Cybersecurity Risk Assessment Scorecard

The purpose of a cybersecurity risk assessment is to understand the organization's ability to defend against and respond to an attack.

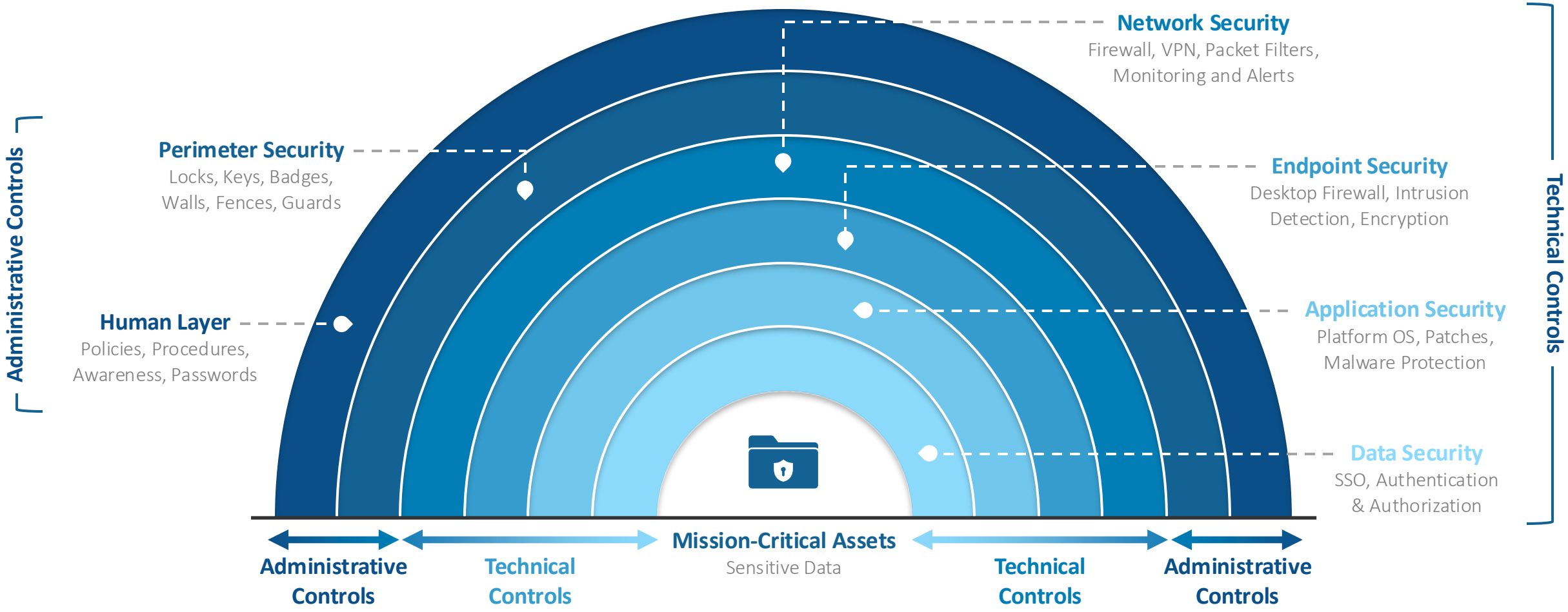
	CIS Control	Policy	Implementation	Reporting	Weighted Average	Grade
1	Inventory and Control of Enterprise Assets	60%	77%	70%	75%	C
2	Inventory and Control of Software Assets	56%	71%	72%	70%	C-
3	Data Protection	48%	59%	57%	58%	F
4	Secure Configuration of Enterprise Assets and Software	79%	81%	85%	81%	B-
5	Account Management	70%	87%	87%	85%	B
6	Access Control Management	63%	86%	83%	83%	B
7	Continuous Vulnerability Management	46%	60%	58%	58%	F
8	Audit Log Management	53%	72%	72%	70%	C-
9	Email and Web Browser Protections	70%	87%	87%	85%	B
10	Malware Defenses	100%	100%	93%	99%	A+
11	Data Recovery	70%	93%	89%	90%	A-
12	Network Infrastructure Management	66%	80%	80%	79%	C+
13	Network Monitoring and Defense	57%	52%	52%	53%	F
14	Security Awareness and Skills Training	63%	79%	79%	77%	C+
15	Service Provider Management	53%	69%	69%	67%	D+
16	Application Software Security	67%	85%	84%	83%	B
17	Incident Response Management	42%	66%	28%	60%	D-
18	Penetration Testing	67%	80%	79%	79%	C+
	Overall Grade	**63%**	**75%**	**73%**	**74%**	**C**

United Community

elliott davis

Cybersecurity Defense Layered Security Model

Breaking down and implementing a layered security model.



United Community

Source: IANS

Incident Response Plan Playbook Components

- Objective/Purpose
- Incident Level Definition
- Plan Distribution
- Roles & Responsibilities
- Event Procedures
- Evidence Gathering & Handling
- Contact Information
- Incident Reporting Form
- Communications
- Testing & Training
- Plan Review & Updating