cyberconIQ

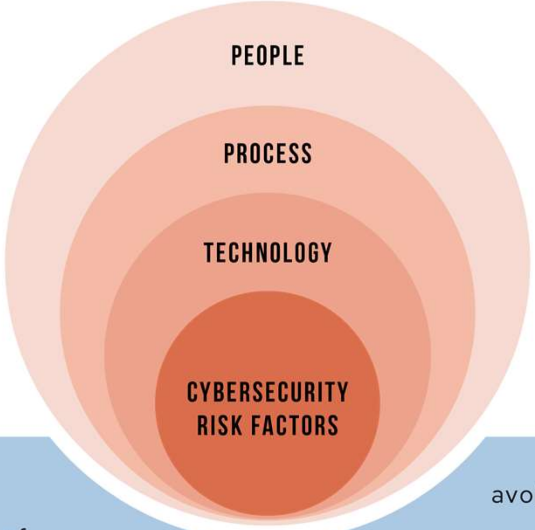
CLIENT DEMO & Discussion

Organizational Mission

Most organizations focus on technology and risk-controlled process designs as their primary risk mitigation tools. Yet, their higher risk is people-based and less predictable. A cyber-based view of the firm tackles total cybersecurity risk from an integrated perspective targeting management attention on the people elements first!

ORG OBJECTIVE:

1. PREDICT
2. DETECT
3. INTERDICT



Our **target audience** is any employee with any kind of system access across the whole organization.

The consequences and costs of an attack inspired or enabled by an insider are much higher than those of an external attack.

And the ROI in terms of total risk avoidance and mitigation are higher by a significant factor than most organizations' current focus on technology and process.

Typical Insider Cybersecurity threat vectors:

SPECIFIC

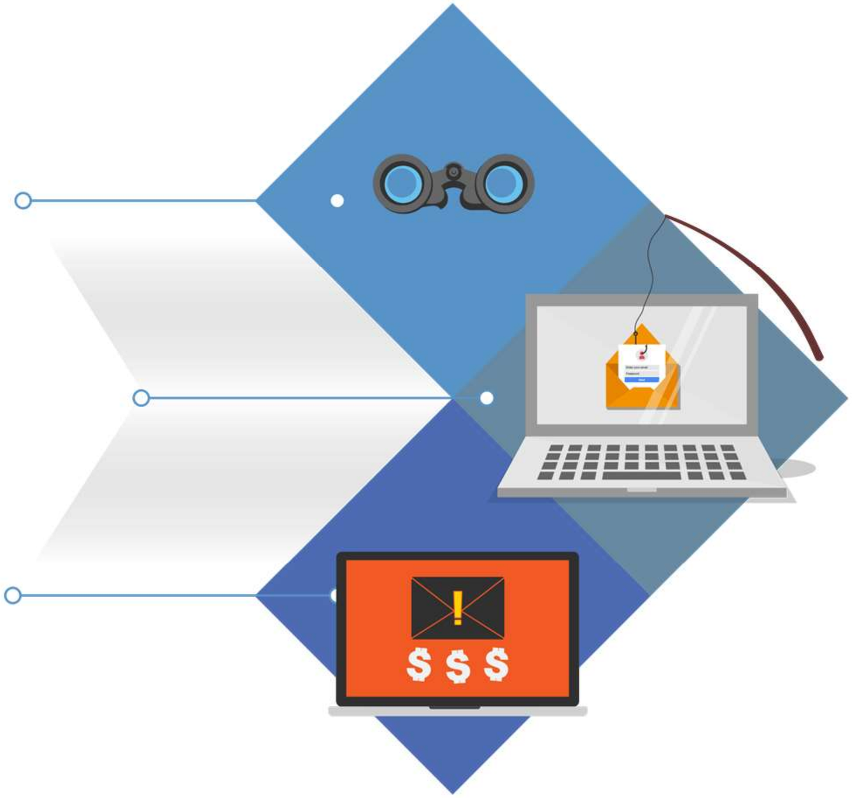
- Spear Phishing
- Catfishing
- Targeted Social Engineering
- Deep Fakes
- Affiliation Manipulation
- Spoofing/Hijacking

