Security Challenges on the Plant Floor

Kenneth Hartman

IEEE Madison Section
March 16, 2006

- Not Overly academic, but rather a perspective from the trenches
- I thought that this would be an engaging topic for discussion.
- Everyone is impacted by computer security (or lack of it).
- You can't go several days without hearing about a virus outbreak, a Phishing scam or some major security lapse such as the one last week where over 200,000 PIN numbers from CitiBank Debit cards were stolen
- When I did a google search on 'Citibank PIN' my first hit was a failed gag order from 2003 where Citibank tried to squelch knowledge of the vulnerabilities
- 'Security by Obscurity' is no longer an adequate defense tactic –But this is often the only security measure employed on the 'Plant Floor'

•I wrestled with the name ‘Plant Floor’ because these issues are not limited to the manufacturing plant floor

•My background is in manufacturing but now I am seeing the same problems in healthcare, on the ‘hospital floor’.

•The ‘Challenges’ that I want to discuss are prevalent anywhere you apply specialized devices to perform a control function and connect those devices to a network

Critical Infrastructure

- 87,000 Food Processing Plants
- 1,600 Municipal Waste Water Facilities
- 5800 Hospitals
- 250,000 Defense Firms
- 2800 Power Plants
- 104 Nuclear Power Plants
- 5000 Public Airports
- 66,000 Chemical Plants

The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets – February 2006

Here are some interesting numbers from the governmental report entitled: “The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets”

Even though this government report deals with physical security, seeing the numbers affirms the importance of increased information security expertise on the plant floor.

One of the big lessons from 9/11 is that everyone has a role in security. In the same way, we cannot just relegate the security of plant floor control networks to the corporate IT security department.

Real Time Operating Systems

AMX KwikNet KwikPeg C EXECUTIVE CMX-RTX
DeltaOS eCos embOS eRTOS ETS EYRX
INTEGRITY INtime® real time extension to Windows® IRIX
iRMX Jbed LynxOS MQX Nucleus PLUS On Time
RTOS-32 OS-9 OSE PDOS PSX QNX Neutrino
QNX4 REDICE-Linux RTLinux RTX 5.0
Portos smx SuperTask! ThreadX Treck
MicroC/OS-II TronTask! TTPos: VxWorks 5.4
SCORE DACSTADS Nimble - the SoC RTOS Nucleus
Fusion RTOS FreeRTOS

Problem Statement

- The plant floor is not as homogenous as the front office
- Very thin technical resources
- Proprietary Control Networks è TCP/IP
- Same Vulnerabilities as on Internet
- Lack of Appreciation of *What is at Stake*
- Misunderstood Security ROI

•The plant floor is not homogenous like the front office. There is a good chance that the IT has standardized on a model of PC, such as IBM or Dell and has migrated most everyone to Windows XP or at least Windows 2000

•This is for good reason – this standardization allows for improved administration & usually security as a result

•The purpose of computing technology on the plant floor is typically to control or monitor one or more diverse processes (such as a conveyor system, robotic arm palletizer, or a high-speed packaging line).

•In manufacturing, the typical approach is to adapt commercially available equipment to the peculiar needs of your new production line or whatever project you are working on.

•Generally, the project engineer will provide the OEM with control system specifications that are in keeping with the plant's electrical standards. These might specify a certain model of PLC, such as the Allen-Bradley ControlLogix platform.

•The OEM may or may not be willing to convert their control system to the specified control platform. If they do convert to the specified platform, then there may be risks to the project if the OEM does not have adequate competency in the specified platform. If the OEM is unwilling to provide the required equipment in the specified control platform, the project team may be forced by the business to compromise their standards.

•Thin Resources – Everyone is being asked to do more with less. There is a shortage of Expertise, Time & Money

•Many controls engineers are moving away from the proprietary control networks (Profibus, ModBus, DataHighway+, RS485, etc.) toward Ethernet TCP/IP. I'll discuss why in a minute.

•What is at stake? Employee health and safety (remote starts/speeds/sequence changes), product integrity, economic viability. (Example: Milk Pasteurization)

•Security ROI will be discussed later – "The payback from doing the right things to minimize security risks"

Why the Move to TCP/IP?

- Lower 'Total Cost of Ownership'
  - Lower Cost of Supporting Hardware
  - TCP/IP Knowledge more widespread
- HMI / SCADA / MES
- Network Tools / Software
  - Ping
  - Packet Analyzers

•Lower Cost of Hardware – Switches, Cabling, NIC's are all commodities

•Almost all computer users now know at least a little about TCP/IP thanks to the $9 billion home networking market

•Another force behind the move to TCP/IP networks has been the need for higher level systems to connect to the process controller. There is considerable information about the process that is available from the device providing the control function.

