HACKED part 2

OCAPDD: Dave Ferguson

Pathway Communications: Daniel Rajanayagam

Today's Speakers

OCAPDD

Dave Ferguson, CEO

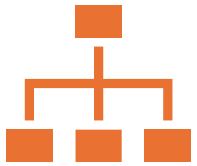
OCAPDD / AOCPDI
Open Hands

Pathway Communications

Daniel Rajanayagam, VP of Client Solutions

pathway
communications
Cybersecurity. Simplified.

Agenda



Chapter 1: Background

Chapter 2: The Breach

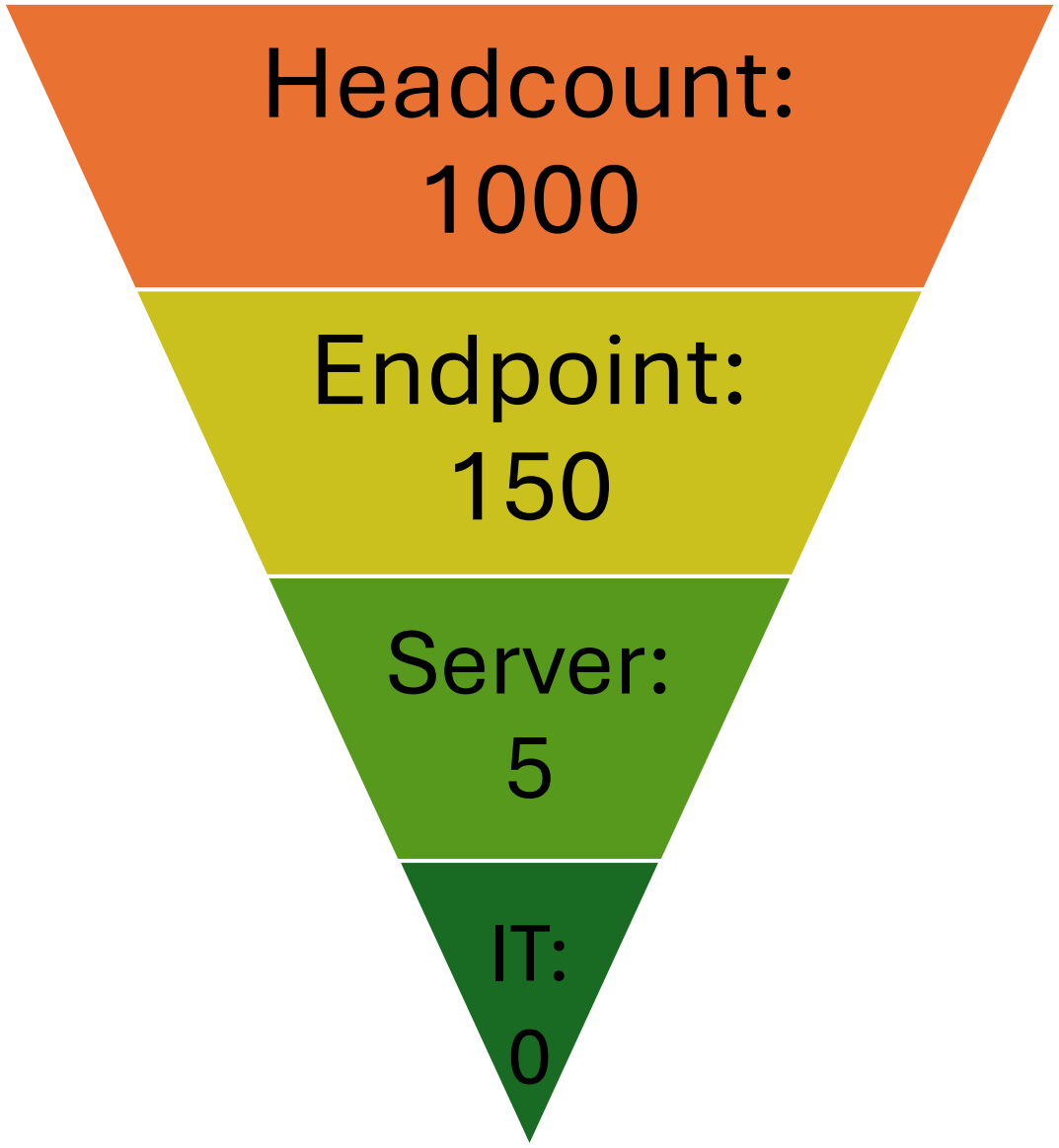
Chapter 3: The Response

Chapter 4: The Lessons

Chapter 1

Background

OCAPDD's Infrastructure



Event State

- Data Backups
- Antivirus

Optimal State

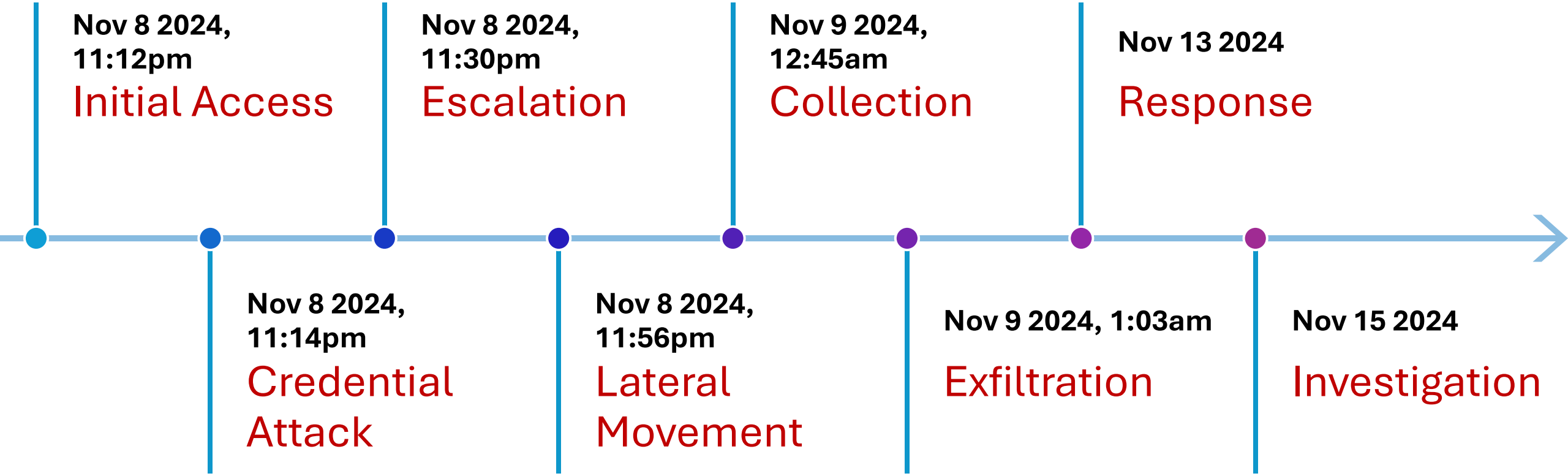
- DR/BCP
- IRP
- Antimalware
- Log analysis

