

# Risi

Repository for Industrial Security Incidents (RISI)

## Quarterly Report on Cyber Security Incidents and Trends Affecting Industrial Control Systems

**3rd Quarter 2009**

(Includes events occurring through 30 September 2009)

Prepared for: Client Company

Prepared by: Security Incidents Organization

Revision: 1.0

Issued on: November 30, 2009

### Executive Summary

Eleven (11) new incidents were added to the RISI database during the third quarter of 2009 raising the total number of incidents in the database from 153 to 164. To date, 35 incidents have been added to the database in 2009, many of which occurred prior to 2009. If incident collection and reporting continue at this rate one can expect that approximately 48 new records will be added in 2009, representing a 37% increase in the total number of incidents in the database.

To date, all incidents added in 2009 have received a reliability rating of either “Confirmed” or “Likely, but unconfirmed”.

### Incident Rates

Incident rates appear to be on the rise again following a decline in the mid-2000’s. A gradual increase can be observed in the incident rate in the late 90’s followed by a spike in the early 2000’s which peaked around 2003. The annual incident rate then declined sharply in the mid 2000’s (2005 – 2007) but appears to be on the rise again in the late 2000’s.

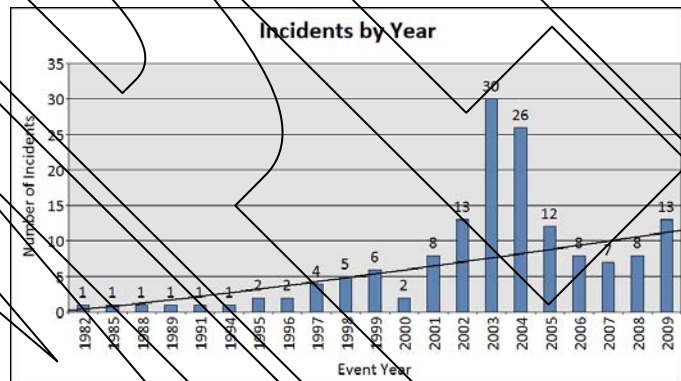


Figure 2.2-1: Incidents by Year

It has been noted that the dip in the mid-2000’s is at least partially attributable to the fact that work on RISI was suspended between 2006 and 2008.

Refer to Section 2.2: *Incidents Over Time* for details.

### Affected Industries

A significant shift has been observed in the incident rates by industry over the last 10 years. There was a decline in the incident rate in the Petroleum and Chemical industries but an increase in the incident rate in the Water & Waste/Water, Power & Utilities and Food & Beverage industries. Details of this observation can be found in Section 2.3 *Industry Type*.

Industry Type	1999-2003	2004-2008	% Change
Petroleum	18	5	-72%
Transportation	8	6	-25%
Chemical	5	4	-20%
Power and Utilities	10	12	20%
Water/Waste Water	4	8	100%
Food & Beverage	3	6	100%

Table 2.3-2: Industry Type by Time Period

While there is not sufficient data to determine the absolute reason for this shift, one possible explanation is that the industries with a declining incident rate have been more proactive in addressing control system cyber security than the industries with an increasing incident rate. This explanation is further supported by the fact that DCS system suppliers, that predominantly supply the industries

with declining incident rates, have also been more proactive in addressing control system cyber security than the PLC and SCADA system suppliers, who primarily supply the industries with increasing incident rates.

### Incident Types and Pathways

Regardless of whether one is looking at global data or just the US, most incidents have been caused by malware (viruses, worms, trojans, etc.). This fact has remained relatively constant over time as well underscoring the need for operators of industrial automation and control system equipment to be more diligent in installing and maintaining good virus protection, especially on their PC based control system equipment.

With the exception of malware, there has been a decline in the number of incidents perpetrated by external sources. Incidents involving external sabotage, denial of service and system penetration are remarkably down in the last five years (2004 to 2008) when compared to the previous 5 year interval (1999 to 2003).

On the contrary, incidents involving unauthorized access or sabotage perpetrated by internal sources, such as a disgruntled former employee or contractor who uses inside knowledge or access privileges cause to harm to the company, are up considerably in the same time period comparison. These incidents also tend to have the greatest impact both financially as well as in lost operation/production. These incidents provide valuable insight into the potential damage that can be caused by a deliberate cyber attack even though they are always focused on causing financial damage to a company and not intended to cause injury or harm. While they are probably the most difficult to prevent there are countermeasures employers can put in place to minimize the probability of these accidents from occurring.

Incident Type	1999 - 2003	2004 - 2008	Percent Change
External - Sabotage	5	0	-100%
External - Denial of Service (DoS)	3	0	-100%
External - System Penetration	6	4	-33%
External - Virus/Trojan/Worm	25	24	-4%
Accidental Incident	2	2	0%
Accidental Equipment Failure	8	10	25%
Accidental Network Failure	4	5	25%
Accidental Inappropriate Control	4	5	25%
Internal - Sabotage	2	3	50%
Accidental Software Failure	2	6	200%
Internal - Non-Authorized Access	0	4	N/A
Internal Incident	0	1	N/A

Table 2.4-2: Incident Type by Time Period

Also on the rise are incidents involving accidental hardware, software and network failures as well as accidental inappropriate control. These are cases where failure of a piece of equipment caused widespread network failure or cases where “unusual” network traffic, such as network scans, induced failures in control system equipment. These types of incidents highlight the need for improvements in network design and network robustness testing. Proper application of Zone & Conduit modeling, as recommended in ANSI/ISA S99.01.01, can help limit the propagation of network failures. Furthermore, network robustness testing will result in equipment that is far more tolerant of network disturbances that can lead to equipment failure.

The conclusion that can be drawn from this data is that the biggest threats to industrial control system security are malware, insider actors and accidental failures. The good news is that countermeasures to strengthen systems against these threats will also serve to strengthen systems against external actors, should that threat increase in the future.

### Impact of Incidents

Incidents can have a variety of outcomes. Some are merely a nuisance while others may result in harm to people, the environment or result in a significant financial loss for the affected company.

This report takes an in-depth look at the attempted results versus the achieved results, the financial impact of these incidents and the amount of lost production.

Of particular interest are those incidents that resulted in significant harm, regardless of the attempted outcome.

Currently there are 132 incidents in the database that have resulted in significant harm. This figure is startling considering only 22 of these 132 incidents, or 17%, were perpetrated by individuals actually intending to cause harm. In fact, there are several incidents whereby a deliberate attack actually caused more harm than was intended by the attacker.

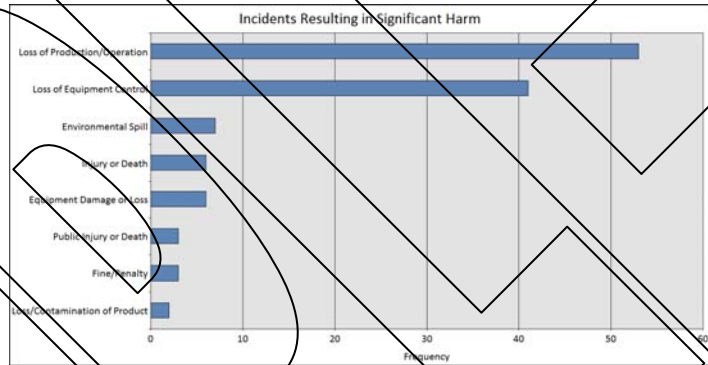


Figure 2.8-7: Incidents Resulting in Significant Harm

This indicates that users of control systems need to be concerned about more than just intentional attacks.

Unintentional incidents (accidents, equipment failure and malware) actually account for a significant number of harmful events.

# Table of Contents

**EXECUTIVE SUMMARY .....II**

    INCIDENT RATES ..... II

    AFFECTED INDUSTRIES ..... II

    INCIDENT TYPES AND PATHWAYS ..... III

    IMPACT OF INCIDENTS ..... IV

**1 INTRODUCTION ..... 1**

    1.1 STRUCTURE OF THE REPORT ..... 1

    1.2 UPDATES IN THIS REPORT ..... 1

    1.3 DATA ENTRY ..... 2

**2 DATA ANALYSIS ..... 3**

    2.1 EVENT LOCATIONS ..... 3

    2.2 INCIDENTS OVER TIME ..... 5

    2.3 INDUSTRY TYPE ..... 7

        2.3.1 *Incidents by Industry Type and Geography* ..... 8

        2.3.2 *Industry Type by Time Period* ..... 10

    2.4 INCIDENT TYPE ..... 11

        2.4.1 *General Incident Classification* ..... 12

        2.4.2 *Specific Incident Classification* ..... 13

        2.4.3 *Incident Type by Time Period* ..... 15

    2.5 PERPETRATOR TYPE AND DETECTION METHOD ..... 16

        2.5.1 *Perpetrator Type* ..... 16

        2.5.2 *Detection Method* ..... 18

    2.6 METHOD AND POINT OF ENTRY ..... 20

    2.7 EQUIPMENT INVOLVED AND PROTOCOLS ..... 24

        2.7.1 *Equipment Involved* ..... 24

        2.7.2 *Protocols involved* ..... 25

    2.8 RESULTS ..... 27

        2.8.1 *Attempted Results* ..... 28

        2.8.2 *Achieved Results* ..... 29

        2.8.3 *Attempted versus Achieved Results* ..... 31

        2.8.4 *Incidents Resulting in Significant Harm* ..... 32

        2.8.5 *Incident Result by Time Period* ..... 33

    2.9 FINANCIAL IMPACT ..... 34

        2.9.1 *Financial Impact by Geography* ..... 34

2.9.2	<i>Financial Impact by Industry</i> .....	37
2.10	OPERATION AND PRODUCTION IMPACT.....	38
<b>3</b>	<b>RECENT INCIDENTS</b> .....	<b>42</b>
3.1	SUMMARY OF MOST RECENT INCIDENTS .....	42
3.2	DETAILS OF MOST RECENT INCIDENTS .....	43
3.2.1	<i>INCIDENT ID#: 155</i> .....	43
3.2.2	<i>INCIDENT ID#: 156</i> .....	44
3.2.3	<i>INCIDENT ID#: 157</i> .....	44
3.2.4	<i>INCIDENT ID#: 158</i> .....	45
3.2.5	<i>INCIDENT ID#: 159</i> .....	45
3.2.6	<i>INCIDENT ID#: 160</i> .....	46
3.2.7	<i>INCIDENT ID#: 161</i> .....	46
3.2.8	<i>INCIDENT ID#: 162</i> .....	47
3.2.9	<i>INCIDENT ID#: 163</i> .....	47
3.2.10	<i>INCIDENT ID#: 164</i> .....	48
3.2.11	<i>INCIDENT ID#: 165</i> .....	49
<b>4</b>	<b>LOOKING AHEAD</b> .....	<b>50</b>
<b>5</b>	<b>CONTRIBUTORS</b> .....	<b>51</b>
<b>6</b>	<b>REVISION HISTORY</b> .....	<b>52</b>

### Table of Figures

Figure 2.1-1: Incidents by World Region .....	3
Figure 2.1-2: Incidents by Country .....	4
Figure 2.2-1: Incidents by Year .....	5
Figure 2.2-2: Number of Incidents Occurring Globally (5 Year Intervals).....	6
Figure 2.2-3: Number of Incidents occurring in the US (in 5 year intervals).....	7
Figure 2.3-1: Incidents by Industry Type (Global).....	9
Figure 2.3-2: Incidents by Industry Type (USA).....	10
Figure 2.4-1: Incidents Categorized by General Incident Type (Global) .....	12
Figure 2.4-2: Incidents Categorized by General Incident Type (USA) .....	13
Figure 2.4-3: Incidents Categorized by Specific Incident Type (Global).....	14
Figure 2.4-4: Incidents Categorized by Specific Incident Type (USA).....	14
Figure 2.5-1: Specific Perpetrator Type (Global).....	17
Figure 2.5-2: Specific Perpetrator Type (USA).....	18
Figure 2.5-3: Incident Detection Method (Global).....	19
Figure 2.5-4: Incident Detection Method (USA).....	20
Figure 2.6-1: General Access Method (Global).....	21
Figure 2.6-2: Point of Entry (Global) .....	22
Figure 2.6-3: General Access Method (USA).....	23
Figure 2.6-4: Point of Entry (USA) .....	23
Figure 2.7-1: Equipment Involved (Global) .....	24
Figure 2.7-2: Equipment Involved (USA) .....	25
Figure 2.7-3: Protocol (Global).....	26
Figure 2.7-4: Protocol (USA) .....	27
Figure 2.8-1: Attempted Result (Global).....	28
Figure 2.8-2: Attempted Result (USA).....	29
Figure 2.8-3: Achieved Result (Global).....	30
Figure 2.8-4: Achieved Result (USA) .....	30
Figure 2.8-5: Attempted vs. Achieved (Global) .....	31
Figure 2.8-6: Attempted vs. Achieved (USA) .....	32
Figure 2.8-7: Incidents Resulting in Significant Harm.....	33
Figure 2.9-1: Financial Impact (Global) .....	34
Figure 2.9-2: Financial Impact Percentages (Global).....	35
Figure 2.9-3: Financial Impact (USA).....	36
Figure 2.9-4: Financial Impact Percentages (USA).....	37
Figure 2.10-1: Production Impact (Global) .....	38
Figure 2.10-2: Production Downtime Percentages (Global).....	39
Figure 2.10-3: Production Impact (USA) .....	40
Figure 2.10-4: Production Downtime Percentages (USA) .....	40
Figure 3.1-1: Location of Recent Incidents .....	42
Figure 3.1-2: Location of Recent Incidents .....	43
Figure 3.1-3: Incident Type of Most Recent Incidents .....	43

### Tables

Table 2.3-1 Critical Infrastructure and Key Resources (CIKR) Resources Related to RISI	
Industry Types .....	8
Table 2.3-2: Industry Type by Time Period.....	10
Table 2.4-1: Specific Incident Types .....	11
Table 2.4-2: Incident Type by Time Period.....	15
Table 2.5-1: Specific Perpetrator Type.....	16
Table 2.5-2: Detection Method Selections.....	19
Table 2.8-1: Available list of Incident Results .....	28
Table 2.8-2: Incident Result by Time Period.....	33
Table 2.9-1: Financial Impact by Time Period .....	35
Table 2.9-2: Financial Impact by Industry (Global) .....	37
Table 2.9-3 Financial Impact by Industry (USA).....	38
Table 3.1-1: Financial Impact by Industry Most Recent Incidents.....	42

# 1 Introduction

Protecting critical industrial processes from attack has become a growing priority for many companies. Power plants, refineries, chemical plants and other industrial facilities have become increasingly vulnerable as proprietary systems have evolved into open systems. These open systems exposed control systems to security vulnerabilities in industrial processes. Heavy use of commercial technologies, such as Windows and Internet, leaves control systems vulnerable to the same viruses, worms and Trojans that infect office environments. Increasing remote and 24/7 system access translates to more vulnerabilities. With the increase in the sophistication and seriousness of some recent incidents, practitioners are feeling pressures to develop security programs for their plant.

The Repository for Industrial Security Incidents (RISI) records incidents of a security nature that directly affect industrial process control systems (and Data Acquisition and Control (DA) and process control systems). This includes both accidental cyber-related incidents, as well as deliberate events such as external (Service) attacks, and insider information infiltrations. It is the largest known repository of this type. Data is collected from private submissions by companies and the RISI team does not publicly report.

Each of the incidents has been investigated and sensitive information has been removed to protect the confidentiality of the enterprise. The data is indexed and categorized according to a set of criteria that include the type of incident and the impact on the system that cannot be otherwise extracted from the incident report.

At the end of the year of 2009, the RISI team has received a total of 164 incident reports providing information on the type of incident, the system affected, and the impact on the system. Furthermore, the RISI team is working on how to prevent incidents from occurring in the future.

## 1.1 Summary of the Report

The analysis of the report presents at what time and in what types of incidents and the people who reported the incidents and the impact on the system. The results they achieved versus the results they were reporting, especially financial and operational impact on the “victim” company.

The summary of the report presents the results analyzing the rate at which the incidents occurred, the impact of incidents to date and the financial impact on the company.

The report also includes the most recent quarter that include descriptions of what happened, the impact of the incident, and what the company did to avoid future incidents.

## 1.2 Update of this Report

Consistent with earlier reports from 2009, this report presents numerous metrics using the entire data set for incidents with a reliability rating less than “Likely, but confirmed”. Because nearly half of the incidents reported have occurred in the USA, metrics are reported globally as well as just for the USA. Custom reporting, focusing for example on other geographies or industries, is available on request.

While RISI Analysis reports have always included selected case studies they were randomly selected from throughout the database to give the reader a sampling of different types of incidents from a variety of industries and applications. Based on customer feedback, starting immediately the report will include case studies for the new incidents occurring since the last quarterly report (see Section3: Recent Incidents). In this way, an annual subscriber will receive case studies for all new incidents added during their subscription period.

Also new for this report is added focus on recent incidents. The increased data set, meaningful comparison of metrics can be provided based on recent incidents (those occurring within the last 12 months) versus metrics based on the entire dataset.

### 1.3 Data Entry

Figure 2-1 shows the data entry screen. The database contains a total of 152 incidents however, the data reported in this report is limited to incidents with a Reliability of “Confirmed” or “Likely, but Unlikely” or “Probably a Legend” incidents were excluded from the analysis. The analysis includes 152 incidents.

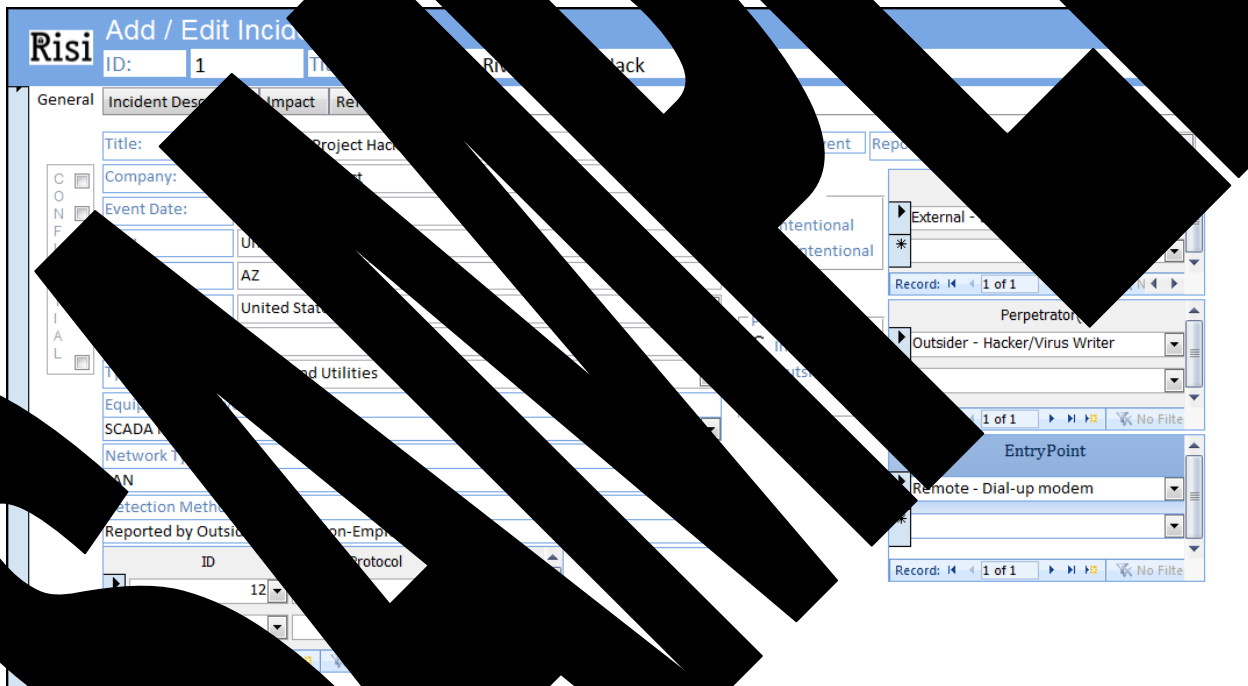


Figure 2-1 Add / Edit Incident

The RISI database structure was revised in April 2009 and again in October 2009 to aid in analysis and reporting. Updates to the existing data was carefully reviewed.

