Security Assessments: Why and How

Dillon Pyron

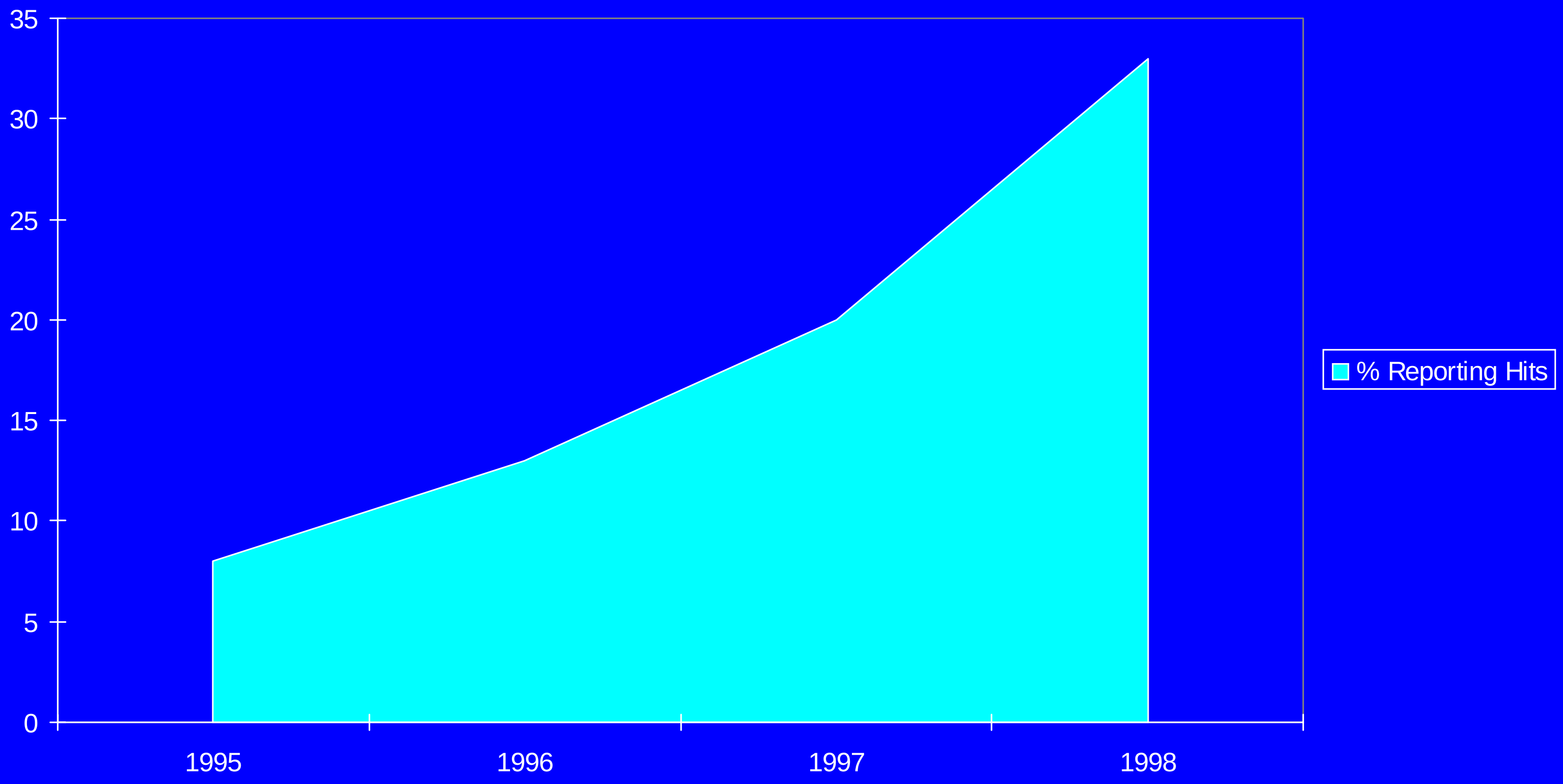
Sprint Paranet, Austin TX

dmpyron@sprintparanet.com

Why A Security Assessment?