•Pressure to increase productivity has led to increased supervisory control and automated coordination over systems that were heretofore isolated.

•There are some great open-source tools that can be used to troubleshoot and monitor TCP/IP networks

•NOT EVERYTHING: Always will be the need for specialized networks that solve specific engineering challenges, such as determinism, servo control etc.

The Downside…

- Widespread Vulnerability Data
  www.securityfocus.com/vulnerabilities
- Plethora of Malware
  Virus - Trojans - Spyware
- Automated ‘Script-Kiddie’ Tools

The Same Threats that exist on the Internet!

•While knowledge about TCP/IP is widespread SO ARE the knowledge of the security vulnerabilities

•Mailing Lists (such as the SecurityFocus bugtraq) disseminate vulnerability discoveries immediately!

•Hackers, Crackers, and Cyber-criminals create tools to exploit these vulnerabilities

•And ‘script-kiddies’ use the tools to hammer away at anything they can reach

•Probably the most common threat is from malware. These might be from diskettes, flash drives, or laptops that are brought into the plant from the outside or were downloaded from the web.

•I’m constantly amazed at the spyware and ‘hijacked’ computers that I see when I am in healthcare facilities.

Latest Mydoom virus may signal dreaded 'zero day' attack

The time lapse between security flaw announcements and exploits is shrinking

News Story by Tom Venetis

NOVEMBER 12, 2004 (ITWORLDCANADA) - The latest version of the Mydoom virus suggests to security experts that a much-anticipated "zero day" attack may have already arrived.

...The time difference between when security vulnerabilities become known and exploits are created to take advantage of those flaws has been shrinking for some time. Two years ago, that time difference was somewhere between four and six weeks.

"For the first six months of this year, [that difference] was about 5.8 business days, and in this most recent case, it was just two days," said Alfred Huger, senior director of engineering at Symantec Corp. in Calgary, Alberta. "The problem is that it is extremely difficult for a vendor to put out a patch in that short of a time."

...

http://www.computerworld.com/printthis/2004/0,4814,97474,00.html

Things are not getting better!

Nimda fix – disabled the Rockwell Software Copy-protection, breaking several plant's HMI

Concern about Day Zero Attacks – Cure could be worse than the problem!

Who is Responsible?

- This question is best resolved upfront
- Accountabilities for security should be defined for the entire asset lifecycle

  Planning è Installation è maintenance è decommissioning

  If everyone is responsible – then no one is

- Use a Cross-Functional Team
- Build a Business Case
- Obtain Sponsorship

Show Leadership – Be Proactive!

Job One is to Avoid a RGE

RGE: Resume Generating Experience

•Project Managers: During the Project Planning Phase, incorporate network security design considerations into the design. Develop a list of questions, such as how will the system respond to a DoS? Can my HMI be accessed remotely in an insecure manner?

•Has the networked control system been installed as designed? Did the designers miss anything?

•Maintenance Phase: Has the network changed? Has System access changed? Are backups being performed?

•Decommissioning: What changes must be made to the systems that the decommissioned system interacts with? Do user accounts need to be deactivated, etc?

•Use the organizational resources available, such as expertise in the IT department. Their security subject matter expertise may augment yours and their lack of control system expertise may serve as a 'fresh set of eyes' detecting things in your blind spot.

•Silo-ism Kills!

Return on Security Investment

- Business Continuity Planning
- Mitigating Business Interruption
- Annual Loss Expectancy (ALE)
- Recovery Time Objective (RTO)
- Recovery Point Objective (RPO)
- Costs of Poor Quality
- Productivity Improvements

The Traditional means of building a business case for security enhancements has been **FUD**

FUD: Fear, Uncertainty, & Doubt ---but that only goes so far

•Security Management is Good Management

•It is doing the right things right to minimize risks

•Don't think of security management as a 'new job' added to your already full plate, but rather a new facet that is part of your existing job function.

•For instance, when you install a new control system, you go through a process of determining what design considerations are required to make the system successful. Now include security considerations into the design process.

•If you do have to cost justify security-related activities, it helps to use the most effective 'buzz words'

•'Business Continuity Planning' – most organizations are sorely lacking effective business continuity plans. It is hard work and takes an in-depth understanding of your business. But your stakeholders ***expect*** you to do this. Some of your security management activities can be performed as part of your 'Business Continuity Planning' bucket of work.