Note that to protect privacy of contributing members; RISI will not publish any information that may identify the contributor.

## 2 Data Analysis

### 2.1 Event Locations

All events in RISI are assigned to the country where the incident occurred unless the contributor requests that information remain confidential. Regardless, all incidents are assigned to a geographical region. Figure 2.1-1: Incidents by World Region shows the distribution of incidents by world region and Figure 2.1-2: Incidents by Country shows the distribution by Country.

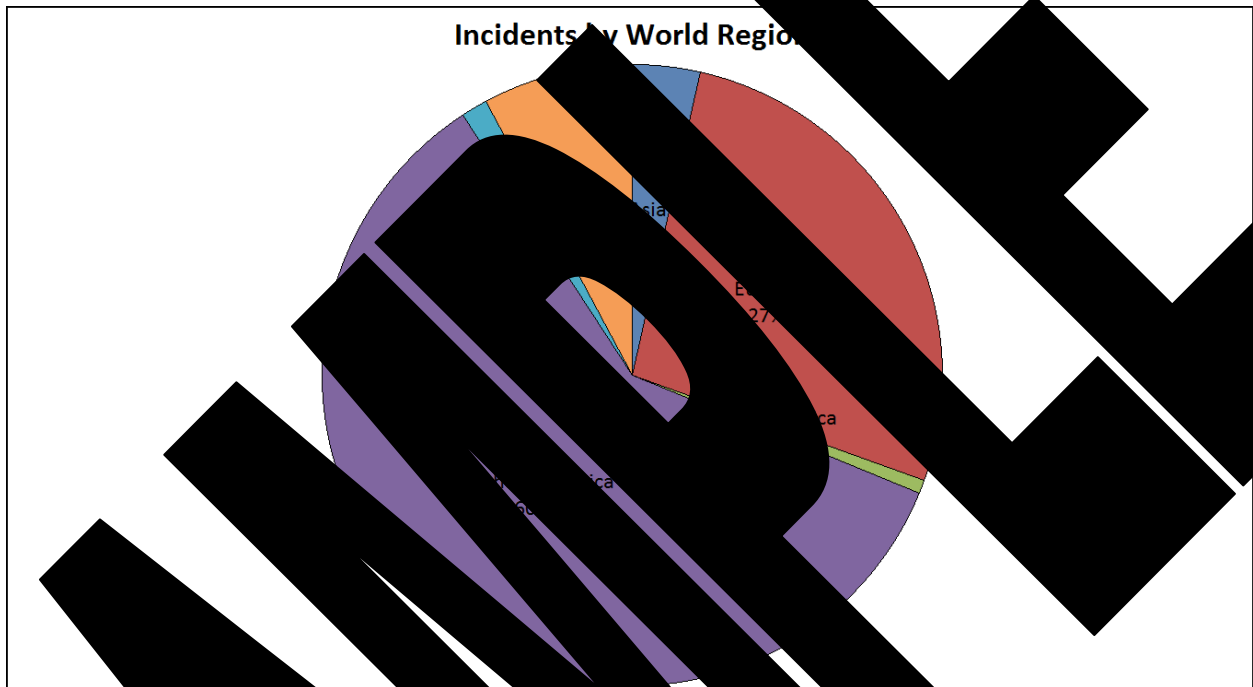


Figure 2.1-1: Incidents by World Region

Industrial security incidents reported to RISI are concentrated in North America. North America accounts for 60% of the incidents reported to RISI. Incidents in Europe account for 27%.

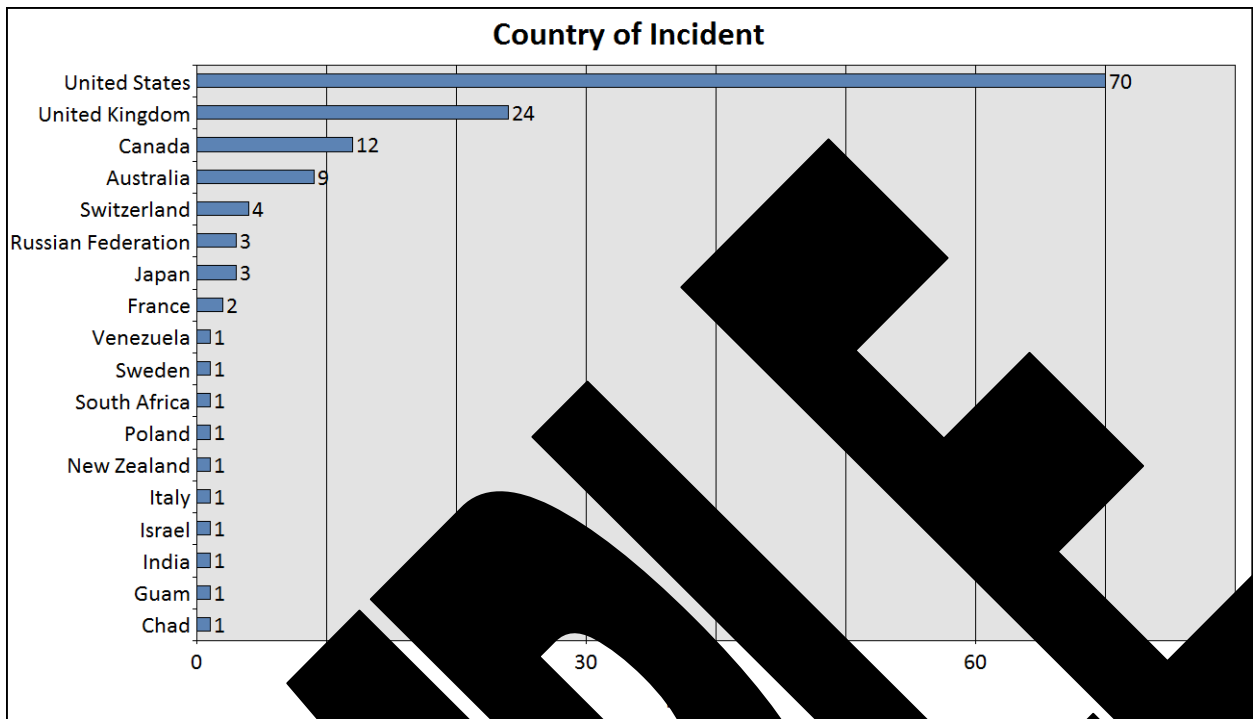


Figure 2.1-2: Incidents by Country

When a distributed incident occurs, it is often shown in the United States shows the highest number of incidents. The United Kingdom Since half of the incidents occurred in the United States, the remainder of the reports presented both globally and for the U.S.

## 2.2 Incidents Over Time

All events in RISI are recorded with the date the incident occurred unless the contributor requests that information remain confidential. Regardless, all incidents are recorded with the year in which the event occurred.

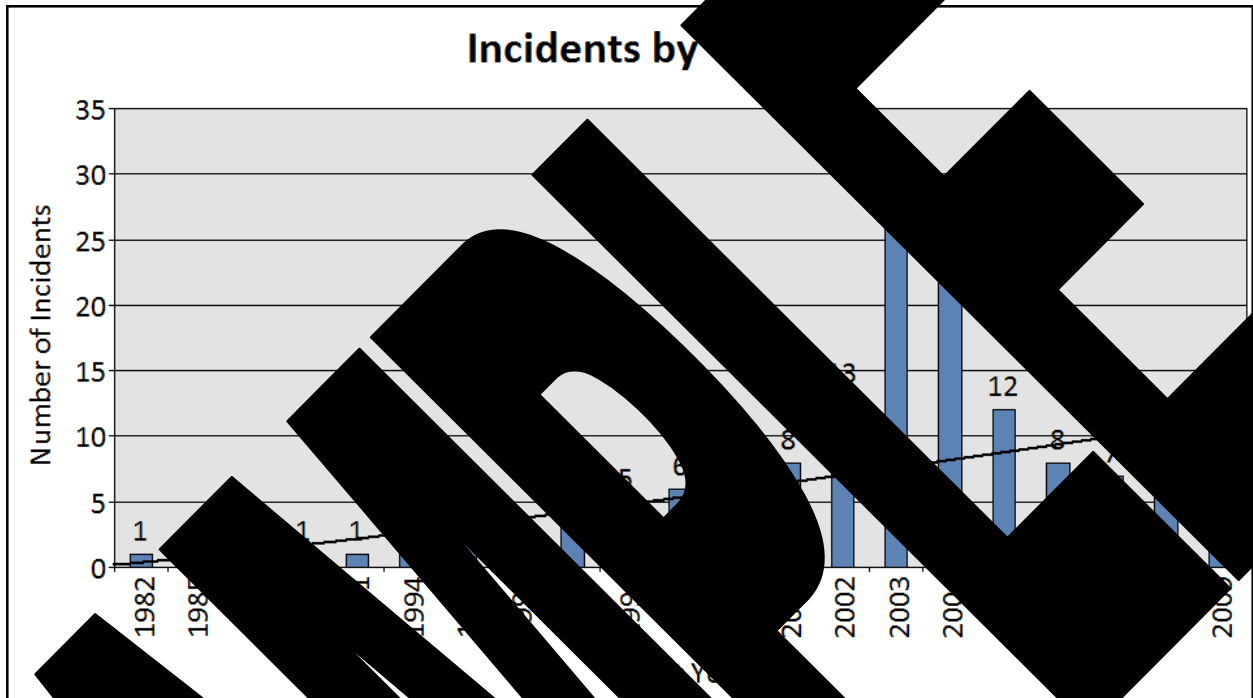


Figure 2.2 Incidents by Year

Figure 2.2 shows the number of incidents that occurred every year since 1982. The chart illustrates several trends. First, there was a steady increase in events in the 1980's and 1990's that can be observed by the increasing number of incidents in the 2000's. The annual rate declines in the mid-2000's but rises again in the last 2000's.

A simple linear trend line was added which indicates that despite the dip in the mid-2000's the rate of incidents has been increasing since 2000. In the last 2000's,

the increase in incidents is partially attributable to the fact that



Figure 2.2-2: Number of Incidents Occurring in the Last Five Years

Figure 2.2-2 shows the number of incidents that occurred in the last five year intervals. As you can see, the number of incidents per year has increased from two in 1995-1999 to 12 in 1999-2003 while the number of incidents in the most recent period has increased to 61.

## Incidents Over Time (USA)



Figure 2.3-3: Number of Incidents Over Time in the USA

Figure 2.3-3 shows the number of incidents over time in the USA. Since nearly half of the incidents in the US, the global trend is that the US mirrors the global trend.

### 2.3 Incidents in the USA

Incidents in the USA are categorized to cover the following list of industry types:

- Aerospace
- Automotive
- Chemicals
- Electronics
- Energy
- Metals
- Mining
- Other
- Petroleum
- Pharmaceuticals
- Power and Utilities
- Pulp and Paper
- Telecommunications
- Transportation

- Water/Waste Water

As one might expect, industries often categorized as Critical Infrastructure and Key Resources (CIKR) reported more incidents than non-critical infrastructure industries. Table 2.3-1 shows the relationship between CIKR Sectors and RISI Industry Types.

Critical Infrastructure and Key Resources (CIKR) Sectors	Industry Types
Agriculture and Food	Food
Banking and Finance	
Chemical	Chemical
Commercial Facilities	
Communications	Communications
Critical Manufacturing	
Dams	
Defense Industrial	
Emergency Services	
Energy	
Governmental Facilities	
Healthcare/Health	Pharmaceutical
Information Technology	
National Monitoring and Control	
Nuclear Reactors, Pipelines and	Utilities
Postal and Shipping	
Transportation Systems	Transportation
Water/Waste Water	

Table 2.3-1: Relationship between Critical Infrastructure and Key Resources (CIKR) Sectors and RISI Industry Types

Occasionally, an incident submitter may withhold this information and in those cases the Incident Category may be recorded as “Unknown”.

### 2.3.1 Incidents by Industry Type and Geography

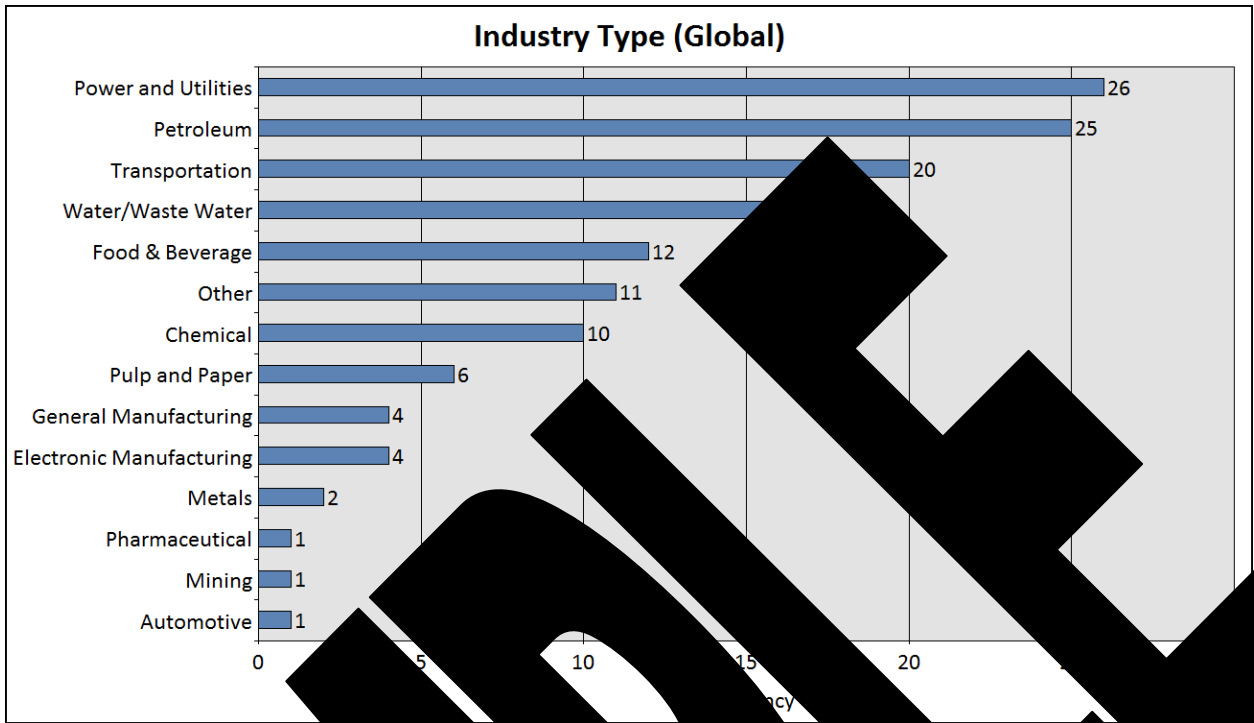


Figure 2.3-1: Incidents by Industry Type (Global)

Figure 2.3-1 shows the following: 15 incidents in the Transportation industry, 11 incidents in the Food & Beverage industry, 10 incidents in the Chemical industry, 6 incidents in the Pulp and Paper industry, 4 incidents in the General Manufacturing industry, 4 incidents in the Electronic Manufacturing industry, 2 incidents in the Metals industry, 1 incident in the Pharmaceutical industry, 1 incident in the Mining industry, and 1 incident in the Automotive industry.

Global Petroleum and Utilities have the highest number of incidents with 25 incidents each. Transportation are the industry with the second highest number of incidents with 20 incidents. Other industries with 10 or more incidents with the industry reported are shown.

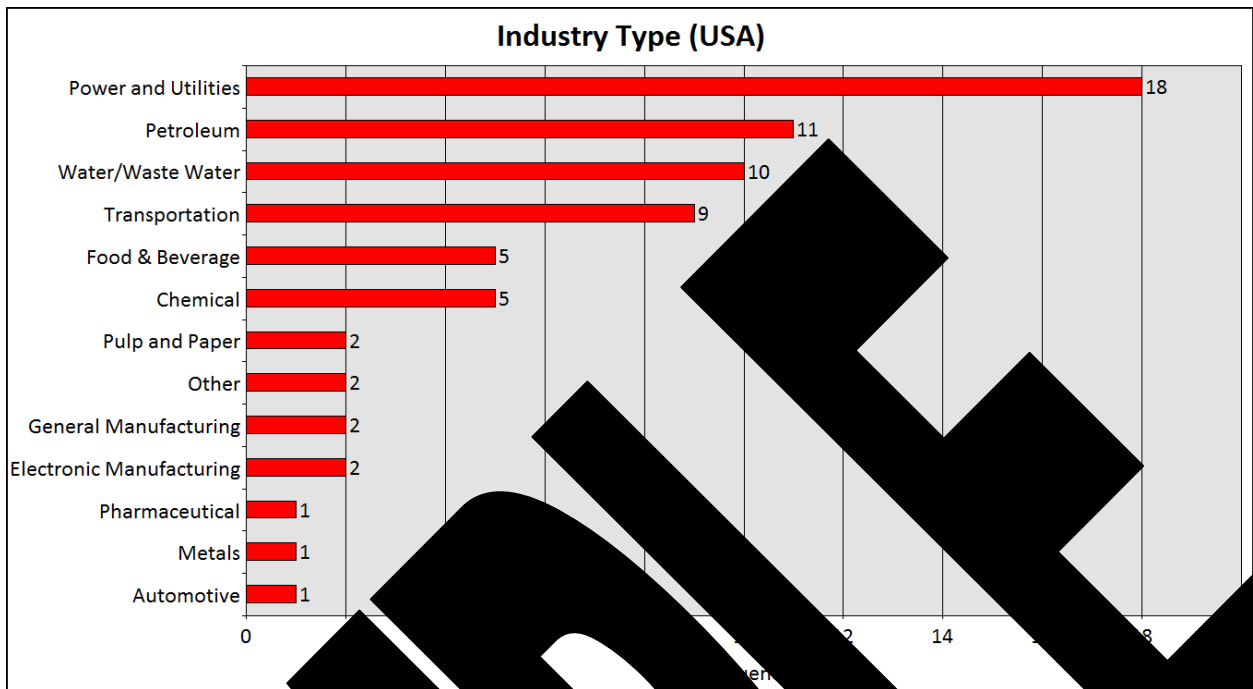


Figure 2.3-2: Incidents by Industry Type (USA)

Figure 2.3-2 is a horizontal bar chart showing the number of incidents by industry type for the top 13 industries in the US. One industry type, Power and Utilities, has the highest number of incidents, with 18 incidents. Other industries with high incident counts include Petroleum (11), Water/Waste Water (10), Transportation (9), Food & Beverage (5), Chemical (5), Pulp and Paper (2), Other (2), General Manufacturing (2), Electronic Manufacturing (2), Pharmaceutical (1), Metals (1), and Automotive (1).

