RESOURCES

Technology risk: 12 questions for the board

A short checklist to gauge, in a few minutes, your institution's maturity in IT governance, cybersecurity and resilience. Tick the questions you can answer today with evidence.

Governance

- [ ] Who is responsible for information security, and who do they report to?
- [ ] Does the board receive a report on technology risk and cybersecurity at least once a year?
- [ ] Is there an up-to-date inventory of systems, critical data and vendors?

Protection

- [ ] Are privileged and remote access protected with multi-factor authentication?
- [ ] When was the last vulnerability assessment or penetration test, and were the findings fixed?
- [ ] Do staff receive regular training on phishing and social engineering?

Resilience

- [ ] Are there immutable backups or backups isolated from the production network?
- [ ] When was a full recovery last tested, and how long did it take?
- [ ] Does the continuity plan cover the outage of a critical vendor?

Third parties and incidents

- [ ] Do contracts with critical vendors include audit rights, SLAs and an exit strategy?
- [ ] Is there an incident response plan with defined roles, rehearsed with senior management?
- [ ] Is it clear when and how an incident is reported to the regulator and to clients?

> If any answer is “I don't know”, that is a good starting point for a conversation.

securetech.com.pa · info@securetech.com.pa