CIS 358
Information Assurance

Lecture 7

Dr. Sutton

Information Assurance Policy

Executive Level Roles

- CIO – Chief information officer
  - Responsible for information systems and information management
- CISO – Chief information security officer
  - Responsible for information security for an organization
- CRO – Chief Risk Officer
  - Responsible for decisions regarding risk
- CSO – Chief security officer
  - Responsible for all security, including both information security and physical security

Guest speaker - Luke DeMott

- Chief Information Security Officer (CISO)
- Talk scheduled on Wednesday 3/15 during class time
- Attendance is mandatory for all students
- You are encouraged to ask questions during the session and/or put them in the shared Google doc

Security Involved Roles

- Information owner / Data owner
  - Has responsibility/ authority for certain information assets in an organization
  - Responsible for determining appropriate use and level of protection necessary on the information asset
  - Provides input to information system owners, who work with ISSO for appropriate security measures

- Information system owner
  - Responsible for an information system. Must balance needs of users with assuring compliance with security plan. Manages access to system, works with ISSO for developing security plan

- Users

  Need to reasonably protect data they have access to (prevent themselves from being the point of failure).

Controls to Reduce Risk

Information Assurance Policy

- Why do we need policies?
- How to make, evaluate, implement policies?

Why Information Assurance Systems Are Vulnerable?

- **Human factors**

  Errors, careless, upset/angry employees, conspiracy, *etc*.

- **Natural disasters**

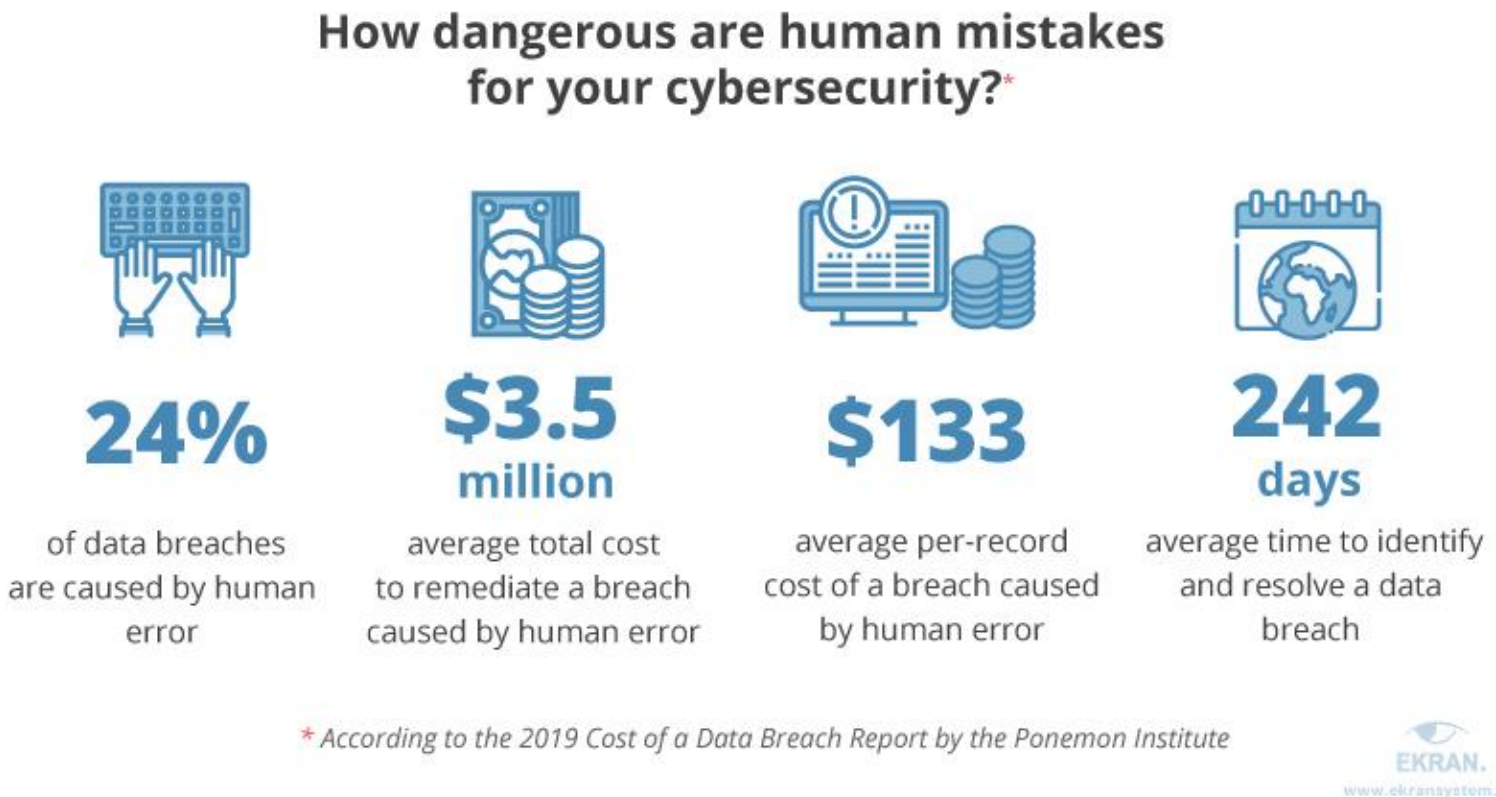
  Power failure, flood, fires, earthquake, pandemic, *etc*.

