Corporate Information Protection Strategy

Hilton Chan PhD, Vice-chairman
Information Security and Forensics Society
(email: hilton@ust.hk)

Corporate Information Protection

Penetration Test

Audit Trail

Firewall

Access Control

User Awareness Training

IT Crisis Management

System/Data Backup

Intrusion Detection

Password

Anti-virus

PIN

Business Contingency Planning

Encryption

Data Recovery

Public Key Infrastructure

Computer Forensics

Virtual Private Network

Incident Investigation

Corporate Information Protection

Corporate Information Protection?

What about IT Security, computer security, and data security?

The World of Data

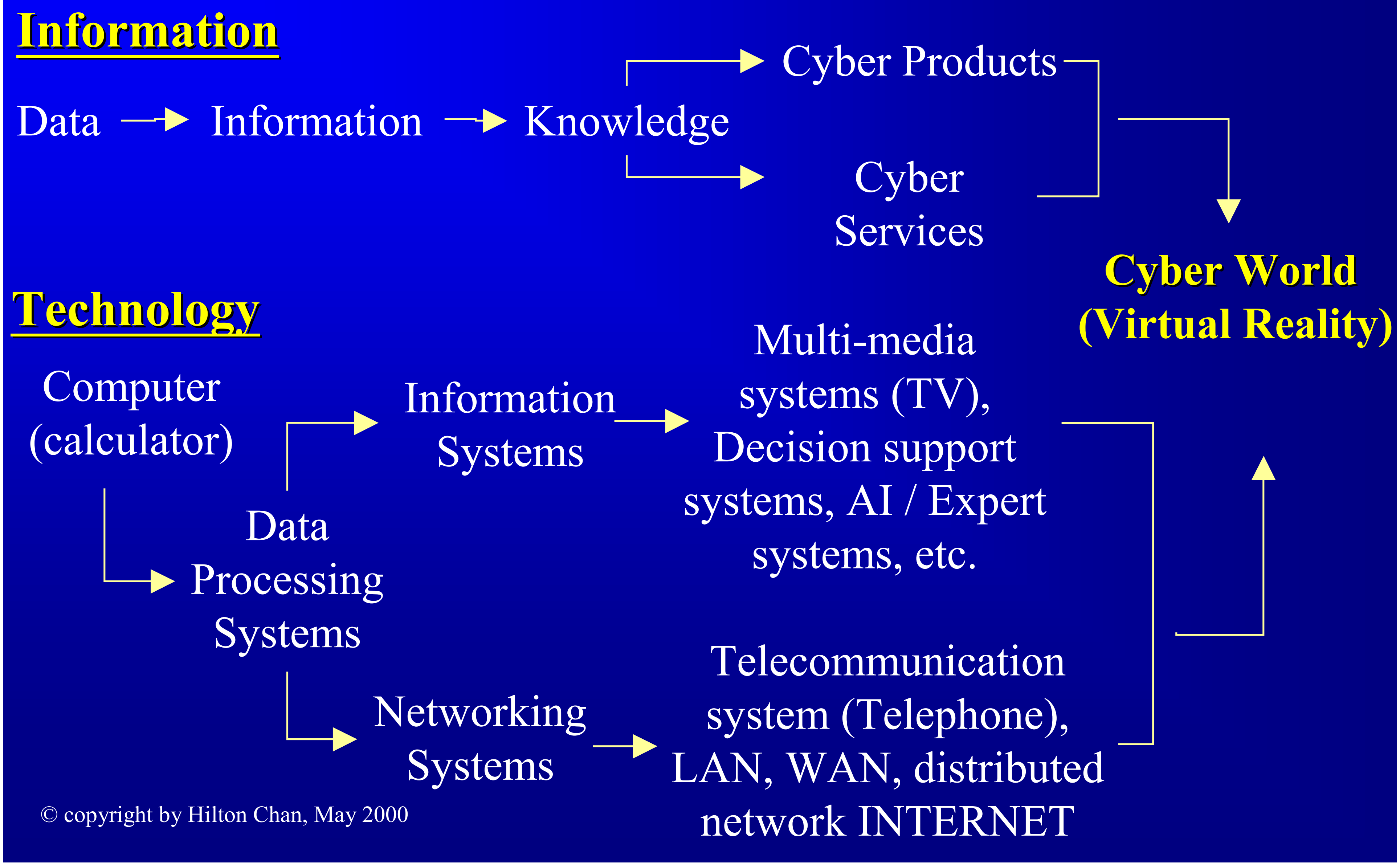
Data (Yesterday)

