RSAConference2020
San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: SEM-M01B

# Time to Reboot: The Industrial and Organizational (I/O) Psychology of Cybersecurity

**Annalea Ilg**
Chief Information Security Officer
Involta
@2GSecurity1

**Keenan Skelly**
President and CEO
Spark Security Solutions, Inc.
@KeenanSkelly

# Agenda

- Organizational Cybersecurity
- I/O Psychology
- Cybersecurity Challenges
- Cybersecurity I/O Psychology Ecosystem & Strategies
- Summary

# Today's Cybersecurity Focus

Controls

Tools

Risk

Vulnerabilities

Monitoring

Awareness Training

# The Problem: Team Dynamics

Change Human Behaviors Strengthen Cybersecurity Teams Improve the job Environment

# Identify Current Corporate Culture

Introspection

Blockers


Solid ground to build

RSAConference2020

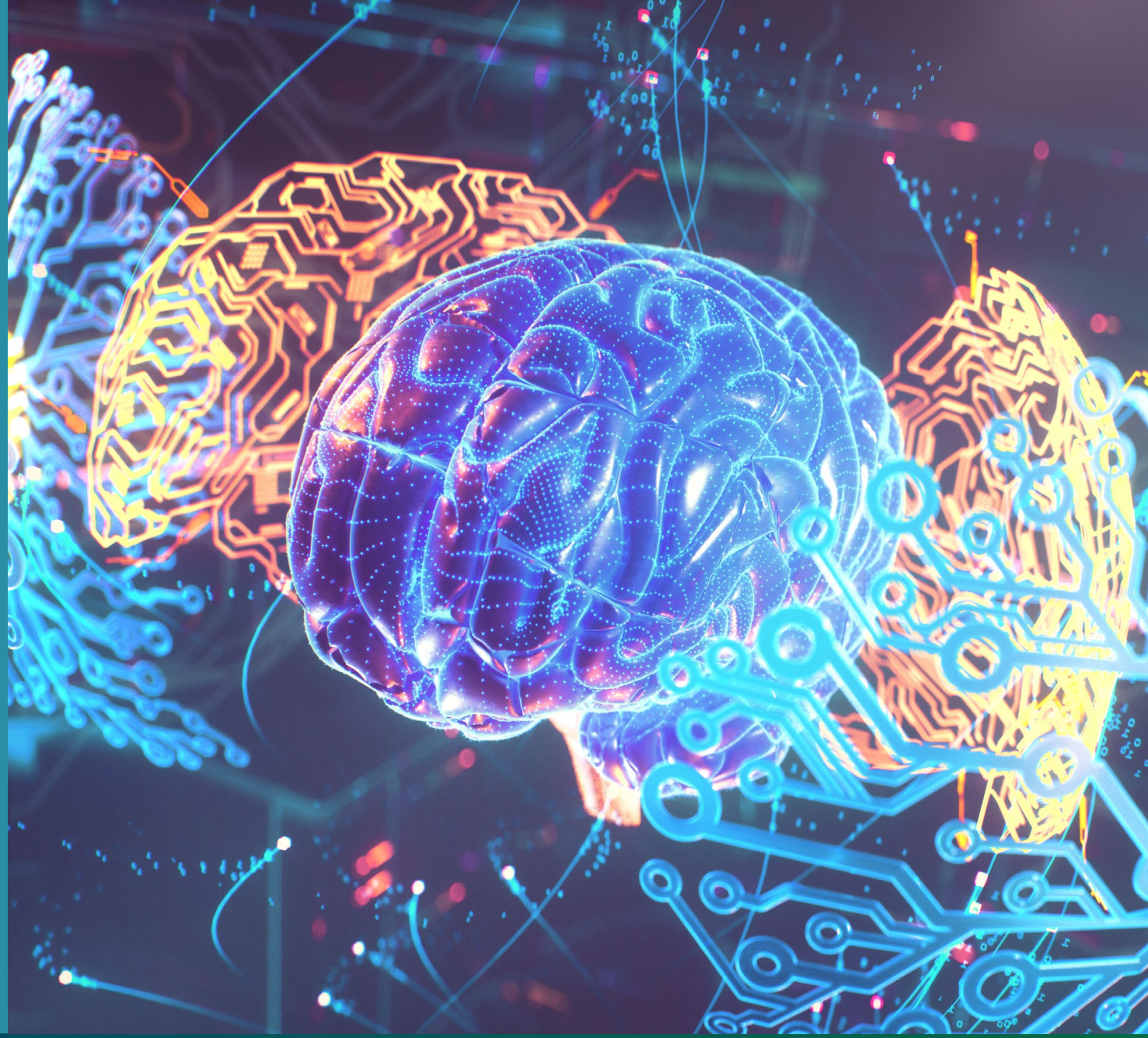
# Cybersecurity Human Elements

- ✓ “Power” Skills Development
- ✓ Strategic Planning
- ✓ Organizational Agility
- ✓ Psychological Contract

# I/O Psychology

The study of industrial and organizational psychology, to **improve workplace issues** facing individuals, teams and organizations.