  Ex: Hurricane Florence phishing scams

- **Technological factors**

  Hardware issues, software issues, network issues, *etc*.

How Dangerous Are Human Mistakes for Your Cybersecurity System?



[Cost of a data breach 2022 | IBM]

Policy

What is a policy?

A document or set of **rules, expectations, patterns of behavior** and **procedures** in written format that specifies what an organization **requires or expects** their employees to do and to not do to protect the organization’s information assets.

Purpose of the Policy

- Recognizing sensitive information assets
- Clarifying security responsibilities
- Promoting awareness for existing employees
- Guiding new employees
- Describes consequences for noncompliance

Policy Today

Guiding Principles

Corporate culture can be defined as the shared attitudes, values, goals, and practices that characterize a company, corporation, or institution.

Guiding principles set the tone for a corporate culture. Guiding principles synthesize the fundamental philosophy or beliefs of an organization and reflect the kind of company that an organization seeks to be.

Not all guiding principles, and hence corporate cultures, are good.

Culture can be shaped both informally and formally.

Informally: shaped by how individuals are treated within an organization.

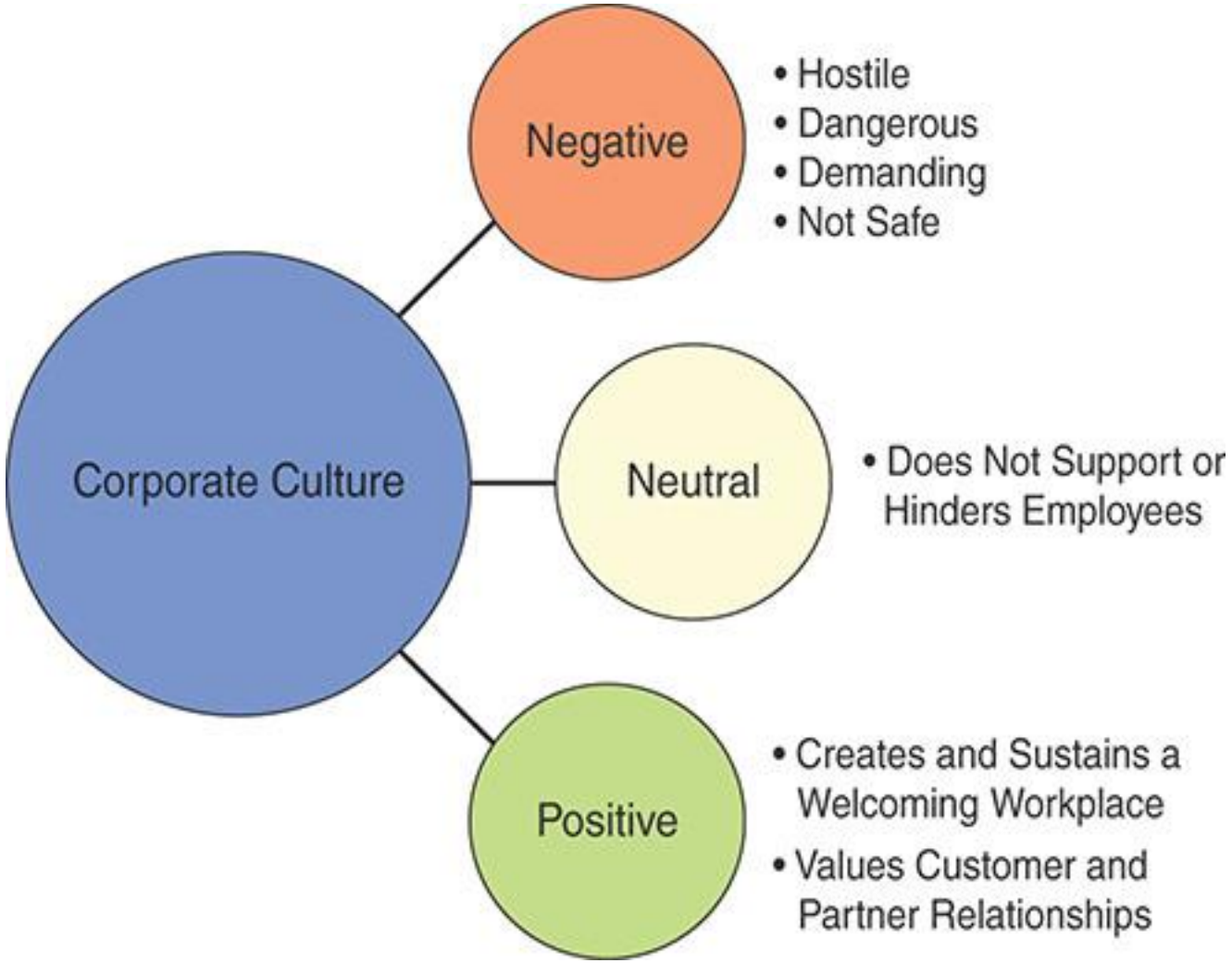
Formally: shaped by written policies.

