



**Leicestershire
Business Voice**

Cybersecurity: 3 Things That Will Strengthen Your Business

25 June 2026

Welcome and scene setting



Dillan Shikotra, Director



Neil McGhee, Director

Aims and purpose of LBV

The influential voice of business in Leicester & Leicestershire

Connects business leaders and decision-makers to shape the long-term economic success of Leicester and Leicestershire

Champions and represents the local business community, providing a strong collective voice while driving growth, collaboration and positive change across the city

Cybersecurity: 3 Things that will Strengthen your Business

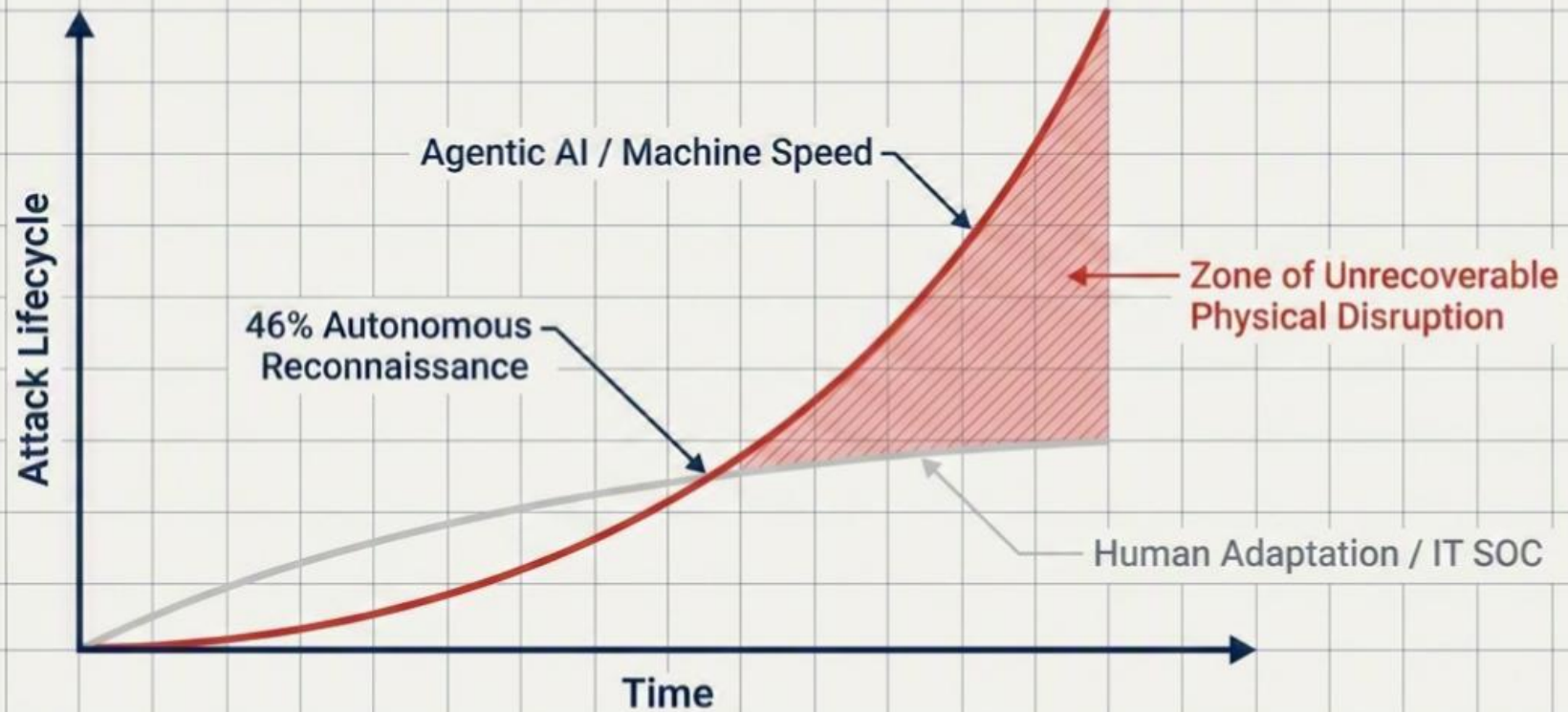
Transforming Risk into Resilience through
Operational Engineering

Anjay Mandalia – TXOne Networks

Principal (Cybersecurity Head - United Kingdom & Ireland)



The Asymmetric Battlefield



Systemic Risk vs. Business Enablement

The Illusion of Savings

- **Lower Immediate Spend:** Skipping paid protections, relying on default settings.
- **Less User Friction:** Staff sign in with only a password.

