HOW TO BUILD A CYBERSECURITY CULTURE

Dr. Mansur Hasib, CISSP, PMP, CPHIMS
Cybersecurity Leader, Speaker, Author, Media Commentator
Program Chair, Cybersecurity Technology, The Graduate School, UMUC
2017 People’s Choice Award in Cybersecurity
2017 Information Governance Expert of the Year
2017 (ISC)2 Americas ISLA Award for Cybersecurity Technology Degree Program at UMUC
Book Cybersecurity Leadership Rated #2 Best Selling Cybersecurity Book of All Time
SESSION GOALS

Understand Cybersecurity
Understand Role of People and Leadership
Understand How to Build Cybersecurity Culture
Understand Potential Barriers
THE WORLD HAS CHANGED – A NEW EPOCH

Hyper Networked World
Digital Leadership Strategy is Key
Everyone Handles Technology and Data
Personal and Work Life Difficult to Distinguish
There is No Organizational Perimeter
Technology Affects Everything
Human Relationships Through Technology
Power of Communications Democratized
People Work from Where they Are
KEY CONCEPTS

- Confidentiality – Right People Can Access Information
- Integrity – Information Can Be Trusted
- Availability – Information Available in Manner, Location, and Duration Planned
- Privacy – Legally Protected Confidentiality
• Maximize Confidentiality, Integrity, and Availability

• Countermeasures: Technology, Policy and Awareness Training

INFORMATION ASSURANCE MODEL - 2001


• People
• Innovation

OBSOLETE: PLEASE DO NOT USE ANYMORE
THE DYNAMIC CYBERSECURITY MODEL

Cybersecurity is the mission-focused and risk-optimized governance of information, which maximizes confidentiality, integrity, and availability using a balanced mix of people, policy, and technology while perennially improving over time.

-Mansur Hasib (2017)
EXPLAINING CYBERSECURITY TO ANYONE

Cybersecurity is the Digital Strategy of Organizations
Digital Strategy Determines Organizational Success
Cybersecurity Requires Perpetual Innovation
Strategy Must Be Based Around People
People Innovate, Choose, and Configure Technology
If You Base Cybersecurity on Technology Alone You Will Fail

Cybersecurity is People Powered Perpetual Innovation
Ethical Leadership is Key to Success

YouTube Video: https://youtu.be/TPzpHVY8Xwo
• Develop Cybersecurity Culture
• Engage People at All Levels
• Inspire, Educate, Innovate
• Focus on Job Related Technical Proficiency and Empowerment not Awareness
• Teamwork, Communications, Transparency
• Develop Leaders Not Followers
• More Decisions at Lower Levels of Organization

CYBERSECURITY IS NOT A ONE BRAIN SPORT
Cybersecurity governance is the leadership of people to achieve cybersecurity culture and perpetual innovation in an organization.

-Mansur Hasib (2016)
HOW DO WE BUILD CULTURE?

Values
Heroes
Rituals
Social Network Guarding Against Deviations

Leadership is Essential for Developing Culture

Note: For comprehensive discussion and citations of literature see Hasib, 2013
CULTURE BASED ON PEOPLE

Data Classification
Data Tagging
Data Leak/Loss Prevention
Data Encryption
Separate Identity and Health Record
Accounts and Access Management
Privileged Account Management
Incident Response Drills
Continuous Monitoring and Improvement
VALUES

Data Safety
Data Quality
Innovation -> Ideation
Service -> Help Each Other
CYBERSECURITY CULTURE RESEARCH FINDINGS

Organizational Level for Cybersecurity Governance
CIO Role and Reporting Level
Executive Management Engagement
Benevolent Management (Ethical Leadership)
Employee Empowerment (Use Their Brains)
Policy Enforcement
Rewards and Gamification (Fun)
Monitoring

Governance Does Not Mean Control
BENEFITS OF CYBERSECURITY CULTURE

• Lower Costs Over Time
• Increased Productivity and Innovation
• Improved Cybersecurity Behavior
• Strengthened and Improved Over Time
• Addresses Key Source of Incidents
• Can be Used in Any Organization

-Mansur Hasib (2013)
MACROECONOMIC BARRIERS

- People are Treated as Expenses
- Layoff Culture in Organizations = IP Loss
- Higher Levels of Worker Mobility = IP Loss
- Major Declines in Innovation Since the 1970s
- Major Declines in Benefits of Work
- Erosion of Worker Loyalty = Insider Threats
- Reduced Management Benevolence
- Reduced Investments in Worker Development
- “Skills Gap” = Hire Purple Squirrels at Mouse Pay
ORGANIZATIONAL BARRIERS

CFOs in Charge in 50% Organizations
Lack of Cybersecurity Leaders
Treatment as Cost Center Not Innovation
Focus on Short Term Personal Profits
No Executive Accountability
QUESTIONS/DISCUSSIONS/MORE INFORMATION

References:

Twitter: @mhasib
Mansur.Hasib@umuc.edu
240-684-2425

Copyright© - This work is the intellectual property of the author Dr. Mansur Hasib to supplement presentations by the author and not for public distribution. Written permission required for any commercial use.

www.cybersecurityleadership.com