Policy Today

Corporate culture

Corporate cultures are often classified by how corporations treat their employees and their customers.

The three classifications are negative, neutral, and positive



An Example of Corporate Cultures

Let’s consider an example of two companies. Both experience a data breach that expose customer information; both companies call in experts to help determine what happened.

In both cases, the investigators determine that the data-protection safeguards were inadequate and that employees were not properly monitoring the systems.

The difference between these two companies is how they respond to and learn from the incident.

An Example of Corporate Cultures

Negative corporate culture

Company A

Quick to respond by blaming the department management, firing key employees, and looking for ways to avoid legally required customer notification.

Company B

Positive corporate culture

Leadership shares the report with the department, solicits internal and external feedback on how to improve, researches new controls, methodically implements enhancements, and informs customers in a timely manner so they can take steps to protect themselves.

High level components

- Policy Statement
  - Goals of policy, who it applies to, high level rule to be enforced
    - Ex: Accounts must have strong password
- Standard
  - Furthermore, detailed rules that support the policy statement
    - Ex: 12-character passwords with complexity
- Procedures
  - Step by step instructions that should be followed to comply
    - Ex: Select Ctrl-Alt-Del and choose “change”
- Guidelines
  - Advice to help reader comply with policy

Policy Elements

- Policy statement
- Objectives
- Scope
- Definitions
- Responsibilities
- Compliance / enforcement
- References
- Related docs
- Effective date
- Signature
- Exception / exemption process

GVSU Policy Example

Email Policy - University Policies - Grand Valley State University (gvsu.edu)