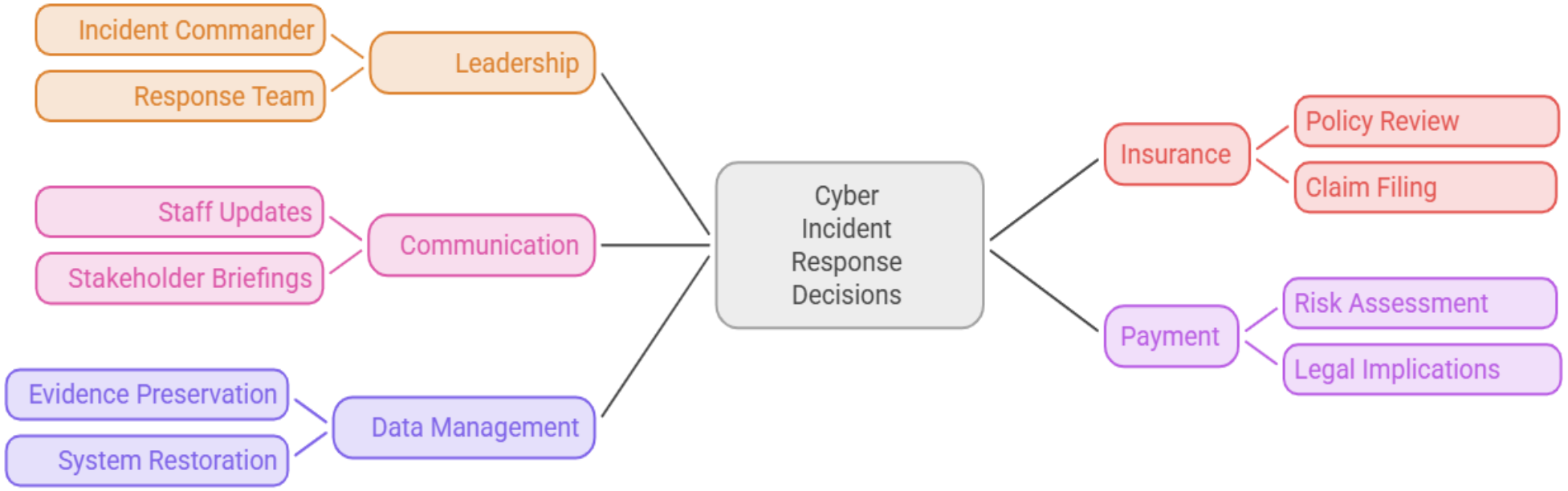
Chapter 2

The Breach

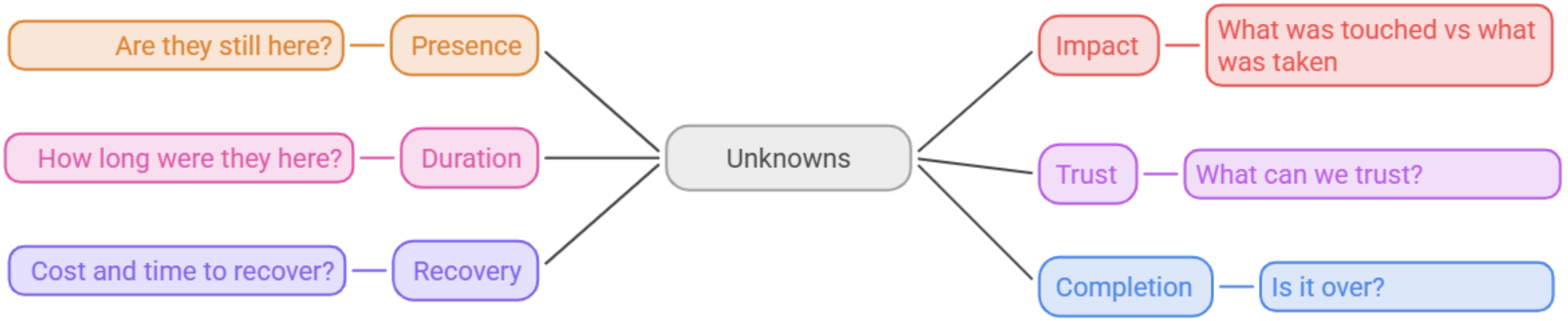
Attack Vector	Target	Dwell Time
• Training account	• PII, PHI, Financials	• 5 days

