



Joel Rakow, Ed.D.  
eCrimes Practice Lead



Copyright © 2003 Steelcase and Tatum, LLC



*your world*  
*your issues*  
*your goals*





# *your future?*

*Dear Customer:*

*It has come to our attention that the personal information you provided us is in the possession of parties that we cannot identify.*

*An intruder may have taken your social security number, your date of birth and full legal name. The potential use of this information puts you at grave financial risk. We encourage you to ...*



e-gads!  
*new rules. new risks.*

e

*business*

e

*this*

e

*that*

e

*Crime*



*the premise*

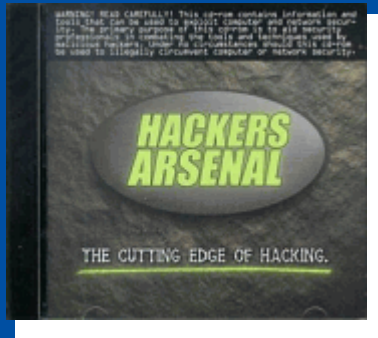
*eCrime is different!*





# *Crime*

- *Greater volume*
  - *Many false positives*
- *Disparate geography*
- *Disparate jurisdictions*
- *No loss to company*



**\$12.95**

*plus s/h*

# *Hackers Arsenal*

- *Password crackers*
- *Port scanners*
- *Denial of service utilities*
- *Trojan horse wrappers*
- *Much more*



*eCrimes new dimension?*





## *eCrime's new dimension?*

- *CA SB 1386*
- *HIPAA*
- *Gramm-Leach-Bliley Act*
- *Sarbanes-Oxley Act*



## *Why is this new? So What?*

- *Duty to Protect*
- *Breach and Cause of Harm*
- *Tort Law Applies*
  - *Class action suits*
  - *Shareholder suits*



## *The Insurance Gambit!*

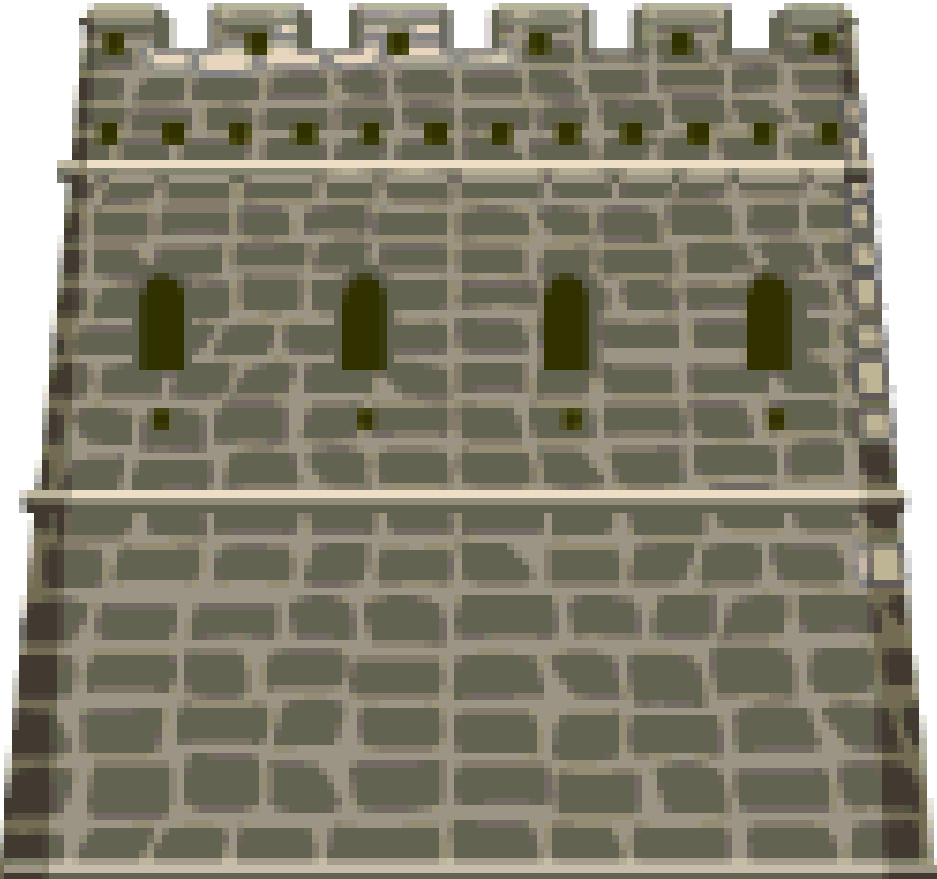
- *Information Loss Policy*
- *ISO 17799 Standard*
- *No Coverage: Intangible Assets*
- *Managed Security*
- *\$7K to \$25K / \$Million*
- *Exclusions*