GENERIC

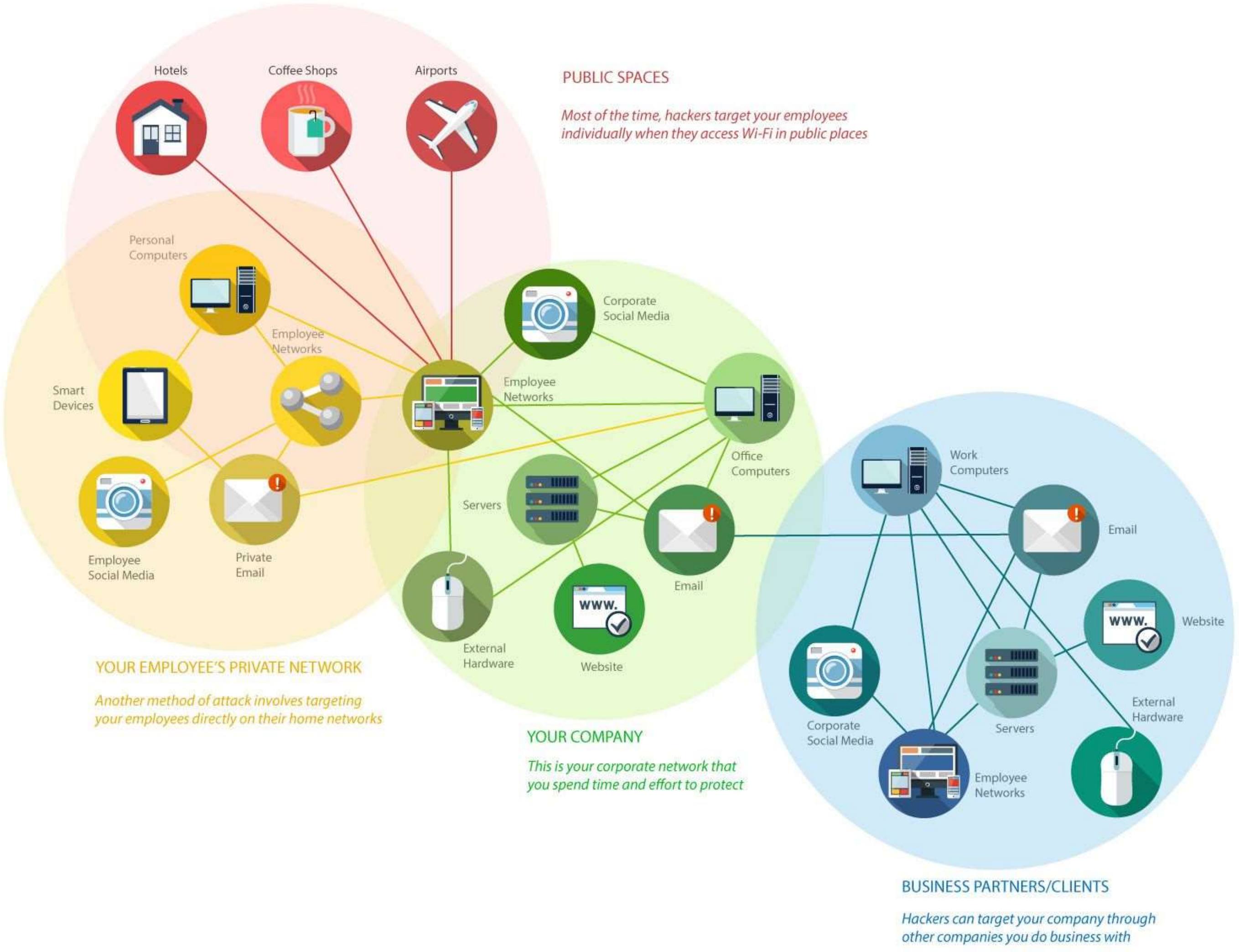
- General Phishing
- Bait & Click
- Malware Attacks
- SQL Injections
- Embedded Trojans/Worms

SITUATIONAL

- IP Theft
- Coercion
- Corruption/Fraud
- Blackmail
- Extortion



CYBER ATTACK SURFACE



PUBLIC SPACES

Most of the time, hackers target your employees individually when they access Wi-Fi in public places

YOUR EMPLOYEE'S PRIVATE NETWORK

Another method of attack involves targeting your employees directly on their home networks

YOUR COMPANY

This is your corporate network that you spend time and effort to protect

BUSINESS PARTNERS/CLIENTS

Hackers can target your company through other companies you do business with

How am I most personally vulnerable?