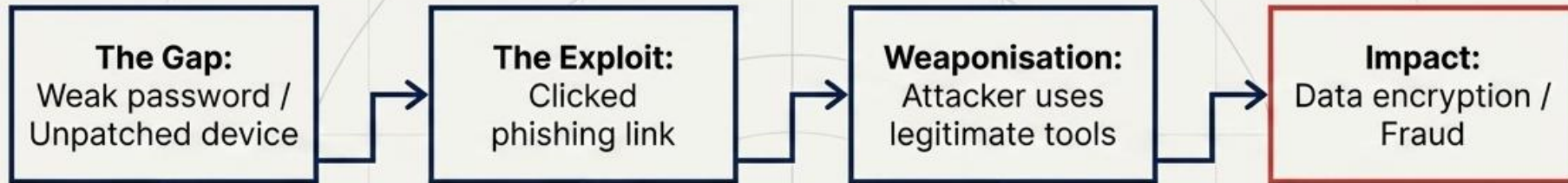
Resulting Risk: High likelihood of severe downtime, financial exposure, halted order processing.

The Reality of Protection

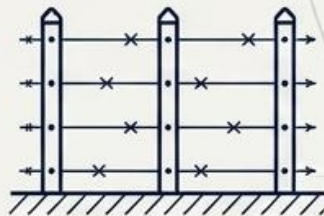
- **Reduces Breach Risk:** Controls stop attackers even if a user clicks a bad link.
- **Faster Recovery:** Rebuilding in hours, not days.

Resulting Value: Cybersecurity becomes a business enabler. Builds customer trust and wins tenders.

The IT Reality



The Burglar Analogy



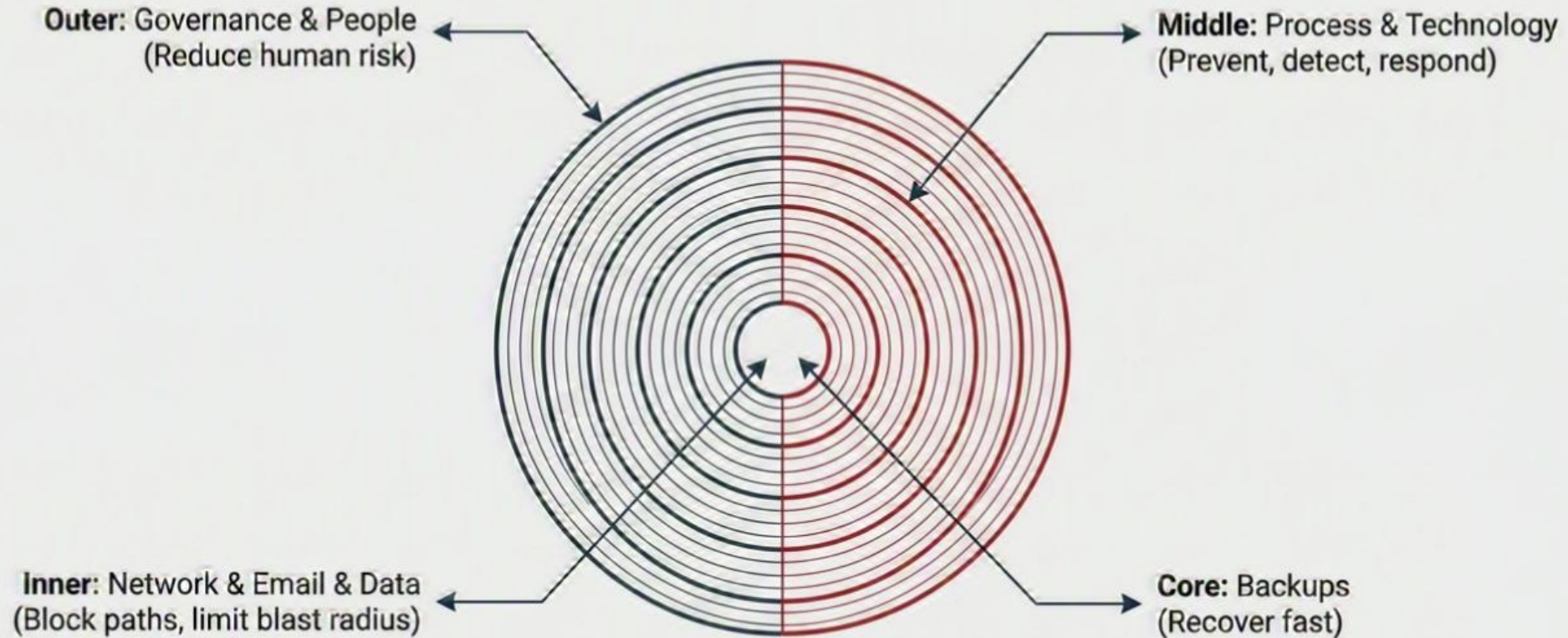
The Perimeter =
The Garden Fence
(Easily jumped)



