Top 5 Challenges & Mistakes in Breach Detection and Response

RSA

What you will NOT hear from me today...

Next-Gen Anti-Virus ?

Secure Web Gateway ?

Malware Sandboxing ?

Next-Gen Firewall ?

Application Whitelisting ?

The Five P's

Lack of Practice

- Do you have an incident recovery plan?
  - The plan exists…but it is not up-to-date
  - Exercising the plan – tabletop “live drill” exercises
  - Know your stakeholders – this is not just a technical remediation
- Other wrinkles in “the plan”
  - Format (online, physical, location) of the plan
  - Out-of-band communications during an incident

Misreading the Punch

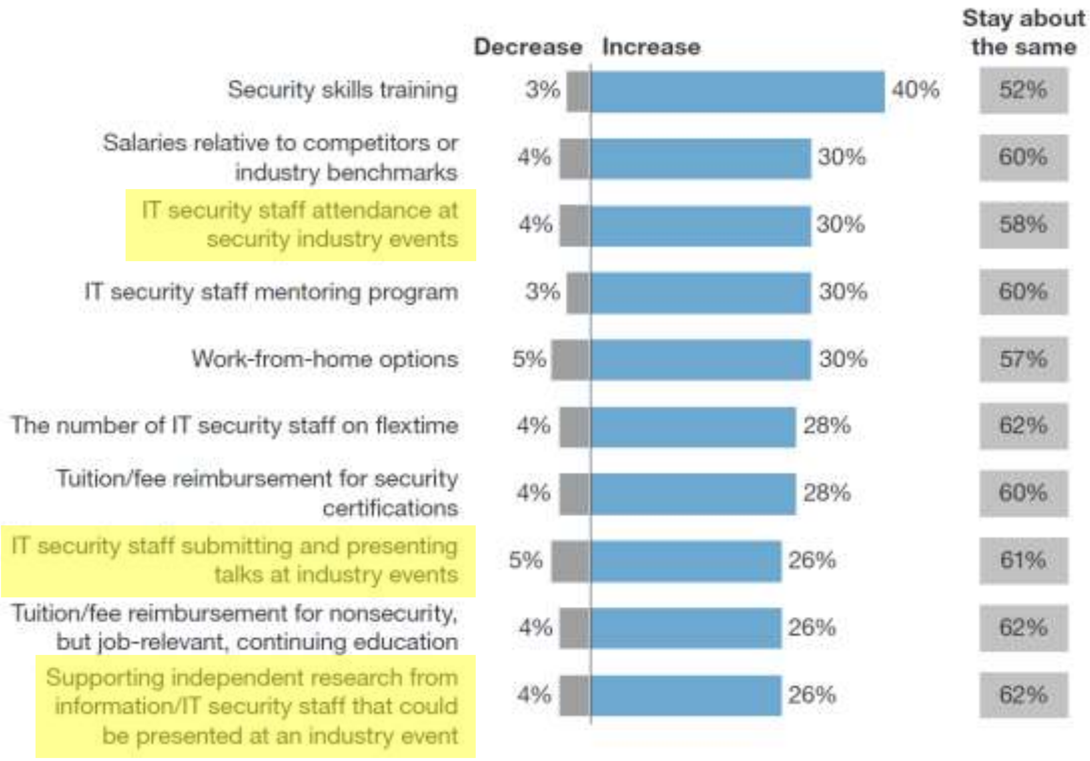
- Measuring the true impact to the business
  - Business context
  - Asset criticality
    - What is an “asset” anyway?
- The “small fire, large fire” attack

People Aren’t Cogs in a Wheel

- Job rotations for personnel
  - *Benefit:* address skills shortage, career path aspirations
- “Champion” or “mentor” designation where appropriate
  - *Benefit:* peer recognition/respect without a formal promotion
- MSSPs (managed security solution providers)
  - *Benefit:* skills transfer during/end of engagement
- Hiring (sourcing) *vs.* retention – which is harder?
  - Keep the bench warm/filled at all times!
- All of your employees are members of your extended security team!

People Aren’t Cogs in a Wheel

“Thinking about what your company is doing to attract and retain IT security professionals, how do you expect the following policies to change at your company over the next 12 months?”



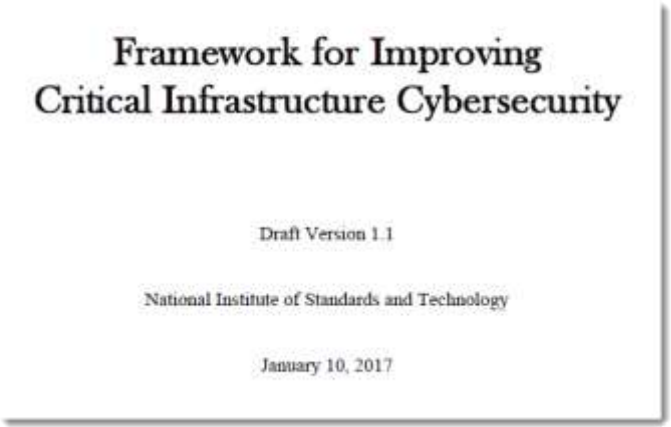
Forrester, “Maintain Your Security Edge: Continuous Improvement – The Security Architecture And Operations Playbook” (Mar 2016) [61487]

The Partner-to-Target Vector

- Supply Chain risk

[Hackers Lurking in Vents and Soda Machines](#)

