The Human Element of Cyber Security
Overview

- Who We Are
- The Evolution of Cybersecurity
- The Human Element of Cybersecurity
- How to Address the Human Element
- Q & A
Who We Are

Former offensive operators from the CIA, NSA, and FBI

We specialize in developing holistic cybersecurity and insider threat programs from the offensive perspective
The Human Element of Cybersecurity

Attackers will always take the easiest, most effective method for gaining access.
Traditional boundaries have shifted; companies operate in a dynamic environment that is increasingly interconnected, integrated, and interdependent.

- Organization are **built around a model of open collaboration and trust**
- Constant **information flow is the lifeblood of the business ecosystem**

**Trusted parties have access to more information than ever before**
In 2015, the most prevalent successful attack types hinged on the human factor.

*2016 ISACA, State of Cybersecurity

- **95%** Of all security incidents involve human error
  *IBM 2014 Cyber Security Intelligence Index

- **60%** Phishing
- **41%** Social Engineering

*2016 ISACA, State of Cybersecurity
Changing Employee Behavior Reduces Risk of Security Breach by 45% to 70%...

... *The Last Mile in Cyber Security; Aberdeen Group*

... The Good ...

... or they can be your best line of defense

Turn you employees into proactive sensors
Yet companies are still more focused on outside threats …

- **Outsider threats**
  - 32% Of insider attacks are more costly than outsider attacks

- **Insider threats**
  - 71% Of insider attacks involving IP had an impact of over $100,000
  - 48% Of insider attacks involving IP had an impact of over $1,000,000
And their defenses reflect that focus

55% of breaches are blamed on insiders – anyone who has physical or remote access to a company’s assets. *IBM 2015 Cyber Security Intelligence Index

28% Of respondent victims couldn’t determine if the incident was caused by an insider or outsider. *US State of Cybercrime Survey, 2015
How to Address the Human Element

There is no solution that will be able to completely protect you
Any solution must be holistic and balanced

People
Provides the skills and changes one’s behavior

Process
Tells you what to do and how to do it

Technology
Protects you and enables you to do it
People
Education & Training

76% Less is spent on security events when employees are trained\(^1\)

YET

54% Do NOT provide security training for new hires\(^1\)

1 US State of Cybercrime Survey 2014
People
Education & Training

Threats
Vectors
Policies
Resources