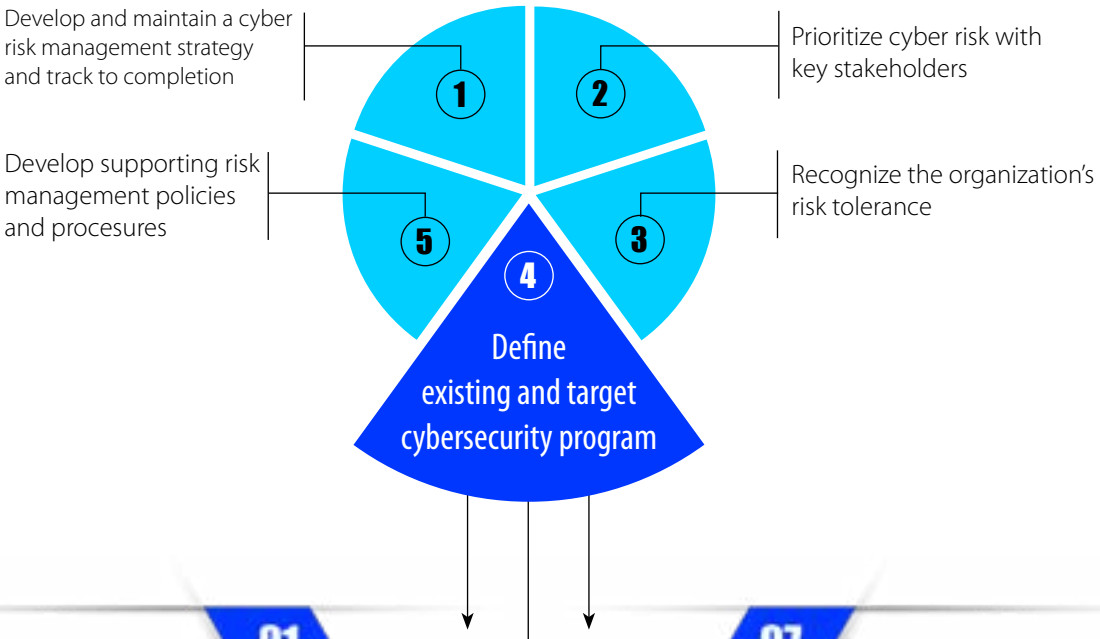
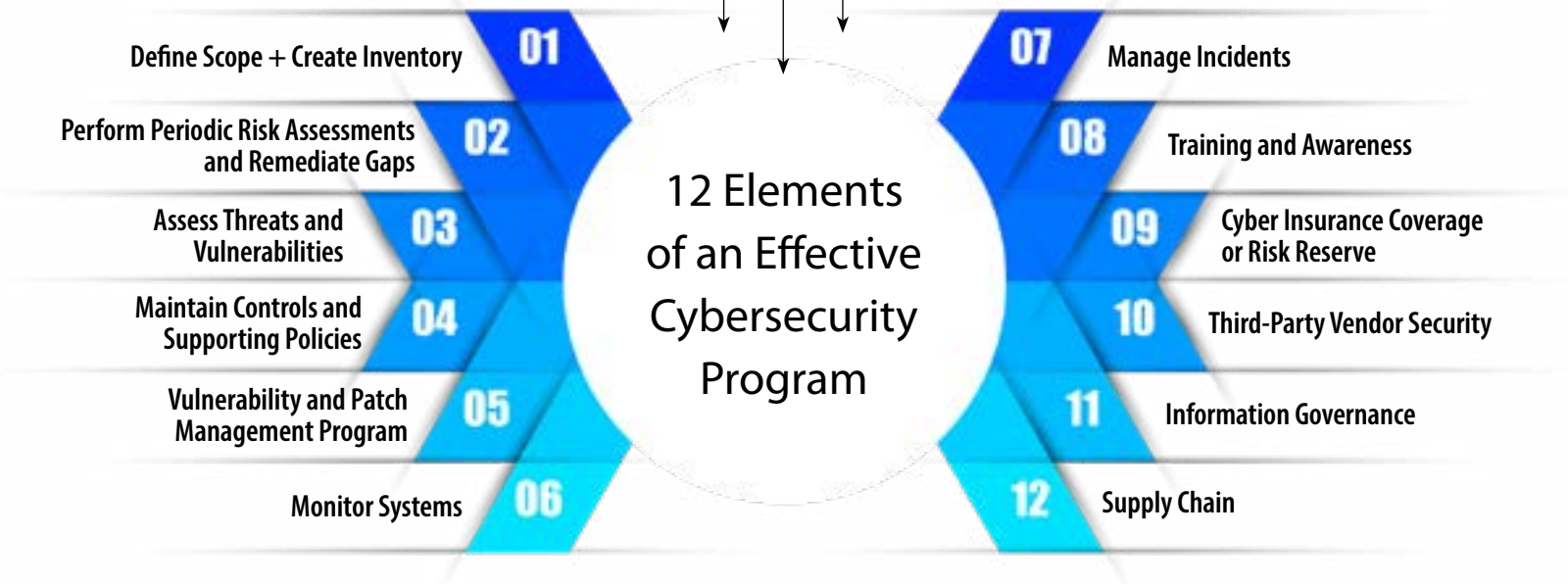
ALSTON & BIRD

# 12 Elements for Effective Cybersecurity

## What Does 'Reasonable Security' Look Like Organizationally?

### Cyber Risk Management Framework



# 12 Elements of an Effective Cybersecurity Program

1. **Define Scope + Create Inventory:** Examine and reexamine the cyber corporate mission, culture, objectives, and priorities, especially in light of any corporate reorganizations, acquisitions, or spinoffs, to appropriately scope the cybersecurity program. Update the inventory of all systems, assets, vendors, data, and functions that support the organization and each process or business unit.