Our Goal:

Build a Deep Cyberaware Culture

This is NOT about more technology, filtering tools or our SEG. Instead, our focus is the 10% - 15% of the instances on which we rely on the human component to avert disaster!!!

cyberconIQ

THE SCIENCE BEHIND OUR PATENT-PENDING TEST

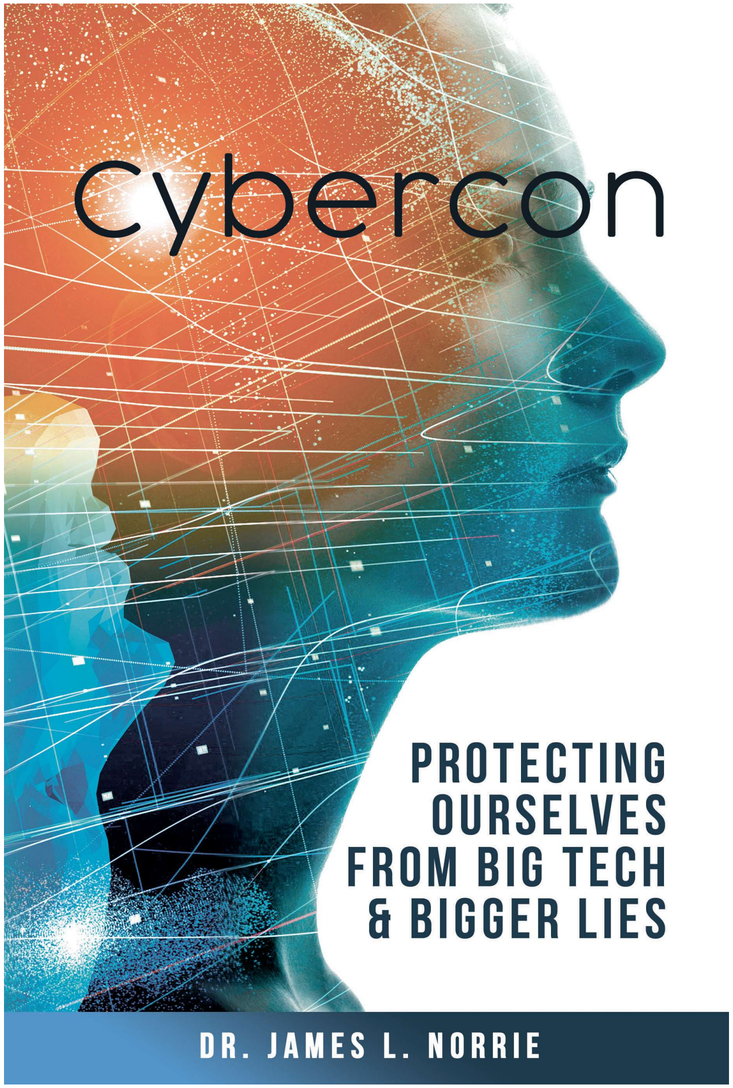
The instrument is based on ground-breaking research, the results of which are *patent-pending and proprietary* to CyberConIQ Inc. The foundation of this is trait-based personality theory circa 1952 – 1980.

The tool is 93.7% reliable in producing a personalized cybersecurity profile for any respondent based on 2 scalable personality traits.

Application of retrogressive correlation analysis against reported IOC's in a pilot produced a statistically valid result indicating predictable correlation to the 98% confidence level for each personality type against likely common attack vectors.

The latest quarterly data (NSA) suggests more than 70+% of successful corporate attacks in the US that resulted in economic losses involved human-factors rather than only technical in origin/nature.

In controlled early pilots, the tool and training produced 56% more self-reported changes in on-the-job behavior than generic alternatives, 1.6 times better recall at 30 day retests and generated ~40% fewer IOC's.

