BISHOP FOX

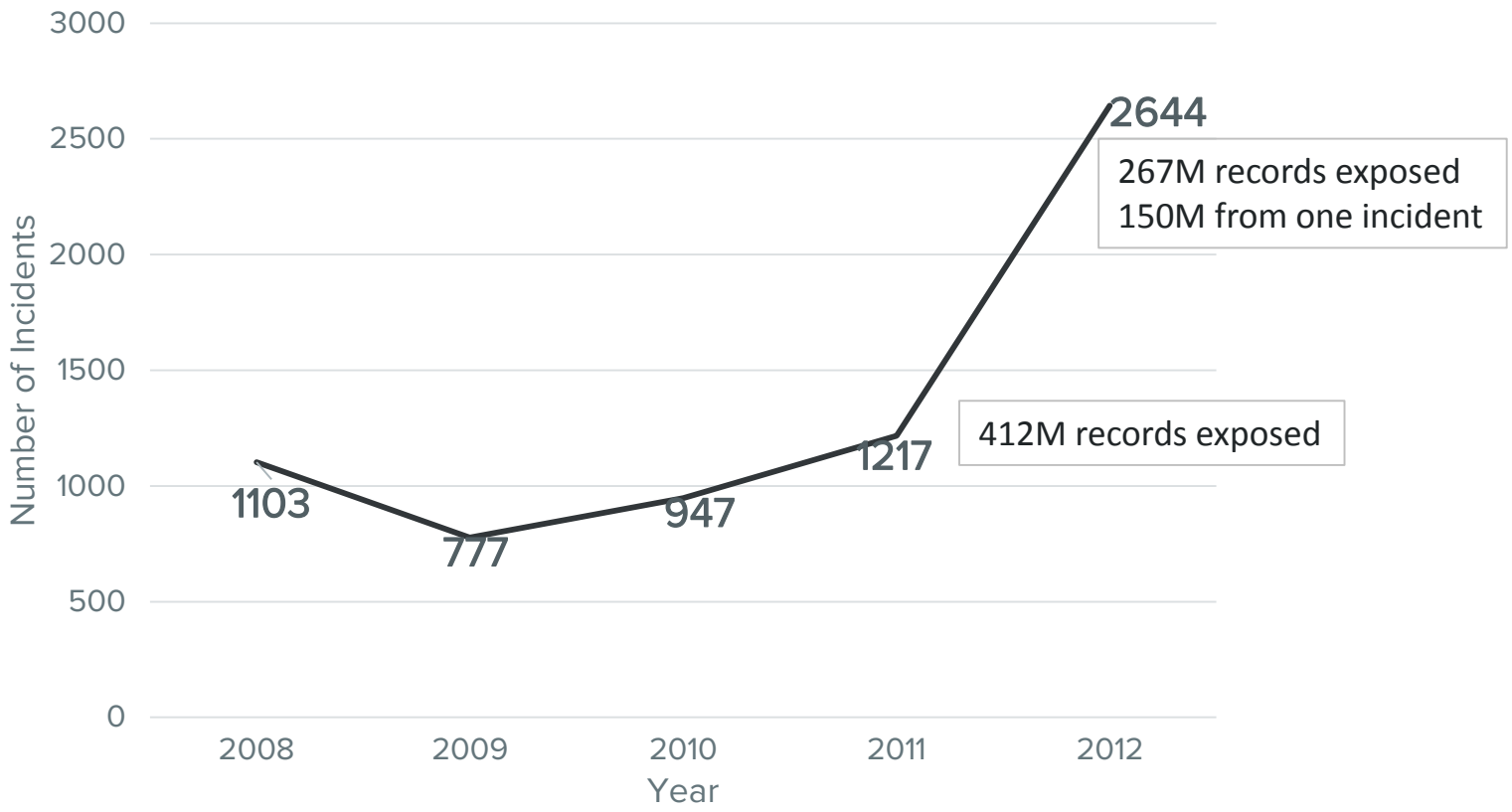
Are You Prepared?