Legacy Systems
= The Valuables
(Need a safe)



Inline Prevention
= Motion Sensors
(Catch them in the hallway)



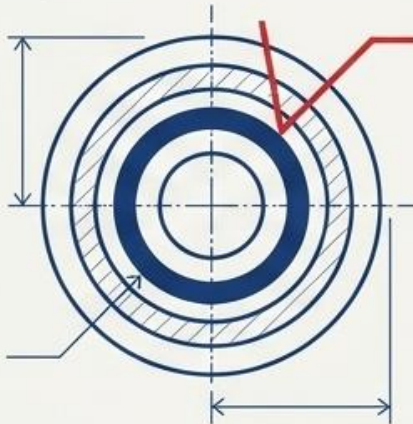
Assume something will fail. Design so failure is contained.

The Architecture of Resilience

01.

**Assume the
Perimeter Will Fail**

Design for Containment



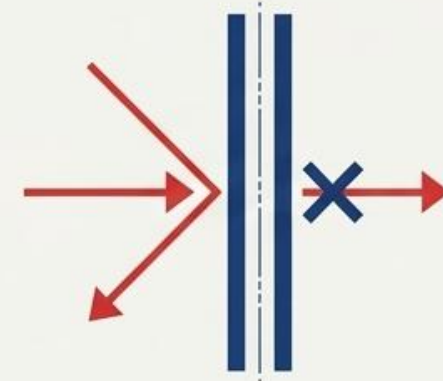
02.

**Secure Legacy
Assets in Place**



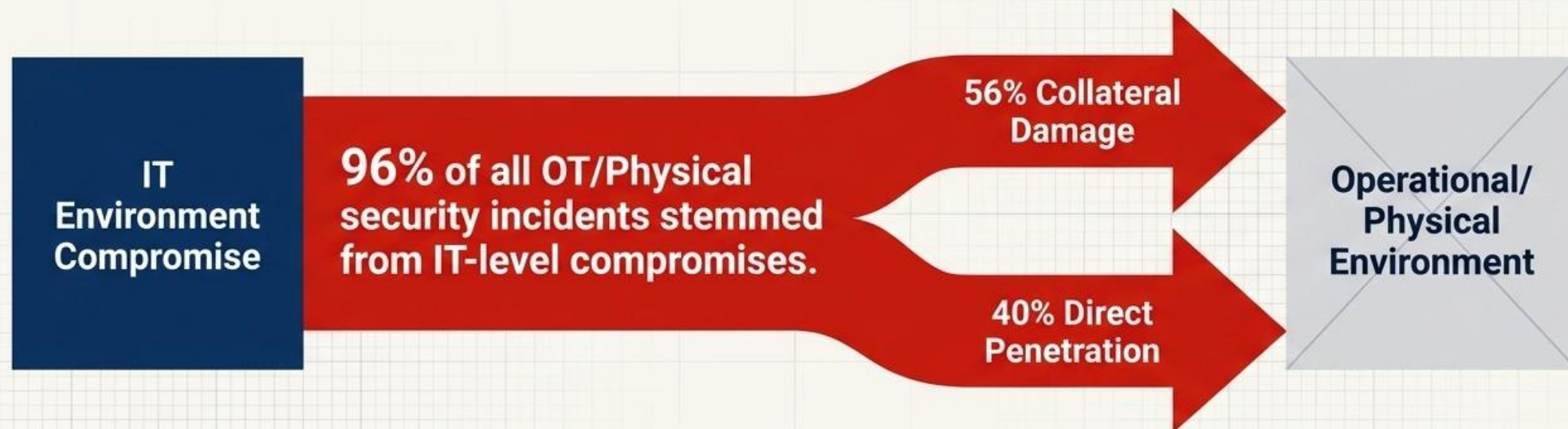
03.