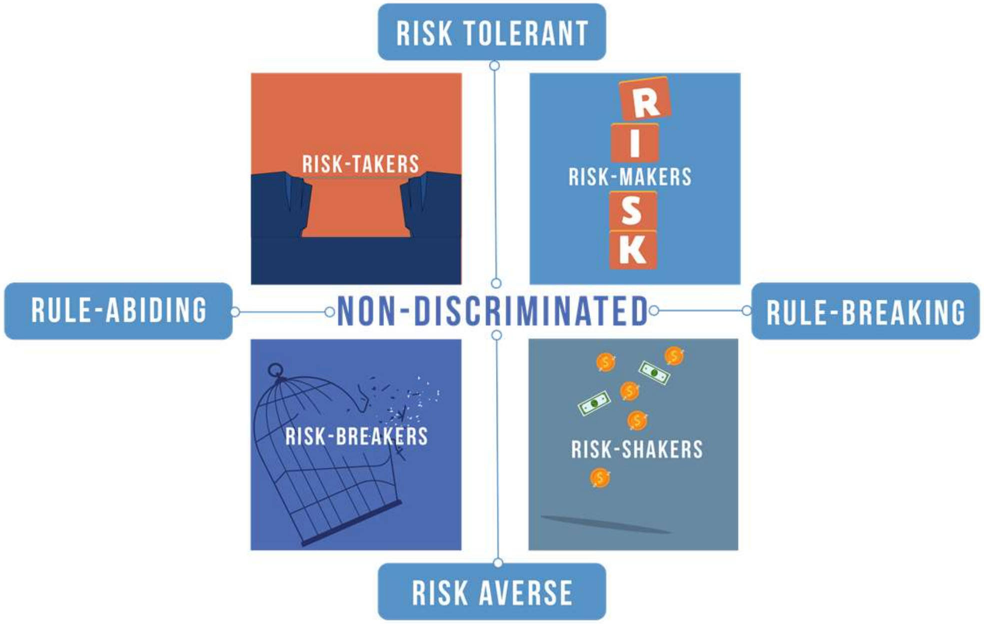


Forthcoming Publication Date: 12/2019

The basic System

Our System Includes:

1) The CyberconIQ test
2) Cybercon (the book)
3) Onsite training workshops (leaders)
4) Style-aligned CBT training (employees)
5) Management/Board reporting
6) Posters and other culture change tools
7) Optional: Customized, style-aligned social penetration testing campaigns



cyberconIQ

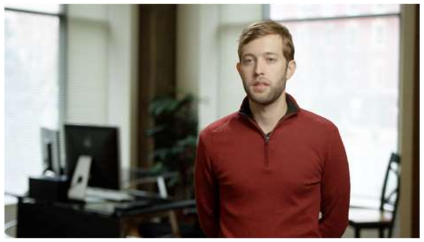
THE RESPONDENTS SAY:

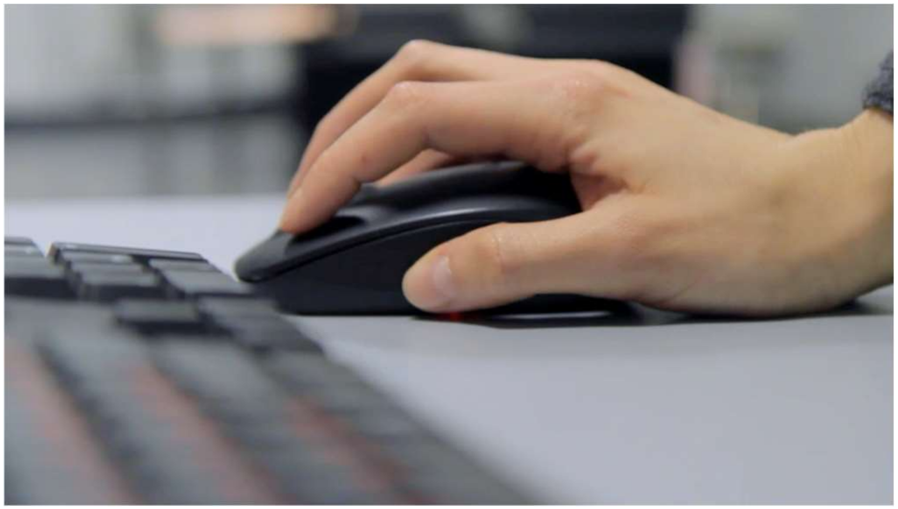
Most employees (96+%) report the test as “easy to do”, “helpful”, “useful” and that it provided “insights” and “new knowledge”. We have experienced less than a 4% objection, query or refusal rate.

