Staffing the Information Security Organization

Rationalizing the Staffing Requirements of a Reliable INFOSEC Team

AGENDA

1. Our Findings: INFOSEC Staffing Issues
2. Information Security Areas of Influence
3. Day-to-Day Security Staff Responsibilities
4. How Much Time Should be Spent on What?
5. Follow-Up Considerations
6. Security Budget as a Percentage of IT
7. Example INFOSEC Hierarchy

Our Findings Regarding INFOSEC Staff

- Most organizations' security personnel have ancillary duties
- There is simply not enough time to complete non-security tasks and security-specific tasks
- Functions that are not an immediate need (audit reviews and contingency planning) are often put on hold
- The time-sensitive tasks like credential granting or integrity checking are completed as quickly as possible with no time to review or revise procedures if needed

VOSTROM

INFOSEC: Key Areas of Influence

- Audit
  - Systems, Networks, Processes
- Physical Security Technologies
  - Proximity systems, Biometrics, RFID, tokens
- Disaster Recover / Contingency Planning
- Solution Investigation / Procurement
  - Industry-specific product research
  - Pre-deployment investigation of secure operation

VOSTROM

INFOSEC: Key Areas of Influence - Cont'd

- Security Education, Training, & Awareness
  - Training other internal staff on policies
- Personnel / Credential Issues
  - Performing computer forensic investigations
- Risk Assessment/Management
  - Technology training for the Risk Mgmt group
- Systems and Network Management
  - Systems hardening
  - Creating secure software distributions
  - Reading network device logs

VOSTROM

INFOSEC: Key Areas of Influence - Cont'd

- Training for Internal Staff Education
  - Career training, conference attendance
- Telecommunications Security
  - Periodic check-ups on service providers
  - Turn-up of new VPNs and other connections
- Maintenance of Security Program
  - Upkeep of the overall security posture
  - Development of processes and policies as required

VOSTROM

Day-to-Day Basic Staff Responsibilities

- Reading mailing lists and checking websites for new vulnerabilities that may pose threats
- Reviewing system logs for spurious activity
- Investigating issues / forensic activities
- Developing “hardened” application and system configurations (builds) for IT use
- Upgrading key network defenses to keep up with new threats and software enhancements

Where do we Spend our Time?

Since all organizations are different, the best way to determine how much staff is required is to look at the percentage of time spent daily per area of responsibility based on one staff member. This will serve as the baseline.

Then, the baseline can be multiplied by the complexity and size of the environment to determine the actual staff requirement.

VOSTROM

Where do we Spend our Time?

Based on research from several various-sized organizations that have studied INFOSEC, and determined a dedicated security staff is important, the following percentages are best practice…

Source: Derived from a study by the National Institute of Standards and Technology (NIST)—modified to remove Government requirements

~ Amount of Time Spent per Key Area

Security Staff Functions	Ideal % of Time	Minimum % of Time
Audit	50%	35%
Physical Security Technologies	10%	5%
Disaster Recovery / Contingency Planning	25%	15%
Solution Investigation / Procurement	15%	5%
Security Education, Training, and Awareness	100%	75%
Personnel / Credential Issues	100%	75%
Risk Management / Planning	50%	15%
System and Network Management	100%	50%
Telecommunications Security	50%	25%
Help Desk	15%	5%
Maintenance of Security Program	100%	75%
Totals	6.15 staff years	3.80 staff years

VOSTROM

Follow-up Considerations

- The numbers do not take into account whether line-management is required to perform some of the security duties listed

- Personnel security functions and physical security functions may be areas where staffing levels could be reduced because of management's participation.

  - Security budget compared to overall IT budget is a major factor in determining staffing levels

VOSTROM

Security Budget Compared to IT Budget

- We interviewed several CIOs and CSOs of varying sized organizations in the state of Arizona and found that their security budget was ~ 10% of the overall IT budget.

- CSO magazine suggests 10% of the IT budget spent on security is average nationally.

