OΣQ

Cyber Security Management
ISSA – DC Chapter

April 19, 2016

© 2015 OEQ, Inc. All Rights Reserved

Cyber Security Management

The next 55 minutes…

- Establishing the context
- Cyber Security Management
- Getting a ‘Handle’ on things…
- Cyber Risk Management
- How do you …
- Reference Architecture
- Q & A

© 2015 OEQ, Inc. All Rights Reserved

Establishing the context…

The multi billion dollar WILD GOOSE CHASE?

- **200%** 0 Days in 2016, compare with 125% in 2015
- **40%+** techniques not attributable
- **60%+** cyber crime focused, this number is increasing…
- **125%** Increase in 10M + Identity Exposure Hacks
- **429M** Total Identities Exposed in 2015
- **$500B** Impact of Cyber Attacks
- **88%** CEOs worried about Cyber Threats

Its not a question of 'IF' only 'WHEN' you will be Hacked…

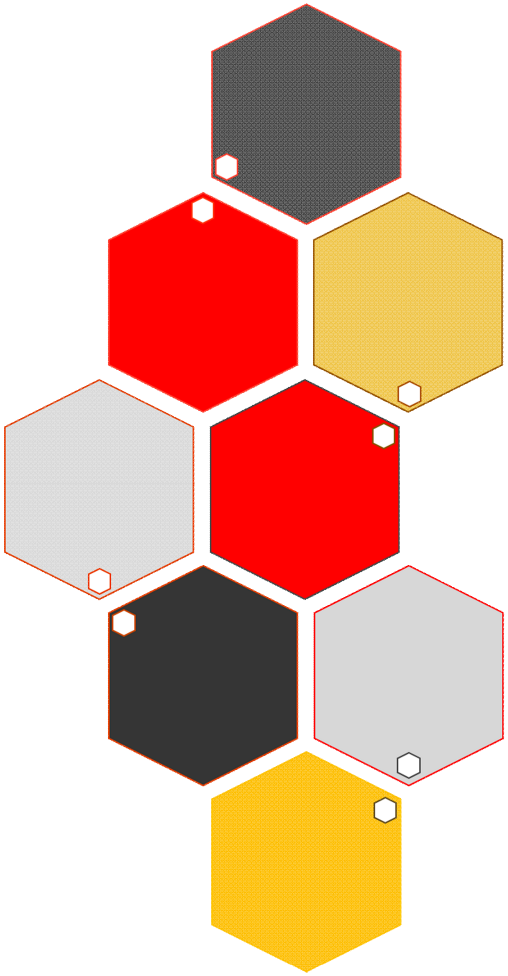
- The Cyber Security Community

© 2015 OEQ, Inc. All Rights Reserved

Cyber Security Management

Building blocks…

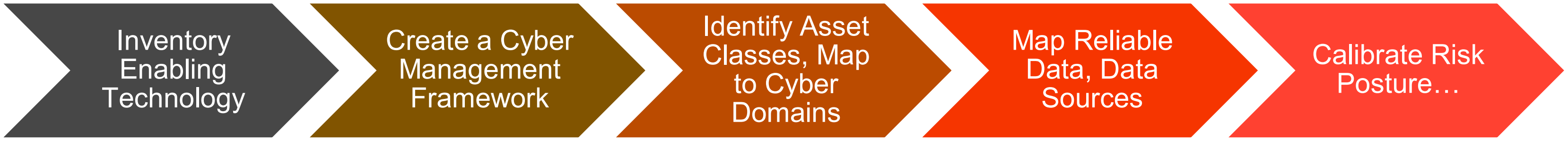
- **The Usual Stuff:**
  - Tone at the Top
  - Organizational Alignment
  - ‘World Peace’
- **Technology Hygiene**
  - Secure Infrastructure
  - Proactive Compliance
  - Monitoring / SIEMs etc.
- **The Innovative Stuff**
  - Analytics for Cyber
  - Risk Posture Analysis
  - Effective Cyber Security Metrics



