Cyber Security, or Cyber Safety Culture? Convert the weakest link into the force

Slava Borilin
INDUSTRIAL SECURITY IS FOR THE SAKE OF RELIABILITY AND SAFETY.
ICS/SCADA “Triangle”

CEO

Doesn’t see how Cyber Security spending relates to Revenues

Engineers

Are more concerned about security measures than malware

ICS Security

Not in control of security of Industrial sites

IT Security
Building the way through “SCADA Triangle”

– Fun & engaging
– Team-work builds cooperation
– Competition fosters initiative & analysis skills
– Develops understanding of cyber security measures

Kaspersky Industrial Protection Simulation

13 countries, 4 languages
OF ALL THE SCARY THINGS THAT CAN SABOTAGE A NETWORK, THIS ONE IS BY FAR THE DEADLIEST.

Human Error Is The Single Biggest Cause of Information Security Breaches. Statistics show that up to 80% of security problems are caused by people.
Cyber Security posters

Password:

Length Does Matter

Create secure, memorable passphrases of 14 or more characters by joining unrelated words with numbers (e.g., Beautiful16JazzyCanada).
Employee vs. Security Officers =

![Two dogs playing on the beach](image-url)
Industrial Security Equation

• Engineers don’t listen / don’t trust to IT

• Management (C-level) doesn’t care;
  – Just “go to IT”
  – No budget, no attention, no real support

• Employees seen as enemies, they don’t understand security, see it as an added burden

1 equation with 3 variables
WE HEAR CALLS FOR CYBER SECURITY CULTURE

But most do not offer any practical solutions, as it's neither posters nor just trainings.
THIS IS NOT THE FIRST TIME THIS PROBLEM OCCURRED

Not long ago, the issue of industrial safety culture was in the same boat, exactly the same problems seemed intractable
Industrial SAFETY

– Existed always;
– Vastly improved in the last 25 years.
Safety culture is now a big topic, a corporate-wide initiative of most industrial companies:

- It has funding
- C-level support and visibility
- Shell, Siemens, Du Pont, SIBUR, TATA, SINALCO, BHP
- Developed and Emerging Economies
3 whales of SAFETY CULTURE

1. ZERO INCIDENT

2. NEAR MISS REPORTING

3. ABC (BEHAVIORAL ANALYSIS)
1. ZERO INCIDENT

THIS IS THE ONLY ACCEPTABLE TARGET TODAY
Zero incident culture – key elements

1) Top-level Commitment
e.g. ACLOA: CEO requires all incidents reported in 24 hours.

2) Leadership
Middle management and supervisors cultivate practice

3) Employee Involvement Employees know “what is in it for them,” they own the different aspects of safety in their area and they care about themselves and their coworkers – they feel responsible for each other.
Zero incident culture – key elements

4) Accountability
WHEN EVERYONE DOES IT, IT GETS DONE The obligation to meet performance expectations or bear the consequences for failure to perform as expected, when expectations are clearly communicated and agreed upon. Each person is accountable for everyone’s actions, including the decision to take no action within the work environment.

5) Training
Equipping employees with the knowledge and skill to
• perform their job safely and
• perform the health & safety functions that aid organizations in reaching their overall health and safety goals
A “near miss” is an unplanned event that did not result in injury, illness or damage - but had the potential to do so. Sometimes called a “near hit” or “close call”;

“Near misses” should be reported without penalty or punishment;

Reporting “near misses” is the cornerstone of safety culture.
Feedback culture

The system is designed so that everyone talks about safety, it becomes a habit (e.g. “yesterday i went to a supermarket…”)

Feedback on observed behaviors has to be specific (task focus, concrete, timely and balanced);

Everyone should be able to feedback, regardless of rank or status, when they observe an unsafe behavior.
3. ABC - Every behavior is a function of its consequences

Antecedent: What happens before the behavior;
Behavior: What actually happened, what can be observed;
Consequence: What happens after the behavior.
ABC sequence defined

- IDENTIFY BEHAVIOR
- IDENTIFY ANTECEDENTS
- IDENTIFY CONSEQUENCES
- WORK ON CONSEQUENCES TO CHANGE BEHAVIOR
ABC ANALYSIS – Driving Fatigue

Behavior is a function of consequences

ANTECEDENT
- In a hurry
- Working more than one job
- Sleep debt

BEHAVIOR
- Driving tired
- Driving for long periods
- Not taking breaks

CONSEQUENCE
- Near miss: running a stop sign
- Car accident
- Injury
- Death(s)
Important Roles in the cyber safety culture commitment

**Line Managers**
- Create cyber safe environment
- Enforce Cyber Safe behavior of employees

**IT Security team**
- Provide Security measures
- Design Secure behavior (ABC)

**Employees**
- Share cyber safety
- Act cyber safely
- Report near misses
- Help IT Security team

**Safety Managers**
- Understand cyber threats
- Include cyber content into safety program

**Board/Tops:** Policy, Goals, Procedures
Developing Cyber Safety Culture by Gamification

Employees
- Cyber Safety training
- Gamefication
- Motivation

Managers (Safety/IT/OT)
- Understand cybersecurity strategy
- Develop cooperation principles

Line Managers
- Cyber Security Awareness
- Security-Efficiency win-win
- Cyber Safety enforcement

IT Security team
- Security expertise
- Behavior (ABC) and its redesign

Kaspersky Cyber Safety Games
Kaspersky Industrial Protection Simulation
Kaspersky Security Power
Kaspersky Security Design Studio
Kaspersky
Cyber Safety Games

CYBER SECURITY AWARENESS
BY GAMIFICATION
Kaspersky
Industrial Protection Simulation
Cyber safety – value proposition

– No difference btw Cyber and Physical Safety.
– Merge Cyber Security and Industrial Safety.
– Speak the language Engineers & Managers.

– **Enterprise (and ITSec):** convert your weakest security link into acting cyber security guards;

– **Employee:** Living Cyber Safety keeps your personal values, makes your better recognized and valued employee.