HOW TO PREPARE FOR THE INEVITABLE

July 10, 2014

Breaches on the Rise

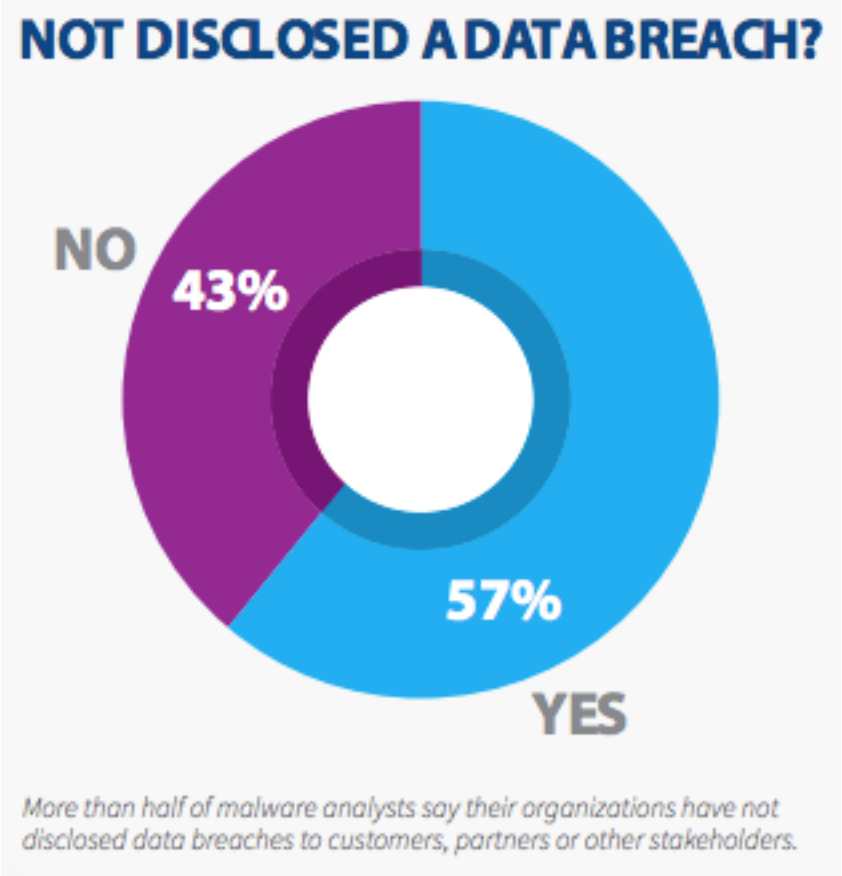
YOU CAN RUN, BUT YOU CAN'T HIDE



Source: Data Breach QuickView by Open Security Foundation and Risk Based Security LLC
http://www.riskbasedsecurity.com/reports/2012-DataBreachQuickView.pdf

