The Industrial Security Incident Database

Eric Byres, P.Eng.
Director, Industrial Security
Wurldtech Analytics Inc.
ebyres@wurldtech.com

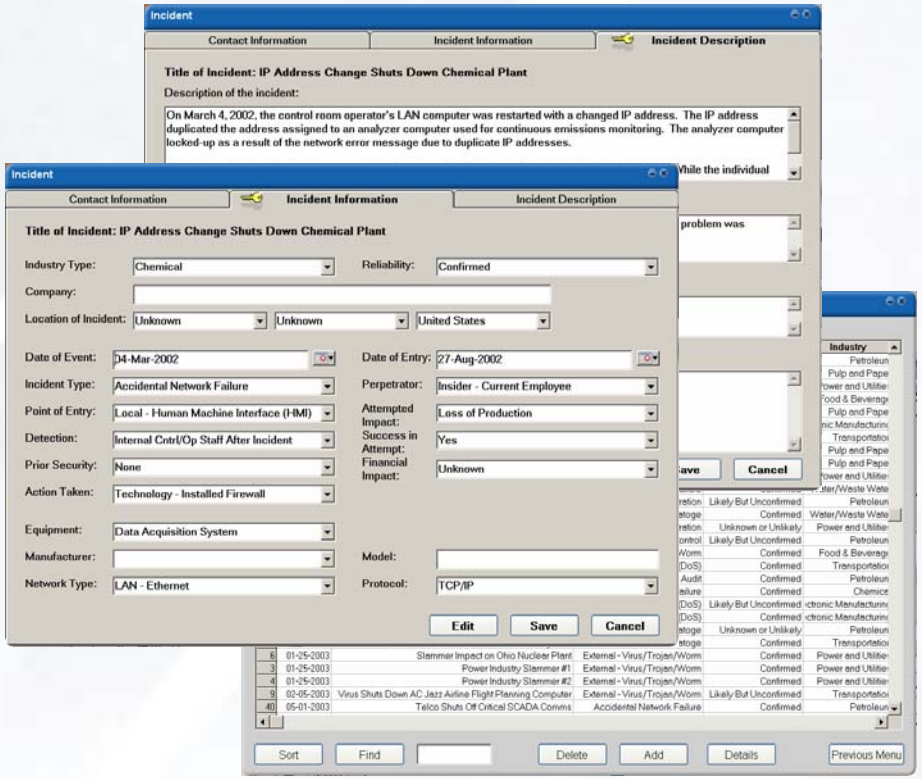
David Leversage
Faculty, Electrical & Computer Engineering Technology
British Columbia Institute of Technology
david.leversage@gmail.com

Summary

- We feel that the ISID database is representative with the goal of becoming part of a statistically significant database sometime in the future.
- The ISID is designed to help its contributors make informed decisions about mitigating actions to get the best bang for their buck.
- The real strength of the ISID is the reliability, and therefore quality, of the incidents in the database – particularly by those contributed by our human sources.
- We follow standard HUMINT (human intelligence) procedures to grow, harvest, and most importantly, protect our sources.

What is the Industrial Security Incident Database (ISID)?

- ISID tracks network cyber incidents that directly impact industrial and SCADA operations.
- Both malicious and accidental incidents are tracked.

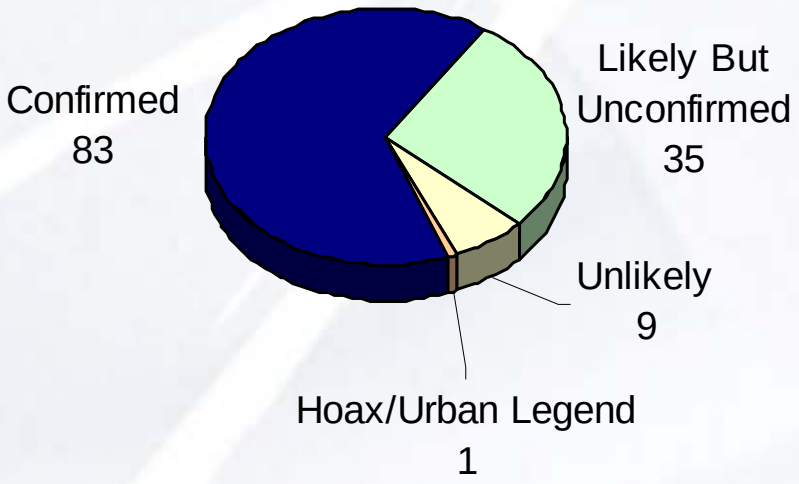


What Data Do We Collect?

