



Insidious threat to control systems

By Eric Byres and Justin Lowe

The move to open standards is letting hackers take advantage of the control industry's ignorance.

It is widely accepted in industrial security analysis that the security risk faced by an organization is a function of both the *likelihood of successful attack* against an asset and the consequence of such an attack.

The second variable, *consequence*, while highly site-specific, is generally the easiest to understand. Often it can be estimated in terms of financial loss, acute health effects, or environmental impacts—concepts well understood from years of safety analysis of hazardous processes.

Estimating the *likelihood of successful attack* is far more difficult. According to American Institute of Chemical Engineers guidelines, it is a function of three additional variables:

Threat: Any indication, circumstance, or event with the potential to cause the loss of, or damage to an asset

Vulnerabilities: Any weakness that an adversary can exploit to gain access to an asset

Target attractiveness: An estimate of the value of a target to an adversary

These terms are more difficult to estimate, particularly with respect to cybersecurity.

This difficulty is largely because we have little reliable historical or statistical data to work with. The details of safety-related incidents have gone on record for over a century, while cybersecurity incidents have less than two decades of occurrence, never mind record keeping.

Furthermore, most organizations are highly reluctant to report security incidents as they can cause embarrassment to the company. In fact, many organizations have denied that there even is a risk to industrial systems from cyber attack. For example, an article in CIO magazine entitled "Debunking the Threat to Water Utilities" stated there was no credible risk to supervisory control and data acquisition (SCADA) systems from a network-based attack:

"Most public utilities rely on a highly customized SCADA system. No two are the same, so hacking them requires specific knowledge."

Yet this flies in the face of a number of well-documented cyber-related incidents such as the Slammer Worm infiltration of an Ohio nuclear plant and several power utilities and the wireless attack on a sewage SCADA system in Queensland, Australia. Clearly, the merging of common information technologies such as Ethernet, Windows, and Web Services into industrial controls technology has removed the dubious protective barrier of *security by obscurity*.

Obviously, industrial control systems face some security risk and, as difficult as it is to estimate, we still need to understand it. We can't ignore the risk, and yet we can't afford the infinite cost of perfect security.

Sound business practice requires we balance off the cost of measures to mitigate a risk event with the potential cost of the event occurring. To do so, we need to understand the variables at play in defining the cybersecurity risk for an industrial facility.

Furthermore, we need to continuously monitor these risk variables to determine if they are changing. To be effective from both a technical and cost perspective, our mitigation response must adapt to changes in threats, vulnerabilities, or target attractiveness.

The first two variables are changing rapidly and demand attention. The consequences of successful attacks are not insignificant.

Database tracks breaches

The British Columbia Institute of Technology (BCIT) maintains an industrial cybersecurity incident database designed to track incidents of a cybersecurity nature that directly affect industrial control systems and processes. This includes events such as accidental cyber-related impacts, as well as deliberate events such as external hacks, Denial of Service (DoS) attacks, and virus/worm infiltrations.

Data is collected through research into publicly known incidents (such as the Australian sewage spill) and from private reporting by member companies that wish to have access to the database. Each incident is investigated and then rated according to reliability on a scale of 1 to 4 (1=Confirmed, 2=Likely but Unconfirmed, 3=Unlikely or Unknown, 4=Hoax/Urban Legend).

The data collected includes the following:

- Incident title
- Date of incident
- Reliability of report
- Type of incident (accident, virus, and others)
- Industry (petroleum, automotive, and others)
- Entry point (Internet, wireless, modem, and others)
- Perpetrator
- Type of system and hardware affected
- Brief description of incident
- Impact on company
- Measures to prevent recurrence
- References

As of late 2004, we had investigated 41 incidents and logged them into the database, with 11 more incidents still pending investigation. Of these, seven were hoaxes/urban legends, and we removed them from the study data, leaving 34 events of sufficient quality for statistical analysis.

The trend of these events between 1995 and 2003 shows a sharp increase in events occurring around 2001. This may be indicative of an actual increase in attacks or the result of the increased efforts to collect data.

