What Went Wrong?

A Study of Actual Industrial Cyber Security Incidents

Zach Tudor

Mark Fabro

SRI International

RISI Advisory Panel Member

SCADA Security is Making Headlines

A excess of rumour and a shortage of facts

Separating Fact from Fiction

How much of what is reported is real versus hype?

Need a realistic assessment of the risks to our critical infrastructures:

- What is fact and what is urban myth?
- How urgent is the security risk?
- What vulnerabilities are exploited?
- What are the threat sources?
- How serious are the effects?

What is RISI?

- Database of incidents of a cyber security nature that directly affect industrial Supervisory Control and Data Acquisition (SCADA) and process control systems
- Includes accidental cyber-related incidents, as well deliberate events such as external hacks, Denial of Service (DoS) attacks, and virus/worm infiltrations
- Data is collected through research into publicly known incidents and from private reporting
- Includes expert analysis and commentary on lessons learned and recommended mitigation techniques

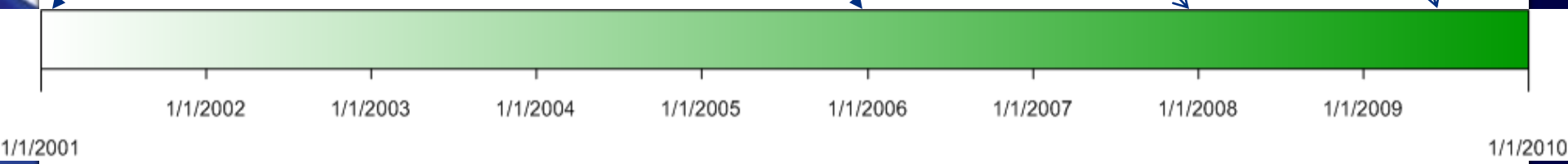
History

Industrial Security Incidents Database (ISID) developed through academic research project at the British Columbia Institute of Technology (BCIT).

ISID was discontinued in 2006. Byres Research acquired the rights to ISID from inventors

Project initiated to develop the Repository of Industrial Security Incidents (RISI) using ISID data plus incidents collected since 2006

Exida acquired Byres Research and created the Security Incidents Organization™, a 501c(3) non-profit, to operate and maintain RISI



The Security Incidents Organization™

- The Security Incidents Organization is a 501(c)(3) non-profit company that operates the Repository of Industrial Security Incidents (RISI)
- Funding for operating The Security Incidents Organization is provided by private membership dues

Value

- Identify common factors contributing to incidents, such affected equipment, entry point, type of incident, impact, etc. to prevent future incidents
- Sharing of lessons learned through historical data
- Provide an industry benchmark for continuous improvement
- Provide statistics for business cases that security managers must write to get funding

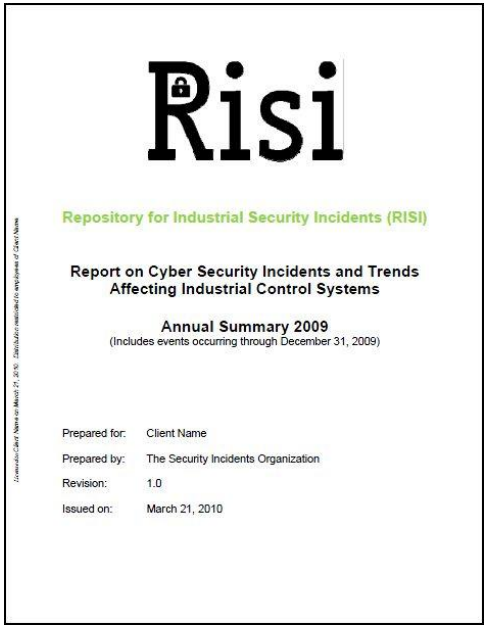
Type of Data Collected

- 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, Outside Hack, Virus, etc.)

