
THE
UNITED STATES
SECRET SERVICE

Secret Service Dual Mission

Protection

- President
- Vice-President
- Former Presidents
- Candidates for POTUS
- Foreign Heads of State
- Others by appointment

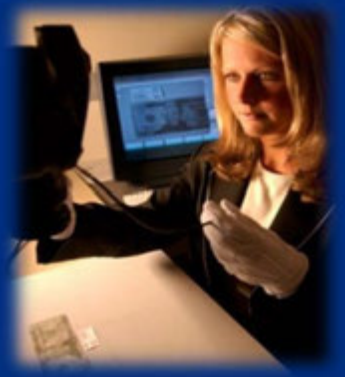
Investigations

- Cyber Crimes
  - Hacking
  - Computer / Internet Fraud
  - Data Breaches
- Counterfeit
  - Currency
  - Treasury Obligations
- Financial Crimes
  - Identity Crime
  - Check Fraud
  - Access Device Fraud
  - Bank Fraud
  - Mortgage Fraud

United States
Secret Service

Secret Service Resources

- 142 Domestic Offices
- 24 Foreign Offices
- 3,500 Special Agents
- 1,400 Uniformed Division Officers
- 2,000 technical, professional and support personnel



United States
Secret Service

Secret Service Resources to Investigate Cyber / Financial Crimes

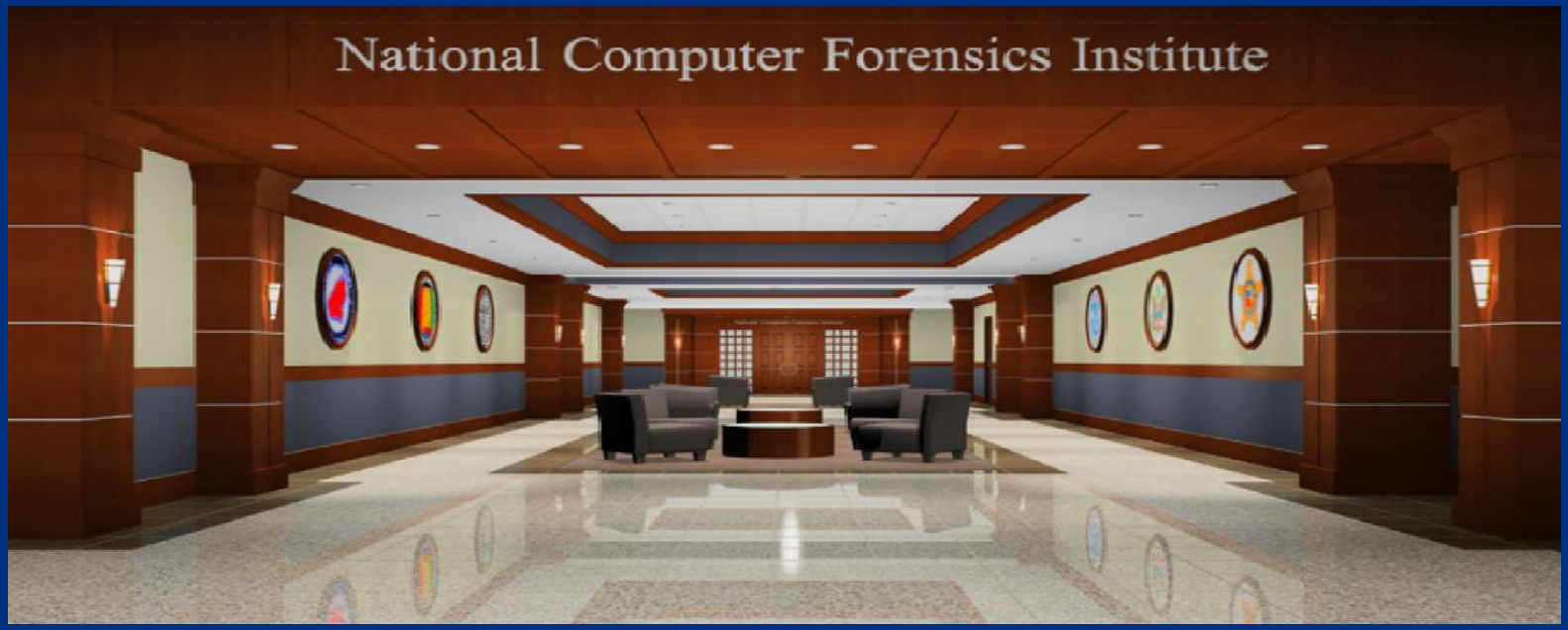
- *Electronic Crimes Special Agent Program (ECSAP)*
- *Electronic Crimes Task Forces (ECTF) - 31*
- *Financial Crimes Task Forces (FCTF) - 38*
- *Cell Phone Forensic Facility – Tulsa, OK*
- *National Computer Forensic Institute (NCFI) – Hoover, AL*
- *Computer Emergency Response Team (CERT)*
- *DOJ/CCIPS(Computer Crimes and Intellectual Property Section)*