The test collects NO demographic or other identifying information except the employee’s work e-mail address. It can be done anywhere and anytime the employee wants.

We do NOT store individual responses to test questions, we only score the pattern of responses to generate their individual cybersecurity profile. That is available to them by e-mail and to print out.

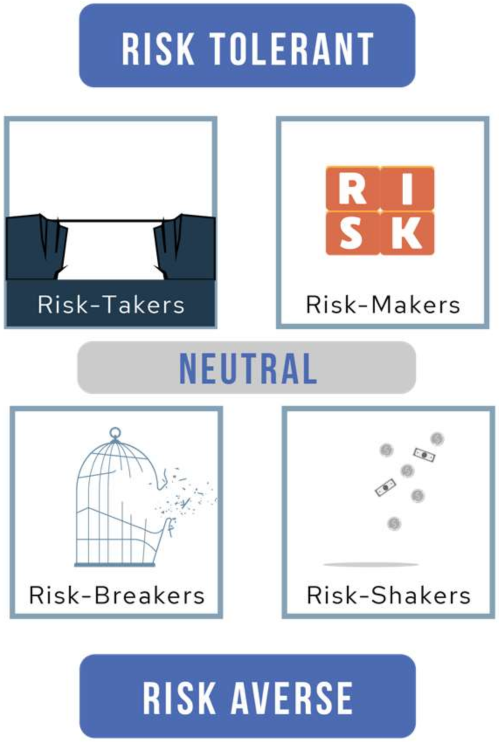
The test does not violate any EECO criteria and has been deemed legally to constitute a bona fide work-related assessment tool.





cyberconIQ

This style is risk tolerant and still inclined to be rule abiding. They strive to understand the rules, but will break them if the returns or the situation seem to justify it. This makes them more susceptibility to social engineering attacks. If these users are trained to understand the risk/reward trade-off of the rules, there is more likelihood they will follow them consistently.

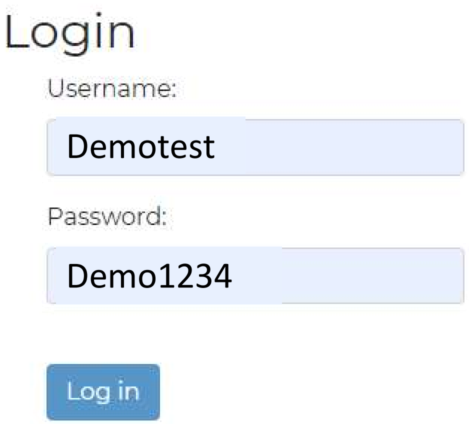


This style is both risk tolerant and willing to break the rules. They feel most situations are unique and prefer relying on their own instincts and judgment vs. broadly applicable rules. This makes them susceptible to multiple kinds of attacks/hacks . They feel is it their prerogative to break the rules, and they often won't follow a rule unless they have played a role in creating or approving it first.

This style is risk adverse and inclined to be rule abiding. They prefer rules to less structured alternatives which they see as leading to chaos. As a result, they tend to respect the rule once it has been established and shared. They are less vulnerable to most common attack because they follow the rule except for those attackers who mimic the identity of those in authority who instruct them to suppress or digress from the rules.

