

Integrating Security – Adding Value and Reducing Risks

Steve Lund

Director of Security

Intel Corporation

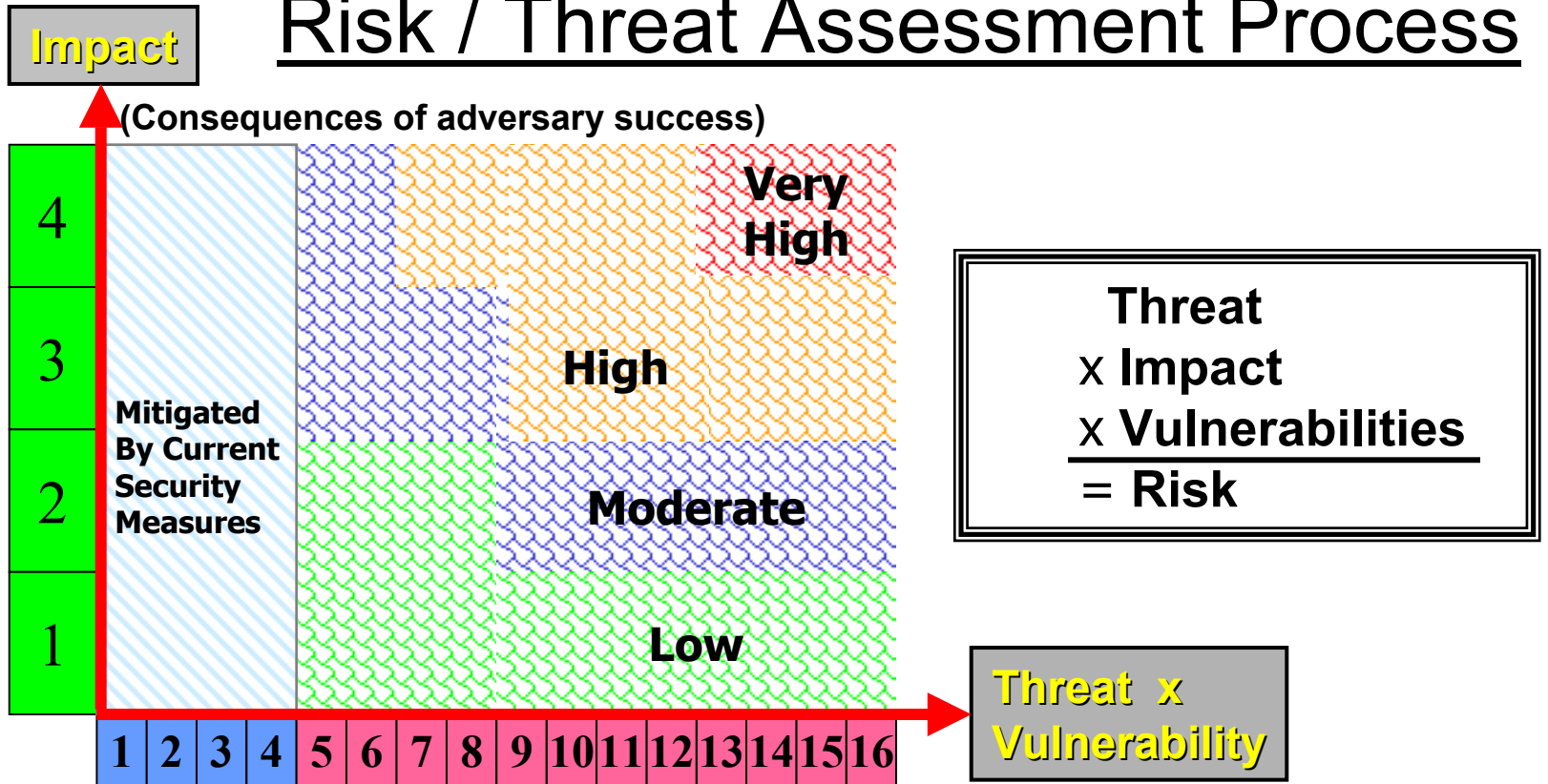
Focus Areas of Protection / Response

- Factory Operations
 - Manufacturing--including automation / networks
- Support Services
 - Equipment, utilities, network connectivity, alternate workspace, facility maintenance, phones, email, etc.
- Supply Chain
 - Take orders, fill orders, ship orders, *ensure delivery*
- Employee Services
 - Payroll, internal communications, contingency plans, family support, traumatic event response, transportation
- Business Continuity
 - Commitment by Business Groups to own and sustain, with guidelines and coaching from process experts