•Consider doing Business Continuity Planning as part of your Capital Project Planning Process. The reason to do this is because that to appropriate the capital, a cross-functional team is already in place that understands the business value of performing the project and should be readily able to document a contingency plan for the benefit of the decision-makers approving the finances.

•Mitigating Business Interruption—The security countermeasures that you can put in place will either reduce the likelihood that an 'attack', 'security incident' or innocent mistake will interrupt your business or they will be able to reduce the severity of the impact.

•For quality sake—we need to stop winking at this.

•{NEXT SLIDE} http://www.cio.com/archive/021502/security.html

Google 'Security ROI'

Annual Loss Expectancy

ALE

=

Frequency of Security Incident

X

Dollar Cost per Incident

- One methodology of quantifying ROSI (Return on Security Investment) is to use Annual Loss Expectancy (ALE)
- ALE = Frequency of Security Incident X Dollar Cost per Incident
- It may be happening more often than you think! For instance: Unauthorized tweaking of a ‘recipe’ or ‘calibration setting’

Recovery Time Objective (RTO)

How much time will pass after a disaster before the data necessary for re-launching operations is recovered?

How much time is required for data to be recovered?

Here is a Scenario to explain how you can make RTO work for you:

Lets say that you have a mission critical Windows-Based HMI, on a packaged pizza line?
How long will it take you to get the line back in operation if the system develops a hard disk failure?
•Four Hours if you have to rebuild the OS after replacing the HDD
•Longer if you have not archived the latest copy of HMI program files
•20-30 Minutes if you just need to restore a back-up image of the drive
•5 minutes to swap out the PC with a pre-imaged system
•Zero with a redundant HMI

Cost Benefit Analysis
Should be part of the maintenance planning process
Planned Work vs. Reactive Work
Sign in Gator's Bar, Dallas, TX-- *"It is hard to drain the swamp when you are so busy fighting alligators"*

Somewhat akin to Mean Time To Repair (MTTR), except MTTR is based on actual recovery time and RTO is a goal.

Recovery Point Objective (RPO)

How far back in time does data need to be recovered in order for a business to re-launch operations after a disaster occurs?

How old is your backup?

If a back-up is performed every night at midnight and a failure occurs at 3:00 PM, your RPO is midnight.

Is that acceptable to your stakeholders?

This should be discussed at a minimum.

Most Everyone understands that higher service levels require higher costs. This can fund your security enhancements

HDD Failure could have been caused by a Virus or a Power Surge.

--It does not matter, this is just good management!

Verify your backups! Test your plan!

For example, if you have a production line that is not in use then perform the following recovery test:

•Remove the PLC Processor and time the service personnel to see how long it takes them to check out a new PLC processor from the supply room, find the program and restore it.

•Discuss the lessons learned and identify the ways to improve MTTR

As the say in the military: “A plan that is not exercised is not a plan at all”

Security Management is an Essential Component of Good Management

TQM Movement “Cost of Poor Quality”

Little things that eat your lunch

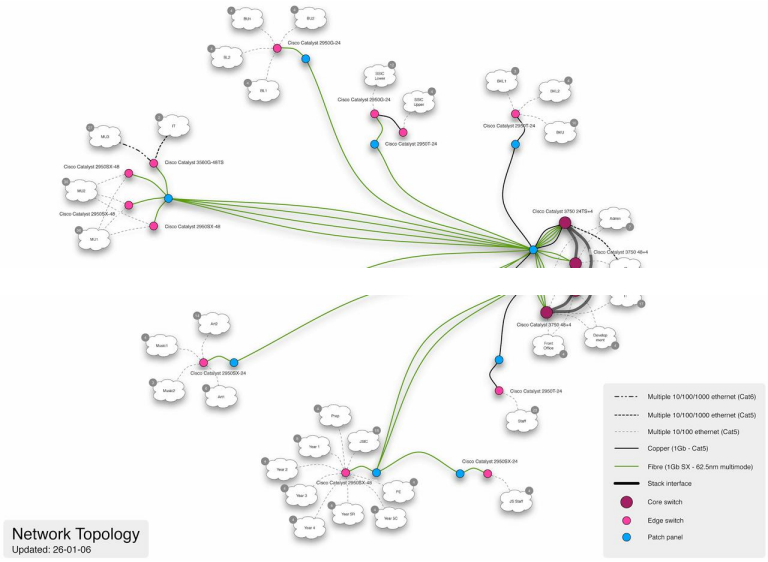
“Death of a Thousand Cuts”

Incremental productivity gains are achieved from making the right choices and doing the right things

Now that we have the “Business Issues” out of the way, we can transition into the more interesting/technical stuff

But first a thought from Tom Peters—”You want to become excellent, stop doing non-excellent stuff”

To Segment or Not to Segment?



