Practice makes perfect

> Using micro-exercises to stay on top of your game

James Allman-Talbot, Head of Cyber Incident Response

BAE SYSTEMS
INSPIRED WORK

Practice makes perfect

You wouldn’t run a marathon without training

You wouldn’t sit an exam without revising

You wouldn’t respond to a cyber attack without practicing

... or would you?

BAE SYSTEMS
INSPIRED WORK

Incident response

☒ Responding to incidents is not a tick box exercise

☒ Every incident brings its own challenges

☑ Successful response requires speed, agility, and preparation

BAE SYSTEMS
INSPIRED WORK

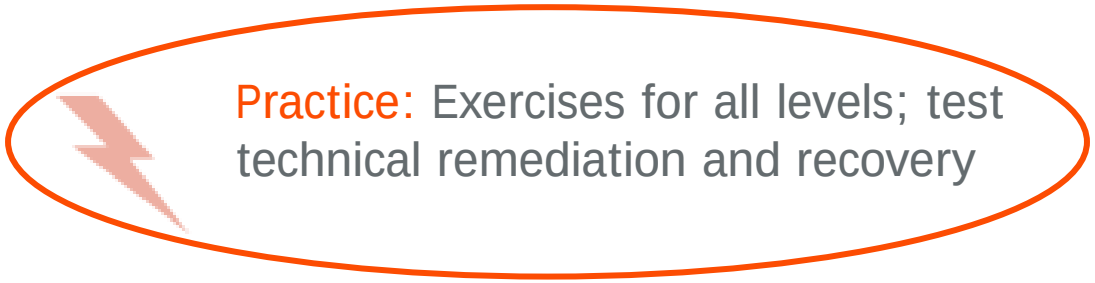
Preparing to respond

Plan & process: Crisis and Incident Response plans, checklists; pre-prepared communications

Resource: Experts on standby – Incident Response teams, public relations, legal

Investigation and Remediation: Capabilities, people and the right data

Threat aware: Understand risks and impacts and how to mitigate them



Practice: Exercises for all levels; test technical remediation and recovery

Authorities: Who makes those critical decisions and when are they available

Systems and data: Understand your estate's critical data and systems

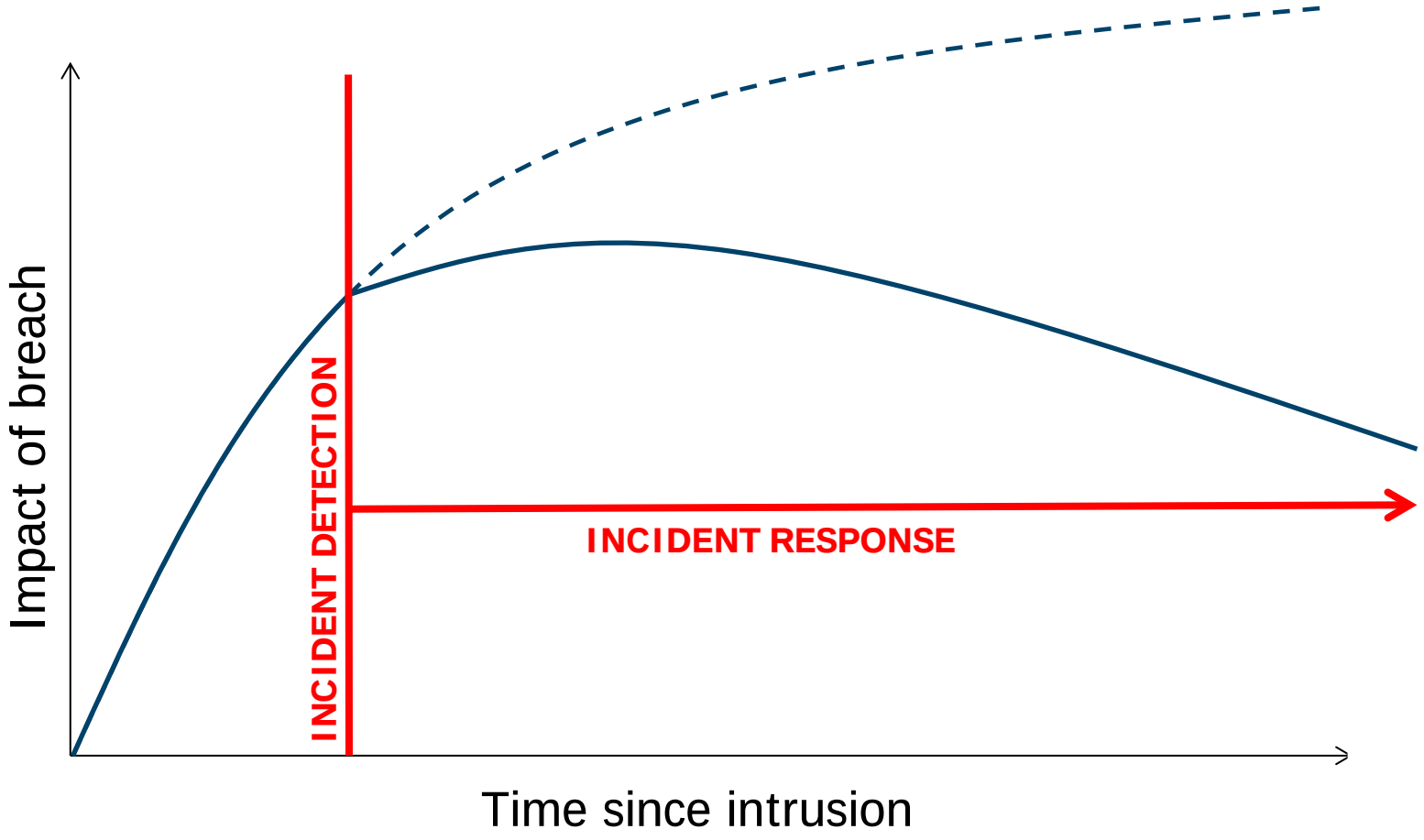
Legal / Regulatory: Understand what you have to report/do and when