*New Perspective! Old Myths!*



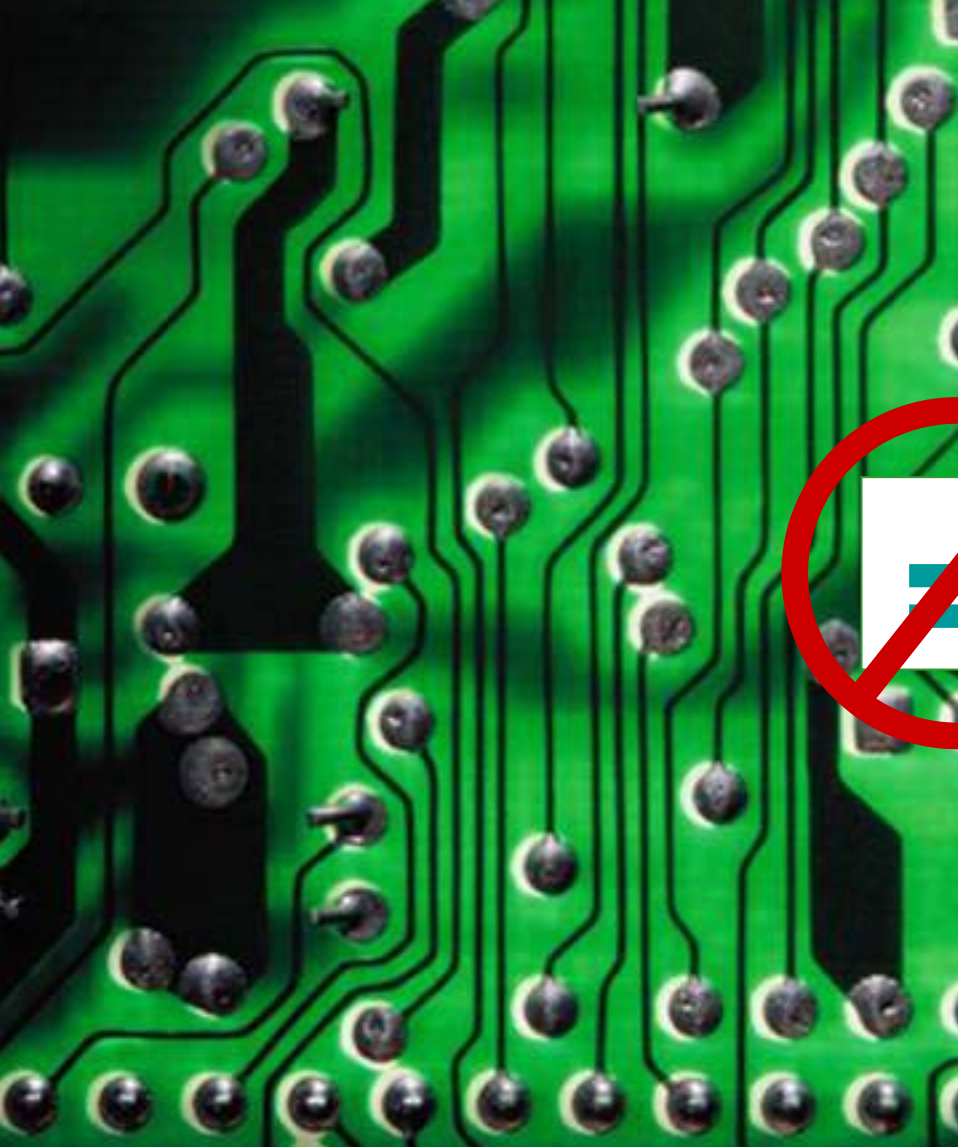
## *Myth #1: High, thick walls keep bad guys out.*



- Firewalls
- Intrusion detection systems
- Sign on procedures
- Virus detection

The “Fortress” myth.







