Cyber Security Management
Lesson Introduction

- Understand **organizational context** for cyber security
- Understand the **people, process and technology dimensions** of cyber security management
- Assessing **cyber risk and its relationship** to security management

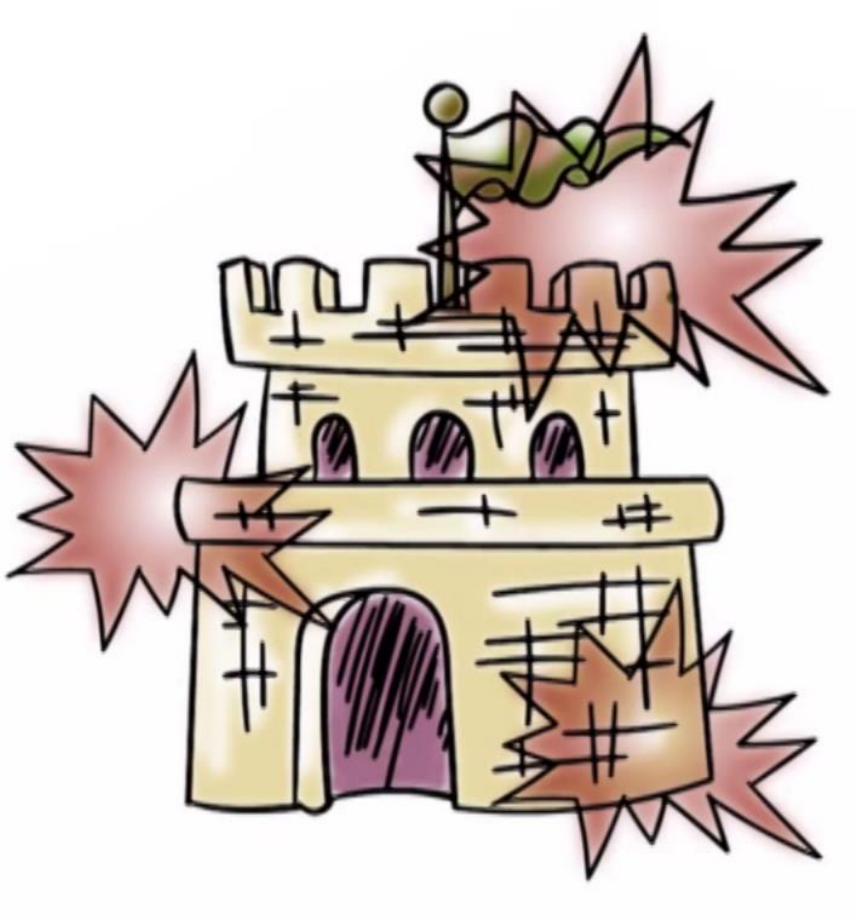
Managing Security

- **Technical controls** (authentication, access control etc.) are used to reduce the risk of attacks on valuable assets.
  - **What assets need to be secured and from whom?**

