The "Trusted" Insider: Investigating Intellectual Property Theft

A Case of Stolen Intellectual Property

Warren G. Kruse II, CISSP, CFCE, DFCP, EnCE
Principal, Booz Allen Hamilton

George Wade, DFCP, CISSP
Senior Associate, Booz Allen Hamilton

Michael Barba, CISSP, CPP, DFCP, CNE, EnCE
Director, BDO USA LLP

22nd Annual ECI Conference

Agenda

1. Presenters' Background
   - ✓ Warren Kruse
   - ✓ George Wade
   - ✓ Michael Barba
2. In The News
3. A Company and Its Intellectual Property: The Investigation
   a. The Company's IP Defined & Life Cycle
   b. The Investigation Process
4. Working with Internal Corporate Personnel and Law Enforcement
5. The Aftermath, and Lessons Learned

E·C·I
Economic Crime Institute
UTICA COLLEGE

Warren Kruse Background

- **Principal, Booz Allen Hamilton, Cyber Technologies**
- **Author of "Computer Forensics: Incident Response Essentials," an Addison Wesley textbook**
- **A Recipient of the "High Technology Criminal Investigation Association Case of the Year Award"**
- **Experience in computer forensic cases involving some of the largest law firms and corporations in the world, for example:**
  - ✓ **Consulting expert for AMD on the AMD vs. Intel antitrust litigation, which settled for $1.25 Billion.**
  - ✓ **Consulting expert for Continental Airlines, US Air, Cirrus Aircraft, for electronic discovery preservation, collection and identification of electronically stored information.**
  - ✓ **Testified as a computer forensic expert for the US Securities and Exchange Commission (SEC), on issues involving the intentional destruction of data.**
- **2005 International President of the HTCIA**
- **President Digital Forensic Certification Board (DFCB.org)**

E·C·I
Economic Crime Institute
UTICA COLLEGE

George Wade Background

- Senior Associate, Digital Forensics, Booz Allen Hamilton
- Over 20 years of investigative experience, including matters of:
  - ✓ Unauthorized access and hacking
  - ✓ Intellectual property theft
  - ✓ Fraud, theft, waste and abuse
  - ✓ Violations of business code of conduct
- Security and Investigation Management
- Adjunct Instructor for Utica College ECM Graduate Program teaching:
  - ✓ Fraud Management and Technology & Advanced Fraud Analysis
- Past-President of the Northeast Chapter of HTCIA
- Secretary Digital Forensic Certification Board (DFCB.org)

E·C·I
Economic Crime Institute
UTICA COLLEGE

Michael Barba Background

- Director, BDO USA LLP Computer Forensics and Electronic Discovery Practice
- Thirteen Years of Physical Security
  - ✓ Managing security staff of 30 people
  - ✓ Loan Office Defalcation Investigations
  - ✓ Employee Code of Conduct Investigations
  - ✓ Executive Protection Planning
- Over Twelve Years IT Security, Investigations , Computer Forensics, and Electronic Discovery Engagements
  - ✓ Employee Code of Conduct Investigations
  - ✓ Intrusion Investigations
  - ✓ Theft of Intellectual Property
  - ✓ A Recipient of the “High Technology Criminal Investigation Association Case of the Year Award”
  - ✓ Member Digital Forensic Certification Board (DFCB.org)

E·C·I
Economic Crime Institute
UTICA COLLEGE

Keeping the Investigation "Internal"

- "This will not make the press"
- World Events: Spy Plane
- Meeting with Heads of State
- Confidentiality

E·C·I
Economic Crime Institute
UTICA COLLEGE

Why Now?

- Processes Used are Still Relevant
- Method of Investigation Still Relevant
- Experiences are Still Relevant
  - Successes
  - Pitfalls
- Continues to be Used as a Case Example
  - Public Sector - Private Sector Discussions

E·C·I
Economic Crime Institute
UTICA COLLEGE

Company Intellectual Property Defined

- Voice Over IP
- Internet Service Providers
- Internet Telephony
- Intellectual Property bundled into this product
- Still being sold by the Victim Company and being licensed overseas today
- New Generation: Switches built off the same technology
- Product of the Year
  - ✓ 1998
  - ✓ 1999
- 93% of the Market Share
- Saturated the Market through 2000

E·C·I
Economic Crime Institute
UTICA COLLEGE

Company Intellectual Property Lifecycle (continued)

1. Announced the discontinuation of product in January 2001
2. Discontinued due to costing the Victim Company $1.5 Million in expenses per week
3. Remaining units were literally being shipped out for scrap and destroyed at the time this matter was reported

E·C·I
Economic Crime Institute
UTICA COLLEGE

The Investigation

Employee reported a theft:

a. Subjects of Theft

- ✓ Consider "Super Stars" Within their Organization
- ✓ "Smartest People on the Planet" as it related to telephony software and hardware

b. Equipment being removed in gym bags

c. Employee was concerned for his physical safety

d. "You Dumb; They Smart"

