



Converging Security: Policies and Procedures

Gov Tech 2009

HBMG



HBMG

NOVUS
EDGE

Raak
TECHNOLOGIES

BLUEWAVE
security



Panel Members

- Mance Harmon; CEO, Blue Wave Security
- Dan Cunningham; CEO, RAAK Technologies
- Michael Cation; Founder, Novus Edge
- Frank Fayyaz; Network Services Director, HBMG Inc.
- Moderator: Sloan Foster, VP Marketing, HBMG Inc.



Purpose of this Panel

To help integrate policies and procedures (best practices) that bridge the gap between cyber and logical security.

Physical, logical, and cyber/data security are no longer optional elements to any enterprise; they are necessities. They create an interwoven security blanket.



What is Security Convergence?

“The true meshing of physical security, cyber security and business continuity management, putting an organization in a position to make security a functional strategy and a business opportunity.”

What it *IS*:

Integrating historically stovepiped functions of operational risk management to achieve better security, oversight of enterprise-wide risk and cost efficiencies.

What it *ISN'T*:

**Putting IT security under the thumb of the physical security group, or vice versa.
Creating one big “cost center” out of several smaller ones.**

It's all in how you present it...

DOCTOR FUN



Copyright © 2006 David Farley, d-farley@ibiblio.org
<http://ibiblio.org/Dave/drfun.html> Used with permission



“Convergence Engineering”

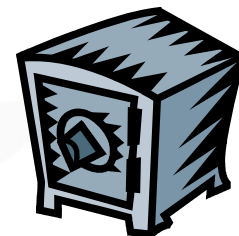
- *A strategic approach to solving the technical problems associated with the integration of logical & physical security*
- Driven by:
 - FIPS-201 under Presidential Directive HSPD-12 developed by NIST
 - Increased security functionality
 - Ex: Physical presence in building required before login
 - Cost savings
 - Synergy savings
 - Strategic technical implementations
- Focuses on *technical* not “people” issues.



The “S” Word – Synergy

Some Key Opportunities:

- Access control, “Common Card” systems
 - DoD’s Cross Credentialing Project
- Log monitoring
- In-house IP video surveillance and DVR recording
- Computer acquisition and forensics
 - Investigations are often prime driver
- Employee termination and de-provisioning
- Theft of computer assets
- Theft of electronic data
 - Breach Laws
- Chain of custody and legal issues
- Physical safety risks
- Security Awareness initiatives