Integrated Tools / Processes

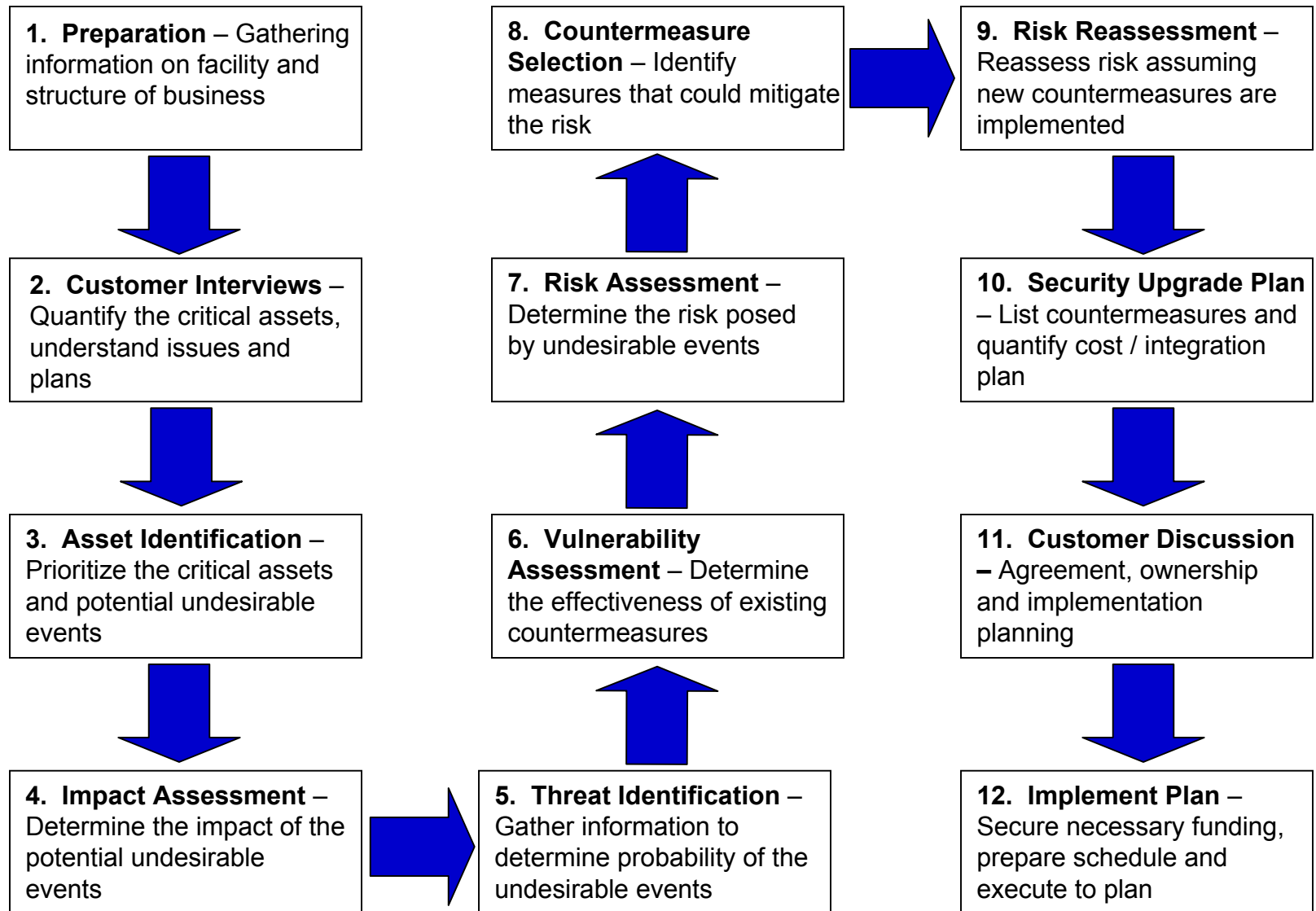
- Threat / Risk Assessment Protocol
 - Standard process applied individually
 - Cyclical refresh based on new/emerging data/trends
- Intelligence
 - Collection – External and Internal resources
 - Collation – What does it mean?
 - Dissemination – Keep data flowing
 - Action – Identify and Deploy Necessary / Appropriate Actions
- Security Operations
 - Deter, Detect, Delay, Respond – Concentric Rings philosophy
- Security Operating Systems
 - Access control, employee databases, records
 - “Universal Front End” – (See Backup)
- Communication
 - Clear paths, identified responsibilities, contingency contact capability

