INFORMATION SECURITY DECISIONS

Hosted by SearchSecurity.com

# Outfox SOX

**How to Make Regulations Work for You**

*Presented by Dan Blum*
*Senior VP, Group Research Director*
*dblum@burtongroup.com*

INFORMATION SECURITY DECISIONS

Hosted by SearchSecurity.com

## Thesis

- **The Sarbanes-Oxley Act (SOX) was created to address accounting fraud**
- **IT did not cause the problem, but feels the fallout**
- **Internal controls (including IT) fall under SOX 404, and auditors are digging deeper than ever to find any flaws**
- **Though SOX compliance is costly, companies should take it as an to opportunity to strengthen information security programs**

INFORMATION SECURITY DECISIONS

Hosted by SearchSecurity.com

## Agenda

- **Demystifying Sarbanes-Oxley**
- Compliance Approaches
- Recommendations

INFORMATION SECURITY DECISIONS

Hosted by SearchSecurity.com

## Background

- **"Enronomics:" A decade of excess…cooked books…fraud…crowned with complicit audits**
- **Enter the Sarbanes-Oxley Act (SOX): Legislation to restore corporate accountability to all public cos. filing annual reports with SEC**
  - **Strengthens executive responsibility: CEOs/CFOs must certify financial statements…jail or fines the consequence for cooked books…ignorance is no defense**
  - **Strengthens independent auditor: Public Company Accounting Oversight Board (PCAOB)…creates guidelines**
  - **Strengthens internal corporate controls**
  - **Many other provisions**

INFORMATION SECURITY DECISIONS

Hosted by SearchSecurity.com

## Key requirements of SOX impacting IT

- **SOX 404: Requires annual report on internal controls…auditors must sign off**
- **SOX 302: Requires quarterly disclosure by management to auditors of all material weakness in internal controls**
- **SOX 906: Additional disclosures and specifications of penalties**
- **SOX 409: Real-time issuer disclosures…a sleeper requirement for IT?**

INFORMATION SECURITY DECISIONS

Hosted by SearchSecurity.com

## SOX 404 – High Level, not prescriptive

**SEC. 404. MANAGEMENT ASSESSMENT OF INTERNAL CONTROLS.**

(a) RULES REQUIRED.—The Commission shall prescribe rules requiring each annual report required by section 13(a) or 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78m or 78o(d))
to contain an internal control report, which shall—

(1) state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and
(2) contain an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.

(b) INTERNAL CONTROL EVALUATION AND REPORTING.—With respect to the internal control assessment required by subsection (a), each registered public accounting firm that prepares or issues the audit report for the issuer shall attest to, and report on, the assessment made by the management of the issuer. An attestation made under this subsection shall be made in accordance with standards for attestation engagements issued or adopted by the Board. Any such attestation shall not be the subject of a separate engagement.

INFORMATION SECURITY DECISIONS

Hosted by

## How a results-oriented act became more prescriptive

- **PCAOB Audit Standard 2**
  - **Prescribes that management should use an "internal control framework" similar to that of COSO**
- **COSO: Committee of Sponsoring Organizations**
  - **A good thing: Prescribes risk management to achieve internal control objectives including efficiency and effectiveness of operations, financial reporting, and legal/regulatory compliance**
- **Auditors have mapped COSO to COBIT, as well as other frameworks (beware of their checklists!)**
  - **COBIT: Control Objectives for IT**

INFORMATION SECURITY DECISIONS

Hosted by

## SOX is having heavy impacts

- **582 firms disclosed material weaknesses or significant deficiencies in internal controls in 04**
- **Nearly all companies suffer a decline in share price when a SOX deficiency is disclosed**
- **469 companies told the SEC they needed more time to file annual reports (3/22/05)**
- **Average compliance cost estimated at $4,400,000 (3/05)**
- **Boardroom changes elevate role of "chief risk officer", "chief governance officer", etc.**