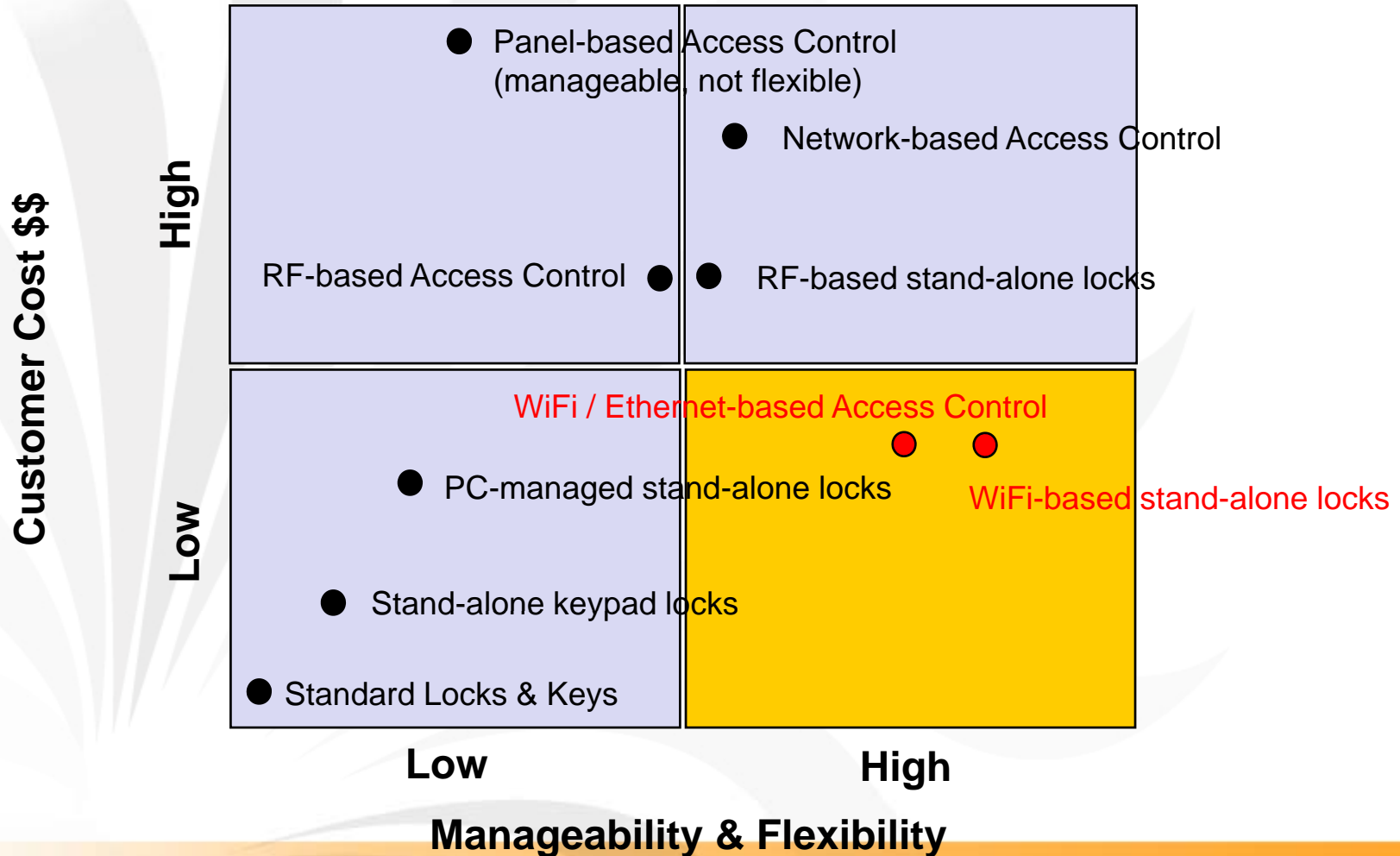
Proven Success in Convergence

- Recent Aberdeen research on Security Governance and Risk Management (November 2007) showed that by taking a more holistic view of risk, organizations with top performance have demonstrated their ability to improve security, sustain compliance, improve leverage from existing IT resources, make faster decisions, optimize business processes, and improve visibility across organizational and geographical “silos”.



