DOIT INFORMATION SECURITY

CYBERSECURITY AND RESILIENCY – INCIDENT RESPONSE OVERVIEW

AGENDA

- What is Incident Response?
- Auditing Incident Response Programs
- Focusing on Improvement
- Takeaways
- Questions?

DoIT
Illinois Department of Innovation & Technology

Which one describes your last security incident?

DoIT
Illinois Department of Innovation & Technology

WHY INCIDENT RESPONSE MATTERS

- Cyber security events are *inevitable*; chaos is not
- Response success depends on **people, process, and communication**, not just technology
- “In any moment of decision,
  - The best thing you can do is the right thing,
  - The next best thing is the wrong thing, and
  - The worst thing you can do is nothing.” – Theodore Roosevelt

DoIT
Illinois Department of Innovation & Technology

OPENING SCENARIO

"It's Monday morning – and nothing works. Ransomware has locked up your websites and call center…"

- Who acts first?
- Who communicates externally?
- Who are the right people to get involved?
- Who makes the decision on when to pay, or not to pay?

DoIT
Illinois Department of Innovation & Technology

INCIDENT RESPONSE (ABRIDGED)

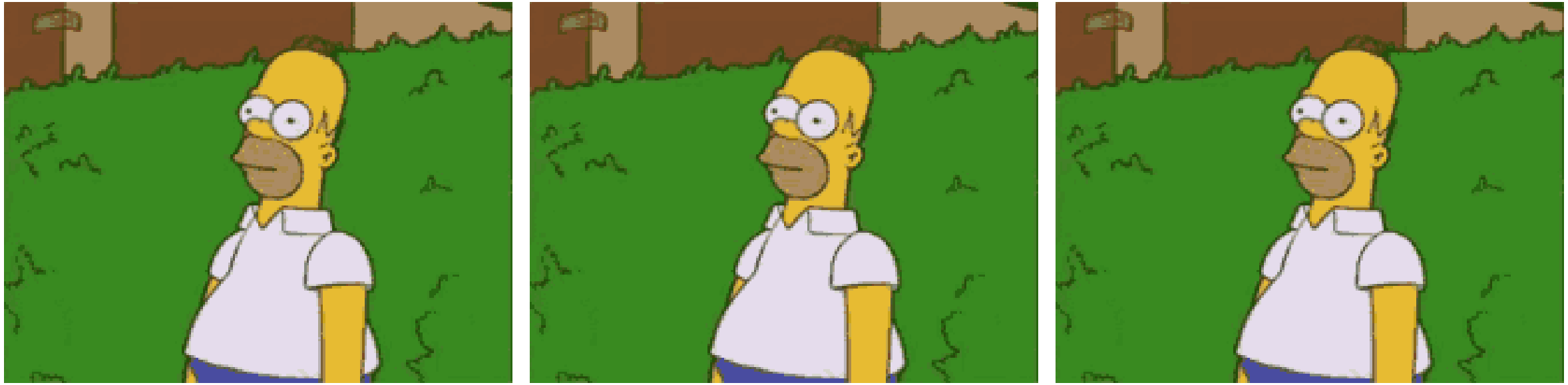
- Organizing people, decisions, and communication under pressure
- Not an IT process – incident response is a governance activity
- Why should auditors care?
  - Security incidents are a risk to the State providing service to residents
  - Incidents may bring legal exposure to the State
  - Incidents happen; how we respond to them builds or erodes trust

DoIT
Illinois Department of Innovation & Technology

INCIDENT RESPONSE LIFECYCLE (ACCORDING TO NIST)

- Phases
  - Preparation
  - Detection
  - Containment
  - Eradication
  - Recovery
  - Lessons Learned
- Incident Response isn’t linear

DoIT
Illinois Department of Innovation & Technology



When the same incident response finding shows up three years in a row

DoIT
Illinois Department of Innovation & Technology

WHAT AUDITORS SHOULD SEE

Phase	What Good Looks Like	Common Gaps
Preparation	Roles, Training, Testing	Outdated Plans
Detection	Clear Escalation Criteria	Unclear Thresholds
Containment	Defined Authority, Communication, Clear Success Criteria	Siloed Response, Absence of Containment Validation
Eradication	Defined Authority, Communication, Clear Success Criteria	Siloed Response, Absence of Eradication Validation
Recovery	Prioritized Restoration	No Linkage to BCP, DR Plans
Lessons Learned	Tracked, Updated	"We'll get to it", Fix Symptom vs. Systematic Issues

DoIT
Illinois Department of Innovation & Technology

Trying to reconstruct what happened when you didn't collect logs

DoIT
Illinois Department of Innovation & Technology

THE AUDIT LENS:

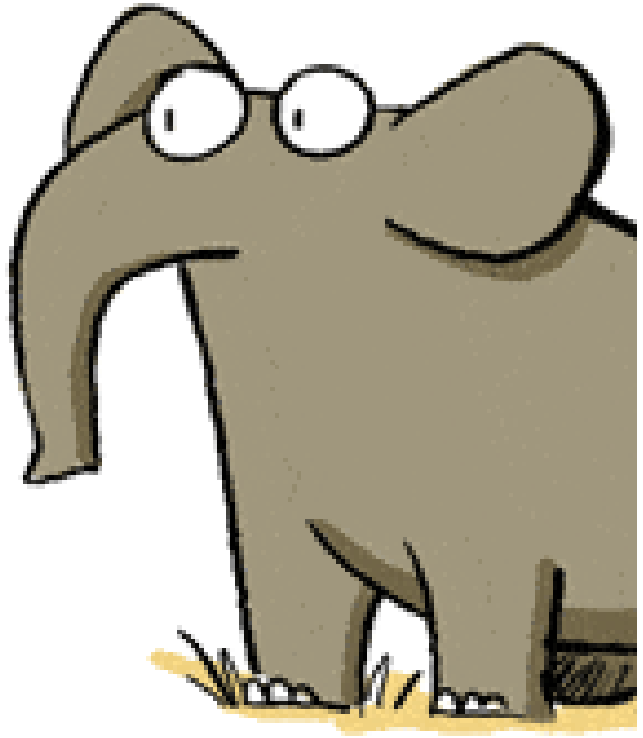
- Internal Audit evaluates:
  - **Governance:** Ownership, scope, authority
  - **Processes:** Testing, review cycles
  - **Evidence:** Logs, lessons, updates
- Improvement comes from identifying:
  - Gaps in coordination
  - Missing stakeholders
  - Lessons not implemented

DoIT
Illinois Department of Innovation & Technology

INCIDENT RESPONSE MATURITY LADDER

Level	Description	Indicators
Ad-Hoc	Reactive, no formal plan	Response depends on individuals
Documented	Policy and plan both approved	Roles defined, version control
Tested	Annual exercises, metrics	Cross-functional participation
Integrated / Evolving	Business and technical participation	IR, BCP, legal, comms, agency leadership all participate

DoIT
Illinois Department of Innovation & Technology



Illinois Department of Innovation & Technology

CASE STUDY

Scenario: Ransomware Event

- Before:
  - Written plan, not practiced
  - IT-led response
  - Lessons never tracked; isolated symptoms fixed
- After:
  - Annual exercises with executive support / involvement
  - Governance-led response
  - After-action reports drive updates

DoIT
Illinois Department of Innovation & Technology

Don't try to align incident response to <u>every</u> regulation – only what matters to the Agency

REGULATORY CONTEXT – WITHOUT THE OVERLOAD

- Frameworks to reference:
  - NIST CSF: Respond and recover
  - NIST SP 800-61 rev. 2: Computer Security Incident Handling Guide
  - Security Improvement Act; Other local regulations/statutes/requirements
- Key: Frameworks help define maturity – they don't dictate it

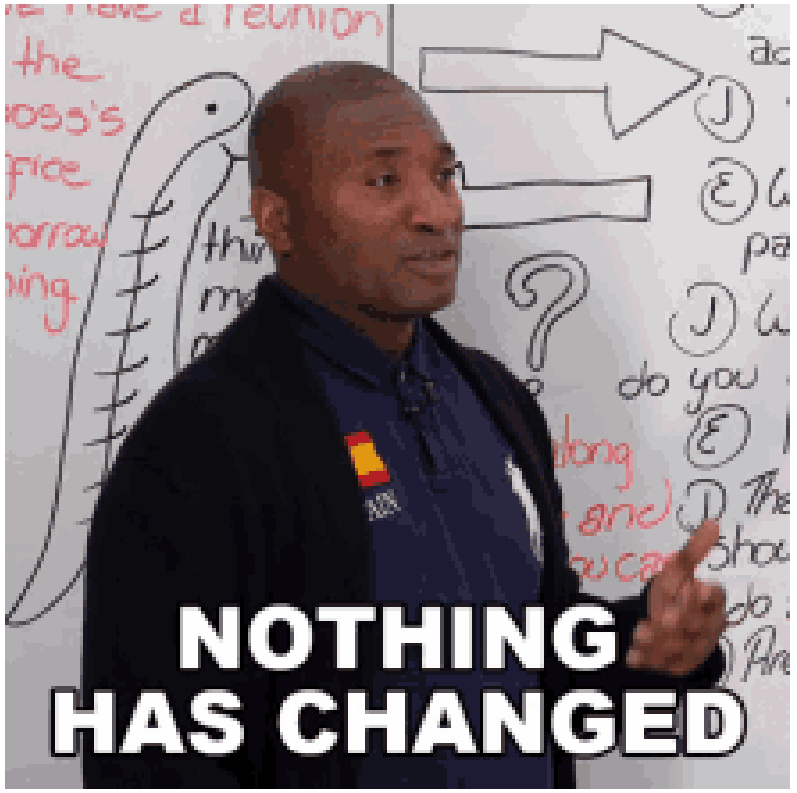
DoIT
Illinois Department of Innovation & Technology

