Prove it!

Gaining Confidence Through Effective Cyber Security Training.

Jeff Arsenault
Director

Noah Powers, CISSP
Senior Associate

March 2016

Who we are

Jeff Arsenault

- US Air Force Reservist, Cyberspace Ops
- 15+ years cyber operations
- Penetration Testing
- Red Teaming
- Cyber Exercises

Noah Powers

- Prior US Air Force
- 10+ years intelligence operations and cyberspace
- Red Teaming
- Cyber Exercises
- Operational Assessments

Delta Risk Background

- Established in 2007 by cadre of former military cyber warfare operators – became affiliate of The Chertoff Group in 2015
- Focused on the application of methods and approaches from the national security arena to evaluate and improve Cyber operational readiness in the private sector
- Global provider of focused strategic advice, Cyber defense and security risk management solutions

Nothing has changed in 20 years

“insufficient awareness and understanding of information security risks among senior agency officials”

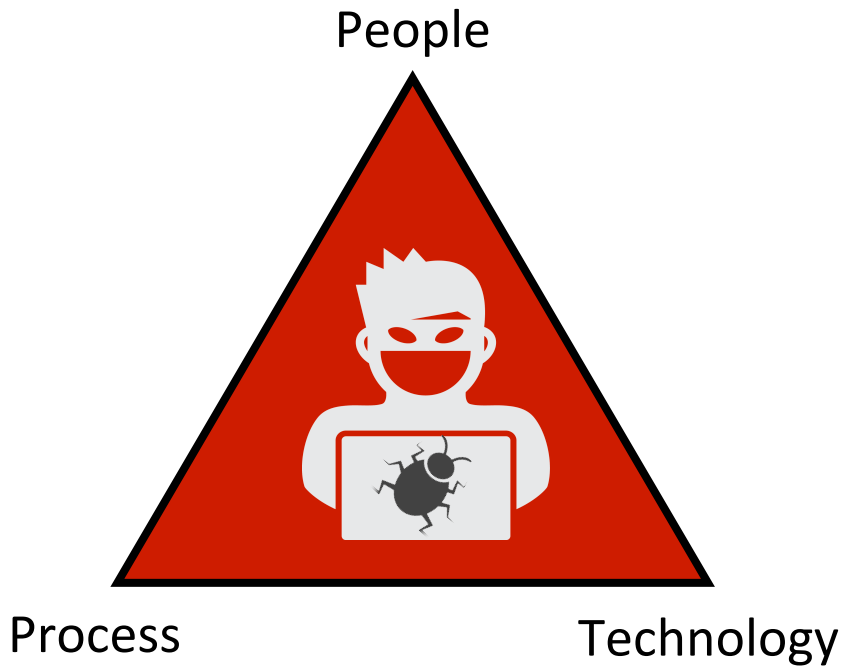
“poorly designed and implemented security programs that do not adequately monitor controls or proactively address risk”

“shortage of personnel with the technical expertise needed to manage controls in today’s sophisticated information technology environment”

GAO/HR-97-30

We Believe…

- Security is about interactions
  - People
  - Process
  - Technology
- Adversaries target these interactions
- Vendor agnostic training
  - Sorry, [insert vendor name here]!



Quest for the Unhackable Human

Increasing Penetration of Enterprise Network Defenses

Denial of Service, Hijacked Sessions, Web Defacements, Viruses & Malware, Known or One-Off Exploits

Stealthy Infiltration, Embedded Malware & Agents, Social Engineering, Zero-Day Exploits, Rapidly Changing

Hacker Groups

Hacker

Script Kiddies

State-Supported

Corporate / Criminal

Cyber Terrorist

Hacktivists

"1st Generation" Information & Network Security

- Security by prevention
- System & software vulnerability assessment
- Penetration testing
- Respond to most-recent event
  - Effectiveness rarely assessed
  - Prepared for the "last war"
- Hyper focus on technology & compliance

Emerging "2nd Generation" Threats

- Quickly evolving; seeks asymmetric advantage
- Persistent & patient; waging long-term campaigns
- Structured organization & planning
- Well-resourced (money, people, skill)

Unhackable Human

- Theoretically speaking…
  - Knowledge of malicious and non-malicious
  - Understanding of the consequences (organization and person)
  - Experience to do what is right at all times

