

# **Process Control Security In An IP World The Rules Have Changed**

**William Crowell**

[Wcrowell@wcrowell.com](mailto:Wcrowell@wcrowell.com)

# We Live In a Technology Driven World

## Devices that are:

- Smaller
- Faster
- Cheaper
- Digital
- And now **Connected**.... This is the fulcrum for most new innovation in applications, and now includes Process Control

***Connectivity through Internet Protocol (IP) Networks changes the Security environment entirely***

# The Digital Revolution

- ◆ **Driven by the Internet Protocol (IP or TCP/IP)**
- ◆ **Promotes:**
  - **Common platforms and devices**
  - **Common interfaces**
  - **Connectivity .... But not security of the connected elements**
  - **Integrated applications across diverse locations and operations**
  - **Productivity enhancement**

# Technology Leading to Convergence in Applications

- ◆ IP Networks have created an explosion of applications that:
  - Create whole new services
  - Increase mobility in providing services
  - Increase Productivity (through self service and reduced downtime)
  - Reduce errors and costs (bar codes)
  - Combine many processes into one

*The Web has multiplied the trend many fold*

## But Technology is a Double-Edged Sword

- ◆ Technology can also be used by terrorists and criminals to increase their effectiveness in :
  - Planning operations
  - Surveillance and selection of targets
  - Recruiting their forces
  - Providing the logistics support to operations
  - Coordinating the attack
  - Assessing the success of the operation

*We have to stay ahead of our adversaries*

# Homeland Security: The Challenge Is A Robust and Secure Economy

- **Building upon the productivity enhancing elements of Information Technology and the Internet we have created global and intertwined economies with significant new vulnerabilities**
- **To survive the effects of simple attacks on our complex structures we have to use technology to make us more secure**
  - **Make Security a part of our future systems**
  - **Ensure Defense in Depth on vital elements of our economy and critical infrastructure**
  - **Redesign and organize the elements of our business and economy to contain the effects of attacks**
  - **Make Security more affordable, predictive and productive**

# New Threats

## ◆ Terrorist threats within the US

- 9/11 – Imagining the unimaginable
- Physical attacks on Critical Infrastructure
- Cyber terrorism

## ◆ Enterprise Threats

- External threats like Hackers/Phishing
- Insiders who enjoy access to systems
- Physical threats to assets and employees
  - Disgruntled employees to criminals

*And a new attack tool: Disruption*

# Paradigm Shift in National Security

- ◆ **Prevent/contain, not just recover**
  - Threats are too serious to rely on recovery
  - Alert to potential threats – provide time to react
  - Real time notice and interaction to manage situations
- ◆ **A Target Rich Environment for Terrorism**
  - Government assets and leadership
  - Critical infrastructure – financial, transportation systems, power, etc.
  - Public areas like Sports arenas, shopping centers, ...

# The Security Industry

## ◆ Elements of Security

- Physical Protection
- Information Security: Networks & Applications
- Personnel Risk Assessment
- Process: How to institutionalize approaches that work and can be verified

***Most of the systems that are available today treat all of these elements separately. There are few suppliers or integrators who work across all of them***

# Security – State of Solutions

- ◆ **Technology – “points of light”**
- ◆ **User experience – “darkness”**
- ◆ **Business integration – “paste on”**
- ◆ **Trustworthiness is about:**
  - **Technology** ...plus
  - **People** ...and
  - **Policy and Process**

## Security – State of the Market

- ◆ **The Leadership is the wrong generation**
- ◆ **The Proponents are too “techie”**
- ◆ **The ROI proposition is unclear**
- ◆ **The Mandate is unclear and often product-oriented rather than policy or solution-oriented**
- ◆ **Regulation has its flaws – One size does not fit all**

# Role of Technology in Security

- **Create new capabilities not before possible:**
  - Robust Identity Management & authentication
  - Surveillance of valuable information & physical assets
  - Analysis and correlation of threats and attacks in real time
  - Command and control of security assets and responses
  - Information sharing within and outside the organization
- **Make these capabilities and processes more efficient and productive**
- **Commercialization of technology can make huge differences in the cost of ownership and interoperability (e.g. mass storage, video surveillance, network systems and network security)**

