CyberSecureDeck: *Defend the Network!* Card Game

GAME PURPOSE, OBJECTIVE and COMPONENTS

Purpose of the Game:

A fun way to promote conversation about cybersecurity and ways to identify threats and vulnerabilities, protect vital infrastructure, detect security threats, respond to incidents, and recover from attacks to promote cyber resiliency. Players in the 8 Roles must guide the Organization through a Scenario by helping Identify, Protect, Detect, Respond and Recover from a cybersecurity Incident.

Components:

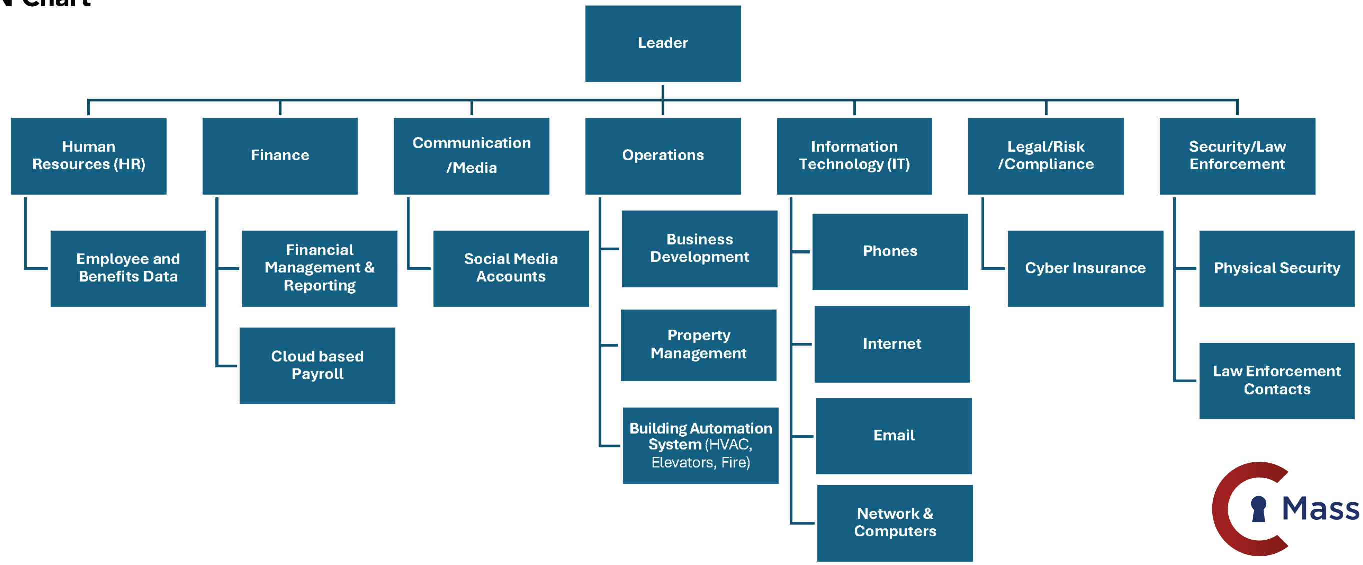
FACILITATOR (1): The Facilitator guides players through the game. They do not "play" the game or represent a Role or have a purpose within the Organization.

ROLES (8): Each player chooses one or more Role cards within the Organization. All 8 Roles must be played.

SCENARIOS and INJECTS: There are Scenario cards, which can be used individually for a 15-Minute Discussion or as a 1-Hour GAME (with associated Injects) to help players experience how a cybersecurity incident might occur.

ORGANIZATION (1): The Organization is based in Massachusetts and represents a business, corporation, non-profit, school, public agency or local government.
The Organization provides services to citizens/customers/students and is made up of the 8 Roles.
The Organization may collect and/or hold citizen/customer/student data, and that data will include employee data and may include citizen/customer/student.
Personally Identifiable Information (PII) and Personal Health Information (PHI) as well as financial information.
Citizens/customers/students rely on the Organization.

ORGANIZATION Chart



- Leader
  - Human Resources (HR)
    - Employee and Benefits Data
  - Finance
    - Financial Management & Reporting
    - Cloud based Payroll
  - Communication /Media
    - Social Media Accounts
  - Operations
    - Business Development
    - Property Management
    - Building Automation System (HVAC, Elevators, Fire)
  - Information Technology (IT)
    - Phones
    - Internet
    - Email
    - Network & Computers
  - Legal/Risk /Compliance
    - Cyber Insurance
  - Security/Law Enforcement
    - Physical Security
    - Law Enforcement Contacts

MassCyberCenter
at the MassTech Collaborative

GAME PLAY: 1-HOUR GAME For 5+ Participants (1 FACILITATOR, 4+ PLAYERS)

MassCyberCenter
at the MassTech Collaborative

Instructions: To get the full value of the game, an organization should play the full 1-hour game first. The purpose of the 1-hour game is to:

Collaborate and practice cyber incident response actions within a safe, training environment
Assess what information and resources are needed to respond to and recover from an incident
Identify opportunities to improve cyber incident response plans

Setup:

The Facilitator chooses a Scenario card and related Injects. No information is shared. Additional 1-hour Scenarios will be available at MassCyberCenter.org.

The Facilitator places all 8 Role cards on a table, along with the Organization Chart; GAME PURPOSE, OBJECTIVE, and COMPONENTS SHEET; and 1-hour game Instructions.
The Facilitator asks players to each take a Role card and familiarize themselves with the Role and the game (using the materials on the table).
If there are less than 8 players at the table, have players take a second Role card to fill all the Roles. Every Role should be filled, and every player at the table must participate.
Players should take their Roles seriously, even if they do not perform that function in real life.
Give players 5 minutes to familiarize themselves with the game and their Roles.

Gameplay:

Facilitator hands Injects, one-by-one (in order) to each Role indicated on the Inject card and asks, "What do you do with this information?"
When a player in a Role receives an Inject card, they may choose to share the information with other Roles or the Organization (all 8 ROLES) in-whole, in-part, or not at all.
Wait for discussion after each Inject. If there is none, the Facilitator may ask leading questions about the Inject to the Role or Organization to help generate discussion.
After last Inject is used, and discussion has ended, read the Scenario to the Organization and go through Hot Wash card questions.

Responsibilities:

The Facilitator's responsibility is to guide the players through the game. The Facilitator does not "play" the game, represent any Role, or have a purpose within the Organization. Scenario information and Injects will be provided by the Facilitator only.

GAME PLAY: 15-MINUTE DISCUSSION For 5+ Participants (1 FACILITATOR, 4+ PLAYERS)

Instructions: The purpose of the 15-minute discussion is to promote a culture of cybersecurity and raise awareness of how stakeholder actions impact cybersecurity incidents.

Use the Scenario cards as a tool to promote healthy discussion about cybersecurity incidents and incident response actions in a no-fault environment. There are no "right" or "wrong" answers -- just an opportunity to understand what happens during an incident and how to respond to it.

The Facilitator should choose one Scenario card for the discussion.
The Facilitator reads the Scenario card to the discussion participants.
The Facilitator may ask participants, "If this happened at our Organization, what would we do?"
Using the Notes on the bottom of the Scenario card, the facilitator may ask probing questions about who should be involved in identifying and responding to an incident and what actions and processes might be appropriate to mitigate the situation and recover. Consider policies, processes, and communications appropriate to the Scenario.

[OPTIONAL] Identify one area for improvement and the tasks needed to implement any changes.