RSA Conference2016
San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

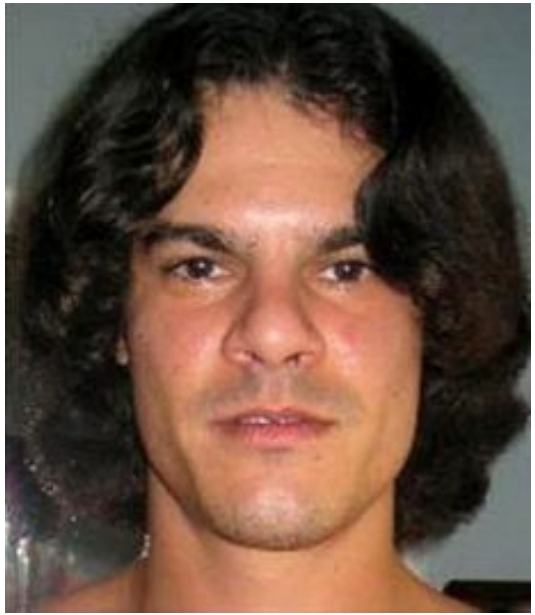
SESSION ID: **CRWD-W09**

Breach Fixation. How Breaches Distort Reality and How Should We Respond?

John B. Dickson, CISSP
Principal
Denim Group, Ltd.
@johnbdickson

#RSAC

Anybody Remember this Guy?



His New Home

Why is this Important?

The day security became important to business executives

Breach Fixation Overview

- What is Breach Fixation?
- How Does Breach Fixation Manifest Itself?
- How you can Use Breach Fixation to Your Advantage

Breach Fixation Overview

Breach Fixation

- A phenomena created by media fixation on breach stories
- Breach Fixation distorts reality by putting most of the focus on external activities that we don't control…
- At the expense of internal security activities that we do
- Affects strategy and resource allocation in a potentially negative way
- Takes focus away from addressing the root cause while treating the symptom

What Drives Media Consumption?

Breach Fixation

- Does anyone know the top security stories consumed by readers of the major security publications?

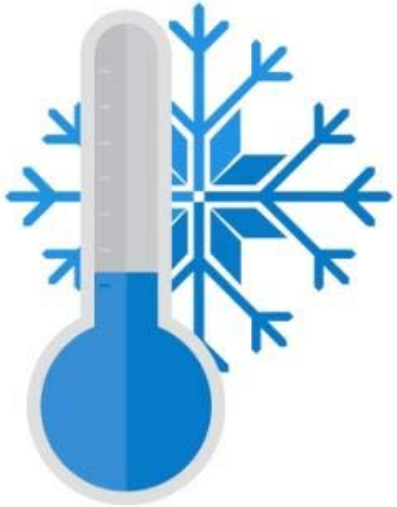
A Rubbernecking Culture?

What's Hot in Security

- Breaches
- APT & Zero Days
- External Threats
- Cyberwar
- Russians, Chinese, Iranians, oh my!
- Finding Vulnerabilities

What's Not…

- Internal Security Practices
- Coding Standards
- Patch Management
- User Awareness
- Actually Fixing Vulnerabilities



What Does that Create?

- A Situation Where Basic Security Blocking & Tackling Remains Problematic
  - Window of Exposure of Application Vulnerabilities Remains Egregious
  - Well-known Security Weaknesses Continue to be an Avenue of Approach for Attackers
  - Outside the largest and most sophisticated organizations, security only covers a subset of the enterprise

What Does that Create?

- A Situation Where External Threats Might Distract Security Focus
  - Whipsawed by #ToD (Threat of the Day) or #YABS (Yet Another Breach Story)
  - “Incumbent Spend” around FW, Endpoint, AV, dwarf other areas
  - Focus on latest outwardly-focuses security “shiny rock” technologies as panaceas

The Risk?

- Returning to a FUD Culture…

Examples of Impact

- Press DDoS on speaker by the entire media
- Gartner: By 2020, 60% of enterprise information security budgets will be allocated for rapid detection and response approaches, up from less than 20% in 2015.
- EY: A Shift to “Active Defense” and its implications
- A cautionary tale: State of Texas Public Utilities Commission war story

How Can You Address Breach Fixation

- Recognize Breach Fixation When a Layperson (e.g., “Executive”) References it.
  - The First Step to Recovery is Admitting you have a Problem!

How Can You Address Breach Fixation

- Constantly Quantify Internal Security Posture
  - Measure, measure, measure

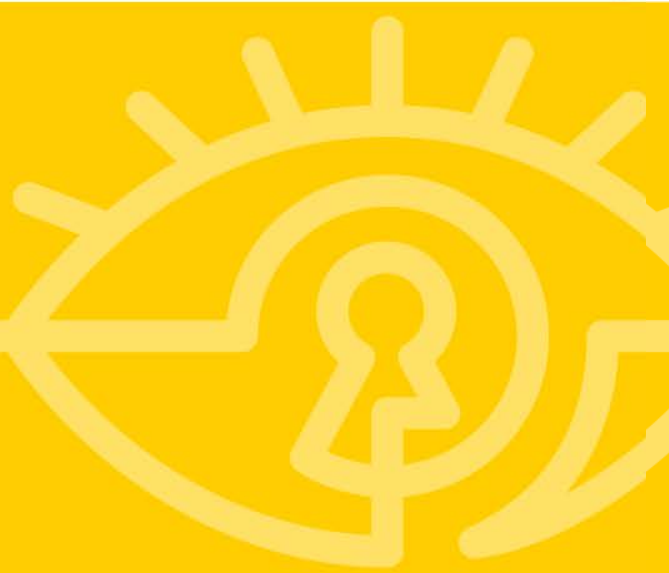
How to Use Breach Fixation to Your Advantage

- Use the Positive Force from the Attack Side & Map to Your Strategy

Other Strategies Use Breach Fixation…

Wrap up

- Breach Fixation distorts reality by putting most of the focus on external security activities that we don't control at the expense of internal security that we do.
- Sophisticated security practitioners understand how Breach Fixation can help or hurt them, if not managed
- Once recognized, there are several basic strategies that one can use to take advantage of Breach Fixation



Questions and Answers…

Subhead if needed