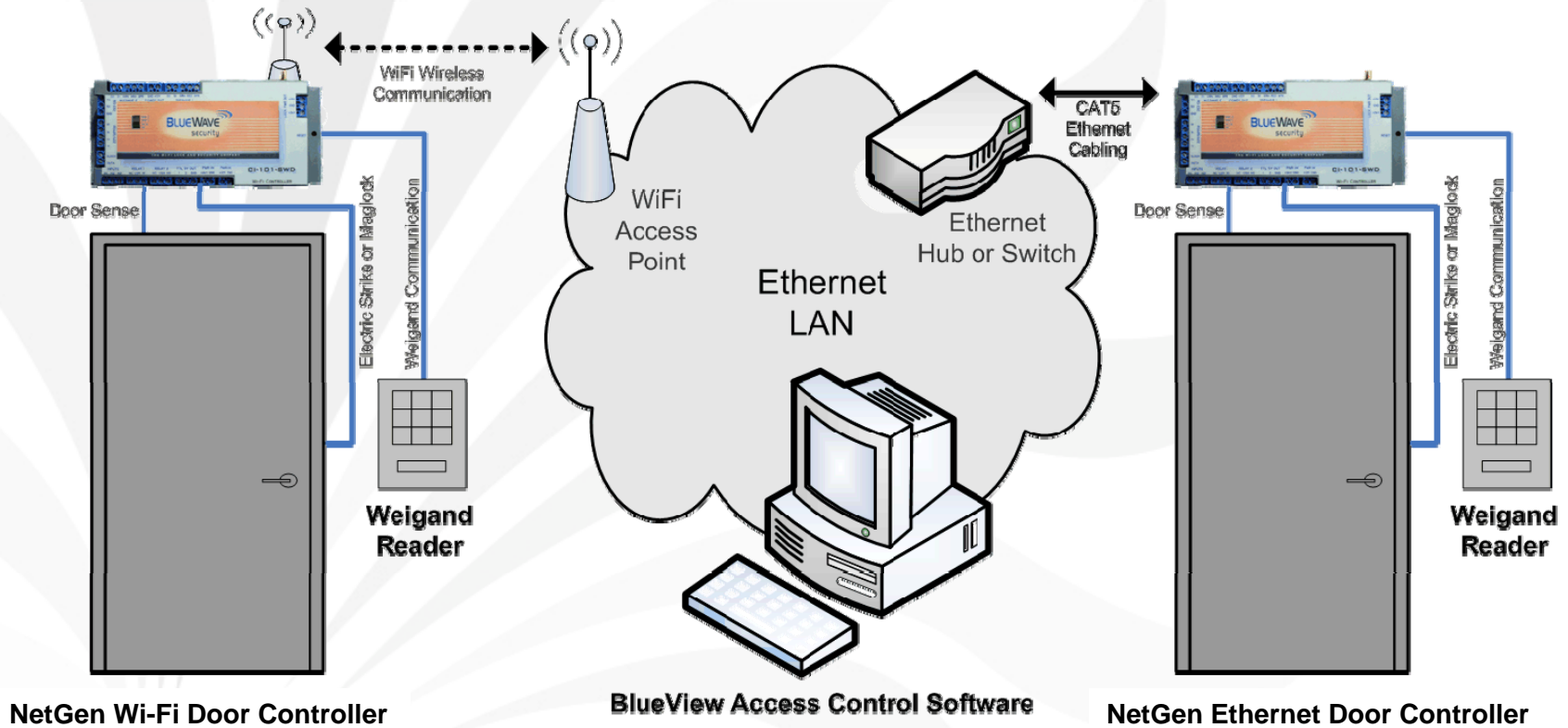
Changing The Game In Access

Control





BlueLink Wi-Fi and Ethernet Controllers





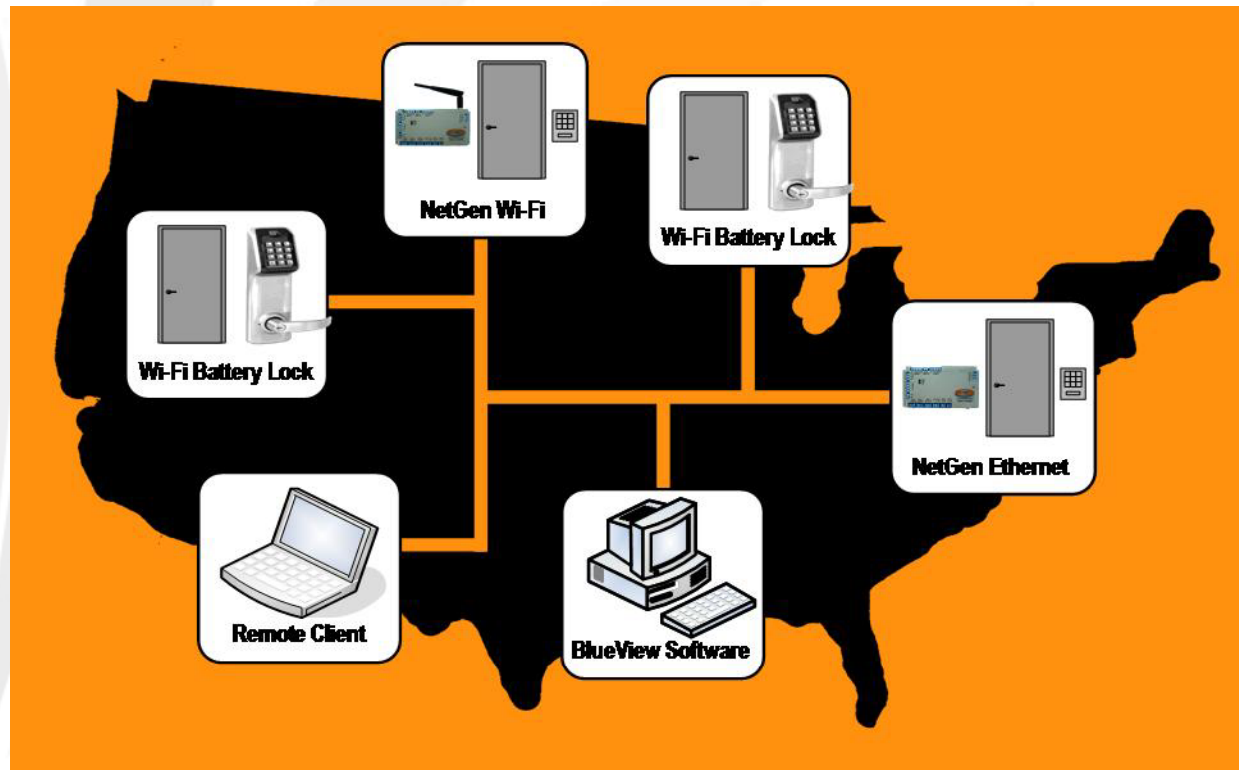
Wi-Fi Modem



- BlueLink Wi-Fi Module
 - The only Wi-Fi modem anywhere that can run on an off-the-shelf battery pack for years without recharging
 - Modem is licensed to stand-alone, battery powered lockset manufacturers
 - Provides central management of battery powered locksets over Wi-Fi
 - Enables lockset manufacturers to compete directly with panel-based access control solutions at about 25% of the cost



Open Standards Converged Solutions





Strong Authentication: Smart Cards and Smart Tokens

- Strong authentication: two factor authentication - something you know, a PIN; and, something you have, a smart card or smart token.
- Smart card: conforms to credit card form factor; contains an integrated circuit.
- Token: USB device with an USB interface and integrated circuit.





