Completeness in Cybersecurity Defence: Moving Beyond Defence-in-Depth

In cybersecurity, the term “defence-in-depth” has been a longstanding approach, encouraging organisations to layer their defences across multiple fronts. While effective, this concept has limitations as cyber threats evolve and infrastructures become more complex. A more encompassing approach is the notion of “completeness” in cybersecurity defence, which considers the entire breadth of an organisation’s defensive posture—not just layers of protection, but also the maturity and interconnectedness of each element within the security architecture.

In this article, I shall explore why a completeness-based perspective offers a more holistic understanding of cybersecurity risk. I will examine how to measure this completeness and propose a framework for calculating a protection profile based on a completeness score. Finally, I will propose a checklist to help organisations assess, plan, and evaluate their cybersecurity strategy.

Why Completeness Matters in Cybersecurity

Completeness in cybersecurity defence looks at how thoroughly an organisation's cybersecurity architecture covers all potential vulnerabilities and risk vectors, rather than simply layering technologies or security protocols. Here's why it's beneficial:

Holistic Risk Management

Completeness emphasises a well-rounded defence that identifies and mitigates all gaps. Rather than relying on isolated defensive layers, completeness ensures a cohesive approach, covering people, processes, and technology.

Better Adaptability

Modern threats change rapidly, so defences need to adapt in real-time. Completeness helps identify areas where flexibility is required, enabling security measures to evolve with emerging risks.

Enhanced Efficiency and Resource Allocation

Completeness encourages focused investment in critical areas, reducing redundancy and ensuring each defence layer provides unique value rather than overlapping with others unnecessarily.

Stronger Compliance and Governance

By evaluating completeness, organisations can ensure that regulatory and compliance requirements are met without leaving blind spots, which might expose the organisation to non-compliance risks.

Understanding Completeness in Cybersecurity Defence

The concept of completeness in cybersecurity defence requires a holistic view, encompassing various dimensions that together provide a robust defence posture. Completeness is achieved when all critical aspects of an organisation's cybersecurity strategy are adequately covered, integrated, and monitored. Here are the 12 key dimensions, each representing a core component of a well-rounded cybersecurity strategy:

1. **Threat Coverage**: Ensures that known, emerging, and zero-day threats are identified and addressed. This dimension includes threat intelligence, vulnerability management, and monitoring of emerging threats.

2. **Protection Mechanisms**: Encompasses security measures applied to network, endpoint, data, and access control. This dimension ensures that the organisation's technology defences are layered and adaptive, covering everything from firewalls and intrusion prevention to data encryption and multi-factor authentication.

3. **Incident Response and Recovery**: Evaluates the maturity of incident response plans, threat-hunting capabilities, forensic resources, backup procedures, and disaster recovery protocols. A high score in this dimension indicates readiness to detect, respond to, and recover from security incidents effectively.

4. **User Education and Awareness**: Gauges employee training on cybersecurity best practices, regular phishing simulations, and awareness of reporting procedures. Employees are often the first line of defence, so ongoing education and tailored training are crucial.

5. **Compliance and Governance**: Assesses alignment with regulatory frameworks (e.g., GDPR, PDPA, HIPAA) and the organisation's internal policies. This dimension also includes internal audits, policy enforcement, and third-party risk management to ensure compliance and adherence to security best practices.

6. **Physical Security**: Covers security measures for physical access to facilities and sensitive areas, including surveillance systems, access control, and environmental protections against physical threats like fire and flooding.

7. **Monitoring and Logging**: Evaluates the presence of a Security Information and Event Management (SIEM) system, log management practices, anomaly detection, and adherence to data retention policies. This dimension is critical for real-time detection of threats and maintaining a historical record for analysis and compliance.

8. **Business Continuity**: Ensures that business continuity plans, disaster recovery procedures, and redundancy measures are established and tested. This dimension reflects the organisation's ability to sustain operations and minimise disruption in the event of an incident.

9. **Asset Management**: Involves maintaining an up-to-date inventory of hardware, software, and cloud assets, asset classification, lifecycle management, and controls for shadow IT. Effective asset management ensures that all resources are accounted for and properly protected.

10. **Policy and Documentation**: Looks at the organisation's security policies, procedures, change management processes, and controls for securing sensitive documentation. Comprehensive documentation supports consistent and transparent security practices across the organisation.

11. **Cloud Security**: Covers the security of cloud configurations, access controls, data protection, and periodic assessment of cloud providers for compliance and risk. As organisations increasingly rely on cloud environments, this dimension ensures secure and compliant cloud operations.

12. **Supply Chain Security**: Assesses the security of third-party vendors, contractual security clauses, continuous monitoring of vendor products, and management of dependencies on third-party services. Given the rise in supply chain attacks, robust supply chain security is essential.

A Checklist for Cybersecurity Completeness

To aid in evaluating completeness, the following checklist outlines critical elements across each dimension. I tried to be as comprehensive as I can for this article, but you should tailor it for your organisation's needs. Use this checklist to assess your organisation's cybersecurity strategy and identify areas for improvement.