Secret Service
Tulsa Initiative

- Partnership with the University of Tulsa, Digital Forensic Center of Information Security
- Expands the forensic capabilities of law enforcement regarding cellular telephones, smart phones and other mobile computing devices
- Tulsa supplies interns who specialize in information technology / digital forensics

United States
Secret Service

National Computer Forensic Institute Hoover, Alabama



The mission of the National Computer Forensic Institute (NCFI) is to provide state and local law enforcement, prosecutors and judicial officials a national standard of training in electronic crimes investigations, network intrusion response, computer forensics and high tech crime prosecution

OFFICE OF INVESTIGATIONS

INTERNATIONAL PROGRAMS DIVISION

United States Secret Service
CYBER ASSET LOCATIONS

Electronic Crimes Task Forces

Not listed: London, England

Rome, Italy

Electronic Crimes Task Force Initiative

A Different Law Enforcement Model for the Information Age

United States
Secret Service

Providing Appropriate Tools Required to Intercept and Obstruct Terrorism

USA PATRIOT ACT OF 2001

HR–3162, 107th Congress, First Session

October 26, 2001

Public Law 107-56

Sec. 105

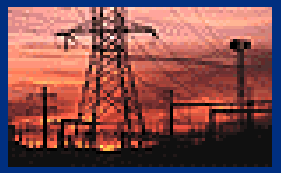
Expansion of National Electronic Crime Task Force Initiative

The Director of the United States Secret Service shall take appropriate actions to develop a national network of electronic crime task forces, based on the New York Electronic Crimes Task Force model, throughout the United States for the purpose of preventing, detecting, and investigating various forms of electronic crimes, including potential terrorist attacks against critical infrastructure and financial payment systems.

Critical Infrastructures

Transportation

Government Services



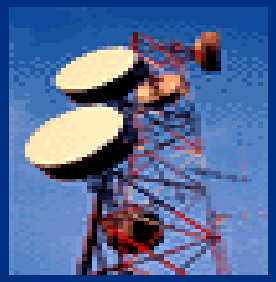
Energy

Water

Public Health

Defense Industrial Base

Emergency Services



Telecommunications

Chemical Industry

Agriculture

Banking and Finance

Postal & Shipping

Food

United States Secret Service

Goals of an Electronic Crimes Task Force

- ✓ Establish a strategic alliance of federal, state and local law enforcement agencies, private sector technical experts, prosecutors, academic institutions and private industry.

- ✓ To confront and suppress technology-based criminal activity that endangers the integrity of our nation's financial payments systems and poses threats against our nation's critical infrastructure.

Electronic Crimes Task Force

Three principles of a successful Electronic Crime Task Force:

- Prevention/Response/Resiliency
- Trusted Partnerships
- Criminal Investigations

Prevention

- The guiding principle of the Electronic Crime Task Force's approach to both our protective and investigative missions is our "focus on prevention".
- "Harden the target" through preparation, education, training and information sharing.
- Proper development of business policies and procedures before the incident.

Response & Resiliency

- Strong documentation and reporting practices starting at the beginning of the incident.
- Internal computer forensics and log analysis.
- Technical briefings for law enforcement during the entire course of the investigation.
- Contingency planning to bring operations back on line.

Trusted Partnerships

- Ongoing Task Force liaison with the business community.
- Business community provides technical expertise and assistance to law enforcement in the rapidly changing technology world.
- Development of business continuity plan, risk management assessment and return on investment.
- Task Force provides “real time” information on issues whenever possible.
- Table Top exercises with private industry and government.