Undisclosed Breaches

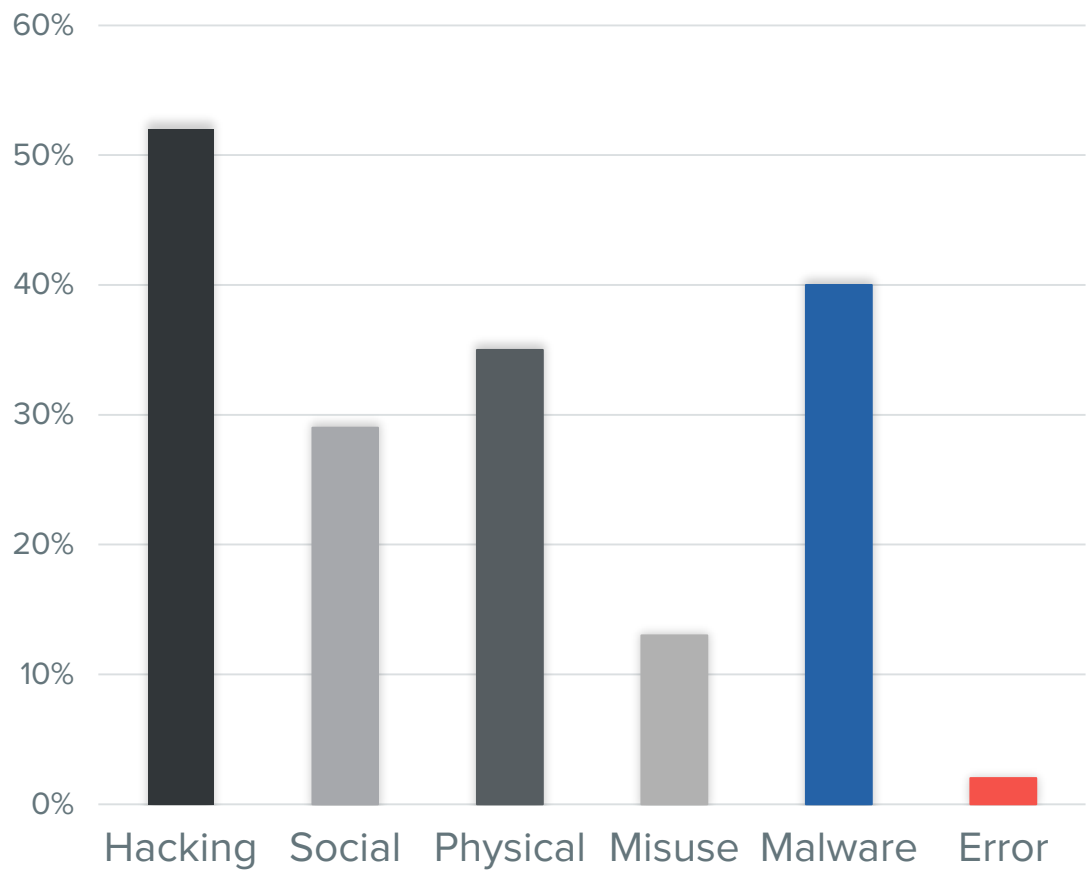
MOST BREACHES GO UNREPORTED



Source: Malware Analysts Have the Tools to Defend Against Cyber-Attacks, But Challenges Remain http://www.threattracksecurity.com/documents/malware-analysts-study.pdf

Incidents by Type

GREATEST RISKS



WHAT IS INCIDENT RESPONSE?

INCIDENT RESPONSE LIFECYCLE

Incident Response

INCIDENT RESPONSE PYRAMID

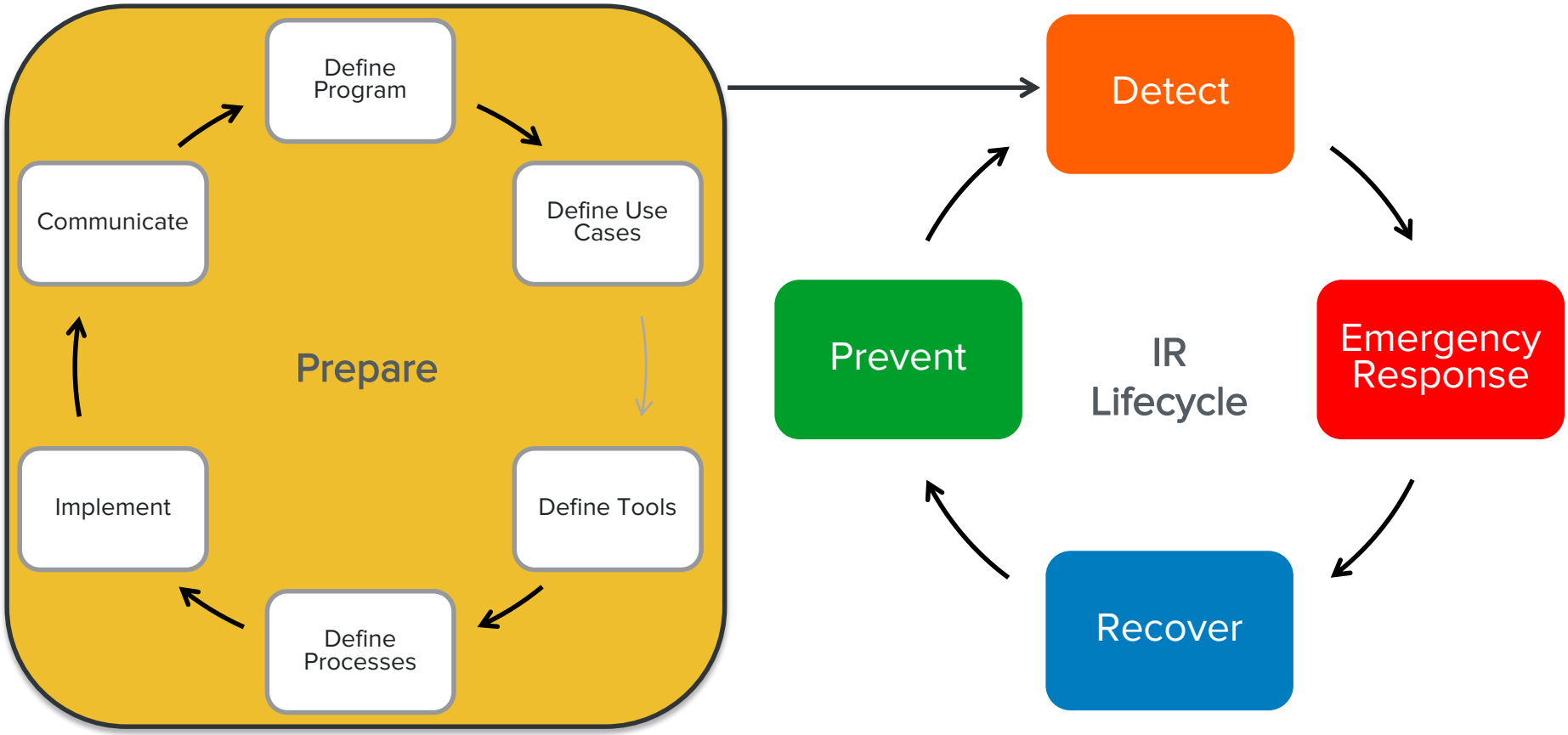
Where is my Hat?

