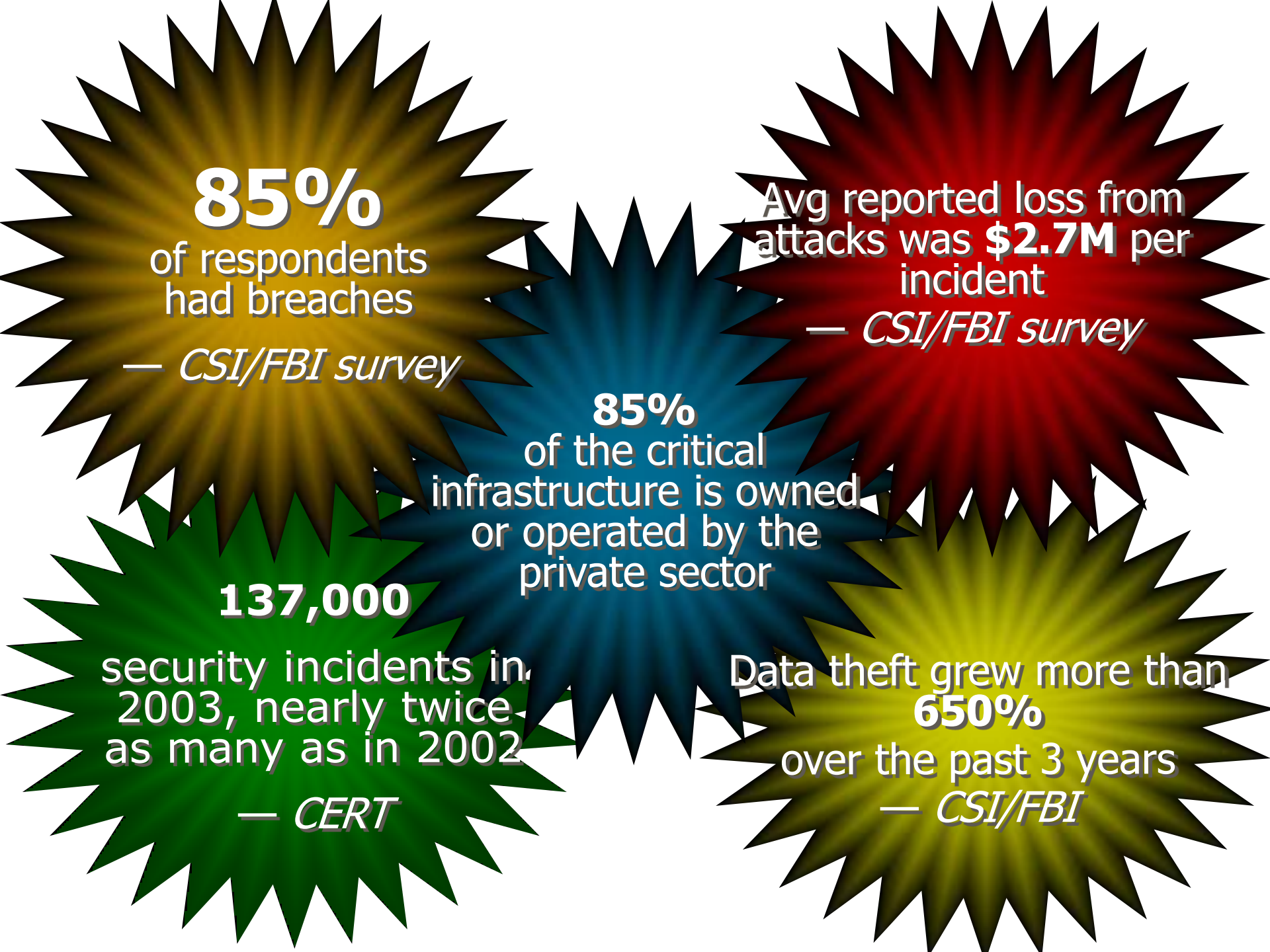
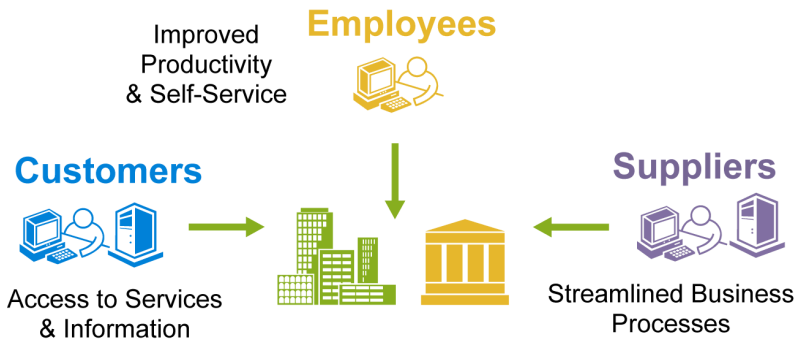

