray beyond them.

5) Employees: your best friend – or worst enemy. Even though they aren't authorised, employees often can't help speaking to the media. Therefore, you should keep your employees informed. The more accurate information they have, the more reassured they will be and less likely they will repeat rumours. Remind them that all media enquiries should be directed to your designated spokesperson. That may not stop all leaks, but it should plug most.

Source: Healthcare Business & Technology

Image Credit: Pixabay

Published on : Tue, 9 Oct 2018