Unhackable Technology and Processes

- Perfect cyber security would never rest solely on human operation
- Building an Unhackable Human would close the front-door to attackers, who would find another non-human way in
- Humans need to write as if unhackable were obtainable
  - Better, more concise and secure code
  - Documented and tested operational processes
  - Security as a forethought

What we are seeing most often today…

- SOCs and CISOs…
  - Security Operations Centers and Chief Information Security Officers
  - Well-intentioned, but sometimes under-staffed and under-resourced
  - Some aspects can be outsourced – but risk and strategy should not
- An inevitable breach – the savvy ones no longer expect their defenses to hold.
  - Companies are seeking help with procedures for handling and managing the incidents; testing and exercises are their most effective weapon

Unhackable isn't a factor in risk calculations

- Leaders and managers want less damage
  - Faster detection, reaction, remediation
  - Better communication and awareness
- Leaders and managers want confidence in their people, and to be informed
  - Confidence in the trusted experts
  - Confidence technology is well implemented and secure
  - Confidence hacking won't destroy the organization/reputation

Current training efforts build knowledge

- Realization learning comes before application
- Bootcamps largely focused around building knowledge and understanding something
- Knowledge gained is benchmarked against common body
  - May lead to a certification (proof)

A bridge too far…

- Knowledge Certifications
  - "I know what I'm doing, because I have this cert."
- Let's be fair
  - Certifications do hold value, but do not translate into performance
- Spectrum
  - Knowledge  Experience
- Training to experience increases confidence

Confidence, not Over-Confidence

- Confidence is a *belief* in a choice/decision/process
- Over-Confidence can
  - Mislead leaders and co-workers
  - Damage
- Confidence triad
  - Know
  - Understand
  - Experience

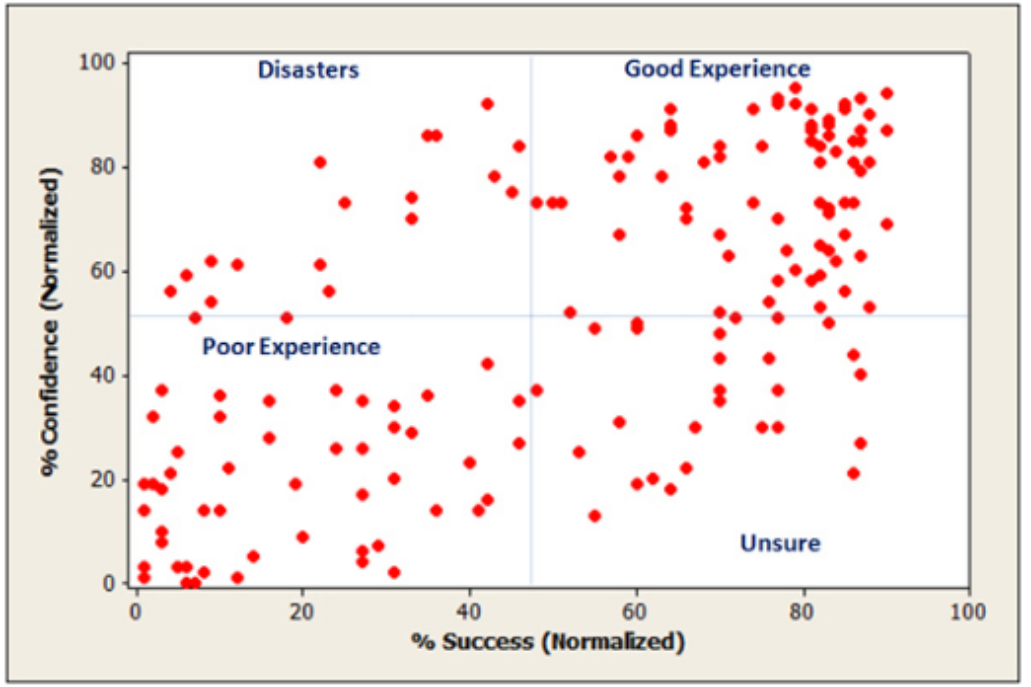


Image from http://www.measuringu.com/blog/ui-disasters.php

Our Approach to Building Confidence

- Job task-based, emphasizing team work
- Realistic
- Varying levels of difficulty
- Never try and show our smarts, but allow students to demonstrate theirs
  - To themselves
  - To co-workers
  - To leaders

Train how you (cyber) fight

Exercise-training must be realistic.