85%
of respondents had breaches
— CSI/FBI survey
Avg reported loss from attacks was $2.7M per incident
— CSI/FBI survey
85%
of the critical infrastructure is owned or operated by the private sector
137,000
security incidents in 2003, nearly twice as many as in 2002
— CERT
Data theft grew more than 650%
over the past 3 years
— CSI/FBI

The New Business Reality

Extended Enterprise



Governance & Regulation

- SEC Reporting Requirement?
- Federal Version of SB 1386?
- PIPEDA
- CA SB1386
- EU Data Protection Act
- SEC Regs
- FISMA
- Sarbanes-Oxley
- HIPAA
- GLBA
- BASEL II

Securing Digital Identities & Information

Information Security Governance

Task Force Recommendations

1. Organizations should adopt the information security governance framework described in this report to embed cyber security into their corporate governance process.
2. Organizations should signal their commitment to information security governance by stating on their Web site that they intend to use the tools developed by the Corporate Governance Task Force to assess their performance and report the results to their board of directors.
3. All organizations represented on the Corporate Governance Task Force should signal their commitment to information security governance by voluntarily posting a statement on their Web site. In addition, TechNet, the Business Software Alliance, the Information Technology Association of America, the Chamber of Commerce and other leading trade associations and membership organizations should encourage their members to embrace information security governance and post statements on their Web sites. Furthermore, all Summit participants should embrace information security governance and post statements on their Web sites, and if applicable, encourage their members to do so as well.
4. The Department of Homeland Security should endorse the information security governance framework and core set of principles outlined in this report, and encourage the private sector to make cyber security part of its corporate governance efforts.
5. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) should revise the Internal Controls-Integrated Framework so that it explicitly addresses information security governance.

Information Security Governance Framework Summary

- **Board responsibilities**
  - Strategic oversight; alignment
- **CEO responsibilities**
  - Assign resp./accountability/ authority; oversee compliance
- **Executives responsibilities**
  - Security commensurate with risk; integrate with operations
- **Senior Managers responsibilities**
  - Risk assessment, implement policies, secure operations
- **All employees responsibilities**
  - Awareness; compliance; reporting
- **Security program**
  - Providing security for networks, systems (ref. ISO17799)
  - Periodic assessment of risk
  - Policies/procedures to address security risks; full lifecycle
  - Security awareness training
  - Periodic testing; remedial action processes
  - Incident response procedures
  - Business continuity plans
- **Reporting**
  - Adequacy, effectiveness, acceptable residual risk reported to executives
  - Independent evaluation reported to the board

Reporting to the Board

Simple summary of risk assessment

Security Practices	Risk Level*		
(based on ISO 17799 chapters)	R	Y	G
Security Policy	0	1	1
Organizational Security	1	4	5
Asset Classification and Control	1	0	2
Personnel Security	1	4	5
Physical and Environmental Security	2	4	12
Communications & Operations Management	2	12	22
Access Control	5	13	14
Systems Development and Maintenance	1	4	13
Business Continuity Management	1	2	2
Compliance	2	5	4
TOTAL	**16**	**49**	**80**

***Sample numbers only**