Lock down your business; secure opportunity

CSO Perspectives

CSO
BUSINESS RISK LEADERSHIP

Research about Attitudes on the Benefits and Controls of Web 2.0* in the Enterprise

(*Social networking sites, video sharing sites, wikis, blogs)

Security Executive Council

Risks:

- Information leakage or reputational issues
- Vulnerabilities in applications
- Malicious attacks (cyberbullying)
- “Social worms,” phishing
- Attackers dynamically altering exploits -- difficult for signature-based protection engines to detect each instance

Poll to Security Executive Council members: Allow employees to connect to Web 2.0 applications?

67% yes

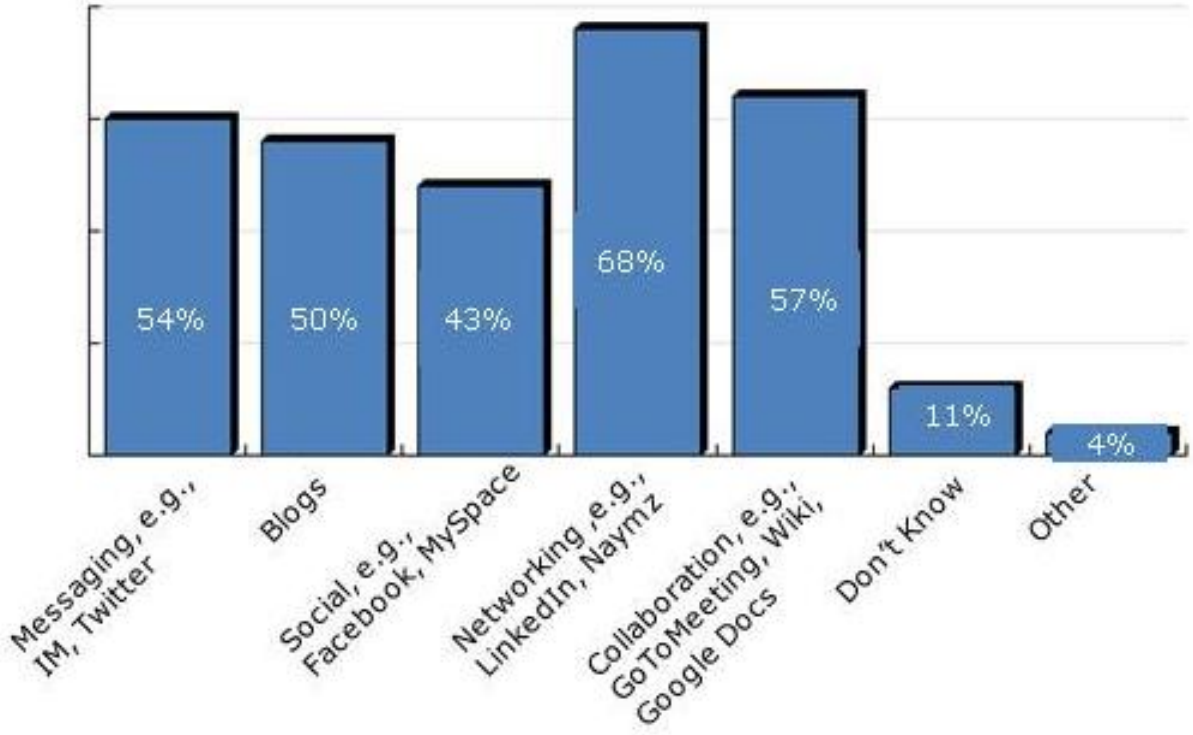
33% no

Open survey (Council and CSO): Allow employees to connect to Web 2.0 applications?

86% yes
14% no

To take the survey:
https://www.securityexecutivecouncil.com/web2

Open survey (Council and CSO): Yes



Poll of Council members: Why not?

- Bandwidth
- Productivity
- Risks (intrusion, virus, malware, etc.)
- Blocked but…

Poll of Council members: Specific policy?

- Most often reported no formal policy beyond allowance of occasional, appropriate personal use

Countermeasures:

- Technology approaches (e.g., scanning, filtering, heuristics based detection)
- People: web developer education; employee education; cross-functional team decisions