- Military
  - Live-Fire
  - Replica towns with streets and buildings
- Law Enforcement
  - Practicing arresting aggressive people
  - Practice citing irritated people
  - Walk-through hostage scenarios
- Firefighters
  - Burn replica aircraft and buildings, put out fire and save dummies with real-life body weight/mass
- Emergency Medical Staff
  - Robotic simulations of medical conditions

- Cyber Exercises-based Training
  - Bare-metal or virtual machine environment
  - Realistic enterprise architecture with replica internet
  - Replicated user traffic simulation (web/email)
  - Realistic services within the enterprise
  - Adversarial presence that mirrors actual, modern threats
    - May use actual malware
  - Provide a realistic mission to cyber defenders with tasks they have to respond to
  - Allow defenders to operate as they would outside exercise

Training & Evaluation Combined Approach

Position-Specific Individual and Team Training

Beginner to Advanced Levels

Recurring Training on Latest Threats

- Security Analytics
- Monitoring & Detection
- Security Architecture
- Network Defense
- Digital Forensics
- Threat Intelligence
- Adversary Tactics

"Threat of the Month Club"

- Latest threats, attacks
- Learn Detection, response, mitigation
- Constantly updated based on threat intel

Training

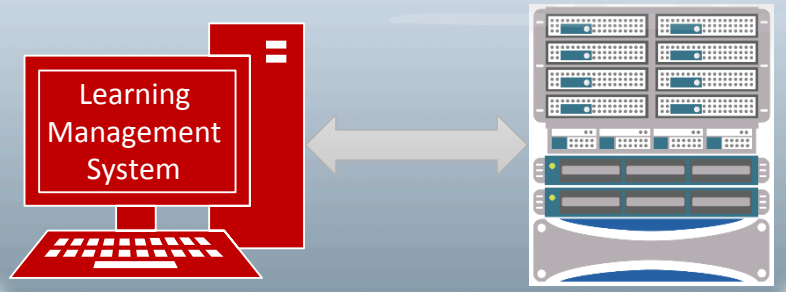
- Full position-specific curriculums
- Live in-person
- Live virtual
- Online/On-demand

Evaluation

- Individuals and Teams
- Against defined job qualification standards
- Measure effectiveness and maturity of ops

Technical Training

- Objective- and standards-based
- Custom—design and assembly
- Practitioner focused



Virtualized Range

- Real-world network simulation
- Isolated and safe
- Customizable to match specific environments