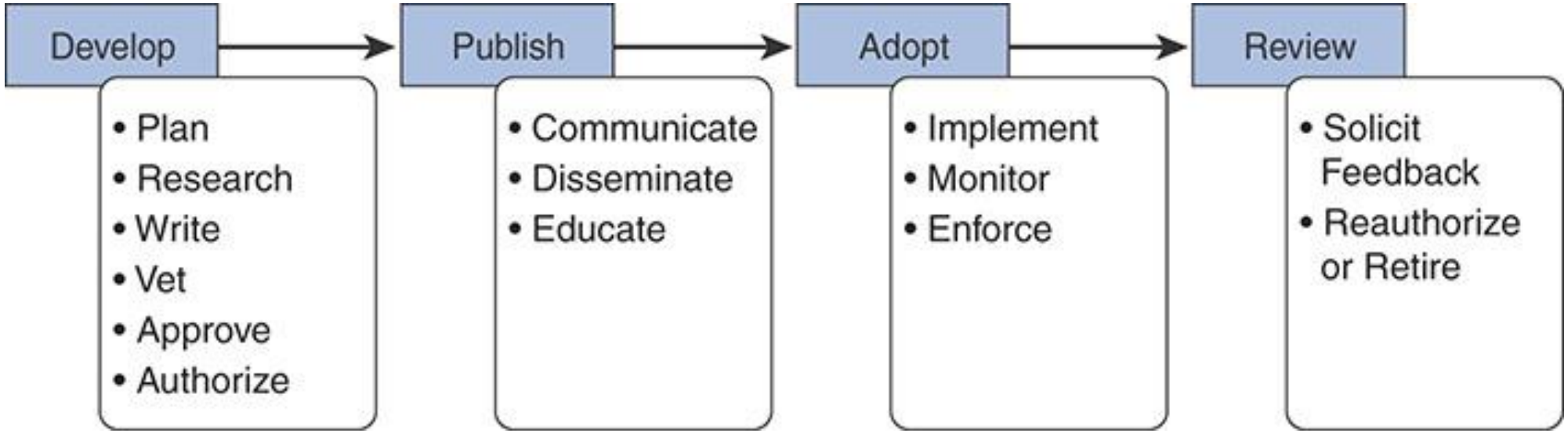
formation Security Policy Templates | SANS Institute

Policy Organization

- Singular Policy
  - Each policy is separate document
  - Single topic short documents make it easy to find appropriate information

- Consolidated Policy
  - Related policies grouped together
  - Easier to find related information
  - Easier to maintain consistency

Cybersecurity Policy Life Cycle



Plan-Do-Check-Act cycle

Policy Development

- Information gathering
  - An overview of IT infrastructure and a list of IT systems.
  - Current policies, standards, guidelines or procedures.
  - Risk management or audit reports as references
  - Security incidents or other loss-related historical information.
- Policy framework definition
  - A list of topics covered
  - How to present the policies
  - Etc.

Policy Publication

- The objective of the communication task is to deliver the message that the policy or policies are important to the organization.
- Disseminating the policy – make it available.
- Company-wide training and education build culture.

Policy Adoption

- Implement the policy
  - Make sure it is well understood when the policy goes into effect
  - Prior to the effective date, support transitional activities
- Monitor and enforce compliance with policy
  - If there are no consequences for non-compliance, then there is no reason why anyone should comply
  - Enforcement should be uniform
    - Management should be subject to same policy as other employees
    - Exceptions may be made if well-justified