1. Threat Coverage

Component	Checklist Item	Score	Notes
Threat Intelligence	Are real-time threat intelligence feeds integrated?		
Vulnerability Management	Are systems regularly scanned for vulnerabilities?		
Zero-Day Threat Monitoring	Is there a response plan for zero-day vulnerabilities?		
Emerging Threat Awareness	Is the team aware of new cybersecurity threats?		

2. Protection Mechanisms

Network Security

Component	Checklist Item	Score	Notes
Firewalls	Are firewalls configured to protect the network perimeter?		
IDS/IPS	Are IDS/IPS systems implemented and monitored?		
Network Segmentation	Is network segmentation in place to limit access?		
Secure Remote Access	Are VPNs or encrypted channels used for remote access?		
Wireless Network Security	Are wireless networks secured with WPA3 or equivalent?		

Endpoint Security

Component	Checklist Item	Score	Notes
Endpoint Protection	Is endpoint protection installed and updated?		
Endpoint Detection and Response (EDR)	Are EDR solutions implemented?		
Device Hardening	Are endpoints hardened to reduce vulnerabilities?		

Data Security

Component	Checklist Item	Score	Notes
Data Encryption	Is sensitive data encrypted at rest and in transit?		
Data Loss Prevention (DLP)	Are DLP tools implemented to prevent data leakage?		
Data Classification	Is sensitive data classified and managed appropriately?		

Access Control

Component	Checklist Item	Score	Notes
Authentication Mechanisms	Is multi-factor authentication (MFA) enforced?		
Privileged Access Management	Is privileged access monitored and controlled?		
Role-Based Access Control (RBAC)	Are RBAC policies enforced for minimal privilege?		

3. *Incident Response and Recovery*

Component	Checklist Item	Score	Notes
Incident Response Plan	Is there a comprehensive incident response plan?		
Regular Drills	Are drills conducted to test incident response?		
Threat Hunting	Is proactive threat hunting conducted regularly?		
Forensics Capability	Are forensic tools available for incident investigations?		
Backup and Recovery	Are backups regularly performed, encrypted, and tested?		
Communication Protocols	Are communication protocols established for incident reporting?		

4. *User Education and Awareness*

Component	Checklist Item	Score	Notes
Security Training	Are employees trained on cybersecurity awareness?		
Phishing Simulations	Are phishing simulations conducted?		
Reporting Procedures	Are employees aware of incident reporting protocols?		
Role-Based Training	Is training tailored to specific roles?		

5. Compliance and Governance

Component	Checklist Item	Score	Notes
Regulatory Compliance	Are regulatory requirements monitored and enforced?		
Internal Audits	Are regular security audits conducted?		
Policy Enforcement	Are security policies enforced organization-wide?		
Third-Party Risk Management	Are third-party vendors evaluated for security?		
Legal and Regulatory Review	Are updates monitored for compliance implications?		

6. Physical Security

Component	Checklist Item	Score	Notes
Facility Access Control	Is physical access to facilities restricted and logged?		
Surveillance Systems	Are surveillance systems operational and monitored?		
Environmental Controls	Are environmental controls in place for physical threats?		

7. Monitoring and Logging

Component	Checklist Item	Score	Notes
SIEM (Security Information and Event Management)	Is SIEM implemented for real-time monitoring?		
Log Management	Are logs collected, stored, and reviewed systematically?		
Anomaly Detection	Are tools in place to detect anomalies?		
Monitoring Retention	Are monitoring data retained as per policy?		

8. Business Continuity

Component	Checklist Item	Score	Notes
Business Continuity Plan	Is there a documented and tested continuity plan?		
Disaster Recovery Plan	Is there a disaster recovery plan that's tested regularly?		
Redundancy and Resiliency	Are redundancy measures in place for critical systems?		
Crisis Management	Are crisis management processes clearly defined?		

9. *Asset Management*

Component	Checklist Item	Score	Notes
Asset Inventory	Is there an up-to-date inventory of all assets?		
Asset Classification	Are assets classified based on sensitivity and risk?		
Lifecycle Management	Is lifecycle management in place for assets?		
Shadow IT Detection	Are unauthorized IT assets detected and managed?		

10. *Policy and Documentation*

Component	Checklist Item	Score	Notes
Security Policies	Are security policies comprehensive and accessible?		
Procedure Documentation	Are security operations documented and standardized?		
Change Management	Is a change management process in place?		
Documentation Control	Are sensitive documents securely controlled?		

11. *Cloud Security*

Component	Checklist Item	Score	Notes
Cloud Configuration Management	Are cloud resources configured securely?		
Access Controls	Are access controls managed for cloud environments?		
Data Protection	Is cloud-stored data encrypted and access-controlled?		
Cloud Provider Assessment	Are cloud providers assessed for compliance and risk?		