- Industry (e.g. Petroleum, Pulp, Automotive, etc.)
- Entry Point
- Perpetrator
- Brief Description
- Impact on Company
- References
- And more…

Highlights from Annual Report

- Issued quarterly
- Most recent report issued 22 Mar 2010
- 161 incidents (confirmed or likely)
- Averaging about 10 new incidents per quarter
- Only confirmed or likely incidents are included in the report


Risi

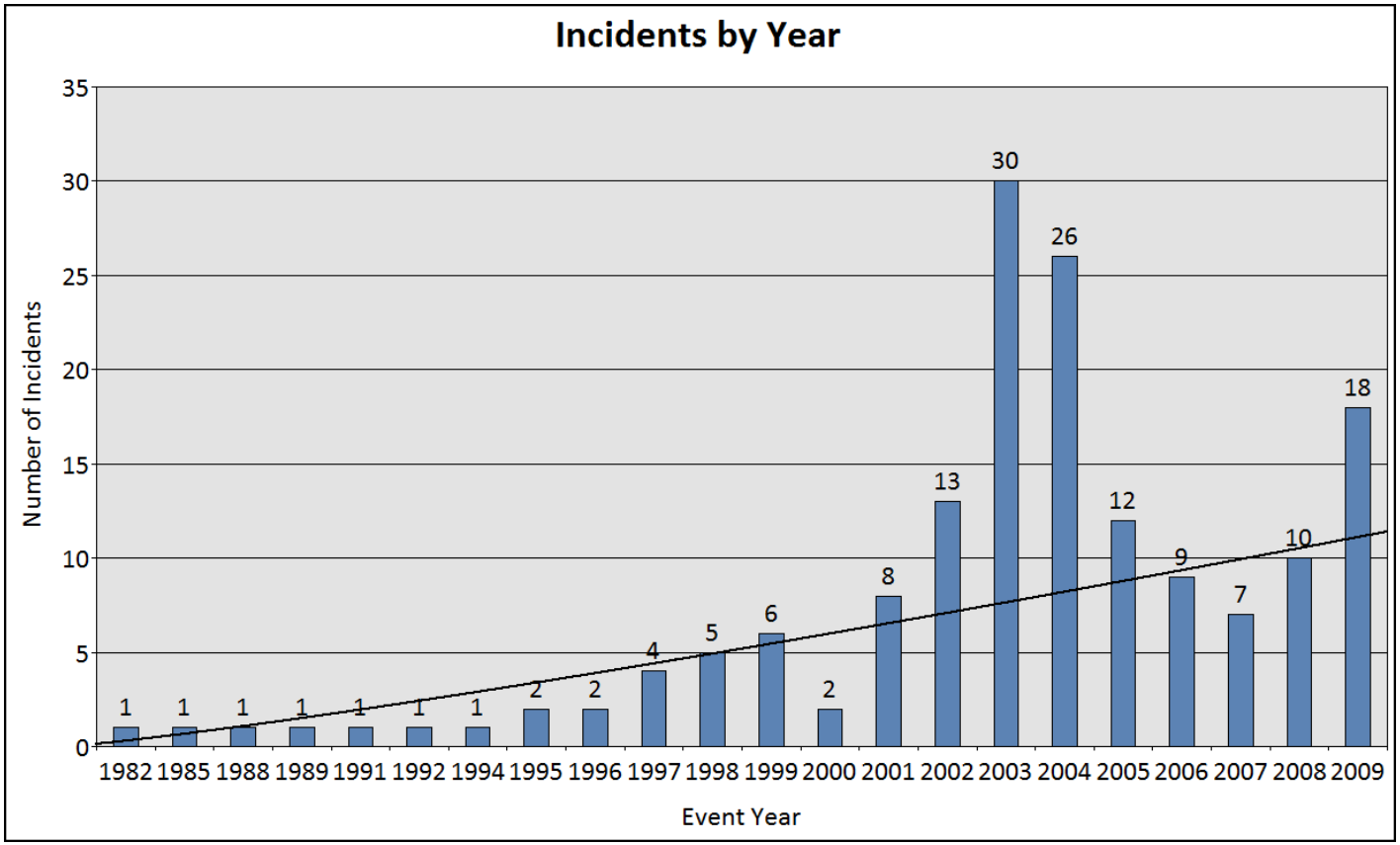
Repository for Industrial Security Incidents (RISI)

Report on Cyber Security Incidents and Trends Affecting Industrial Control Systems