Discovery Timeline





Event Apprehended → Chaos



Chapter 3

The Response

Response Methodology → Order

- Identify breach
- Isolate systems
- Implement fix

Containment

- Collect evidence
- Analyze attack
- Document findings

Investigation

- Assess requirements
- Draft communication
- Execute

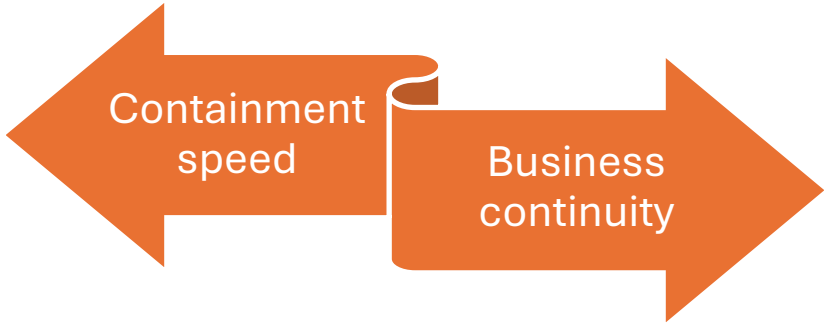
Notification

- Restore systems
- Patch vulnerabilities
- Monitor systems

Recovery

Containment: Stop the Bleeding

- Goals and decisions
- Isolate vs shutdown
- Preserving evidence
- Cutting off attacker access
- Credential resets at scale



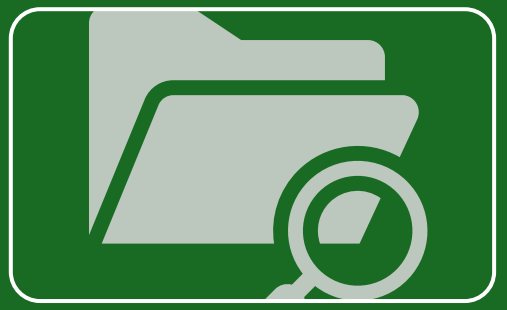
Containment: Expertise

Incident Command	authority, coordination, non-technical
Network / Infrastructure	executes isolation, disables entry points
Systems Administration	resets and audits accounts and logs
Threat Detection	deploys response to endpoints
Legal Counsel	governs privilege, evidence preservation, obligations
Communications	manages internal and external notifications

Investigation: Forensics 101

- Imaging
- Log analysis
- Malware reverse engineering
- Establishing root cause and scope

Investigation: Following the Evidence

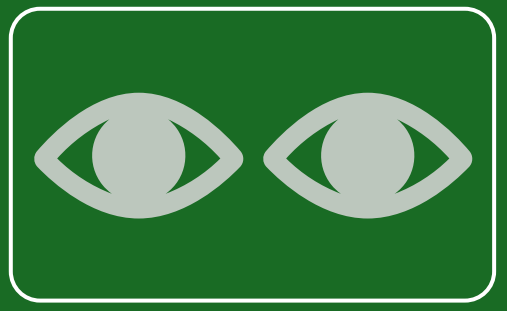


Walkthrough of the Investigation

- Reconstructed attack chain
- Evidence correlation
- Iterative process across months

Logs versus Gaps

- Windows Security Event Logs, MegaSync application logs
- Limited log Retention, no centralized log aggregation