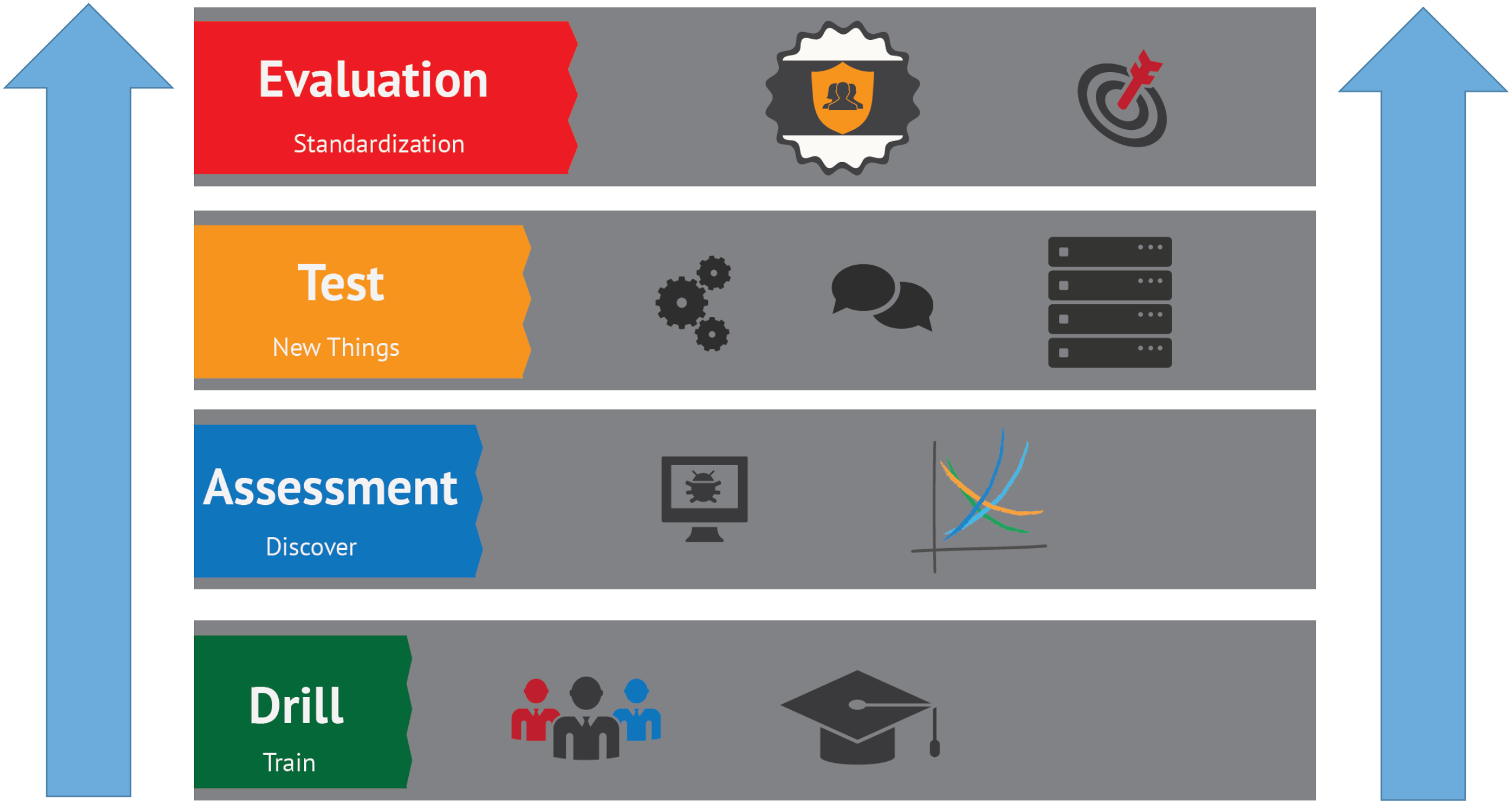
Fully integrated platform provides the ecosystem for the entire training and evaluation process.

Training and **Evaluations** can be individual or joint offerings, but are united in knowledge, skills, and abilities.

RESULT:
Your team is constantly trained and effective at their job; and you have confidence in their abilities

Cyber Exercise Spectrum

Exercise?! Is it going to hurt?


Evaluation
Standardization
Test
New Things
Assessment
Discover
Drill
Train

Drills

- Applicable to nearly all types of cyber learning
- Tasks that require “muscle memory”
  - User-Awareness is perfect here!
  - Here’s a process, let’s run through it

Assessment

- Using a process, how well did you do?
  - Able to execute Incident Response triage checklist in 30 min, 3 min less than last time.
- Start using metrics to determine the effectiveness of an operator or a technical configuration.

Test

- Teams and position-based training
  - Teams practice effective cross-communication
  - Individuals try new application features or security configurations
- Focus towards identifying gaps, and finding solution that works
  - Burdensome solutions are not successful, and will fail

Evaluation

- Complex (realistic) environments and tasks
- End-to-end scenarios with roles for each position being played
- Goal to aid the team in growing towards standardizing their modus operandi
  - Fully standardized equals repeatable performance

How do we determine how well groups do?

- As a group we look for how effective you operate together
  - Typically includes a Embedded Observer and/or White Cell
  - Use enhanced logging features to determine the ground truth
- Tasks are still job oriented, but focused on what your position provides to the team.

How do we determine how well you do?

