Seven Questions Board Members Should Ask About Insider Threats

While board members may not be the first line of defense against insiders trying to do damage, board members are responsible for helping make the right decisions to reduce insider risk. To that end, they must first understand the right questions to ask their cybersecurity leaders in order to provide the resources and tools needed to build an effective program.

1 Is your insider threat strategy and program aligned with the objectives of the business continuity team?

Cybersecurity is a business continuity issue. As such, cyber leaders should be in continuous communication with the business continuity team and understand which assets the business continuity team would protect first if a natural disaster hit. Chances are those are the same assets cyber leaders want to protect first as well.

2 Are all key stakeholders aligned and engaged to address insider threat?

There are always natural team members such as IT and Security engaged in addressing insider threat. However, to create a successful and robust program, it's critical to broaden beyond IT and Security. Proper governance requires a holistic approach with team members from other parts of the organization including Legal, Human Resources, R&D, and the Audit team.

3 Does your corporate governance address the identification and management of critical data and infrastructure assets?

Identifying and gaining alignment around which assets the broader organization deems critical and should be protected is key to driving a sound security strategy. Management of whom and when people access infrastructure, data, and critical IP provides the first level of control. Creating a repeatable and straightforward audit process enables ongoing certification maintenance and ensures regulatory compliance.

4 How do you determine who can access critical data, and how do you control that access?

Depending on their role, certain individuals may require visibility and access to sensitive data across various functional areas. It can be challenging for security to create internal controls for these privileged users while simultaneously empowering their business needs and managing potential risk, including regulatory and federal laws that vary by region and country.

5 Who is responsible for responding to insider threat investigations?

It's important to take a holistic approach to insider threat investigations, as they often involve actions and actors that are not malicious in intent. It should include practices which remove bias, follow proper governance, are compliant with federal laws, and are repeatable and auditable.

6 How automated is your insider threat governance?

There are tools available that move beyond mere incident detection to maintain security and improve situational awareness. These tools include guided prompts and coaching in real-time that enforce proper cyber-policies for an end user. Other tools can detect and block non-compliant policy activities—preventing breaches—and create behavioral narratives across privileged users, providing easy to review data sources that can help mitigate risk quickly.

7 Can you take proactive measures to help prevent incidents?

Many of today's security solutions take an antiquated approach, which involves simple incident detection. However, it's a holistic picture of human behavior and actions that best provides early indication of potential risk—benefitting the prosperity of a business and the safety of its people. Partnering with a provider who offers modern security tools that inform and investigate intent and provide insight into actors, versus simply viewing systems, can up-level how investigations and governance function.

FORCEPOINT