Annual Summary 2009
(Includes events occurring through December 31, 2009)

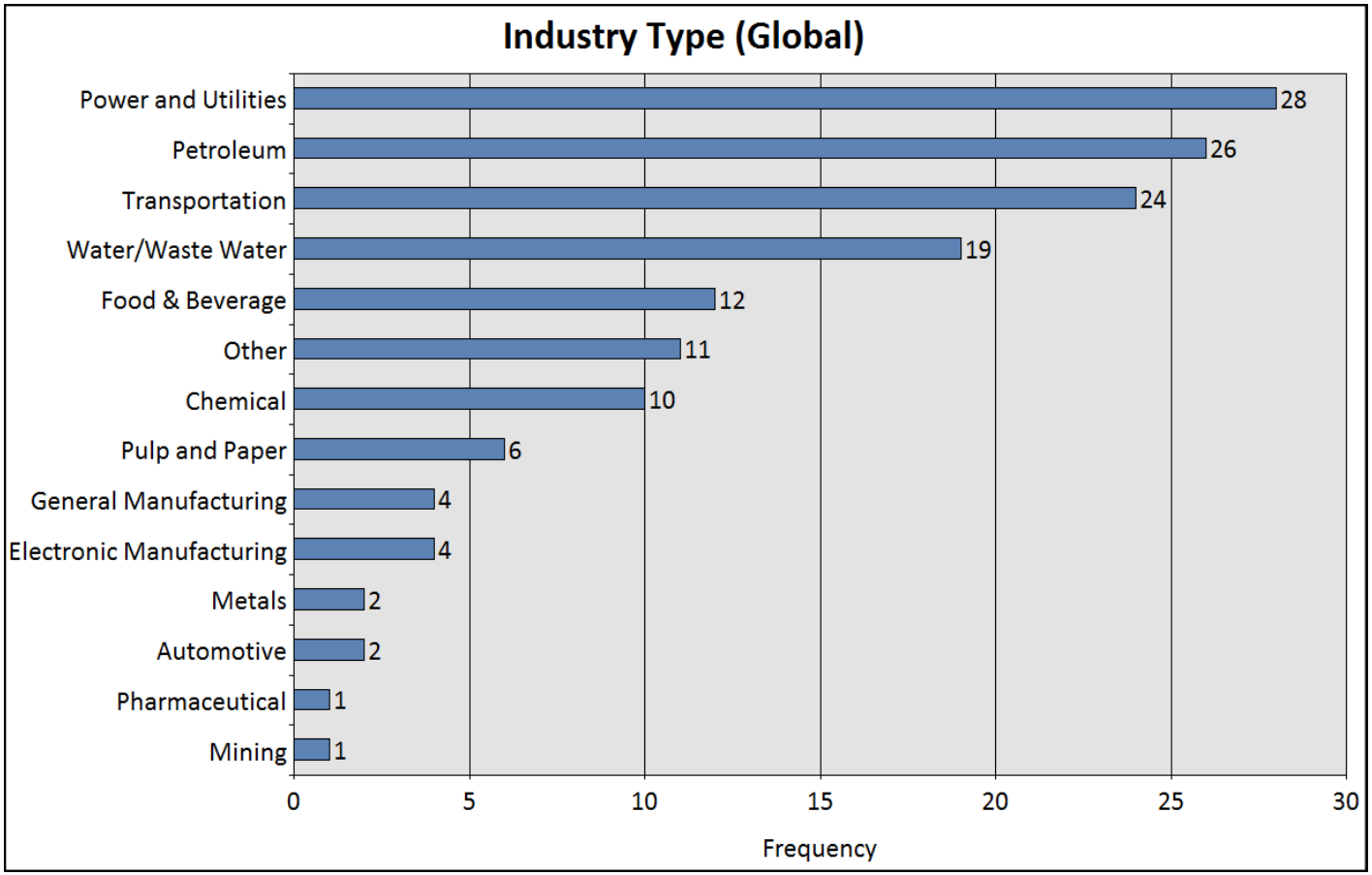
Prepared for: Client Name
Prepared by: The Security Incidents Organization
Revision: 1.0
Issued on: March 21, 2010

Time will tell



The number of Industrial cybersecurity incidents has remained stable but is expected to rise based on recent reporting rates.