……to **improve productivity, efficiency and effectiveness** while striving to make the workplace better.



# Challenges Industry Individuals Face

## Security Professional

- No continuing training
- Not up to date on latest attacks and methods
- Lack of coordination with DevOps and other key units
- Overworked 24/7 Talent gap
- Burnout
- Budget
- Where do fit in Big Picture

## Information Technology Staff

- No training or inadequate on Security
- Expectation to be ”on” 24/7
- Managing secure cloud migration
- Data protection
- Burnout
- Budget
- Big Picture

## Business Staff

- No training or inadequate on Security
- Difficulty understanding the value of Security
- Need to tie security and IT to direct revenue
- Budget
- Business Strategy

# Organizational Strategic Dependencies

Company direction and human capital is unclear on priority, focus and authoritative guidance.

Company vision, strategy and the competitive advantage is not aligned with talent structure and development needs.

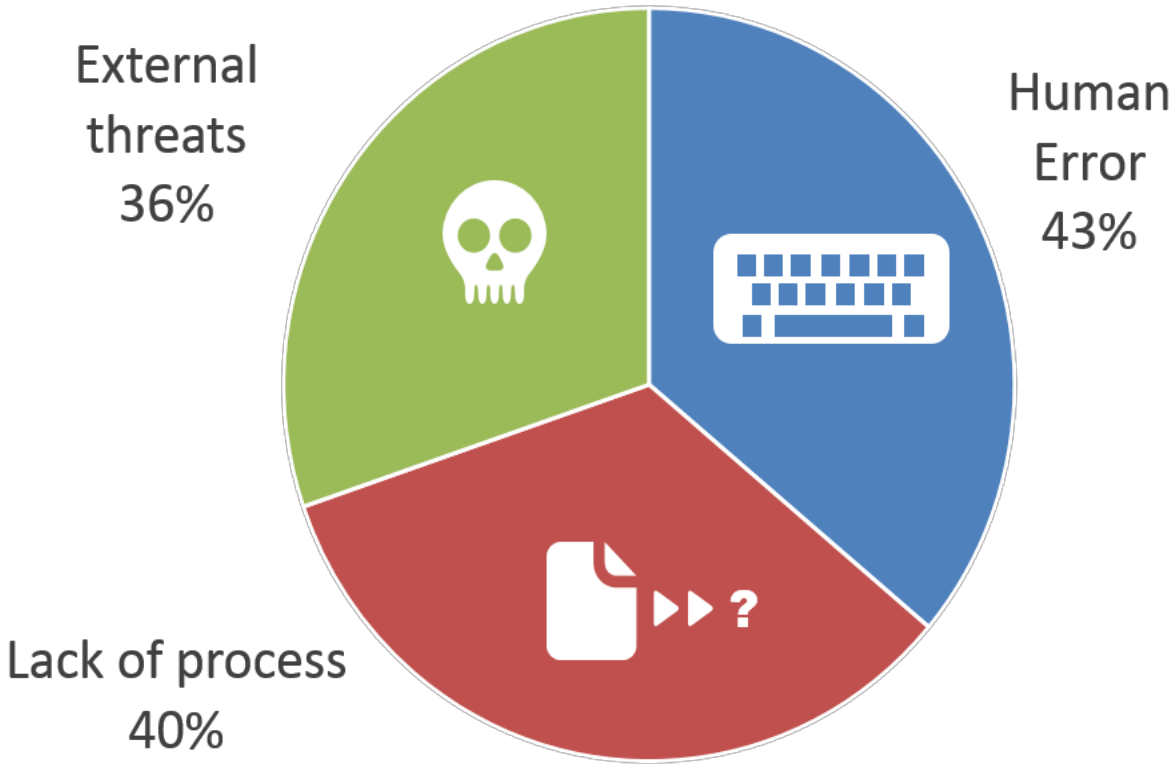
Company priorities fall short, resulting in turnover

- Cultural and leadership styles are misaligned
- Team efforts are siloed
- Employees feel insecure

# Changing Face of Cybersecurity

Cybersecurity is an enterprise problem. One that includes every single employee

- Emerging Threats
- $3.92 Spent Globally in 2019
- Human attack surface still the most vulnerable.