Strong Authentication: Drivers

- External threats
- Internal threats
- Compliance with external regulations – government or industry
- Compliance with internal policies
- End user trust/confidence



Implementing Strong Authentication

- Standards based – Win 2003 server
- Client (PC/Laptop) software
- Card/token applet
- Strong controls: from data gathering to issuance to revocation
- Card Management System (CMS) required for large roll-outs



Benefits

- Secure audit trail
- Non repudiation
- Auto log off
- Greater security both internally and externally
- Ability to add third factor (e. g., biometric) if required



Convergence: Physical and Logical Access

- Single card – RFID for building access; smart card chip for logical access
- Or, RFID for both physical and logical access
- Front end – cards and issuance software are available today
- Back end – in process
- Embraced by both camps

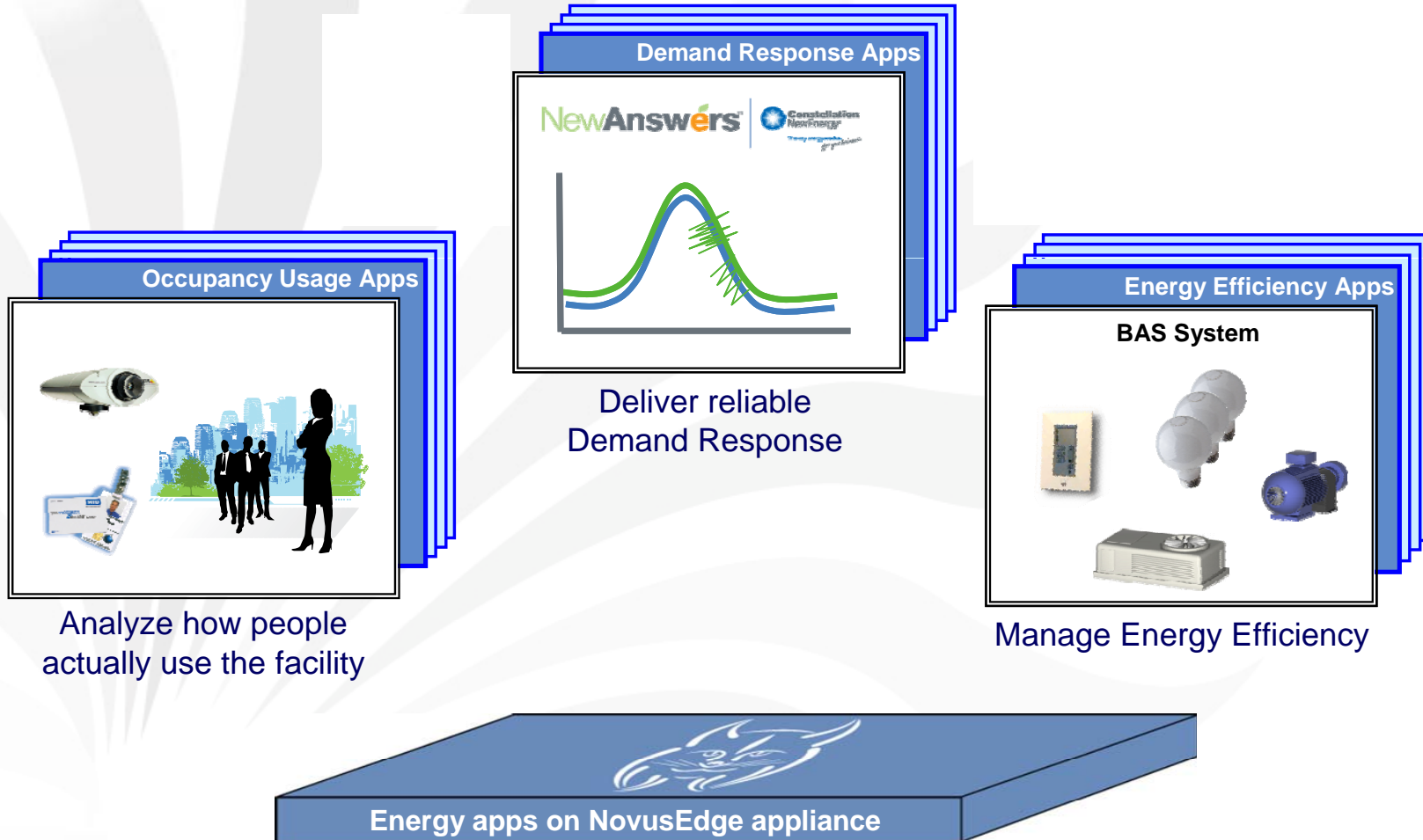


Safety, Energy Conservation & Convenience

- Convergence of control systems in the building
- Security systems tell you where people are in a building
- Other systems can use this information!