# Security Technologies Are Changing

- ◆ **Smarter components**
  - Sensors (Video Analytics, Biometrics, UAVs, Radar-IR-Optical)
  - Viewing (Remote Access, Visualization, GIS mapping, dashboards)
  - Communications (WiFi, Internet, Satellites)
- ◆ **Integrated systems**
  - Access control, Alarms, Surveillance
  - Network systems - ESM, sharing information and correlation of events
  - Open architecture for easy integration of new technology and services
  - Industry standard formats will prevail to promote interoperability and interaction
- ◆ **Users are more connected**
  - Network access/notification from anywhere
  - Escalation of information and decisions to anyone/anywhere

# Benefits From New Security Technologies

- ◆ **Improved protection**
  - Sensors are more specific and aid detection
  - Instant notification
  - Access video and data from anywhere – the Security Operations Center can now be a Call Center
- ◆ **Better data**
  - HR/legal evidence (forensics)
  - Unified Facilities management and security
  - Marketing/customer patterns
- ◆ **Security becomes another IT application**
  - Better support and maintenance
  - More cost effective

# Implications of IP to Security

- ◆ **The Internet and Network Centric Business presents new threats to the Security System**
  - What's your dog's name – the password game
  - The firewall myth – Justice's scale
  - Worms, viruses, spybots
  - How secure is encryption? Weep about WEP
  - What about Intrusion Detection vs. ESM
  - The double whammy – Insiders & Outsiders

# How to Cope with Network Threats

## ◆ Five basic tools

- Access Management – the ID Game
- Firewalls – Manage the connections to the outside
- Enterprise Security Management – using IDS, Firewall, Access Control, and Signatures
- Anti-virus and Spybot scanning
- Encryption

*.....Oh, and also the “Air Gap”*

## Some New Concerns As Well - Privacy

- ◆ **Security systems have privacy implications**
  - **Get to know the law and the popular issues**
  - **Build into systems the policy constraints and auditing to prevent misuse**
  - **Notify and educate the customers, users, and public about the policies and constraints that are exercised**
  - **Perceived Privacy violations can kill products and services**
  - **Real Privacy violations can send you or your customer to jail or cost money**

# Managing Risk - A New Business Driver

- ◆ **Physical and network security becoming intertwined**
  - Protecting the platform is critical
- ◆ **New area of compliance monitoring and internal controls**
  - **Sarbanes-Oxley (SOX)** – corporate compliance with risk assessment, notification and internal controls
  - **HIPAA** – Health Information Portability Act that protects privacy of health records in electronic form
  - **Graham-Leech-Bliley** – protects privacy of financial records
  - **FISMA and DITSCAP** for the government sector

*There will be more Compliance laws !*

# Predictions

- ◆ **Open architecture will prevail**
  - Easy integration
  - Standard formats
  - Lower costs
- ◆ **Integrated platforms that make the CIO more confident about putting Security into the Network**
  - Video Systems with integrated analytics and remote viewing
  - Enterprise Security Management (ESM) that enables detection of *insider threats*
  - ID Management Systems that keep the hordes of hackers at bay
  - Security Dashboards to notify specialists and executives of compliance and oversight issues

# The Adoption Curve

- ◆ **Lot's of innovative technology companies are in this market, but they are not making money**
- ◆ **So.....When will it happen?**
  - **Technology points of light vs. the integrated solutions ... and standards**
  - **Costs and risks – the hype vs. the real**
  - **A consolidation in the market – always helps the hype factor and “margins”**
  - **A deadline – Is SOX the Y2K? Or an event?**

# Looking Ahead

- **We have created incredibly efficient business processes and systems**
- **These complex systems increase our vulnerability to attack by criminals and terrorists**
- **We should treat Security as a business enabler that assures continuity of operations and productivity**
- **Unless we make Security more affordable, it will not be as robust as we need**
- **Unless we make Security more of an integrated business function, it will fail**
- **The ROI on security is continued productivity and prosperity of the Nation and our global partners**