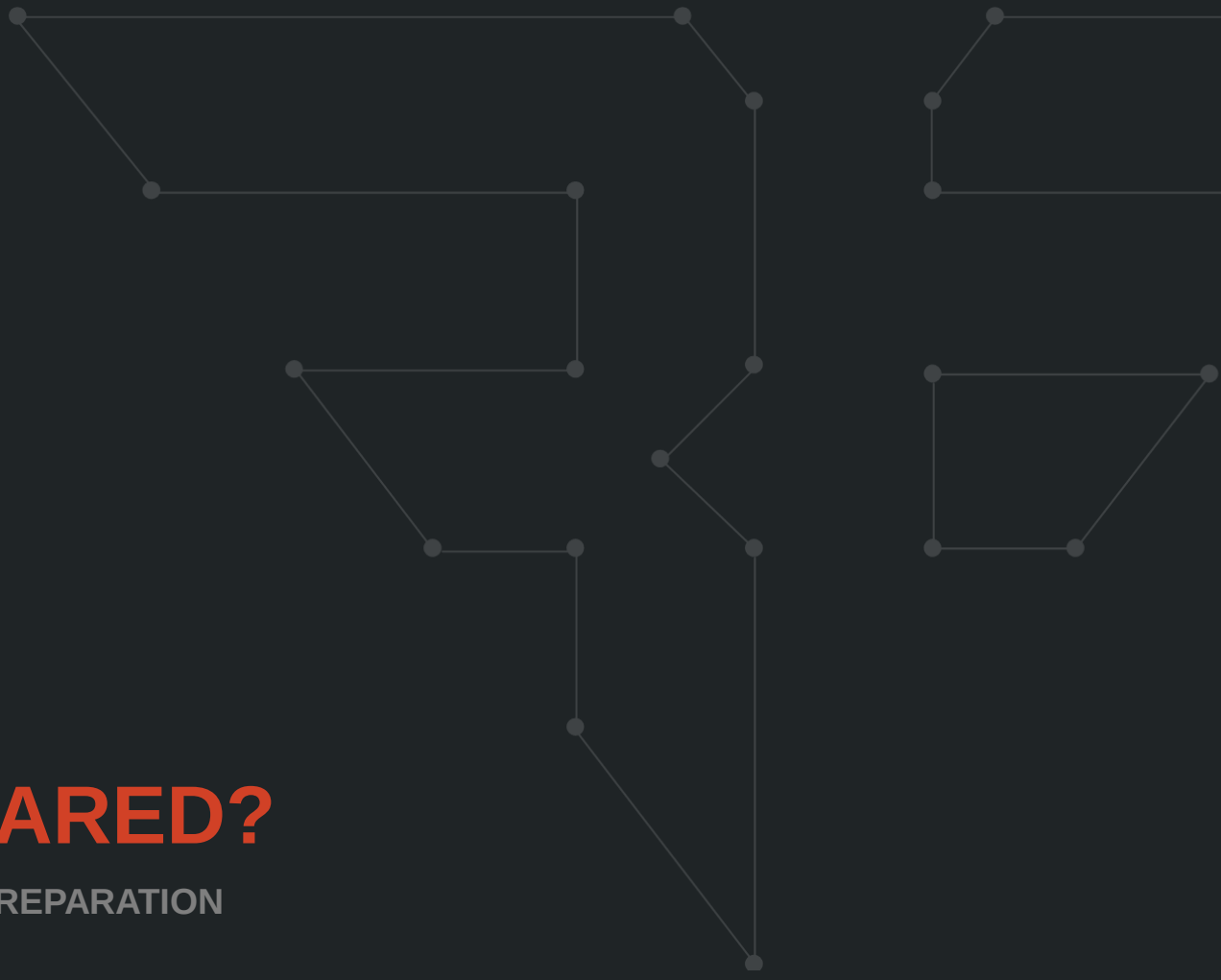
RESPONSE VS. HANDLING

	Response	Handling
Typical Duties	Technical Analytical Containment Remediation	Logistics Communication Coordination Planning
Typical Roles	System Admins Analysts	Legal Directors Public Relations Executives/Mgmt
Summary	Hands on the Keyboard	Jugglers

Preparation to Act

IR PREPARATION LIFECYCLE





AM I PREPARED?