INFORMATION SECURITY DECISIONS

Hosted by

## Agenda

- Demystifying Sarbanes-Oxley
- **Compliance Approaches**
- Recommendations

INFORMATION SECURITY DECISIONS

Hosted by SearchSecurity.com

## Basic compliance approach

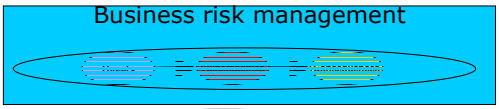
- **Establish a risk management framework**
- **Determine the scope of SOX compliance**
- **Establish a control framework**
  - **Control objectives**
  - **Control activities**
- **Process mapping, remediation, testing, change management**
- **Documentation, documentation, documentation**

INFORMATION SECURITY DECISIONS

Hosted by SearchSecurity.com

## Establish risk management framework

- **Traditional risk management focuses on controlling business losses**
- **SOX focus on financial reporting runs a bit sideways to traditional risk management, but similar frameworks can be used**




**Accept / Transfer / Mitigate / Avoid**

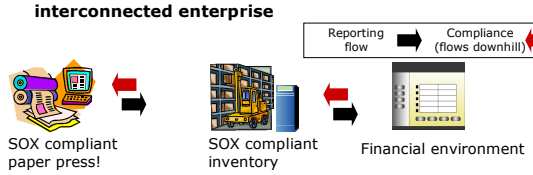
- **SOX raises risk level of financial reporting processes, systems, and applications**

INFORMATION SECURITY DECISIONS

Hosted by SearchSecurity.com

## Determine the scope of SOX compliance

- **Best starting point: Consolidated financial information systems (FIS) into ERP systems (may have well-designed internal controls)**
- **Worst starting point: Fragmented FISes rolling up, spreadsheets and financial applications everywhere**
- **Reality or destination for some? Highly interconnected enterprise**



INFORMATION SECURITY DECISIONS

Hosted by

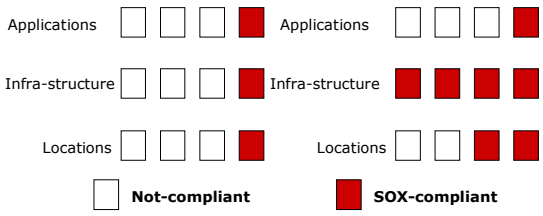
## Isolate financial systems, or raise the bar?

- **Strategic decision: Where to end up?**

**SOX-compliant components must be isolated to lower costs**

**OR**

**Make more components SOX-compliant (to enable various business needs)**




**Not-compliant** **SOX-compliant**

INFORMATION SECURITY DECISIONS

Hosted by

## Develop control framework

- **Example (partial)**

| Control Objectives | Control Activities |
|---|---|
| Separation of duty for accounting functions | Role based access control |
| Changes to financial information are audited | Secure log server<br>Tamperproof audit record |
| Financial information is protected from unauthorized access | Network isolation<br>User authentication<br>Managerial sign-off on new accounts |
| Financial information integrity is maintained | Application code formally tested before move to production |

INFORMATION SECURITY DECISIONS

Hosted by

## Common problems or mistakes

- **Scoped too narrowly or too broadly**
- **Lacked mature risk management or internal control structure**
- **Lacked documentation**
- **Lacked change management**
- **Used inexperienced audit teams**
- **Did not capture lessons learned**
- **Froze inadequate systems in place to avoid re-documenting the next year**

INFORMATION SECURITY DECISIONS

Hosted by SearchSecurity.com

## Agenda

- Demystifying Sarbanes-Oxley
- Compliance Approaches
- **Recommendations**

INFORMATION SECURITY DECISIONS

Hosted by SearchSecurity.com

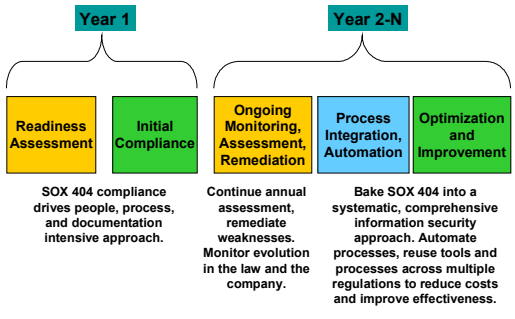
## Turn lemons into lemonade

- **SOX is the law, and a strong compliance approach in IT is prudent at this time**
- **Many companies are ALSO subject to other regulations (GLBA, HIPAA, 21 CFR11, …)**
- **SOX compliance and info security benefits**
  - **Protects the company from business risks, compliance risks**
  - **Leads to better investment ratings**
  - **Helps company become more outsourceable, marketable – can respond to business partners' compliance demands**
  - **Leads to competitive advantage**
- **SOX is a strong driver to fund sensible security**