Tabletop exercises – like a real life game

5 QUESTIONS TO ASK

- When was your incident response plan last tested OR when was your last incident?
- Are executive and communication roles documented and practiced?
- How quickly can the organization declare an incident?
- Are lessons learned tracked and implemented?
  - Broadly or specifically?
- How does incident response integrate with continuity and risk functions?

DoIT
Illinois Department of Innovation & Technology



Lessons learned…added to SharePoint…never read again

DoIT
Illinois Department of Innovation & Technology

CONTINUOUS IMPROVEMENT

Best incident response programs:

- Treat testing as normal business, not a special event
- Capture lessons, not blame
- Update the plan after every exercise
- Communicate outcomes organization-wide

DoIT
Illinois Department of Innovation & Technology

Post-incident report: “everything went as planned”

DoIT
Illinois Department of Innovation & Technology

REFLECTION

- What is one improvement you could recommend after your next audit?
- If an incident hit tomorrow, would your leadership know their role?
- What's one barrier to testing your plan – and how could you remove it?
- What is one question you wish I would have asked?

DoIT
Illinois Department of Innovation & Technology

TAKEAWAYS

- Incident response is organizational, not technical
- Auditors are catalysts for readiness, not compliance enforcers
- Testing transforms a plan into a capability
- Collaboration builds resilience and trust
- Offer to participate in the next plan

DoIT
Illinois Department of Innovation & Technology

QUESTIONS?

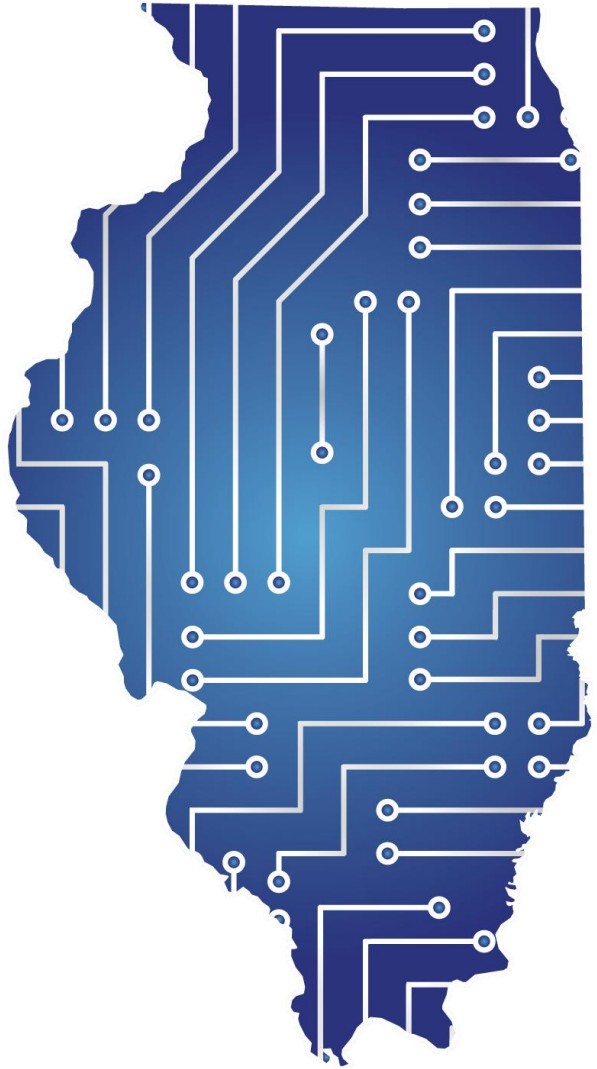
Illinois Department of Innovation & Technology

CLOSING & CONTACT US

- Jason Bowen:
  - jason.bowen@illinois.gov
- Ryan Lewis:
  - ryan.c.lewis@illinois.gov
- DoIT Security Operations Center:
  - DoIT.Security@illinois.gov

DoIT
Illinois Department of Innovation & Technology

THANK YOU!



Illinois Department of Innovation & Technology