RSAConference2020

# The Balancing Act

- Continuously evolving landscape challenges ‘readiness’
- Escalating attack methods need to be engaged
- Security budgets need more prioritization
- Technical and architecture debt impedes progress.
- Continuous justification efforts for ”buy-in” exhausts leadership

Involta CIRCADENCE

# Strategic Planning for Cybersecurity

Elevate the cyber workforce.

Its MORE than culture awareness.

It’s the HUMAN element of the organization.

- Collaboration
- Accountability
- Motivation

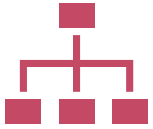
# Cybersecurity I/O Psychology Ecosystem

Vision

Strategy

Cultural Intelligence

Human Capital Development



Organizational Outcomes

Psychological Contract

Measurement

Cybersecurity Leader must….

**Communications**

VISION

STRATEGY

# Organizational Agility

Companies are just beginning to prioritize the messaging.

Cybersecurity culture is not getting the attention it needs for real changes to occur.

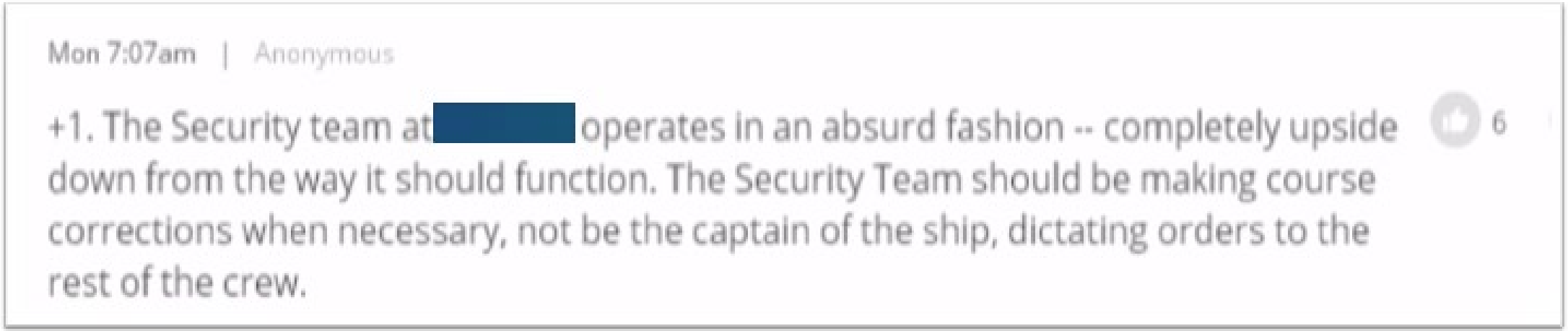
They don't know the how, means or impact.

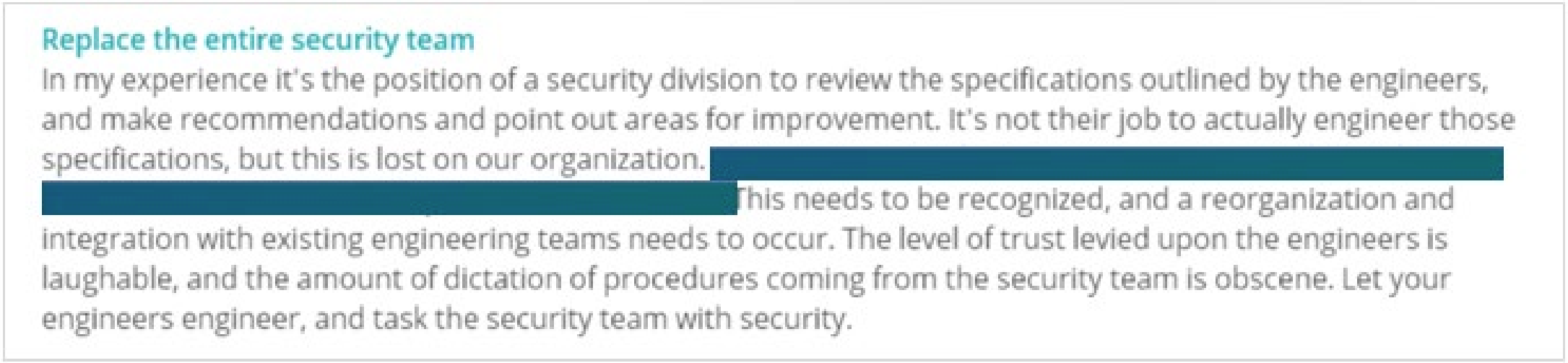
I like the notices, but I'm going to create a rule to put them into a folder just like the service now disruptions...where I can read them at the time I want to...too many disruptions are hard to deal with for those who hold large datasets in their minds while working on projects.

