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

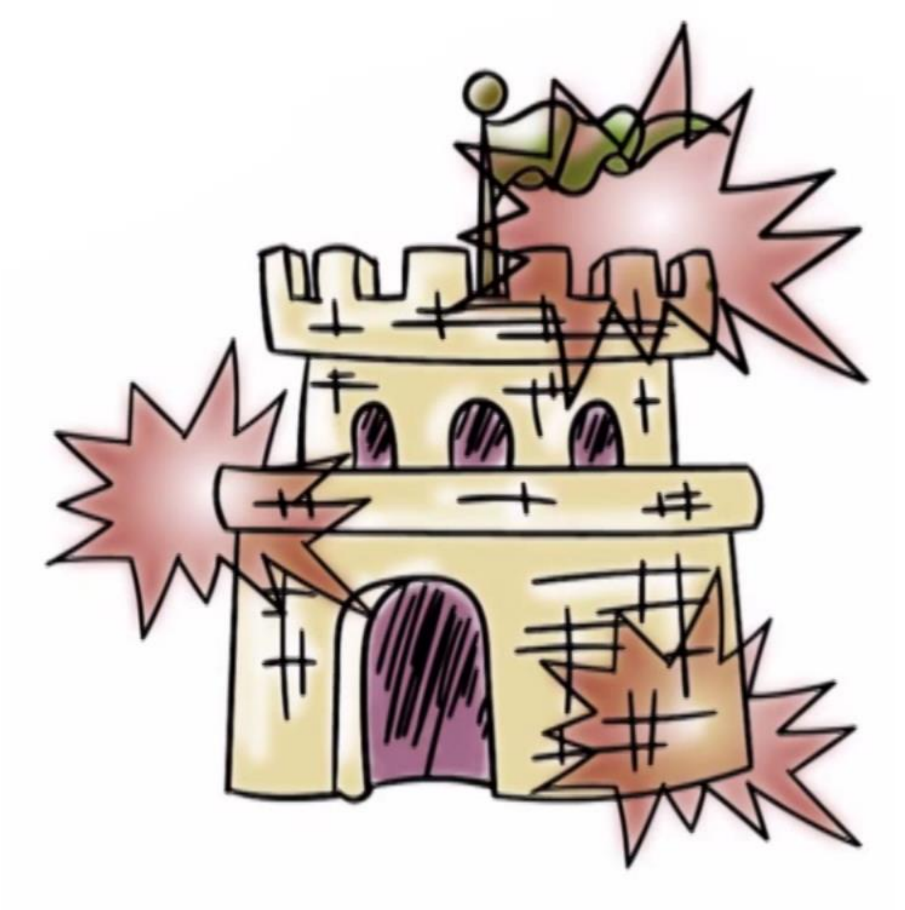
- **Technical controls** (authentication, access control etc.) are used to reduce the risk of attacks on valuable assets.

