# HIPAA Security: Case Studies for Small to Medium Health Organizations (Compliance Methods)

Jeff Bardin, CISSP, CISM, NSA IAM, OCTAVE[SM]

Principal & CSO

Treadstone 71

www.treadstone71.com

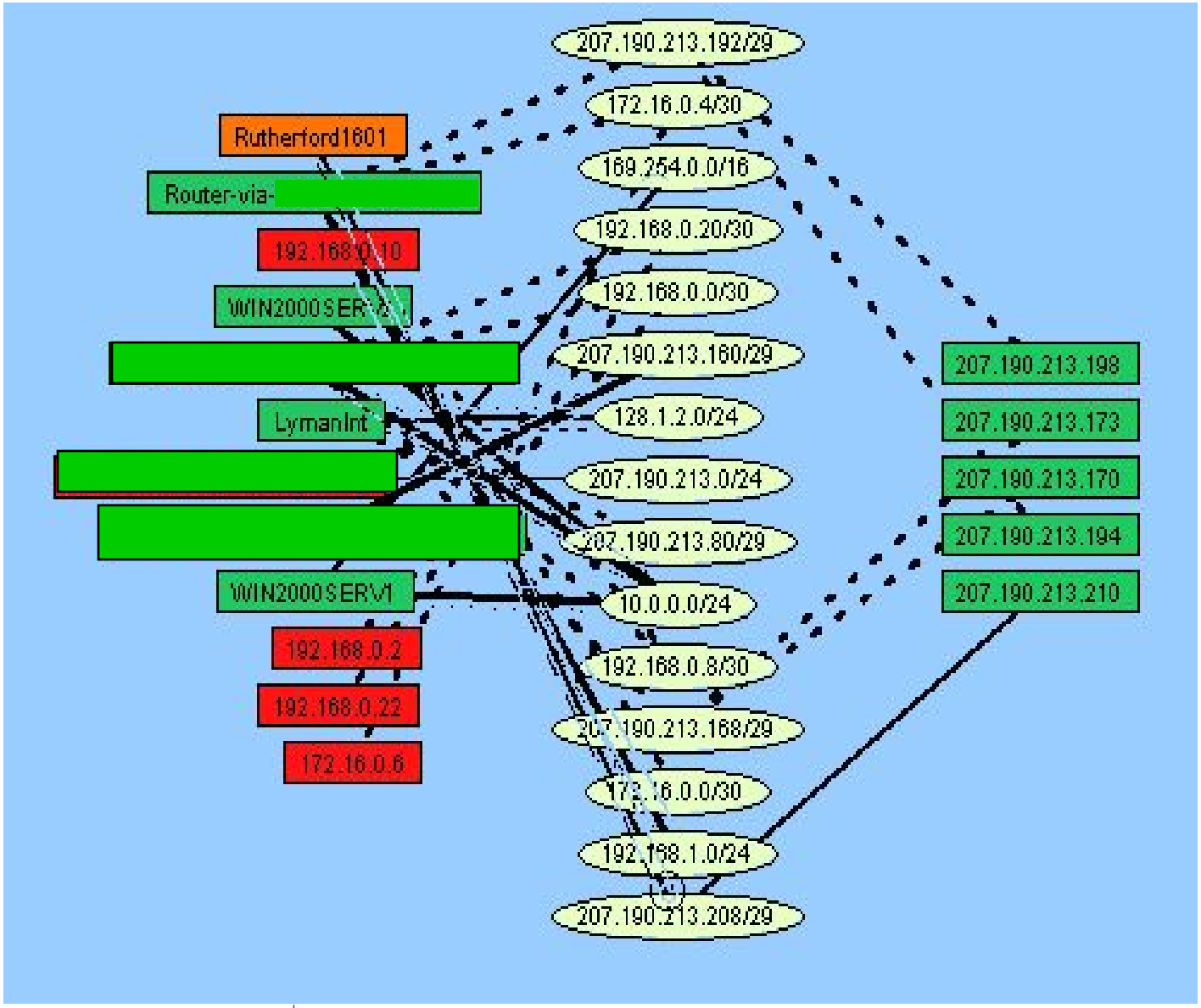
jbardin@treadstone71.com

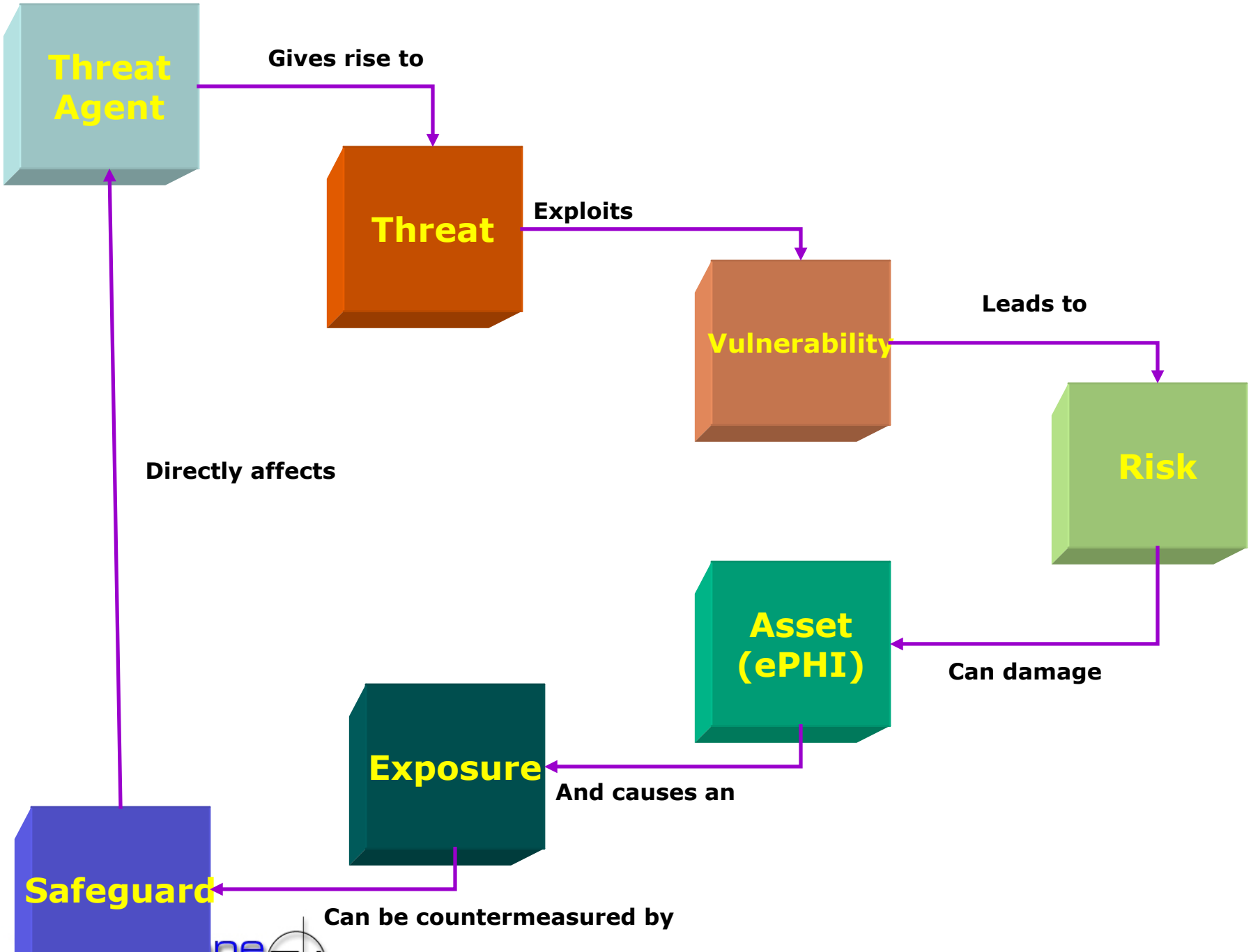
Treadstone 71

# Agenda

- From Threat Agent to Safeguard
- The NSA IAM Method
  - Criticality of Information Matrix
  - Systems Criticality Matrix
- OCTAVE[SM] Method
  - Human Actors Using Network Access
  - Threat Profile: System Problems
  - Basic Risk Profile
- Initial Findings
- Scorecards
- HIPAA & ISO17799
- Roadmap
- Q&A

# Vulnerabilities available for exploit




Threat Agent
Gives rise to
Threat
Exploits
Vulnerability
Leads to
Risk
Directly affects
Asset (ePHI)
Can damage
Exposure
And causes an
Safeguard
Can be countermeasured by

# Criticality of Information Matrix

| | Confidentiality | Integrity | Availability |
|---|---|---|---|
| Patient Records | H | H | H |
| Medical Staff Records | M | H | M |
| Employee Records | M | H | M |
| Vendor Contracts | M | H | M |
| Employee Health Records | M | H | M |
| Legal Files (lawsuit information) | M | H | M |
| Contracts w/Agency People | M | H | M |
| Meeting Minutes (Board) | M | H | M |
| Survey Reports (Joint Commission (Medicare/Medicaid) | M | H | M |
| Docs – Security Eng Tests & Inspections | M | H | M |
| Patient Accounts | H | H | H |
| Financial Audits | M | H | M |
| Planning Documents (Strategic/Master Facility Plan) | H | M | H |
| Payroll Records | H | H | H |
| Psych/Drug/Alcohol/HIV | H | H | H |