**Pivot to Inline
Prevention**



In a fragmented world, sovereignty equals systemic resilience.

Pillar 01: The Convergence Trap



Your operational environment is only as secure as the weakest link in your IT network.

Pillar 02: Coexisting with Risk

The Blind Spot

75% of operational environments consist of legacy systems exposed to modern warfare.

88% of organisations choose to coexist with legacy risk due to economic unfeasibility.

The Paradox

94% CISOs reporting satisfaction with current posture.

----- *versus* -----

60% Organisations breached in the last 12 months.

Replacing legacy systems is economically unfeasible. The strategy must shift to securing them in place.

Pillar 03: The Speed of Destruction



Inline Prevention

Continuous Core Protection.
Blocks automated paths instantly.

Pillar 04: From Strategy to Execution

1. Containment

2. Secure in Place

3. Inline Prevention

High-level operational engineering is achieved through simple, repeatable, low-cost tools.

1. Identity & MFA

2. Repeatable Patching

3. Tested Backups

Quick Win 1: Multi-Factor Authentication (Identity)

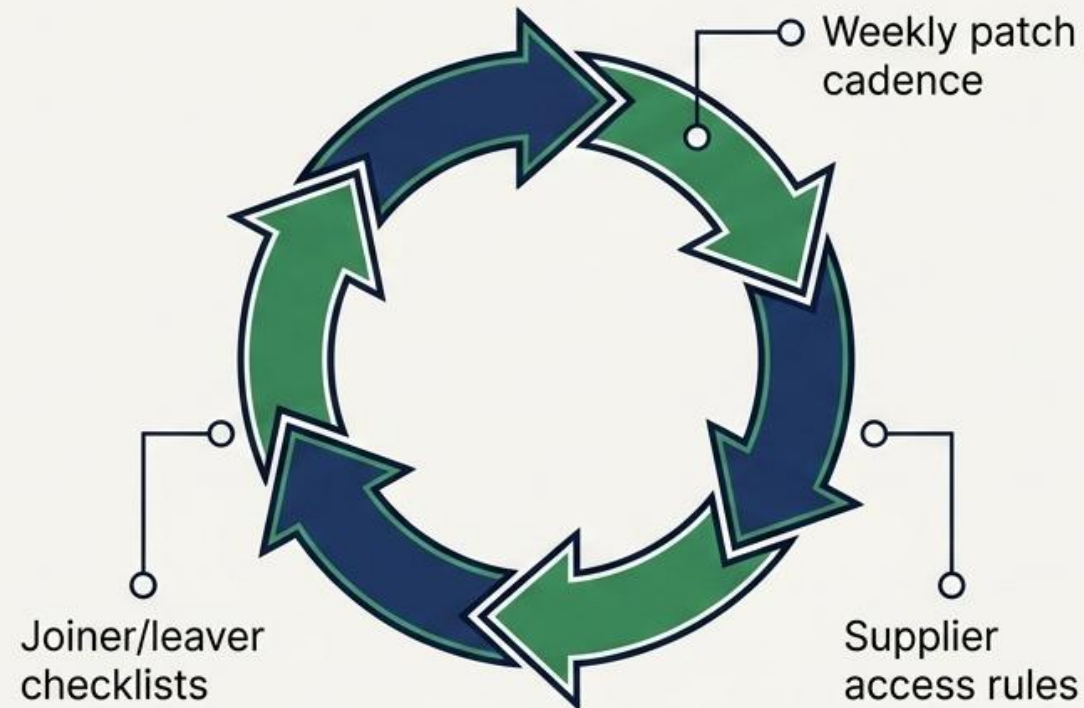


Tech Quick Wins

-  Mandate MFA everywhere (Built-in Microsoft/Google Authenticator).
-  Disable legacy authentication.
-  Stop password reuse with a company password manager.