© 2015 OEQ, Inc. All Rights Reserved

Getting a ‘Handle’ on things…

Where do you start…



Inventory Enabling Technology

Create a Cyber Management Framework

Identify Asset Classes, Map to Cyber Domains

Map Reliable Data, Data Sources

Calibrate Risk Posture…

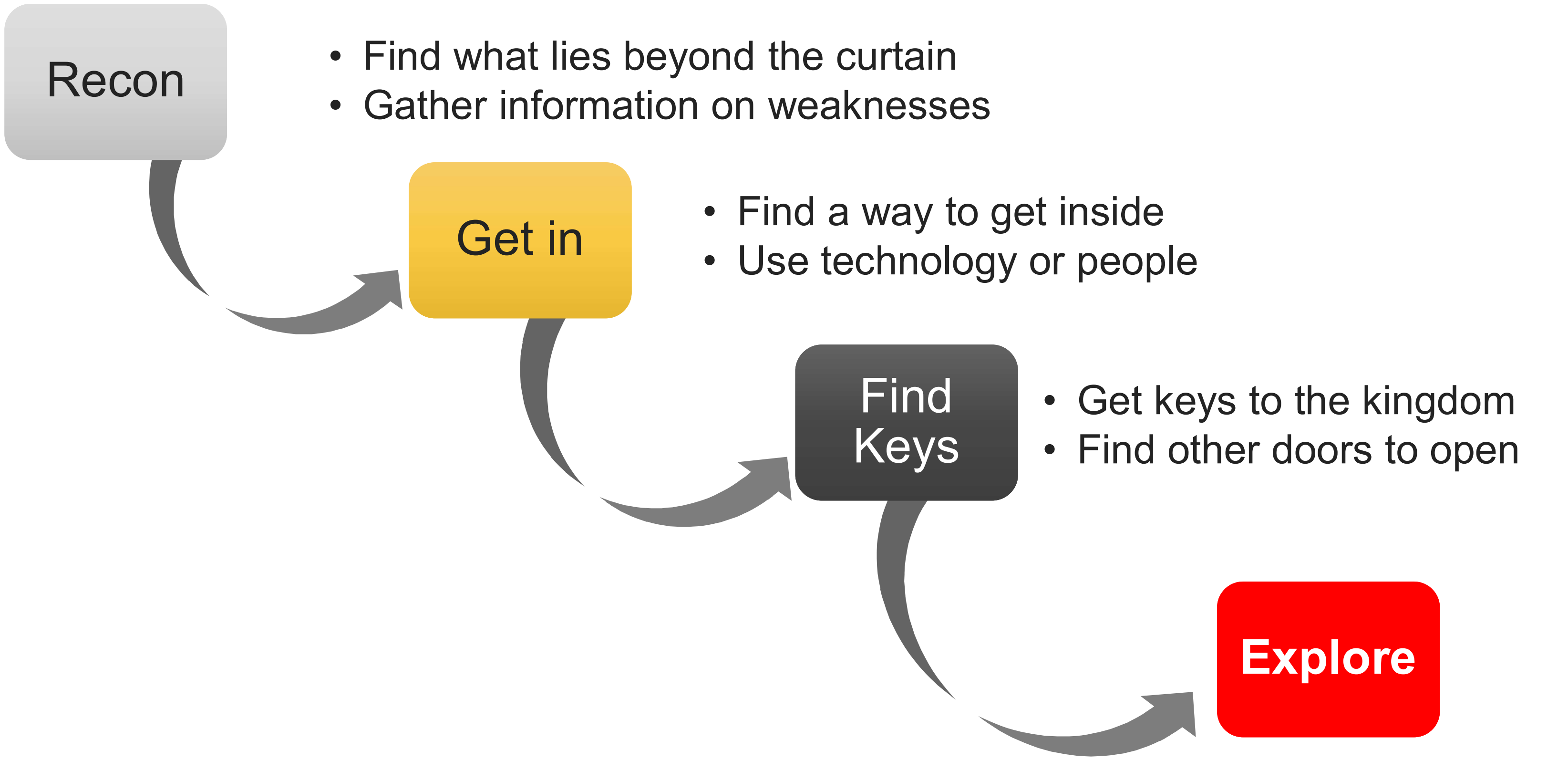
- Organizations often invest in a plethora of tools and technology. Include all GRC, SIEM, Access Controls, Change & Configuration Management as well as Security Log Management Software
- Technology Maturity vs. Organizational Maturity
- Technology Sophistication vs. Ease of Use
- Remember if buying a piece of technology could have solved the ‘Cyber Security’ challenge, we would not have had the challenge to begin with…

The case for change first begins with the acknowledgement of a problem / need…

© 2015 OEQ, Inc. All Rights Reserved

Getting a ‘Handle’ on things…

The anatomy of a hack



Recon

- Find what lies beyond the curtain
- Gather information on weaknesses

Get in

- Find a way to get inside
- Use technology or people

Find Keys

- Get keys to the kingdom
- Find other doors to open

Explore

© 2015 OEQ, Inc. All Rights Reserved

Getting a 'Handle' on things…

Case Studies

Case #1

The Strange Case of Transactional Monitoring

Case #2

I've got Access… Privileged Access!