12. *Supply Chain Security*

Component	Checklist Item	Score	Notes
Vendor Risk Assessment	Are vendors evaluated for security risks?		
Contractual Security Clauses	Are security clauses included in vendor contracts?		
Continuous Monitoring	Are vendor products monitored for vulnerabilities?		
Dependency Management	Is there a process to manage third-party dependencies?		

Calculating the Completeness Profile

To create a more accurate measure of cybersecurity posture, a completeness score can be calculated by assessing each dimension's coverage and maturity. Here's a sample formula for calculating a completeness profile:

Completeness Score (CS) = (Σ Dimension Scores) / Total Dimensions

Each dimension score is rated on a scale from 1 to 5 based on predefined criteria, such as:

- 1: **Minimal** — Insufficient coverage or maturity.
- 2: **Basic**—Some coverage but lacks depth or integration.
- 3: **Moderate**—Adequate coverage, though some gaps exist.
- 4: **Good**—Strong coverage with minor improvements needed.
- 5: **Comprehensive**—Fully matured, integrated, and monitored.

The goal is to reach a high completeness score across all dimensions, ensuring no weak links in the cybersecurity posture.

Example Calculation

First, we score each dimension on its own. Let's break down an example for one dimension, **Protection Mechanisms**, and how to assign its score based on coverage:

- **Endpoint Security** — Basic protections but no EDR — Score: 3
- **Data Security** — Partially implemented with data encryption but lacking DLP — Score: 3
- **Access Control** — Good coverage with MFA and RBAC but lacks privileged access management — Score: 3

Average score for **Protection Mechanisms** dimension:

Protection Mechanisms Score= (5+3+3+3)/4 = 3.5

Rounding down, the **Protection Mechanisms** dimension would be scored as **3**.

Assume we assess a company across the following **12 dimensions**, with a maximum possible score of 5 for each dimension.

1. **Threat Coverage** — Score: 4
2. **Protection Mechanisms** — Score: 3
3. **Incident Response and Recovery** — Score: 5
4. **User Education and Awareness** — Score: 4
5. **Compliance and Governance** — Score: 3
6. **Physical Security** — Score: 4
7. **Monitoring and Logging** — Score: 2
8. **Business Continuity** — Score: 5
9. **Asset Management** — Score: 4
10. **Policy and Documentation** — Score: 3
11. **Cloud Security** — Score: 4
12. **Supply Chain Security** — Score: 3

Step-by-Step Calculation

Sum of All Dimension Scores:

$$4+3+5+4+3+4+2+5+4+3+4+3 = 44$$

Total Number of Dimensions: 12

Completeness Score:

Completeness Score = 44/12 ≈ 3.67

In this case, the **Completeness Score is 3.67** out of 5. This score reflects that the organisation's cybersecurity program is moderately well-rounded, with room for improvement, especially in areas scoring below 4.

Interpreting the Score

- **0–2**: High-risk profile with significant vulnerabilities across multiple dimensions. Immediate attention is needed to bolster defences.
- **2–3**: Basic protections in place, but there are noticeable gaps that could expose the organisation to security risks.
- **3–4**: Moderate-to-strong coverage. The organisation is generally secure but should aim to address minor weaknesses to strengthen its posture.
- **4–5**: Comprehensive coverage. The organisation demonstrates robust cybersecurity across all dimensions, with minimal to no gaps.

Using the Checklist to Build a Cybersecurity Strategy

This checklist can be used as follows to assess and enhance your cybersecurity strategy:

1. **Evaluation**: Go through each item in the checklist, marking off completed items and noting any gaps. This will help identify areas with insufficient protection or oversight.

2. **Prioritisation**: Based on the completeness score, prioritise the dimensions with lower scores. For example, if “User Education” scores poorly, focus efforts on building a stronger security awareness program.

3. **Resource Allocation**: By identifying specific gaps, allocate resources more effectively. For example, if there’s a gap in “Incident Response,” invest in incident response tools, team training, or tabletop exercises.

4. **Continuous Improvement**: Cybersecurity is a dynamic field, so periodically revisiting the checklist ensures that all dimensions of completeness are up-to-date and reflect the latest threat landscape.

5. **Reporting and Monitoring**: Track the checklist over time to monitor progress and report the organisation’s cybersecurity posture to executive leadership. Completeness scores offer a clear metric for improvement and can demonstrate the value of cybersecurity investments.

Conclusion

Completeness in cybersecurity defence represents a step beyond traditional defence-in-depth, emphasising a holistic, interconnected approach that considers not just layering but the maturity and adequacy of every dimension. By assessing completeness, organisations can better understand their risk exposure and strengthen their protection profile. The checklist and completeness score offer practical tools to identify gaps and guide investment in a more cohesive cybersecurity strategy, moving from isolated defences to a unified, resilient framework. Embracing completeness can help organisations better anticipate and mitigate cyber threats, safeguarding their assets and ensuring long-term operational resilience.