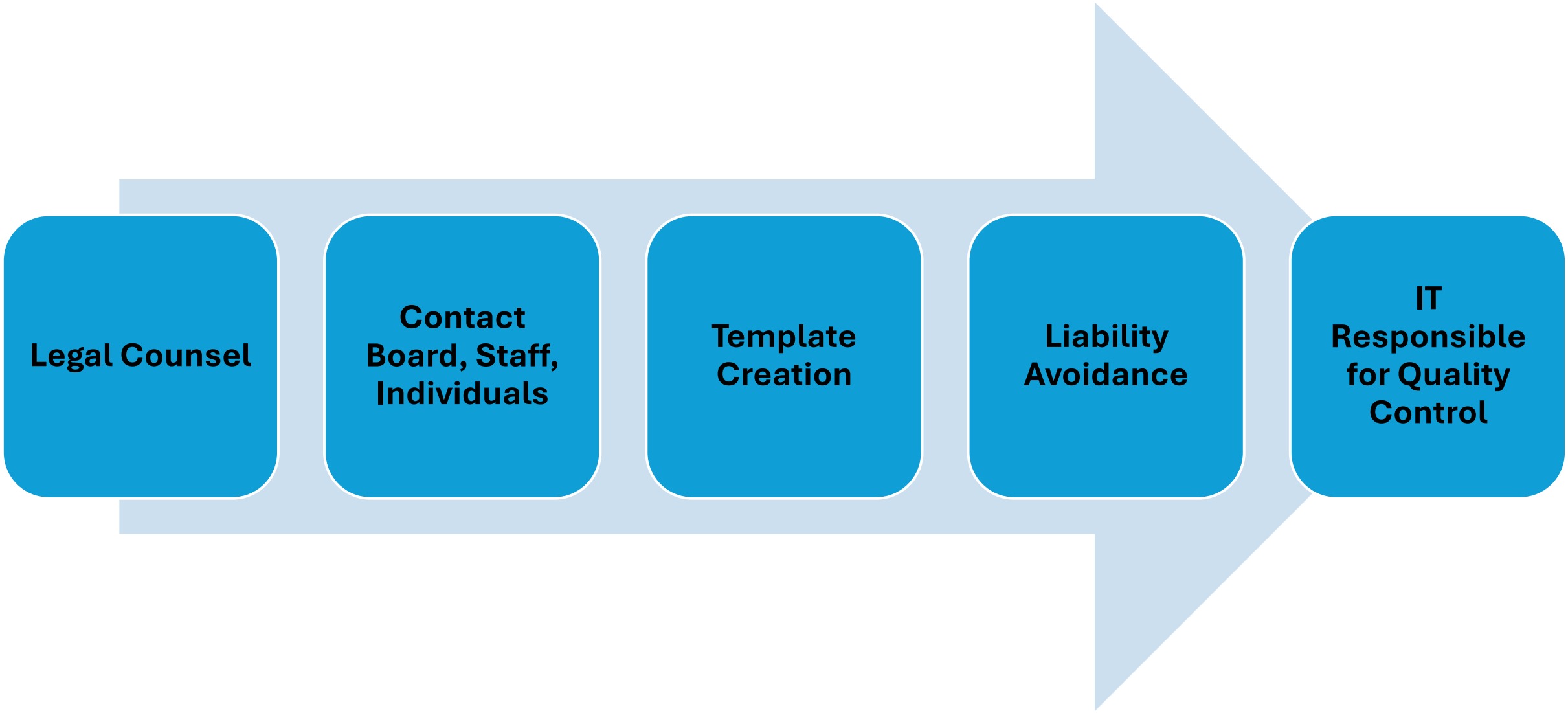
Scope of Data Access

- Access vs exfiltration
- Scope of affected individuals had to be manually established

Notification: Obligations

- Privacy legislation
- Breach reporting requirements
- Contractual obligations to funders
- Insurance notification clauses

Notification: Communicating under fire



Recovery: Rebuild vs Restore

- Trusting backups
- Danger of restoring compromised systems
- Rebuilding from known-good data/states
- Recovery time vs expectations