Risk / Threat Assessment Process



Risk level	Score	Interpretation
Very High	49-64	The risk is high, human and critical assets under threat, added countermeasures should be implemented to eliminate/reduce the risks
High	27-48	The risk is potentially high, countermeasures should be implemented to reduce the risks
Moderate	17-26	The risk is elevated, but may be acceptable -- all countermeasures should be reviewed
Low	1-16	The risk is acceptable and the countermeasures are adequate

12 Steps of Risk Assessment

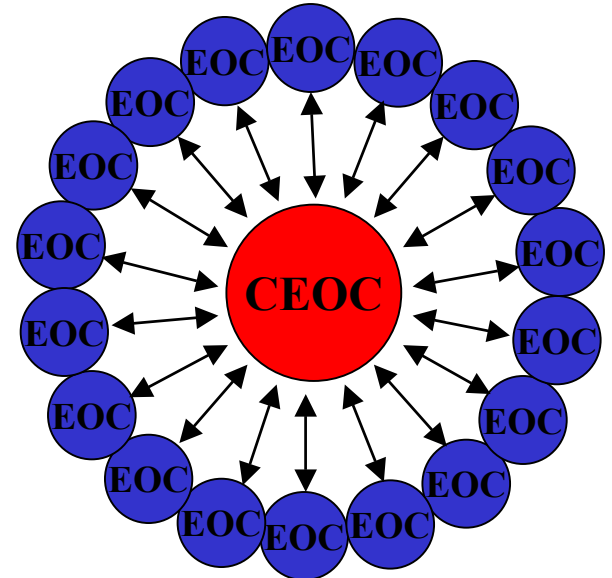


Site Emergency Operations Centers (EOC's)

- Located at each major site worldwide
- Locally managed, with EOC director from major business group, with cross-functional participation:
 - Local business groups
 - Security
 - EHS
 - Public Affairs
 - Site Services
- Established location on-site, with equipment and procedures as required by Corporate Emergency Management program, including:
 - Response templates for various scenarios
 - Multiple computer connections
 - Media connection (e.g. satellite TV news)
 - Redundant communications
 - PBX phone lines
 - Dedicated copper phone lines
 - Local channel radios
 - Satellite telephones
 - Ham Radio equipment / operators