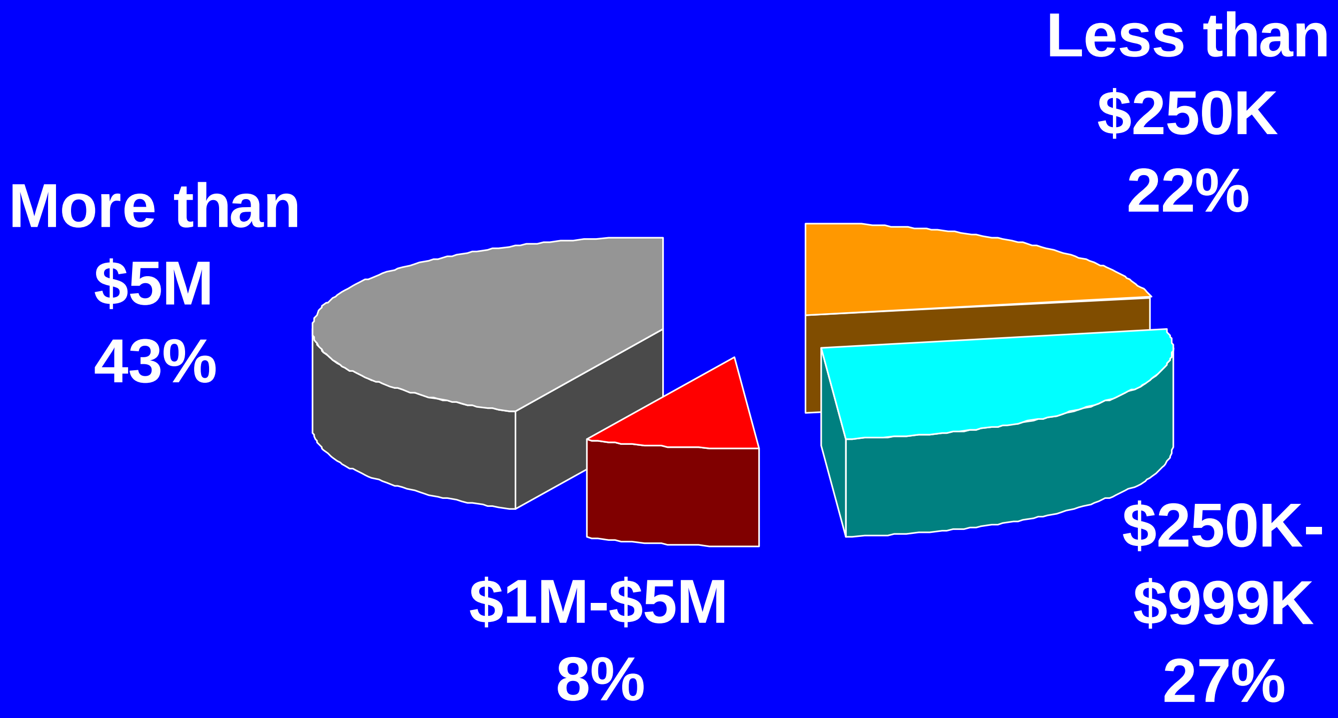
- ***Do you really know your current status?***
- ***Keep up with trends in security***
- ***Verify that procedures are valid***
- ***Ensure that procedures are being followed***