Recovery: Hardening while Rebuilding

Recovery vs opportunity

Decisions made during rebuild

New technologies

- MFA rollout
- EDR
- SIEM

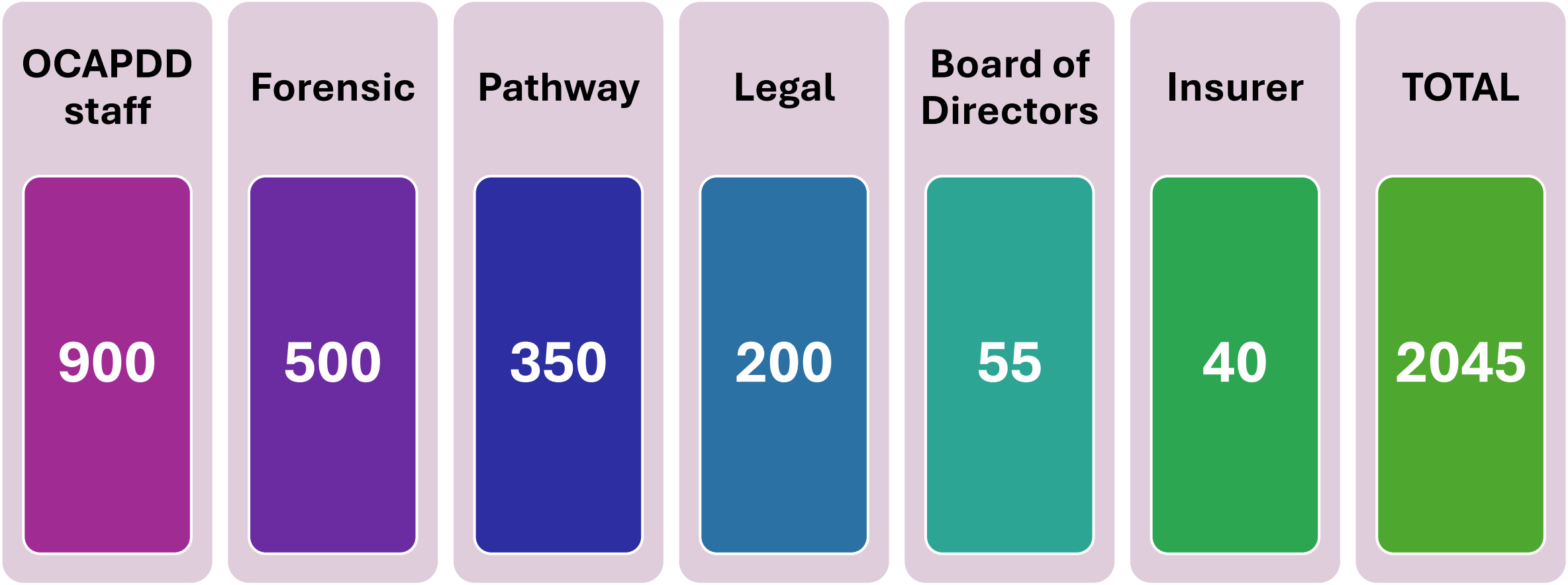
New architecture

- network design
- systems isolation

New processes

- testing recovery
- annual training
- round tables

Total Response Effort (in hours)



Chapter 4

The Lessons

IT Manager’s Real Job

You own the risk

- Breach response burden lands on you regardless of the cause

Myths

- “We’ve never had a problem” is not a security posture
- “Too small to be a target” assumes a lack of automation

Reality

- Attackers automate, targeting vulnerabilities not victims
- NFPs hold valuable data (PII, PHI, donor financials) and have below-average defenses

Assess and Measure

Do you know your dwell-time detection capability?

Can you produce 90 days of authentication logs right now?

When did you last test a restore?

Who do you call first at 2am?

