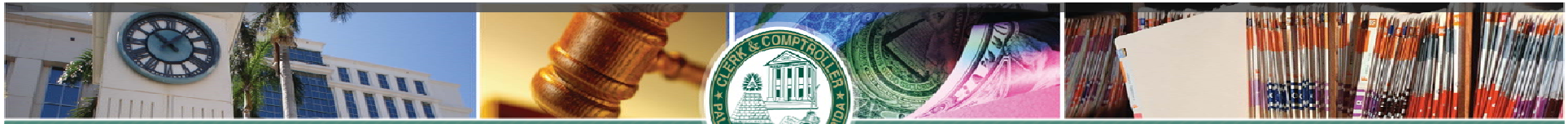


SHARON R. BOCK
Clerk & Comptroller
Palm Beach County

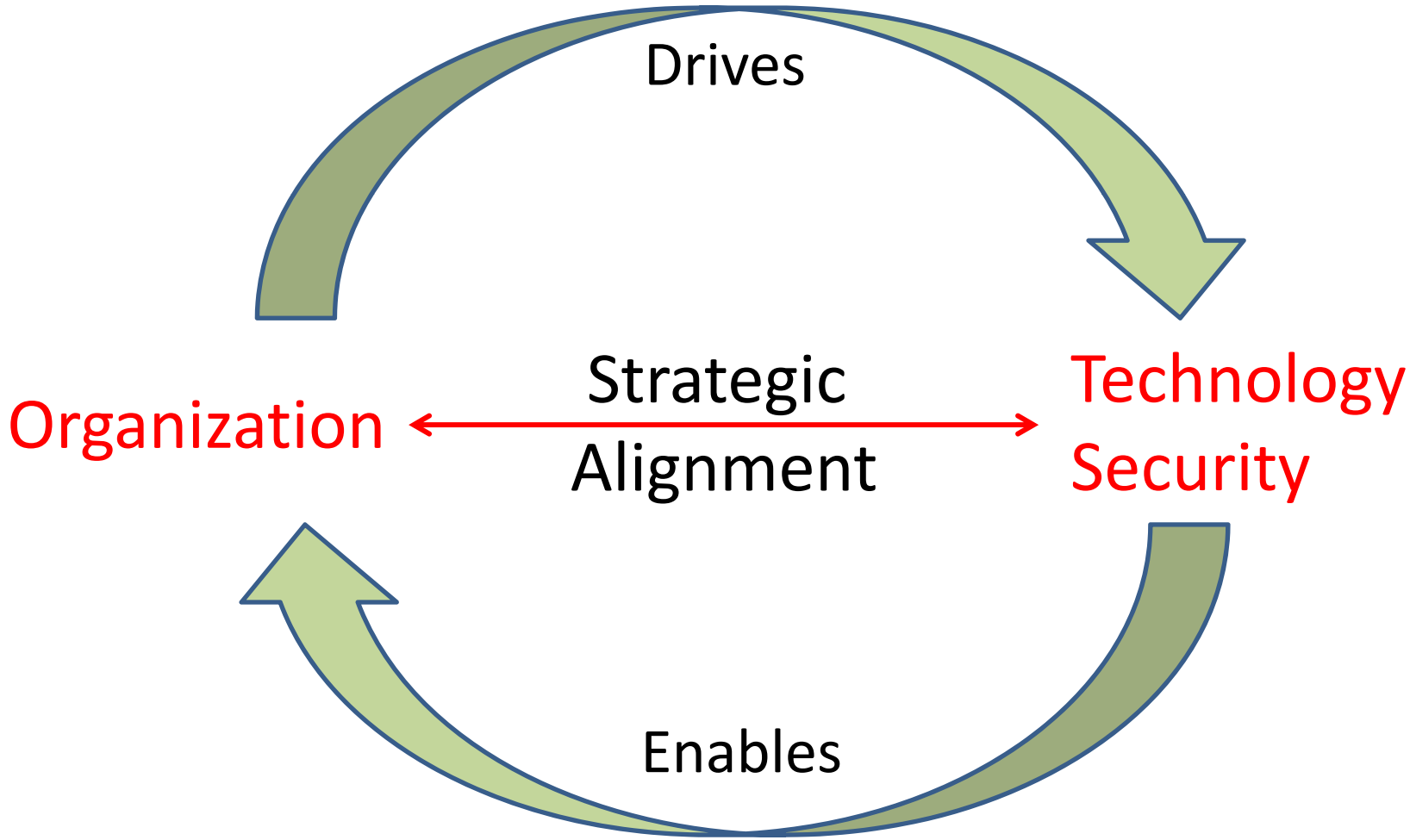
Security Across the Organization

Paul Jones
CIO – Clerk & Comptroller Palm Beach County
CISSP, ITIL Expert, Security+, Project+