Discussions with operators of traditional business crime reporting databases indicate that the typical incident database collects less than one in ten of the actual events. Ten incidents entered the database in 2003, so it is likely that industry is experiencing at least 100 incidents per year now.

If nothing else, one conclusion we can draw from

this statistic is that a security problem exists, and it may be more widespread than most engineers believe.

The good old days inside job

We next analyzed the data for incident type to get an idea of the threat sources. We looked at 13 incidents between the years 1982 and 2000. Incidents split almost evenly between accidental, internal, and external sources, with only 31% of the events generating from outside the company.

Accidents, inappropriate employee activity, and disgruntled employees accounted for most of the problems. These statistics correlate well with the numbers reported by security researchers in the traditional IT world at that time. For example, this statistic was widely quoted in 2001:

A study on cyber crime by the FBI and the Computer Security Institute, released in 2000, found that insiders carried out 71% of the security breaches.

The study team then analyzed the period from

The emergence of automated worm attacks starting with Code Red on 19 July 2001 has meant that many of the intrusions have become nondirected and automated.

2001–2003. Externally generated incidents account for 70% of all events, indicating a surprising and significant change in threat source.

Interestingly, the IT world appears to be experiencing the same shift. For example:

Deloitte & Touche's 2003 Global Security Survey, examining 80 Fortune 500 financial companies, finds that 90% of security breaches originate from outside the company, rather than from rogue employees.

"For as many years as I can remember, internal attacks have always been higher than external," said Simon Owen, Deloitte & Touche partner responsible for technology risk in financial services.

"Sixty to 70% used to be internally sourced. But most attacks are now coming from external forces and that's a marked change."

Why did the threat source change so significantly in such a short period? We have no definite answers, but a few possibilities can explain the impact on industrial control systems. First, the emergence of automated worm attacks starting with Code Red on 19 July 2001 has meant that many of the intrusions have become nondirected and automated. The control system has become just a target of opportunity rather than a target of choice.

Second, common operating systems—Windows 2000 or Linux—and applications, like SQL Server, now dominate the human-machine interface (HMI), engineering workstation, and data historian systems. These often come configured more appropriately to business requirements and are vulnerable to a wide variety of common IT attacks and viruses. Issues with applying patches to these critical systems exacerbate the problem.

Finally, the increasing interconnection of critical systems has created interdependencies that we haven't been aware of in the past. The Slammer incident—doc-

umented by North American Electric Reliability Council—illustrates that Internet incidents can indirectly affect a system that doesn't even use the Internet. In this case, the power utility used frame relay for its SCADA network, believing it to be secure. Unfortunately, the frame relay provider utilized a common Asynchronous Transfer Mode (ATM) system throughout its network backbone for a variety of its services, including commercial Internet traffic and the SCADA frame relay traffic. The worm overwhelmed the ATM bandwidth resulting in and subsequently blocking SCADA traffic to substations.

Regardless of the reasons, the threat sources are moving from internal to external, and this needs consideration during the risk assessment process. Determining the actual perpetrators and their proba-

The Slammer incident—documented by North American Electric Reliability Council—illustrates that Internet incidents can indirectly affect a system that doesn't even use the Internet.

bility of attack is currently beyond the ability of the database, but security risk analysts should look at governmental studies of threats to critical infrastructure to obtain some possible threat estimates. A good starting place is the National Infrastructure Security Coordination Centre's (NISCC's) report *The Electronic Attack Threat to Supervisory Control and Data Acquisition (SCADA) Control & Automation Systems*.

The back door into the plant

If the threats are becoming increasingly external, then this begs the question, "How are they getting in?" While Internet connections may be the obvious source, it isn't the only one. For example, database records show that the Slammer Worm had at least four different infiltration paths in the control systems it affected:

- The Davis-Besse nuclear power plant process computer and safety parameter display systems via a contractor's T1 line
- A power SCADA system via a virtual private network (VPN)
- A petroleum control system via a laptop
- A paper machine HMI via a dial-up modem

To answer this question, the study team analyzed the point of entry data for each of the incidents in the database. These incidents were in two groups, namely 14 internal and 25 external incidents.