### 2.3.3. Industry Type - Time Period

Industry Type	1999-2003	2004-2008	Change
Transportation	8	6	-25%
Chemical	5	4	-20%
Power and Utilities	6	7	20%
Water/Waste Water	6	6	100%
Food & Beverage	6	6	100%

Table 2.3-2: Industry Type - Time Period

Table 2.3-2: Industry Type - Time Period looks at the top 6 industry types reported for incidents occurring in the earlier time period between 1999 and 2003 and again for the five year period between 2004 and 2008. Both time periods had approximately 60 incidents (see Figure 2.2-2).

Significant differences in incident rates for each industry were observed between the earlier and the more recent time periods. The most dramatic difference is the Petroleum industry which, having the highest incident rate between 1999 and 2003, dropped 72% for the time period between 2004 and 2008. Also notable is that the Transportation and Chemical industries also



## 2.4.1 General Incident Classification

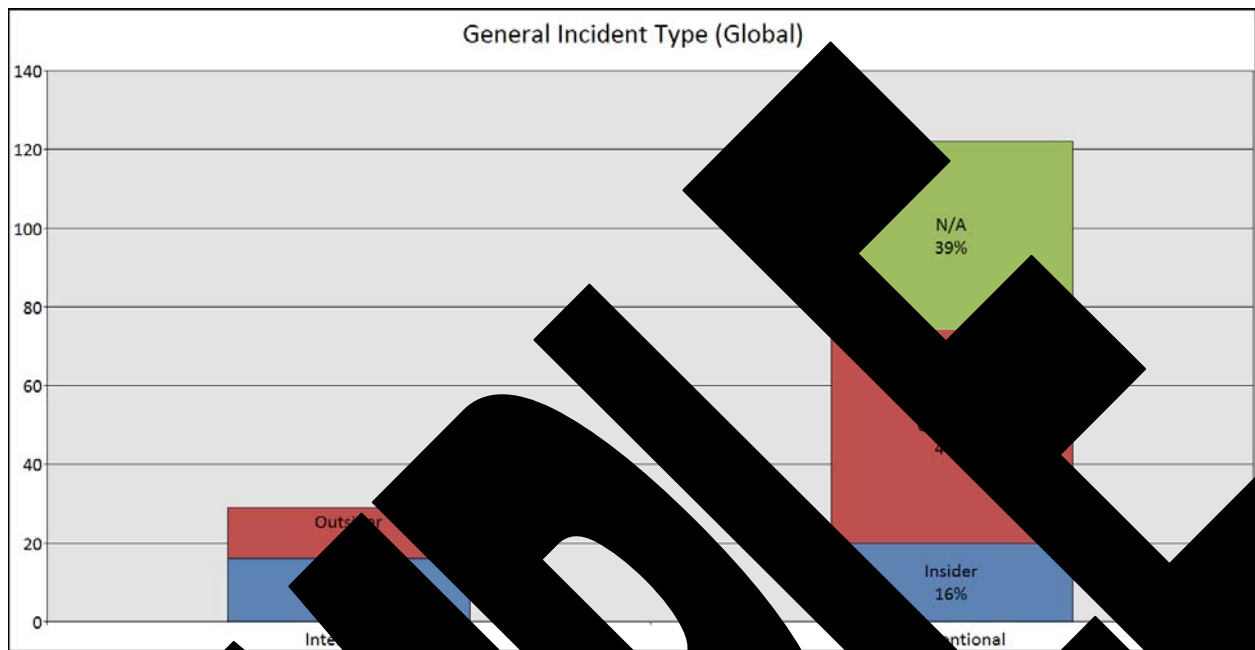


Figure 2.4-1: Incidents Authorized by General Perpetrator Type

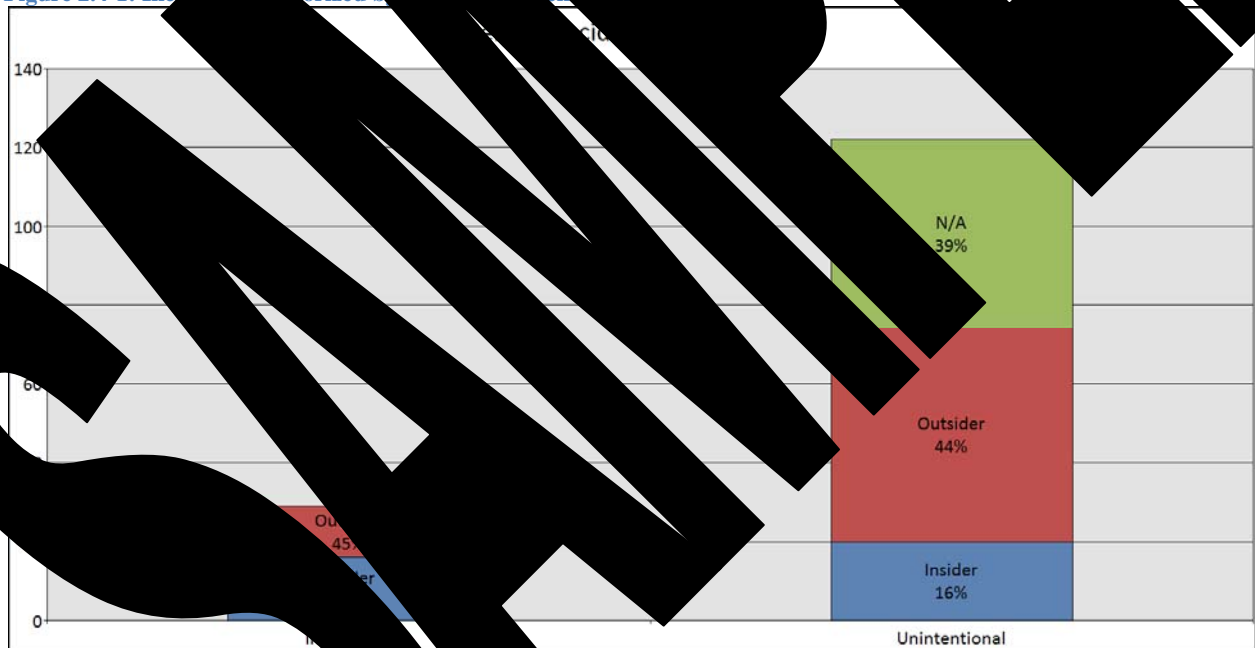


Figure 2.4-1 is a stacked bar chart which shows the distribution of General Intent for all incidents globally as well as the distribution of General Perpetrator Type for both Intentional and Unintentional Incidents. This chart reveals valuable insight into the types of incidents occurring. First, it reveals that the largest percentage of all incidents is unintentional outsider events which are primarily non-directed events such as viruses, worms and trojans. The next largest percentage is unintentional N/A incidents which are generally incidents caused by accidental equipment or software failures. Second, the charts also reveal that only 29 of all incidents

recorded are intentional and of those, the distribution of whether they are insider or outsider attacks is roughly the same.

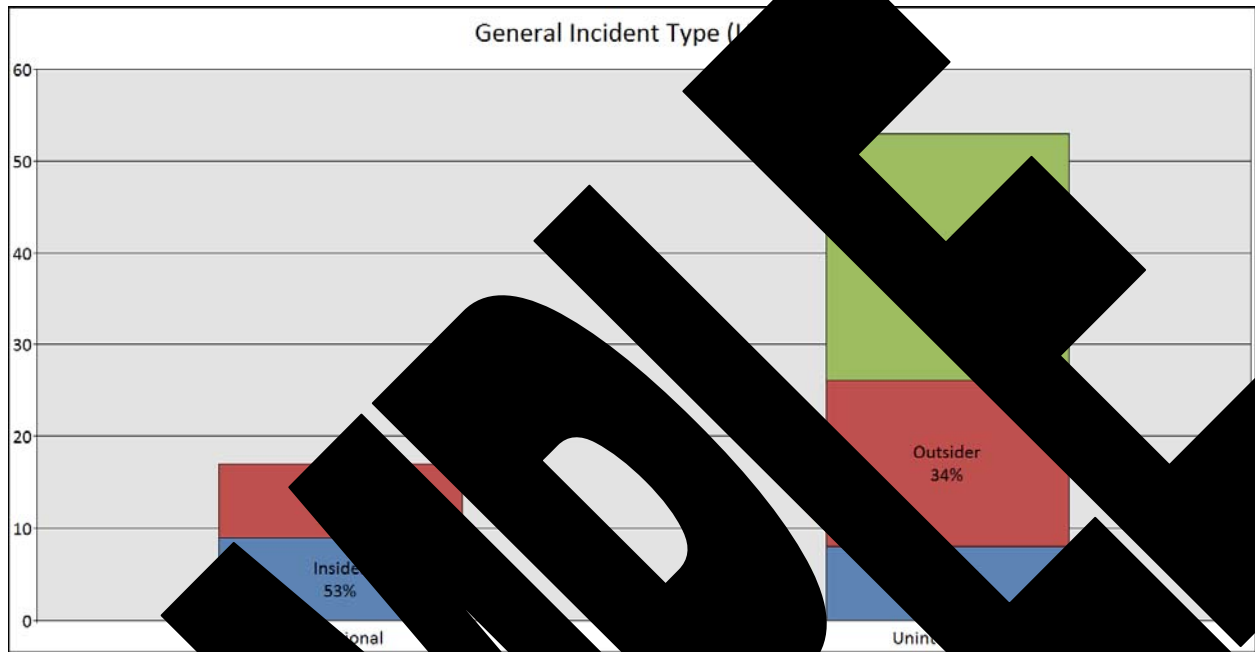


Figure 2.4-2: Incident Type by General Incident Type (1)

Figure 2.4-2 is also a good example of how the distribution of General Intentional incidents was the biggest driver of General Performance for both Intentional and Unintentional incidents. However, the data for intentional incidents occurring in the USA.

One striking difference between the data for global incidents and the data for the USA the largest percentage is intentional USA incidents (intentional incidents used to identify equipment or software malfunctions) where the majority of unintentional incidents are primarily non-directed incidents such as those involving projects. The percentage of intentional incidents and the breakdown of them is consistent with the global data.

In conclusion, the data indicates that US industrial plants are doing a slightly better job of preventing intentional incidents than the rest of the world.

## 2.4.2.2. Conclusion

Figure 2.4-3 and Figure 2.4-4 compare the frequency of specific incident types globally and the USA respectively.

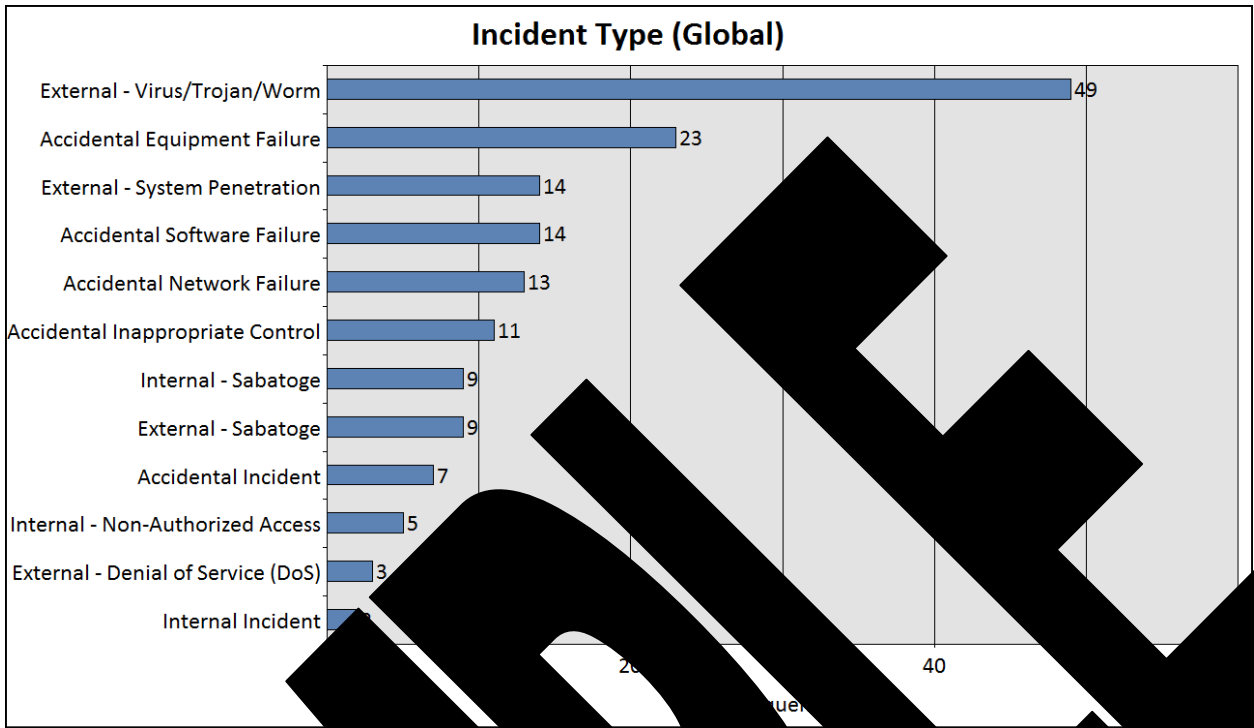


Figure 2.4-3: Incidents Categorized by Specific Incident Type (Global)

Figure 2.4-3 shows that external virus/trojan/worm was the most common type of incident seen globally for the period. Other common incident types include accidental network failure and external system penetration. Sabatoge is also a significant incident type, with a relatively high frequency. Research and development is the most common sector for all incident types, with 20% of all incidents prevented.

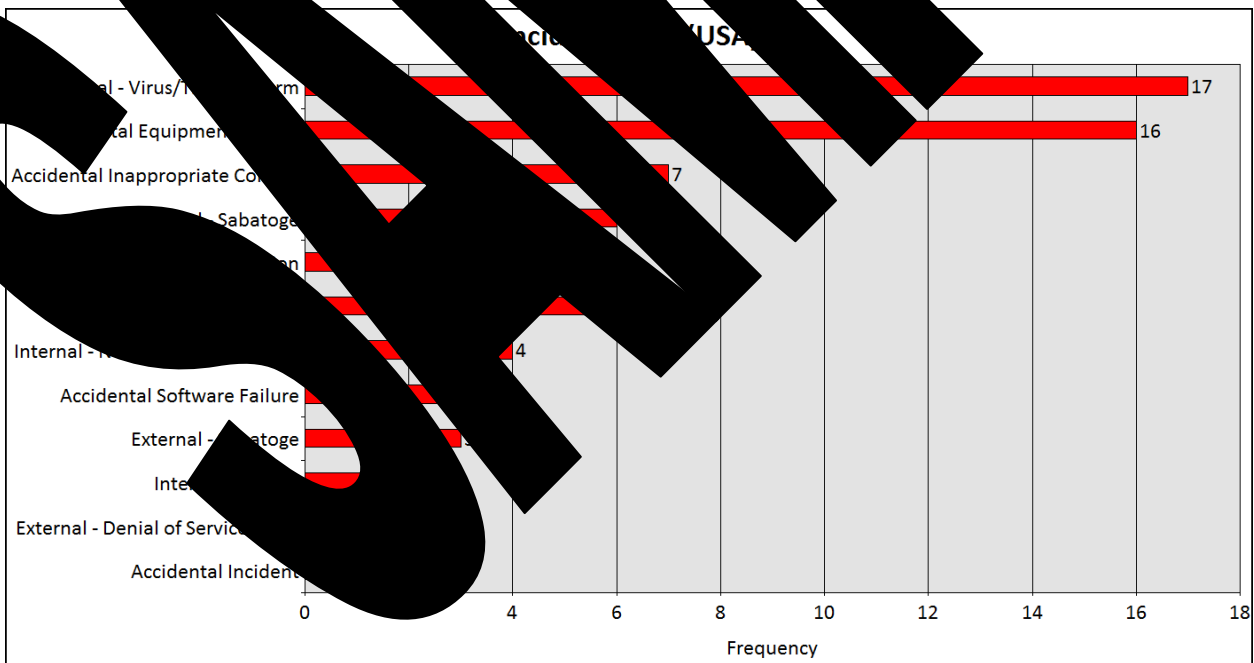


Figure 2.4-4: Incidents Categorized by Specific Incident Type (USA)

Figure 2.4-4 indicates that while malware (viruses, trojans, worms, etc.) was also the incident type most prevalent in the USA that Accidental Equipment Failure was a close second.

### 2.4.3 Incident Type by Time Period

Incident Type	1999 - 2003	Percent Change
External - Sabatoge	5	-100%
External - Denial of Service (DoS)	3	-100%
External - System Penetration	6	-33%
External - Virus/Trojan/Worm	25	
Accidental Incident	2	2
Accidental Equipment Failure		10
Accidental Network Failure		5
Accidental Inappropriate Control	4	5
Internal - Sabatoge		3
Accidental Software Failure		200
Internal - Non-Malicious	0	N/A
Internal Incident	0	N/A

Table 2.4-2: Incident Type by Time Period. This table shows the number of incidents that occurred in the years 1999 to 2003 and again in the period between 2004 and 2008. Both time periods had approximately 60 incidents.

Significant differences in the number of incidents were observed between the earlier and the recent time periods. The most dramatic change is that incidents involving external denial of service and system penetration have gone down in the last five years (2004 to 2008) compared to the five year period (1999 to 2003). On the contrary, incidents involving denial of service and sabotage by internal sources are considerably higher in the same period. In addition, there are incidents involving accidental hardware, software, and network errors as well as accidental inappropriate control.

The number of incidents caused by malware (viruses, worms, trojans, etc.) has remained constant over the period. Operators need to be trained in identifying and maintaining good virus protection on the equipment.

The conclusion drawn from this data is that the biggest threats to industrial control system security are malware, denial of service, and accidental failures. The good news is that countermeasures to strengthen systems against these threats will also serve to strengthen systems against external attacks should they increase in the future.



shows the specific perpetrator types globally.

