THE CYBERSECURITY TALENT GAP

Isn't What You Think

A Business Capability Development Model

Prioritize capability. Reduce risk. Define opportunity. Develop judgment.

Jacob Pender | CornCon

Why I See the Talent Gap Differently

The practitioner's frustration, viewed from the student's side



JACOB PENDER

Former Practitioner
Former IT Executive
Cybersecurity Educator

20 YEARS IN SECURITY

45 | MARRIED | 2 KIDS

PRACTITIONER

Lived the same hiring and readiness frustrations as cybersecurity leaders.

EXECUTIVE

Led IT before age 30 and saw the operational cost of capability gaps.

EDUCATOR

Now sees the gap from the student side and asks what organizations are missing.

"I had the same frustrations. Teaching made me ask: How are we getting this so wrong?"

A familiar hiring frustration

“They looked great on paper. Then the problem became ambiguous.”

Who has experienced this?

What if the candidate is not the entire problem?

Hiring signals

Degrees
Certifications
Years of experience
Product familiarity

Workplace demands

Ambiguity
Business context
Communication
Accountability

Leadership responsibility

Practice
Feedback
Boundaries
Increasing ownership

The gap may exist between qualification and the organization’s development system.

The cybersecurity talent gap is also a business capability-development gap.

Organizations must decide what capability to build, how to control risk, and how judgment will grow.

What CISO actually need

Curiosity

Asks what changed

Communication

Explains risk clearly

Accountability

Owns the next step

Adaptability

Learns unfamiliar tools

Documentation

Leaves usable evidence

Judgment

Acts within boundaries

Knowledge and experience are not enough

Knowledge + Experience + Reflection Context Accountability = Professional Judgment

Knowing how to make a change is different from knowing whether, when, and under what conditions.

The firewall test

Vendor request

“Just create an ANY rule.”

Technical capability

Can configure the rule correctly.

Professional judgment

Challenges scope, assesses risk, compares alternatives, and escalates.

The gap is not always technical skill. Sometimes it is decision quality.

The small-business dilemma

Training cost

Time and attention

Production risk

Customer impact

Turnover risk

Capability may leave

Scale

One departure can remove half a function

The concern is legitimate: How do we develop capability without creating more risk?

The four-step Business Capability Development Model

1

PRIORITIZE

Capability
business return

2

REDUCE RISK

Blocker
safety net

3

DEFINE OPPORTUNITY

Boundaries
support

4

DEVELOP JUDGMENT

Review
targeted practice

Each step produces the decision needed for the next step.

Step 1 | Prioritize the capability investment

IMPACT

Revenue
Customers
Security
Continuity

DEPENDENCY

One person
One vendor
Fragile process

FUTURE NEED

Growth
Succession
Technology change

DEVELOPABILITY

Documentation
Cross-training
Bounded decisions

FEASIBILITY

Time
Access
Leadership attention

Output: Invest, pilot, prepare first, defer, or stop.

Training completion is not the return

Business value

Reduced dependency
Improved continuity
Preserved knowledge

Operating value

Less senior rework
More work inside boundaries
Added capacity

Decision value

Continue
Expand carefully
Adjust
Stop

Increased business capability is the return.

The objection: “We cannot afford it.”

You may be right.

This model does not assume the investment must be made.

A Smaller, Controlled Investment

Not a program

No company-wide rollout
No equal investment in everyone

Start small

One capability
One blocker
One bounded decision

Control exposure

Defined authority
Review
Escalation
Rollback

Require evidence

Pilot
Measure
Continue, revise, or stop

Can we afford one bounded pilot, and what evidence would justify continuing it?

Step 2 | Reduce development risk

Documentation

Can another person follow the process?

Backup

Can essential work continue?

Mentoring

Can reasoning be reviewed?

Boundaries

What may be decided or escalated?

Safe practice

Can work be tested or reversed?

Ownership

Does knowledge remain with the business?

Safety nets make development possible

DOCUMENT

Procedure and exceptions

BACK UP

Minimum continuity

REVIEW

Approval and rollback

ESCALATE

Stop and challenge criteria

PARTNER

Outside capacity where scale is limited

Output: One blocker, one safety net, and a proceed / restrict / pause decision.