The Partner-to-Target Vector

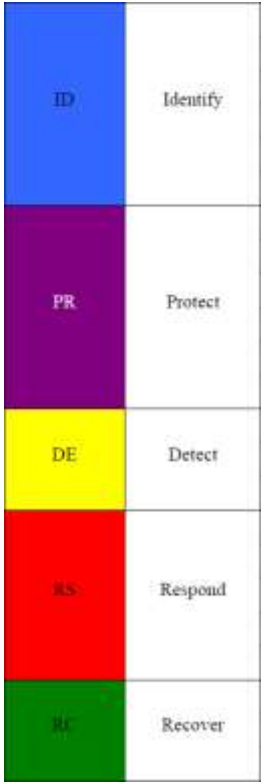


Framework for Improving
Critical Infrastructure Cybersecurity

Draft Version 1.1

National Institute of Standards and Technology

January 10, 2017



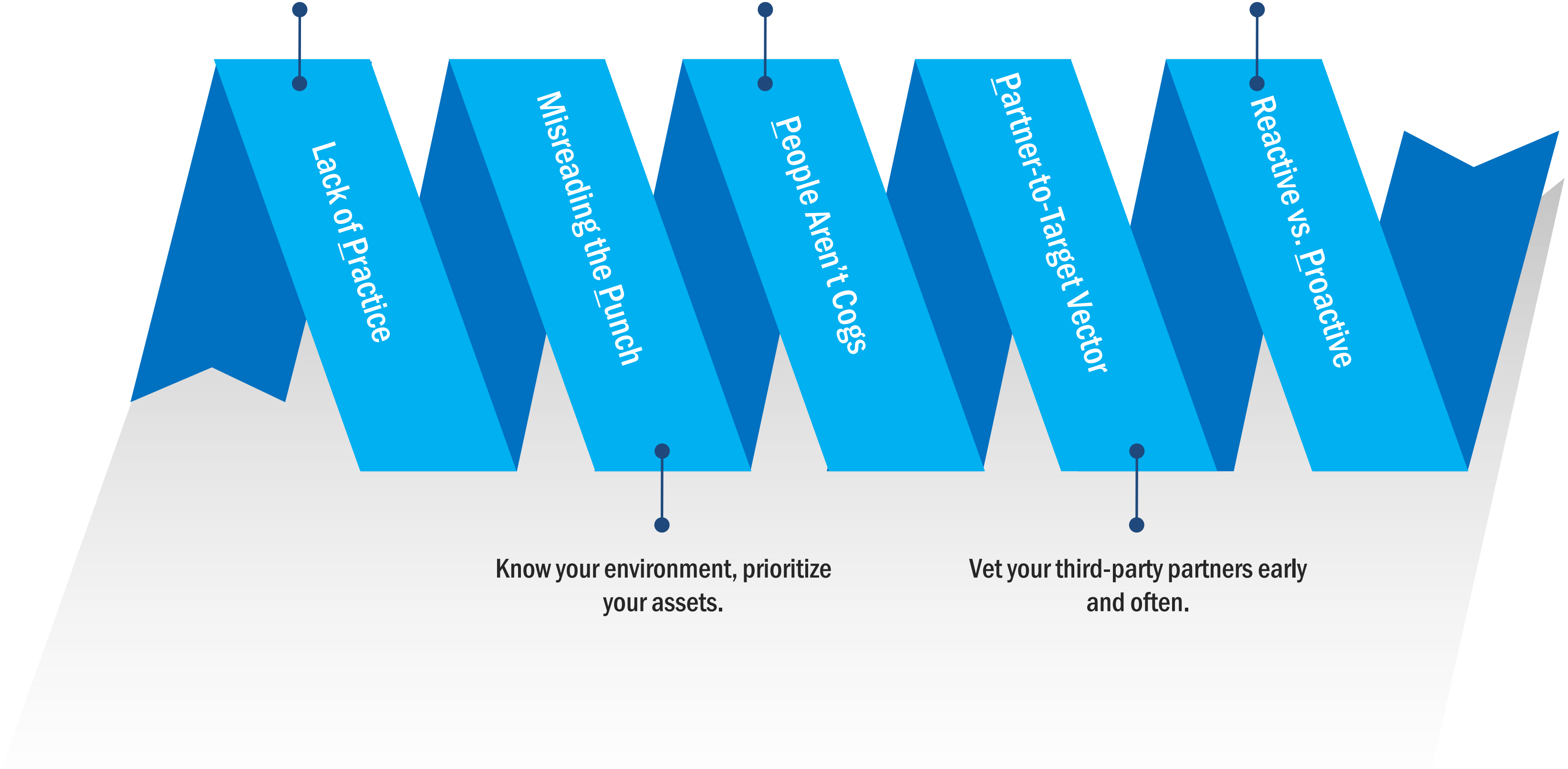
ID	Identify
PR	Protect
DE	Detect
RS	Respond
RC	Recover

NIST Cybersecurity Framework Draft Version 1.1

Reacting vs. **Proactively** Hunting

- Reacting, reacting, reacting to alerts?
  - Alert fatigue; false positives; paralysis by analysis
- Time to detection
  - Minimizing the adversary’s “dwell time” within your environment
  - Lateral movement
- The “right” skills in your hunters
  - Curious; passionate; love to unravel mysteries
  - Knowledgeable about your environment
- True situational awareness = comprehensive visibility

The Five P's



Prepare through tabletops involving all groups.

Job rotations can be an effective retention tool.

Active hunting grows your analysts & finds badness.

Know your environment, prioritize your assets.

Vet your third-party partners early and often.

RSA