Building Security Policies

1

What am I afraid of?

- List the top 5 or 10 ways you believe a computer or network-related problem can damage your business
  - Put an asterisk by those that could be affected by computer security
- If you have more than one or two asterisks, then you really have to worry about computer security

2

Worksheet: Big Inc.

- Big Inc. Online Banking Service:
  - Downtime
    - Power outage
    - Hacking our webserver
  - Negative publicity
    - System unreachable
    - System too slow
    - System unreliable
    - Public web site hacked

3

Worksheet: Big Inc. *(cont)*

  - Disclosure of business records
    - Through external action
    - Through internal action
    - By accident
  - Alteration of records
    - Through internal action
    - Through external action
    - By accident

4

What am I risking?

- For each identified risk, attempt to estimate how much an incident in that area can hurt you
  - Try to assign a best-to-worst case range

5

Worksheet: Big Inc.

- Hacking our webserver: uptime
  - Customer satisfaction problem if customers cannot access E-bank application
  - Duration is variable
  - While E-bank is down, we lose estimated $40,000/hr revenue from service fees
  - best: barely noticeable downtime
  - worst: extended downtime

6

Worksheet: Big Inc. *(cont)*

- Hacking our webserver: publicity
  - Negative publicity, short duration
  - best: May lose a handful of customers
  - worst: May depress stock values
  - Loss range: $0 - $1m (temporary)
  - Note: While this may seem like a disaster it is one of short duration

7

What is likelihood of Damage?

- Attach likelihood estimates to the list of risks you have established
  - If you have a lot of high-likelihood risks associated with computer security then you have major cause for concern

8

Worksheet: Big Inc.

- Likelihoods
  - 1: Hacking external website (embarrassment and downtime)
  - 2: Disclosure of business records
    - Through internal action
    - Through external action
  - 3: Alteration of records
    - Through internal action
    - Through external action

9

Procedures and Protections

- Identify technical means of addressing the risks you have listed
  - This forms a blueprint for your technical response plan

10

Worksheet: Big Inc

Hacking external website: **firewall and strong website security**

Disclosure of business records

- Through internal action: **restricted access to critical servers, isolation of production systems from rest of backbone, internal firewall**
- Through external action: **firewall at Internet connection, dial-in pool secured w/one-time password**

11

Worksheet: Big Inc. *(cont)*

3: Alteration of records

- Through internal action: **same as for disclosure, plus background checks for employees with access to financial processing system**
- Through external action: **financial production systems are not connected to externally accessible networks**

12

Policy Consistency

- Make sure your list is consistent with non-computer-related risks or other practices within the organization

13

Worksheet: Big Inc.

Disclosure of business records

Through internal action: restricted access to critical servers, isolation of production systems from rest of backbone, internal firewall

NOTE: this does not address disclosure via telephone or taking data out on floppy disks or hardcopies. print-outs of account data should be shredded.

14

Communication?

- Does the staff understand their responsibilities?
  - Everyplace in your technical plan where user training would help, ask yourself if responsibilities are being adequately explained to staff

15

Worksheet: Big Inc.

Disclosure of business records

Through internal action: restricted access to critical servers, isolation of production systems from rest of backbone, internal firewall

Training: Employees should be educated on the necessity of protecting customer records - not to share them, disclose them, browse them unnecessarily, and to be alert for social engineering

16

Incident Response?

- Do I have an effective incident response plan?
  - Who to contact in the event of an incident
  - Who can make key decisions
  - Information to collect in event of an incident
  - Backup and recovery procedures
  - Press contact rules of engagement

17

Worksheet: Big Inc.

- E-Bank incident response plan:

  In event of incident contact **sysadm@biginc or page the on-call at X1232**

  On-the-spot decision making authority resides with the director of E-bank or the SVP of Online services

  In the event of a break-in immediately:

  Start a backup of systems: harpo, groucho, and karl
  Turn on full network logging at the router
  Write-protect the transaction log tape recorder

18

Worksheet: Big Inc. *(cont)*

If press contacts staff about security related to E-bank, refer them to Fred @X1938 and if Fred is not reachable offer no information

19

Security Management

- How are you managing your security process?
  - Intervals to review policies for relevance
  - Who maintains what aspects of security
  - Policy review points for assessment of new technology
  - Vendor contacts for security and how often to probe for upgrade needs

20

Worksheet: Big Inc.

- Web site integrity audit process
  - Web site will be checked quarterly for:
    - Unauthorized software installed
    - New CGI scripts
    - Alteration of system binaries (tripwire)
    - Logs reviewed for “su” access
    - File upload logs checked
    - Write permissions on data area checked for change

21

Worksheet: Big Inc. *(cont)*

- Al @X1920 is responsible for audit of new CGI scripts prior to installation
- Frank @X9210 is responsible for basic platform security
- New applications to be installed on server must be signed off by Al and Frank prior to Frank’s installing them
- Frank will check w/Sun and Netscape bi-monthly for patches affecting the server

22

Summary

- This is a sketchy outline of how to build a policy
- Always Remember - ***security is a process not a product!***

23