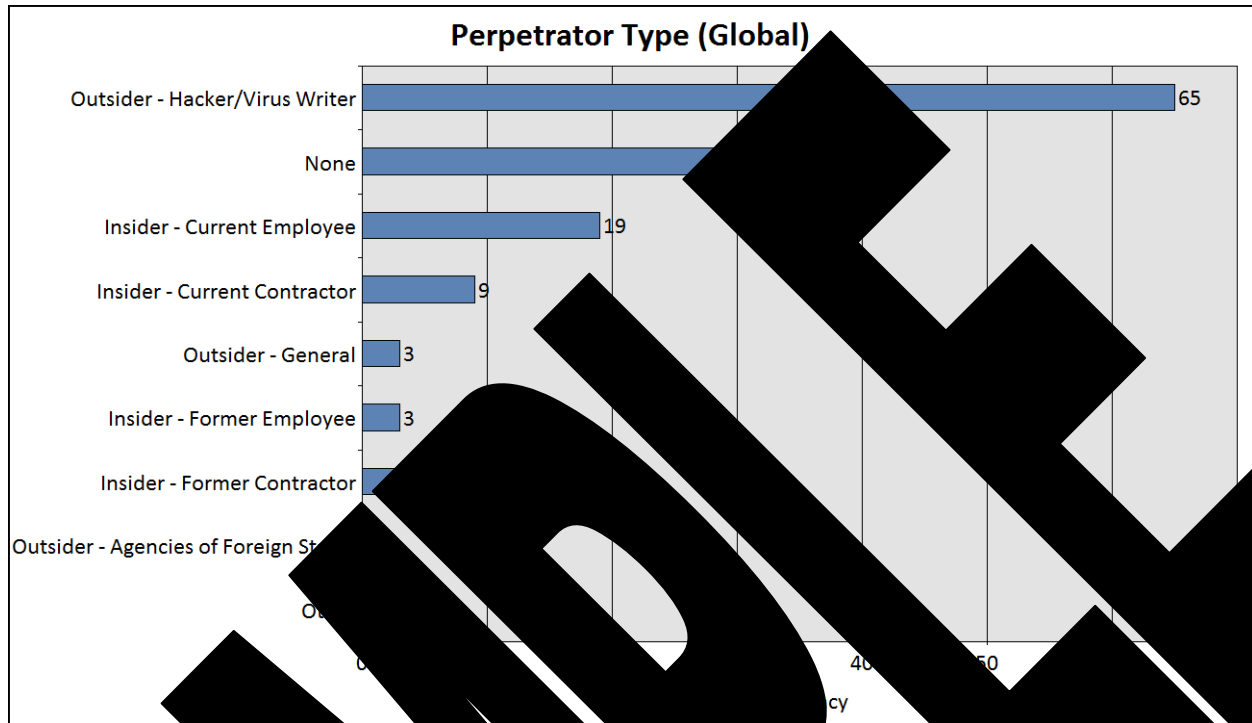


Figure 2.5-1: Specific Perpetrator Type (Global)

As shown in Figure 2.5-1, the most common incident type is Outsider - Hacker/Virus Writer is the most common perpetrator type which accounts for 65% of all incidents. This is the dominant Incident Type. Current employees (6%) and current contractors (8%) are the most common known perpetrators involved in incidents. The majority of incidents are caused by accidentally introducing a virus into a system or database. The majority of errors involve a combination of incidents involving Current Employees and Contractors. These incidents involve a combination of unauthorized access, botnets/Trojan horses and external system penetration. In the case of Former Insiders (Former Employees and Contractors) the situation is somewhat different. Former Insiders were responsible for 6% of all known incidents. However, in the case of Former Insiders (Former Employees and Contractors) Former Insider incidents included: multiple former employees and contractors are immediately prevented from accessing systems, especially the systems that they supported when active.

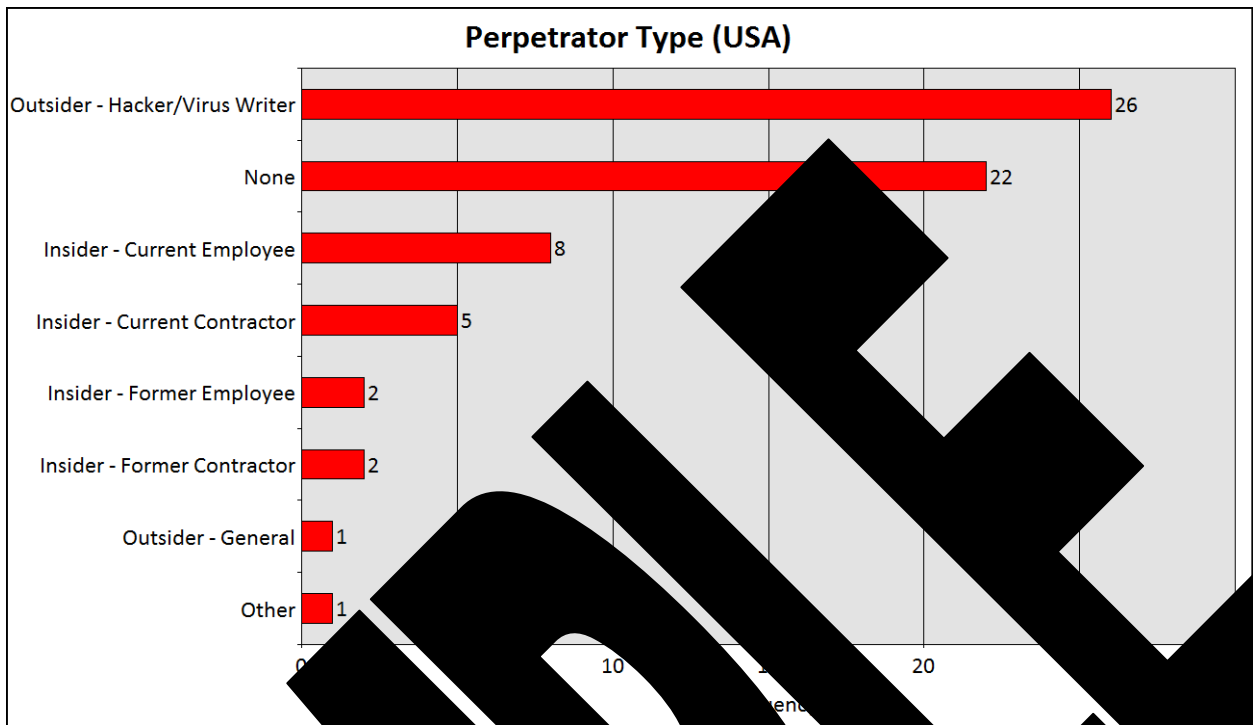


Figure 2.5-2: Specific Perpetrator Type

Figure 2.5-2 shows the specific perpetrator type for each incident.

The data generally shows a global trend.

### 2.5.3 Detection Method

All events are recorded in the system when an incident was detected. Available detection methods include:

Detection Method
Star
Security Service/Alert D
Incident
Security Consultant/Investigator
System Control/Op Staff During Incident
System Control/Op Staff After Incident
System Administrator During Incident
System Administrator After Incident
Device/Log Alert
Device/Log Alert After Incident
Found During Routine Audit Activity
Reported by Outside Agency/Non-

Employee
Other
Unknown

Table 2.5-2: Detection Method Selection

Figure 2.5-3 shows a summary the methods by which incidents were detected globally.

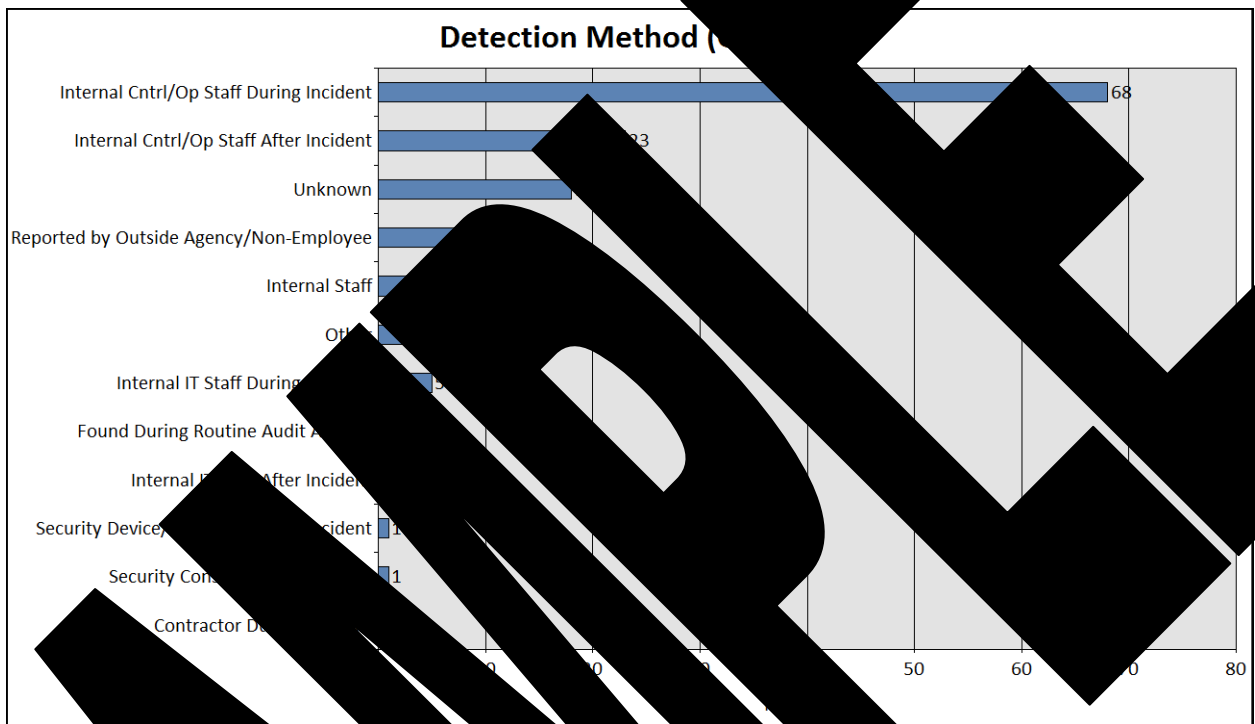


Figure 2.5-3: Detection Method Selection

Most incidents were detected by internal personnel operating outside the incident. In a considerable number of cases, detection occurred through internal incident

Licensed to Client Company on 30 November 2009. Distribution restricted to employees of Client Company.

**SECRET**

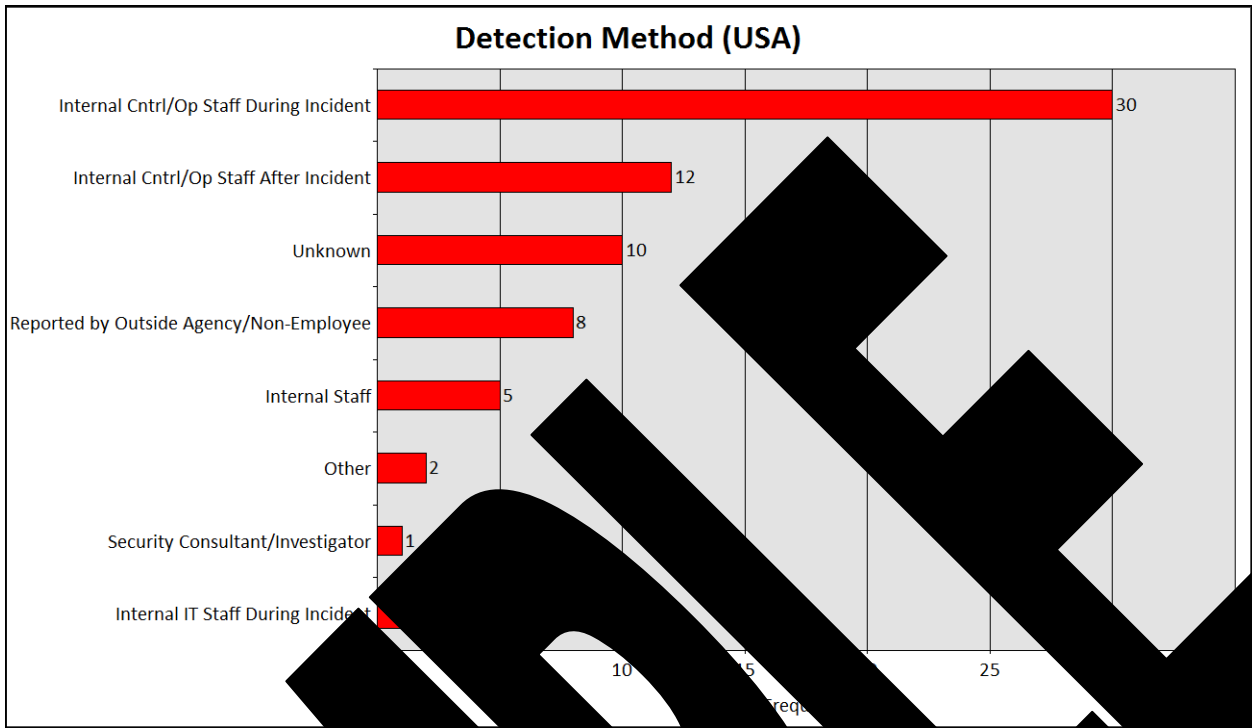


Figure 2.5-4: Incident Detection Method

Figure 2.5-4 shows the primary methods used to detect incidents were internal control/operations staff during the incident. As with the global incident data, 67% of incidents were detected by internal control/operations staff during the incident.

## 2.6 Incident and Point of Entry

Whenever possible, the method of entry and point of entry are recorded for each incident. The following methods are available for those incidents where they are available for selection.

- Local
  - Local - Business Network
  - Local - Community/Shared Media
  - Local - Direct Access (D)
  - Local - Layer 2
  - Local - Physical Access
  - Local - Terminal
- Remote
  - Remote - Covert
  - Remote - Direct
  - Remote - Indirect
  - Remote - Network
  - Remote - Physical
  - Remote - Trusted 3rd Party Connection
  - Remote - Via Business Network
  - Remote - VPN Connection

- Remote - Wireless System
- Remote Access
- None
- Other
- Unknown

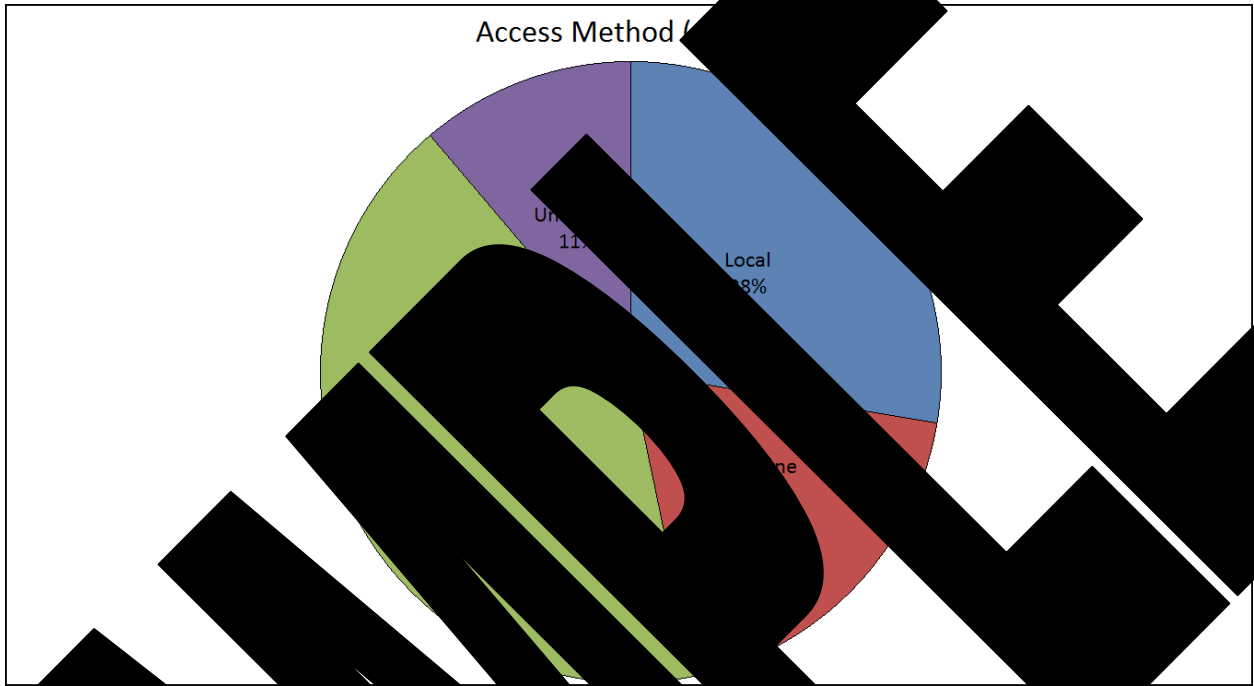


Figure 2: General Access Method Distribution

Figure 2 shows the general method of access into systems recorded globally.

Remote access is the primary method of entry into systems. While not surprising, this supports the assumption that working with automation and systems made the systems more vulnerable to cyber security incidents. Local access at 28%, is significant.

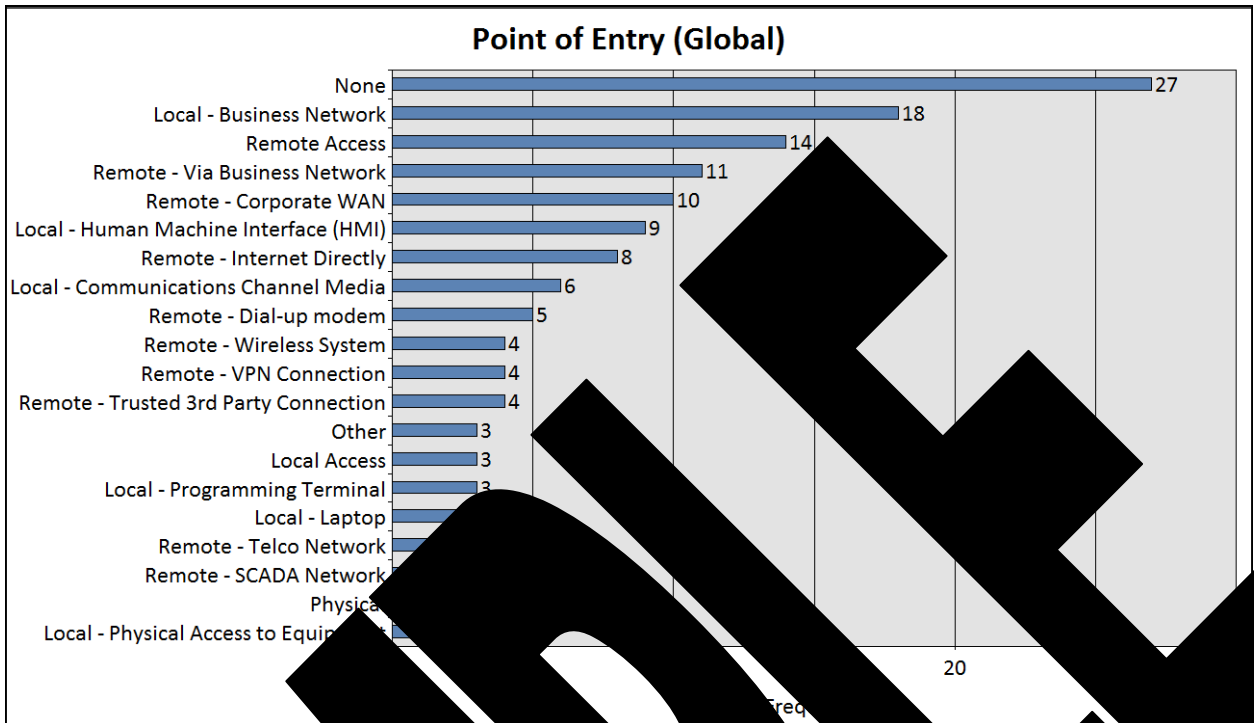


Figure 2.6-2: Point of Entry (Global)

Figure 2.6-2 provides a detailed breakdown of the various points of entry to enterprise systems.