Some Organizations create a separate network segment for networked plant floor devices

This may or not be appropriate for your organization.

•One of the benefits are that you can constrain most of the plant floor traffic to the plant floor network segment

•The other benefit is that you can use *Access Control Lists* in the routers to limit what type of traffic should be permitted to pass between segments.

- •For instance, you can create a rule that allows only selected source addresses on the office segment to access the plant floor segments and another rule that allows only HTTP traffic from the plant floor segments to the Internet, etc

There is a common misconception by some that do not understand network security:

"we are secure, we are behind a firewall"

The firewall at the edge of your company network simply provides a layer of protection from *external* connections

IT DOES NOT protect you from the traffic WITHIN your network

Reference: *The Firewall Fetish*

Generally the company firewall will be configured to block all incoming traffic except for VPN Traffic and perhaps Web Traffic (HTTP protocol, port 80) which would be directed to a dedicated web server. Generally, the firewall will allow most outgoing protocols (HTTP, HTTPS, FTP) but may block other protocols such as SMTP

They would allow SMTP from the only company mail server to prevent unauthorized mail servers sending mail from the company network. The Nimda virus actually propagated itself via becoming a SMTP server. Unfortunately many embedded control systems use SMTP to send alerts via email

Firewall Piercing

When an internal user asks you system administrator to open an outbound port to an external machine, or an inbound port to an internal machine, then you should do it for him. Of course you should help the user to make sure that his transactions are secure, and that his software is robust. But a flat out denial of service is plain incompetence.

For unless he is so firewalled as to be completely cut from the outside world, with no **ssh**, no **telnet**, no web browsing, no email, no dns, no **ping**, no phone line, no radio, no nothing, then the user can and will use firewall piercing techniques to access the machines he wants nonetheless, and the net result for security will be an unaudited connection with the outside world.

Firewall Piercing mini-HOWTO
François-René Rideau
v0.97, 24 November 2001
http://www.faqs.org/docs/Linux-mini/Firewall-Piercing.html

There are many different techniques to Pierce a firewall. The techniques usually involve a initiating the communication session from the inside the trusted network using a protocol that is permitted.

•I have a great software package called 'Remote Help' that allows a client of mine to download a single file executable, that when run gives me remote control over their system.

•GoToMyPC is another commercial software that allows an end user to come in via circumventing the perimeter firewall

•My company uses a system that converts files sent to it via FTP into email messages. We use this to get real-time alerts from equipment we have installed at client sites

Personal Firewalls are a great thing! Use them

Windows XP comes with an integrated firewall.

One of the problems with Windows, especially, is to many 'open ports'

Ports are how network enabled software applications communicate with each other

•A personal firewall will allow you to open only the incoming ports that you need. For example, if you are running a web server on your computer, you could open port 80, which is the default port for HTTP

•In general, most computers do not need any ports open at all. Therefore, blocking all unneeded ports will go a long way to securing your network and reducing virus propagation

Most personal firewall software will also allow you to grant which programs on your computer are allowed to access the network.

•Very Useful if they are turned on. I cannot think of any good reason not to use them on a business network

TCP Wrappers is the Unix/Linux way of configuring which source IP addresses can access services running on a particular computer

•This functionality may or may not be available on the embedded operating systems used on your plant floor.

•If your device has this functionality –use it

•If you build devices with an embedded OS, then expose this functionality to make your device more secure

So, lets saw that you do decide to create a separate ‘plant floor’ segment and you have restrictive access control lists that limit what traffic the router will pass. One of the things that folks may be tempted to do is to used a ‘Dual Homed Computer’. This is simply a PC that has two network interface cards. It is even worse if they enable connection sharing as that will permit their computer to function as a router for other PC’s.

I have seen some people who are so fed up with their IT folks that they have had their own DSL or Cable Modem set up, totally circumventing the IT department

There have been times where I am on a very restrictive network where I have had to use the analog phone line plugged into the fax machine for dial-up Internet access

Password Considerations

- Too Many Passwords
- No Passwords
- Weak Passwords
- Strong Passwords
- Single Sign On
- 2/3 Factor Identification

If you ask the average computer user, they will tell you that they have too many passwords—so they use the same password for everything.