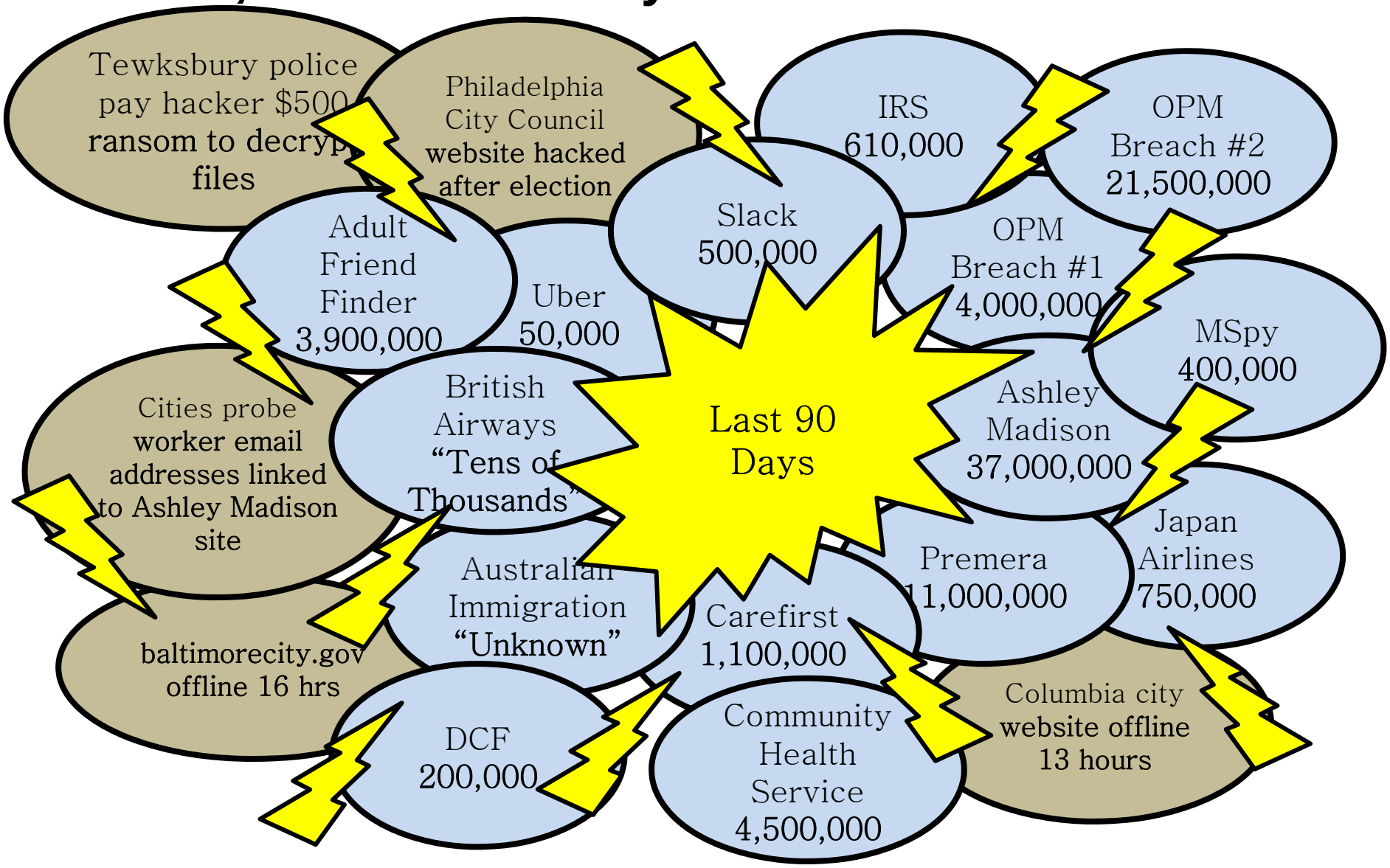
Objectives:

- **Organization wide security**
- **IT's role**
- **Security awareness**
- **Risks and liabilities**
- **The three tiers**
- **Leadership support**
- **The life cycle**

The Paradigm Shift



Breaches, breaches everywhere



The Security Chess Game

- MALWARE & VIRUSES
- SOCIAL ENGINEERING
- PHISHING
- RANSOMWARE
- PHYSICAL SECURITY
- PATCHES
- DENIAL of SERVICE
- INSIDER THREATS
- MISUSE

