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.

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.

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.

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.

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.

![Figure 2.8-7: Incidents Resulting in Significant Harm](Image)
# 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
# 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 for critical industrial processes. Heavy use of commercial technologies, such as Windows, SQL and Ethernet, leaves control systems vulnerable to the same viruses, worms and Trojans that impact office environments. Increasing remote and 24/7 system access translates to more connections. With the increase in the sophistication and seriousness of some recent incidents, plant operators face growing pressures to develop security programs for their plant.

The Repository for Industrial Security Incidents (RISI) records incidents of a cyber security nature that directly affect industrial Supervisory Control and Data Acquisition (SCADA) and process control systems. This includes accidental cyber-related incidents, as well as deliberate events such as external hacking and denial-of-service (DoS) attacks, and virus and worm infiltrations. It is the largest known collection of incidents of this type. Data is collected from private submissions by member companies and through research into publicly reported incidents.

Each of the incidents has been rigorously investigated. Sensitive information has been removed to protect the confidentiality of the reporters. Records are indexed according to the types of critical industrial systems and the type of incident, and cannot be linked to the company and the individuals that cannot be linked to the individuals.

At the end of the third quarter of 2009, the RISI database contained a total of 164 records. RISI provides information that can be used to formulate a security plan. Furthermore, understanding how other incidents occurred can help prevent future attacks.

1.1 Structure of the Report

The analysis of the repository is at the level of each incident. The types of incidents and the people who committed them, the methods and tactics they used to gain entry, the results they achieved versus the results they were attempting to achieve, the financial and operational impact on the “victims”, and the outcomes are detailed. This section provides an overview of the reasons analyzing the rate at which incidents occur, their geographic and industrial impact, the impact of incidents to date and finally best practices are summarized.

The report includes case studies from the most recent quarter that include descriptions of what happened, the impact of the attack, and what the company did to avoid future incidents.

1.2 Updates in this Report

Consistent with earlier RISI Analysis reports from 2009, this report presents numerous metrics using the entire data set of 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 Section 3: 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. With 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 164 records. However, the data reported in this report is limited to those incidents with a Reliability Rating of “Confirmed” or “Likely, but Unconfirmed.” “Unknown or Unlikely” or “Hoax/Urban Legend” incidents were excluded from the analysis. The data set included in the analysis contains 152 incidents.

The RISI database structure was enhanced in April 2009 and again in October 2009 to aid in analysis and reporting. Upon completion, existing data was carefully reviewed.

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

![Incidents by World Region](image)

North American incidents account for 60% of all confirmed or likely incidents in RISI. Incidents in Europe account for 27%.
When a distribution of incidents by country is examined, as shown in Figure 2.1-2, the United States shows the highest number of incidents followed by the United Kingdom and Canada. Since half of the incidents occurred in the US, for the remainder of the report, data will be presented both globally and specifically for the US.
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.

![Incidents by Year Graph](image)

Figure 2.2-1: Incidents by Year shows the number of incidents that occurred every year since 1982. The data illustrates some notable trends. First, a steady increase in events in the late 90's can be observed followed by a spike in the early 2000's. The annual rate declines in the mid-2000's before rising again in the last 2006.

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 steadily over the last 20 years.

It should be 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.
Figure 2.2-2: Number of Incidents Occurring Globally (5 Year Intervals)

Figure 2.2-2 shows the same annual incident data but plotted in five year intervals. In this view, the number of incidents peaked in the period between 1999 and 2003 while the number of incidents in the subsequent period is approximately equal.
Figure 2.2-3 shows the number of incidents occurring in the US. Since nearly half of the incidents are in the US, it is not surprising that the trend in the US mirrors the global trend.

### 2.3 Industry

Incidents in RISI are assigned to one of the following list of industry types:

- Aerospace
- Automotive
- Chemical
- Electronic Manufacturing
- Food & Beverage
- General Manufacturing
- Metals
- Mining
- Other
- Petroleum
- Pharmaceutical
- 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.