•Find out the password and you can access almost everything they have access to

In my experience, passwords are typically not used in control systems—if they are optional.

•For example, most engineers do not use passwords in PLC processors because you need the programming software (or do you?)

•At one large company, where I previously worked, I was able to demonstrate how I could go-online with a PLC in Fullerton California from Madison. I found the PLC by doing a network scan

Weak Passwords are certainly better than no password at all. Often these are the name of a pet or family member.

•Subject to Guessing or 'Dictionary Attack'

Strong Passwords – usually enforced by password complexity rules

•Often written on a post-it note somewhere on the desk, or under the keyboard

•Better: Use an Acrostic –> "Too Many Passwords Cause Me Headaches" = 2 M P C M H

•It is a matter of education

Single Sign On

•Is it really a panacea? What happens when the single password gets compromised?

•Not realistic in the near-term for control systems, particularly with PLC's and Embedded Controllers

Two Factor Identification (what you have and what you know)

•Typically a device that generates a numerical key that gets entered along with your password

•Great for VPN's –prevents password sharing

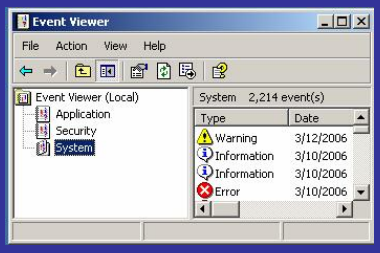
•Not realistic for control systems

Three Factor typically includes a Biometric characteristic-such as a fingerprint "who you are"

•Pyxis Medstation – uses a biometric fingerprint reader (great application – medication dispensing)

Common Omissions

- Failure to Make Back-ups
- Open Ports / Unneeded Services
- Unprotected Network Shares
- Failure to Apply Patches / Updates
- Failure to Review Logs



We have discussed backups –test them

•Also protect them from Damage (offsite location) and theft (maybe easier than accessing the system itself)

•Open Ports – Usually caused by unneeded services running on the box / Personal Firewall Helps

•Unprotected Network Shares –local chamber of commerce had their C-drive shared to the world and was wondering why they had virus problems

- •I have a coworker who put an anonymous FTP server on the internet and within 15 minutes had a Spanish version of *Runaway Jury* uploaded to the computer (Honeypots)

•Use 'Windows Updates' feature ---Greatly improved.

•Review Logs – The Windows Event Logs, Firewall Logs, Personal Firewall Logs, AV Logs, etc

- •Use Tools to Automate the Process

Inappropriate Software

- Unneeded Software
  - Games, Outlook Express, etc
- Sample Code / Scripts
- Insecure Code
  - VNC
- Untrustworthy Code

  Any cracker knows, "If I can get you to run MY program on YOUR computer, it's now MY computer."

Do not allow any unneeded software on plant floor computers, especially those dedicated to control functions

•Strictly Enforce

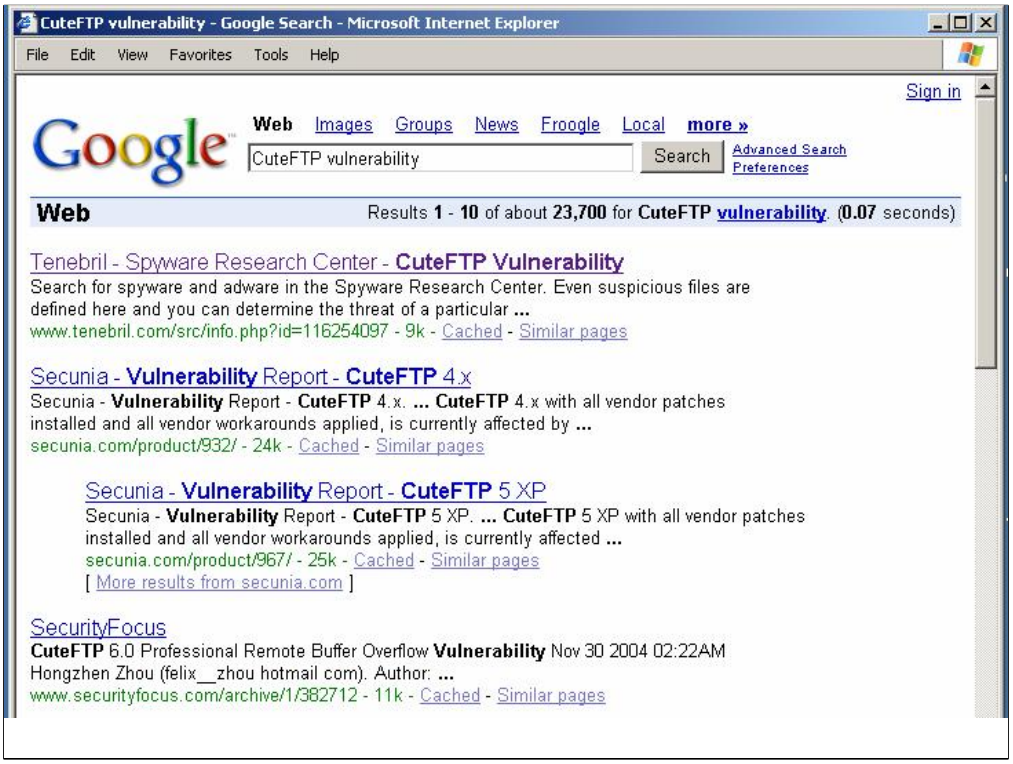
•Get a separate computer for them to read their mail on. Do not compromise a PC that is essential to control