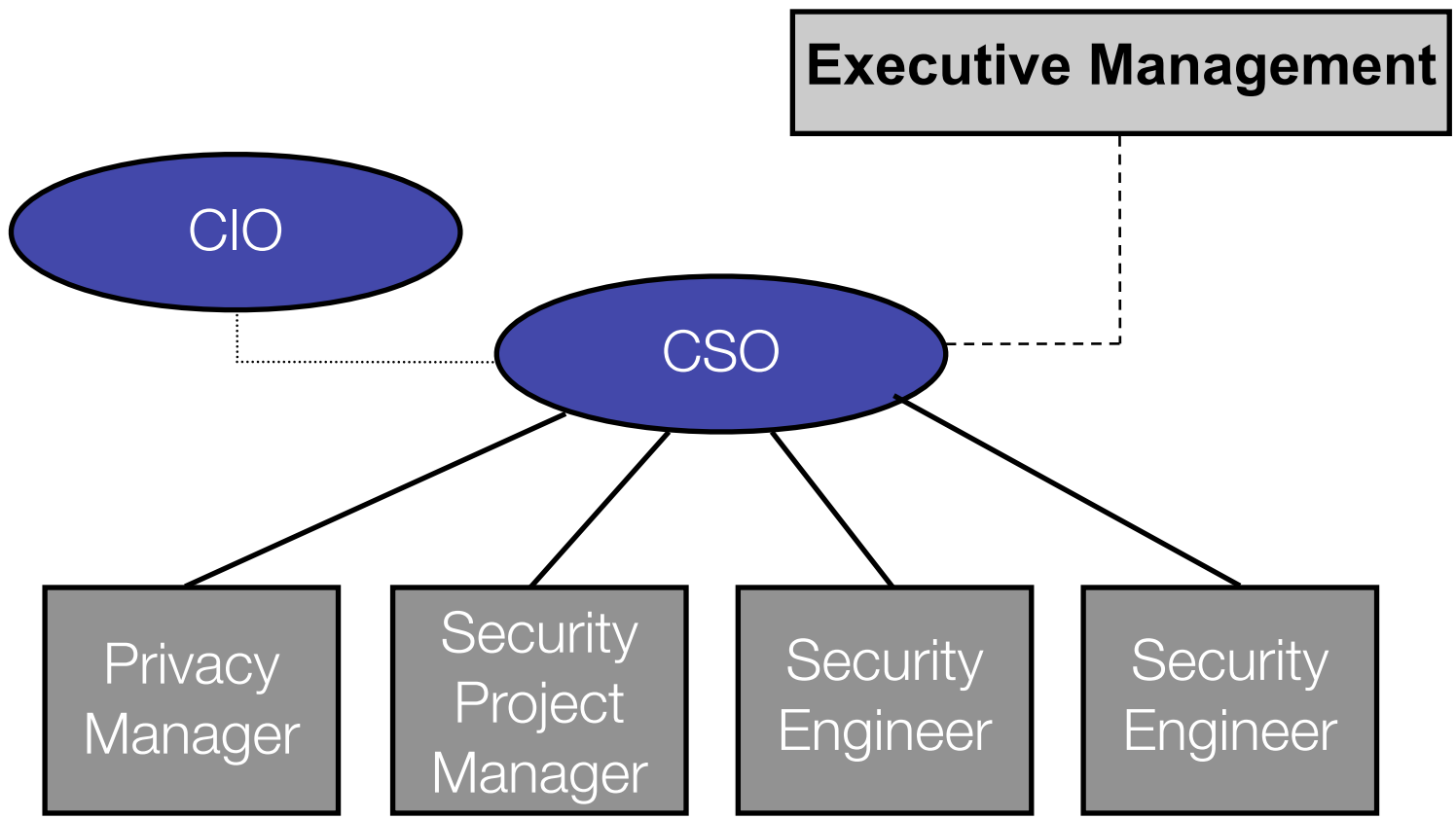
VOSTROM

Security Budget Compared to IT Budget

- In a recent CSO magazine article, one financial industry CSO stated the number should be more like 4-10% of overall revenues (not IT budget), which we believe is extraordinarily high.

VOSTROM

Example Hierarchy and Personnel



VOSTROM