Jeanine Baisi, GSLC

- Over 20 years of experience in Cybersecurity related standards & frameworks within multiple technologies
- Active member of several Security Awareness forums
- Strong passion for Cybersecurity education
- Instrumental in the development of the Motorola Solutions Cybersecurity Champion program
- Educates customers & internal teams to strengthen their overall awareness & knowledge within Cybersecurity
AGENDA

NIST CSF 4 Tiers
- Keeping It Simple - Cyber Risk Management
- Understanding What It Means
- How Can You Get There

Business Continuity
- Resilience
- Have a Plan - Exercise the Plan

Culture Change
- Culture and the Human Factor
- Culture Change - Motivating Change
- Managing Change – Measure, Metrics, KPIs

Training and Awareness
- Educating Champions
- Measuring Impact
- Planning & Programs
NIST CSF 4 TIER FRAMEWORK

 CYBERSECURITY FRAMEWORK - KEEPING IT SIMPLE
NIST 4 TIERS - UNDERSTANDING YOUR RISK

Tier 1:
- Partial
  - Ad-hoc, reactive
- Inconsistent planning & risk awareness

Tier 2:
- Risk-Informed
  - Piecemeal Implementation
  - Reactive protections

Tier 3:
- Repeatable
  - Fully Implemented CSF Adoption
  - Policies applied, employees fully informed

Tier 4:
- Adaptive
  - Preparing - total adaptation & prevention
NIST FRAMEWORK - HOW DOES THIS WORK?

Tier 1 (Partial)
Tier 2 (Risk Informed)
Tier 3 (Repeatable)
Tier 4 (Adaptive)

Risk Management Process
Integrated Risk Management Program
External Participation

The functionality and repeatability of cybersecurity risk management
The extent to which cybersecurity is considered in broader risk management decisions
The degree to which the organization benefits by sharing or receiving information from outside parties

NIST
National Institute of Standards and Technology
U.S. Department of Commerce
BUSINESS CONTINUITY

HAVE A PLAN
RESILIENCE

Business Resilience

Emergency Response Plan

Crisis Management Plan

Business Continuity Plan
HAVE A PLAN - Yes, it can happen to you!

Business Continuity

- A proactive plan - keep your business running and recover from any incidents
- Practice exercising the plan
- Disaster Recovery
- Crisis Management/Incident Response
- Vulnerability Management
CULTURE CHANGE vs. STRATEGY

EFFECTIVE & IMPACTFUL
CULTURE ATTRIBUTES - The Culture Factor

Define your culture & shape it!
UNDERSTANDING YOUR CULTURE

- What type of culture are you?
- Already have a security culture?
- Behaviors impact security
- Every organization’s security culture reflective of overall culture
CULTURE CHANGE

Motivating Change

● Start with **WHY**

● For change to happen, understand the need
  ○ Executive sponsors - add credibility and drive leadership support
  ○ Stakeholders understand the value - support it
  ○ Workforce understand the value - implement it

SELL THE CONCEPT OF CHANGE - BUSINESS STRATEGY!
CULTURE CHANGE

The “Human Factor” Risk

Cyber Risk - reduce risk by reducing each of the three variables

Human risk we reduce each variable by changing human behavior

THREATS x VULNERABILITY determines the probability of an incident. IMPACT is the measurement of that harm.
CULTURE CHANGE

Business / Strategic Metrics & KPIs

- Compliance metrics:
  - Regulatory Changes
  - Risks

- Behavior metrics:
  - Phishing - clicking links
  - Attachments

- Strategic metrics:
  - # of policy violations
  - # of incidents

People are not the weakest link - they are the primary attack vector
TRAINING & AWARENESS
Cybersecurity Training and awareness
A Strategy to prevent and mitigate user risk

SECURITY AWARENESS MATURITY MODEL
The Human Factor

- Most compromises are due to human mistakes and are the top human risks:
  - Phishing / Social Engineering Attacks
  - Passwords
  - Accidental
- Most often left unaddressed
- Proactive measures
- Protections in place
HELPFUL PROGRAMS

Cyber Champion Program

- Cyber career path & raises awareness of best practices
- Influence Cyber strategy
- Distributed and Scalable

Onboarding/Annual Refresh

- Maintaining company health and security

Surveys and Phishing Campaigns

- Measuring awareness & change within your org
Have some level of risk management & mature over time…

- Have a plan and exercise the plan - business continuity, disaster recovery! Be proactive not reactive!

- The Culture Shift - it can help your company strategy & minimize your risk for compromise

- Training & Awareness - the human factor that is one of the highest causes of compromises - get the word out!

To change behavior we need a mature awareness program using a proven framework
QUESTIONS
THANK YOU!