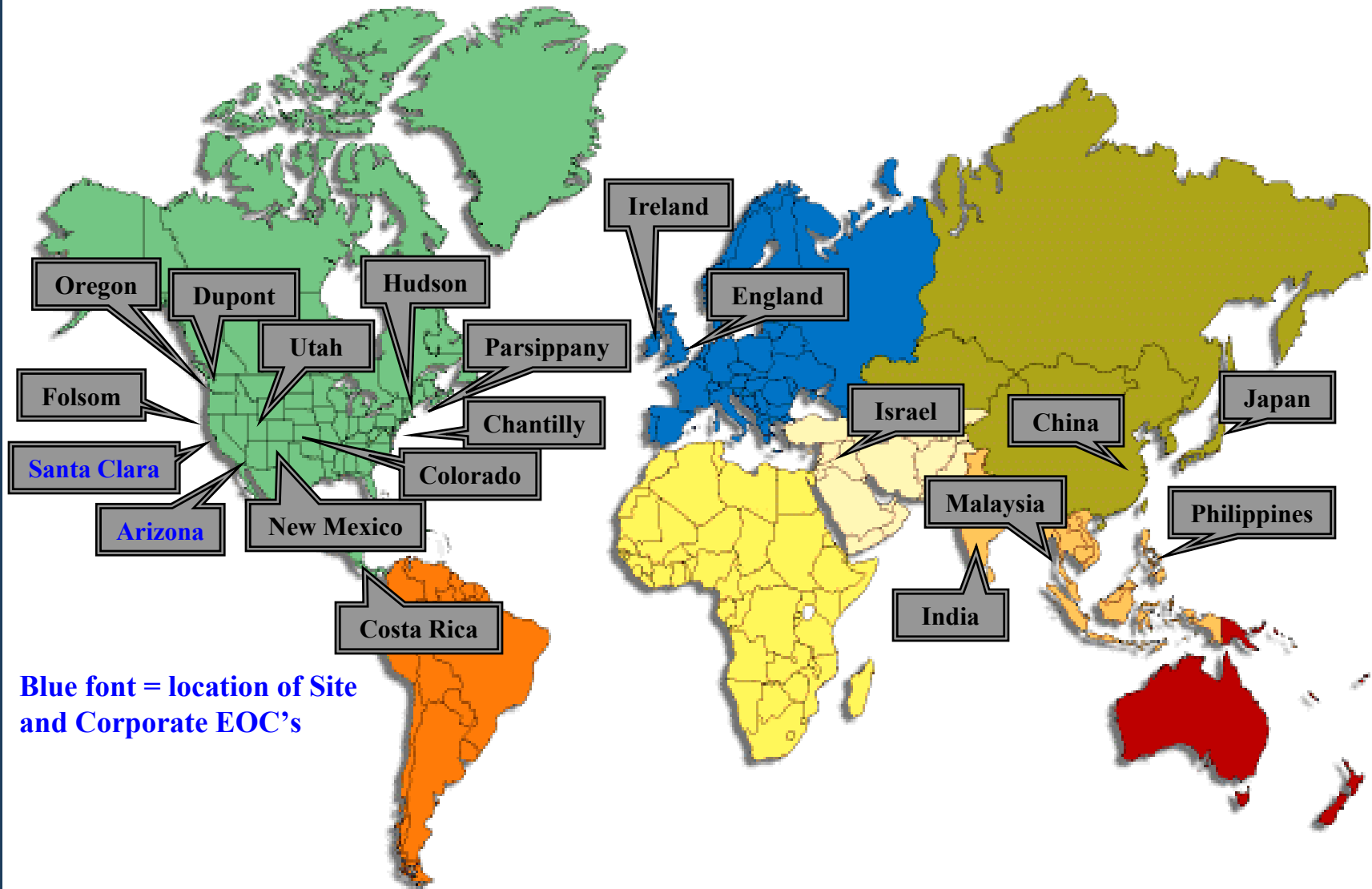
Corporate EOC

- Mission:
 - Manage global/multi-site issues and threats so as to best protect employees, facilities, production, sales, distribution, and other assets
 - An umbrella organization for other emergency response organizations
 - Ensure informed, effective, and timely internal and external communications
 - Coordinate, **not** manage the response
- Multiple locations for redundancy and efficiency
- Membership at senior-level management
 - Core CEOC – Director, Coordinator, Security, EHS, Corporate Communications, CEOC Scribe
 - Extended CEOC – Legal, HR, Sales, Finance, other business groups
- Established rooms, fitted with all site EOC elements
- CEOC guidelines specific to CEOC operations
 - Controlled document, scheduled revisions
- Activation linked to existing Security or EOC escalation actions, or at discretion of core team members