  - **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

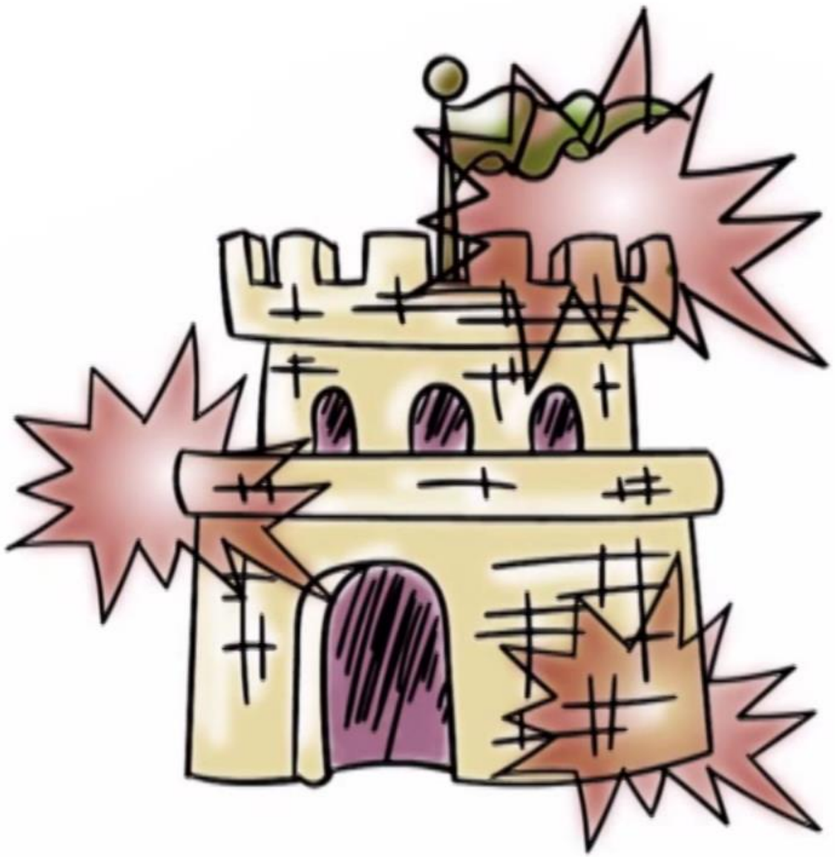


- What assets are under risk?

- **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?

Network Use Policy Quiz

Cyber security planning and management in an enterprise must define allowed computer and network use by employees. Georgia Tech’s computer and network use policy strives to do this for students, faculty and staff. **Check all that you think are required by this policy:**

- □ Georgia Tech account passwords should be changed periodically.
- □ A compromise of a computer should be reported to someone responsible for cyber security at Georgia Tech.
- □ Georgia Tech computers cannot be used to download illegal content (e.g., child pornography).

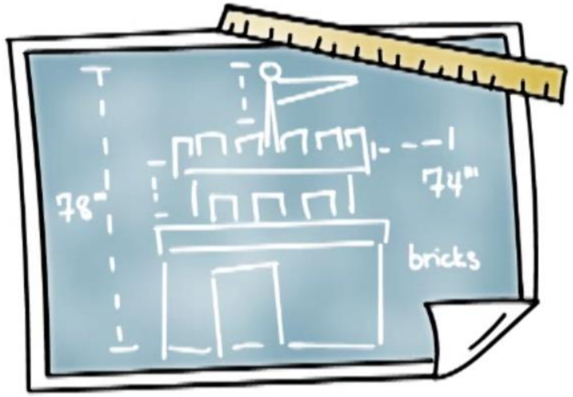
Botnet Quiz

A botnet operator compromises a number of computers in a company. The malware executed by the bots only sends large amounts of spam email but does not exfiltrate sensitive data or interfere with legitimate activities. **Choose the appropriate action by the company in this situation:**

□ The company should detect and prevent abuse of its resources by unauthorized parties.

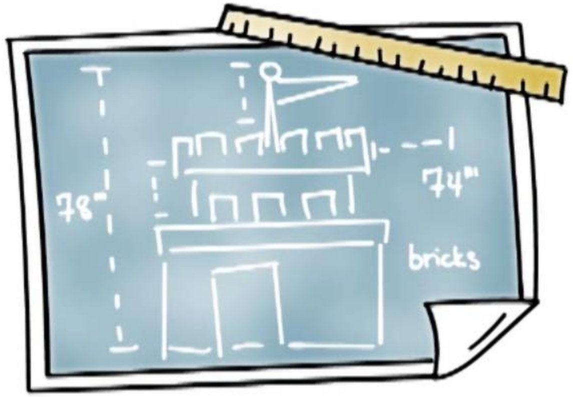
□ Since it poses no risk to company’s sensitive data or normal operations, it can be ignored.

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 Audit Quiz

A news story in 2014 reported that an inspector general’s report gave Veteran Affairs (VA) a failing grade for 16th straight year. The CIO of VA discussed a number of challenges that could explain this grade. **Mark the ones that you think could be possible reasons:** (See the **instructor notes** for a link to the article)

- □ The need to manage cyber security for over a million devices each running many services
- □ Lack of sense of urgency in fixing cyber vulnerabilities.
- □ Choosing to support key functions even when this could introduce vulnerabilities.

CISO Quiz

Choose the best answer.

Chief Information Security Officer (CISO) is the executive who is responsible for information security in a company. Did Target, the major retailer, have a CISO when it suffered the serious breach?

□ Yes

□ No

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

Computer Use Policy Quiz

Choose the best answer.

Does Georgia Tech’s computer and network use policy prohibit personal use of university resources?

□ Yes

□ No

Student Privacy Quiz

Choose the best answer.

Georgia Tech systems store student data such as grades. The Institute must protect such data due to...

□ Regulatory reasons

□ Because the data is sensitive it can only be disclosed to student and his/her family

Anthem Breach Quiz

Choose the best answer.