This style is less risk tolerant but still willing to break the rules. But they don't like to get caught doing it! This makes them a covert risk that if their clandestine behavior is detected renders them more vulnerable to specific types of online attacks/hacks. Adversaries often exploit this vulnerability by threatening shaming or exposure of a first hack to gain leverage for further escalations.

https://beta.cyberiqtest.net/account/login



Login

Username:

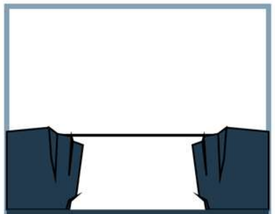
Demotest

Password:

Demo1234

N.B. This is early access to a final beta version of our tool associated with your connection to an "insider" – forgive the pun! We are in final late stage pilots with select commercial clients already under contract for early 2020.

cyberconIQ



Risk-Takers

SEEKS: Returns and Rewards

PREFERS: Selective Exceptions

METHOD: Contrive

Risk-Makers

SEEKS: Innovation and Change

PREFERS: Personal Judgment

METHOD: Devise

Risk-Breakers

SEEKS: Order and Structure

PREFERS: Compliance with Rules

METHOD: Derive

Risk-Shakers

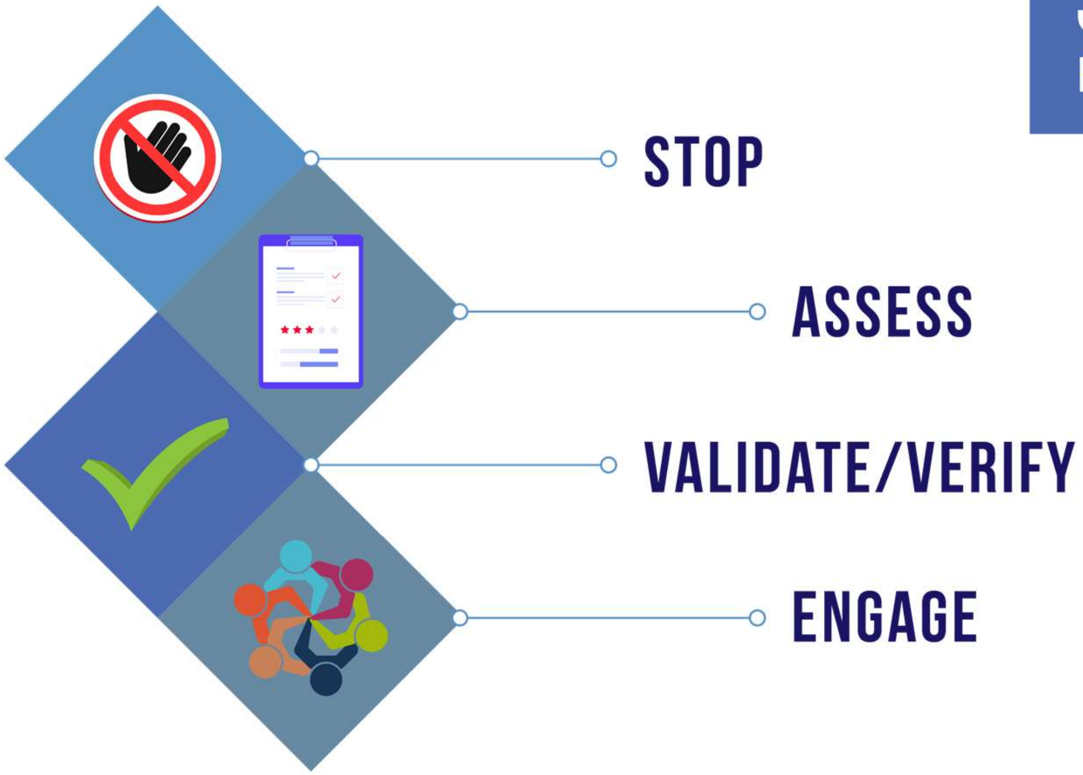
SEEKS: Sensation and Control

PREFERS: Autonomy to Choose

METHOD: Connive

cyberconIQ

SAVE Yourself From Yourself!