Step 3 | Define the right opportunity

Foundation

Completes and explains routine work

Learning

Applies feedback

Transparency

Reports uncertainty and errors

Evidence

Gathers relevant information

Questions

Explores context and assumptions

Boundaries

Knows when to proceed or escalate

Documentation

Leaves usable evidence

Follow-through

Closes actions and communicates gaps

Different roles need different judgment

Reliable execution

Follow standards
Recognize exceptions
Escalate correctly

Independent decisions

Gather evidence
Compare alternatives
Manage risk

Develop others

Explain reasoning
Set boundaries
Coach decisions

The implementation should not be one size fits all.

“I Don’t Have the Right Candidate.”

The model does not assume a suitable internal candidate is already available.

If the capability matters but no candidate is ready, the organization has identified the capability gap more precisely.

NARROW

Create a smaller, lower-risk opportunity.

BUILD

Develop prerequisite technical skills and work habits.

HIRE

Recruit specifically for the missing technical foundation, decision behavior, or mentoring capacity.

PARTNER

Use external expertise while preserving internal knowledge.

DEFER

Delay the investment until value, safeguards, or readiness improve.

“No candidate is ready today” is a valid business conclusion, not a failure of the model.

Capability before candidate means the business can still choose to narrow, build, hire, partner, defer, or stop.

Step 4 | Develop judgment through review

Problem

Was the real problem clear?

Evidence

What was known and limited?

Assumptions

What was believed, not known?

Alternatives

What other paths existed?

Risk

What consequences were accepted?

Escalation

Were authority limits clear?

Reasoning

Why this option?

Transfer

Can another person reuse it?

The 10-minute decision review

1	**Name the decision**	What was known at the time?
2	**Expose the assumption**	What belief mattered most?
3	**Compare alternatives**	What was rejected and why?
4	**State risk and boundaries**	What risk was accepted? When should escalation occur?
5	**Choose one improvement**	What should repeat or change next time?

An approval queue can protect the business and still fail to develop judgment

Gatekeeping only

Approve or reject
Little explanation
Technician waits

Developmental approval

Reason is visible
Risk and alternatives discussed
Next boundary clarified

Growth signal

More decisions owned
Better questions
Less reconstruction
Clearer escalation

Exposure to technology is not the same as participation in decision-making.

Four questions for less-experienced firewall technicians

1

When a change is approved or rejected, do you understand why?

2

What firewall decisions can you make now that you could not make six months ago?

3

What is the approver evaluating that you are not yet evaluating?

4

If approval disappeared tomorrow, what change would still make you uncomfortable, and why?

Listen for missing feedback, missing context, missing ownership, and unclear boundaries.

Evidence the investment is working

Dependency

Another authorized person can continue routine work

Senior rework

Approvers do not rebuild the entire analysis

Boundaries

More decisions stay inside approved limits

Knowledge

Evidence, rationale, approval, and rollback remain

Capacity

More routine work is completed safely

Protection

Customer and production safeguards remain effective

Apply the Model

Start with one capability. Keep the investment bounded, measurable, and reversible.

NEXT WEEK **Choose the capability and expose the development barrier.**

1 IDENTIFY

- Select one cybersecurity capability with customer, security, continuity, or dependency impact.
- Name the expected business return.

2 LISTEN

- Ask one experienced approver and one developing technician where the current process blocks learning.
- Look for missing feedback, context, ownership, or boundaries.

3 BOUND

- Define one decision that may be owned, one that requires review, and one that must be escalated.

WITHIN 90 DAYS **Run one bounded pilot → add one safeguard → review real decisions → measure whether capability improved.**

Measure: dependency | senior rework | knowledge transfer | decisions completed within approved boundaries

The Executive Decision Path

How the capability model changes the cybersecurity talent-gap conversation

1

CAPABILITY BEFORE CANDIDATE

What capability creates measurable business value?

2

RISK BEFORE AUTHORITY

What safeguard must exist before responsibility expands?

3

OPPORTUNITY BEFORE AUTONOMY

What bounded decision is appropriate now?

4

JUDGMENT BEFORE EXPANSION

What did the reasoning reveal, and what comes next?

THE TALENT GAP IS NOT ALWAYS A SHORTAGE OF PEOPLE.

It is often an organization's inability to build, transfer, and retain cybersecurity capability.

At every step, leadership may continue, adjust, restrict, defer, partner, hire, or stop.

PRIORITIZE CAPABILITY

REDUCE RISK

DEFINE OPPORTUNITY

DEVELOP JUDGMENT

Develop people. Preserve knowledge. Reduce dependency. Build resilience.

The gap narrows when organizations deliberately build capability and judgment.