Good Governance in times of 2020 crisis

COVID-19
9 April 2020

Good Governance Institute

Is your board asking the right cybersecurity questions?

Today's guest post has been written by Andrew Fitzmaurice, CEO of Templar Executives, a cybersecurity advisory services and solutions company operating across the public and private sectors.

As the coronavirus pandemic unfolds, NHS organisations are making increasing use of digitally-enabled capability to enable delivery of patient care. Digital solutions can also help to reduce the risk of working in close proximity with others. Some are accelerating investment in solutions such as video consultation, others are providing more staff with facilities for home-working.

Most people recognise their role and responsibilities in keeping their organisations and related data safe. Unfortunately, there are also those who see the pandemic as an opportunity to mount new scams and attacks to exploit the unwary.

This includes the healthcare sector – despite claims by some criminal groups that they will not attack healthcare at this time, overall ransomware attacks are estimated to have risen by 36% this quarter.

Health-related organisations in the US and the Czech Republic as well as the UK have been affected during the past month. Vulnerabilities will increase as networks of devices and people become more dispersed.

Below are some key cybersecurity questions for NHS boards to consider so that their organisations remain robust and resilient through the pandemic and beyond.

1. How do any new digital measures sit against the **risk appetite** for your organisation? Moving to new digital platforms potentially brings new risks and vulnerabilities. As the workforce disperses, what is their understanding of what you as a board consider to be acceptable risk?

2. What support is your organisation providing to **help staff work appropriately**? For example, are they being provided with any IG awareness before they are given laptops? Are the laptops encrypted? Are they equipped with virtual private networks (VPNs) to enable secure use of Wi-Fi? Do staff know how to use them? Do they have robust passwords?

"Ransomware attacks are estimated to have risen by 36% this quarter"

3. Healthcare staff at the front line will be under severe, and growing, pressure. This is when mistakes are easily made, for example inadvertently clicking a malicious link in an email. Such errors can let in malware that can immobilise whole networks. What steps are your communications team taking to support **ongoing awareness of the cybersecurity risk**?

4. What advice is being provided for staff who might have to fall back on **personal mobile devices**? Do you have a clear policy for the use of apps and social media? Are staff aware of the policy and do they know where to find it?

5. Sensitive data includes corporate as well as personal information. Patient data requires the same protection whether it is written, digital, image or voice and however it is shared. Do staff understand that, while the pandemic requires flexibility, **information must still be handled within the law**?

6. New ways of working may place new strains on your IT system. And not all staff will be confident working from home. **Demands on the IT team and helpdesk** are likely to increase. Have you considered staggered hours for staff logging on remotely? What other guidance can you provide to ensure your IT team does not become overwhelmed? Might there be opportunities for burden-sharing with other local NHS IT teams?

7. Are you confident that the systems of your **suppliers and providers** are resilient and that they will be able to assure **business continuity** for your organisation?

8. Home/remote working is a new environment for many. Are you encouraging staff to be discreet, **safeguard information** and lock devices when not actively used? Conversely, it can be tempting to work excessive hours – partly due to the crisis, partly due to not being allowed out. What **personal wellbeing** policies and guidance can you offer those working from home? What contingencies do team leaders have in place should anyone fall ill?

9. What can your leadership teams do to **keep all staff feeling involved**? Daily team calls at start and close of play? Use of conferencing capabilities such as Microsoft Office Teams, Skype or Zoom?

10. Do staff know what constitutes a **cybersecurity or information incident**? Do they know where to **report** it?

COVID-19 presents a range of challenges to all organisations and to everybody working for and with them. By ensuring that the above questions are addressed, and by setting the appropriate example themselves, NHS board leaders can help your organisation and your staff to weather the immediate risks.

Good habits embedded now, under these exceptional circumstances, will also pay dividends for the resilience of your organisation into the future.

GGI would like to thank Andrew Fitzmaurice for today's update. We are publishing this article as part of our work to share knowledge related to COVID-19. GGI has no commercial connection to Templar Executives and has received no funding from the company.

As ever, GGI is interested to hear your perspective and experiences on the COVID-19 crisis. If you have any questions or comments about this briefing, please call us on 07732 681120 or email **advice@good-governance.org.uk** and we will aim to respond within 24 hours.