STOP

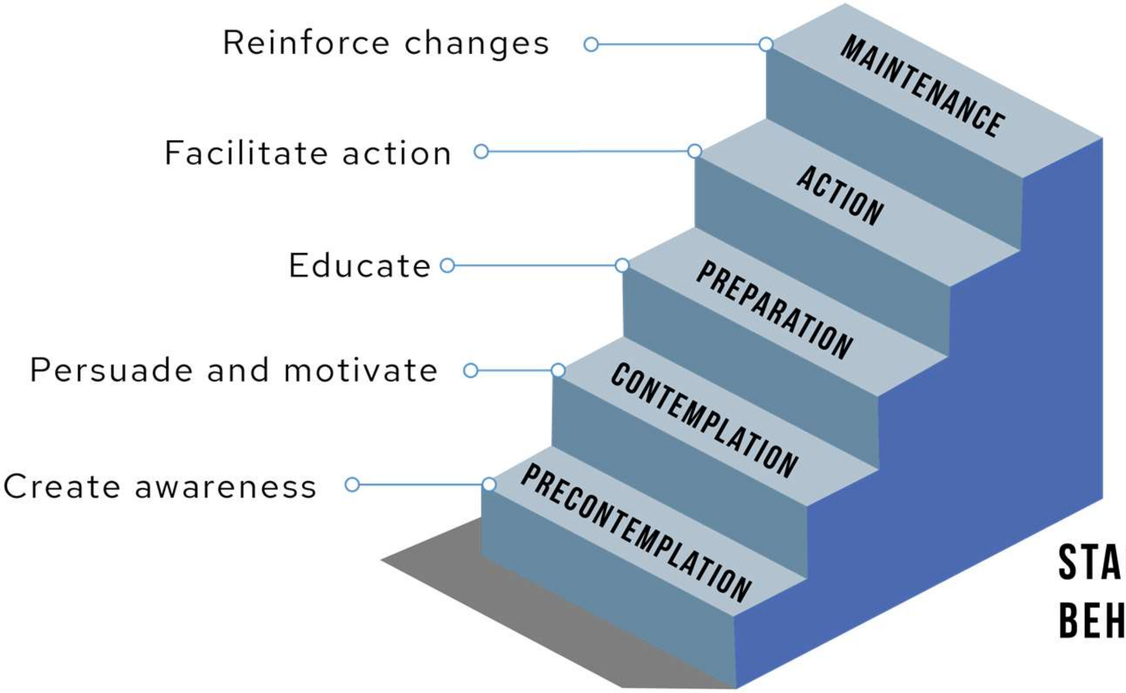
ASSESS

VALIDATE/VERIFY

ENGAGE

cyberconIQ

Approach: Use Communication to Drive Change



Reinforce changes — MAINTENANCE

Facilitate action — ACTION

Educate — PREPARATION

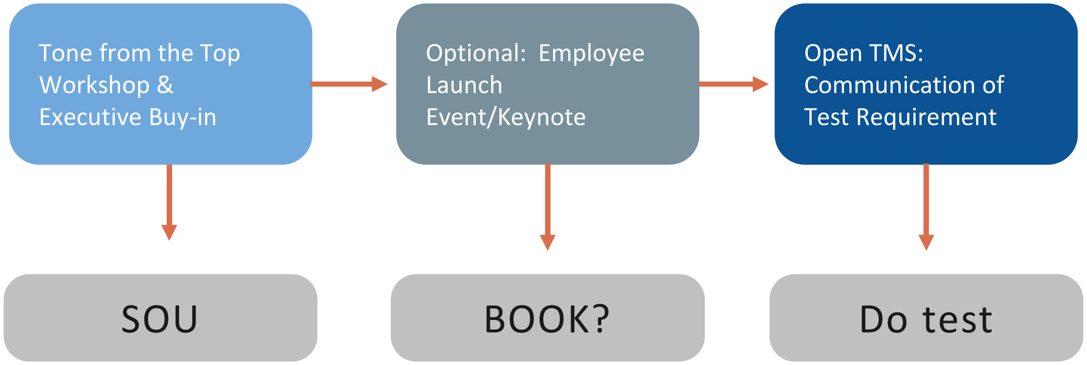
Persuade and motivate — CONTEMPLATION

Create awareness — PRECONTEMPLATION

STAGES OF BEHAVIOR CHANGE

cyberconIQ

Our typical core engagement:



Tone from the Top Workshop & Executive Buy-in

Optional: Employee Launch Event/Keynote

Open TMS: Communication of Test Requirement

SOU

BOOK?