<table>
<thead>
<tr>
<th>Critical Infrastructure and Key Resources (CIKR) Sectors</th>
<th>Industry Types</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agriculture and Food</td>
<td>Food</td>
</tr>
<tr>
<td>Banking and Finance</td>
<td></td>
</tr>
<tr>
<td>Chemical</td>
<td>Chemical</td>
</tr>
<tr>
<td>Commercial Facilities</td>
<td></td>
</tr>
<tr>
<td>Communications</td>
<td></td>
</tr>
<tr>
<td>Critical Manufacturing</td>
<td></td>
</tr>
<tr>
<td>Critical Manufacturing</td>
<td></td>
</tr>
<tr>
<td>Critical Manufacturing</td>
<td></td>
</tr>
<tr>
<td>Energy</td>
<td></td>
</tr>
<tr>
<td>Energy</td>
<td></td>
</tr>
<tr>
<td>Government Facilities</td>
<td></td>
</tr>
<tr>
<td>Government Facilities</td>
<td></td>
</tr>
<tr>
<td>Healthcare</td>
<td></td>
</tr>
<tr>
<td>Healthcare</td>
<td></td>
</tr>
<tr>
<td>Healthcare</td>
<td></td>
</tr>
<tr>
<td>Information</td>
<td></td>
</tr>
<tr>
<td>Information</td>
<td></td>
</tr>
<tr>
<td>Information</td>
<td></td>
</tr>
<tr>
<td>National Monuments and Icons</td>
<td></td>
</tr>
<tr>
<td>National Monuments and Icons</td>
<td></td>
</tr>
<tr>
<td>National Monuments and Icons</td>
<td></td>
</tr>
<tr>
<td>Natural Monuments and Icons</td>
<td></td>
</tr>
<tr>
<td>Natural Monuments and Icons</td>
<td></td>
</tr>
<tr>
<td>Natural Monuments and Icons</td>
<td></td>
</tr>
<tr>
<td>Postal and Shipping</td>
<td></td>
</tr>
<tr>
<td>Postal and Shipping</td>
<td></td>
</tr>
<tr>
<td>Postal and Shipping</td>
<td></td>
</tr>
<tr>
<td>Transportation Systems</td>
<td></td>
</tr>
<tr>
<td>Transportation Systems</td>
<td></td>
</tr>
<tr>
<td>Transportation Systems</td>
<td></td>
</tr>
<tr>
<td>Water/Waste Water</td>
<td></td>
</tr>
<tr>
<td>Water/Waste Water</td>
<td></td>
</tr>
<tr>
<td>Water/Waste Water</td>
<td></td>
</tr>
</tbody>
</table>

Occasionally, for confidentiality reasons an incident submitter may withhold this information and in those cases the Industry Type will be recorded as “Unknown”.

### 2.3.1 Incidents by Industry Type and Geography
Figure 2.3-1: Incidents by Industry Type

Figure 2.3-1 is a chart showing the Industry Type and the corresponding incidents in the data set.

Globally, Petroleum, Power & Utilities, as well as Transportation, are the industries with the highest numbers of industrial security incidents. There were ten incidents with the industry reported as unknown.
Table 2.3-2: Industry Type by Time Period

<table>
<thead>
<tr>
<th>Industry Type</th>
<th>1999-2003</th>
<th>2004-2008</th>
<th>% Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Petroleum</td>
<td>18</td>
<td>5</td>
<td>-72%</td>
</tr>
<tr>
<td>Transportation</td>
<td>8</td>
<td>6</td>
<td>-25%</td>
</tr>
<tr>
<td>Chemical</td>
<td>5</td>
<td>4</td>
<td>-20%</td>
</tr>
<tr>
<td>Power &amp; Utilities</td>
<td>10</td>
<td>12</td>
<td>20%</td>
</tr>
<tr>
<td>Water/Waste Water</td>
<td>4</td>
<td>8</td>
<td>100%</td>
</tr>
<tr>
<td>Food &amp; Beverage</td>
<td>3</td>
<td>6</td>
<td>100%</td>
</tr>
</tbody>
</table>

Table 2.3-2: Industry Type by Time Period looks at the top 6 industry types reported for incidents occurring in the USA between 1999 and 2003 and again for the five year period between 2004 and 2008. The 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
dropped during the same time period. Going the other direction, Water/Waste Water, Food & Beverage and Power & Utilities all experienced increases, some quite dramatic.

While it is difficult to say with certainty, it is possible that the drop in petroleum and chemical industry incidents is at least in part due to the proactive response these industries and their control system suppliers have taken to addressing control system cyber security.

2.4 Incident Type

RISI incidents are also assigned to a couple of general categories as well as to one or more specific incident types from the list in Table 2.4-1: Specific Incident Types:

The first general category is the called the “General Intent”. “General Intent” can be either Intentional or Unintentional.

The second general category is “General Perpetrator Type”. General Perpetrator Type can be Insider, Outsider or Not Applicable. “Not Applicable” is used for non-targeted incidents such as accidental equipment or software failures.

| Specific Incident Type | Accidental Equipment Failure | Accidental Inappropriate Control Incident | Accidental Incident | Accidental Network Failure | Accidental Software Failure | Audit External - Denial of Service (DoS) | Audit External - Fraud | Audit External - Information Theft | Audit External - Sabotage | Audit External - System Penetration | Audit External - Virus/Trojan/Worm | Audit External Incident | Audit Internal - Insider Fraud | Audit Internal - Non-Authorized Access | Audit Internal - Sabotage | Audit Other Incident | Other Incident | Unknown |
|------------------------|------------------------------|------------------------------------------|--------------------|----------------------------|---------------------------|--------------------------------------|-------------------|-----------------------------------|----------------------|----------------------------------|-----------------------------------|----------------------|-----------------------------|----------------------------------|----------------------|-----------------|----------|

Table 2.4-1: Specific Incident Types
2.4.1 General Incident Classification

Figure 2.4-1 is a stacked bar chart showing the distribution of General Intent for all incidents globally as well as the breakdown of General Perpetrator Type for both Intentional and Unintentional Incidents. This 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 threats 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: Incidents Categorized by General Incident Type

Figure 2.4-2 is a stacked bar chart showing the distribution of General Intent for all incidents as well as the breakdown by General Intention for both Intentional and Unintentional Incidents. However, the chart illustrates events occurring in the USA.