Security Enables Energy Management



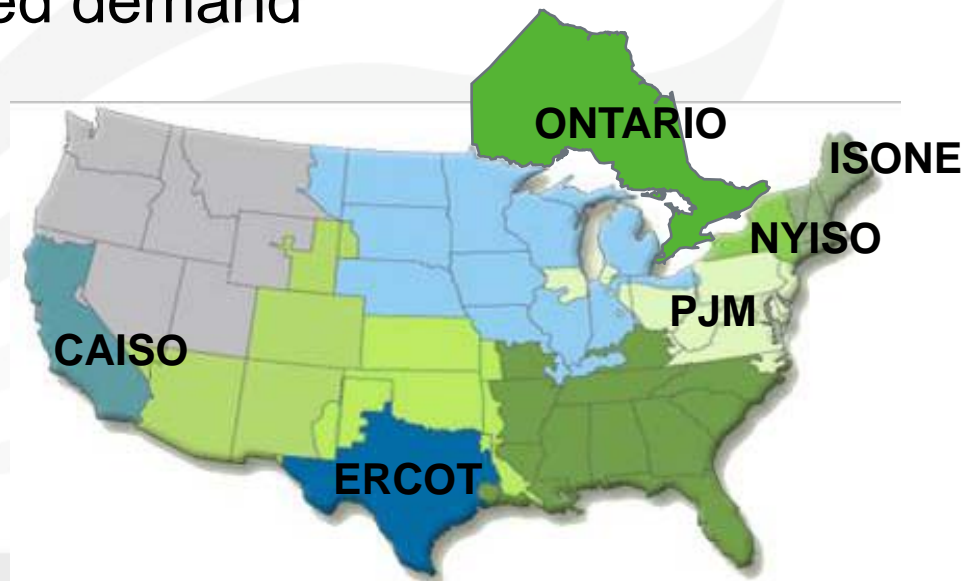


Energy Economics

(Demand Response)

- Electric power suppliers provide financial incentives to reduce electric power consumption at times of peak demand
- Payments average approximately \$69,000 per year per Megawatt of reduced demand

(A "typical" office building represents a Megawatt of reducible demand)





Problem of National Importance

Electric Demand Growing Faster Than Electric Supply	Amount
Increase in U.S. Generation Required during the next 10 years	19%
Increase in U.S. Generation Scheduled for the next 10 years	6%
Demand Response Implications	Amount
U.S. Demand Response Market (Annual)	\$4.2 billion



What is Cyber Security

- Identifying a threat and protecting your Network against that threat
- Hardware, Software, Data and Physical Locations
- Preparation and Implementation
- Making Confident decision



Early 2000's Cyber Security

- Event Driven
- Management Lack of Enforcement
- Network Scan Performed on Occasions
- Not Many School Offer classes
- Security not integrated, just an add-on



Security Threats

- **SPAM**
 - 200 billion messages each day
 - E-mail, Txt Messages, Mail and Phone
- **Phishing**
 - Social Engineering
 - Email, malicious web sites
 - E-mail or call from Fake financial institute asking for Personal Data
- **Botnets and Root kits**
 - Zombies or Robots
 - Viruses or malware
 - Taking control or Redirect
- **Social engineering**
 - E-mail, IM, Text Messages, Phone
 - Entice victims to open a file
 - Used by the adult sites
- **Reputation hijacking**
 - Online Criminals
 - Real E-mail accounts
 - 7.6 percent of top three provider e-mails

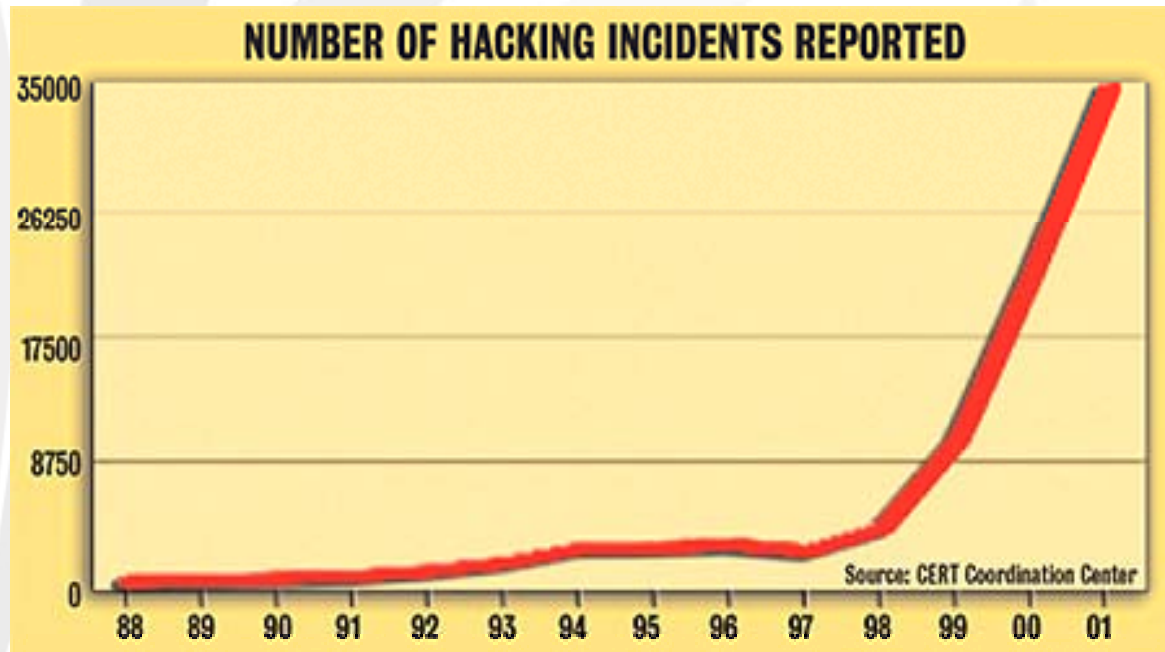


Before 911

- Major vulnerabilities were laptops
 - Theft, loss of data
- Desktop workstations vulnerable to viruses
 - Installing virus protection software
 - Constantly upgrading
- Defenses primarily
 - Access control software
 - Front door to applications
 - Emphasis on authorized users