Who is getting attacked?

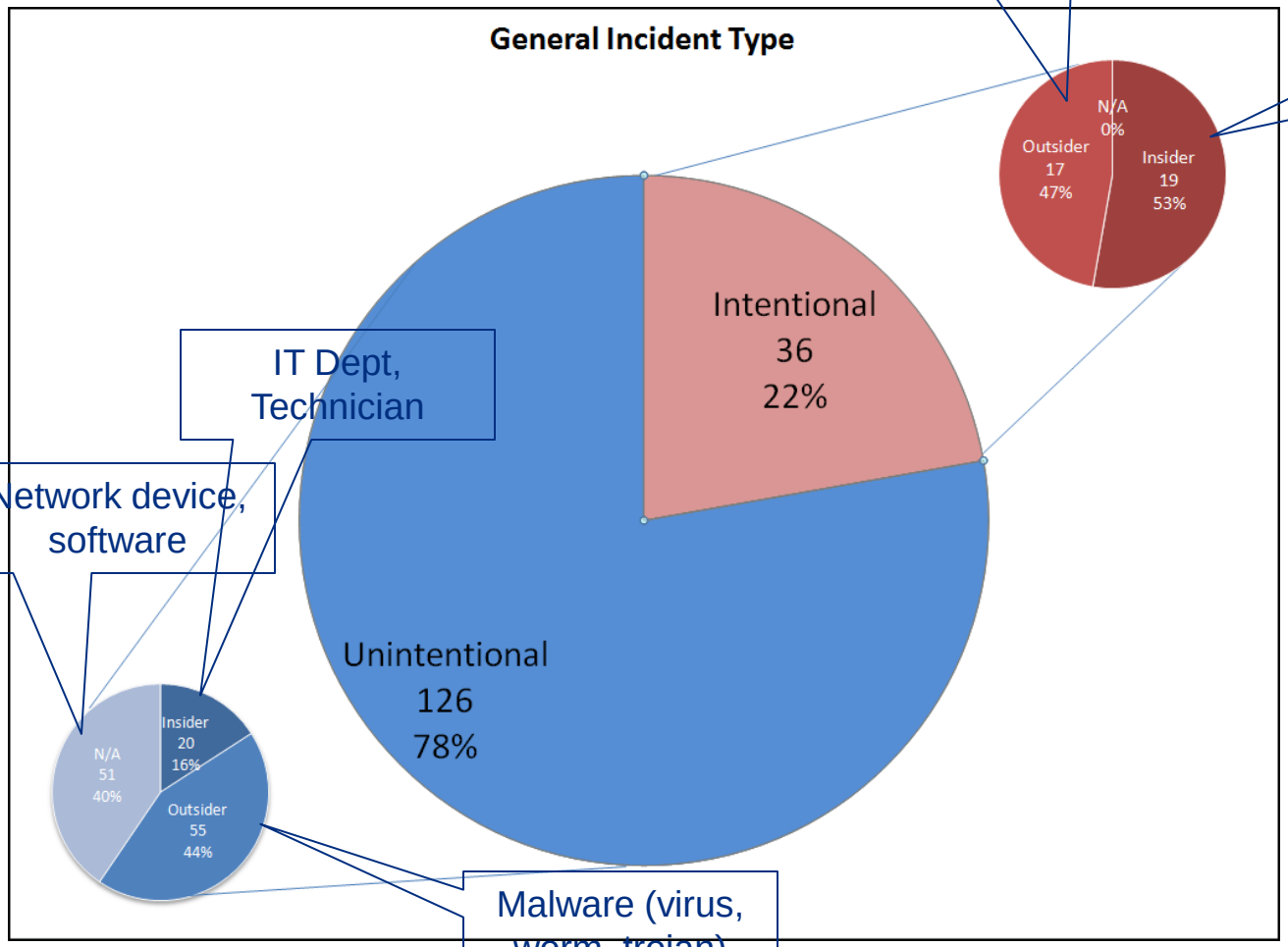


Power and Utilities, Petroleum and Transportation industries experience the majority of cybersecurity incidents

How has it changed?