E·C·I
Economic Crime Institute
UTICA COLLEGE

The Investigation

To Determine Validity of Report:

a. Conducted cursory search of offices
b. Photographed potential evidence
c. Micro-dotted equipment to identify it
d. Performed computer preservation
e. Analyzed findings
f. Spoke with the Victim Company management and in-house counsel

A few days later…

E·C·I
Economic Crime Institute
UTICA COLLEGE

Confirmation of Allegation

- Assets for the Suspect Company being that of the Victim Company's Intellectual Property
- Victim Company's Source Code listed as asset for Suspect Company
- Additional Victim Company Proprietary source code in the hands of subjects
- Officers are current and former Victim Company employees

The Investigation

Fresh Probable Cause

E·C·I
Economic Crime Institute
UTICA COLLEGE

The Investigation: Fresh Probable Cause

- Identification of Suspect Company name
- Suspect Company employees from Victim Company, and other technology companies
- Suspect Company Officers are current and former Victim Company employees

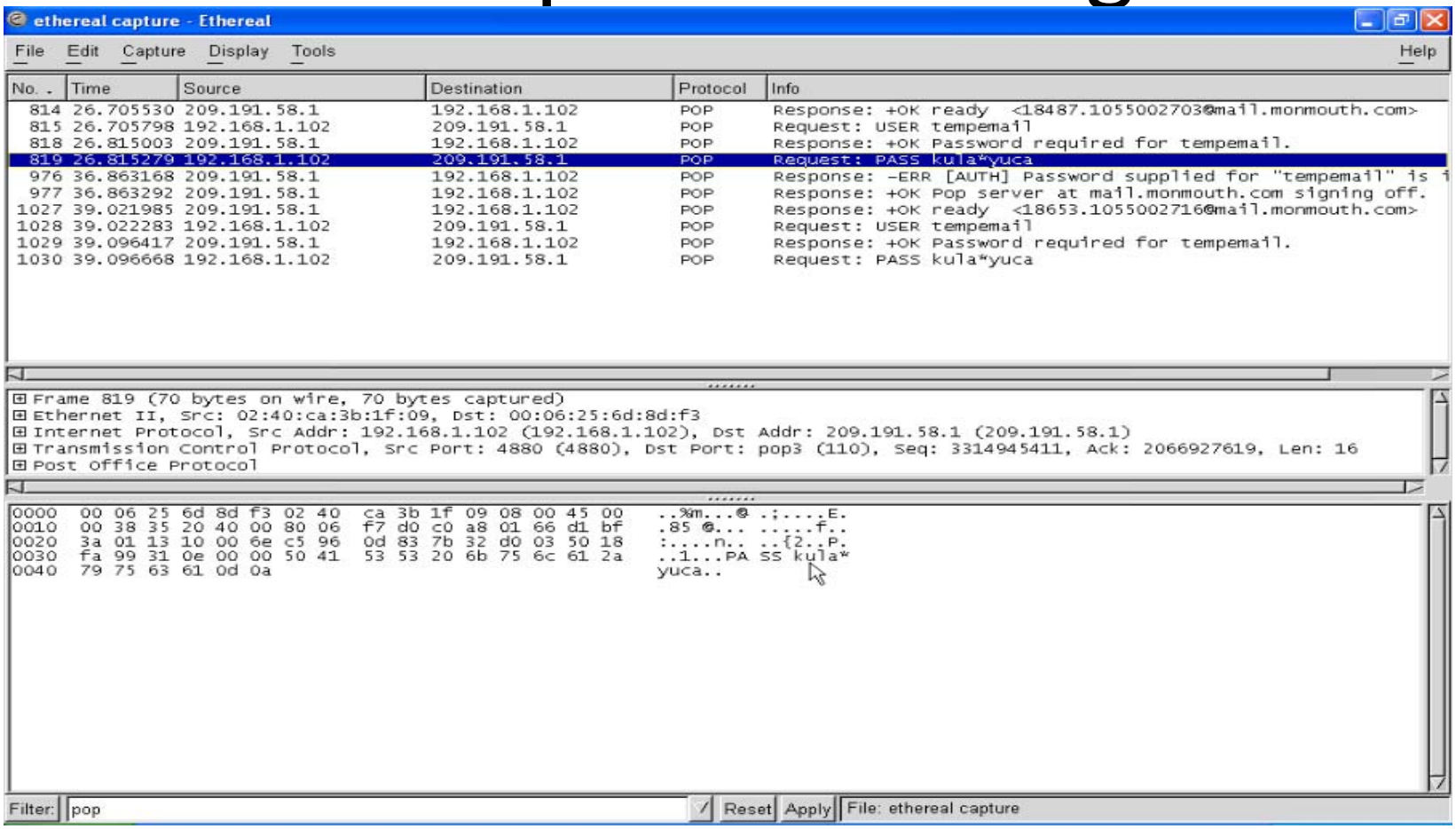
The Investigation: The Search for Fresh Probable Cause