Criminal Investigations

- Liaison and instructions to victims
- Early law enforcement involvement is critical
- “Solve the problem”
- Follow up and ongoing dialogue with the victim

“Cyber Intelligence Section”

U.S. Department of Homeland Security

United States Secret Service

USSS-Cyber Intelligence Section (CIS)

Analysis & Exploitation Unit

Cyber Threat Unit

- **Investigations Group**
- **Transnational Groups**
- **Operations Group**


Belgium


Ukraine


Netherlands


Latvia


UK


Lithuania

United States
Secret Service

Cyber Threat Unit

Investigative Group – responsible for investigating large scale data breaches or other major cyber related cases.

Operations Group – responsible for conducting proactive undercover investigations against major cyber criminals and organized groups.

Transnational Group – Temporary Duty Assignments around the world to liaison and actively work with foreign law enforcement entities.

Cyber Intelligence Section

- Databases of over 15 years worth of cyber evidence:
  - Seized media
  - E-mail search warrants
  - Images of criminal forums/sites
  - Data from when experienced criminals were new
- Combination of agents and analysts.
- Liaison with cyber components of domestic and foreign agencies:
  - US law enforcement and intelligence
  - Foreign law enforcement
  - Private sector research

United States Secret Service

Questions?

Brian Busony

Assistant to the Special Agent in Charge

San Francisco Field Office

Electronic Crimes Task Force

415/273-8504

Brian.Busony@usss.dhs.gov

United States
Secret Service

Data Breach Study

US Secret Service and Verizon Business

- Publication based on real case statistics
  - Law Enforcement Perspective
  - Incident Response Perspective
- Goal
  - Make business decisions based on real data
  - Focus resources on true threat

Summary

WHO IS BEHIND DATA BREACHES?

- **98%** stemmed from external agents (+6%)
- **4%** implicated internal employees (-13%)
- **<1%** committed by business partners (<>)
- **58%** of all data theft tied to activist groups

HOW DO BREACHES OCCUR?

- **81%** utilized some form of hacking (+31%)
- **69%** incorporated malware (+20%)
- **10%** involved physical attacks (-19%)
- **7%** employed social tactics (-4%)
- **5%** resulted from privilege misuse (-12%)

WHAT COMMONALITIES EXIST?

- **79%** of victims were targets of opportunity (-4%)
- **96%** of attacks were not highly difficult (+4%)
- **94%** of all data compromised involved servers (+18%)
- **85%** of breaches took weeks or more to discover (+6%)
- **92%** of incidents were discovered by a third party (+6%)
- **97%** of breaches were avoidable through simple or intermediate controls (+1%)
- **96%** of victims subject to PCI DSS had not achieved compliance (+7%)

2012 Data Breach Investigations Report

- Law Enforcement Participation:
  - USSS
  - Dutch National High Tech Crime Unit (NHTCU)
  - Australian Federal Police (AFP)
  - Irish Reporting & Information Security Service (IRISSCERT)
  - London Metropolitan Police Central e-Crime Unit (PCeU)

- Over **855 new breaches** since the last report
  - Total for all years = 2500+

- Just under **174 million records compromised**
  - Total for all years 2008 -2012= 1.08 Billion