INFORMATION SECURITY DECISIONS

Hosted by SearchSecurity.com

## Develop compliance roadmap



INFORMATION SECURITY DECISIONS

Hosted by SearchSecurity.com

## Build compliance into IT governance

- **IT-related compliance requirements should be driven by Legal, CSO/CISO, and other organizations**
  - **Fix gap: Legal must have some IT knowledge or CSO/CISO must be high enough in the reporting chain to "negotiate"**
  - **Some organizations seek to give compliance weight and balance by creating a new executive position – Chief Compliance Officer, Chief Risk Officer, etc.**
- **CIO, CFO, others carry out control activities (under separate reporting chain from CISO)**
- **Internal audit verifies compliance**

INFORMATION SECURITY DECISIONS

Hosted by SearchSecurity.com

## Establish a risk management framework

- **Must be driven by senior management, down into the projects**
- **Sets thresholds that help determine which locations or components are in scope for SOX**
- **Influences strategic perspective on isolating financial reporting, or raising the bar**
- **Risk management guidelines for the company affect control objectives and activities**
  - **Example: Relatively isolated SOX environment may have its own controls, or controls may be reused across SOX, other needs**

INFORMATION SECURITY DECISIONS

Hosted by SearchSecurity.com

## Develop appropriate control framework

- **Security policy should specify control objectives and control activities**
- **Control objectives can be based on COBIT, ISO 17799 or other frameworks**
- **Don't adopt any framework's controls blindly**
  - **Must show evidence that ALL the controls your company specified are working**
    - **COBIT has 34 control domains; each requires as many as 10 control activities**
  - **However, be prepared to justify differences from COBIT to SOX auditors**

INFORMATION SECURITY DECISIONS

Hosted by

## Avoid worst practices, seek guidance

- **The industry has nothing like a list of "best practices" for SOX (Sorry!)**
- **But for systems in scope, worst practices –**

  **such as** 
  
  **are a sure-fire way to fail an audit**
- **To implement your companies selected control activities, refer to the good industry guidance at SANS, NIST and other sites or sources**

INFORMATION SECURITY DECISIONS

Hosted by

## Select tools carefully

- **Vendor claims of SOX-relevance are often exaggerated, yet compliance would be almost impossible without tools**
- **Many tools are required, all have limitations, and not all are well-integrated**
- **What is realistic?**
  - **FIRST, develop an information security technology architecture with compliance input, THEN select tools that fit**
  - **Use any other tools that help with the compliance project's own project management and documentation needs**

INFORMATION SECURITY DECISIONS

Hosted by

## What to look for: SOX tools taxonomy

| Tool Type | Compliance Function |
|---|---|
| Financial applications | Native security capabilities |
| Project management, workflow | Compliance project, sign-offs |
| Documentation (everywhere) | Compliance project, evidence of control activities |
| Identity management | Separation of duty, access control, audit |
| Management and monitoring | Audit, change management, control, etc. |
| Firewalls, perimeter devices | Isolation, layered defense |
| SIM/SEM, forensics | Layered defense |
| Compliance dashboards | As yet mythological |

INFORMATION SECURITY DECISIONS

Hosted by

## Prepare for external audit

- **Choose a good auditor**
  - **Multiple organizations have input into this decision**
  - **Find a reputable, well-resourced auditor with strong partner overseeing the project**
- **Consider using the audit firm for up front risk management consulting**
- **Do a good job – well-thought out control structure and documentation are key**
- **Don't be afraid to debate overly prescriptive audit staff**

INFORMATION SECURITY DECISIONS

Hosted by

## Conclusion

- **SOX is here to stay, along with other regulations**
- **Avoid common mistakes by addressing SOX strategically – get governance, accounting, information security, and IT firing on all cylinders**
- **Compliance and a sound information security program makes good business sense**

INFORMATION SECURITY DECISIONS

Hosted by

## Audience response

Question?