BAE SYSTEMS
INSPIRED WORK

Why practice?

- Develops organizational muscle memory
- Ensures everyone is aware of their responsibilities (and others)
- Tests the process
- Helps review and refine the process

Benefit of Incident Response



BAE SYSTEMS
INSPIRED WORK

So... practice?

Exercise

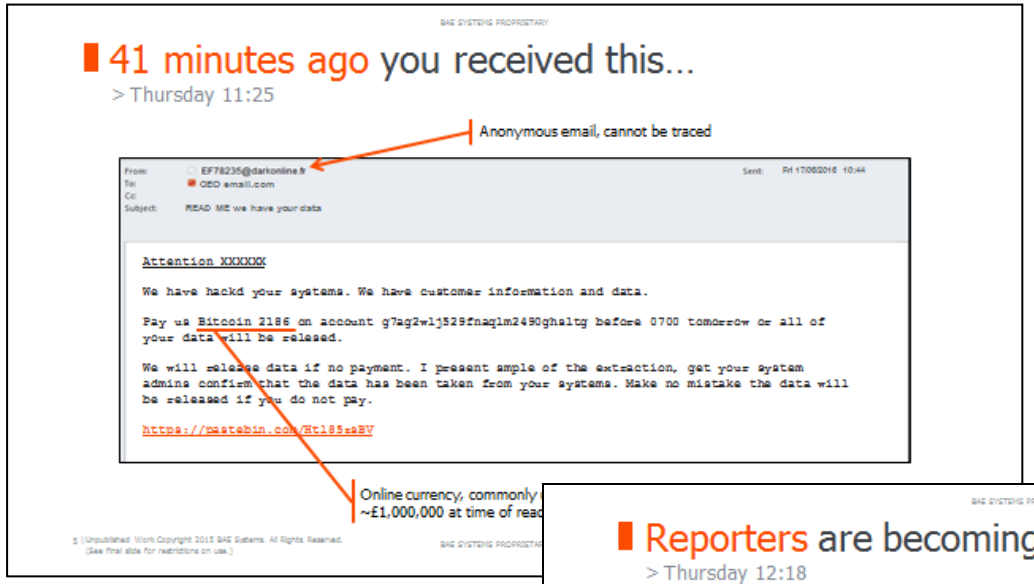
Condensed scenario for both technical staff and C-suite execs, run separately. Designed to run through a realistic scenario in a 3-4 hour session and test knowledge of plans, or encourage awareness.

