# Infosheets: Security Program Roadmap Planning

## Goals

* Quick, interactive practice of a process for developing a security program plan
* Build from a foundation of understanding institutional business and goals
* Review of the scope of the information security program

## Process structure

1. Organizational alignment
   * Review your institution’s general strategic goals
   * If you have a risk management team, review their risk reduction plans/goals
   * Review your IT department(s) initiatives and goals
   * Highlight items with clear security involvement and also unclear items
2. Business risks
   * Review and brainstorming of risk landscape (example items provided)
   * Highlight items with high risk in your environment and those that could potentially be addressed with IT controls/processes
   * Focus on convergence of high risk and potential for IT-based mitigations
3. Mitigations
   * List existing mitigations for the highlighted risks
   * Rough estimation of effectiveness of mitigation and remaining risk
   * Brainstorm new mitigations that could be pursued
   * Highlight high value mitigations
4. Prioritization and planning
   * Rank the potential security initiatives identified above by biggest risk reduction potential
   * Identify and prerequisites or “order of operations” items that need to be added to the list or change the order of the list
   * Basic t-shirt size evaluation of effort (one for time and another for money)
   * Slot items into “tracks” and begin mapping out high level timeline by quarters

## Business risk examples:

* Financial
  + Breach notification/credit monitoring costs
  + Fines or other business impact due to compliance failures
  + Fines related to breaches/incidents (PCI-DSS, HIPAA, etc.)
  + Lost revenue due to inability to processes credit card payments
  + Direct financial theft (wire transfer, direct deposit, ghost employees, fake vendors, insider fraud, etc.)
  + Theft of physical assets (stolen laptops, poor physical security, altered physical security, etc.)
  + Decrease in alumni giving (if there is a breach of alum PII?)
  + Consume internal staff time to respond (IT, legal, executives, etc.)
  + Incident investigation costs (third-party forensics, breach investigation, etc.)
  + Service/data restoration costs (third-party expenses)
  + Lost productivity due to key IT services being offline
* Legal
  + Internal and external resources consumed by law suits brought by individuals or business partners
  + Increased work from FOIA requests following an incident
  + Heightened regulatory scrutiny after an incident brings work for legal, administrative and IT teams
* Safety
  + Payroll failure puts paycheck-to-paycheck employees at risk for housing and food
  + Patient care risks due to medical device or data unavailability or integrity issues
  + Do labs or heavy equipment areas put employees or students at risk during a power outage? (SCADA security)
  + Unable to place emergency call (911) during a phone system outage
  + Exposure of PII for privacy-enacted students could lead to safety risk for those who enacted privacy due to stalking, celebrity status or other threat
* Reputational
  + Occupy PR staff time with media response
  + Lose political capital in lobbying for political issues and funding
  + Customer turn-over reaction from merchant related breaches (bookstore, events, etc.)
  + Decreased applicant pool reaction from applicant related breaches (no documented cases?)
  + Negative alum reaction?
  + Time and cost resulting from increased regulation from government entities in reaction to incidents

## Risk framework definitions

**Likelihood**:

* High: Threats have been observed frequently in higher education, healthcare and other relevant industries within the last 3 years
* Moderate: Threats have been observed occasionally in higher education, healthcare and other relevant industries within the last 3 years
* Low: Threats have been observed rarely in higher education, healthcare and other relevant industries within last the 3 years