- Incident Title
- Date of Incident
- Reliability of Report
  - 1=Confirmed
  - 2=Likely But Unconfirmed
  - 3=Unlikely
  - 4=Hoax/Urban Legend
- Type of Incident (e.g. Accident, Virus, Hacker, etc.)
- Perpetrator
- Industry (e.g. Petroleum, Pulp, Automotive, etc.)
- Entry Point
- Method of Detection
- Brief Description
- Impact on Company
- References

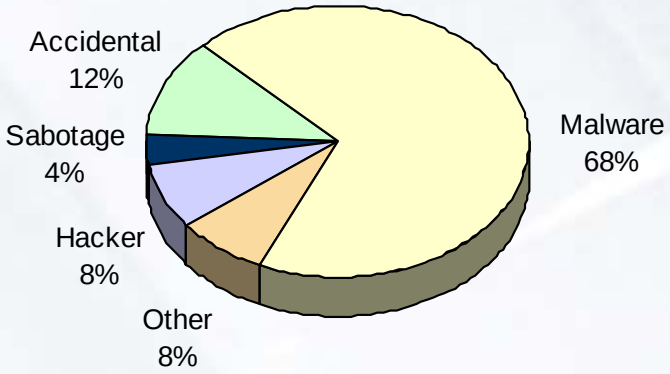
Spring 2006 ISID Status

- 135 Incidents (7 Pending)
- 10 to 15 New incidents are being added to the ISID quarterly
- 22 Contributor companies from:
  - USA, Canada, UK, France and Australia
  - Oil/Gas, Chemical, Power, Food, Water…

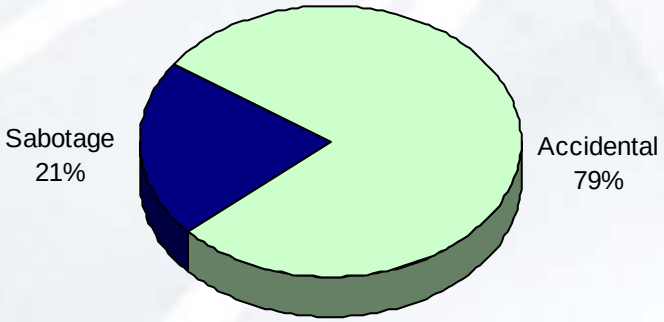


Selected Stats: Financial Impact

- Targets of choice risk greater financial impacts than targets of opportunity
- Accidental breaches also have surprisingly high financial impacts



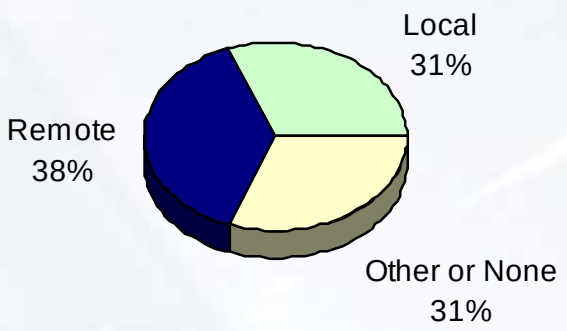
Financial Impact < $100,000



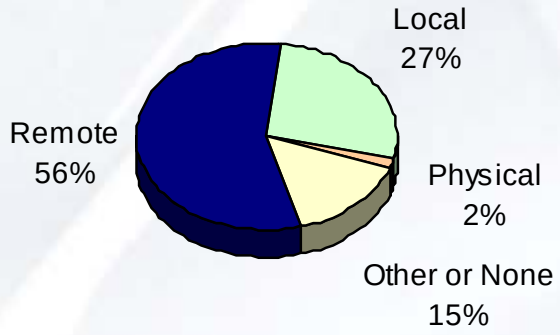
Financial Impact > $100,000

More Selected Stats: Entry Point

- Entry changed significantly after 2001
- Major contributors
  - Deployment of commercial off-the-shelf technology
  - Direct or indirect connections to the Internet



