

The healthcare sector is among the top target sectors that faces major security risks from a number of threat agents that take advantage of emerging cyber threats. In this survey, we aim to assess how you experts in the healthcare sector view the cybersecurity nature of the sector. By doing so, we aim to identify emerging cyber threats, how you percieve threat agents across the sector and your risk management plans. In particular, we aim to assess how you perceive state-sponsored attackers, and if the current risks assessments methods you apply take into consideration such highly skilled and well-funded attackers. Furthermore, due to the elusiveness of post-breach data, we aim at gaining an insight into what risks and harms patients face when cyber-attackers at different levels compromise the sector.

---

**In your opinion, what is the general state of cybersecurity in the healthcare sector?**

- ☐ L1 - Very weak
- ☐ L2 - Weak
- ☐ L3 - Strong
- ☐ L4 - Very strong
- ☐ L5 - Constantly improving
- ☐ I do not know

**In comparison to other critical sectors (for example, finance, energy, etc), what is the state of cybersecurity in the healthcare sector?**

- ☐ L1 - Very weak
- ☐ L2 - Weak
- ☐ L3 - Strong
- ☐ L4 - Very strong
- ☐ L5 - Constantly improving
- ☐ I do not know

**What emerging security threats are there in the sector that can disrupt a healthcare's organization ability to offer required patient care?**

In case of a data breach, does your incident management plan integrate incident response and security operations?

- ☐ Yes
- ☐ No
- ☐ I don't know

The healthcare compliance environment is growing even more complex. Could you list some of the popular standards /policies that are currently in place and are being used across healthcare organizations?

With the ever-changing threat landscape and given the current geopolitics, do you think that healthcare organizations are prone to state-sponsored cyber-attacks?

- ☐ Yes
- ☐ No
- ☐ Maybe
- ☐ I do not know

Do you think healthcare organizations are prepared against state-sponsored attackers?

- ☐ Yes
- ☐ No
- ☐ I do not know

What is the first point of compromise for most major security incidents in healthcare?

- ☐ Unpatched vulnerabilities
- ☐ Zero-day vulnerabilities
- ☐ Social engineering
- ☐ Human (staff)
- ☐ I do not know

In comparison, could an attack from a non-state-sponsored attacker be compared to that of state-sponsored attacker?

- ☐ Yes
- ☐ No
- ☐ I do not know



Do you think it is hard to implement information security and privacy goals at the same time?

- ☐ Yes
- ☐ No
- ☐ I do not know

Do you think that when implementing information security and privacy goals, there is a trade-off between security and privacy goals?

- ☐ Yes
- ☐ No
- ☐ I do not know

In the event of a low-level non-state sponsored cyber-attack, what privacy harms are likely to affect patient(s)?

- ☐ Physical harm
- ☐ Financial harm
- ☐ Psychological harm
- ☐ Reputational harm
- ☐ Societal harm
- ☐ None of the above
- ☐ I do not know

In the event of a state sponsored cyber-attack, what privacy harms are likely to affect patient(s)?

- ☐ Physical harm
- ☐ Financial harm
- ☐ Psychological harm
- ☐ Reputational harm
- ☐ Societal harm
- ☐ None of the above
- ☐ I do not know

Have you had an incident where patient(s) have reported privacy harms as a result of a healthcare data breach?

- ☐ Yes
- ☐ No
- ☐ I do not know

Could you tick which privacy harms tend to affect patients after a healthcare data breach?

- ☐ Physical harm
- ☐ Financial harm
- ☐ Psychological harm
- ☐ Reputational harm
- ☐ I do not know

When evaluating risks, two key risk analyses can be used during a risk management process: qualitative and quantitative. Between the two, which do you apply?

- ☐ Qualitative
- ☐ Quantitative
- ☐ Both
- ☐ I do not know

Do you have an impact assessment tool that can allow experts to quantify privacy harms to patients after a post-data breach?

- ☐ Yes
- ☐ No
- ☐ I do not know

Do you perform risk assessment before, during and after the implementation of a health information system within a health information system infrastructure?

- ☐ Yes
- ☐ No
- ☐ I do not know

Does the risk assessment and controls used in your organization take into consideration skills and motivations of state-sponsored attackers?

- ☐ Yes
- ☐ No
- ☐ I do not know



Do the risk treatments have adverse implications for quality of care?

- ☐ Yes
- ☐ No
- ☐ Sometimes