**Impact**:

* Financial – direct or indirect monetary costs to the university
  + High – direct or indirect monetary costs to the institution where liability must be transferred to an organization which is external to the campus, as the institution is unable to incur the assessed high end of the cost for the risk; this would include for e.g. Use of an insurance carrier
  + Moderate – direct or indirect monetary costs where liability is transferred to the campus as the business unit/school is unable pay the assessed high end cost for the risk
  + Low – impact results in direct or indirect monetary costs to the institution where business unit/school can solely pay the assessed high end of the cost for the risk
* Reputation – Loss of institutional reputation
  + High – when the impact results in negative press coverage and/or major political pressure on institutional reputation on a national or international scale
  + Moderate – when the impact results in negative press coverage and/or minor political pressure on institutional reputation on a local scale
  + Low – when the impact has a nominal impact and/or negligible political pressure on institutional reputation on a local scale
* Safety – Places campus community members at risk for injury
  + High – Threat places community member(s) at eminent risk of injury
  + Moderate – Threat noticeably increases likelihood of injury to community member(s)
  + Low – Threat has nominal impact on safety of campus community members
* Legal – results in legal or regulatory action against the university
  + High – when the impact results in significant legal and/or regulatory compliance action against the institution or business
  + Moderate – when the impact results in comparatively lower but not insignificant legal and/or regulatory compliance action against the institution or business
  + Low – when the impact results in none or insignificant legal and/or regulatory compliance action against the institution or business

## Examples of high-level methods and common mitigations:

* Exploiting commercial software vulnerabilities (desktop software, web applications, infrastructure, etc.)
  + Subscribing to vendor vulnerability notifications
  + Well-developed processes for testing and deploying updates
  + Mature vulnerability management process (scanning, reporting, remediating)
  + Configuration management processes (to know software deployment scope and versions)
  + Application sandboxing
  + IDS/IPS systems
  + Web application firewall systems
* Exploiting in-house software vulnerabilities (custom web applications, etc.)
  + Mature software development lifecycle with security considerations
  + Security training for developers
  + Application security assessment training, tools and periodic testing
  + IDS/IPS systems
  + Web application firewall systems
* Endpoint malware infections (data stealers, credential stealers, backdoors, etc.)
  + Well deployed and monitored anti-malware software on endpoints
  + Email virus scanning
  + Application whitelisting
  + Training/awareness about malicious emails
* Phishing or other social engineering
  + Email filtering and/or rewriting of links in email
  + Separate accounts for privileged access and regular use
  + Multi-factor authentication for appropriate users/functions
  + Business process controls (approval workflows, etc.)
  + End-user awareness/training
* Physical access to equipment (theft, buying surplus, dumpster diving, etc.)
  + Whole disk encryption software
  + Device disposal process that includes drive wiping
  + Training/awareness on handling equipment while out of the office
  + Good physical security on site (access management, cameras, etc.)
* Abuse of access by insider
  + Least privilege access systems
  + Business process controls (approval workflows, etc.)
  + Good audit trails for privileged user actions
* Exploit weak network access control to reach controlled systems/data
  + Critical and sensitive systems contained within hardened network segments (firewalls, multifactor auth on VPN, jump-boxes, etc.)
  + Use of reverse proxies or other methods for managing access to end-user services

## High level example attackers/threats

* Individuals seeking personal information from data repositories and systemic data flows (large scale PII theft)
* Individuals seeking credit card or financial account information from data repositories and systemic data flows
* Individuals altering records
  + Students changing grades
  + Employees committing fraud
* Individuals seeking network or system resources
  + Spammers
  + Bitcoin miners
  + Host phishing web forms
* Individuals causing outages of IT services
  + Ransomware encrypting data
  + Politically motivated DDoS attack on website
* Individuals altering information or services to disrepute the institution (e.g. defacing of websites)
  + Hacktivism protesting institutional decisions, individuals, etc.
* Individuals seeking research data content (e.g. designs, formulae, process details)
  + Industrial espionage from commercial entities
  + Competing research organizations
  + Foreign governments
* Individuals seeking personal or account information from end-users
  + Workstation malware that steals consumer online banking logins
  + Personal conflicts motivate stealing access to email, social media, etc.

## Potentially targeted systems

* Credit card processing systems
* Advancement/fundraising systems
* ERP systems (HR, student information system, finance)
* Online course systems (learning management systems)
* Authentication systems (e.g. Active Directory, LDAP, web authN)
* Research data repositories
* VPN services
* Email servers
* Library journal access services (proxy or VPN services)
* Physical access control systems (e.g. card swipe servers)
* Medical records systems (hospital or student health center)
* Database servers
* Internet-facing websites, particularly the primary domain one