

# SECURITY PROGRAM ASSESSMENT & ROAD MAP DEVELOPMENT

## Gauge Your Cybersecurity Program to Improve Your Security Posture

Tangible Security's Security Program Assessment **measures the maturity** of your security program against industry standards and delivers actionable recommendations that will improve your **security posture, close any gaps, reduce risk, and increase your cyber resilience.**

Tangible uses current standards such as NIST, ISO, COBIT or other formats as a starting framework, coupled with our expertise to understand your security program's current state and gaps to determine its capability maturity level.

Tangible will work with you to examine the quality and effectiveness of your program, identify and understand weaknesses and vulnerabilities, and evaluate your readiness to defend and respond to today's cyber threats.

Additionally, Tangible may incorporate a **cyber resilience review (CRR)** as part of the assessment. The CRR is based on DHS CERT standards, and measures incident response management capability.

Tangible also performs a **technical configuration assessment**, to ensure that a sample of the security devices are configured correctly and best able to provide protection when needed.

### Security Program Areas Covered:

- Security Program Strategy and Architecture Governance
- Gap Assessment (based on ISO 27001, NIST, HIPAA, GDPR, PCI DSS, COBIT, or other standard)
- Policies and processes including:
  - Overall Security
  - Access Control
  - Data Protection
  - Vulnerability Management
  - Incident Management
  - Secure System Configuration
  - Configuration Control
  - Wireless Use
  - Security Reporting and Metrics
  - Security Awareness Training
- Cyber Resilience Review (based on DHS CERT standards for IR)



### Quick Glance:

- WHO:** Cybersecurity leaders and managers
- WHAT:** Assess the quality / effectiveness of your security program
- WHY:** Improve your security posture and close gaps in the face of increasing threats

Credential theft, social attacks, and errors cause

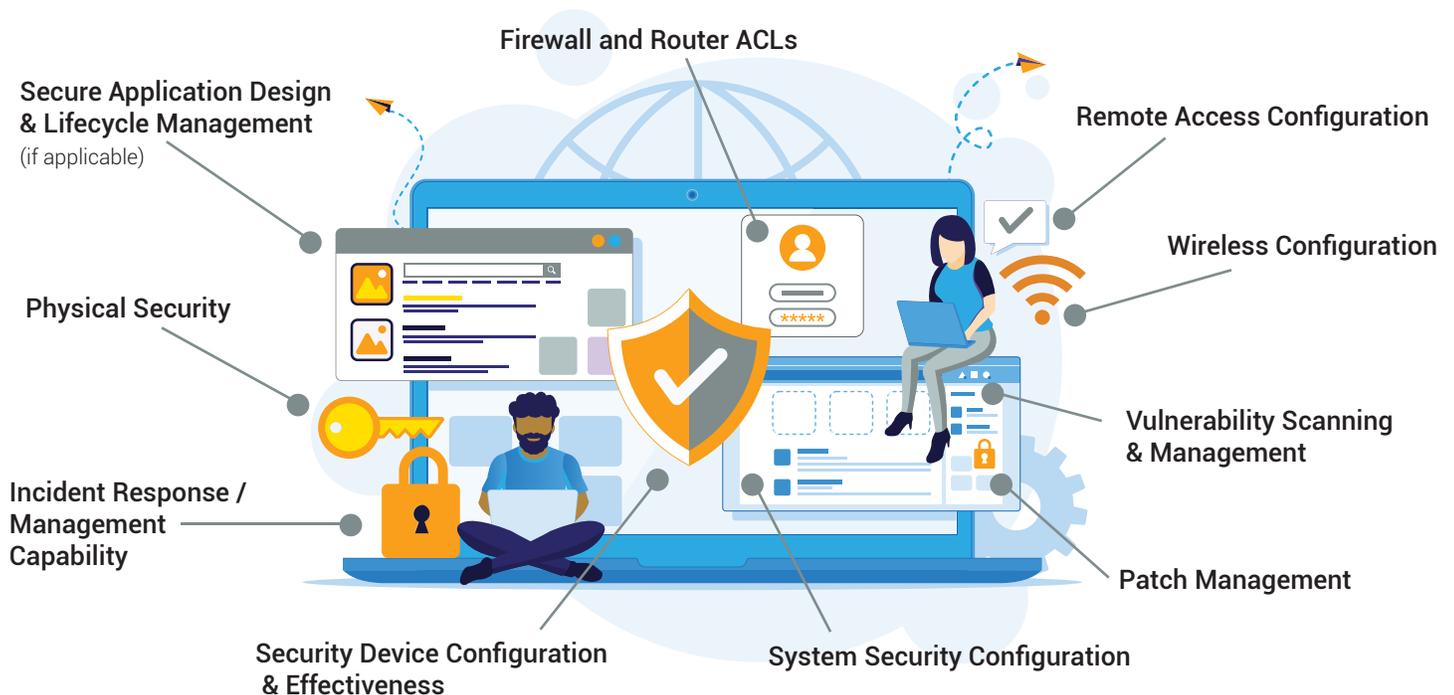
**2/3**  
of breaches  
in cyber attacks

**70%**  
of breaches  
by external actors

## SECURITY PROGRAM ASSESSMENT & ROAD MAP DEVELOPMENT

### Technical Capabilities Reviewed

In addition to policies, the Security Program Assessment reviews the technical capabilities your security posture, identifies capability gaps or configuration errors, and suggest ways and priorities to improve.



### Security Road Map Development

Tangible Security will build on the findings during the Security Program Assessment and create a Security Road Map, taking into consideration:

- Findings from recent Cybersecurity Assessment
- Findings from the Security Program Assessment
- Your Regulatory and Industry Compliance Requirements
- Your Information Security capability and staffing level
- Your specific business goals and budget

A security "**Current State**" is established during the assessment. A custom security "**Target State**" will be established during the Security Road Map development that takes into consideration your specific industry and compliance requirements.

The Security Road Map typically outlines a three year **strategic and tactical plan** with recommendations on sequencing and priority for improving the effectiveness of your Security Program's maturity Level over time, and will also provide preliminary budget information for planning purposes.