In many cases, the point of entry was not known or “unknown”. Even in those cases, the point of entry most often occurred through the business network, either remotely or locally. In many cases, the point of entry occurred through the Business Network, a significant finding. This data supports the warnings that enterprise systems security is at risk when direct internet connection and its ability to connect to equipment.

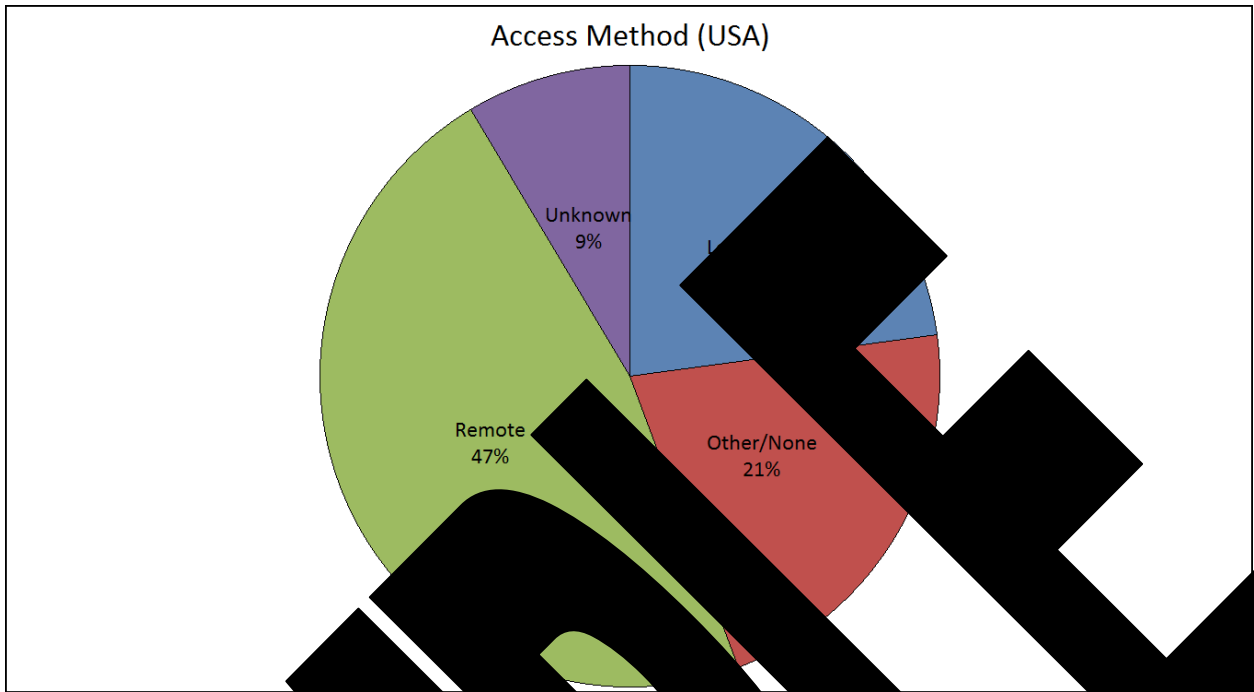


Figure 2.6-3: General Access Method (USA)

Figure 2.6-3 shows the general method of access to systems in the USA. Similar to the general remote access method, 47% of the primary methods of access to systems were remote access. This is slightly higher than the general data and security incidents, which were slightly higher than the general data, accounting for more than half of the incidents.

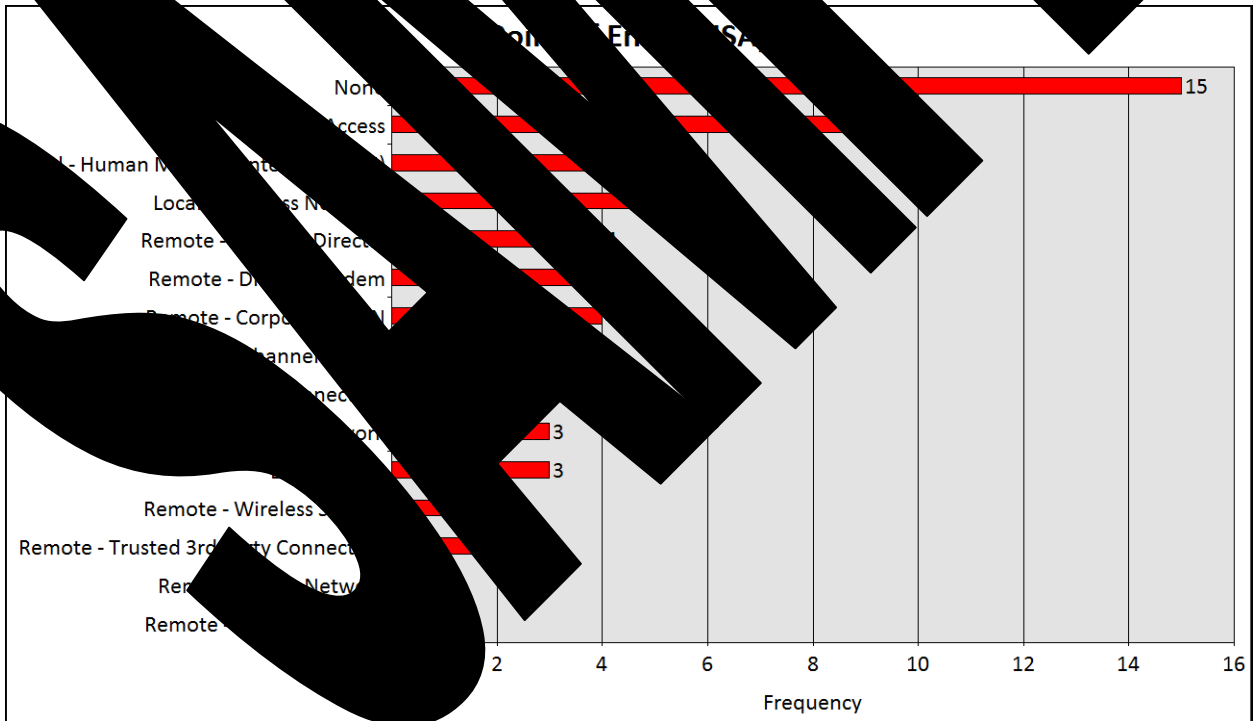


Figure 2.6-4: Point of Entry (USA)

Figure 2.6-4 shows detailed information on the various points of entry into industrial control systems in the US.

Excluding “none” or “unknown”, the US entry point distribution shows that non-specific remote access was seen most often. Local Human Machine Interface (HMI) and local business network access follows in frequency.

## 2.7 Equipment Involved and Protocols

### 2.7.1 Equipment Involved

When known, the type of equipment involved is recorded for each incident. Sometimes multiple pieces of equipment are involved in a single incident, so the total number of pieces of equipment involved will exceed the total number of incidents.

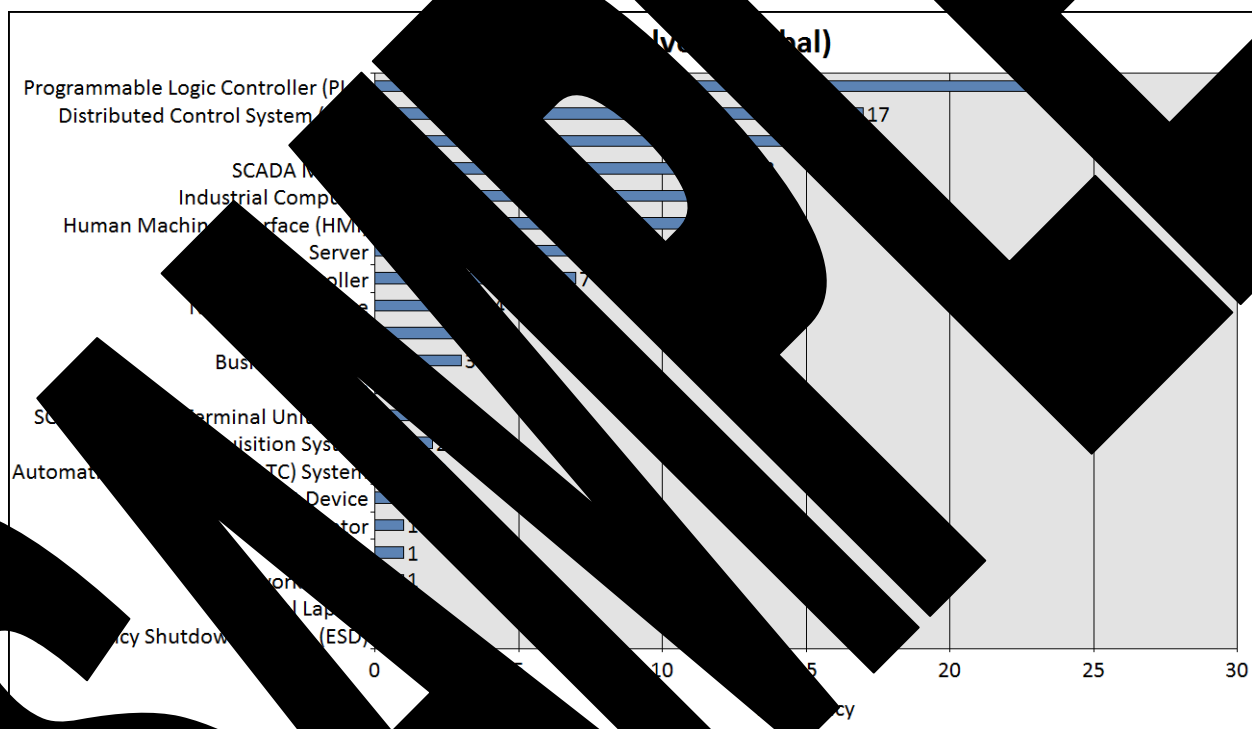


Figure 2.6-5 shows the types of equipment affected in industrial security incidents globally. The equipment involved in industrial security incidents is Programmable Logic Controllers (PLC) and Distributed Control Systems (DCS). This is not surprising but some of the other types of equipment involved, such as SCADA's, RTU's and RTU's might be.

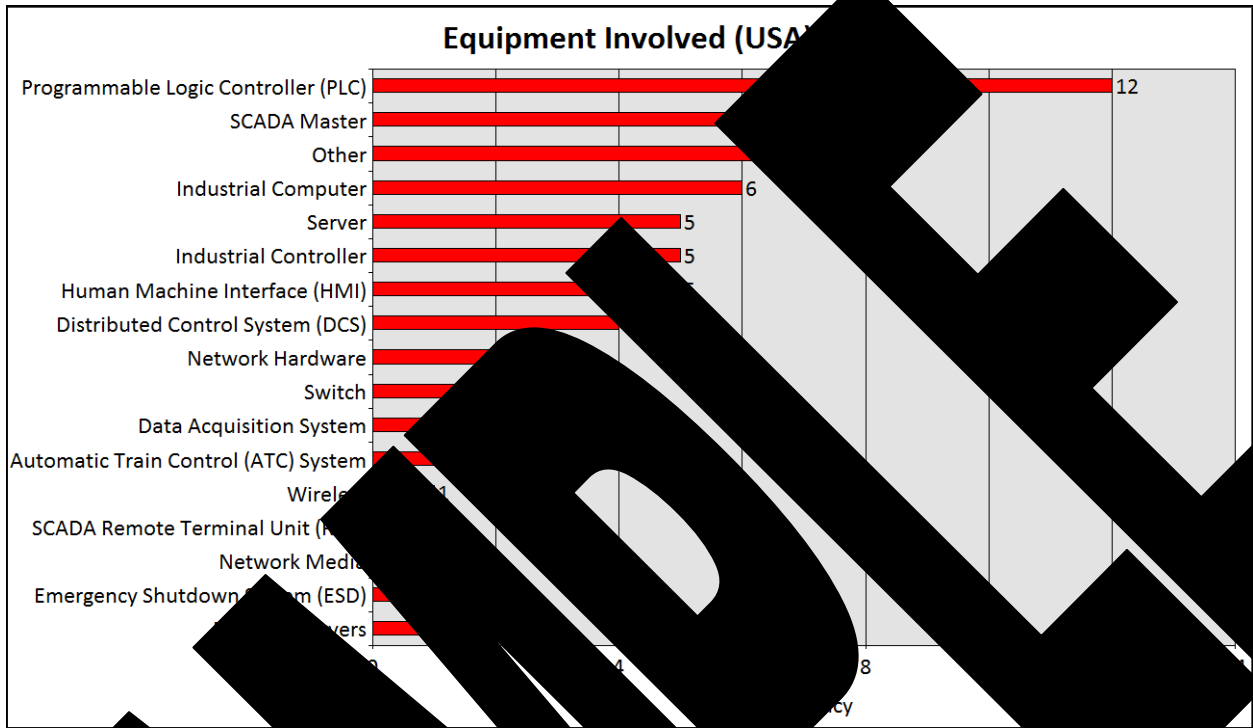


Figure 2. Equipment Involved

Figure 2 shows the type of equipment involved in industrial security incidents in the US.

PLC's are most often involved in industrial security incidents, followed by SCADA Masters and other.

Protocols Involved

When known, the type of protocol involved is recorded for each incident.

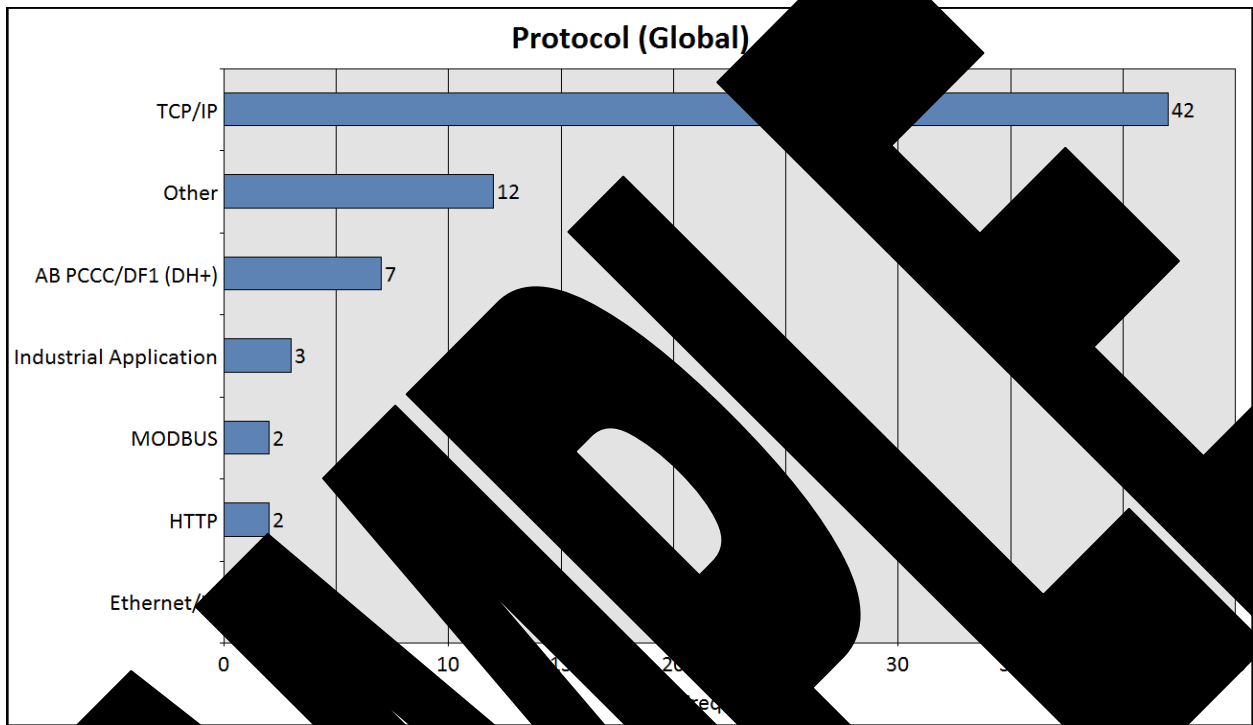


Figure 2.7-... (Global)

Figure 2.7-... frequency of... protocols... many cases... unknown... this most frequently

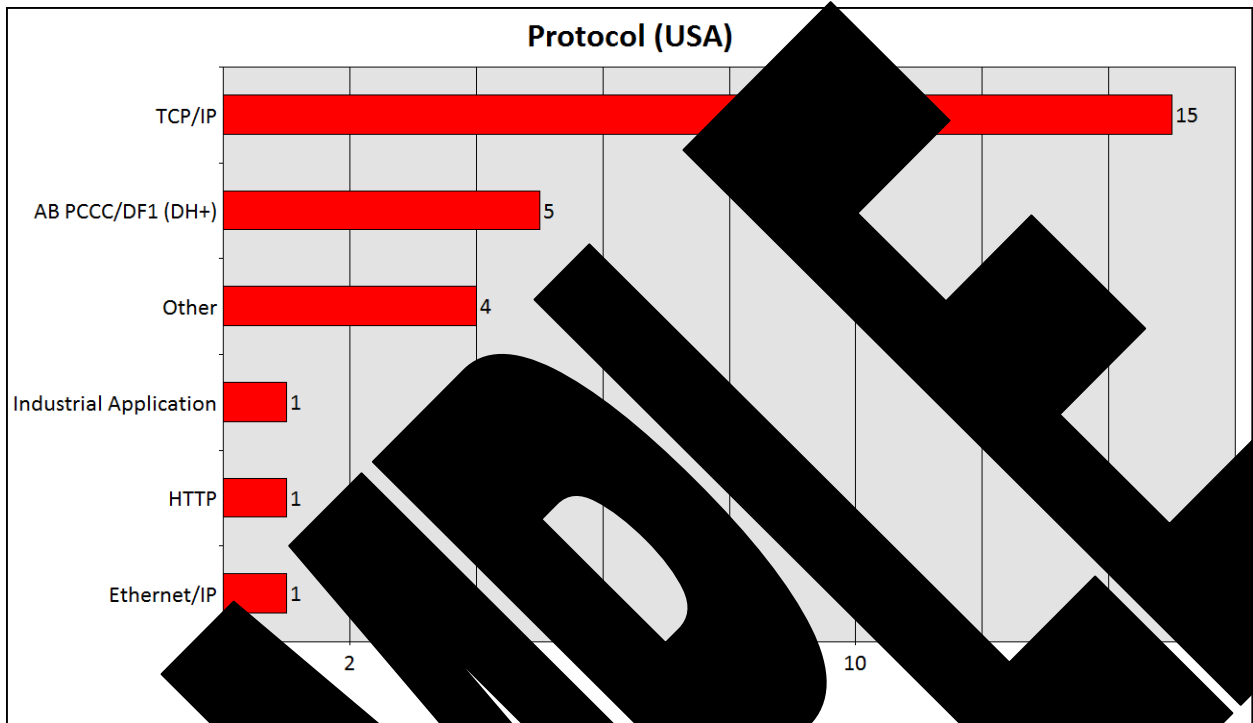


Figure 7-4: Protocol (USA)

Figure 7-4 shows the number of identified and confirmed security incidents by protocol type. Again, the majority of incidents were reported with the protocol unknown. When the protocol was known, the most reported incidents were for TCP/IP followed by AB PCCC/DF1 (also known as Data Highway 2).