Demographics

Figure 3. Industry groups represented by percent of breaches

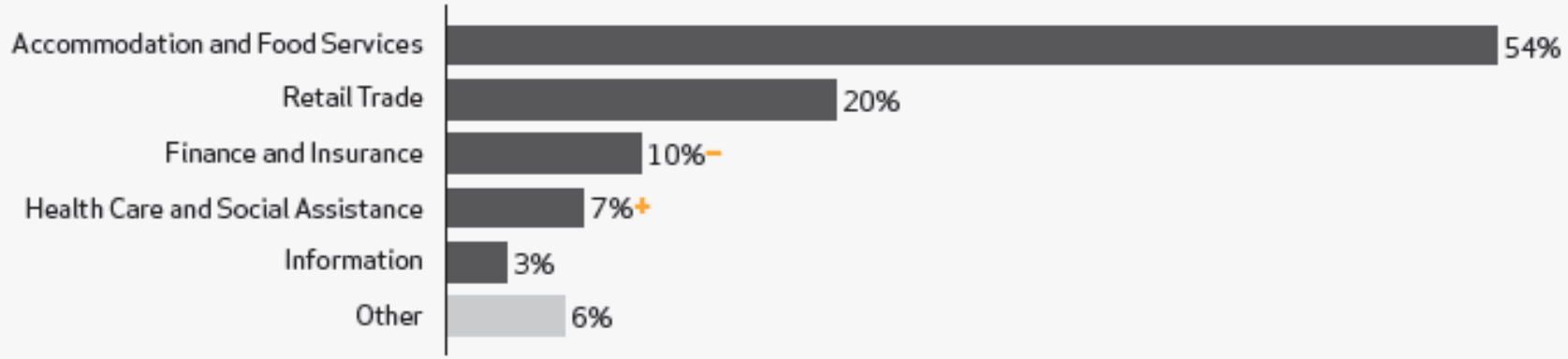
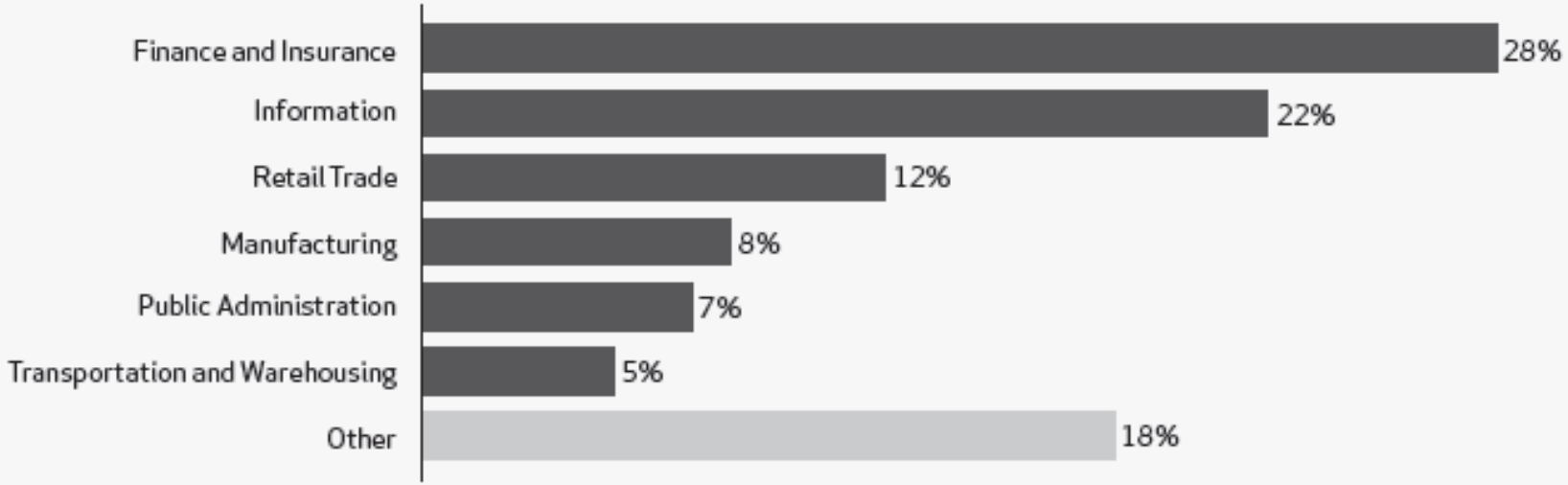