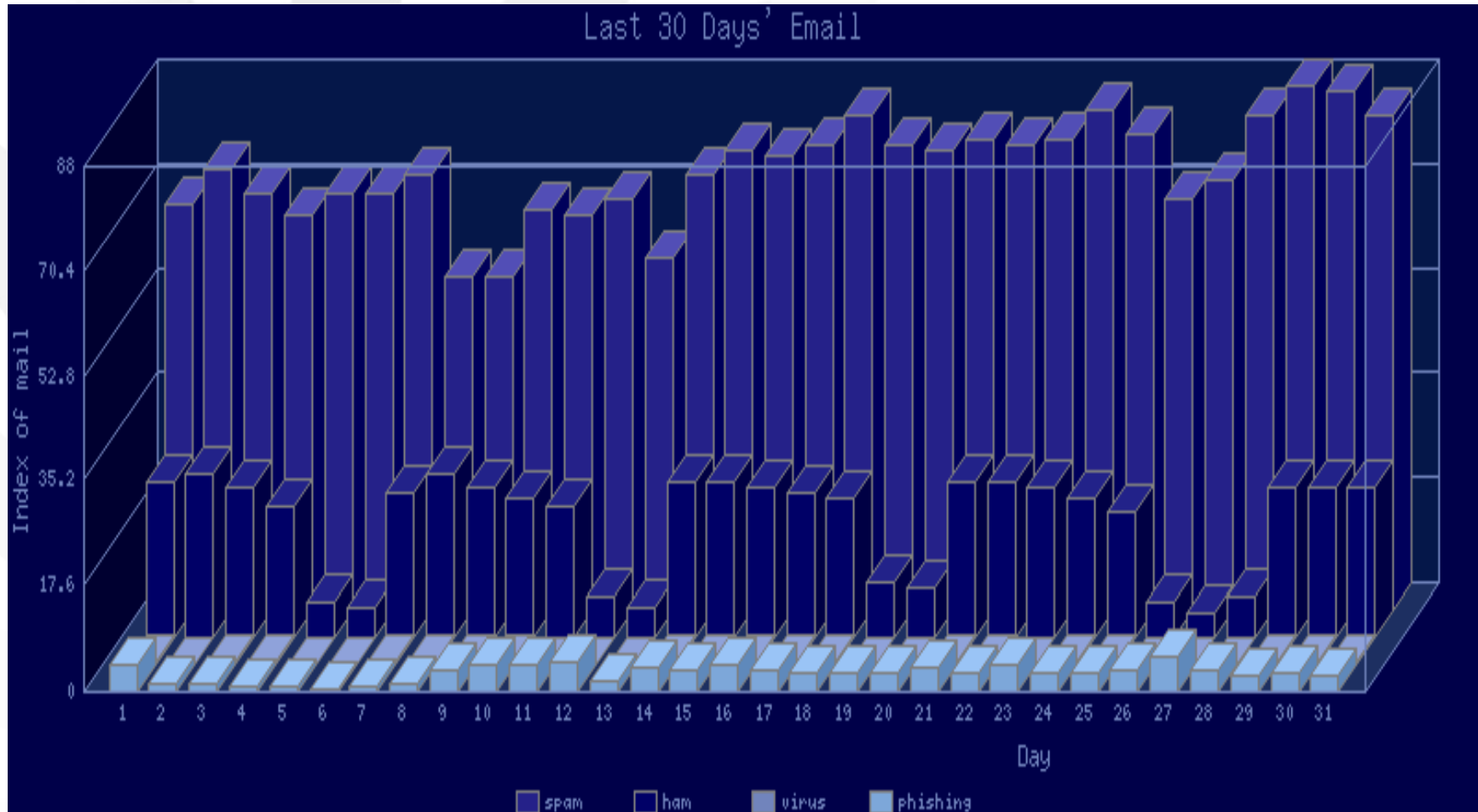


Attacks going up





WWW & SPAM





Standard & Certification

- ISA Standard - SP 99
- Government Regulations
- ISA Security Compliance Institute (ISCI)
- **ISO 17799**
- **IEEE 1402**
- **NERC**



Government and Banking

- Cyber Security Serious meter
 - Maximum Investment
 - Gaining customer confidence
 - Proving to share holder
- Levels of Cyber Security
 - Customer Level
 - Industry Level
 - Firm level



Government and Banking

- Legal & Law enforcement take action
- Legislation to combat Identity theft
- Take action at federal level
- Awareness among general public



Convergence: Physical and Logical Access (cont)

- Enables new security measurements
 - How can you log on to the network if you have not entered the building?
 - How can you log on from home when you are in the building?
- Industry movement
 - HID Crescendo launch February 2007
 - SCM/Hirsch merger December 2008