Intel Site Emergency Operations Centers (EOC's) and Corporate Emergency Operations Centers (CEOC's)

INTEL SECURITY



Emergency Response Drills

- Corporate Emergency Management group, site EOC's, and various business groups have historically utilized tabletop exercises and full drills – Corporate Drill Roadmap
- After September 11th, some drill scenarios were added, and scope of drills increased to comprehend all operational elements
 - Anthrax response (based on existing plans) – included test kits, expanded communication, employee awareness (mail rooms)
 - Other biohazard scenarios
 - Aviation disaster response
 - Function-specific business recovery
 - CEOC and EOC emergency response capability
 - “Dirty bomb” scenario
- Typically 10-12 separate drills per quarter
 - Designed and led by affected business group
 - Site EOC and CEOC participation as warranted by scenario

Drill Protocol

- Business unit drills designed to include all potentially impacted elements of that group
- Clear and detailed drill scenarios outlined—including:
 - Participants and their roles
 - Design of drill
 - Objectives of the exercise
 - In scope / Out of scope
 - Artificialities of the drill (assumptions)
 - Starting script
- Drills involve accelerated timelines, role-playing, simulated supplier engagement
- Key suppliers have been engaged in establishing Business Continuity and identifying gaps and focus areas
- Supply network rebalance/reset has become a key aspect of drills

Response Coordination Tools

- Emergency Contact Database (ECDB)
 - On-line database of key management, business group, and response group personnel
 - Updated routinely to include travel contact data
 - Hard-copy backups of main contact info in EOC/CEOC's
- CEOC Status Board
 - Online tool, accessible to authorized users via intranet and internet
 - Single point of status for CEOC events and drill
 - Displays current status of an event, it's location, impact, description, key contacts, etc.
 - Shows activation levels for EOC, Security, IT and other corporate capabilities or business groups
 - All communications related to event—Press releases, Q&A's, Circuit Articles, etc. to ensure consistency
 - View access tied to ECDB groups

Mode **Actual** Drill

Legend **Operational** On Alert Emergency

Events Communications Administration

**** ACTUAL MODE ****

CEOC Director
GARY HENSLEY
[History](#) [Change](#)

Viewer's Time
10-Jul-2003 11:23 PT
[Change Timezone](#)

Next CEOC Meeting: 30-May-2003 11:00 PT [Update](#)

Next CEOC / Site EOC Meeting: 30-May-2003 11:30 PT [Update](#)

[Add Event](#)

[Add Communication](#)

Global Events

Display Status EOC Security

Show **Active & Notify Events**

Show For **Last 30 Days**

Global Events Timeline

Group By: Date Event Msg Type

Active Events

Notified Events

[D2 Service Yard Lime Spill](#)

Sites Affected

Corporate Capabilities

Occurred On:

Local Time: 02-Jul-2003 16:42 PT

Viewers Time: 02-Jul-2003 16:42 PT

Last Updated: 02-Jul-2003 16:44 PT

Updated By: MARY PIMM

*California, Santa Clara

Security

02-Jul-2003 16:43 [D2 Service Yard Lime Spill](#); Status Change By PIMM MARY Security Corporate Capability has been set to "A-Operational".

02-Jul-2003 16:42; [D2 Service Yard Line Spill](#); New Event Entered By MARY, PIMM
Notified by: Mary Pimm, Site EOC - Source
Activation Level: EOC Level 3