### Results

All incidents in RISI were assigned to one or more of the following list of possible outcomes:

Loss of Confidentiality
Loss of Integrity
Loss of Availability
Loss of Confidentiality/Integrity/Availability
Loss of Confidentiality/Integrity
Loss of Confidentiality/Availability
Loss of Confidentiality/Integrity/Availability/Control
Loss of Confidentiality/Integrity/Availability/Control/Ownership
Loss of Confidentiality/Integrity/Availability/Control/Ownership/View
Loss of Confidentiality/Integrity/Availability/Control/Ownership/View/None
Loss of Confidentiality/Integrity/Availability/Control/Ownership/View/None/Intellectual Property Theft
Loss of Confidentiality/Integrity/Availability/Control/Ownership/View/None/Intellectual Property Theft/Fraud
Loss of Confidentiality/Integrity/Availability/Control/Ownership/View/None/Intellectual Property Theft/Fraud/Injury or Death
Unknown
Loss of View
None
Intellectual Property Theft
Fraud
Injury or Death

Public Injury or Death
Fine/Penalty
Loss of Communications
Loss of Data
Public Nuisance/Inconvenience

Table 2.8-1: Available list of Incident Results

Often the outcome (achieved result) does not match the intended (attempted result). Therefore, both the attempted and the achieved results are reported for all incidents. In many cases, more than one result was attempted and achieved. The results are presented as a total.

### 2.8.1 Attempted Results



Figure 2.8-1: Attempted Results (Total)

This chart shows the frequency of the various results of the incidents in the RISI database.

Except for the category of "None", "Loss of production / operation" and "Spill" are the types reported most often.

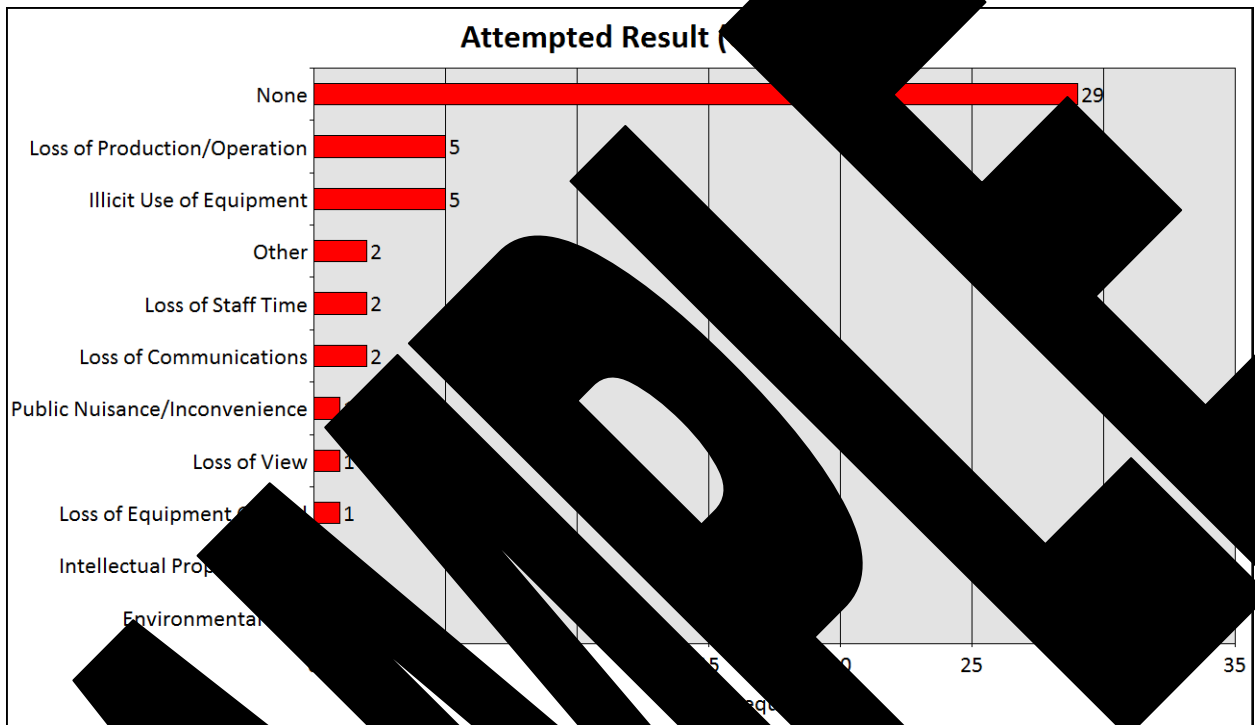


Figure 2.8-2. Attempted Result (USA)

Figure 2.8-2 shows the number of records reported for each attempted result in the RISI

data, which were widely reported. The most common attempted results were "Loss of Production/Operation" as well as "Illicit Use of Equipment" and "None".

### Attempted Result

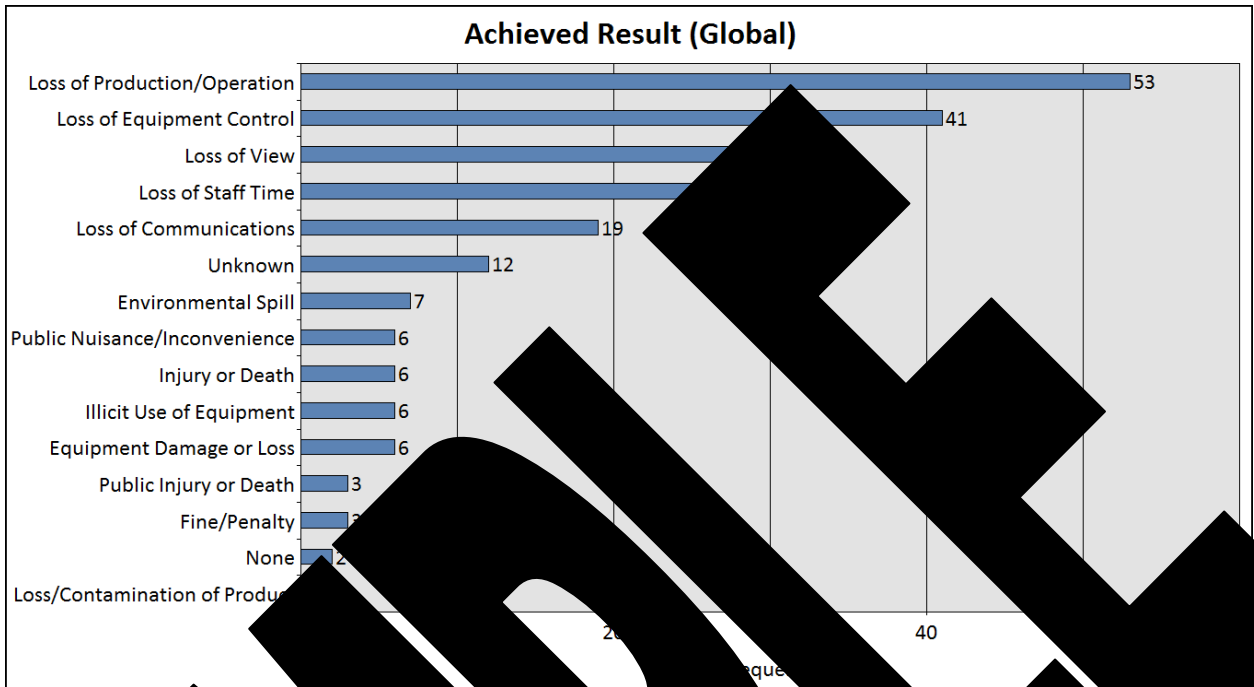


Figure 2.8-3: Achieved Result (Global)

Figure 2.8-3 shows the achieved result for all incidents reported. The achieved results are a subset of the attempted results. “None” or “Unknown” are excluded from the attempted results. Loss of equipment control and loss of production are the most frequently reported achieved results. In 9 incidents, injury or death occurred as a result of a security incident in 2009.

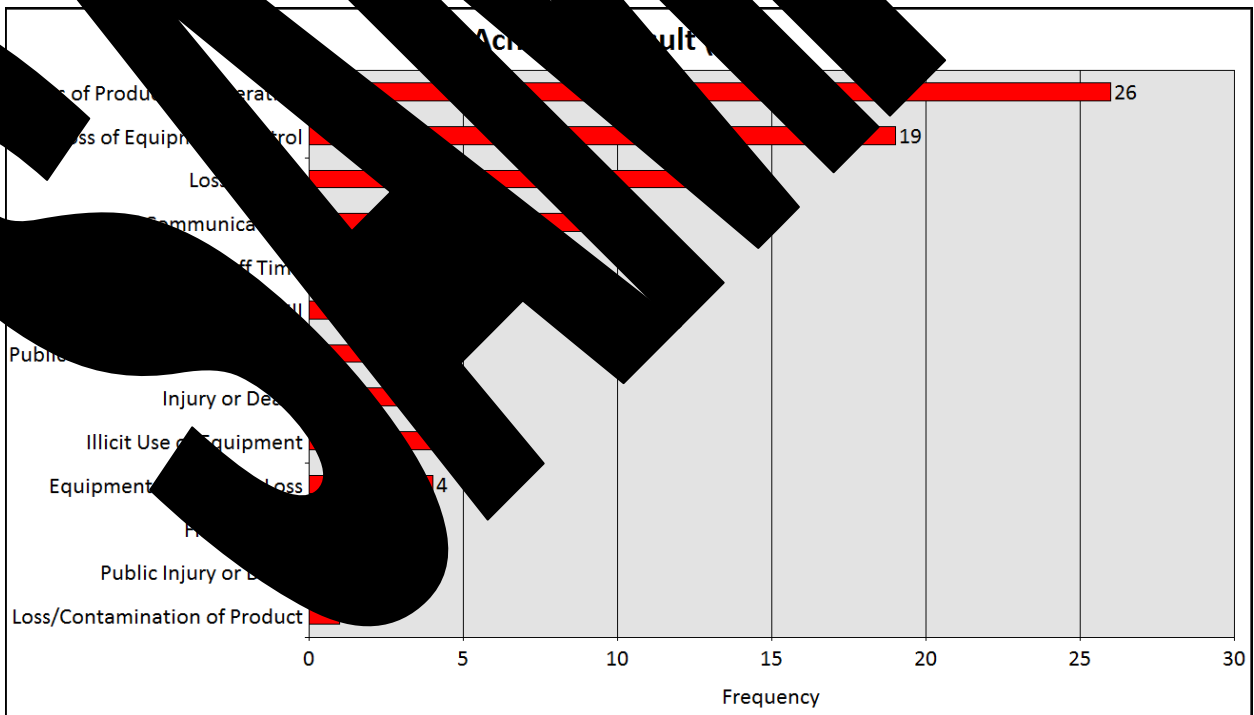


Figure 2.8-4: Achieved Result (USA)

Figure 2.8-4 shows the achieved results for all US incidents reported.

“Loss of production/operation”, “Loss of equipment control” and “Loss of view” have been most frequently reported.

In 5 US cases, injury or death resulted from industrial security. The new incident involving public injury or death was reported this quarter.

### 2.8.3 Attempted versus Achieved Results



Figure 2.8-4 (Global) Achieved Results

Figure 2.8-5 shows the comparison of attempted results to achieved results of reported incidents.

The most striking feature of this analysis is that more was achieved than was known to be attempted. Most of the attempted results were “Unknown” or “None” as is the case with accidents or malware. The achieved results most often achieved “Loss of production/operation”, “Loss of equipment control” and “Loss of view”. All of which, can lead to catastrophic consequences.

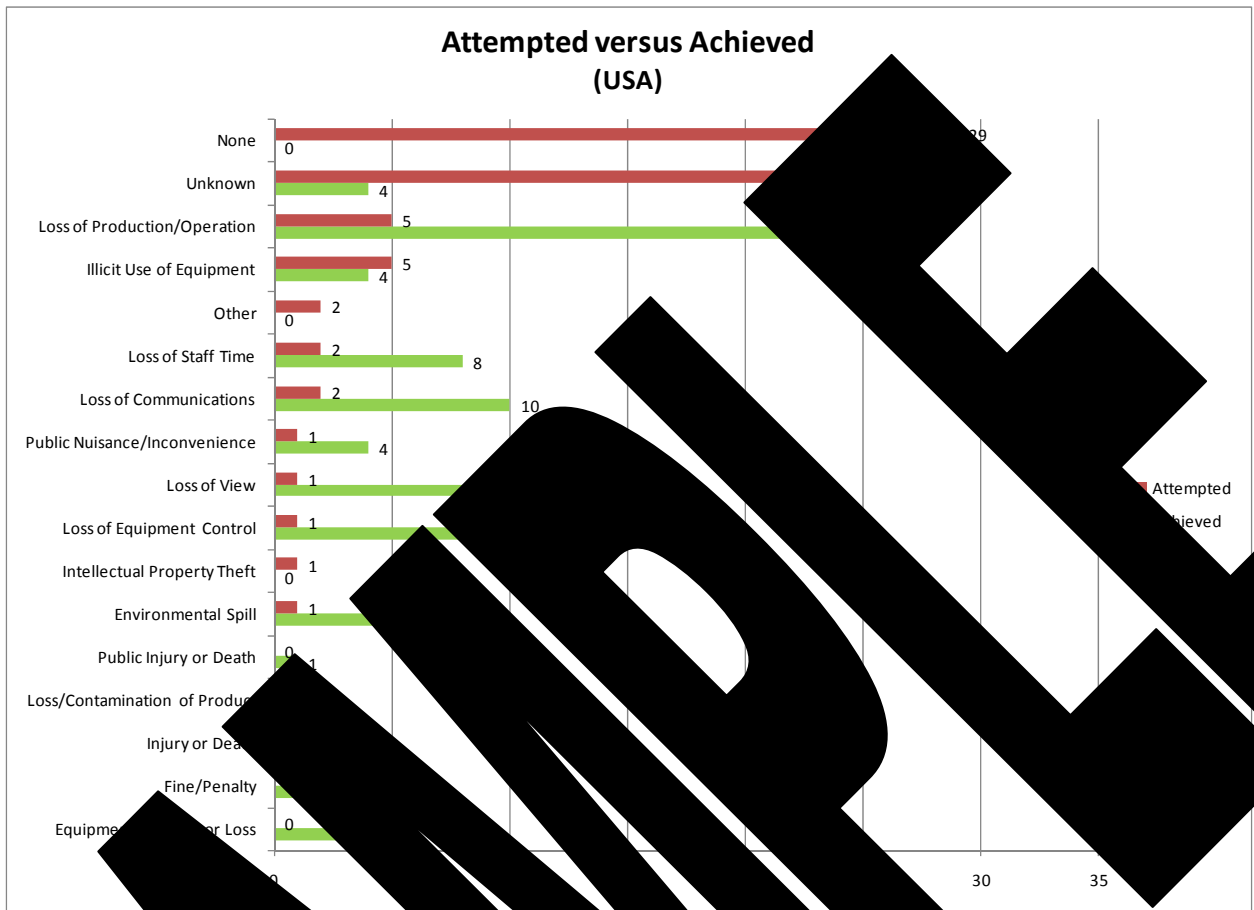


Figure 2.8-6: Attempted versus Achieved (USA)

Figure 2.8-6 shows the comparison of attempted versus achieved results for the results of reported incidents.

The US incidents show some categories such as “Loss of view” that were not achieved, but were attempted. “Loss of production/operation”, “Loss of equipment control” and “Loss of view” are among the top results achieved. The data indicates that the US is remote access with the leading cause of incidents.

### 2.8.4 Incidents Resulting in Significant Harm

Incidents resulting in “Significant Harm” are those that caused harm to people, the environment or resulted in a significant financial loss. Typically, for this analysis we include the following categories:

- Environmental Spill/Release
- Fine/Penalty
- Equipment Damage or Loss
- Injury or Death
- Loss of Equipment Control
- Loss of Equipment View

- Loss of Production/Operation
- Loss/Contamination of Product

Currently there are 132 incidents in the database that have resulted in significant harm. This figure is startling considering only 22 of these 132 incidents, or 17%, were perpetrated by individuals actually intending to cause harm. In fact, there are 2 incidents whereby a deliberate attack actually caused more harm than was intended.

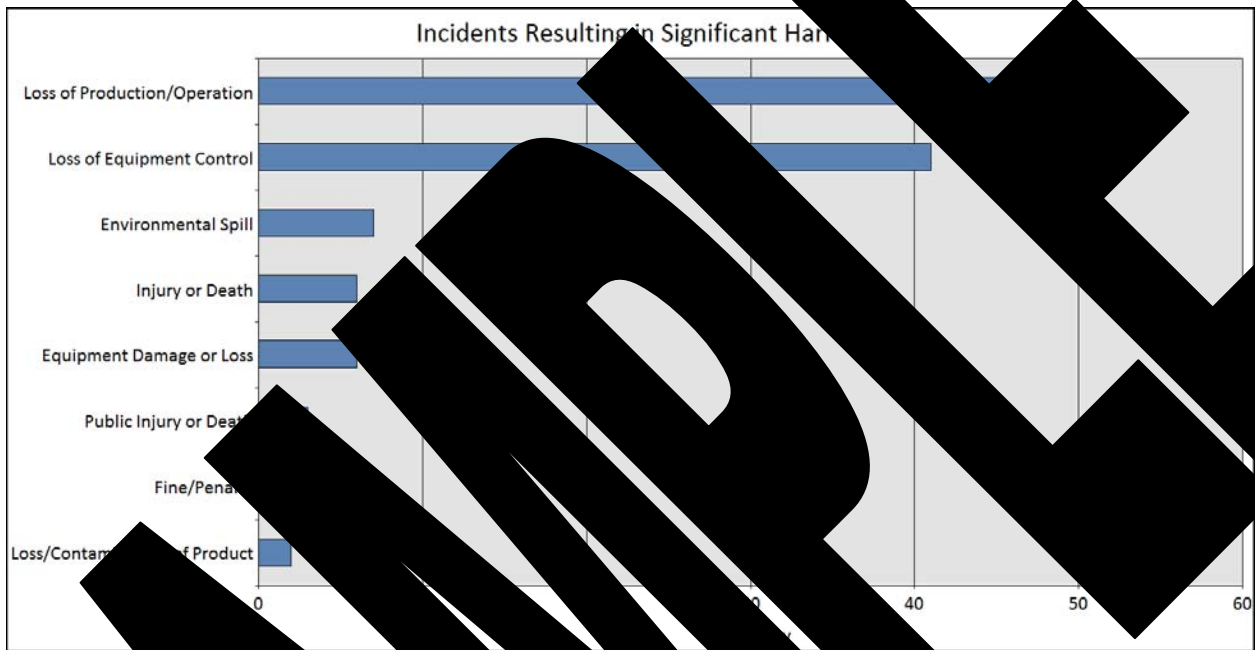


Figure 2.8-7: Incidents Resulting in Significant Harm

...indicates that the control systems need to be improved, not just intentional...  
 ...intentional incidents, equipment failure and... actually account for  
 ...number of...  
 ...