Security as a Strategic Process

Benefits

- Saves security budget dollars
- Increases efficiency
 - Centralized risk management
 - Combined monitoring
 - Better detection and tracking
- Streamlines incident response
 - Better information sharing
- CSO functions as single point of contact
 - Provides oversight for all security issues
 - Increased value to the company as scope includes physical & information security, risk management and business continuity
- IT Security becomes less of an “optional” choice
 - Embeds security and risk management into business processes and executive decision making
- Raises security awareness
- Cross training creates motivated employees
- Consistent policies across the enterprise



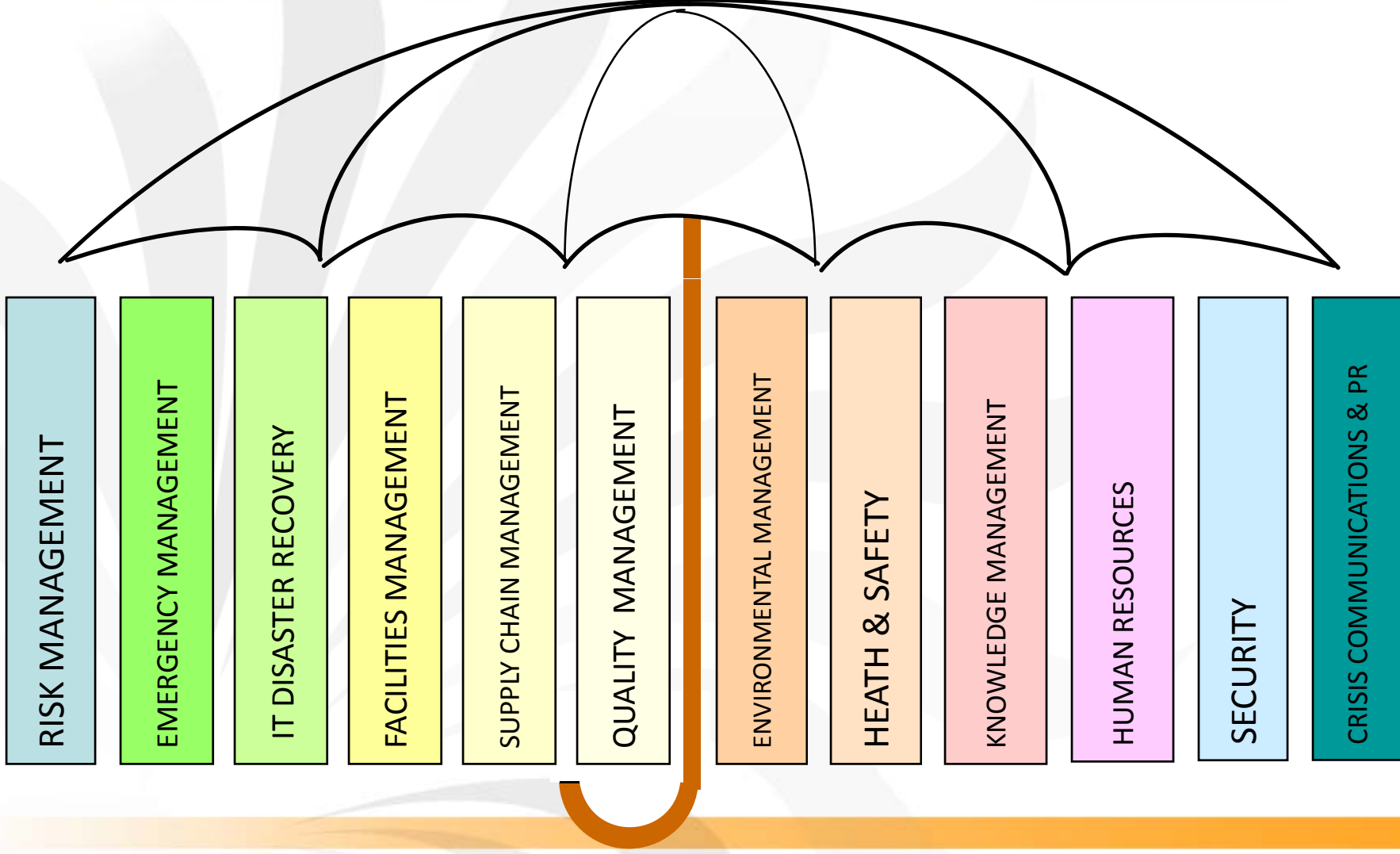
The “Competitors”

Physical Security	IT Security	Financial Security
Typically drawn from law enforcement or military	Typically drawn from technology ranks	Typically drawn from financial community
Reports to Facilities, Administration, or HR	Reports to CIO or IT Operations	Reports to CFO
Frames issue as protection of people, facilities, operations	Frames issue as availability, integrity, confidentiality of information and systems	Frames the issue as “Risk Management”
Values authority and command	Values creativity and technology innovation	Values financial efficiency and loss prevention
Contributes prevention skill sets	Contribution is continuity, availability, and integrity of IT capacity & technology	Contribution is regulatory compliance and quantitative rigor



HBMG

THE UNIFYING PROCESS



RISK MANAGEMENT

EMERGENCY MANAGEMENT

IT DISASTER RECOVERY

FACILITIES MANAGEMENT

SUPPLY CHAIN MANAGEMENT

QUALITY MANAGEMENT

ENVIRONMENTAL MANAGEMENT

HEALTH & SAFETY

KNOWLEDGE MANAGEMENT

HUMAN RESOURCES

SECURITY

CRISIS COMMUNICATIONS & PR



A Riskier World?