Identity is the new perimeter. The cheapest layers have the highest impact.

Quick Win 2: The Patching Process



- ☒ Enable **auto-updates** on OS & Apps.
- ☒ **Remove local admin rights** (Stops malware from installing system-wide).
- ☒ **Enforce device encryption** (BitLocker/FileVault).

Objective: Prevent drift. Repeatable processes beat heroics.

Quick Win 3: Backups & Recovery (The Core)



Protect Like Gold:

Protect Like Gold: Separate admin accounts and mandatory MFA for backup consoles.

Test Monthly:

A backup you haven't successfully restored is a hope, not a backup.

The Implementation Roadmap

Identity	Use built-in M365/Google MFA. (Zero extra cost)
Endpoint	Microsoft Defender, BitLocker. (Zero extra cost)

Days 0-30: Block easy paths

- ☐ Enforce MFA
- ☐ Auto-updates
- ☐ Remove admin rights.

Days 31-60: Make it repeatable

- ☐ Establish patch cadence
- ☐ Joiner/leaver lists.

Days 61-90: Prove resilience

- ☐ Implement 3-2-1 backups
- ☐ Execute first restore test.

Start by turning on what you Already Have

True cybersecurity is defined by the ability to sustain uninterrupted physical operations under duress.

It is not a grudge purchase. It is the operational stability that builds trust, protects your margins, and wins the contract.

