

PREPARING FOR WHAT'S NEXT

Cybersecurity planning for 2027

Faster attacks • AI prompt risk • Credit union consolidation

CyberOps 2026



The 2027 planning brief

Three shifts are converging, and each one amplifies the others.

1 Attack tempo

Automation lowers the effort required to research, target, and execute attacks. Defense must make containment a business process, not an analyst hero moment.

2 AI prompt risk

Employees can create a new data-loss channel simply by trying to work faster. Visibility and guardrails must arrive before broad adoption.

3 Consolidation risk

Mergers combine identities, vendors, workflows, and legacy systems. A common operating platform becomes a resilience strategy.

The attack economy is scaling faster than budgets

Reported losses are rising while tooling makes sophisticated fraud easier to industrialize.

\$20.877B

reported cyber-enabled crime losses
in 2025

+26%

year-over-year increase in reported
losses

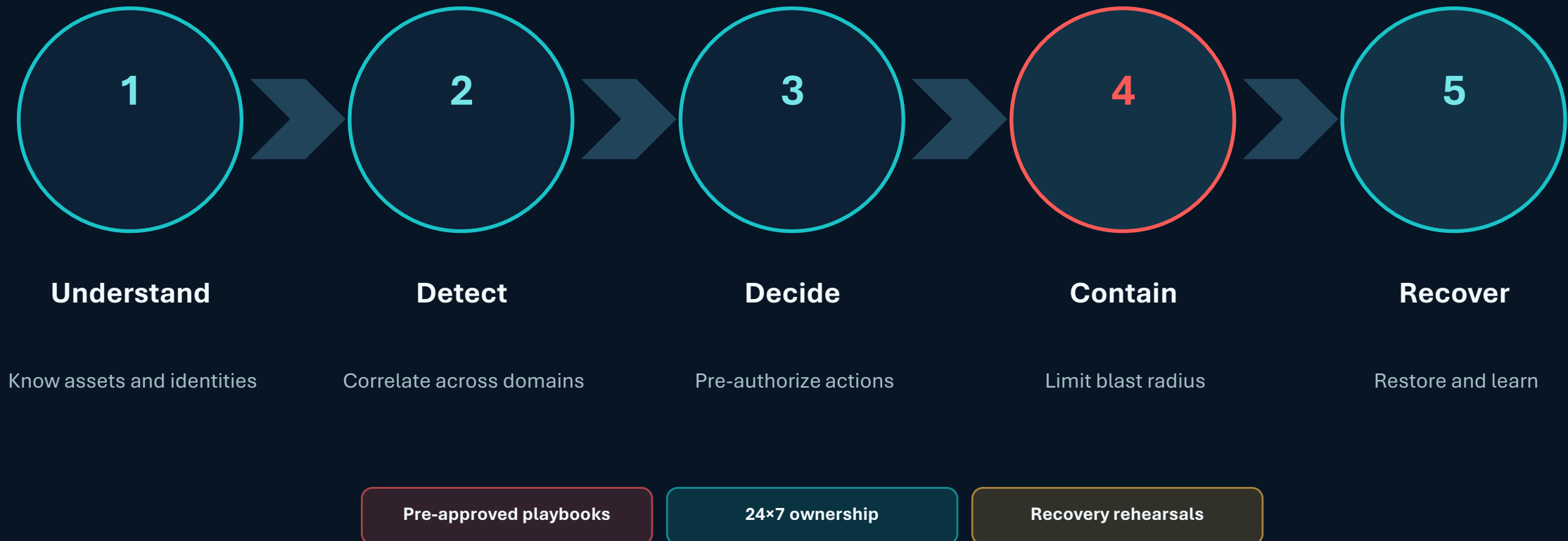
\$3.046B

reported business email
compromise losses



Faster attacks require a faster operating model

Speed is a design constraint across people, process, and technology.



Board-level metric: "How long until the business is safe again?"

AI prompt security: the new human data-loss path

The employee may be well-intentioned. The data can still cross a boundary.



What can leak

Member data • financial data • credentials • contracts • internal code

Why “just block it” fails

Teams will route around blanket restrictions when AI is useful and business pressure is real.

The control objective

Discover AI use, classify the interaction, and allow, warn, redact, or block based on risk.

Build an AI use policy employees can actually follow

Govern the interaction, not only the application name.

DISCOVER

Which AI tools are actually in use?

Inventory sanctioned and shadow AI usage.

CLASSIFY

What data and action are involved?

Separate public, internal, confidential, and regulated data.

ENFORCE

What should happen in the moment?

Allow, coach, redact, block, or require approval.

AUDIT

Can you reconstruct the decision?

Retain policy, user, application, and event evidence.

Employee rule of thumb

If you would not send it to an outside vendor, do not paste it into an unapproved AI tool.

Credit union consolidation can multiply cyber risk

A merger joins more than balance sheets. It joins trust boundaries.

Identity overlap

Duplicate accounts, roles, and privilege models

Legacy dependencies

Unsupported systems and hidden integration paths

Vendor sprawl

Inherited third parties and broken telemetry

Control inconsistency

Different patching, logging, backup, and response practices



Build internal IT around a platform, not a pile of tools

Standardize the operating model first. Integrate and retire technology second.

GOVERNANCE

Risk appetite • policy • evidence

IDENTITY

One identity model • least privilege • lifecycle

OPERATIONS

Asset inventory • patching • configuration • support

SECURITY

Telemetry • detection • response • recovery

DATA

Classification • retention • member privacy

Shared telemetry

Shared workflows

Shared accountability

A practical 90-day preparation plan

Start with decisions and evidence, not a shopping list.

0–30

Baseline

- Map critical services, data, identities, and vendors
- Measure containment and recovery time
- Inventory employee AI use
- Freeze high-risk merger changes

31–60

Design

- Define AI data classes and controls
- Pre-authorize incident playbooks
- Select platform standards
- Reconcile identity and admin roles

61–90

Exercise

- Run ransomware and data-leak tabletop
- Test restore and communications
- Pilot AI guardrails with real workflows
- Retire one redundant control path

Questions for leadership and the board

Use these to expose operational gaps before an incident or merger does.

1 What must be contained in 15 minutes, and who is authorized to act?

2 Which AI tools are employees using that we cannot currently see?

3 What confidential data is prohibited from entering external AI services?

4 Which inherited systems cannot meet our patching, logging, or recovery standards?

5 Can we restore critical member services without the primary platform?

6 Which third parties can materially disrupt multiple business services at once?

Three commitments for 2027

Make the strategy memorable and measurable.

1 OUTRUN

Design response around containment and recovery speed.

Measure:

- Time to decision
- Time to contain
- Time to restore

2 GOVERN

Enable AI productivity without surrendering confidential data.

Measure:

- Discovered AI apps
- Prevented disclosure
- Policy exceptions

3 UNIFY

Use consolidation to simplify controls, evidence, and accountability.

Measure:

- Redundant tools retired
- Identity exceptions
- Recovery coverage

Outcome: faster, safer decisions with less operational complexity.

WHAT WILL YOU CHANGE BEFORE 2027?

Questions & discussion

Attack speed • AI prompt security • Platform resilience