Fortune 100 Companies



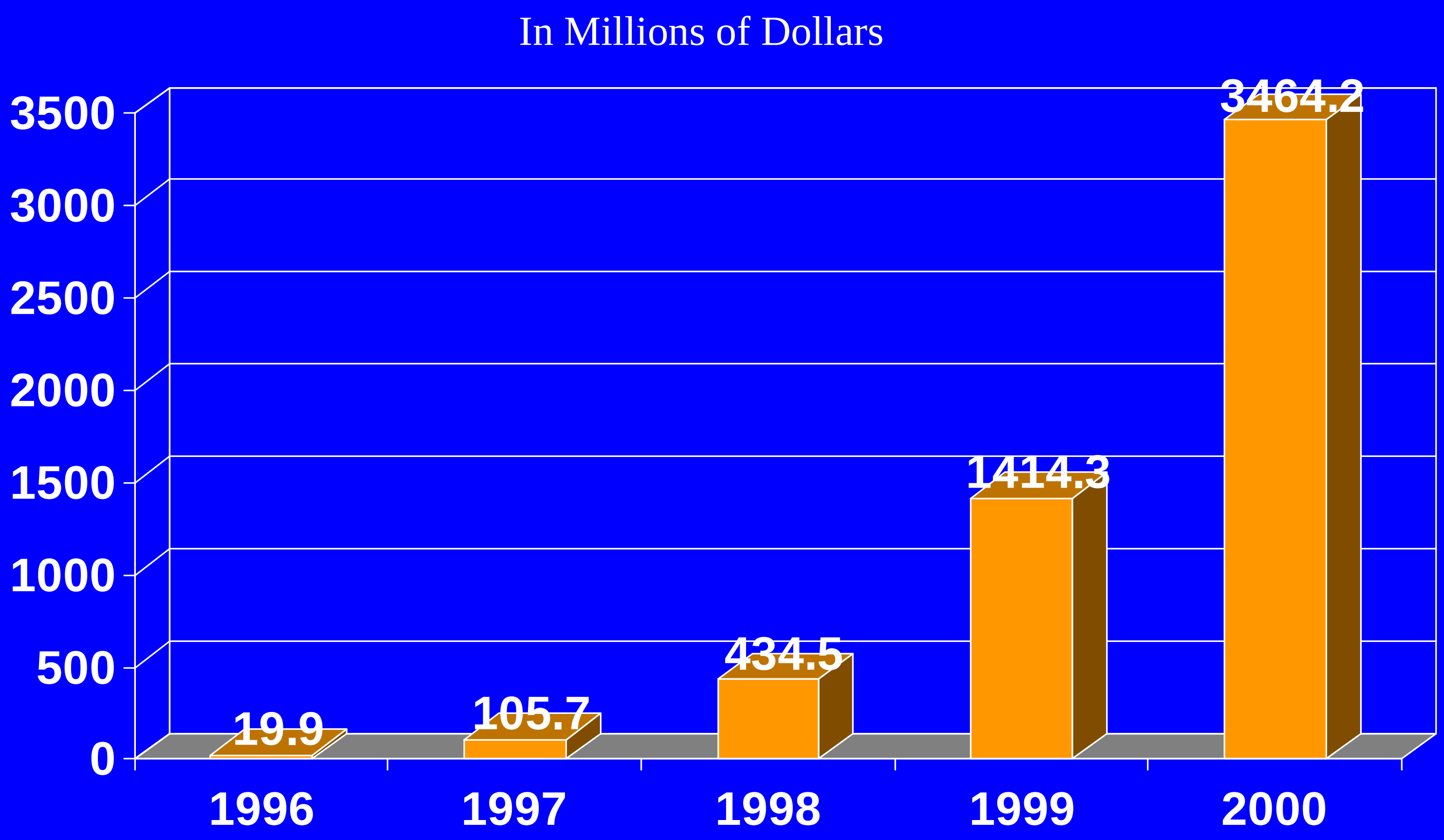
Source: CERT

Value of Data Losses



Source: InfoSecurity News

Security Expenditures



Assessment Functions

- ***An assessment is not an audit***
- ***Review current best practices***
- ***Establish security goals***
- ***Compare goals against current status***
- ***Make rectification plans in deficient areas***

How to Perform an Assessment

- *Inside vs Outside*
- *Establish Goals*
- *Restrict access to reports*
- *Layout entire process first*

What Is An Assessment?

- *Evaluation of current status*
- *Benchmark the industry*
- *Set your goals*
- *Develop an action plan*
- *Execute*
- *Start over!*