One striking difference between the data is that globally the largest percentage is unintentional N/A incidents (incidents caused by accidental equipment or software failures), whereas in the USA and among unintentional incidents, it is primarily non-directed malware such as viruses, worms, and trojans. The percentage of intentional incidents and the breakdown of them is in contrast with the global data.

2.4.2 Specific Incident Classification

A potential conclusion one could draw from this is that US industrial plants are doing a slightly better job at protecting their control systems from malware.

Figure 2.4-3 and Figure 2.4-4 summarize 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 malware (viruses, trojans, worms, etc.) was the incident type most often seen globally followed by accidental equipment failure. Accidental network failure and external system penetration were nearly equal in frequency. Refer to the recommendation section for commentary and suggestions on how many of the most common incident types could be 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

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

Table 2.4-2: Incident Type by Time Period. The table reports on the number of incidents occurring over the five-year period between 1999 and 2003 and again for the period between 2004 and 2008. Both periods had approximately 60 incidents.

Significant differences in the number of different incident type were observed between the earlier and more recent data. The most obvious difference is that incidents involving external sabotage, denial of service and system penetration are considerably down in the last five years (2004 to 2008) in comparison to the earlier 5 years (1999 to 2003). On the contrary, incidents involving unauthorized access or sabotage by internal sources are considerably up in the same period. There is a pattern on the rise in incidents involving accidental hardware, software and network failures and accidental inappropriate control.

The number of incidents caused by malware (viruses, worms, trojans, etc.) has remained relatively constant over time underscoring the need for operators of industrial automation and control system equipment to be more diligent in installing and maintaining good virus protection software on their PC based control system equipment.

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 the systems against these threats will also serve to strengthen systems against external actors should their threat increase in the future.
2.5 Perpetrator Type and Detection Method

2.5.1 Perpetrator Type

As noted in section 2.3, the General Perpetrator Type (Insider, Outsider, N/A) type is recorded for each incidents. In addition, if known, RISI also records further specifics on the perpetrator for each incident per the options in Table 2.5-1: Specific Perpetrator Type.

<table>
<thead>
<tr>
<th>Perpetrator Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insider - Current Employee</td>
</tr>
<tr>
<td>Insider - Former Employee</td>
</tr>
<tr>
<td>Insider - Current Contractor</td>
</tr>
<tr>
<td>Insider - Former Contractor</td>
</tr>
<tr>
<td>Outsider - General</td>
</tr>
<tr>
<td>None</td>
</tr>
<tr>
<td>Other</td>
</tr>
<tr>
<td>Insider - General</td>
</tr>
<tr>
<td>Outsider - Agencies/Foreign State</td>
</tr>
<tr>
<td>Outsider - Terrorist</td>
</tr>
<tr>
<td>Outsider - Activists</td>
</tr>
<tr>
<td>Outsider - Hacker/Virus Writer</td>
</tr>
<tr>
<td>Outsider - Script Kiddie</td>
</tr>
<tr>
<td>Unknown</td>
</tr>
<tr>
<td>Insider - Former Contractor</td>
</tr>
<tr>
<td>Insider - Current Contractor</td>
</tr>
<tr>
<td>Insider - Former Contractor</td>
</tr>
<tr>
<td>Outsider - Competitor</td>
</tr>
</tbody>
</table>

Table 2.5-1: Specific Perpetrator Type
shows the specific perpetrator types globally.

As shown in Figure 2.5-1, the dominant perpetrator type is the Hacker/Virus Writer, which accounts for 65% of all incidents. Current Insiders (current employees) make up 28% of all known perpetrators involved in security incidents. While some of these incidents were caused by accidentally introducing a virus into the control system or by honest mistakes, a significant portion of incidents involving Current Insiders were intentional. The perpetrators included exfiltration of sensitive data, sabotage, stealing/TP-IDMs, forming botnets, and exploiting system penetration.

In the case of Former Insiders (former employees), the situation is somewhat different. Former Insiders were responsible for 6% of all known incidents. However, in these cases, all incidents were deliberate. Former Insider incidents included:
- sabotage
- denial of service
- unauthorized access

This data suggests that operating companies must take significant steps to prevent terminated employees and contractors from gaining access to systems, especially the systems that they supported while active.
Figure 2.5-2: Specific Perpetrator Type (USA)

The data generally mirrors the global trend.

