

Secure Enterprise 2.0 Working Group

David Lavenda
WorkLight - VP Marketing & Product Strategy

Open Group Conference San Diego, California Feb 5, 2009



AGENDA

- Why was the Secure Enterprise 2.0 Working Group formed?
- The Secure Enterprise 2.0 Working Group goals
- What has been done so far?
- Next steps





This is Where People Spend Their Time...































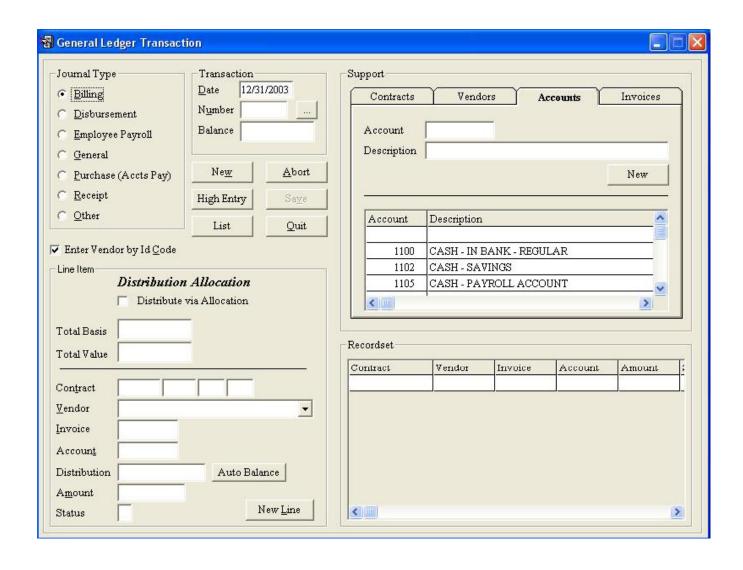








And Then They Go To Work...







But This is Changing Web 2.0 Goes To Work







86% of corporate end users already use at least one

consumer technology in the workplace

Source: Yankee Group





78% of IT organizations are concerned about the

risks of employee-driven, unsanctioned use of Web 2.0

tools and technologies

Source: Forrester Research





50% of respondents said they "customize their work environment moderately or aggressively" (including the use of unsanctioned tools) and will continue to do so.

Source: Gartner Research poll





Facebook company networks typically include tens of thousands of employees





On The Other Hand...Web 2.0 is Still "Web"

- Web applications have been in enterprise use for over a decade
- Attack vectors are well understood
 - O XSS
 - CSRF
 - SQL Injection
 - O DoS
 - Phishing
- Best practices are tried and true

So why are we here?





But Web 2.0 is Different







Secure Enterprise 2.0 Working Group Goals

- Promote Awareness
 - Promote the business opportunity generate awareness around the secure use of Web 2.0 services and technologies to do business
 - Publicize information about the risks associated with the use of Web 2.0 services and technologies for business
- Develop Policy and Best Practices
- O Deliverables
 - Case studies
 - Recommendations
 - White papers
 - Policies and best practices
 - Standards





What Have We Done So Far?

- Three Meetings and a web conference London, New York, Chicago
- O Deliverables
 - Business Case Study Repository approximately 10 cases where Web 2.0 technologies are being used securely to solve business problems
 - Technology Risk Document first draft of a document that catalogs Web
 2.0 risks





Sample Case Studies

- Retail bank using secure widgets to do business with customers
- Multinational bank using Facebook securely to foster collaboration among employees working in different countries
- Multinational consultancy that allows consultants to report billable hours to an SAP system via secure widgets
- Book publisher that publishes personalized product and event updates to book stores. Stores
 can then order products via secure widgets
- Manufacturing company where managers can approve purchase requests in an SAP system via secure widgets
- Company that provides Sharepoint document and task updates through Facebook
- Cable TV provider that lets customers order VOD from secure widgets running on the desktop, personalized homepages (web), or mobile devices
- Telecom operator that lets customers view account details and pay their bills via secure widgets





Sample Threats

- Cross Site Scripting (XSS)
- Cross Site Request Forgery (CSRF)
- Phising
- Information Leakage
- Injection Flaws
- Information Integration
- XML poisoning
- Malicious AJAX code execution





Next Steps

- Case studies
 - Add new case studies to the repository
- Risk Library
 - Refine the risk document
 - Add documented exploits
 - Publish techniques for mitigation
- Develop a white paper describing the current state of Web 2.0 security
- Publish best practices for using Web 2.0 technologies in the enterprise covering
 - Acceptable use policies
 - Policy enforcement
 - Liability
 - Intellectual property
 - Deployment architecture
 - Security
 - Integration
- Present case studies and findings at future events





Get Involved





Thank You

David Lavenda

WorkLight - VP Marketing & Product Strategy

Tel: (617)674-3260

Email: david@myWorkLight.com

www.myWorkLight.com

