5 Security questions your board will ask

How secure are we? Why do we need more money for security, when we just approved X last year? What do you mean we've had four incidents? I thought you had everything under control.

Source: pixabay.com

Chances are, most security and risk leaders have heard these questions, possibly multiple times, from their boards of directors. But the problem is that these questions are unanswerable. They are driven by exaggerated, incomplete or contradictory public information, and are a distraction from more relevant questions.

Gartner estimates that by 2020, 100% of large enterprises will be asked to report to their boards of directors on cybersecurity and technology risk at least once a year. Boards today are more informed about security risk, with just 15% of directors reporting to their boards have very little to no knowledge of cyber risk, down from 22% in 2015.

Further, boards are using the increased focus on cybersecurity to guide business decisions. In 2019, a Gartner survey of security and risk leaders found that four of every five respondents noted that risk influences decisions made at the board level.

Additionally, security leaders need to be able to give the board something that they care about and that is meaningful to them. Beyond individual passions and concerns, boards collectively generally care about three things:

- **Revenue/mission**: Operating or non-operating income and enhancing non-revenue mission objectives
- **Cost**: Future cost avoidance and immediate decrease in operating expenses

- **Risk**: Financial, market, regulatory compliance and security, innovation, brand, and reputation

“As board members realise how critical security and risk management is, they are asking leaders more complex and nuanced questions,” says Sam Olyaei, director analyst at Gartner. “Boards today are becoming more informed and more prepared to challenge the effectiveness of their companies’ programs.”

Most board questions can be categorised into five areas.

1. The trade-off question

What it sounds like: Are we 100% secure? Are you sure?

Why it’s asked: Questions like this are often asked by board members who don’t truly understand security and the impact on the business. It’s impossible to be 100% secure or protected. The CISO’s role is to identify the highest-risk areas and allocate finite resources toward managing them based on business appetite.

How to respond: Begin with something like: “Considering the ever-evolving nature of the threat landscape, it’s impossible to eliminate all sources of information risk. My role is to implement controls to manage the risk. As our business grows, we have to continually reassess how much risk is appropriate. Our goal is to build a sustainable program that balances the need to protect against the need to run our business.”

2. The landscape question

What it sounds like: How bad is it out there? What about what happened at X company? How are we compared to others?

Why it’s asked: Board members will come across threat reports, articles, blogs and regulatory pressure to understand risks. They will always ask about what others are doing, especially peer organisations. They want to know what the “weather” looks like and how they compare to others.

How to respond: Avoid guessing at the root cause of a security issue at a different company by saying, “I don’t want to speculate on the incident at Company XYZ until more information is available, but I’ll be happy to follow up with you when I know more.” Consider discussing a series of broader security responses such as identifying a similar weakness and how it’s being fixed or updating business continuity plans.

3. The risk question

What it sounds like: Do we know what our risks are? What keeps you up at night?

What it’s asked: The board knows that accepting risk is a choice (if they don’t, that’s a challenge you need to solve). They want to know that the company’s risks are being handled. CISOs should be prepared to explain the organisation’s risk tolerance to defend risk management decisions.

How to respond: Explain the business impact of risk management decisions and ensure that your positions are supported by evidence. The second part is vital because boards are making decisions based on risk tolerance. Any risks outside the tolerance level requires a remedy to bring them within tolerance. This doesn’t necessarily require dramatic changes in short periods of time; beware of overreacting. The board will be seeking assurances that material risks are being adequately managed, and that subtle, long-term approaches may be appropriate in some instances.

4. The performance question

What it sounds like: Are we appropriately allocating resources? Are we spending enough? Why are we spending so much?

Why it's asked: The board will want reassurance that security and risk management leaders are not standing still. Board members will want to know about metrics and ROI.

How to respond: Use a balanced scorecard approach in which the top layer expresses business aspirations and the performance of the organisation against those aspirations is illustrated using a simple traffic-light mechanism. As much as possible, explain aspirations in terms of business performance, not technology. Performance is underpinned by a series of security measurements that are evaluated using a set of objective criteria.

5. The incident question

What it sounds like: How did this happen? I thought you had this under control? What went wrong?

Why it's asked: This is asked when an incident or event has occurred and the board either already knows or the CISO is informing them of it.

How to respond: An incident is inevitable, so be factual. Share what you know and what you are doing to find out anything you don't currently know. In short, acknowledge the incident, provide details on business impact, outline weaknesses or gaps that need to be worked out and provide a mitigation plan. Be cautious not to endorse one option as the ultimate choice when in front of the board. The responsibility for oversight of security and risk remains with the security leader, but the accountability has to always be defined at the board/executive level.