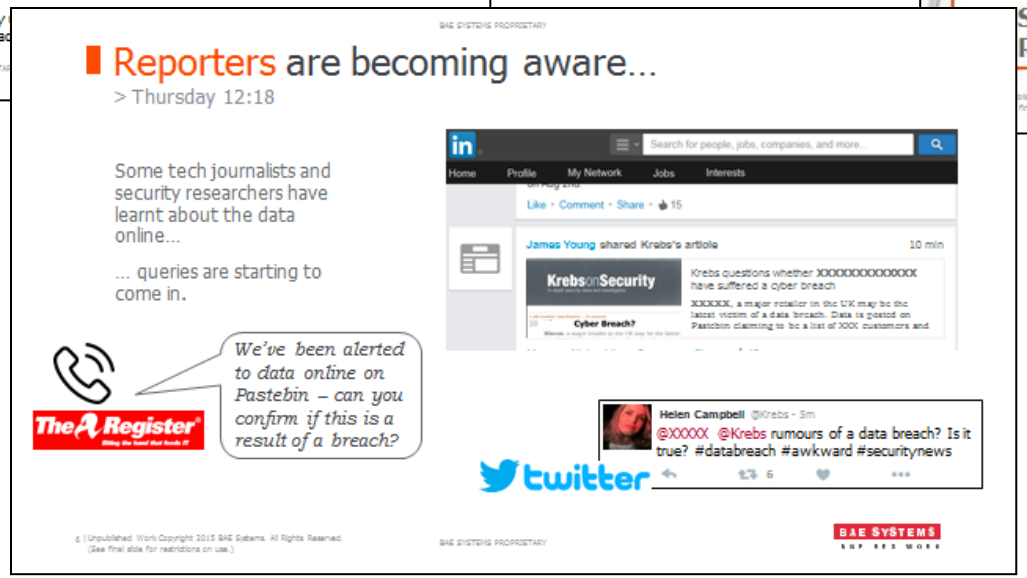
Wargame

Red-teaming, but includes Crisis Management response. Designed to put plans in to practice and test their suitability and feasibility from every angle. Typically run over 3-4 days, possibly longer.

BAE SYSTEMS
INSPIRED WORK

Incident Exercises





BAE SYSTEMS
INSPIRED WORK

Three reasons to exercise

Raise Awareness

- Highlights the need for a process if one is not in place
- Typically only at C-level
- Designed to highlight holes and encourage board buy-in

Test the Process

- Tests the suitability of a process after it is developed
- Usually at CMT/technical level
- Designed to put the process through its paces

Exercise the Process

- Builds awareness and muscle-memory
- Usually at all levels, including tech and C-level
- Designed to bring familiarity to the process and ensure participants are aware of responsibilities

BAE SYSTEMS
INSPIRED WORK

Three reasons not to exercise

Time

Blocking out 3-4 hours is difficult, especially with C-Suite execs.

Cost

Exercises take a lot of preparation, logistical planning, and expertise.

Fatigue

Getting one exercise done is hard enough, repeating the process can be tedious.

BAE SYSTEMS
INSPIRED WORK

What do we do?

Introducing....

Micro-Exercises

BAE SYSTEMS
INSPIRED WORK

Two types

Pre-planned

- 1 hour exercise
- Delivered over WebEx
- Choice of 3-4 scenarios
- Designed to raise awareness to board members or wider business

Spontaneous

- The ‘Fire Drill’ option
- Short scenario of pre-defined length
- Delivered over WebEx, at a random unplanned time
- Incidents never happen at an appropriate time...

BAE SYSTEMS
INSPIRED WORK

Pre-planned micro-exercises

Pre-planned micro-exercises allow organizations to test Crisis Management Teams, without the cost or logistical overhead.

For more mature organizations, allows for a simple test of an established process.

For less mature organizations, raises awareness of a potential lack of preparedness.

Spontaneous micro-exercises

You run yearly fire drills, do you run yearly cyber drills?

Cyber drills provide a realistic test of your cyber incident management process.

Builds muscle memory, and ensures an effective response when the time comes.

BAE SYSTEMS
INSPIRED WORK

Spontaneous exercises - planning process

1. Determine the length and content of the scenario
2. Identify the point of escalation
3. Agree approximate timeframes
4. During one of the time windows, we will engage the incident through the agreed process
5. Crisis Management Team convenes and dials-in to our WebEx, where we will run the session

Comparison

	Traditional Exercise	Micro Exercise
Cost	$40,000 - $80,000	$12,000 - $27,000
Logistics	4-5hrs in duration Delivered in-person at one location	1hr in duration Delivered remotely over WebEx
Target Audience	Can be tailored to all audiences	Useful for C-Suite execs and Crisis Management Teams, less useful for tech teams
Scenario Selection	Custom scenario tailored to your business	Selection of 3-4 scenarios relevant to all sectors

Key messages

An effective response lowers costs and mitigates risks

Cyber exercises are a key component of an organizations preparedness to respond effectively

Micro exercises allow exercises to be run more often, at lower cost, and with less logistical overhead

BAE SYSTEMS
INSPIRED WORK

Questions?

BAE SYSTEMS
INSPIRED WORK

BAE SYSTEMS
Surrey Research Park
Guildford
Surrey
GU2 7YP
United Kingdom

T: +44 (0)1483 816000
F: +44 (0)1483 816144