Anthem suffered from a major breach in 2015. Based on an analysis of its response to the breach, did Anthem respond well to the breach? (see the **instructor notes** for a link to the analysis)

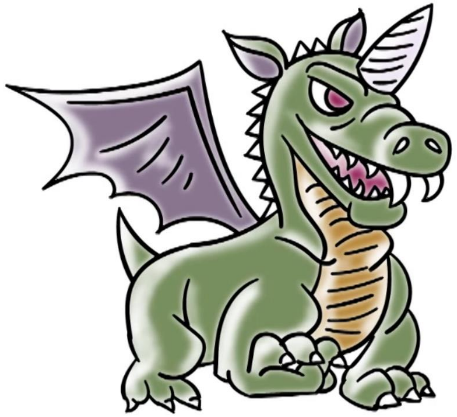
□ Yes

□ No

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

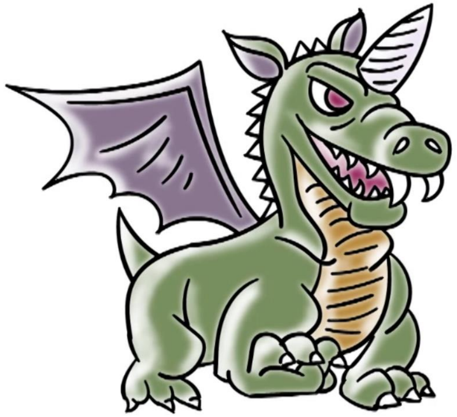


Risk exposure = Prob. [Adverse security event] * Impact [adverse event]

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

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

Security Breach Quiz

Mark all applicable choices.

A company stores sensitive customer data. The impact of a breach of such data must include...

- □ Cost of purchasing identify theft protection for customers
- □ Loss of business due to reduced customer confidence
- □ Compensation for new cyber security personnel the company hires to better manage cyber security in the future

Reducing Exposure Quiz

Choose the best answer.

A company is considering two possible IDS solutions to reduce its exposure to attacks on its network. The first one costs $100K and reduces risk exposure by $150K. The second one costs $250K but reduces risk exposure by $500K. Which solution would you recommend?

- □ Cheaper solution that costs $100K
- □ More expensive solution that costs $250K

Cyber Insurance Quiz

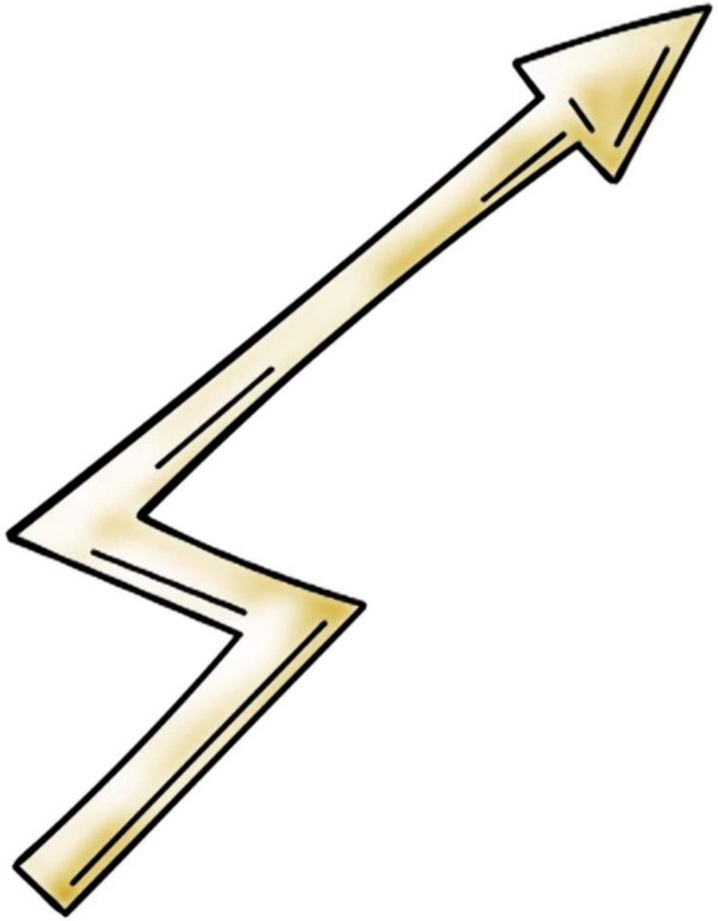
Choose the best answer.