MFA coverage %

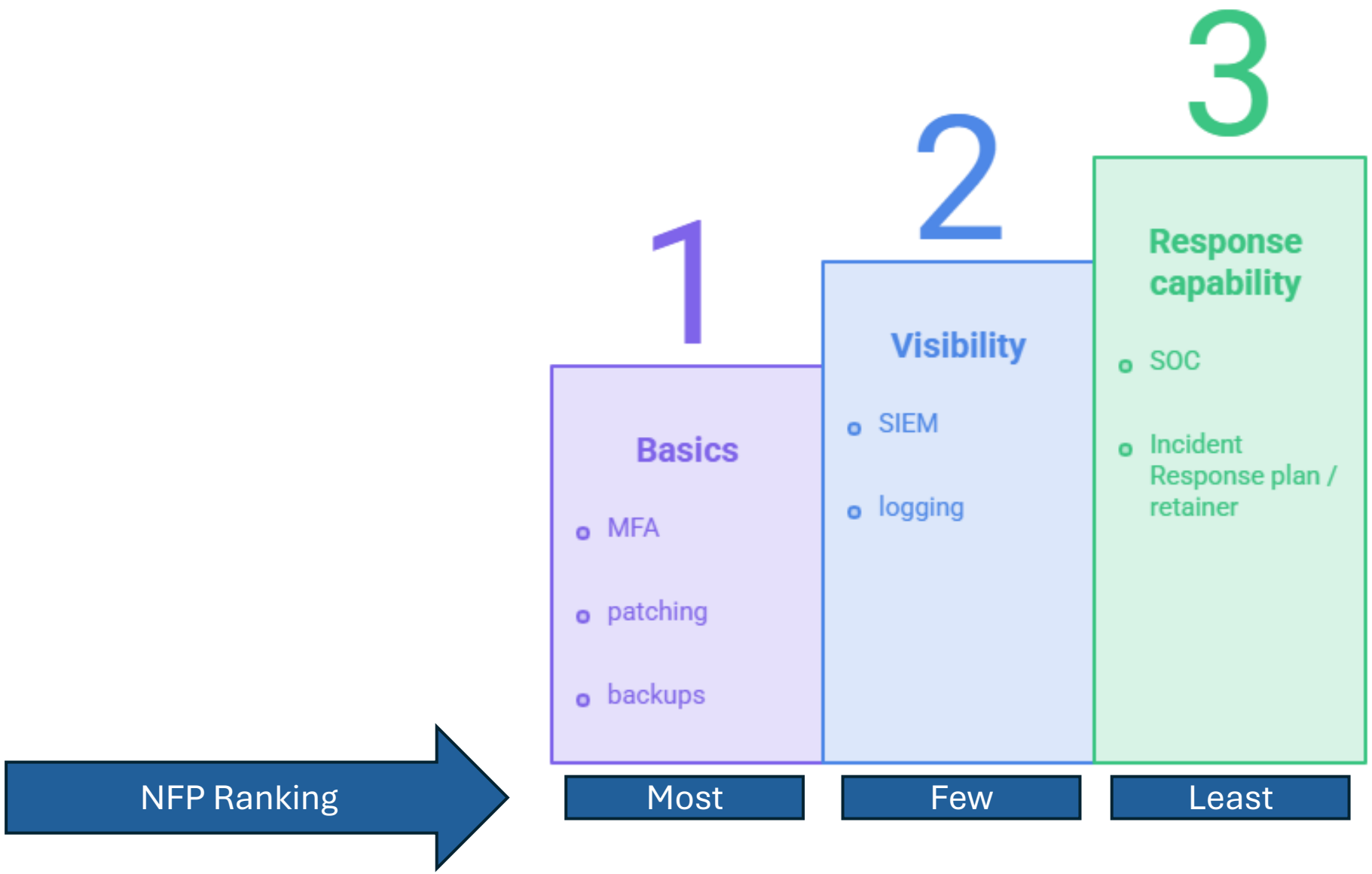
EDR coverage %

Backup restore test recency

Incident response plan existence / age

Log retention period

Maturity Ladder



Next Steps

01

Get a security assessment

02

Enable MFA

03

Test your backups regularly

04

Establish and Incident Response contact now

05

Establish telemetry via SIEM

Disclosure

Q&A

Contacts:

Daniel.Rajanayagam@corp.pathcom.com

Walter.Zenko@corp.pathcom.com