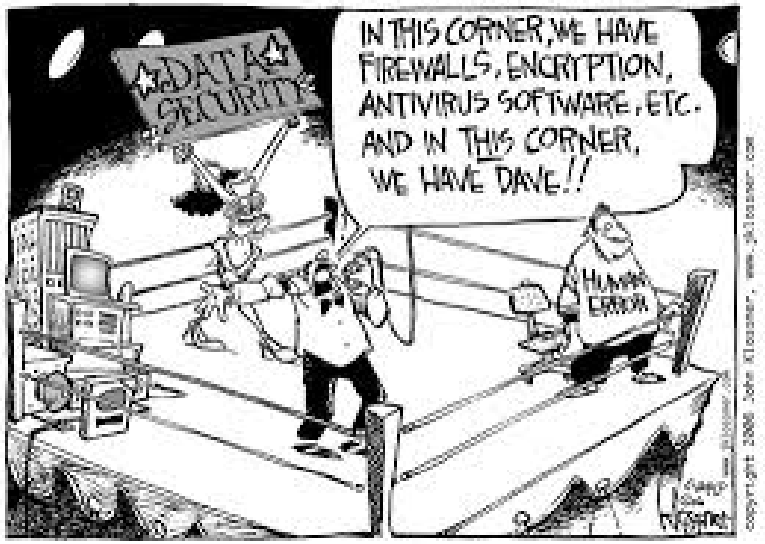
image source: mangosalaute.com

THE ODDS ARE WORKING AGAINST YOU!

Misconception – “Security is an IT thing”

“A new study reveals that more than 8 out of 10 (88%) companies surveyed admit their organization experienced a significant security event in the last twelve months with as many a **73% of the companies indicating that the cause was insiders**” (The Norris Corporation, 2015)

“While shadowy hackers in Eastern Europe often get the blame for these attacks, more than **80% of the breaches** that Bruemmer's group works with had a root cause in **employee negligence”** (Michael Bruemmer, Experian's data breach resolution group, 2015)



Internal disclosures

- Disgruntled employee
- Social engineering scams
- Phishing scams
- Human errors
- Privilege escalation

The Balancing Act

- Ease of Use
- Maintenance
- Speed to Delivery
- Cost Cutting
- Simplicity
- Reactive
- Get-R-Done
- Invisible Success

- Compliance
- Stability
- Quality
- Availability
- Functionality
- Proactive
- Customer Service
- Visible Issues

Risk Mitigation

Legal Risks

Regulatory Risk

Financial Risks

Compliance Risks

Political Risks

Resource Risks

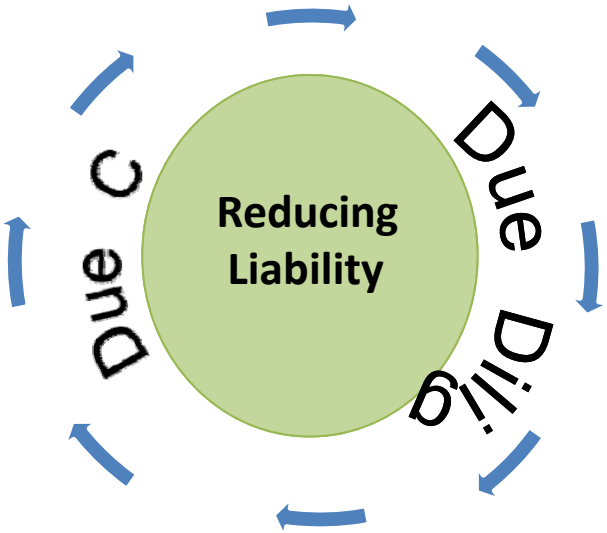
Credibility Risks

Reducing Liability

"If an organization does not practice due care and due diligence pertaining to the security of its assets, it can be legally charged with negligence and held accountable for any ramifications of that negligence" (Harris, 2010, p. 110)

Due Diligence is the act of continually investigating and understanding the risks and vulnerabilities the organization faces.

Due Care is implementing security policies, procedures, standards and countermeasures to provide protection from those threats.



The Three Tiers
Above and Beyond the Technical

TECHNICAL

THE TECHNICAL LAYER – deals with putting in place the technical infrastructure designed to recognize and prevent breaches from occurring.

ADMINISTRATIVE

THE ADMINISTRATIVE LAYER – deals with having in place security policies, procedures, and processes designed to lay a foundation for managing and administering security across the organization.