### 2.8.5 Incident Result by Time

Incident Type	2004 - 2008	% Change
Loss of Production/Operation	22	-50%
Loss of Equipment Control	16	7%
Environmental Spill	3	50%
Injury or Death	3	200%
Public Injury or Death	1	N/A
Loss/Contamination of Product	1	N/A
Fine/Penalty	2	N/A

Table 2.8-2: Incident Result by Time Period

Table 2.8-2: Incident Result by Time Period looks at the rate of incidents resulting in significant harm occurring in the five year period between 1999 and 2003 and again for the five year period between 2004 and 2008. Both time periods had approximately the same number of incidents.

The most dramatic difference is the increase in incidents resulting in injury or death. The figure jumped from 1 to 4, representing a 300% increase.

## 2.9 Financial Impact

### 2.9.1 Financial Impact by Geography



Figure 2.9-1 shows the financial impact of industrial security incidents world-wide.

The total number of incidents with a financial impact of less than \$100,000 (36 incidents) is equal to the number of incidents with a financial impact exceeding that amount (37). However, the number of incidents with a financial impact greater than \$10,000,000, up from 8 reported incidents in 1999-2003 to 15 incidents with a financial impact was 8.

The industries suffering the most financial impact due to industrial security incidents are Petroleum, Power & Utilities and Transportation (see Table 2.9-2: Financial Impact by Industry (Global)).

### Financial Impact Percentages (Global)

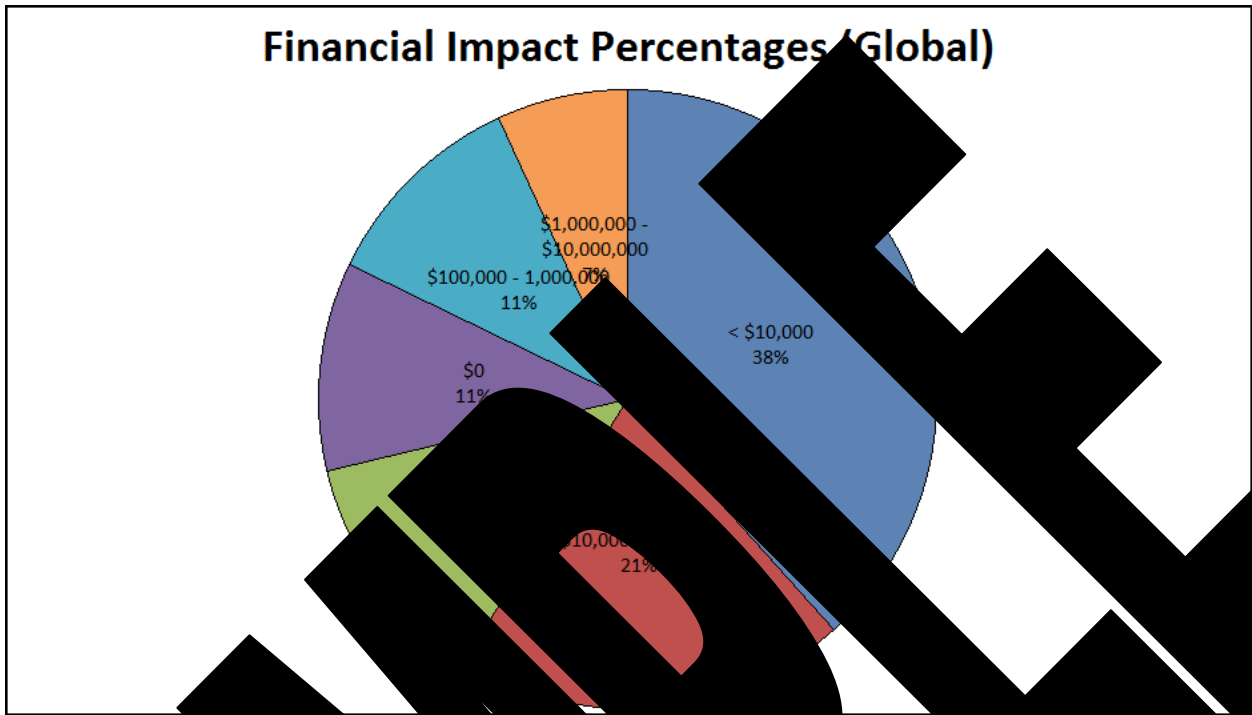


Figure 2.9-2: Financial Impact Percentages (Global)

Figure 2.9-2 shows the financial impact of security incidents world-wide as a percentage of total incidents. The largest percentage of incidents, 38%, resulted in financial impact of less than \$10,000.

38% of incidents reported resulted in financial impact in the range of \$1-\$10,000. When incidents resulted in no financial impact, the percentage of incidents resulting in \$0 was 11%.

Figure 2.9-1: Financial Impact by Time Period shows the financial impact of incidents over the five year period between 2004 and 2008. The number of incidents in the five year period between 2004 and 2008 was approximately the same number of incidents.

Financial Impact Range	2004-2008	2009	% Change
< \$10,000	5	8	67%
\$10,000 - \$100,000	8	5	-33%
\$100,000 - 1,000,000	5	3	67%
\$1,000,000 - \$10,000,000	3	4	33%
\$10,000,000 - \$100,000,000	1	2	100%
> \$100,000,000	3	1	-67%

Figure 2.9-1: Financial Impact by Time Period

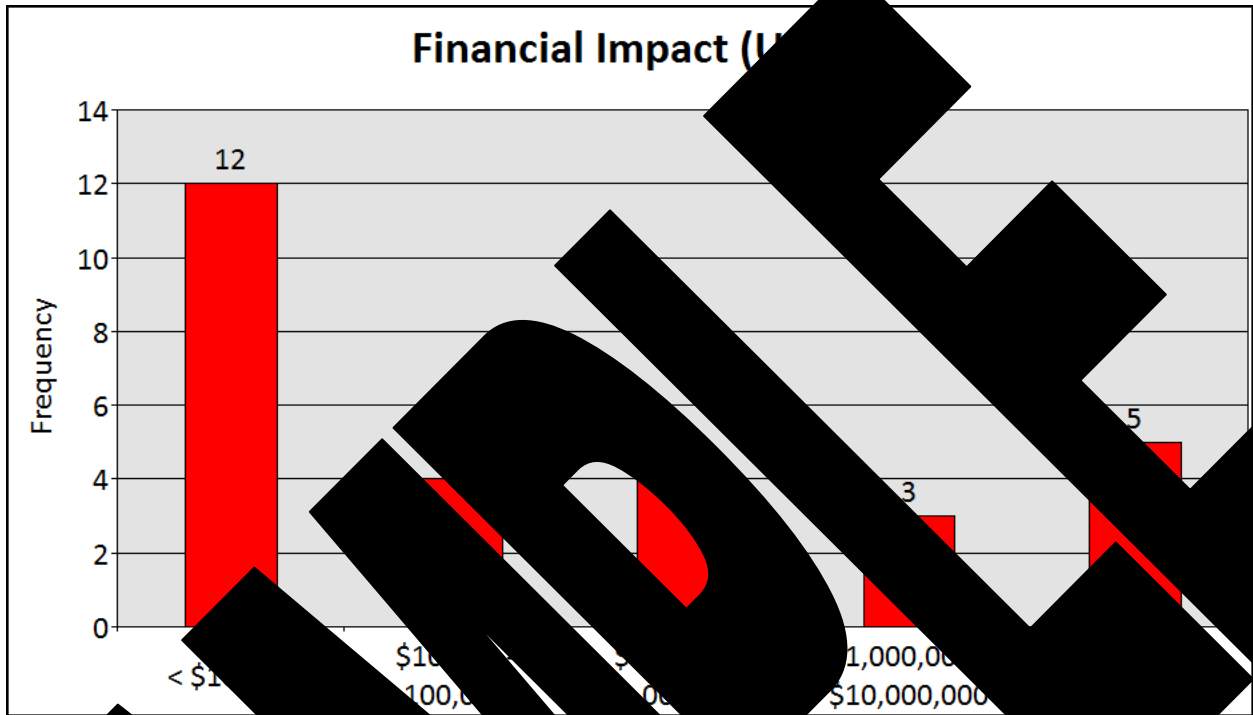


Figure 1. Financial Impact (US)

Figure 1 shows the financial impact of material security incidents in the US.

In the US, 12 incidents were reported with no financial impact. Data for the remaining incidents show that the greatest number of incidents with financial impact was in the range of \$100,000 to \$1,000,000. The number of incidents with financial impact exceeding \$10,000,000 was 5.

### Financial Impact Percentages (USA)

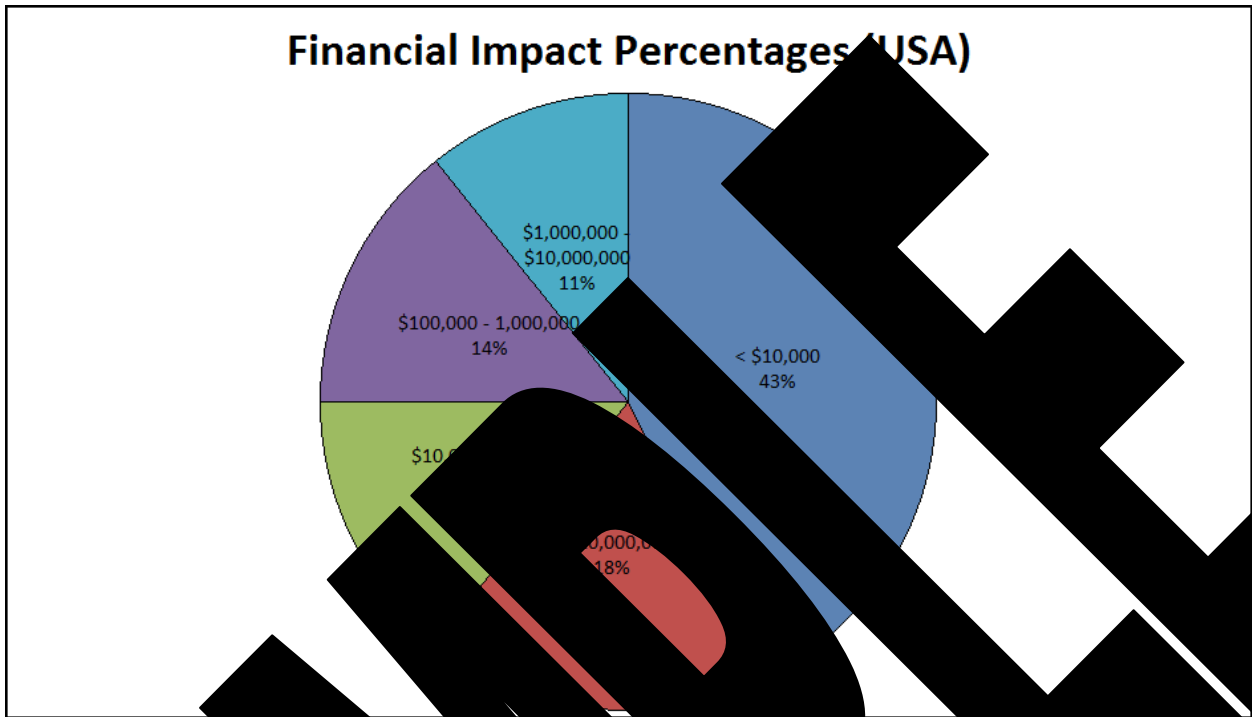


Figure 2.9-4: Financial Impact Percentages (USA)

Figure 2.9-4 shows the financial impact of all US security incidents in the US by percentage. The chart shows that 43% of all incidents have a financial impact of less than \$10,000.

Thirty-nine percent of the incidents in the US had a financial impact of \$10,000 or less, down by 11 percentage points from 2Q2008. The chart also shows that 18% of all incidents had a financial impact between \$10,000 and \$100,000, up from 14% in 2Q2008. Forty-nine percent of all incidents had a financial impact of more than \$100,000.

### Financial Impact by Industry

Industry	< \$10,000	\$10,000 - \$100,000	\$100,000 - \$1,000,000	\$1,000,000 - \$10,000,000	> \$10,000,000	Grand Total
Food & Beverage	1	1	2			19
Water	2		1			14
Power and Energy	1	1	2			10
Chemical			1			6
Transportation		1			3	4
Other				1		4
Food & Beverage	1	2	1			4
Pulp and Paper	2	1				3
General Manufacturing		1				2
Electronic Manufacturing		1			1	2
Metals	1					1
Pharmaceutical				1		1
<b>Grand Total</b>	<b>8</b>	<b>26</b>	<b>14</b>	<b>8</b>	<b>5</b>	<b>70</b>

Table 2.9-2: Financial Impact by Industry (Global)

Table 2.9-2 shows the financial impact on specific industries globally.

The industries suffering the greatest financial impact are Petroleum, Power & Utilities and Transportation. These industries suffered at least one incident exceeding \$10,000,000. Electronic Manufacturing and Water/Waste Water had one incident resulting in costs over \$10,000,000. One incident was reported since 2Q2009 that exceed \$10,000,000 losses in transportation.

IndustryType	< \$10,000	\$10,000 - 100,000	\$100,000 - 1,000,000	> 1,000,000	Grand Total
Petroleum	6			1	7
Power and Utilities	1	2		1	6
Water/Waste Water	3	2		1	6
Food & Beverage			2		3
Chemical	1				2
Other	1				1
Transportation				1	1
Pharmaceutical				1	1
Electronic Manufacturing				1	1
Grand Total	3			2	2

Table 2.9-3 Financial Impact by Industry Type

Table 2.9-3 shows the financial impact of security incidents by industry type. The industries in the US that suffered the greatest financial impact are Petroleum, Power & Utilities, Water/Waste Water, and Transportation. Petroleum, Power & Utilities, and Water/Waste Water have suffered the most incidents in costs exceeding \$10,000,000.

## 2.10 Production and Downtime Impact

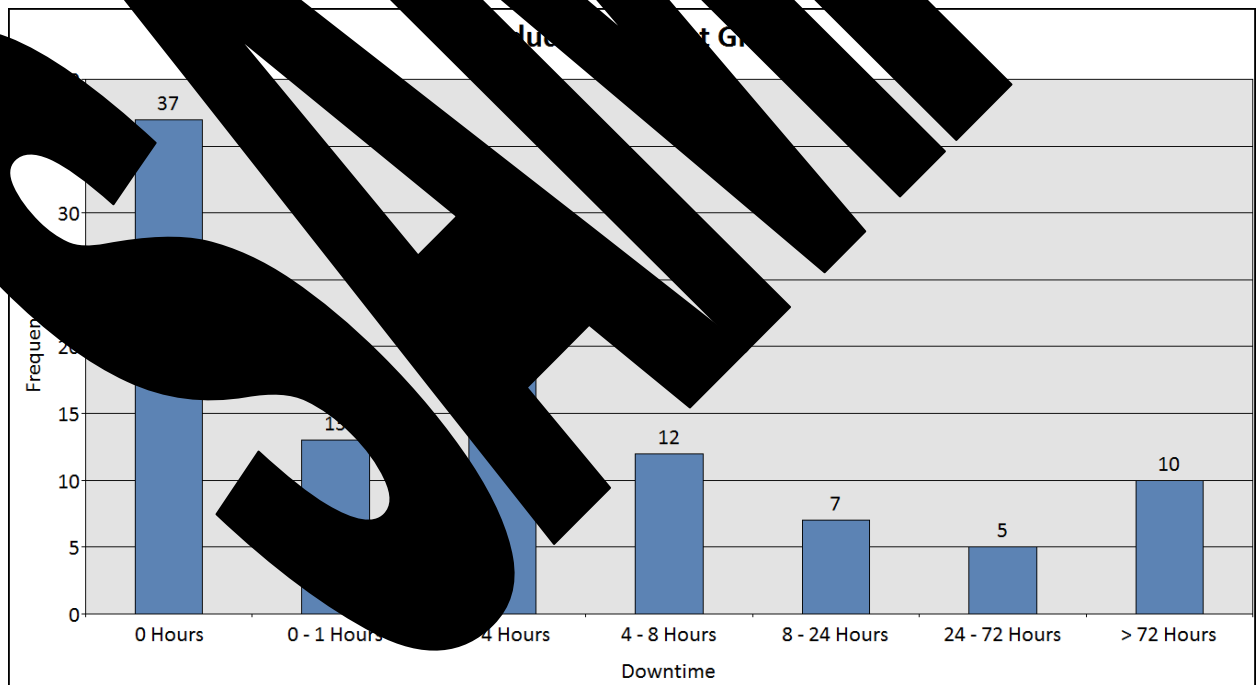


Figure 2.10-1: Production Impact (Global)

Figure 2.10-1 shows the effect of industrial security incidents on production. The incidence frequency is plotted against downtime.

The production downtime was not always known. When a downtime was reported, the number of downtime hours reported most frequently was zero followed by 1-72 hours. There were 10 incidents that resulted in downtime exceeding 72 hours.

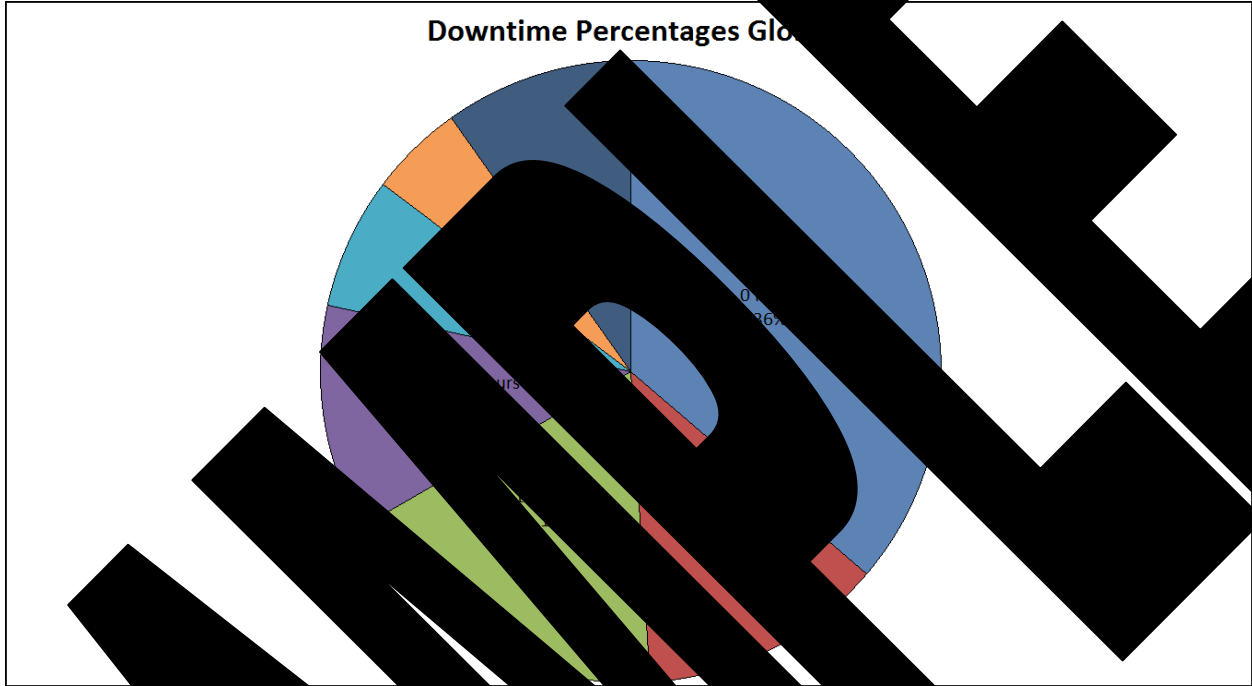


Figure 2.10-2: Downtime Percentages Global

Figure 2.10-2 shows the production downtime percentages for the world.