2.5.2 Detection Method

All events are recorded with the method by which the event was detected. Available selections include:

- **Internal Staff**
- **Security Device/Log Alert**
- **Incident During**
- **Incident After**
- **Security Consultant/Investigator**
- **Outside Agency/Non-**
Figure 2.5-3 shows a summary the methods by which incidents were detected globally.

![Graph showing detection methods]
Figure 2.5-4 shows a summary of the methods by which incidents were detected in the US.

As with the global data, most incidents were detected by internal control or operating staff during the incident.

2.6 Method and Point of Entry

Whenever possible, the method and point of entry were recorded for each incident. The following are the available methods and points of entry for selection.

- Local
  - Local - Business Network
  - Local - Communications Channel Media
  - Local - Human Machine Interface (HMI)
  - Local - Laptop
  - Local - Physical Access to Equipment
  - Local - Programming Terminal
  - Local - Remote Access Terminal

- Remote
  - Remote - Corporate WAN
  - Remote - Dial-up Modem
  - Remote - Internet Directly
  - Remote - SCADA Network
  - Remote - Telco Network
  - Remote - Trusted 3rd Party Connection
  - Remote - Via Business Network
  - Remote - VPN Connection
- Remote - Wireless System
- Remote Access

- None
- Other
- Unknown

Figure 2.6-1: General Access Method (Global)

Figure 2.6-1 shows the general method of access into affected systems recorded globally. Remote access, at 42%, is the primary method of entry into industrial control systems. While not surprising, this is important to the assertion that the networking of industrial automation and control systems has made these systems more vulnerable to cyber security incidents. Local access, at 28%, is significant because...
Figure 2.6-2: Point of Entry (Global)

Figure 2.6-2 shows the detailed information on the types of entry into industrial control systems.

In many cases, the point of entry was documented as "none" or "unknown". However, the most frequent entry points were access through the Business Network, either remotely or locally. Interestingly, the data shows that access through the Business Network is significantly higher than through direct connection to the Internet. This data supports the warnings by control system security experts that systems without a direct internet connection are still susceptible to cyber security incidents.
Figure 2.6-3: General Access Method (USA)

Figure 2.6-3 shows the general method of access into affected systems in the USA. Similar to the global data, remote access, at 47%, is the primary method of entry into industrial data and security systems. However, it is slightly higher than globally, accounting for just over half of all incidents.
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. Often times multiple pieces of equipment are involved so the total number of pieces of equipment involved will exceed the total number of incidents.

Figure 2.7-1: Equipment Involved (Global)

Figure 2.7-1 shows the type of equipment affected in industrial security incidents globally. The equipment most often involved in security incidents are Programmable Logic Controllers (PLC) and Distributed Control Systems (DCS). This is not surprising but some of the other types of equipment involved, such as HMI’s, servers and RTU’s might be.
Figure 2.7-2 shows the type of equipment involved in industrial security incidents in the US. PLC’s are involved most often in industrial security incidents in the US, followed by SCADA masters and controllers.

Protocols Involved

When known, the types of protocols involved are recorded for each incident.
Figure 2.7-3: Protocol (Global)

Figure 2.7-3 shows the frequency of incidents by protocol used. In many cases the protocol is unknown. When the protocol is known, TCP/IP is most frequently reported.
Figure 2.7-4: Protocol (USA)

Figure 2.7-4 shows the number of reported US incidents by protocol used.

Again, there were many incidents where the protocol was unknown. When the protocol was known, the one most-often reported was TCP/IP followed by AB PCCC/DF1 (also known as Data Highway Plus).

2.8 Results

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

- Environmental Spill
- Equipment Damage or Loss
- Loss/Contamination of Product
- Loss of Production/Operation
- Loss of Data
- Loss of Equipment Control
- Loss of Equipment
- Unknown
- Loss of View
- None
- Intellectual Property Theft
- Fraud
- Injury or Death
Often the outcome (achieved result) does not match the intended result (attempted result). Therefore, both the attempted and the achieved results are recorded for all incidents. In many cases, more than one result was attempted and achieved. The data is presented as a total.

2.8.1 Attempted Results

Exhibit 2.8-1: Attempted Result (Global)

Figure 2.8-1 summarizes the attempted results for the incidents in the RISI database. Except those where the attempt was “None”, “Loss of production/operation” and “Illicit Use of Equipment” are the ones reported most often.
Figure 2.8-2 summarizes the recorded attempted results for the US incidents in the RISI database.

For the US data, when there was an attempted result, "Loss of production/operation" as well as "Illicit use of equipment" were among the most frequent results reported.