Case #3

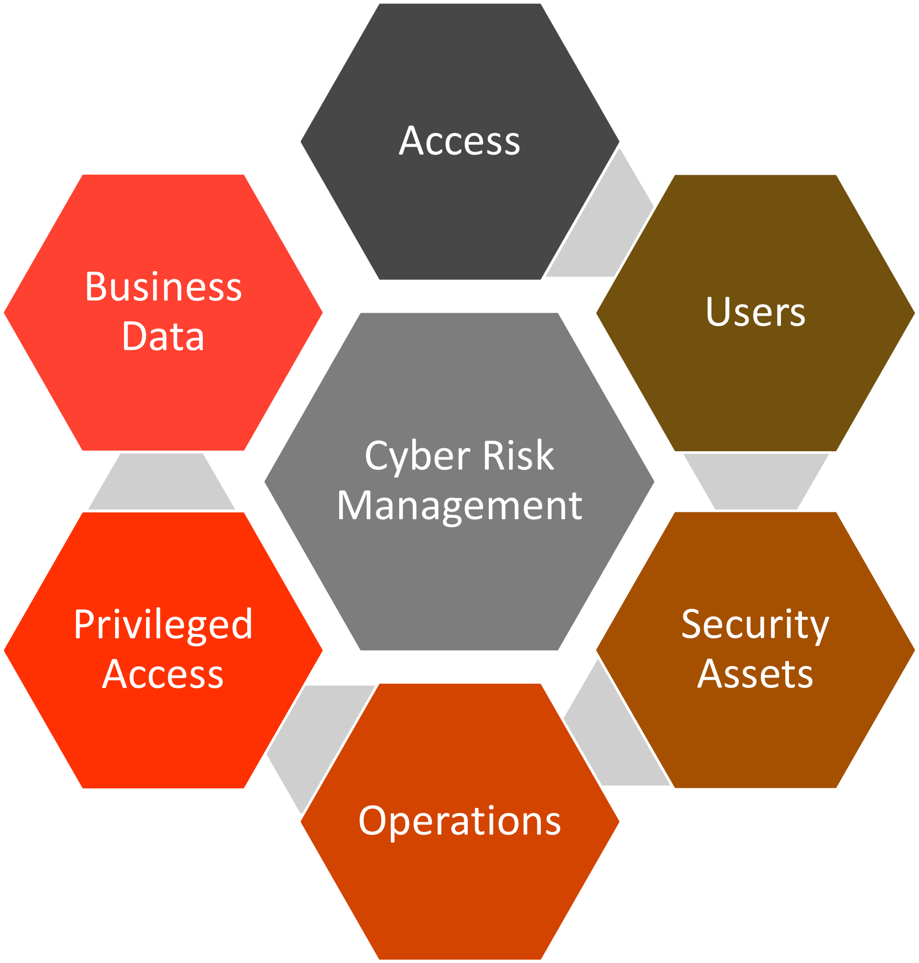
We use Advanced Analytics

Image © Unixmen.com used under creative license

© 2015 OEQ, Inc. All Rights Reserved

Cyber Risk Management

Understanding Cyber Risk



Access

Users

Security Assets

Operations

Privileged Access

Business Data

Cyber Risk Management

© 2015 OEQ, Inc. All Rights Reserved

Cyber Risk Management

Measuring Cyber Risk

Establish Objectives, Priorities

- What are we protecting, and Why?
- Risk / Cost / Value manifestation
- Third Parties, Outsourcing
- Strategy, Revenue, Legal impact
- Where the power is…
- Wall Street Journal First Page Items

Identify Impacted Assets

- Sound asset management
- Every asset is on the Internet
- People are assets too
- Audited vs. Unaudited Assets
- Ignored Assets
- End User Computing

Measure Risk

- Risk Metrics
- Gathering data, connecting the dots
- Aggregating Risk Metrics
- Monitoring Risk Posture
- Normalizing Risk Posture
- Operationalizing Risk Posture

Link to Financial Numbers

- Current spend, alignment to risk
- Opportunity price of spend
- Under served areas of risk
- Areas with excess risk coverage
- Cost of Mitigating the Risk
- Time required to Mitigate Risk

© 2015 OEQ, Inc. All Rights Reserved

How do you…

Cyber Security Management, Analytics in Action…

© 2015 OEQ, Inc. All Rights Reserved

Questions?

Krish Krithivasan
***President & CEO*,**
OEQ, Inc.

Krish.Krithivasan@oeq-inc.com