Numbers

Words

Records

Information Technology



Information

Data → Information → Knowledge

Cyber Products

Cyber Services

Cyber World (Virtual Reality)

Technology

Computer (calculator)

Information Systems

Data Processing Systems

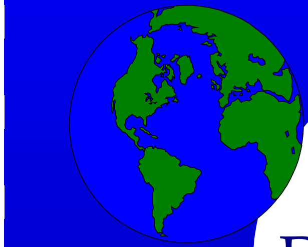
Networking Systems

Multi-media systems (TV), Decision support systems, AI / Expert systems, etc.

Telecommunication system (Telephone), LAN, WAN, distributed network INTERNET

Knowledge Economy
(Personal, Social and Commercial Activities)

Data → Intellectual Products/Services



E-mail Voice mail Video phone E-cash

Digitized video (movie)/audio (music) News group

Digital signatures Search engines Business web sites

Encryption keys IRC/ICQ Cyber advertisement

Internet Content/carrier service providers

Chat groups Cyber-medical services E-auction

Cyber-entertainment Video conference

Internet Shopping E-business, etc.

Virtual Reality

Corporate Information Protection

- CIA or AIC Model (Confidentiality, Integrity and Availability)
- DDUM (Destruction, Disclosure, Use and Modification)

Corporate Information Protection

- Data Security
- Technology Dimension (Computers, Telecommunication Networks, Software)

Corporate Information Protection

- Data Security
- Computer/IT Security
- Business dimension (legal/social/ethical)

Expanded Data Security Model

Confidentiality and Possession

- Secrecy and Control

Integrity and Authenticity

- Completeness and Validity

Availability and Utility

-Usability and Usefulness

Source : Donn Parker 1998

Four Phase model – DIER (Discovery, Investigation, Escalation and Revelation)

Discovery

-Deterrence (User Awareness Program)

-Prevention (Firewall, Anti-virus, Penetration Test)

-Warnings (Intrusion Detection, Audit Trail Analysis)

Investigation

-Computer Forensics/Evidence Gathering (Tracing, Logs Analysis)

-System Restoration (Disaster Recovery, IT Crisis Management, Business Contingency)

-Problem-solving

Escalation

-Internal

-External (PR Strategy – Business Partners, Public, Law Enforcement, Stakeholders)

Revelation

-Post-restoration (Policy Review, BPR, Organization restructuring, Strategic repositioning)

-Legal Action (Computer Forensics & Digital Evidence)

Forensics and Digital Evidence

Business Contract

- Eye-witnesses, paper, ink, signature, company seal, watermark, fingerprint, DNA (saliva), etc.
- Process and procedures (laws in the physical science)