2.8.2 Achieved Results
The achieved results reported are very different than the attempted results. When "none" or "unknown" are excluded, "Loss of production/operation", "Loss of equipment control" and "Loss of view" are most frequently reported for achieved results.

In 9 cases, injury or death resulted from an incident, up 3 since 2Q2009.

---

**Figure 2.8-3: Achieved Result (Global)**

<table>
<thead>
<tr>
<th>Achieved Result</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loss of Production/Operation</td>
<td>53</td>
</tr>
<tr>
<td>Loss of Equipment Control</td>
<td>41</td>
</tr>
<tr>
<td>Loss of View</td>
<td></td>
</tr>
<tr>
<td>Loss of Staff Time</td>
<td></td>
</tr>
<tr>
<td>Loss of Communications</td>
<td>19</td>
</tr>
<tr>
<td>Unknown</td>
<td></td>
</tr>
<tr>
<td>Environmental Spill</td>
<td>7</td>
</tr>
<tr>
<td>Public Nuisance/Inconvenience</td>
<td>16</td>
</tr>
<tr>
<td>Injury or Death</td>
<td>16</td>
</tr>
<tr>
<td>Illicit Use of Equipment</td>
<td>16</td>
</tr>
<tr>
<td>Equipment Damage or Loss</td>
<td>16</td>
</tr>
<tr>
<td>Public Injury or Death</td>
<td>3</td>
</tr>
<tr>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Loss/Contamination of Product</td>
<td>2</td>
</tr>
<tr>
<td>Fine/Penalty</td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>

---

**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 incidents. One new incident involving public injury or death was reported this quarter.

### 2.8.3 Attempted versus Achieved Results

Figure 2.8-5 shows the comparison of attempted results to achieved results of reported incidents. The most striking feature of this plot is that far more was achieved than was known to be attempted. Most often, the attempted result is “Unknown” or “None” as is the case with accidents or malware. Most 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 a comparison of the attempted results to the achieved results of reported incidents.

US incidents show a trend similar to the global trend in which much more was achieved than was known to have been attempted. “Loss of production/operation”, “Loss of Equipment control” and “Loss of view” were among the top results achieved which can lead to disastrous outcomes. The data reviewed earlier indicated that the primary access point in the US is remote access with the leading cause of the external hacker/virus writer.

2.8.4 Incidents Resulting in Significant Harm

Incidents resulting in “Significant Harm” refers to those that caused harm to people, the environment or resulted in a significant financial impact. Specifically, 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 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](image)

This indicates that users of control systems need to be concerned not only with just intentional attacks, but also incidents that are unintentional. Accidents, equipment failure, and malware actually account for a large number of incidents.

### 5. Incident Result by Time Period

<table>
<thead>
<tr>
<th>Incident Result</th>
<th>1999-2003</th>
<th>2004-2008</th>
<th>% Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loss of Production/Operation</td>
<td>24</td>
<td>22</td>
<td>-50%</td>
</tr>
<tr>
<td>Loss of Equipment Control</td>
<td>15</td>
<td>16</td>
<td>7%</td>
</tr>
<tr>
<td>Equipment Damage or Loss</td>
<td>2</td>
<td>3</td>
<td>50%</td>
</tr>
<tr>
<td>Injury or Death</td>
<td>1</td>
<td>3</td>
<td>200%</td>
</tr>
<tr>
<td>Public Injury or Death</td>
<td>0</td>
<td>1</td>
<td>N/A</td>
</tr>
<tr>
<td>Loss/Contamination of Product</td>
<td>0</td>
<td>1</td>
<td>N/A</td>
</tr>
<tr>
<td>Fine/Penalty</td>
<td>0</td>
<td>2</td>
<td>N/A</td>
</tr>
</tbody>
</table>

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 exceeding $10,000 (36 incidents) is approximately equal to the total number of incidents with a financial impact exceeding that amount (37). However, there were 9 incidents resulting in a cost impact greater than $10,000,000, up from 8 reported in 2Q2009. The industries with the greatest financial impact were Petroleum, Power & Utilities and Transportation (see Table 2.9-2: Financial Impact by Industry (Global)).
Figure 2.9-2 shows the financial impact of industrial security incidents world-wide expressed as percentages. 38% of incidents reported resulted in a financial impact in the range of $1-$10,000. When incidents reported as having no financial impact are included, the percentage of incidents resulting in $0-$10,000 is 49%.

Table 2.9-1: Financial Impact by Time Period summarizes the financial impact of incidents 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.
Figure 2.9-3 shows the financial impact of industrial security incidents in the US.

In the US, there were no incidents that reported with no financial impact. Data for the remaining incidents shows that the greatest number of incidents where the financial impact was known fell into the range of $1-10,000. Five incidents in the US resulted in an impact exceeding $10,000,000.
Figure 2.9-4: Financial Impact Percentages (USA)

Figure 2.9-4 shows the financial impact of security incidents in the USA expressed as percentages.

