## Worksheet: Security program roadmap planning

**Worksheet 1: Organizational alignment**

* 1. What are the core pillars of your institution’s business? (e.g. undergraduate education, scientific research, patient care, community outreach) What are the top 3 auxiliary business areas of your university (e.g. housing, bookstore, athletics, theater, continuing education)
  2. If you have an enterprise risk management team at your institution, ask them for their list of top institutional risks and if they have any particular focus for the coming 12-24 months. Use their list in place of, or in addition to, the sample business risks provided.
  3. What are your institution’s overall strategic goals for the next 12-24 months? (e.g. enrollment growth, increased NIH research funding, new online programs, administrative efficiencies)
  4. What are your IT department’s (central IT and/or other major campus IT partners) major IT service initiatives for the coming 12-24 months? (e.g. wireless network upgrade, changing learning management system platform, migrating email to a SaaS vendor)
  5. In questions 1.2, 1.3 and 1.4, circle items with a clear need for information security team engagement. For items that require more research to determine the security implications, write the name of the person to whom you need to speak for more information.

## Security program roadmap planning

**Worksheet 2: Business risks and IT involvement**

* 1. Review the attached example business risks document on infosheet page 2 (or your list provided by Risk Management). Add at least two additional items that are focused on business risk.
  2. Place asterisks next to items that are high visibility risks at your organization (a sample risk likelihood and impact document is also provided on infosheet page 3). Circle risks that you feel could be mitigated with IT controls or processes.
  3. Pick two items that were both circled and starred in the last step as being high risk and could be mitigated with IT controls or processes.
  4. Review your security team’s internal processes and documentation for clear gaps and list at least three “low hanging fruit” items you could work on. (e.g. documented incident response process, forensics training, web application assessment plan, etc.)

## Security program roadmap planning

**Worksheet 3: Mitigations – existing and potential**

* 1. For each of the risks from step 2.3, list existing mitigations your institution has in place. Keep in mind the combinations of technical controls, business process controls, policies, training, etc. (Use infosheet page 4 for ideas/reminders)
     1. For example, a threat of financial fraud via banking malware might be mitigated by technical controls like IDS/IPS and antimalware software on endpoints. It might also be mitigated by business controls like requiring two people to authorize money transfers and training about recognizing malicious email attachments.
  2. Do the existing mitigations substantially address the risk? If so, lower the priority and move onto high risk items without good existing mitigations.
  3. Brainstorm additional mitigations that could be implemented to address these risks, focusing on the ones with the fewest (or least effective) existing mitigations. (Use infosheet page 4 for ideas/reminders)
  4. Circle the highest value potential mitigations from the prior step. These could be items with very high risk reduction returns (maybe they mitigate multiple risks) or items that take minimal effort to implement (low hanging fruit).

## Security program roadmap planning

**Worksheet 4: Prioritization and planning**

* 1. Combine the lists of potential future mitigations, the circled and starred items from the first worksheet and the internal items from 2.4. Highlight the required items from institutional or departmental initiatives in the coming months. Identify any dependencies between these items or obvious benefits to order.
  2. For each item, provide high level notes if additional funds are required and which other teams are required to implement the mitigations.
  3. Divide the items into tracks that rely on different resources/teams and can be worked in parallel (e.g. training/awareness, network security, endpoint security, data repository security). The number of tracks that can be effectively worked in parallel will be dependent on the resources available within your Information Security team and the availability of resource dependencies.

## Next steps

* Where will you find institutional strategic goals?
* Contact risk management about their top risks – who do you contact?
* Review IT department plans/proposals for coming months (CIO? Project management team?)
* Reach out to names you put on worksheet 1 to get more information on initiatives/projects with unclear security implications.

|  |  |  |  |
| --- | --- | --- | --- |
| **Activity** | **High level effort estimate** | **High level cost estimate** | **Team(s) needed** |
| Implement commercial IPS product | Medium – two quarters | Large - $250k | Security, Networking |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Resource scope and estimation**

Define what S/M/L mean to your institution for effort and cost:

Effort: S \_\_\_\_\_\_\_\_ M \_\_\_\_\_\_\_\_ L\_\_\_\_\_\_\_\_

Cost: S \_\_\_\_\_\_\_\_ M \_\_\_\_\_\_\_\_ L\_\_\_\_\_\_\_\_

**Tracking and timelining**

Tracking a program can help avoid resource conflicts by limiting the number of security projects a given external team (like networking or desktop support) is working with at a time (hopefully to just one or two). It also helps an information security team to manage their amount of work in progress. Consider the size of your team when determining how many tracks can be successfully handled at a given time.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Track** | **Q1** | **Q2** | **Q3** | **Q4** |
| Network security |  |  |  |  |
| Workstation security |  |  |  |  |
| Data governance |  |  |  |  |
| Security monitoring |  |  |  |  |
| Security assessment within other IT projects |  |  |  |  |
|  |  |  |  |  |

**Other considerations**

* You will need to combine these plans with those of the teams you are engaging to ensure their resources would be available
* You will also have to factor in your budget request cycle for items that need funding. When do funds need to be requested and when will you receive them?