HBMG

Risk Management – A changing framework

Value of Tangible assets

Value of Intangible assets

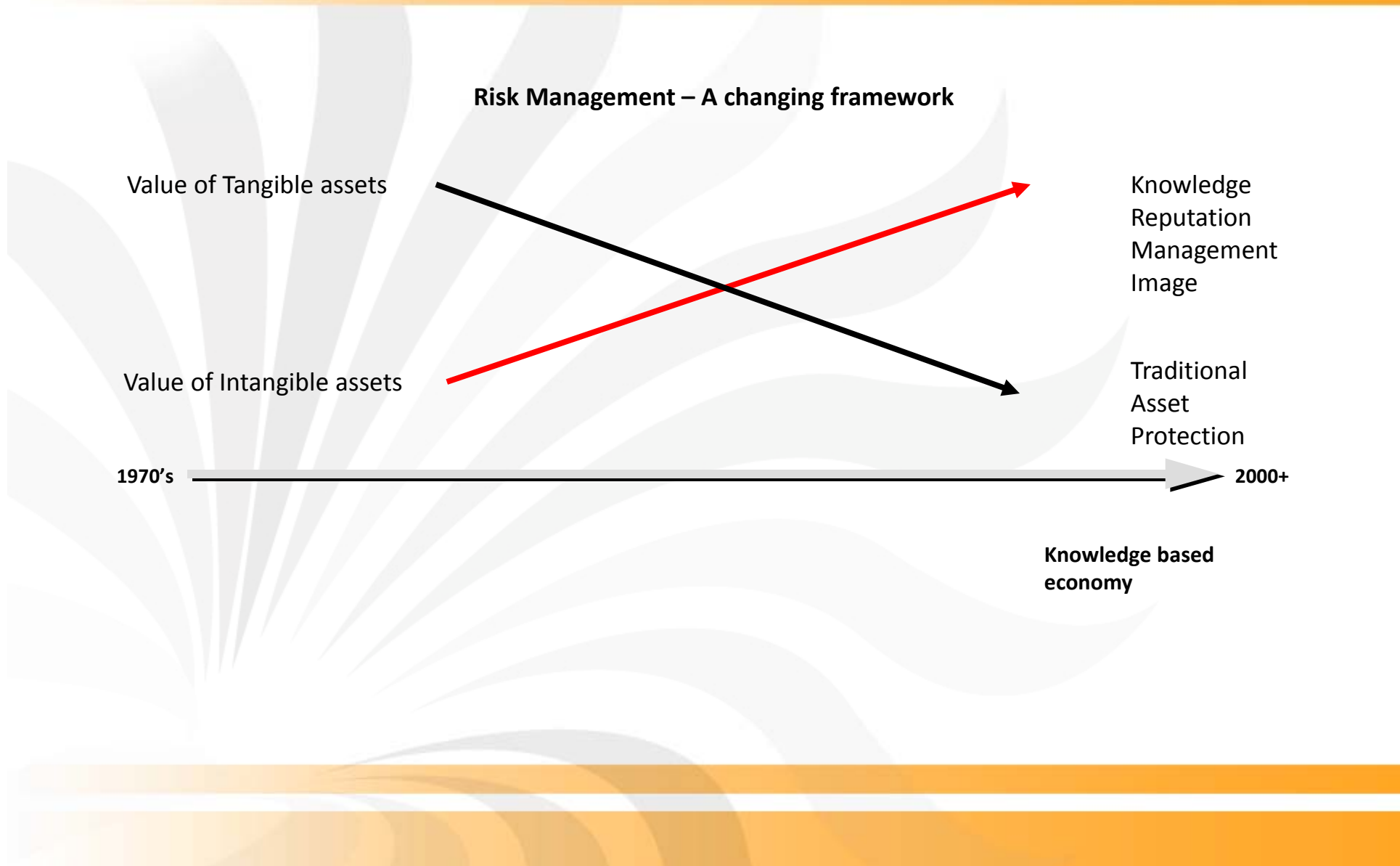
1970's

2000+

Knowledge
Reputation
Management
Image

Traditional
Asset
Protection

Knowledge based
economy





Benefits of Convergence

Organizations set themselves up to compete in the global economy in the global economy with a distinct advantage: not only with an optimized IT infrastructure, but also with better-protection for their digital, physical and human assets.



HBMG

- www.opensecurityexchange.org