Thirty-nine percent of the incidents in the USA resulted in costs totaling $10,000 or less, down by 11 percentage points since 2Q2009 indicating a shift to higher financial impact incidents.

Ninety-nine percent of the incidents were reported to incur costs over $10,000.

2.9.2 Financial Impact by Industry

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

<table>
<thead>
<tr>
<th>Industry Type</th>
<th>$0 - $10,000</th>
<th>$10,000 - $100,000</th>
<th>$100,000 - $1,000,000</th>
<th>&gt; $1,000,000</th>
<th>Grand Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Petroleum</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>19</td>
</tr>
<tr>
<td>Water/Waste</td>
<td>25</td>
<td>4</td>
<td>1</td>
<td>0</td>
<td>14</td>
</tr>
<tr>
<td>Power and Utilities</td>
<td>24</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>10</td>
</tr>
<tr>
<td>Chemical</td>
<td>13</td>
<td>1</td>
<td>6</td>
<td>0</td>
<td>6</td>
</tr>
<tr>
<td>Transportation</td>
<td>13</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>19</td>
</tr>
<tr>
<td>Other</td>
<td>12</td>
<td>2</td>
<td>1</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Food &amp; Beverage</td>
<td>12</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>Pulp and Paper</td>
<td>13</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>General Manufacturing</td>
<td>13</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>19</td>
</tr>
<tr>
<td>Electronic Manufacturing</td>
<td>12</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>19</td>
</tr>
<tr>
<td>Metals</td>
<td>12</td>
<td>1</td>
<td>1</td>
<td>4</td>
<td>19</td>
</tr>
<tr>
<td>Pharmaceutical</td>
<td>12</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>19</td>
</tr>
<tr>
<td>Grand Total</td>
<td>82</td>
<td>6</td>
<td>14</td>
<td>8</td>
<td>70</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Industry Type</th>
<th>&lt; $10,000</th>
<th>$10,000 - $100,000</th>
<th>$100,000 - $1,000,000</th>
<th>&gt; $1,000,000</th>
<th>Grand Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Petroleum</td>
<td>6</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>7</td>
</tr>
<tr>
<td>Power and Utilities</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>6</td>
</tr>
<tr>
<td>Water/Waste Water</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>6</td>
</tr>
<tr>
<td>Food &amp; Beverage</td>
<td></td>
<td>2</td>
<td></td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Chemical</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td>2</td>
</tr>
<tr>
<td>Other</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Transportation</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Pharmaceutical</td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Electronic Manufacturing</td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Grand Total</td>
<td>12</td>
<td>4</td>
<td>3</td>
<td>3</td>
<td>22</td>
</tr>
</tbody>
</table>

Table 2.9-3 Financial Impact by Industry (USA)

Table 2.9-3 shows the financial impact of specific industries in the US.

The industries in the US that suffered the greatest financial impact are Power & Utilities, Petroleum and Transportation. Power & Utilities, Electronic Manufacturing and Water/Waste Water had one incident resulting in costs exceeding $10,000,000.

2.10 Operation and Production 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 to 4 hours. There were 10 incidents that resulted in downtime exceeding 72 hours.

Figure 2.10-2: Production Downtime Percentages (Global)

Figure 2.10-2 shows the production downtime percentages worldwide.

In 36% of the cases when downtime was known, there was no downtime reported due to the incident. That does not translate to a financial loss or loss of employee time. In many cases, production continued, with software or hardware issues being resolved.
Figure 2.10-3: Production Impact (USA)

Figure 2.10-3 shows the US industrial security incidents on production and incidence frequency is plotted against downtime.

When downtime was known, the US incidents in the USA resulted in downtime most frequently followed by 1 to 4 hours. Downtime was not determined in many cases, there could certainly be other effects such as financial losses and lost employee time as updates or other corrective measures are put into place.

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. 76% of incidents resulted in at least 1 hour of downtime. This is alarming due to the fact that downtime can translate into significant financial loss or serious safety issues depending on the equipment involved and the regulated processes.
3 Recent Incidents

3.1 Summary of Most Recent Incidents

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

---

**Figure 3.1-1: Location of Recent Incidents**

<table>
<thead>
<tr>
<th>Location</th>
<th>United States</th>
<th>United Kingdom</th>
<th>Australia</th>
<th>South Africa</th>
<th>France</th>
<th>Unknown</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

---

**Table 3.1-1: Financial Impact by Industry Most Recent Incidents**

<table>
<thead>
<tr>
<th>Industry Type</th>
<th>$10,000-$100,000</th>
<th>$100,000-$1,000,000</th>
<th>$1,000,000-$10,000,000</th>
<th>$10,000,000+</th>
<th>Grand Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Water/Waste</td>
<td>2</td>
<td>4</td>
<td>6</td>
<td></td>
<td>12</td>
</tr>
<tr>
<td>Power and Utilities</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>Transportation</td>
<td>11</td>
<td></td>
<td></td>
<td></td>
<td>11</td>
</tr>
<tr>
<td>Other</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td>2</td>
</tr>
<tr>
<td>Grand Total</td>
<td>18</td>
<td>6</td>
<td>17</td>
<td></td>
<td>42</td>
</tr>
</tbody>
</table>
3.2 Details of Most Recent Incidents

The following are details of the new incidents added to RISI during the 3rd Quarter of 2009.