Organizational Context

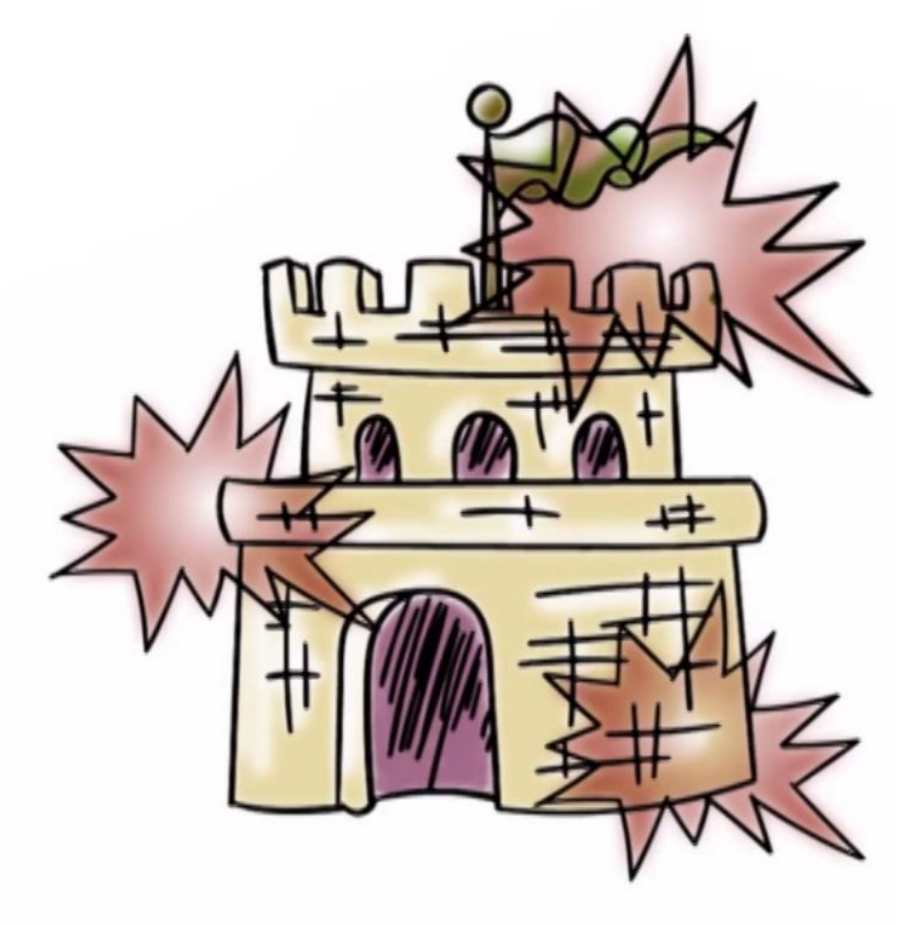
- **Legal and compliance drivers for cyber security**
  - Financial and health data
- **What technical controls should be deployed?**
  - Must understand risks posed by threats
  - Costs and benefits of security measures

Key Challenges



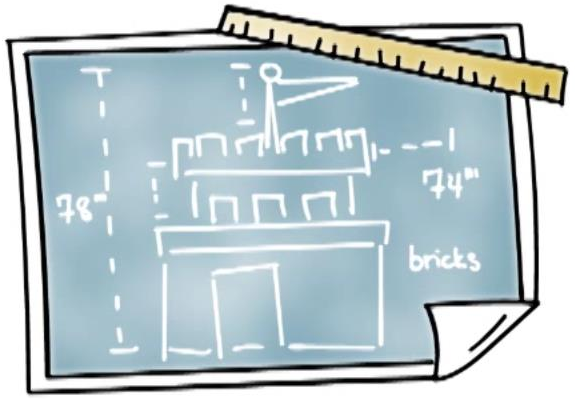
- What assets are under risk?
- **What are the threats and how serious is the risk posed by them?**
  - Likelihood of successful attack and its impact

Key Challenges



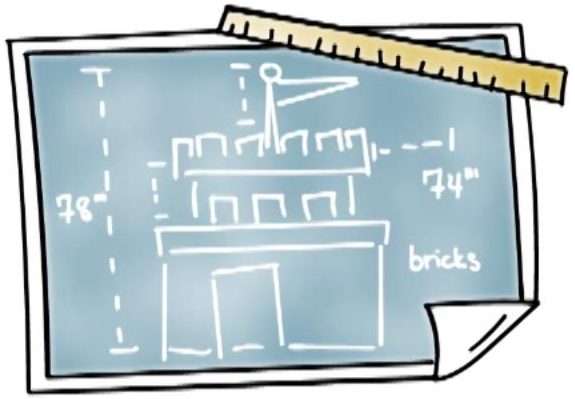
- **What technological solutions/controls exist to counter threats?**
- **How can we address risk in a cost-effective manner?**
  - Cost is less than reduction in risk
- How do we understand people and process aspects of cyber security management?

Security Planning



- **What needs to be secured?**
- Who is responsible for it?
- What technical/non-technical controls should be deployed?
- How are people supported to do what they need to do?
- **What if something goes wrong?**
  - Response and recovery
  - Accountability and consequences

Assets and Threats



- **What Needs to be Secured?**
  - **Hardware, software and services**
    - Servers, routers, switches, laptops and mobile devices
    - OS, databases, services and applications
    - Data stored in databases or files
  - **From whom?**
    - Remote hackers?
    - Insiders?