In some cases, the downtime was known, but the downtime reported due to the incident that does not translate to financial or loss of employee time. In many cases, production continued, with software updates being applied.

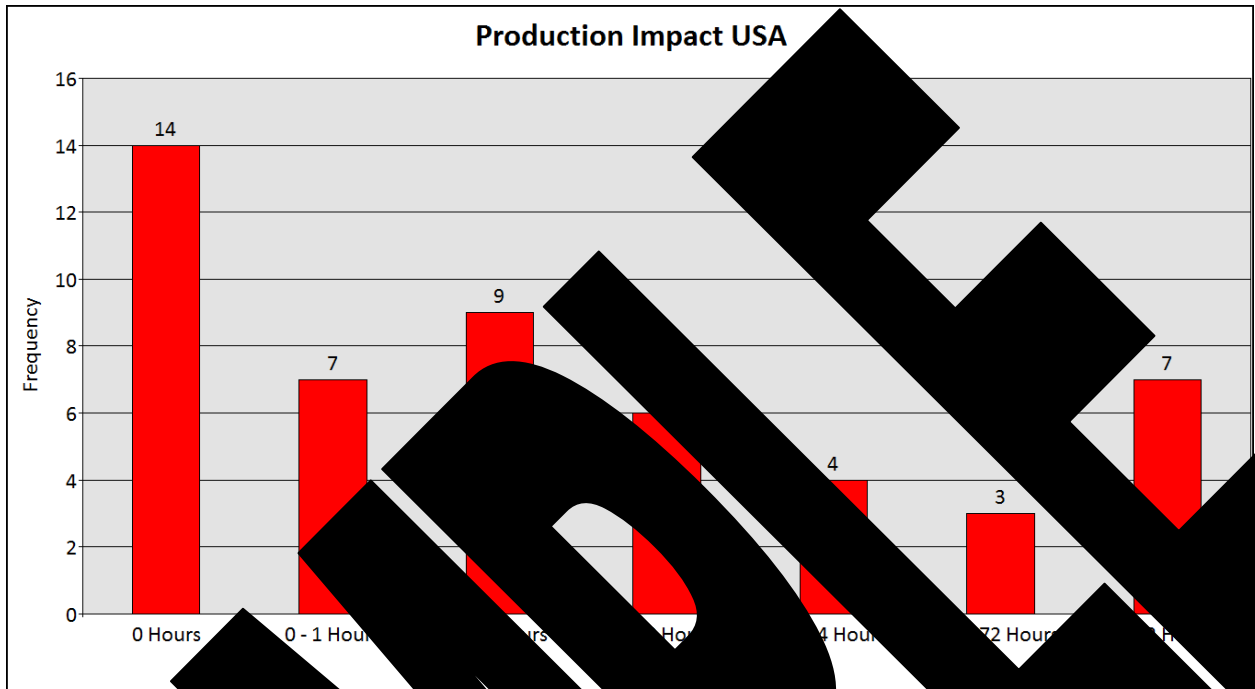


Figure 2.10-3: Production Impact (USA)

Figure 2.10-3 shows the number of US production incidents on production downtime frequency plotted against hours.

When compared to known production downtime in the US, the most downtime most frequently followed by a range of 1 to 4 hours. Production downtime is a major or not known in many cases, there are other reasons for the other frequency of downtime. The most employee time as well as other reasons for downtime are also into production.

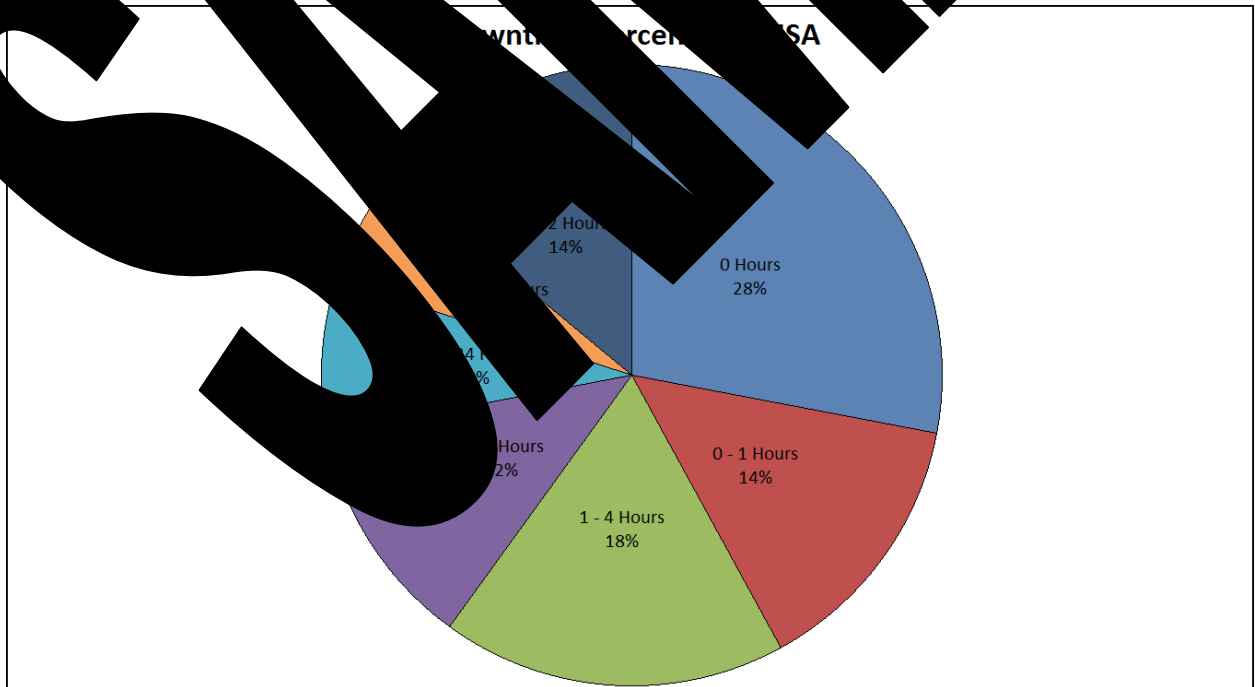


Figure 2.10-4: Production Downtime Percentages (USA)

Figure 2.10-4 shows the production downtime percentages in the US.

When downtime was known, the percentage of incidents resulting in less than 1 hour of downtime was 42%, down 4 percentage points from 2Q2009. 42% of incidents resulted in at least 1 hour of downtime. This is alarming due to the fact that production loss can translate into significant financial loss or serious safety issues depending on the equipment involved and the regulated processes.

**SAMPLE**

### 3 Recent Incidents

#### 3.1 Summary of Most Recent Incidents

Eleven new incidents were researched and entered into RISI. The following charts and tables provide a summary of the most pertinent facts regarding these incidents:



Figure 3.1-1: Location of Recent Incidents

IndustryType	\$10,000 - \$20,000	\$20,000 - \$50,000	\$50,000 - \$100,000	Grand Total
Waste Water	4	0	0	6
Utilities	0	0	0	2
Other	0	0	1	1
Grand Total	1	0	1	10

Figure 3.1-2: Incident by Industry Type



Figure 3.1-2: Location of Incident

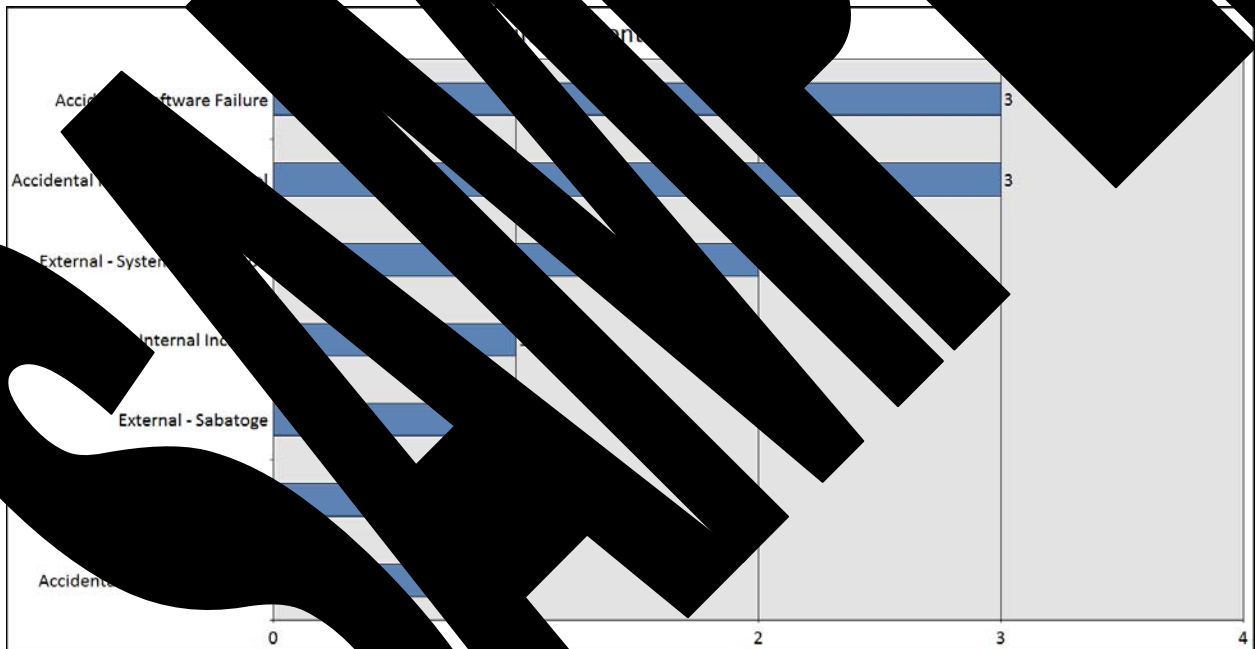


Figure 3.1-3: Incident Type of Most Accidents

### 3.2 Details of Accidents

The following are details of accidents added to RISI during the 3<sup>rd</sup> Quarter of 2009.

#### 3.2.1 INCIDENT ID#: 155

**TITLE:** Computer Glitch Causes 7 Water Mains to Break



The sewage pump stations at Austin Run and Potomac Hills overflowed due to lightning strikes that disabled the flow transducers at both stations. The pump transducers control the pumps that move effluent from the wells to the Aquia treatment center.

The Austin Run station overflowed approximately 2.5 million gallons into Austin Run and Aquia Creek. The Potomac Hills station overflowed approximately 1,000,000 gallons into Aquia Creek. The overflow volumes were higher than normal because the flow transducers for these two stations malfunctioned and did not activate the station alarms. The Aquia plant operators were not aware of the overflow because the alarms did not activate. The overflows were discovered when mechanics rebooted the telemetry system 2 days later.

**IMPACT:**

The Austin Run station overflowed approximately 2.5 million gallons into Austin Run and Aquia Creek. The Potomac Hills station overflowed approximately 1,000,000 gallons into Aquia Creek.

**FOLLOW-UP WORK:**

Stations repaired, and staff is working on the telemetry system to determine how to prevent another malfunction. Staff spent 2 days on the analysis of the spill.

**REFERENCES:**

**3.2.4 INCIDENT ID: 158**

**TITLE:** Sewage Spill Shows Flow Meter Malfunction

**DATE of EVENT:** 5/2/2007

**DESCRIPTION:**

On June 2, 2007, a pump station overflowed pens... flow... the Truro Works... continued to fill... June 3, 2007, when... Truro River. The charges... not reported until 3 days after the...

**IMPACT:**

Sewage in Truro... for 12 days. The local fish... 3,215.

**FOLLOW-UP WORK:**

**REFERENCES:**

**3.2.5 INCIDENT ID: 159**

**TITLE:** Computer Glitch in Neighborhood

**DATE of EVENT:** 9/19/2009

**DESCRIPTION:**

A computer glitch caused pumps on the city's water tank failed to shut down when the tank was full. The electronic equipment used to monitor the tank gave a false reading when the tank was

full. The pump produces 7,000 gallons per minute. Tens of thousands of gallons of water, mud and rocks rushed through a Cedar Hills neighborhood. The flood channel channel, built by the city, was clogged which caused water to go onto the lawn and driveway of the residential home affected. The glitch may have been caused by a brief electrical spike the night before the flood.

**IMPACT:**

Tens of thousands of gallons of water, mud and rocks shot mountainside into the Cedar Hills neighborhood causing minimal damage to one

**FOLLOW-UP WORK:**

**REFERENCES:**

**3.2.6 INCIDENT ID#: 160**

**TITLE:** Computer Failure Causes

**DATE of EVENT:** 6/1/2009

**DESCRIPTION:**

The Air France flight 447 crashed into the Atlantic Ocean. The black boxes were not recovered but based on physical evidence and maintenance records, it is believed that a faulty system was causing a sensor to be sweeping computer. The Airbus A330-300 crashed into the Atlantic Ocean on the morning of June 1, 2009.

**IMPACT:**

The Air France flight 447 crashed into the Atlantic Ocean. All 300 passengers were killed.

**FOLLOW-UP WORK:**

**REFERENCES:**

**3.2.6 INCIDENT ID#: 161**

Faulty software caused the Torrens Weir to open without warning. The gates

**DATE of EVENT:** 2009

**DESCR**

Faulty software caused the Torrens Weir to open without warning. The gates remained open for about two hours, dumping millions of liters of water from the lake. An investigation revealed that alarm that would alert remote operators of a malfunction were muted. The faulty software was developed by Ottoway System Integration, an Adelaide-based firm which went out of business days after the incident. There was no evidence of foul play.

**IMPACT:**

The Torrens Lake was drained. The water levels dropped by more than two meters. The muddy lake bottom contained large amounts of debris. The incident caused a problem for businesses



**DESCRIPTION:**

A virus attack on Integral Energy's computer network forced the company to restructure all of its 1,000 desktops. Eternal security experts were called in to rebuild all of the desktop computers to contain and remove the virus. The malware had not affected the power grid. Chris Gatford a security consultant from Hacklabs had conducted penetration testing on critical infrastructure said there was often "ineffective segregation" or "more typically" between the IT network and the network that monitors and controls the infrastructure. A spokesperson from Integral Energy stressed that the virus attacks Microsoft products and the network doesn't run on Microsoft and there was no way that the virus could make its way to the grid.

The virus was the W32 Virut.CF strain which has been described as a particularly "stealthy" computer file infector" that spreads quickly and is considered difficult to remove. Computer networks were protected by a Symantec security system, a source said. The Symantec website states that the virus installs a back door allowing hackers to issue commands to infected machines via an internet relay chat system. According to Gatford, the Symantec software was not updated in a timely manner and the Symantec product failed to detect it.

Integral Energy supplies electricity to the Sydney area and a portion of New South Wales distributing electricity to 2.2 million people in NSW.

**IMPACT:**

Integral Energy's computer network was infected with the W32 Virut.CF virus and desktop computers were rebuilt.

**FOLLOW UP WORK:**

Integral Energy rolled in a replacement of desktop computers. The company put in place recovery plans to eliminate any virus on public systems. An investigation is underway to determine the cause of the incident and develop strategies to minimize risk in the future.

**REFERENCES:**

**2.10 INCIDENT ID: 164**

Computer

DATE: 09/09/09

**DESCRIPTION:**

An estimated 700,000 gallons of wastewater overflowed from a pumping station on Sisson Street into the Jones Falls. The overflow was not a concern to the public because a screen filtered any macropollutants from the overflow. The overflow was the result of a malfunctioning automatic control system that controls electricity to the station's pumps. City officials are not sure of the cause of this malfunction, but think a design flaw contributed to water backing up in the station. Public works employees opened a valve and allowed the waste water to flow out so that the station would not be damaged.

A spokesman for the Baltimore City Department of Public Works, Kurt Kocher, said this type of overflow is uncommon.

**IMPACT:**

An estimated 700,000 gallons of waste water overflowed from the pumping station into the Jones Falls. There was no "visible" pollution of the Jones Falls because the waste water was filtered of any macropollutants. However, public notice of the overflow was spread along the Jones Falls. The pumping station was being refurbished.

**FOLLOW-UP WORK:**

**REFERENCES:**

**3.2.11 INCIDENT ID#: 165**

**TITLE:** Automated Antiaircraft Cannon Malfunction Kills 9, Wounds 14

**DATE of EVENT:** 10/12/2007

**DESCRIPTION:**

A software glitch is being blamed for an antiaircraft cannon malfunction that killed 9 soldiers and seriously injured 14 others during a simulated exercise. The malfunction is not yet known. The South African National Defence Force is investigating whether a software glitch was the cause. The antiaircraft cannon, an Oerlikon GDF, which has been characterized as fire uncontrollably.

**IMPACT:**

Computerized weapon fire uncontrollably killed 9 soldiers and seriously injured 14 others. A computer glitch was the cause of the malfunction, though the possibility of mechanical failure has not been ruled out.

**FOLLOW-UP:**

**REFERENCES:**



Licensed to Client Company on 30 November 2009. Distribution restricted to employees of Client Company.

## 4 Looking Ahead

While the adoption of commercial technology into control systems has been pervasive over the last 15 years, the reality is that majority of the installed base of industrial automation and control equipment has not yet been upgraded. Worldwide, the ARC Advisory Group estimates there is an ageing installed base of process automation systems reaching the end of their useful life, which in many cases can exceed 25 years, that is valued at \$1.5 trillion<sup>1</sup>. This number gets bigger with each passing year as many manufacturers, particularly small to mid range manufacturers, are facing serious challenges as to how to deal with their installed base. As these systems are upgraded with new technology they introduce the vulnerabilities associated with open system technology.

This observation raises the importance of educating automation equipment users on how to improve the intrinsic security of their automation systems and on control system design best practices.

---

<sup>1</sup> "2007 Marks Another Strong Year for Industrial Automation," ARC Advisory Group, 2008, [http://www.arcweb.com/press\\_releases/press\\_releases/Posts/2007%20marks%20another%20strong%20year%20for%20industrial%20automation%20-%20ARC%20Advisory%20Group%20-%202008](http://www.arcweb.com/press_releases/press_releases/Posts/2007%20marks%20another%20strong%20year%20for%20industrial%20automation%20-%20ARC%20Advisory%20Group%20-%202008), 53

**DRAFT**

## 5 Contributors

E. Byres	Chief Technology Officer	Research Inc.
D. Riggio	Cyber Security Research Analyst	LLC
J. Pancio	Research Assistant	Exida LLC
R. Amkreutz	Research Assistant	Exida LLC
J. Cusimano	Research Assistant	Byres Research Inc.

SAMPLE

Licensed to Client Company on 30 November 2009. Distribution restricted to employees of Client Company.

## 6 Revision History

Revision	Date	Author(s)	Description
1.0	November 30, 2009	J. Cusimano	Issued at Rev. 1

**SAMPLE**