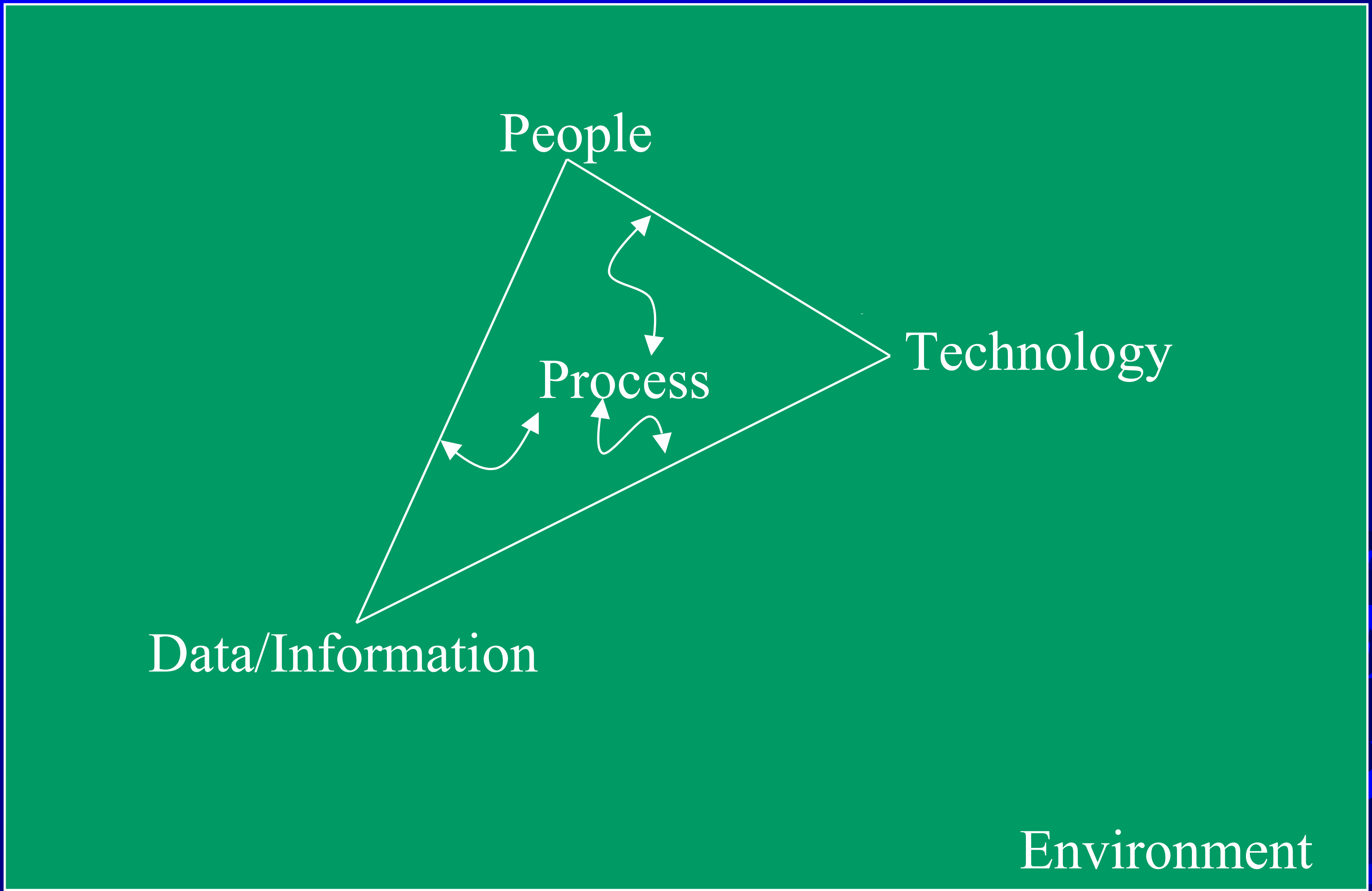
e-Contract

- PKI (keys), digital signature, time stamp, digital watermark, anti-virus software, intelligent agent, etc.
- Process and procedures (virtual reality)

Additional considerations:- key management (key escrow, key deposit, key recovery, etc.)