Do test

Sponsor/Lead
# of employees
Who/Why/When
CSV file of names
Communications

Softcover = $10
PDF = $2
Workplace Posters?

1 – 2 week period
Launch on a Monday/Tuesday
Track completion rates
Follow-up to wrap-up effort
Report on aggregate results
Generate individual profiles

cyberconIQ

OPTIONAL SUPPORT

1st Quarter of 2020

- Generic style-aligned video (included)
- Style-aligned training video (>1 hour)
- Style-aligned threat training (2 – 5 hours)
- Role-specific training (EA/Fin @ ~1 hour)

2nd Quarter of 2020

- Updated CBT (1 – 2 hours/mo.)
- Style-aligned weekly e-mail updates
- Style-aligned immediate threat e-mail
- Optional: Social Penetration Testing

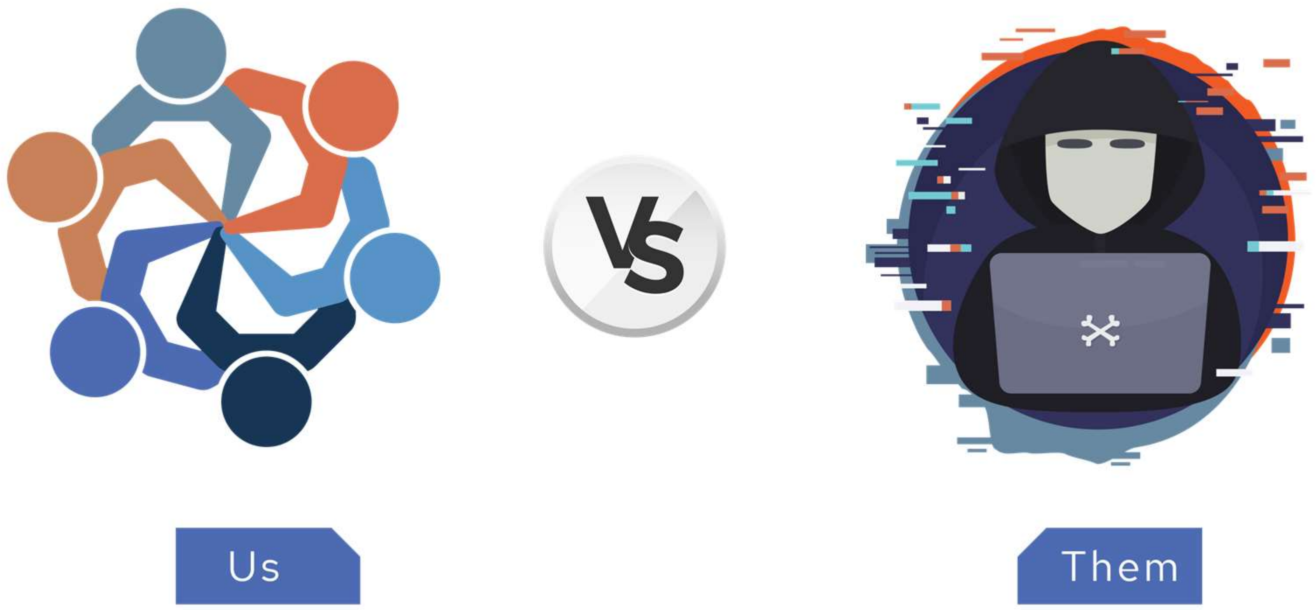
cyberconIQ

From fear…to…hope…BY empowering Your team…

FROM	TO
COMPLIANCE	VOLUNTARY UNDERSTANDING
FATIGUE-BASED COMPLACENCY	EMPOWERMENT
GENERIC COMPUTER-BASED TRAINING	STYLE-ALIGNED TRAINING
INDIVIDUAL FEAR	COLLECTIVE HOPE
TECHNOLOGY ‘PROBLEM’	THE HUMAN ELEMENT

cyberconIQ

RESTORING HOPE: CYBERSECURITY AS A TEAM SPORT



cyberconIQ

Any Questions?
Comments?
Next Steps to Explore?

THANK YOU.