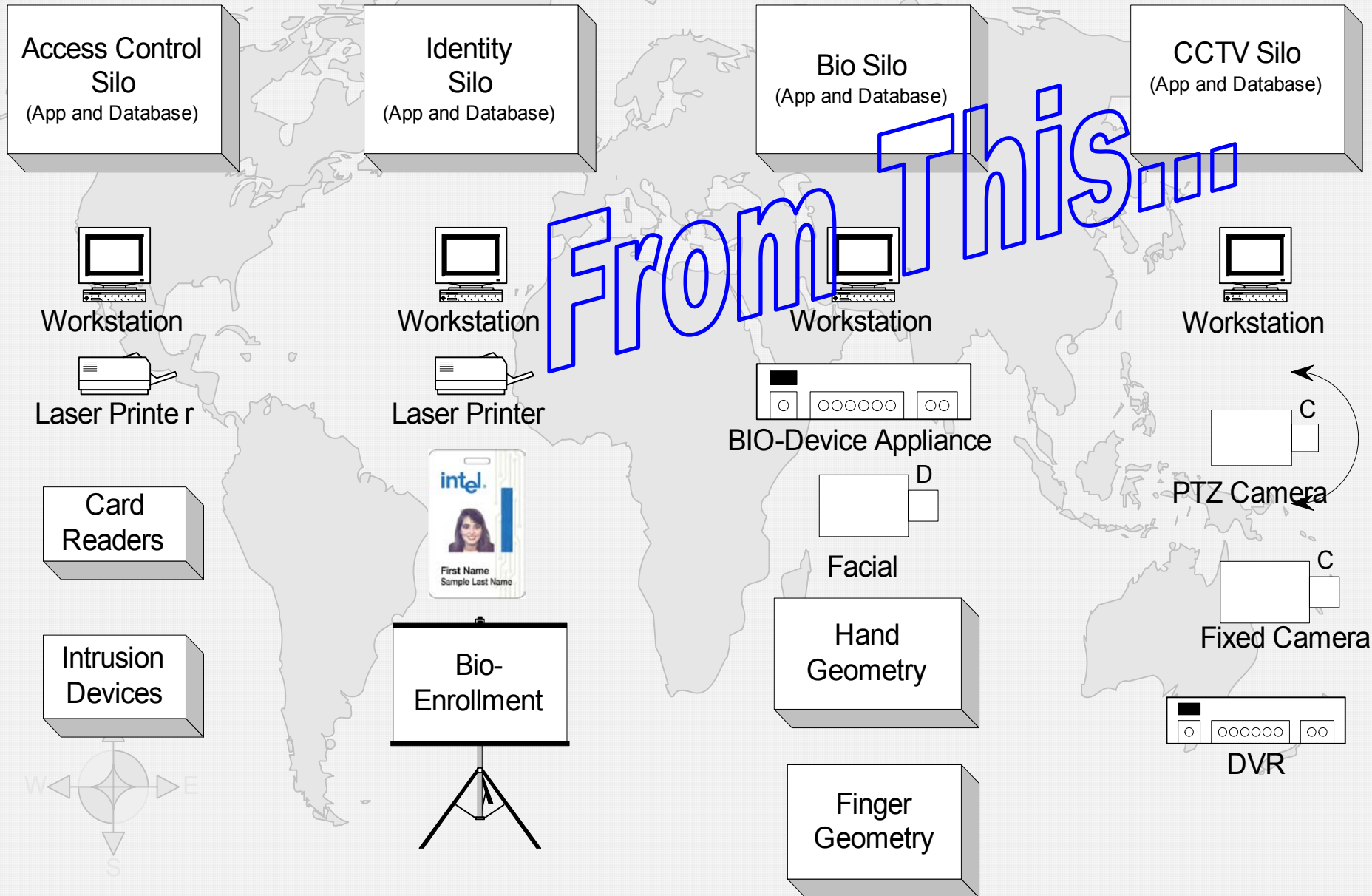
Monitoring Events

DeActivated Events

EXAMPLE

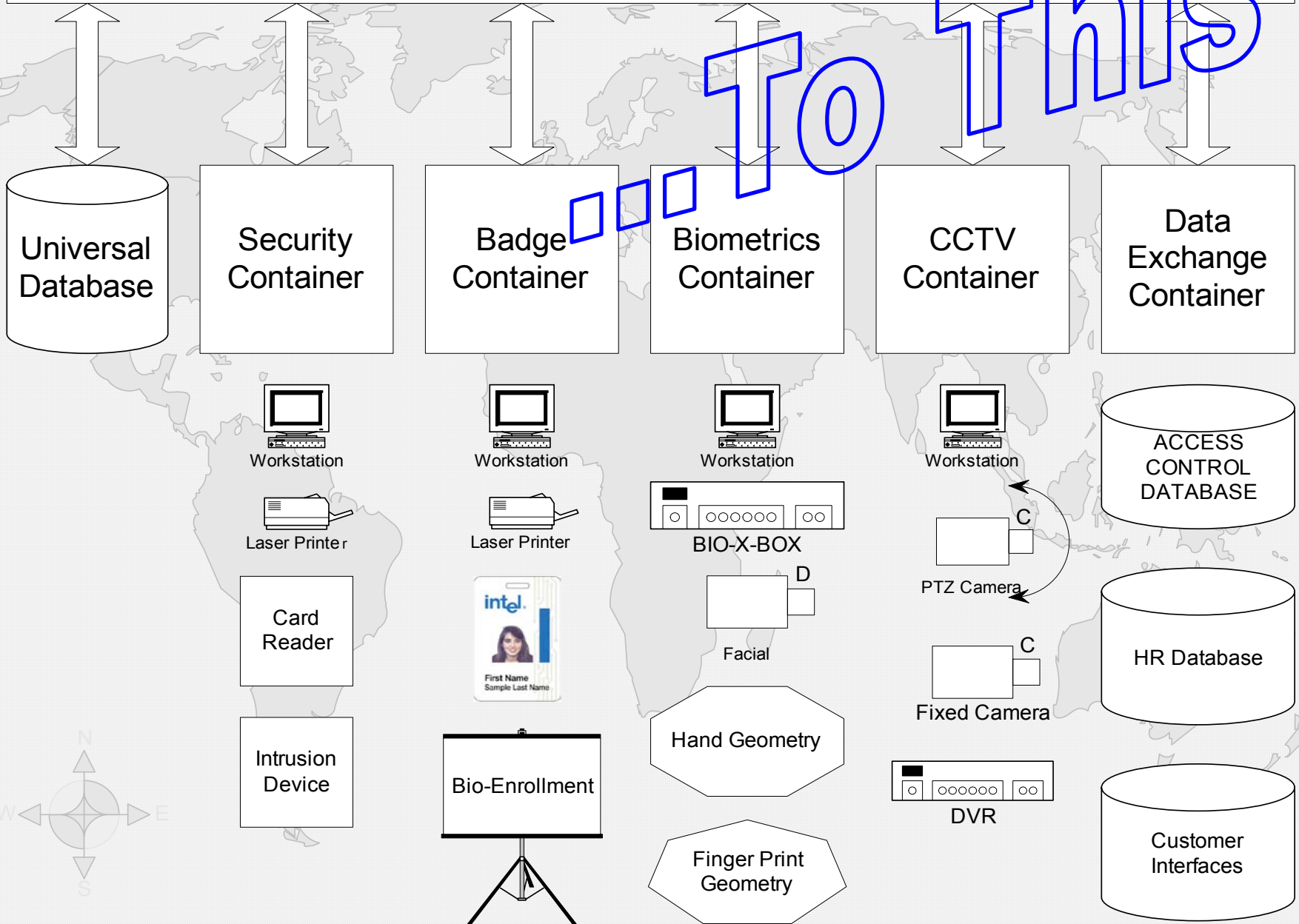
Back-Up

Traditional Security System Infrastructure



Universal Front End Application

To This



Security Next Generation Impacts



Network Bandwidth

- * **Traditional 10 Megabit Prevalent**
- * **100 Megabit Typically Recommended for Digital Video**
- * **Standard Encryption Algorithms**

Network Infrastructure

- * **Security Resident on IT Network**
- * **Security Inside Dedicated Subnets**

Network Security

- * **Intranet/Internet Access**
- * **Standard IT Encryption**

Merging of Security Technologies

- * **Traditional Silo of Products Merging (Access Control, Biometrics, CCTV)**
- * **Dedicated Network Devices to Security (Encryption, Compression)**

Qualified Trained Support Personnel

- * **Security Migrating to a Merged Security/IT Roll**
- * **No Accredited Training Available**