# “Power” Skills Development

Cybersecurity professionals are losing the battle against external threats and failing at building allies with their business peers.

They feel constant defeat which can be paralyzing.





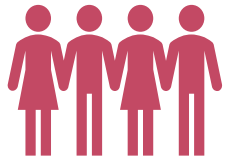
**Replace the entire security team**

In my experience it's the position of a security division to review the specifications outlined by the engineers, and make recommendations and point out areas for improvement. It's not their job to actually engineer those specifications, but this is lost on our organization. [redacted] This needs to be recognized, and a reorganization and integration with existing engineering teams needs to occur. The level of trust levied upon the engineers is laughable, and the amount of dictation of procedures coming from the security team is obscene. Let your engineers engineer, and task the security team with security.

**The severity of the problem is within the *behaviors* of the organization.**

**Change which will cause business upset, if not approached properly.**

# Build Organizational Trust



1. Talk about fear and trust as business topics
2. Step away from blame and shame
3. Get to know co workers &employees personally
4. Value employees as people over production
5. Lead by example
7. Admit mistakes
8. Use a human voice in communications
9. Ask how things are going and listen to the response
10. Be honest

# Effective Cybersecurity Teams

Integrate security into the workplace principles/ corporate strategic plan

Expand training to include ”power skills” to be successful

Partner with HR to ensure that talent and skillsets are aligned with need.

Communicate the intangibles.

Measure to a behavior anchors matrix- not just technical skills

# Paths to Effective Teams

Shift from training to learning

- Experiential
- Immersive

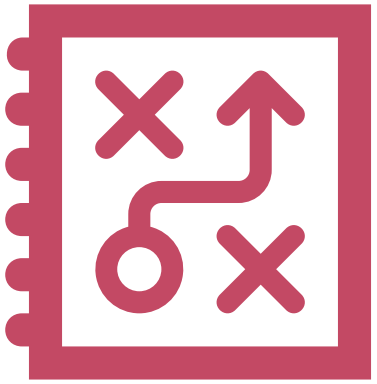
Understand critical skill requirements

- Technical
- And non technical employees

Build an All In culture around cybersecurity awareness and skills

- Align across the organization

# Organizational Agility: Resilient and Adaptive



When working across organizations to secure assets, respond to threats and remediate weaknesses:

- Explain the "why"
- Promote rapid change

Conduct quarterly training sessions to explain what is expected and required.

Integrate security within existing processes

- Organizational change management
- Promote accountability

# Improve Job Environment

Key leaders need to be onboard.

Communicate the psychological contact between employer and employee relating to cybersecurity.

Discuss psychological contract between cybersecurity team and accountable leadership.

# The Culture Code

When cyber professionals are a part of sound culture that reflects who they are and the company strategy and vision; they are most likely to excel.

## Build Safety

- Overcommunicate your listening
- Preview future connection
- Overdo thank you
- Be painstaking about hiring
- Eliminate bad apples
- Create safe, collision-rich spaces
- Make sure everyone has a voice
- Capitalize on threshold moments
- Embrace fun

## Share Vulnerability

- Overcommunicate expectations
- In conversation, resist the temptation to reflexively add value
- Use candor-generating practices like AARs, BrainTrust and Red Teaming
- Align language with action
- Embrace the discomfort

## Establish Purpose

- Name and rank your priorities
- Be ten times as clear about your priorities as you think you should be
- Figure out where your group aims for proficiency and where it aims for creativity
- Embrace catchphrases
- Measure what really matters
- Focus on bar-setting behaviors: translate abstract ideas into concrete terms

# Organizational Cybersecurity Outcomes

- The team is happy and healthy
- Conflicts are resolved quickly and effectively
- Reduce negative employee churn
- Clear organizational communications
- Strong talent
- Accountability and ownership expands beyond the department
- Security is a foundational element within the organizational strategy
- Improve the relationship, behaviors and communications between security and the business

# Summary

- Foster new behaviors
- Expand accountability across the organization
- Enhance "power" skills
- Involve other departments to solve problems
- Overly Communicate the “Why”
- Incorporate strategic thinking

# Apply What You Have Learned Today

## Next week you should:

Identify pain-points and improvement opportunity between the cybersecurity team/individual and the business.

## In the first 3 months following this presentation you should:

Ensure a cybersecurity vision, strategy exists and start the conversations at the top-level.

Initiate a “power skills” learning development program and a mentorship program.

## Within 6 months you should:

Partner with HR to integrate security principles into the foundation.

Conduct first organizational agility training session to get the business aligned with cybersecurity process.

# Questions?