**Pick your 3 quick wins today. Assign an owner.
Set a date for your first restore test.**

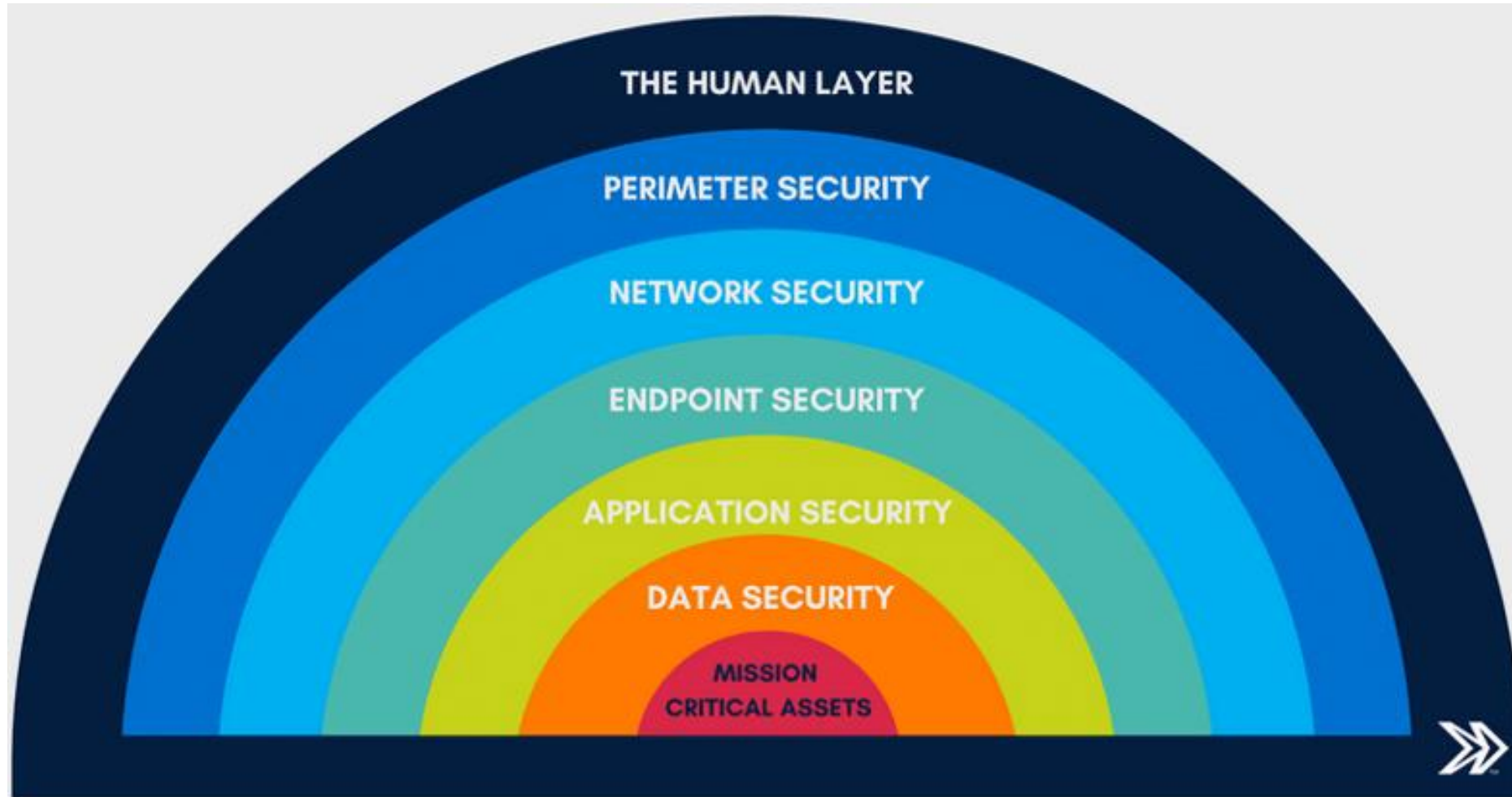
Thank You

Pick your 3 Quick Wins
KEEP THE OPERATION RUNNING

Anjay Mandalia – from TXOne Networks

Principal Head, United Kingdom & Ireland

Seven layers of cybersecurity



What each layer means

Layer	Purpose	Common Gap
1. User Awareness	Educating staff to identify threats such as phishing and social engineering.	Employees are often the weakest link due to lack of training.
2. Endpoint Security	Protecting laptops, desktops, servers and mobile devices.	Outdated antivirus and unpatched devices.
3. Email Security	Filtering malicious emails, links and attachments before they reach users.	Basic spam filtering without advanced threat protection.
4. Identity & Access Management	Securing user accounts through MFA and least-privilege access.	Weak passwords and no multi-factor authentication.
5. Network Security	Protecting internal systems through firewalls, segmentation and monitoring.	Flat networks with little visibility or control.
6. Data Protection & Backup	Ensuring critical data is protected and recoverable.	Backups exist but have never been tested.
7. Monitoring & Response	Detecting and responding to threats 24/7.	No visibility of attacks until significant damage occurs.

Over to you to discuss

Challenges

- What is your biggest cybersecurity challenge today?
- What keeps you awake at night from a security perspective?
- Have you experienced a cyber incident in the last 12 months?

Concerns

- Ransomware
- Business email compromise
- Data breaches
- Supply chain attacks
- Compliance requirements

Current Approaches

- Do you have Cyber Essentials or Cyber Essentials Plus?
- Is MFA enabled across the business?
- How often do you provide cybersecurity training?
- How are you monitoring for threats?
- When was your last backup recovery test?

Membership

If you enjoyed today's event and would like to find out about becoming a Leicestershire Business Voice member, please speak to a Board Director today, visit our website at www.lbv.co.uk/membership or scan the QR code below.

By joining LBV, you can:

- ✓ Help businesses thrive
- ✓ Voice your opinions with local & regional decision makers
- ✓ Influence policy affecting our economy



Membership cost



LBV Ambassadors

The new LBV Ambassador Programme brings together a network of trusted business leaders from across Leicester and Leicestershire who are passionate about supporting the local economy and business community.

Ambassadors play a key role in shaping events and policy priorities, building connections and advocating for LBV, whilst promoting a strong, united business community.

Existing LBV members who are interested in becoming an ambassador can contact voice@lbv.co.uk or apply online at www.lbv.co.uk/membership/

Upcoming events

To learn more about the upcoming LBV events visit www.lbv.co.uk/events or scan the QR code.