2. **Perform Periodic Risk Assessments and Remediate Gaps:** Perform periodic security risk assessments to assess the maturity of the existing cybersecurity program and identify key gaps. Identify and prioritize the filling of these gaps based on risk, cost, and benefit, and create and execute a plan to remediate these gaps in a timely manner (with documentation and accountability for delays).

3. **Assess Threats and Vulnerabilities:** Understand potential and emerging cyber risks, threats, and vulnerabilities to systems, assets, data, personnel, and functions within the context of the most essential business missions for the organization. Operationalize those risks within the program.

4. **Maintain Controls and Supporting Policies:** Develop physical, technical, and organizational measures and safeguards to defend critical assets and data and to mitigate cybersecurity events, threats, and risks in real-time, automating functions where possible. Implement, for example, multifactor authentication and effective user management processes for privileged accounts, adopting the concept of "least privilege." Create multiple backups at frequent intervals, at different levels (mirror, system, and data dump), and ensure that they are air-gapped (even offline, where feasible) and regularly tested. Segment corporate business functions from manufacturing operations, production systems, intellectual property, and sensitive information where appropriate. Implement security policies and standards that reflect current business practices.

5. **Vulnerability and Patch Management Program:** Develop a plan to continuously assess and track vulnerabilities within the organization's technology assets, coding, and infrastructure. Integrate vulnerability scanning solutions with virtual services and cloud platforms for increased visibility where possible. Apply security patches in a timely manner and ensure the secure configuration of all systems. Perform internal and external vulnerability scans regularly and after any significant network or software changes, and conduct penetration testing of network infrastructure and applications at least annually to help prioritize remediation efforts. For internal development, review secure code review processes, scrum procedures, and associated ticketing.

6. **Monitor Systems:** Develop a network monitoring and alerting strategy and produce supporting policies. Continuously monitor all systems and networks. Analyze logs for unusual activity and establish escalation procedures. Consider enhanced logging and extending log retention and deploying endpoint monitoring and detection (EDR) and network sensor monitoring tools.

7. **Manage Incidents:** Develop and maintain effective incident response, disaster recovery, and continuity processes. Assess requirements for regulatory reporting of cybersecurity incidents. Plan internal and external communications. Test processes and plans through tabletop exercises on a regular basis, preferably under privilege where possible, and document and communicate plans and processes to workforce. Enlist internal audit to help with the routine alerting, restores, and tests.

# 12 Elements of an Effective Cybersecurity Program

8. **Training and Awareness:** Develop general and specialized workforce security policies—keeping in mind any remote workforce—covering applicable and secure use of the organization's systems, assets, and data. Provide continually updated education and training, exercises, and resources to employees. Train and evaluate security team on latest technologies including the effective use of modern toolsets. Develop a cadence for content revisions that reflect recent cyber risks.

9. **Cyber Insurance Coverage or Risk Reserve:** Evaluate adequacy of existing and proposed cyber insurance coverage or risk reserves based on the organization's size, data, complexity, and risk profile. Anticipate periodic renewals and plan for the likely growth of premiums or the need to regularly increase risk reserves.

10. **Third-Party Vendor Security:** Evaluate suppliers and contractors with access to the organization's systems, assets, and data, and create a risk-based due diligence program. Incorporate adequate security requirements including incident notification provisions into contractual agreements based on regulatory requirements, industry standards, and recommended practices. Limit network access and implement ongoing accountability mechanisms for non-conformance (for example, monitoring metrics, scorecarding, SLAs, scanning, etc.).

11. **Information Governance:** Adopt a privacy-by-design approach to reduce the amount and scope of sensitive information maintained on the organization's systems. Where sensitive data is required, protect data at rest and in transit by enforcing encryption and data minimization measures such as tokenization, truncation, and anonymization, wherever feasible or appropriate.

12. **Supply Chain:** Third-party vendor security programs do not typically catch attacks within the software and hardware technical supply chain. Inventory the organization's technology providers and understand how each vendor integrates within the enterprise. Enable anomaly-based threat detection, establish strong access and change management controls, and place limitations on remote VPN connections for system maintenance and upgrade. Specify all communication capabilities and address all known security vulnerabilities in the software/hardware.

**Wash, Rinse and Repeat:** Security programs are under continual reassessment. Consider ongoing budget and the need for continual re-examination and improvements both to the program and throughout the organization. The above processes help systematize and escalate security to ensure the whole organization is on mission.