Security Planning: Controls

- **Identity and access management (IAM)**
  - Credentialing, account creation and deletion
  - Password policies
- **Network and host defenses**
  - Firewalls, IDS, IPS
  - Anti-virus
- **VPN and BYOD**
- Vulnerability patching
- **User awareness and education**
  - Phishing attack awareness (Phishme)

Security Planning: Security Policy

- **High level articulation of security objectives and goals**
  - Legal, business or regulatory rationale
  - **Do's and don'ts for users**
    - Password length
    - Web and email policies
    - Response to security events
  - Address prevention, detection, response and remediation as it concerns/impacts users

Georgia Tech Computer and Network Use Policy

- **States guiding principles**
  - Protect GT IT resources
  - Ensure no state or federal laws are violated
- **Some interesting highlights**
  - Copyright and IP
  - Export control
- **Who is responsible?**
  - **Network** – Office of Information Technology
  - **Devices** – Units or individual

Cyber Risk Assessment

- Investments in cyber security are driven by risk and how certain controls may reduce it
- **Some risk will always remain**
- How can risk be assessed?

Quantifying Cyber Risk

Risk exposure = Prob. [Adverse security event] * Impact [adverse event]

$$\text{Risk Leverage} = \frac{\text{Risk exposure before/without a certain control} - \text{Risk exposure after the control}}{\text{Cost of control}}$$

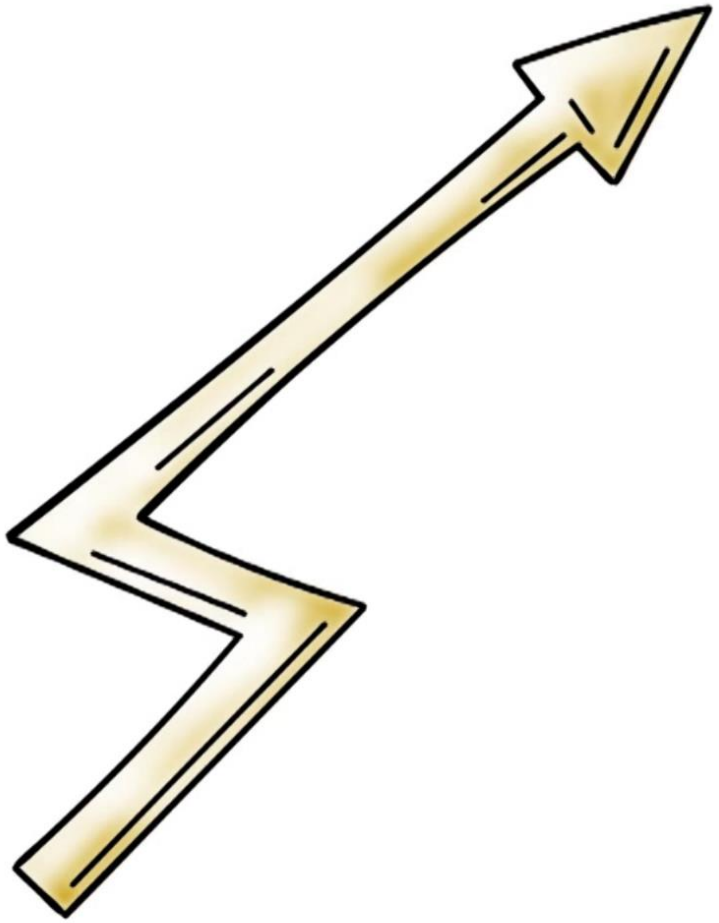
Risk leverage > 1 for the control to make sense

Managing Cyber Risk

How do we assess and reduce cyber risk?

- **Impact**
  - Expected loss (reputational, recovery and response, legal, loss of business etc.)
- **Risk management**
  - Accept, transfer (insurance) and reduce
  - Reduction via technology solutions, education and awareness training