3.2.1 INCIDENT ID#: 155

TITLE: Computer Glitch Causes 7 Water Mains to Break
DATE of EVENT: 7/28/2009
DESCRIPTION:

A computer glitch caused a false low pressure reading and turned on the pumps at a United Water facility. A computer malfunction at the Troy pumping station was blamed for the 7 water main breaks in Jersey City Heights, NJ.

Two firefighters responding to an alarm at a senior center on Hague St. at noon and noticed water in the street. They notified United Water. There were 7 water main breaks at Hutton St. and Cambridge Ave, Bleecker St. and Pierce Ave., Congress St. and Shermann Ave, Thorne St. and Kennedy Blvd., Congress St. and Odgen Ave., and Ravine Ave.

IMPACT:

A boil order was issued. Water in some places was reported to be brown. Low water pressure resulted in some residents not having water for a period of time. Water tankers were posted at two locations in the event of a fire.

FOLLOW-UP WORK:

REFERENCES:

3.2.2 INCIDENT ID#: 156

TITLE: Paperless Chart Recorder Software Hacked

DATE of EVENT: 7/28/2009
DESCRIPTION:

Several installations of paperless chart recorders started to exhibit faults, like "going to sleep" or cyclic rebooting. The recorders were exchanged with spares and returned to the manufacturer. Reliability seemed to improve after the repair. It was discovered that the chart recorders contained an additional module which could not be disabled from the main screen; it locked the operators out. After "lock-out", reliability seemed to improve. Faults were never completely eliminated.

Sellarfield decided to change the recorders for another make.

IMPACT:

Chart recorder faults and lock-out.

FOLLOW-UP WORK:

REFERENCES:

3.2.3 INCIDENT ID#: 157

TITLE: Lightning Strikes Cause Sewage Pump Station Overflow

DATE of EVENT: 8/22/2009
DESCRIPTION:
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 55,000 gallons into Aquia Creek. The overflow volumes were higher than normal because the telemetry system for these two stations malfunctioned and did not activate the station alarms. Utilities 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 55,000 gallons into Aquia Creek.

**FOLLOW-UP WORK:**

Stations repaired, and staff is working with the telemetry contractor to determine how to prevent another malfunction. Staff spread lime to disinfect the area of the spill.

**REFERENCES:**

3.2.4 INCIDENT ID#: 158

**TITLE:** Sewage Spill Shuts Down a Cornish Shellfishery

**DATE of EVENT:** 6/2/2007

**DESCRIPTION:**

On June 2, 2007, a computer and penstock controlling the flow of sewage into the Truro Treatment Works failed. This caused sewage to be directed to a storm tank that continued to fill until June 3, 2007, when the tank reached capacity and overflowed into the Truro River. The discharge was not reported until 3 days after the spill.

**IMPACT:**

Sewage spilled into the Truro River. The shellfishery was closed for 12 days. The local fishermen suffered financially. South West Water was fined £8,215.

**FOLLOW-UP WORK:**

**REFERENCES:**

3.2.5 INCIDENT ID#: 159

**TITLE:** Computer Glitch Floods Neighborhood

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

**DESCRIPTION:**

A computer glitch caused pumps on the city's water tank to fail 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, leading to a flood in the neighborhood.
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, 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 surge the night before the flood.

IMPACT:
Tens of thousands of gallons of water, mud and rocks rushed down the mountainside into the Cedar Hills neighborhood causing minimal damage to one home.

FOLLOW-UP WORK:
REFERENCES:

3.2.6 INCIDENT ID#: 160

TITLE: Computer Failure Causes Jet Crash
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 information from automatic maintenance messages, it is believed that a cascade of system failures started with airspeed sensor failure and progressed to sweeping computer outages. The Airbus A330 en route from Rio de Janeiro to Paris crashed into the Atlantic Ocean during a storm.

IMPACT:
The Air France flight 447 crashed into the Atlantic Ocean. All 228 passengers were killed.