Industry Type	2000-2004	2005-2009	% Change
Water/Waste Water	3	14	367%
Power and Utilities	10	13	30%
Transportation	10	10	0
Food & Beverage	5	3	-40%
Petroleum	19	3	-84%
Chemical	8	1	-88%

Incident Types



Hacker

Disgruntled employee

IT Dept, Technician

Network device, software

Malware (virus, worm, trojan)

Malware accounts for most of the unintentional attacks. However, the remaining 22% are some form of targeted attack

What incident types are on the rise?

Incident Type	2000-2004	2005-2009	% Change
Accidental Software Failure	2	8	300%
External - System Penetration	3	9	200%
Internal - Sabotage	2	6	200%
Control/SCADA System Failure	12	17	42%
Accidental Inappropriate Control	5	4	-20%
Accidental Incident	2	1	-50%
External - Sabotage	4	2	-50%
External - Virus/Trojan/Worm	41	7	-83%
Accidental Network Failure	6	1	-83%
External - Denial of Service (DoS)	3	0	-100%
Internal - Non-Authorized Access	0	3	N/A

Accidental Equipment Failure is proving to be on the rise in the past 5 years.

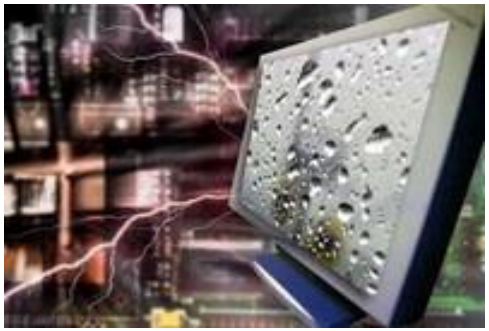
Example incidents

Risi

The Repository of Industrial Security Incidents
www.securityincidents.org

Hackers Penetrate Water System Computers

Date:	October 2006
Company:	Harrisburg Water System
Location:	Harrisburg, PA, USA
Industry:	Water & Wastewater
Incident Type:	Intentional - External - Hacker
Impact:	Unknown



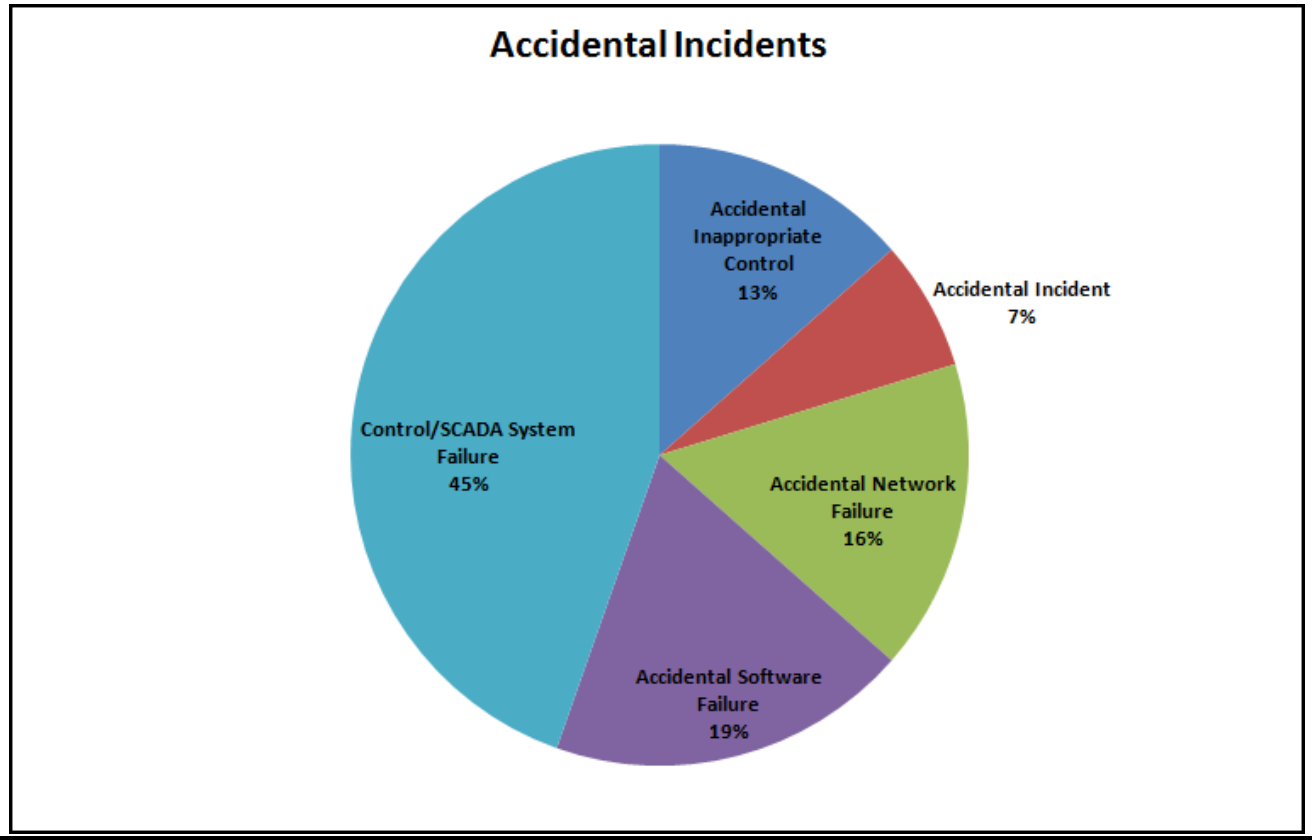
Description:

A foreign-based hacker used the internet to infiltrate the laptop (via internet) of an employee at the Harrisburg water system. The hacker used the employee's remote access as the entry point into the SCADA system and installed malware and spyware on a SCADA HMI computer.

Source: The Repository of Industrial Security Incidents (www.securityincidents.org)

Accidents happen

- Accidental cyber incidents account for 44% of all incidents reported in RISI.
- Consequences can range from nuisance to catastrophe.



Example Accidental Incident

Risi The Repository of Industrial Security Incidents

www.securityincidents.org

INCIDENT ID#: 112

TITLE: Ping Sweep Causes PCS System to Hang

DATE of EVENT: 9/1/1998

DESCRIPTION:

On a PCS network, a ping sweep was being performed to identify all hosts that were attached to the network, for inventory purposes, and it caused a system controlling the creation of integrated circuits in the fabrication plant to hang.

IMPACT:

The destruction of $50K worth of wafers.

FOLLOW-UP WORK:

Unknown.

Example Incidents

Risi

The Repository of Industrial Security Incidents
www.securityincidents.org

Browns Ferry Nuclear Plant Scrammed

Date:	Aug. 2006
Company:	Browns Ferry Nuclear
Location:	Athens, AL, USA
Industry:	Nuclear Power
Incident Type:	Accidental Equipment Failure
Impact:	Unit #3 shutdown