## *Myth #2: Incident Response is an Appropriate Model*



- Prevent incidents
- Develop a response plan
- Respond to each incident

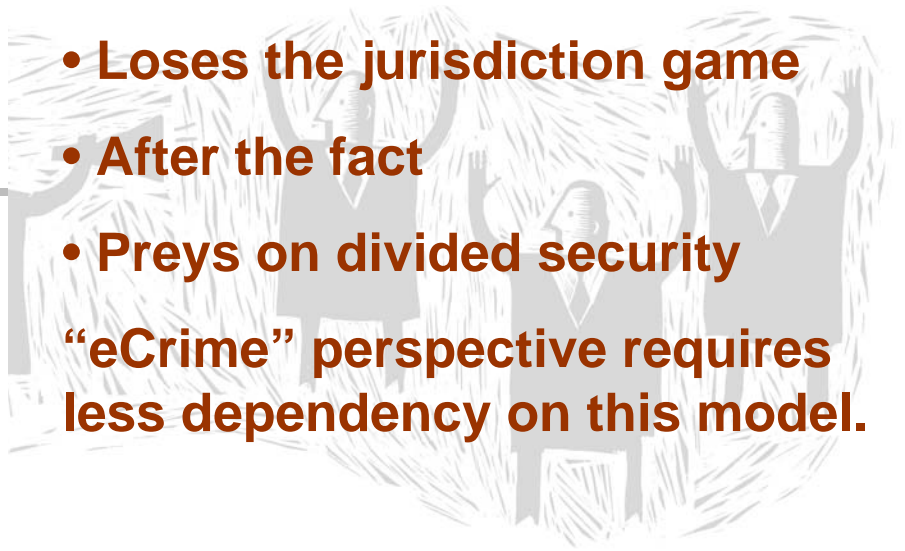




## *Myth #2: Incident Response is an Appropriate Model*



- Does not scale
  - Too simplistic for eCriminals
  - Loses the jurisdiction game
  - After the fact
  - Preys on divided security
- “eCrime” perspective requires less dependency on this model.





## *Myth #3: Data Security is an IT Problem*



- **Related to Myth #1**
- **It's a technical problem**
- **Requires a technical solution**
- **Only IT people can help with IT issues**





## *Myth #3: Data Security is an IT Problem*



- Too simplistic for fraudsters
- Ignores the role of process
- Ignores the value available from physical security professionals
- Formal assessments
- Policy development and enforcement
- Oversight – especially change control





“*The fight against eCrime needs an integrated, proactive, early detection model for managing risk across the entire enterprise.*”



*“The fight against eCrime needs an integrated, proactive, early detection model for managing risk across the entire enterprise.”*

*“A data loss is bad... a loss and being found negligent is unacceptable.”*



“The fight against eCrime needs an integrated, proactive, early detection model for managing risk across the entire enterprise.” --CISO

“A data loss is bad... a loss and being found negligent is unacceptable.” -- CFO



## *eCrime solution*

- Operational Security
- Organizational Security



# FTC Safeguards Rule

*The Safeguards Rule requires each financial institution to “develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical and physical safeguards that are appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue.” See 16 CFR part 314.*



TATUM PARTNERS

Financial and Information Technology Leadership



# FTC Safeguards Rule

*The Safeguards Rule requires each financial institution to "develop, implement, and maintain a comprehensive information security program that is written in one or more readily*

*maintain a **comprehensive** information security program*

*sensitivity of any customer information at issue." See 16 CFR part 314.*



TATUM PARTNERS

Financial and Information Technology Leadership



# Comprehensive Plan

- Define baseline security level
  - Framework (a.k.a. domains)
    - Defined by ISO 17799
    - Alternatives
- Enterprise security policies
  - End user policies for physical and data
  - IT policies for operation and organization
- Emergency Management Plan
  - Incidents, Crises, Disasters
  - Business continuity
- Governance
  - Departmental and Administrative Plan
  - Issues Log
  - Third Party Services
    - Assessments
    - Validations



