

5

Leadership Moves

to Drive Sustainable Security for Compliance

Regulation Lens: Why Now?

Evolving regulations such as **DORA**, **NIS2**, **eIDAS**, the **Cyber Resilience Act**, **PCI DSS 4.0**, **FIPS**, and **Common Criteria** have a global impact and are transforming cybersecurity from a technical function into a strategic mandate.



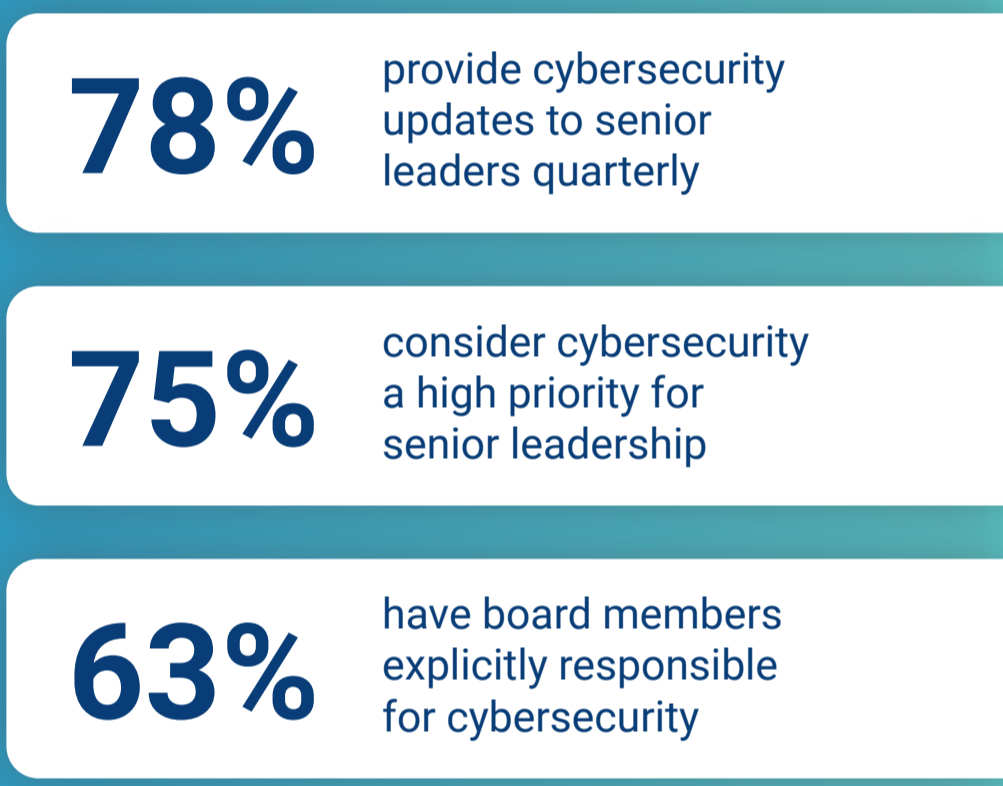
Trust Under Pressure

Confidence in core systems is low while cyber threats continue to rise. **Digital trust is under strain and many organisations are feeling exposed.**



Cyber Moves to the Boardroom

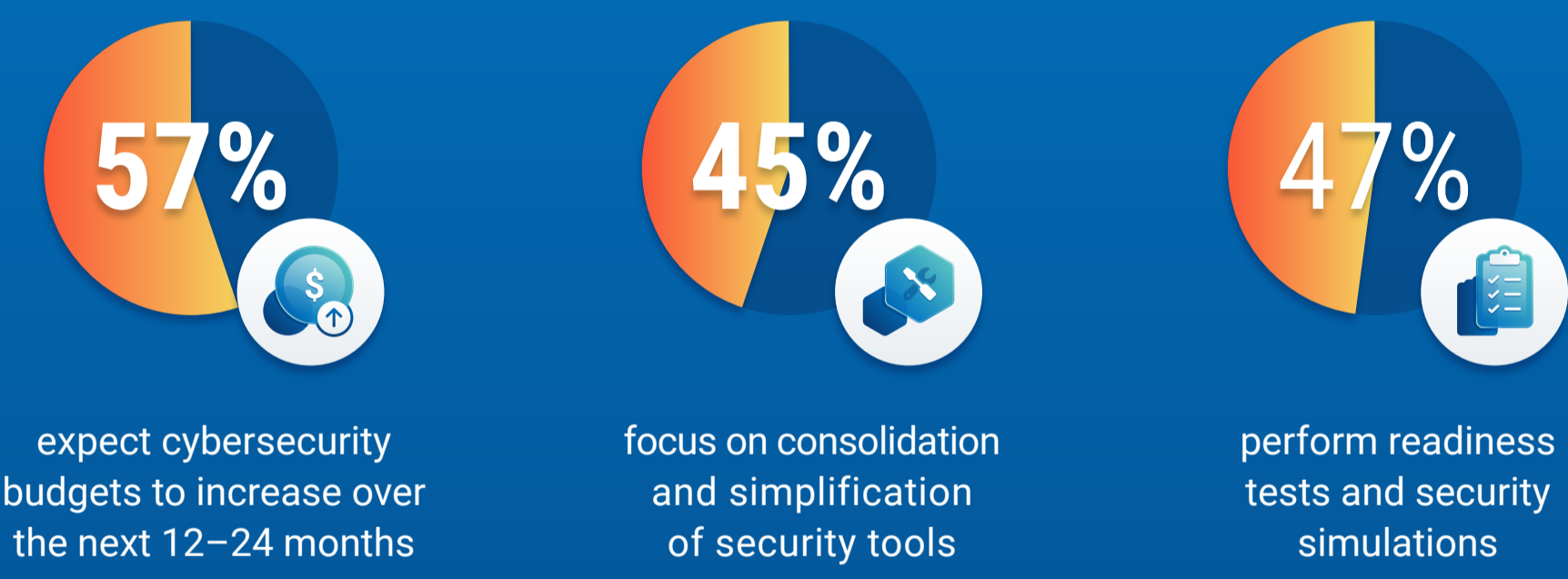
Cybersecurity is a strategic leadership issue, not just an IT line item.



Leadership teams and board members are now responsible/accountable for addressing cyber risk.

Strategic Priorities & Investment

Leaders are increasing budgets, simplifying security toolsets, and strengthening resilience.



A centralised compliance framework is fast becoming the foundation for strategic security alignment. The emphasis is on efficiency, preparedness and human centric defense.

Compliance Builds Confidence

Cybersecurity and compliance strategies deliver business value.



The business case for digital trust has never been clearer.

Compliance by Design

A unified compliance framework is key to long-term digital trust.

Discover how security and compliance leaders are managing compliance and digital trust. **Explore how DigiCert helps support your [regulatory compliance journey here.](#)**