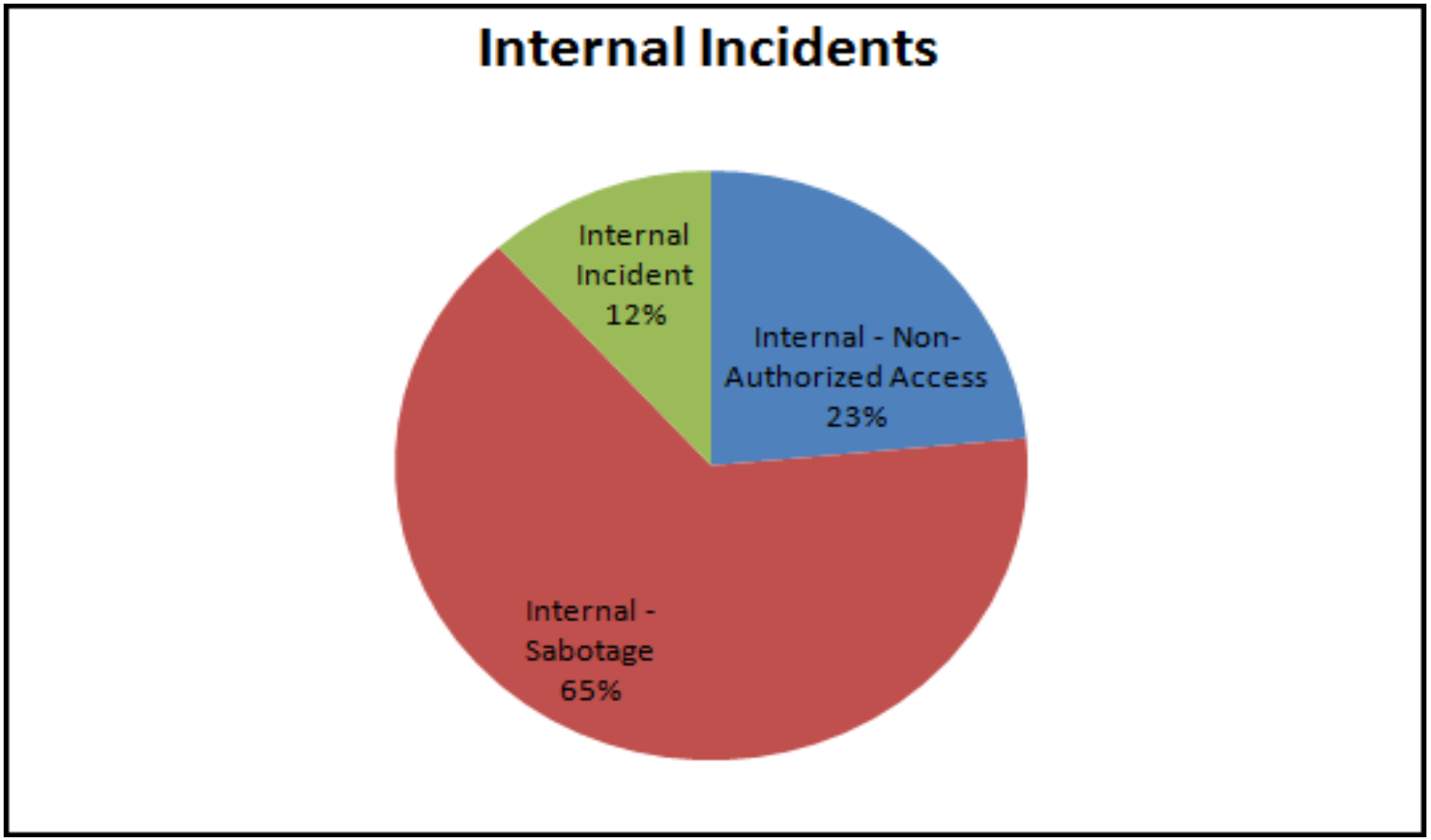
Description:

Operators manually scrammed Browns Ferry, Unit 3, following a loss of both the 3A and 3B reactor recirculationpumps. The root cause was the malfunction of the VFD controller due to excessive traffic on the plant Ethernet based integrated computer system (ICS) network.

Source: The Repository of Industrial Security Incidents (www.securityincidents.org)

Keep your friends close…

Internal attacks account for 12% of reported incidents



Example incidents

Risi

The Repository of Industrial Security Incidents
www.securityincidents.org

Disgruntled Contractor Disables Pipeline Leak Detection System

Date:	March 2009
Company:	Pacific Energy Resources Ltd.
Location:	Long Beach, CA, USA
Industry:	Petroleum
Incident Type:	External Hacker
Impact:	Leak Detection System Disabled

Description:
A disgruntled employee, Mario Azar, accessed the system that monitors the detection of pipeline leaks for three oil derricks off the Southern California coast. He knowingly temporarily disabled the system.

The FBI announced that, on September 14, 2009, Mario Azar pleaded guilty to intentionally damaging a computer system used in interstate and foreign commerce and faced ten years in prison. His sentencing is scheduled for December 7 in the United States District Court of Los Angeles.

Source: The Repository of Industrial Security Incidents (www.securityincidents.org)

Reporting to RISI

You and your company's identity remains completely confidential. It will not be shared with any legal or government entities.

How to submit:

- Download a reporting form (editable PDF) from: http://www.securityincidents.org/register.asp
- Email to submit@securityincidents.org (PGP key available)
- Fax paper form to: 215-257-1657

You will get free membership for 3 months