Cyber insurance is still not very popular. Based on a 2014 survey, what percentage of customers of major insurance brokers were interested in buying cyber insurance? (see the **instructor notes** for a link to the survey)

□ Less than 25%

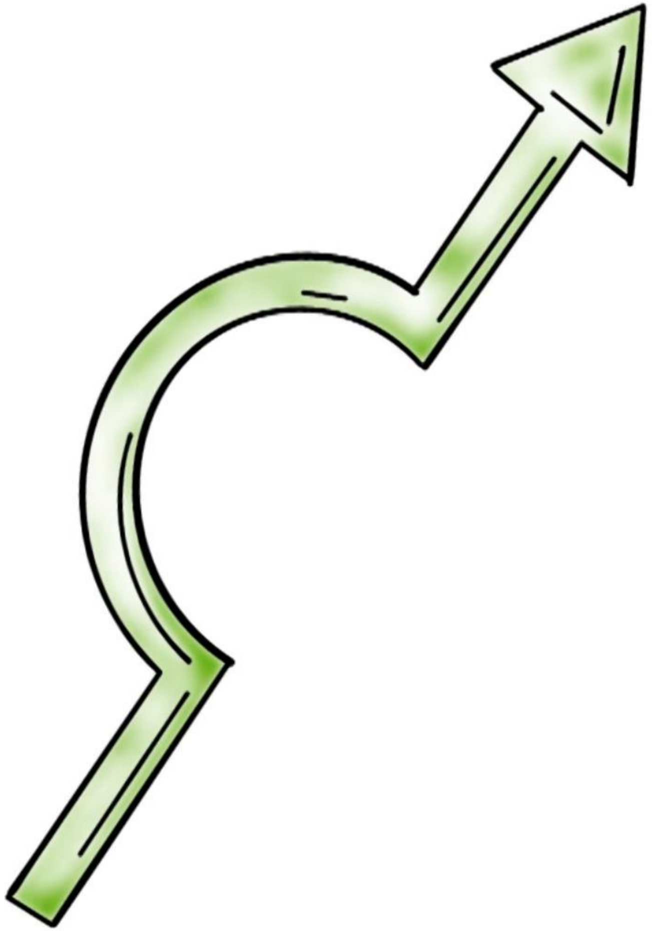
□ Over 50%

Enterprise Cyber Security Posture



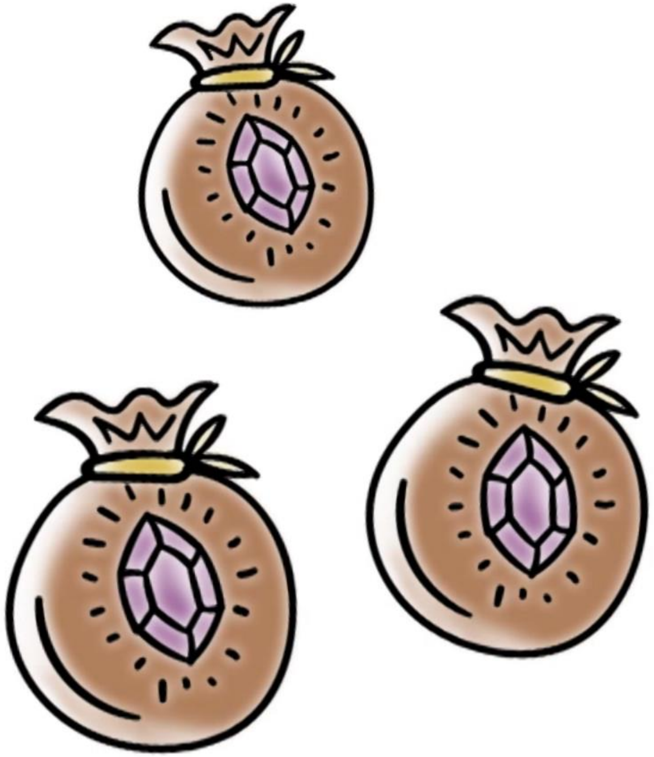
- **Reactive:**
  - Regulation/compliance
  - Customer demands
  - In response to a breach (Target or Home Depot)
  - In response to events

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

Bringing It All Together!

- **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 Budgets Quiz

Choose the best answer.

Are cyber security budgets increasing as the number of reported incidents increases (see the **instructor notes** for a link to the PwC report)?

□ Yes

□ No

Proactive Security Quiz

Choose the best answer.

An example of proactive security measure is...

□ Making sure the company complies with all regulatory requirements

□ Chief risk officer (CRO) of the company addressing cyber risk regularly at highest level (e.g., board) when other risks are discussed

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