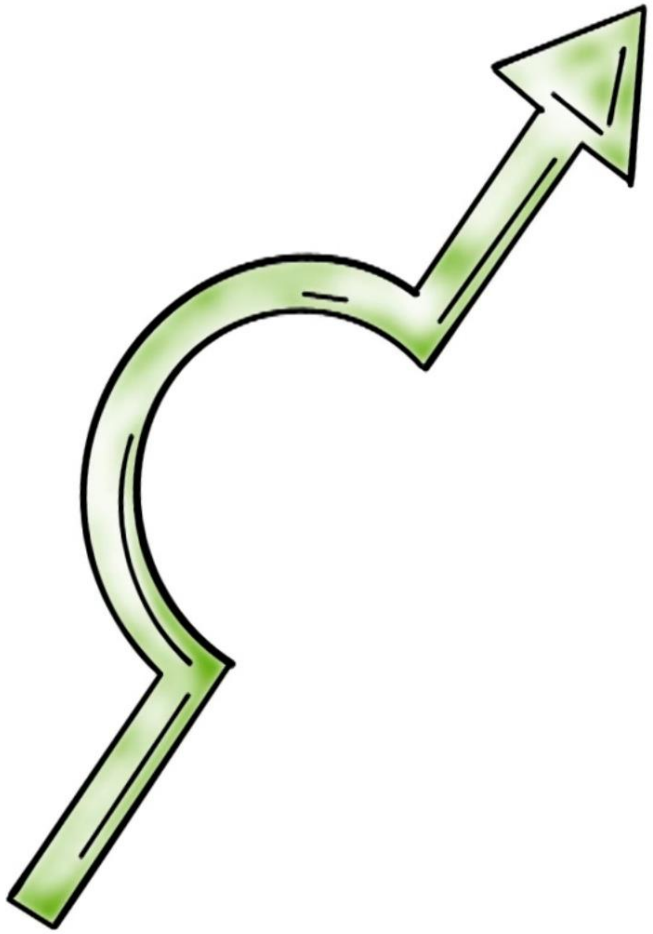
Enterprise Cyber Security Posture



- **Reactive:**

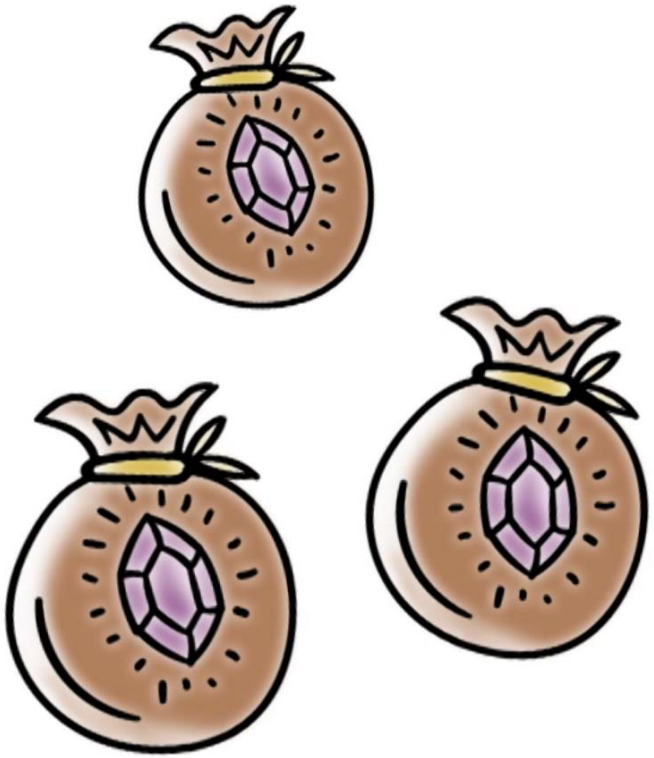
  - Regulation/compliance
  - Customer demands
  - In response to a breach
    (Target or Home Depot)
  - In response to events

Enterprise Cyber Security Posture



- **Proactive:**
  - Champion of an organization who has influence
  - Board level conversation about cyber security and risk

Enterprise Cyber Security Posture



- **Economic value argument:**
  - Return on investment (RoI)
  - Estimating costs and benefits is tricky
  - Perception vs. data-driven risk

Security Planning and Management

- **Values at risk**
  - Assets, reputation etc.
- **Threats and attack vectors**
- **Plan, implement and manage**
  - Deploy appropriate controls
  - Empower people and hold them responsible
  - Plan for response and remediation (do not be surprised)
  - User awareness
- **Understand and proactively address risk**

Cyber Security Management
Lesson Summary

- Managing cyber security is a **complex process that involves technology, people and processes**
- Organizational context and **cost/benefit analysis is necessary** for security controls
- **Risk based argument** for cyber security