FOLLOW-UP WORK:
REFERENCES:

3.2.7 INCIDENT ID#: 161

TITLE: Faulty Software Causes Torrens Lake Drain
DATE of EVENT: 2/11/2009
DESCRIPTION:
Faulty software caused the gates of the Torrens Weir to open without warning. The gates remained open for about two hours, draining millions of liters of water from the lake. An investigation revealed that alarms that would alert remote operators of a malfunction were muted. The faulty software was purchased from Ottoway System Integration, an Adelaide-based firm which went out of business only 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
that relied on the lake. Since the incident, the weir has been opened and closed manually. One positive outcome is that the 17 tons of debris was removed from the lake. A report from GHD Engineering contains 11 recommendations including an overhaul of the software used to regulate the weir. Lord Mayor Michael Harbison was adamant the system would be upgraded.

FOLLOW-UP WORK:

REFERENCES:

3.2.8 INCIDENT ID#: 162

TITLE: Energy Company Exposed to Hackers by a Phishing Attack


DESCRIPTION:

An energy company hired Intreidus Group to investigate an attack that exposed the company to hackers. The investigation revealed that the incident was a result of a phishing attack. The attackers gained access to the system and remained for a period of time. One positive outcome is that the 17 tons of debris was removed from the lake. A report from GHD Engineering contains 11 recommendations including an overhaul of the software used to regulate the weir. Lord Mayor Michael Harbison was adamant the system would be upgraded.

FOLLOW-UP WORK:

REFERENCES:

3.2.9 INCIDENT ID#: 163

TITLE: Energy Company Virus Attack

DATE of EVENT: 9/23/2009

DESCRIPTION:

An energy company hired Intreidus Group to investigate an attack that exposed the company to hackers. The investigation revealed that the incident was a result of a phishing attack. The attackers gained access to the system and remained for a period of time. One positive outcome is that the 17 tons of debris was removed from the lake. A report from GHD Engineering contains 11 recommendations including an overhaul of the software used to regulate the weir. Lord Mayor Michael Harbison was adamant the system would be upgraded.
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 and said there was often "ineffective segregation" or "more typically none at all between the IT network and the network that monitors and controls the infrastructure." A spokesperson from Integral Energy stressed that the virus affected 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 insidious file infector" that spreads quickly and is considered difficult to remove. Computer networks were protected by a Symantec security solution, a source said. The Symantec website states that the virus installs a back door enabling hackers to issue commands on infected machines via an internet relay chat (IRC) channel. According to Gatford, the antivirus software was not updated in a timely manner and the Symantec product could not detect it.

Integral Energy supplies electricity to Western Sydney and Illawarra region of New South Wales distributing electricity to 2.1 million people in NSW.

IMPACT:
Integral Energy's computer network was infected with the W32.Virut.CF virus. All 1,000 desktop computers had to be rebuilt.

FOLLOW-UP WORK:
Integral Energy called in a range of experts to help with the virus infection. The company put in place recovery plans to eliminate the virus from its business systems. An investigation is underway to establish the cause of the infection and develop a strategy to minimize risk in the future.

REFERENCES:
3.2.10 INCIDENT ID#: 164
TITLE: Wastewater pumped into Jones Falls
DATE of EVENT: 4/20/2009
DESCRIPTION: An estimated 700,000 gallons of waste water overflowed from a pumping station on Sisson Street into the Jones Falls. There was no danger to the public because a screen filtered any macropollutants out before entering the Jones Falls. The overflow was the result of a malfunctioning automated switching system that controls electricity to the station's pumps. City officials are not sure of the exact 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 posted 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, 9 Killed, 14 Wounded

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 shooting exercise. The cause of the malfunction is not known. The South African National Defense Force is investigating whether a software glitch was the cause. The antiaircraft weapon is an Oerlikon GDF-005, which is computerized and can fire uncontrollably.

IMPACT:
Computerized weapon fired uncontrollably during shooting exercise, killing 9 spectators and injuring 14 others. A computer glitch is being blamed for the malfunction, though the possibility of mechanical failure cannot be ruled out.

FOLLOW-UP WORK:
REFERENCES:
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 roughly $65 billion1. 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 this 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 manufacturers on how to improve the intrinsic security of their products and automation system end-users on control system design best practices.

---

# 5 Contributors

<table>
<thead>
<tr>
<th>Name</th>
<th>Position</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>E. Byres</td>
<td>Chief Technology Officer</td>
<td>Byres Research Inc.</td>
</tr>
<tr>
<td>D. Riggio</td>
<td>Cyber Security Research Analyst</td>
<td>Exida LLC</td>
</tr>
<tr>
<td>J. Pancio</td>
<td>Research Assistant</td>
<td>Exida LLC</td>
</tr>
<tr>
<td>R. Amkreutz</td>
<td>Reliability Engineer</td>
<td>Exida LLC</td>
</tr>
<tr>
<td>J. Cusimano</td>
<td>President</td>
<td>Byres Research Inc.</td>
</tr>
</tbody>
</table>
6 Revision History

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date</th>
<th>Author(s)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>November 30, 2009</td>
<td>J. Cusimano</td>
<td>Issued at Rev. 1</td>
</tr>
</tbody>
</table>