

5 Initiatives to Grow a Cybersecurity Program

Move from scattered security activity to a deliberate program that leaders can fund, teams can execute and the business can measure.



THE FIVE MOVES

- 01** Establish a credible baseline
- 02** Build a risk-led roadmap
- 03** Strengthen core protections
- 04** Rehearse response and recovery
- 05** Measure what leaders can use



THE EXECUTIVE BRIEF

A growing security program needs more than a longer list of tools. It needs a repeatable way to understand exposure, choose investments, protect critical operations and show whether the work is reducing risk. These five initiatives create that operating rhythm.

1

Establish a credible baseline

Start with the systems, data, vendors and processes that keep the business running. Assess the security controls around those assets and record gaps in a way owners can validate. A baseline gives the program a shared fact base; it also prevents the loudest issue of the week from setting every priority.

Ask: Which business service would cause the greatest disruption if it failed?

2

Build a risk-led roadmap

Translate findings into a sequenced plan with owners, dependencies, costs and expected risk reduction. Separate urgent exposures from foundational improvements. A roadmap should make tradeoffs visible to executives and allow teams to revisit them as the business changes.

Ask: Which investments reduce the most consequential exposure first?

3

Strengthen core protections

Focus on the foundations that support many parts of the business: identity and access, secure configuration, data protection, cloud controls, vulnerability management and third-party oversight. Validate that controls work in the real environment rather than assuming deployment equals effectiveness.

Ask: Where is a basic control inconsistent across critical systems?

THE THROUGH LINE

Treat the five initiatives as a cycle. New business priorities and new threats should change the roadmap, tests and measures over time.



FROM INSIGHT TO ACTION

A useful program connects the control environment to operational decisions. The aim is to make protection stronger while improving the organization's ability to detect, respond and recover.

4

Rehearse response and recovery

Plans become useful when people practice them. Run scenarios that involve security, operations, legal, communications and executive leadership. Test not only technical containment but decision authority, customer impact, evidence handling and restoration of essential services.

Ask: Who decides whether to shut down an affected service?

5

Measure what leaders can use

Report a small set of indicators linked to risk and readiness: critical exposure remediation, coverage of priority assets, time to detect and contain, exercise findings and recovery capability. Explain what each measure means for the business and what decision it calls for.

Ask: What would leadership do differently after seeing this metric?

START THE CONVERSATION

Choose one critical service. Map its dependencies and leading risks, assign improvement owners and schedule a response exercise. Bring the decisions to leadership.



DAN DUFFY

Cybersecurity Practice Lead

Dan leads cybersecurity executive search and security solutions at Consulting Solutions. His work connects leadership requirements with the expertise and services organizations need to strengthen their programs.

FURTHER READING

NIST Cybersecurity Framework 2.0: nist.gov/cyberframework | CISA Cross-Sector Cybersecurity Performance Goals: cisa.gov/cybersecurity-performance-goals

Explore cybersecurity solutions and specialized talent

consultingsolutions.com