For the internal incident, the business network was the major source. Direct physical access to the equipment was also significant. For the external event, the Internet was a major source, but dial-up connections, VPNs, Telco networks, wireless systems, and third-party connections were all contributors. The obvious conclusion is that there are many routes into a system as complex as a modern SCADA or control system. Focusing on a single intrusion point with a single solution—such as the Internet firewall—is likely to miss many possible attack points.

Assessing the consequences of industrial cyber

attack is not simply a case of assigning a financial value to an incident. Although there are obvious direct impacts that may be easily quantifiable financially (e.g., loss of production or damage to plant), other consequences may be less obvious. For most companies, the impact on reputation is possibly far more significant than merely the cost of a production outage. The impacts of health, safety, or environmental incidents could be far more serious to a company's brand image. Even impacts such as minor regulatory contraventions may affect a company's reputation or possibly license to operate.

For most of the incidents reported in the database, the contributors have been unable or unwilling to provide financial impact to these industrial cyber attacks—in fact, only 30% have been able to provide such an estimate. Although the sample data is not large, it does seem significant that nearly 50% of reported incidents that were able to provide a financial impact estimate, reported sizeable financial impacts (>\$1M).

Potentially more significant is the nature of the impacts of the attack. Forty-one percent reported loss of production while 29% reported a loss of ability to view or control the plant. Fortunately, human impacts have been small with only one unconfirmed (and possibly unreliable) report of loss of life. Overall, the reported incidents clearly show that the most likely consequences of industrial cyber attack are loss of view of or ability to control the process.

The likely impact of being unable to view or control the process or system places an increased reliance on emergency and safety systems. Traditionally these systems have been independent of the main control system and generally considered 'bulletproof.' However, mirroring the trend in the design of the main control systems, these emergency systems are starting to sit on standard IT technologies—like TCP/IP. In addition, they are increasingly connecting to or combining with the main control system, consequently increasing the potential risk of common mode failure of both the main control system and the safety systems. Therefore, in the future, the systemic risks of cyber attack need consideration in not just the design of the control systems but also the safety systems.

A brave new world

Looking forward, the study team sees nothing to indicate these trends are likely to reverse in the near future. In fact, if anything the situation is likely to get worse. The hacking community is becoming increasingly aware of SCADA and process systems and is beginning to focus attention on them. For example, a presentation at the Brum2600 Blackhat Conference, held in Birmingham, UK, in October 2003, said:

"Things started to get a little more interesting. The talk, titled 'How safe is a glass of water' was a detailed breakdown of the RF systems that are used by water management authorities in the UK and how these systems can be abused, interfered with, and generally messed."

Six months earlier, a presentation at the CanSecWest conference detailed how to attack embedded operating systems in routers, printers, and cell phones. These

same embedded operating systems are in modern SCADA and controls equipment. Combined, these presentations indicate that the hacking community is beginning to have both an interest and the technical expertise to deliberately attack control systems.

Threats and vulnerabilities

The above analysis indicates a clear shift in the source of cyber attacks on industrial control systems. Threats originating from outside an organization are likely to have a very different attack characteristic than internal threats. Thus, companies may need to reassess their security risk model and its assumptions.

In addition, the variation in the infiltration paths indicates a wide variety of vulnerabilities available to the attacker. Considering the difficulty closing all of these avenues, it would be wise to assume boundary breaches will occur, and to harden the equipment and systems on the plant floor to withstand possible attacks. In effect, companies need to deploy a defense in depth strategy where multiple layers of protection are in place, down to and including the control device.

Achieving a defense in depth solution for industrial systems will require at least four steps. On the system design side, there should be more internal zone defenses and more intrusion detection deployed. As

well, companies may need to re-evaluate boundary security in terms of all possible intrusion points and not just focus on the obvious connections such as the business-process link. A single firewall between the business network and control system network is likely to miss many intrusions and will offer little security once the attacker is inside the control system network.