- **Forensic Preservation and Review of several computers on multiple occasions**
- **Review of Phone Logs**
- **Review of Remote Access Logs into Corporate and Computing Network**
- **Surveillance of Subjects: Victim Company Personnel; Outside Agencies.**

The Investigation: The Search for Fresh Probable Cause

- **Installed three hidden wireless fiber optic cameras with remote monitoring capabilities in different locations.**
- **Four Network Sniffers**
  - ✓ **Packet Capturing Software**
  - ✓ **Monitoring five computing devices**
  - ✓ **Remote Connection to Suspect Company Server Discovered**
- **Locate and identify various off-site addresses**
- **Physical Surveillance On and Off-site**

Sample Sniffer Log



"Encrypted" data burned to CD

E·C·I
Economic Crime Institute
UTICA COLLEGE

Further Confirmation

- Possible Venture Capital from New Jersey based networking company
- Joint Venture with a Technology company in China to be considered “The Cisco of China”
- Potential office location of Suspect Company in New Jersey

Additional Investigative Noise

- Potential for hardware and testing equipment currently on Victim Company property to be removed
- Request by group of employees to get Venture Capital through Victim Company to purchase rights to Intellectual Property
- Three Main Subjects; with possibly an additional eleven.
- Greater Employee Focus Leading to Additional Investigations

E·C·I
Economic Crime Institute
UTICA COLLEGE

Potential Revenue Loss

Between $700 Million to $2 Billion

E·C·I
Economic Crime Institute
UTICA COLLEGE

Agenda

1. Presenters' Backgrounds
2. In The News
3. Victim Company: Intellectual Property Investigation
    a. Intellectual Property Defined & Life Cycle
    b. The Investigation Process
4. **Working with Internal Corporate Personnel and Law Enforcement**
5. The Aftermath, and Lessons Learned

E·C·I
Economic Crime Institute
UTICA COLLEGE

Working with Internal Corporate Personnel

- IT and Physical Security Personnel
- Intellectual Property Business Unit President
- Corporate Counsel
- Corporate Officers
- Business Unit Counsel
- Business Unit Human Resources
- Intellectual Property Subject Matter Experts
- Media Relations

E·C·I
Economic Crime Institute
UTICA COLLEGE


CNBC

Working with Law Enforcement

- Local County Prosecutor's Office
- U.S. Attorney's Office, New Jersey
- Federal Bureau of Investigation
- Department of Justice, Washington D.C.

E·C·I
Economic Crime Institute
UTICA COLLEGE

Law Enforcement Actions

- Subpoena of Internet Service Providers
- Subpoena of Suspect Company Internet Hosting Company
- Subpoena of Post Office Boxes and other mail service providers
- Subpoena phone companies

Law Enforcement Efforts Yielded…

- Complete understanding of Suspect Company
- Access Records of Hosting Company
- Encrypted File Space of Suspect Company
- Over 2000 Messages from Yahoo accounts
- Three subjects named their “new” product using the first initial of their last names: CLX1000

E·C·I
Economic Crime Institute
UTICA COLLEGE

Fresh Probable Cause Obtained Through:

- Corporate Remote Access Log
- Government Subpoena of Online Storage Provider

D-Day

- A call from the AUSA: "FBI is ringing door bells, and if no answer, breaking them down!"
- Three simultaneous morning arrests: two residences, one business
- Found within the residences:
  - ✓ Business Plans for Suspect Company and the China-based company
  - ✓ Intellectual Property manuals and components
  - ✓ Running Intellectual Property backplane within a closet

E·C·I
Economic Crime Institute
UTICA COLLEGE

And Then…

- Gave testimony before Federal Grand Jury
- Collected and preserved additional data, and gave to FBI when subpoenaed
- Answered other Government Agencies' questions
- Determined location of backup tapes
- Conducted interviews of additional current and former employees

And Then… (Continued)

- Worked with internal counsel on court filings by partner companies
- Prepared evidence, and company policies to be produced to defense counsel
- Gave testimony on possible violation of wiretapping laws

- Acted on more calls of suspicious behavior
- Length of Activity and Project: 1999 - 2005

E·C·I
Economic Crime Institute
UTICA COLLEGE

Lessons Learned for Corporations

- Actions of any one employee can attract media attention and greatly impact the organization.
- Negative Effect on Stock Price
- Disruptive Work Environment – Negative Impact on Employees

Panel Discussion

Warren G. Kruse II, CISSP, CFCE, DFCP, EnCE
Principal, Booz Allen Hamilton
kruse_warren@bah.com
732-936-3732

George Wade, DFCP, CISSP
Senior Associate, Booz Allen Hamilton
Wade_George@bah.com
732-936-3715

Michael Barba, CISSP, CPP, DFCP, CNE, EnCE
Director, BDO USA LLP
mbarba@bdo.com
212-515-2551

E·C·I
Economic Crime Institute
UTICA COLLEGE