- As an individual we look at whether a positive condition exists.
  - Did you open all the emails, perform all the tasks, and click on the phishing link?
  - Use enhanced logging features to determine the ground truth
- Scenarios have differing levels of difficulty

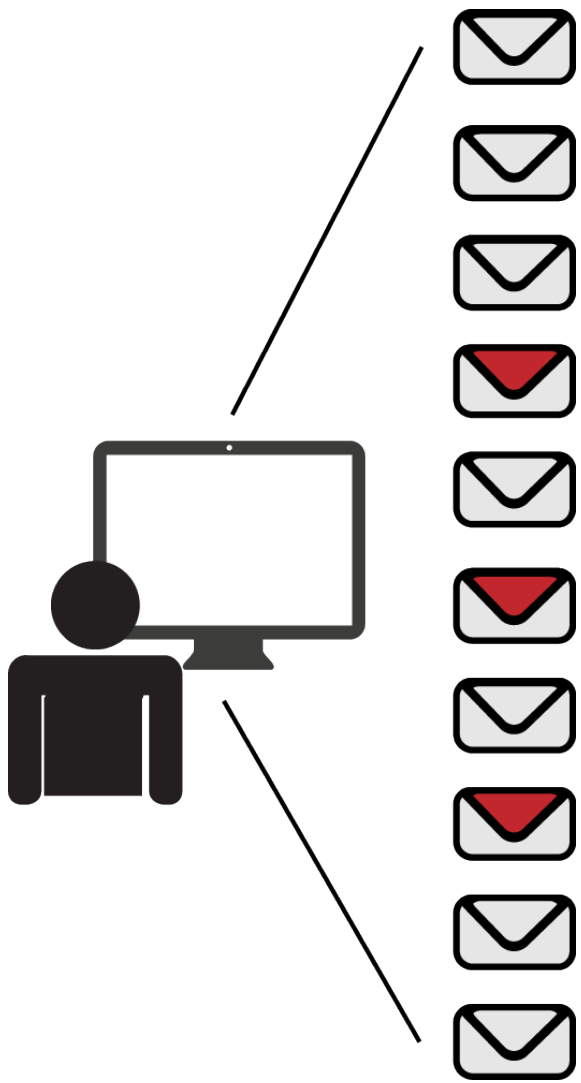
Example User Awareness Training

User logs in to virtual machine, and must review all emails.

User told to email Help Desk with details of any phishing email(s).

Realistic phishing emails, some easier than others to detect.

Can identify whether user fell for phishing, and at what difficulty level.



Nothing, just text

Attachments

HTTP Link

HTTP Link (shortened)

Training highlights:

- who to contact
- what to do **IF**
- how to identify
- Modern adversary methods

Effective Group Based Training

- Major elements contributing to effectiveness
  - Knowledge
  - Performance
- No need to recreate the wheel, we use existing Frameworks and Common Bodies of Knowledge (CBK) to baseline knowledge
- Performance tasks come out of the knowledge teams and positions state they should have to be effective
- Not Delta Risk LLC saying what you should have, rather us training and comparing you to your organization's policies!

When it works, it works

- Effective Group Based Training can tell you whether your people lack knowledge, or whether they need experience
  - Why put your people through more knowledge training when they have already absorbed it?

No shortage of positions needing training

8 Services
37 Capabilities
6 Critical Capabilities

Real-Time Analysis

- Call Center
- **Real-Time Monitoring and Triage**

Intel and Trending

- Cyber Intel Collection and Analysis
- Cyber Intel Distribution
- Cyber Intel Creation
- Cyber Intel Fusion
- Trending
- Threat Assessment

SOURCE: Ten Strategies of a World-Class Cybersecurity Operations Center;
© 2014 by The MITRE Corporation.

Intel and Trending

- **Incident Analysis**
- Tradecraft Analysis
- Incident Response Coordination
- **Countermeasures Implementation**
- On-Site Incident Response
- Remote Incident Response

Artifact Analysis

- Forensic Artifact Handling
- Malware and Implant Analysis
- Forensic Artifact Analysis

SOC Tool Life-Cycle Support

- Border Protection Device O&M
- SOC Infrastructure O&M
- **Sensor Tuning and Maintenance**
- Custom Signature Creation
- Tool Engineering and Deployment
- Tool Research and Development

Audit and Insider Threat

- Audit Data Collection and Distribution
- Audit Content Creation and Management
- Insider Threat Case Support
- **Insider Threat Case Investigation**

Scanning and Assessment

- Network Mapping
- **Vulnerability Scanning**
- Vulnerability Assessment
- Penetration Testing

Outreach

- Product Assessment
- Security Consulting
- Training and Awareness Building
- Situational Awareness
- Redistribution of TTPs
- Media Relations