From the control system manufacturers' side, SCADA and automation devices need to undergo security robustness design and testing prior to deployment in the field. As well, SCADA and control protocols should begin including security features. Currently most devices appear to be highly vulnerable to even minor attacks and have no authentication/authorization mechanisms to prevent rogue control.

Failure to adapt to the changing threats and vulnerabilities will leave the controls world exposed to increasing cyber incidents. The result could easily be loss of reputation, environmental impacts, production and financial loss, and even human injury. ❧

Behind the byline

Eric Byres (eric_byres@bcit.ca) is research faculty—critical infrastructure security at British Columbia Institute of Technology. **Justin Lowe** (justin.lowe@paconsulting.com) is principal consultant at PA Consulting Group in London.

Critical infrastructure attacks surge

Network attacks against critical infrastructure providers such as utilities, telecommunications companies, and government agencies surged 55% from July 2004 to August 2004, according to IBM's Global Security Intelligence Services.

Since July, IBM has seen a 27% increase in overall network attacks against all monitored enterprises and businesses. Businesses are increasingly dependent on information technology and the Internet to run their daily operations.

With their network infrastructures increasingly under attack, IBM, through its Global Business Security Index, helps alert these businesses in advance to the onslaught of threats to help them proactively secure their networks.

The Index—created by IBM's global security experts—is a monthly report that assesses, measures, and analyzes global network security and business threats and attack trends.

It is compiled by harnessing the historical and current data collected by IBM's 2700 information security professionals and half a million monitored devices to provide a picture of the IT and business threat landscape.

IBM's IT security intelligence and business consulting experts analyze the vast amount of data collected by IBM network and system monitoring sensors. The experts then rate the potential severity of known IT threats, producing a unique snapshot of the current IT security landscape.

The report, which customizes as to industry, tracks real and potential IT threats to a business including:

- IT network and infrastructure, including potential and real threats that could significantly damage a customer's business and reputation
- Business continuity trends, statistics and recommendations for keeping employees, customers, suppliers, and partners connected with critical business information during natural disasters, such as hurricanes, and widespread power failures

IBM confirmed 997 Internet attacks in September 2004 directed at networks the company monitors, representing a 27% increase over confirmed Internet attacks in July and August. The most prevalent attacks came from several worms, such as Sasser and Korgo, seeking to exploit a vulnerability

located within the Local Security Authority Subsystem Service, a security component of the Microsoft Windows operating system.

Critical infrastructure providers experienced an increase in worm traffic—as did most IT environments—according to IBM's analysis. The most apparent increases, however, were by attackers seeking vulnerabilities in Web server software like Microsoft IIS, Apache HTTP Server, and Netscape iPlanet. This type of reconnaissance activity typically precedes more complex, singularly directed attacks against systems that are, in fact, vulnerable.

"In the fight against IT security threats, timing is everything," said Stuart McIrvine, director of IBM's security strategy. "Knowing about new threats and vulnerabilities before they become attacks and proactively tak-

"These days, hackers are able to reverse engineer newly published security patches and deploy an attack on an unpatched system in 48 hours." — Stuart McIrvine, director of IBM's security strategy

ing steps to prevent harm is now more critical than ever.

"These days, hackers are able to reverse engineer newly published security patches and deploy an attack on an unpatched system in 48 hours. Companies that have elevated security issues from the server room to the boardroom are tapping into IBM's worldwide security expertise, intelligence, and technological resources to help preempt global attacks," McIrvine said.

Many Fortune 500 companies and government entities in 34 countries around the world use a variety of IBM's monitoring services, such as its Intrusion Detection Service, Vulnerability Testing, and Assessment Service, to keep abreast of current attacks and threats around the clock.

On average, IBM's monitoring services detects 100 million suspected or actual attacks against customers each month. In addition, newly discovered IT threats, such as new vulnerabilities, malware, or general risks posed to IT environments, receive a potential severity score from zero to 10 in various categories. ❧