INCIDENT RESPONSE PREPARATION

Which Framework is Best?

CHOOSE YOUR OWN ADVENTURE

Factors to Consider

- Completeness
- Flexibility
- Best Practices Recognition
- Organizational Size and Fit
- Customization

What is Incident Response?

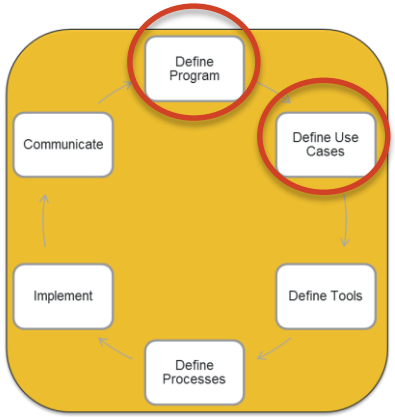
PROGRAM AND USE CASE

Program

- Strategy
- Scope
- Executive Buy In
- Get Out of Jail

Use Case

- What am I Looking For
- How Will I Find It
- What Tools Do I Need



What Do I Do?

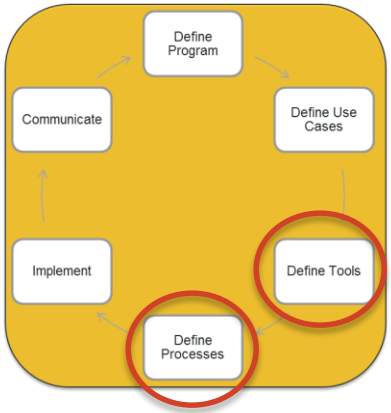
TOOLS AND PROCESS

Tools

- Log Collection
- Incident Tracking
- Response Tools
- Information Sources
- Insource/Outsource

Process

- How
- When
- What
- Who



Now What?

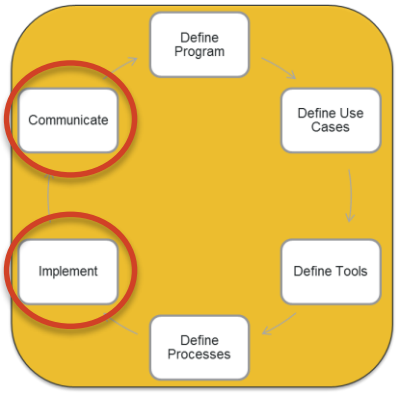
IMPLEMENT AND COMMUNICATE

Implement

- Install Tools
- Document Process
- Train Team

Communicate

- Executive Report
- Spread the Word
- How to Report an Incident



WILL THIS REALLY WORK?

INCIDENT RESPONSE TESTING

I’m Ready for My Close Up!

INCIDENT RESPONSE TESTING

How

- Table Top Exercise
- Penetration Tests
- Red vs. Blue Team

When

- Frequent
- Major Updates
- New Threats
- Unexpected

Pass or Fail?

TESTING RESULTS

Pass Updates

- Update Documentation
- Areas of Improvement
- Add New Use Cases

Fail Updates

- Review the Response
- Praise the Good
- Correct the bad

CAN I ACHIEVE PERFECTION?

CONTINUAL IMPROVEMENT

Good, Better, Best

CONTINUAL IMPROVEMENT

Improve

- Update Documentation
- Refine Processes
- Tune Tools
- Update Training

Add

- Use Cases
- More Logs
- Additional Tools
- New Signatures

Blocking All the Things

"ZERO" INCIDENTS

Think about the Metrics

- If you have zero incidents you are missing something.
- As the number of identified incidents decrease, you should add more detection capabilities.
- Always strive to balance the number of incidents with the ability to respond.
- There is always something under the rocks you pick up.

NEXT STEPS

ONE STEP AT A TIME

Tomorrow is a New Day

STRATEGIC NEXT STEPS

Preparing for incident response is a process and not just a checkbox.

Having an incident response plan is great but testing will validate if it works.

Attackers are not standing still. Continually improving your response capabilities will increase the effectiveness of your incident response.

Thank You

BISHOP FOX®