Policy Review

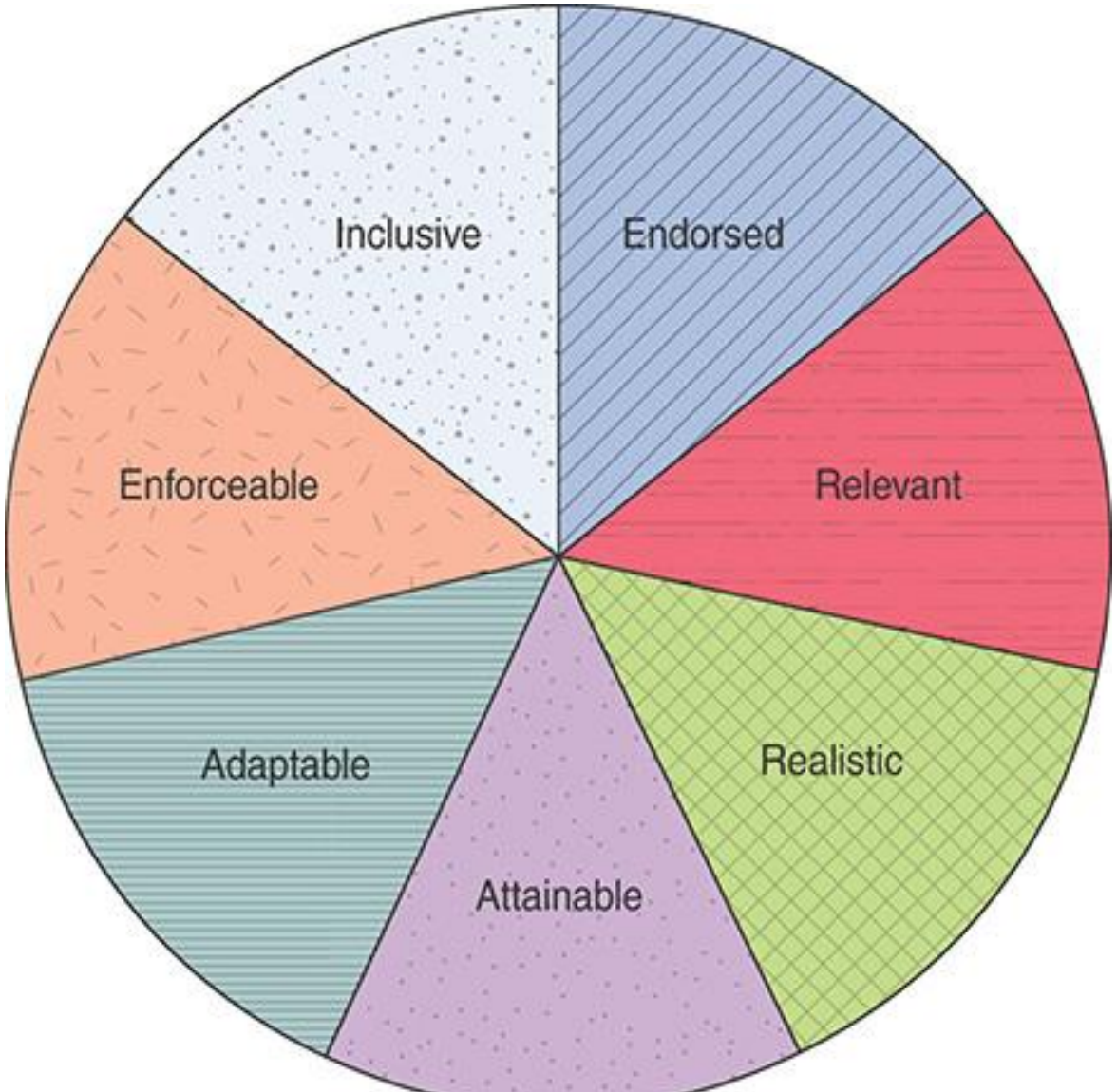
- Policy needs to be reviewed regularly
  - Inconsistent or inapplicable policy creates confusion
- Feedback should be considered
  - There are often unanticipated consequences
- Update the policy if appropriate
  - Policy that does not work should be changed
  - Identify different versions (version number or date)
  - Archive old versions
- Retire the policy if appropriate
  - If it is no longer applicable there is no need for it.

Information Security Policy

Successful policy characteristics

- **Endorsed:** has the support of management
- **Relevant:** applicable to the organization
- **Realistic:** the policy makes sense
- **Attainable:** the policy can be successfully implemented.
- **Adaptable:** the policy can accommodate changes.
- **Enforceable:** the policy is statutory
- **Inclusive:** the policy scope includes all relevant parties.

All Are Equally Important



Group Discussion

Please discuss on the importance of the characteristics.

- **Endorsed:** has the support of management
- **Relevant:** applicable to the organization
- **Realistic:** the policy makes sense
- **Attainable:** the policy can be successfully implemented.
- **Adaptable:** the policy can accommodate changes.
- **Enforceable:** the policy is statutory
- **Inclusive:** the policy scope includes all relevant parties.

Policy Considerations

Cybersecurity Policies Need to Take Into Consideration:

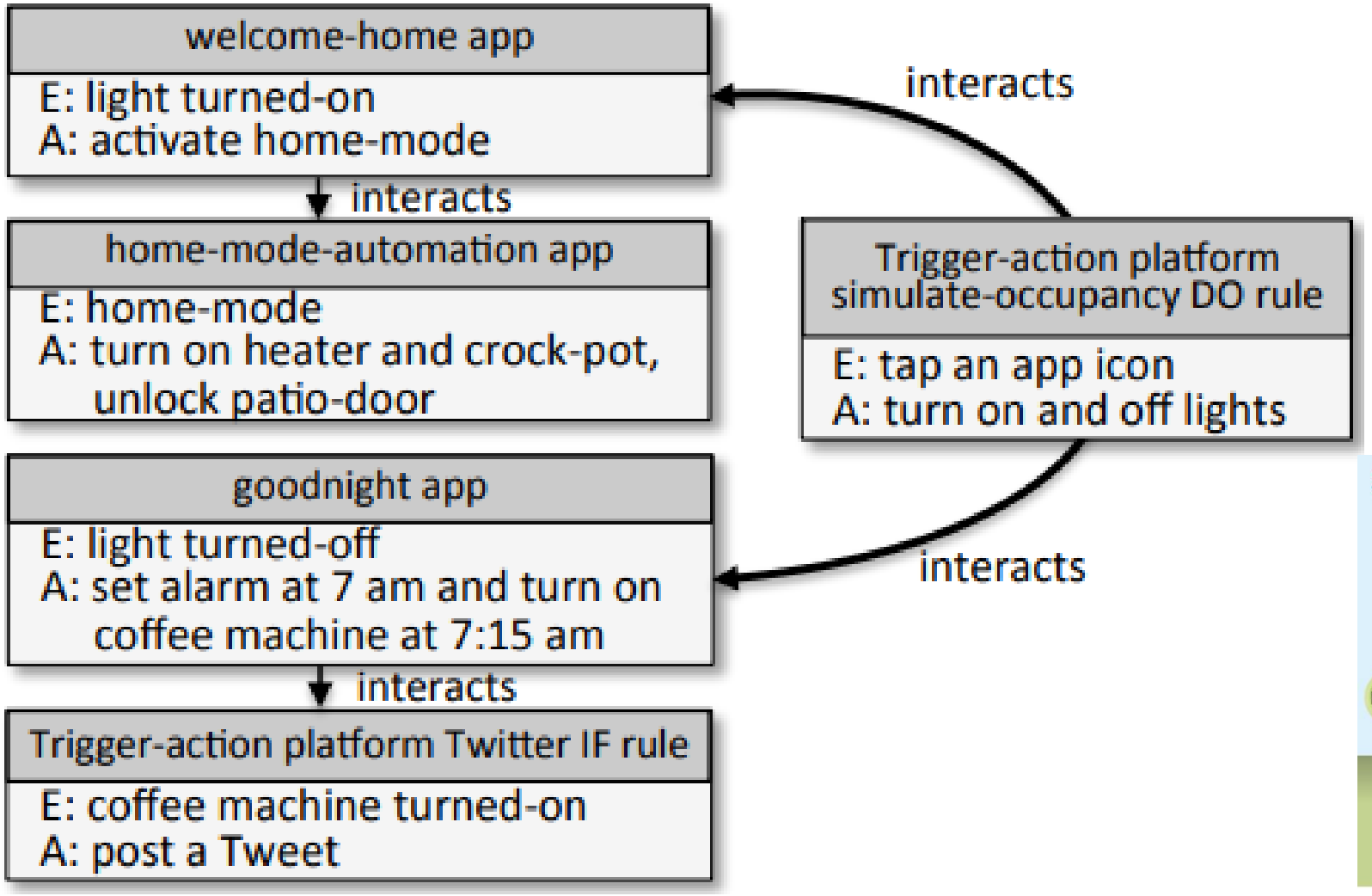
Organizational Objectives

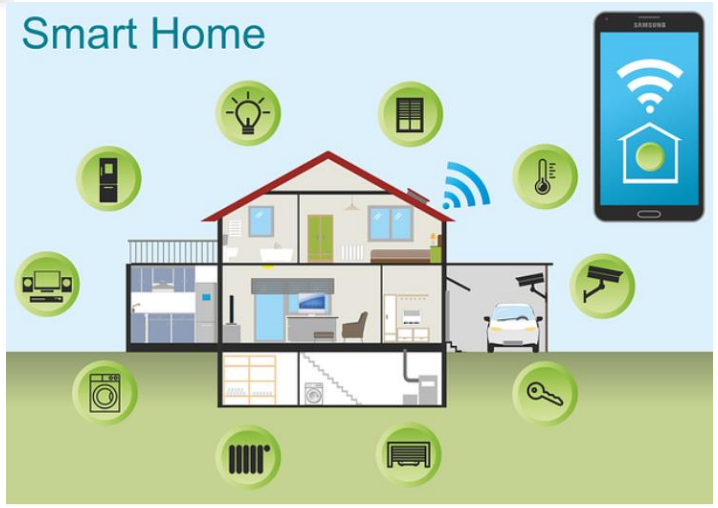
Laws: International laws; state laws; regulations; *etc*.

The Cultural Norms of Its Employees, Business Partners, Suppliers, and Customers

Environmental Impact and Global Cyber Threats

IOT safety policy





IOTGUARD: Dynamic Enforcement of Security