Time for a couple take-aways

Common Pain Points from Cyber Incidents

- No designation of "Crown Jewels"
- Absence of an over arching company incident response plan
  - Missing contact lists
  - Lack of categorization of incidents and escalation criteria
  - Missing or ad hoc incident response kickoff criteria
- Very little focus on incident "management"
  - Missing procedures for internal communications and coordination; correlation of events
  - Inability to determine impact (operations, financial, legal, reputation)
- Lack of preparedness

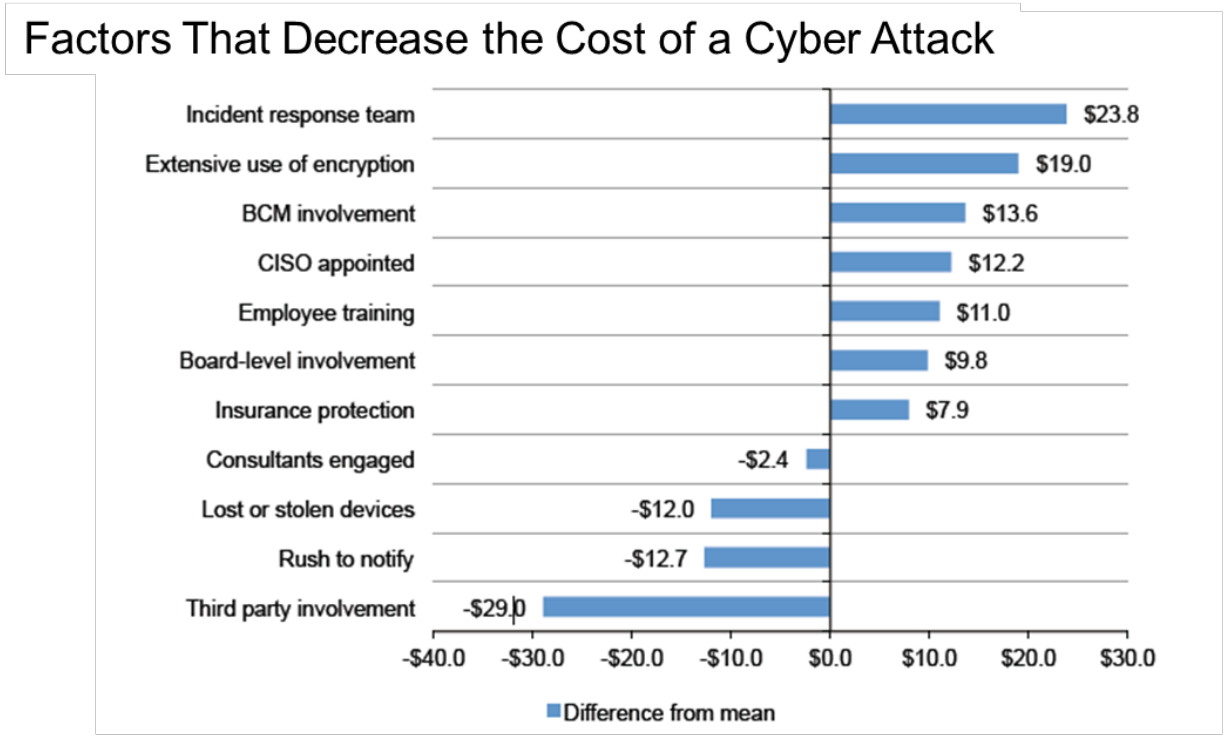
Common (observed) Points of Team Weakness

- No understood plan to pass information between teams
- No communicated tasking process
- Over-reliance on “hero” team members
- Failure to …
  - Understand technologies and what the information tells you
  - Adequately configure technologies
- Little factual information presented to leaders for decisions

Our current advice…

- Prepare for the breach
  - Detection and alerting, or at least logging!
  - Guidance for how and when to report or escalate
  - Rehearse it – at a minimum, talk about it in a tabletop exercise
  - Document your plans or procedures
  - Include your legal team, advisors, and key stakeholders – an incident is not the time to exchange business cards

- An effective RESPONSE could decrease the impact – to the bottom line and the business



PONEMON INSTITUTE, 2015 COST OF DATA BREACH STUDY: UNITED STATES 7 (2015).

Contact Information

Jeff Arsenault
Director
Email: jarsenault@delta-risk.net

Noah Powers, CISSP
Senior Associate
Email: npowers@delta-risk.net