Corporate Information Security Model

Corporate Information Security Model



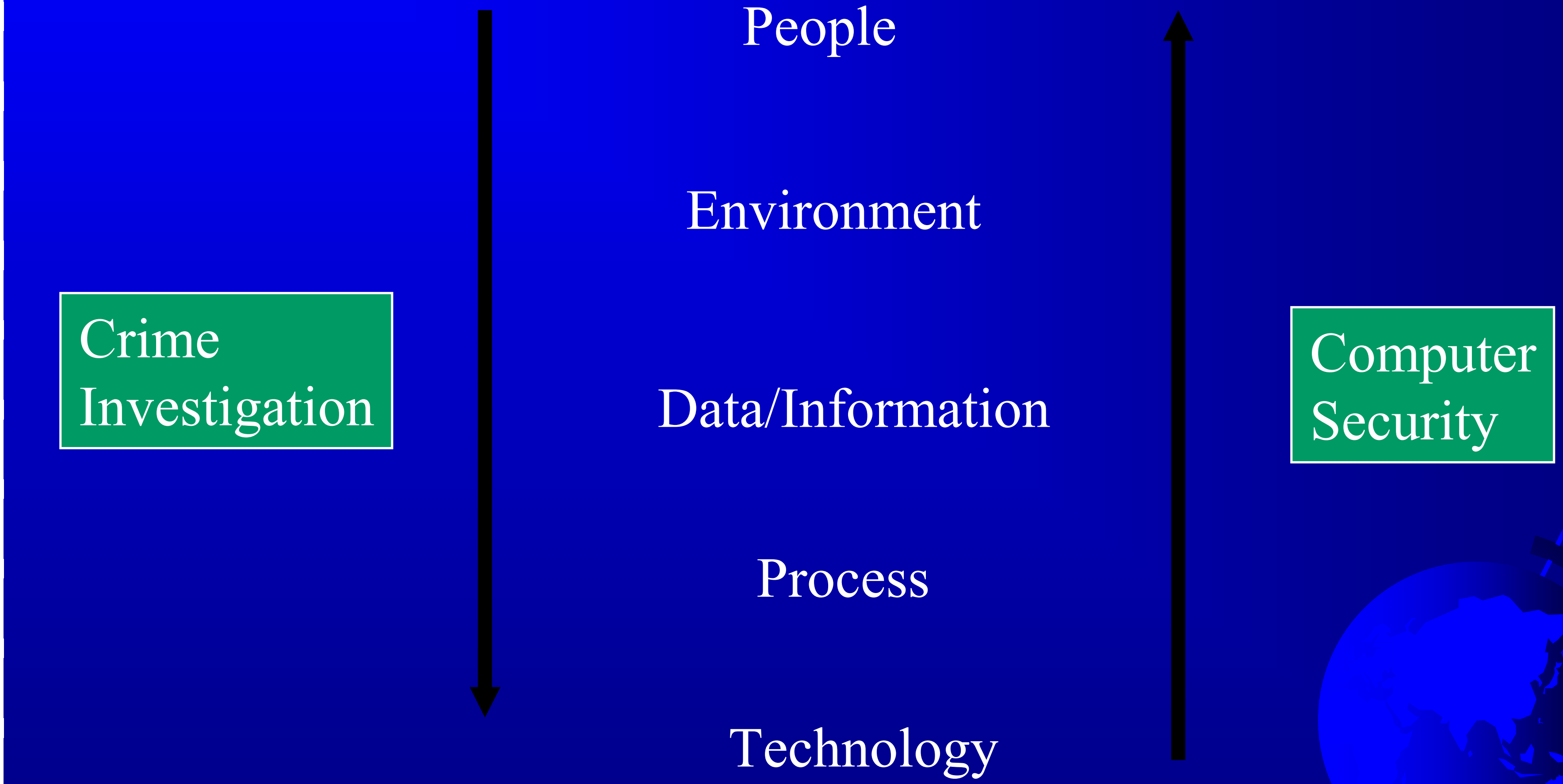
People

Technology

Process

Data/Information

Environment



Crime Investigation

People

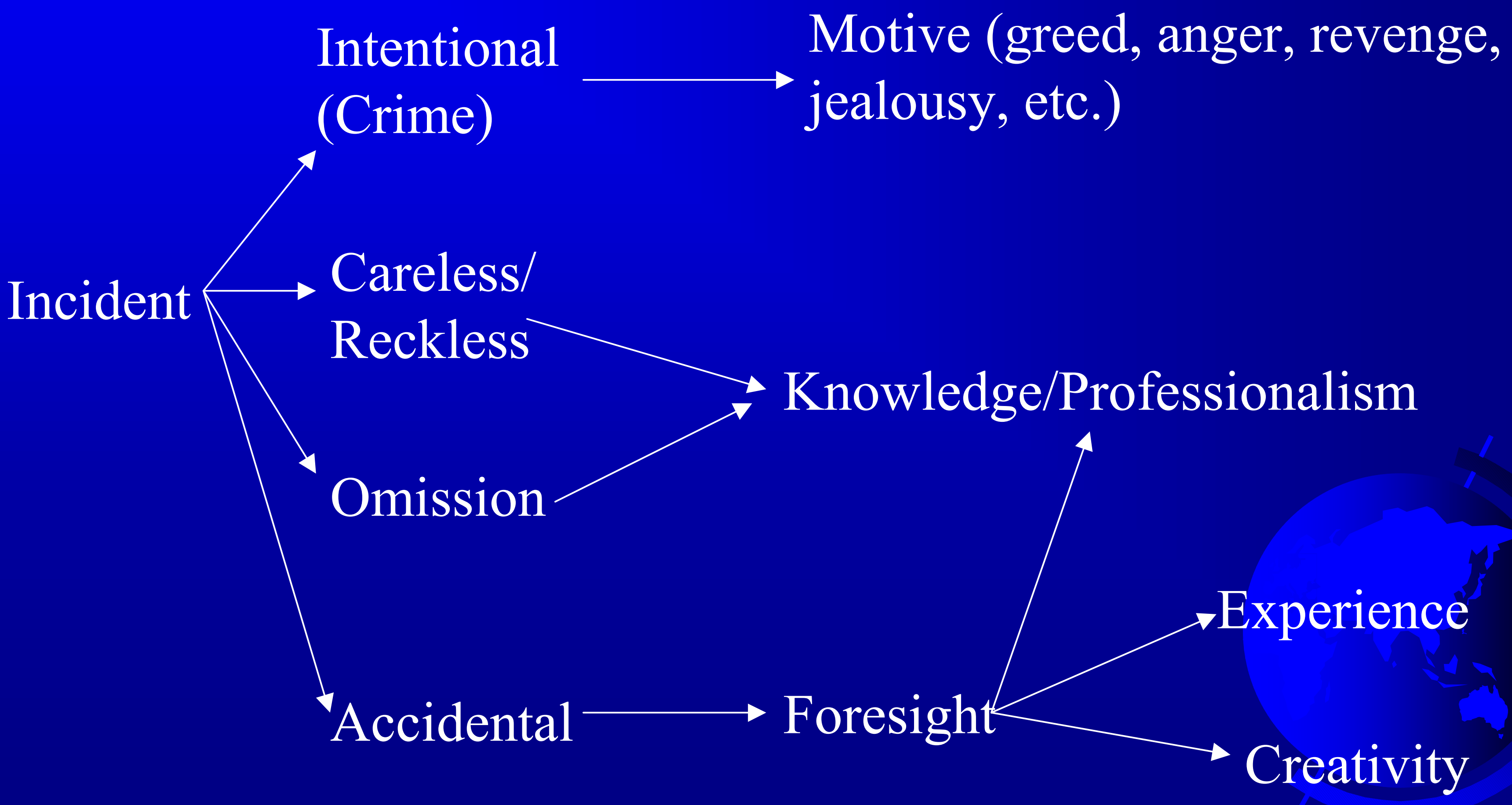
Environment

Data/Information

Process

Technology

Computer Security



Incident

Intentional (Crime)

Motive (greed, anger, revenge, jealousy, etc.)

Careless/ Reckless

Omission

Knowledge/Professionalism

Accidental

Foresight

Experience

Creativity

An Illustration of the Low-level View of Information Protection to support Strategic Use of Information

- Use of Data/Information
  - Control (view, amend, add, delete, ……)
  - Ownership (proprietary, co-owned, shared, ……)
  - User (individual, team, group, corporate, all, ……)

Content of Data/Information

- Validity
- Completeness
- Relevancy
- Timeliness
- * assessment/grading by human or AI

Source of Data/Information

- Reliability
- Single vs. Multiple
- Open vs. Covert
- * assessment/grading by human or AI

Information Protection - Multidisciplinary Approach

Law – Criminal Justice System

Accounting – IT Audit

IT Security

Computer Forensics

Standards – Technical and Management Practice

International Cooperation

Public Awareness and Education

What Corporate Information Protection should achieve?

Business Enabler (Competitive Advantage)

IT Enabler (Operational Efficacy)

Simple (Transparent to the users)

Customer-centric (Privacy and Trustworthy)

Information Protection

↓

“Profit” Driver

Questions?