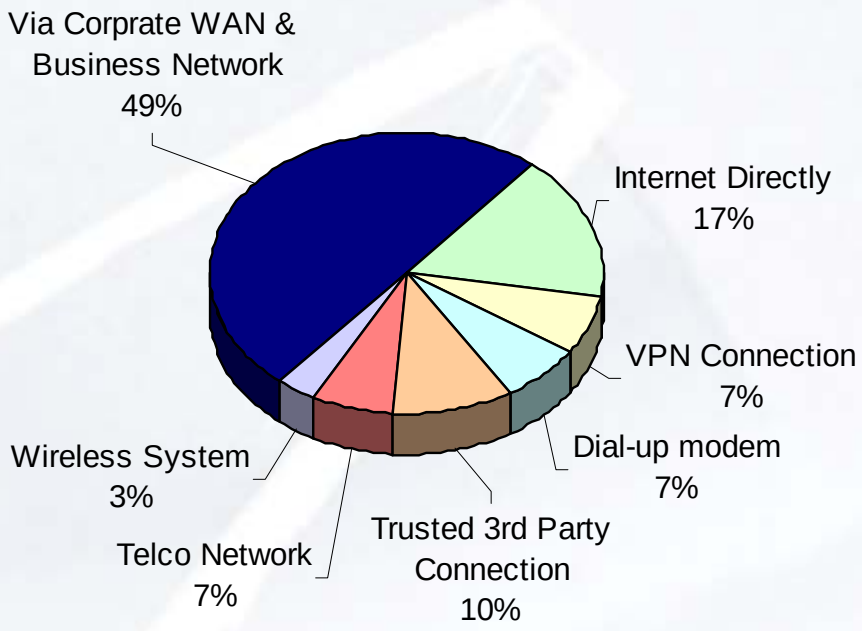
Entry Point Before Jan 2002



Entry Point After Jan 2002

Remote Entry Point

- Connections of particular concern:
  - Corporate WANs & Business Networks
  - The Internet Direct
  - Trusted Third Parties
- On the rise:
  - Infected laptops transferring malicious code when connected directly or indirectly (via VPN) into the PCN



Human Sources:
Our Key to Strong Intelligence

- Our most valuable resource are our human sources
- Human sources provide the highest quality intelligence product
- We have ZERO LEAK TOLERANCE!
  - All reporting is strictly confidential
  - All submitted incident submission forms are carefully scrubbed to remove identifying and sensitive information
  - The ISID is not on the Internet

Handlers & Human Intelligence (HUMINT)

- It takes time and experience to build strong trusted relationships with human sources
- We use tried and proven HUMINT handling techniques, the same techniques that are used by the intelligence community, to manage our human sources
- Our combined experience includes:
  - 7 years handling human sources
  - 8 years industrial cyber security
  - 8 years intelligence service

Sharing Incident Data

- Contributing Members
  - SCADA/Industrial System operators that are actively contributing members
- Strategic Partners
  - A special two-way sharing agreement where both sides contribute significantly to a common database
- Analysis Reports
  - Statistical analysis reports of data in the database

Coming Soon …

Quarterly Reports

- A response to a growing demand for relevant statistical data by corporations and educational institutions that do not fit into any of the previous options
- Subscriptions will be on a per report or annual basis

ISID Needs You to Help us Get The Word Out to Industry

- Industry needs current and relevant statistical data to make intelligent choices.
- We encourage you to:
  - Report any SCADA related incident to ISID.
  - Spread the word and encourage others to contribute to ISID.
- ISID is truly international in scope.

Reporting to ISID

- You and your company's identity remains completely confidential. It will not be shared with any legal or government entities.
- You will get database access and special analysis reports in advance.

Reporting to ISID

- Two ways to contribute:
  - Down load a reporting form (editable PDF) from: http://www.wurldtech.com
  - Contact the Manager of ISID:

David Leversage
Faculty, Electrical & Computer Engineering Technology
British Columbia Institute of Technology
Phone: 604-412-7593
Email: david.leversage@gmail.com
PGP Public Key available upon email request

Questions?