TATUM PARTNERS

*Financial and Information Technology Leadership*



# Comprehensive Plan *(cont'd)*

- The ISO 17799 Framework
  - Organizational security
  - Asset Classification and Control
  - Personnel Security
  - Physical and Environmental Security
  - Communications and Operations Management
  - Access Control
  - Systems Development and Maintenance
  - Business Continuity Management
  - Compliance



TATUM PARTNERS

*Financial and Information Technology Leadership*



## *Organizational Security*

- Create the plan
- Provide governance
- Demonstrate progress



# *eCrime solution*

Operational Security



Integrate  
Physical &  
IT Security



Build &  
Manage  
Business  
Rules

## *eCrime Solution: Early Detection*

Define  
Threats of  
Attack



Monitor  
Traffic and  
Share  
Results





# *Candidate Companies*

- **Sell to consumers**
- **eCommerce companies**
- **Financial service companies**
- **Health care**
- **Regulated companies**
- **Companies that have been breached**





## *Service Offering*

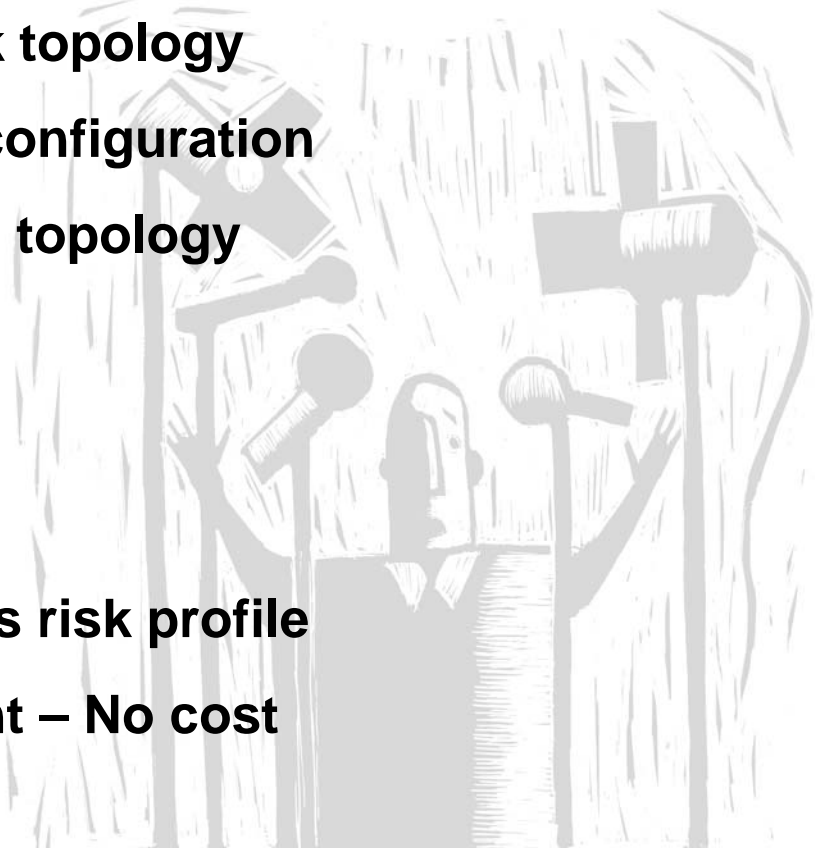
- **Set up and run IT Steering Committee**
- **Align security policies with risk profile**
- **Direct security plan**
- **Direct emergency management plans**
- **Integrate physical and data security**
- **Establish security department**
- **Assist security vendor in market development**





# *Risk Management Offer*

- **FLP request following documents:**
    - **Diagram of network topology**
    - **Diagram of server configuration**
    - **Diagram of telecom topology**
    - **Security plan**
  - **TLP will:**
    - **Review documents**
    - **Assess your client's risk profile**
- No contact with client – No cost**





# *Comments? Questions?*

Joel Rakow, Ed.D.

eCrimes & Risk Management Practice Lead

Tatum Partners

310 418 7322

[joel.rakow@tatumllc.com](mailto:joel.rakow@tatumllc.com)