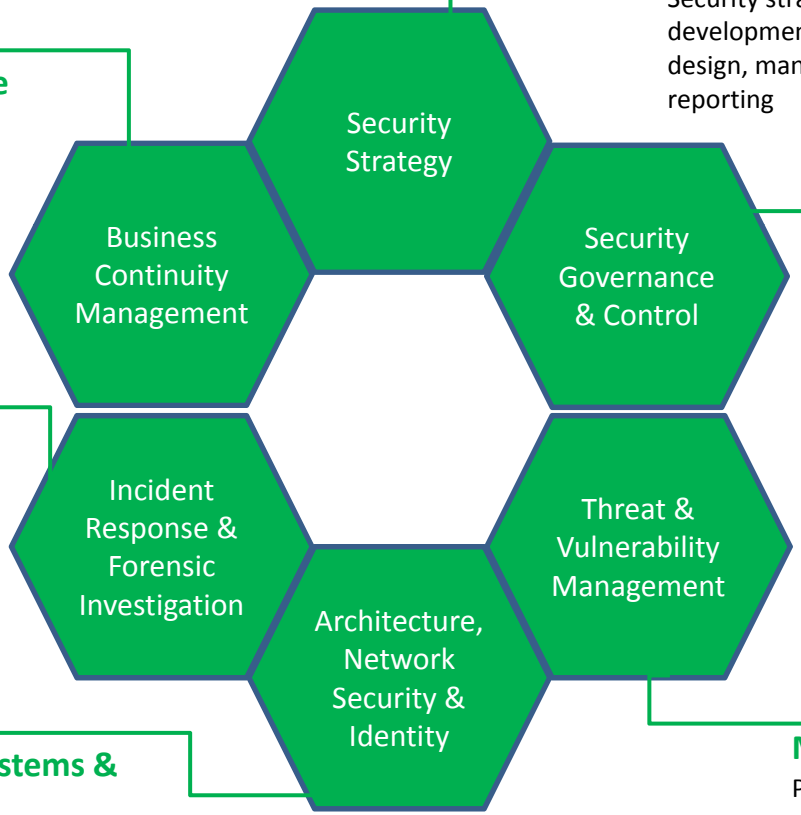
GOVERNANCE

THE GOVERNANCE LAYER – deals with the ongoing verification and validation of all security system implementations, including both the technical and administrative functions

Leadership Support

- Senior leader buy-in （make security important）
- Communicate and educate at all levels
- Create a culture of security awareness
- Establish strong governance （what you permit you promote）
- Incorporate all three tiers （technical, Admin, Compliance）
- Trust but verify （external audits）
- Be prepared for the worst （incident response plan）
- Define responsibility and accountability at all levels
- Demand continual improvement
- Reward and recognize

Security Life Cycle



Setting Direction
Security strategy development, organization design, management reporting

Building in Resilience
Business continuity Management, disaster Recovery, crisis management

Creating a Sound Framework of Control
Risk, policy and privacy review, regulatory compliance assessment, data loss prevention, awareness programs

Managing Incidents
Incident response review, corporate and regulatory Investigations and readiness crisis response

Managing Exposure
Penetration testing, vulnerability scanning and remediation, continuous and global threat monitoring

Building Secure Systems & Infrastructure
Security architecture, network security, cloud computing security, identify and access management solutions, ERP security

Resources

Multi-State Information Sharing & Analysis Center
http://msisac.cisecurity.org/

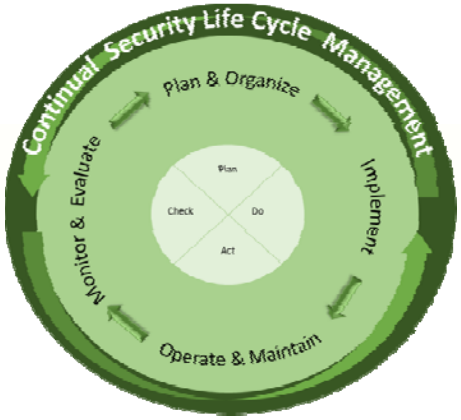
Cyber Security Guides
http://msisac.cisecurity.org/resources/guides/

SANS Information Security Policy Templates
http://www.sans.org/security-resources/policies/?ref=3731

NIST Cybersecurity Framework
http://www.nist.gov/cyberframework/

SANS 20 Critical Security Controls
https://www.sans.org/critical-security-controls/controls

United States Computer Emergency Readiness Team
https://www.us-cert.gov/


Continual Security Life Cycle Management
Plan & Organize
Implement
Operate & Maintain
Monitor & Evaluate
Plan
Do
Check
Act

QUESTIONS?


Continual Security Life Cycle Management
Plan & Organize
Implement
Operate & Maintain
Monitor & Evaluate
Plan
Do
Check
Act