Figure 6. Industry groups represented by percent of breaches – LARGER ORGS



External Agents

Figure 16. Origin of external agents by percent of breaches within External

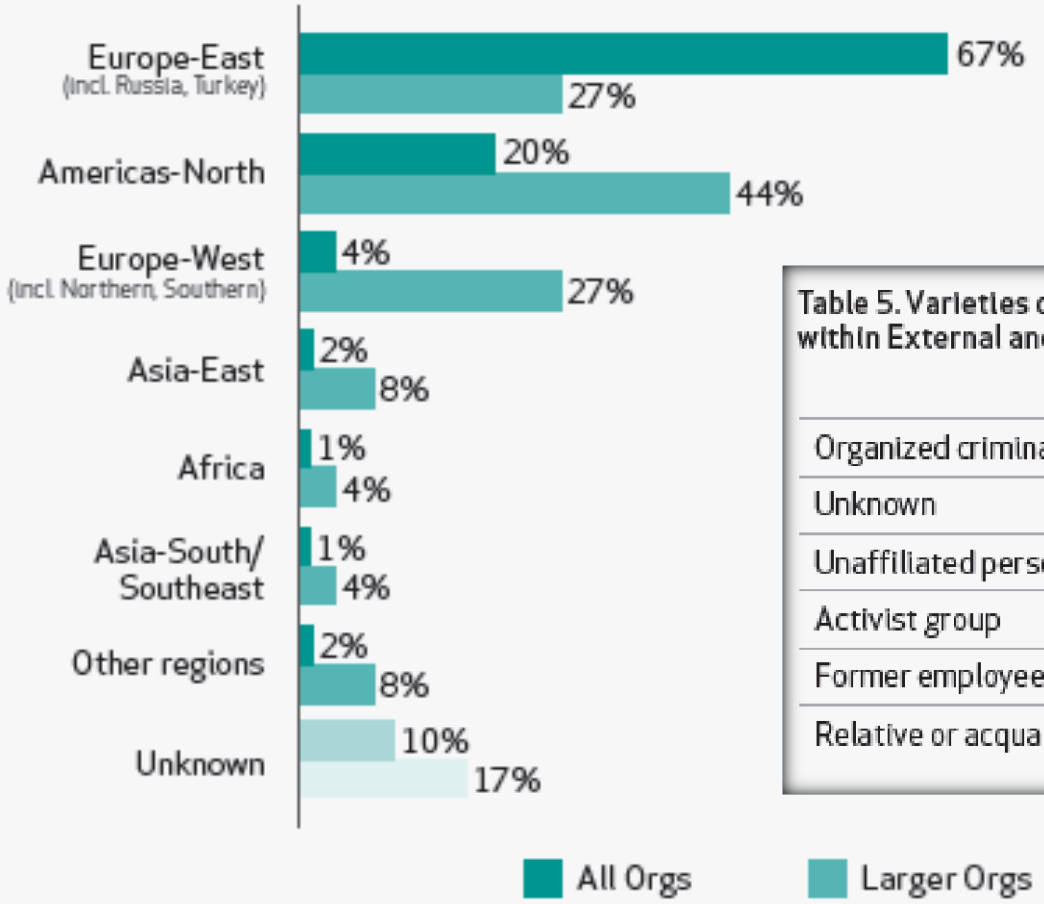


Table 5. Varieties of external agents by percent of breaches within External and percent of records

	All Orgs		Larger Orgs	
Organized criminal group	83%	35%–	33%	36%
Unknown	10%	1%	31%	0%
Unaffiliated person(s)	4%	0%	10%	0%
Activist group	2%	58%+	21%	61%
Former employee (no longer had access)	1%	0%	6%	0%
Relative or acquaintance of employee	0%	0%	2%	0%

Internal Agents

Table 6. Types of Internal agents by percent of breaches within Internal

Cashier/Teller/Waiter	65%
Manager/Supervisor	15%
Regular employee/end-user	12%
Finance/Accounting staff	6%
System/network administrator	6%
Auditor	3%
Executive/Upper Management	3%
Internal system or site	3%
Unknown	3%

We hypothesize that many insider crimes go unreported because the organization is unaware of them, or because they decide for political reasons to handle it internally.

2013 Data Breach Investigative Report

- Due out this spring
- Significant increase of data contributors
- Contains analysis of over 45,000 reported security incidents and 600 confirmed data breaches.

2013 Data Breach Investigative Report Contributors

- US Secret Service
- Australian Federal Police (AFP)
- CERT Insider Threat Center (at Carnegie Mellon University)
- Consortium for Cybersecurity Action
- Danish Ministry of Defence, Center for Cybersecurity
- Danish National Police, National IT Investigation Section (NITES)
- Deloitte
- Dutch Police: National High Tech Crime Unit (NHTCU)
- Electricity Sector Information Sharing and Analysis Center (ES-ISAC)
- European Cyber Crime Center (EC3)
- G-C Partners, LLC
- Guardia Civil (Civil Guard of Spain)
- Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)
- Irish Reporting and Information Security Service (IRISS-CERT)
- Malaysia Computer Emergency Response Team (MyCERT), CyberSecurity Malaysia
- National Cybersecurity and Integration Center (NCCIC)
- ThreatSim
- US Computer Emergency Readiness Team (US-CERT)