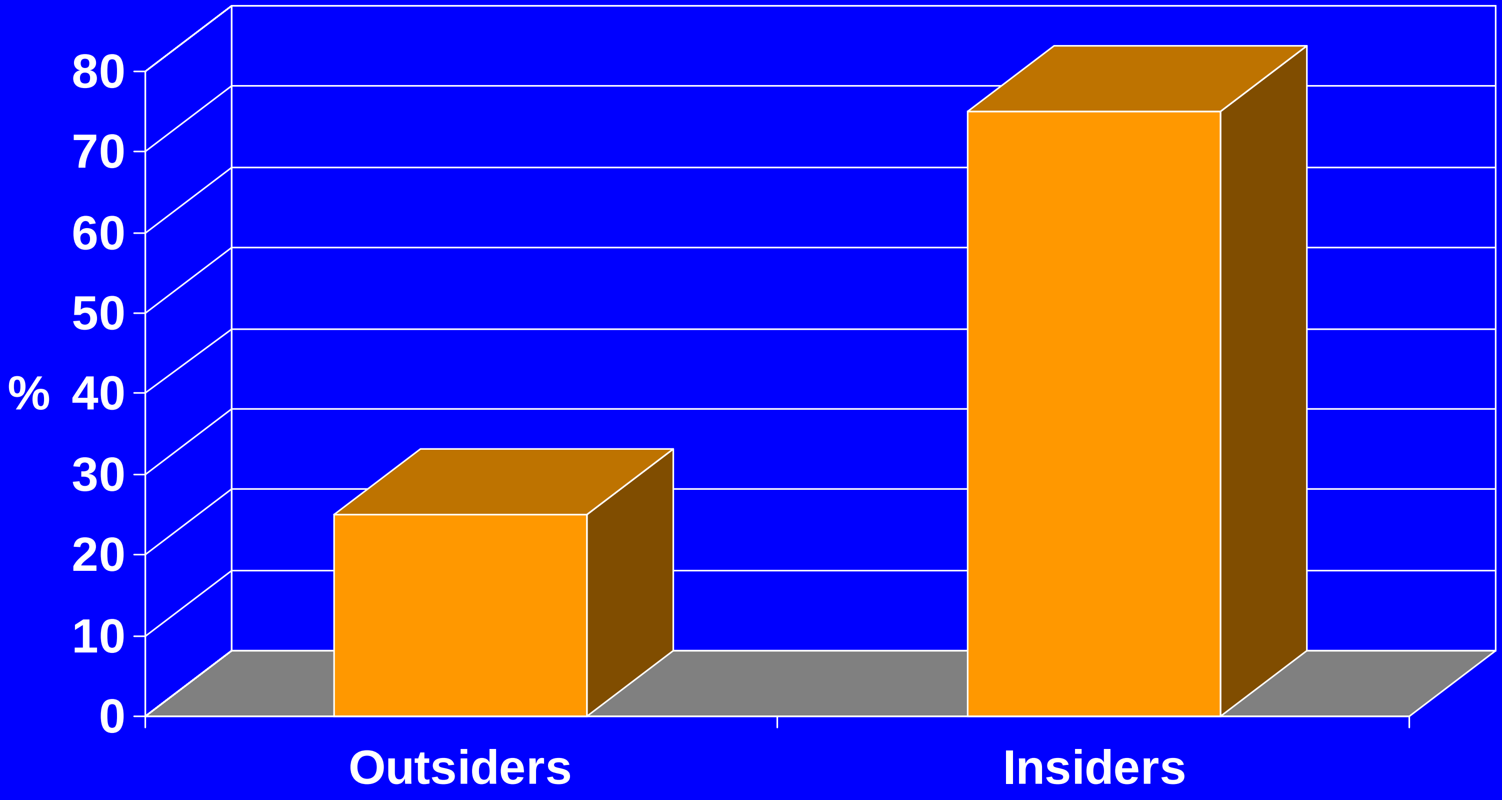
Best Practices

- *“Benchmarks” of industry standards*
- *Examples of successful efforts*
- *Compilations from professional/industry organizations*

Best Practices Areas of Interest

- ***User access***
  - Who
  - Where
  - How much

Why Worry About Users?



Source: American Society of Industrial Security Survey

Areas of Interest

- ***Password***
  - Size
  - Characteristics
  - Aging

Password Example

- ***User is Dillon Pyron, id is pyron***
- ***BAD***
  - dillon never expires
- ***GOOD***
  - 69Erdani! expires in 60 days

Areas of Interest

- ***“Reasonable use”***
  - e-mail
  - Web
  - Usenet

Areas of Interest

- ***Business Continuity***
  - Backup policies
  - Disaster contingencies

Areas of Interest

- ***Incident Reporting***
  - What to report
  - Who to report to
  - Evidence chain

Setting Security Goals

- ***Varies by industry***
- ***Must be realistic***
- ***Needs to include best case and worst case scenarios***

Security Goals

- ***Establish reasonable expectations***
- ***Prioritize achievable goals***
- ***Address specific areas of concern***

Industry Security “Standards”

- ***What is high risk for one business is acceptable for another***
- ***DoD vs banking vs swimming pool contractor***
- ***The key is due diligence***

Rectify Deficiencies

- ***Prioritize deficiencies***
- ***Develop plan***
- ***Schedule next assessment***

Correct Deficiencies

- ***Where does current state vary from goals?***
- ***Which goals are most critical?***
  - Which critical goals are most attainable?
- ***Develop action plan***
- ***Review current status***
  - Endless loop

Reality Intrudes

- *In the ideal world, security would not be an issue*
- *No such thing as “perfect” security*
- *Goals need to enumerate levels of risk and exposure*

Establishing Incident Response Scenarios

- ***What steps need to be taken***
  - – Identify all foreseeable scenarios
  - – Brainstorm some of the more bizarre ones
- ***How to prevent these***
  - – Time for more brainstorming

Assessment Process

- ***What is current state?***
- ***What are best practices?***
- ***What are threat points?***
- ***What are security goals?***
- ***Identify variances from goals***
- ***Modify current procedures***
- ***Start over again***

War Stories & Questions

- *“Now, this is no lie ...”*