Sample Code and scripts are used only to teach a concept and usually contain several vulnerabilities that can be exploited. Never leave on a production system.

Insecure Code—VNC is my favorite example to pick on. VNC is an open source remote control software. Only problem is that it uses a clear-text password. My preference is DameWareNT

Untrustworthy Code---the most poignant recent example was the Sony BMG Music CD's that installed a rootkit on any PC

Beware of Shareware



CuteFTP a popular file transfer program is an example of a program that I would call untrustworthy

Just do a Google search with the program name and the word ‘Vulnerability’

A few minutes of homework might prevent an **R-G-E**

By the way…FTP is another insecure Protocol. The passwords are sent via plan text.

So if you are moving sensitive data, (Like ‘Protected Health Information) encrypt the file, OR use FTP**S**

Physical Security

- Network Jacks
- Circumventing the OS
  - Knoppix
- Removing the HDD
  - USB External Drive Enclosure
- Protect Your Backups
- Lock Your Enclosures

•At most facilities you can simply connect a laptop into any available Network Jack and get right on their network and even out onto the Internet.

•You need to decide if this is OK for your environment.

•Some people do not patch in the jacks in the network closet until they have a legitimate user needing to connect. This provides minimal real protection and it a hassle for the network guy that has to run around plugging the jacks it. Besides, all you have to do is 'borrow' a jack from someone who is not using their computer or unplug a network printer.

•I have one client who uses DHCP Reservations. Basically what this means is that you will not get a Dynamic IP Address unless his DHCP Server recognizes the MAC address of your network card.

- •The work around here is to use PING or IPCONFIG to find an IP Address that is not being used and to set your Laptop to a Static IP Address

•Be Aware that it is possible under most cases to circumvent the Operating System and still access the file system.

- •For example KNOPPIX is an open source operating system that can be Booted from a CD and loads itself into RAM. It will mount a windows file system allowing the user complete access to the data on the hard drive. Any data of interest can be saved to a USB Flashdisk. This is quick and easy and no-one would know.
  - •Two countermeasures:
    - •use the Windows Encrypted File System –makes recovery difficult
    - •Disable/Remove the CD Drive & USB Ports –definite usability trade-offs
- •I have often recovered data by removing the Hard Drive and popping it into a USB External Drive Enclosure.
  - •My Laptop will then detect it as a secondary drive
  - •Works Great for Performing Backups also

•It should go without saying – but protect you backup files. Off-site to protect them from damage/disaster but also lock them up if they contain sensitive data. It may be easier to steal data off the backups than it is by circumventing the OS

•Since we are talking about the plant floor—lock your electrical enclosures.

- •You do not want just anyone 'plugging in' to your control equipment
  - •Or rebooting things---because they say a technician do it, why shouldn't they
  - •Flipping Circuit Breaker anecdote

Configuration Management

CM is a discipline applying technical and administrative direction and surveillance to:

- identify and document the functional and physical characteristics of a configuration item
- control changes to those characteristics
- record and report change processing and implementation status
- verify compliance with specified requirements

http://cs.wwc.edu/~aabyan/435/Configuration.html

IEEE Std. 1042-1987 IEEE Guide to Software Configuration Management

How can you tell if someone is fooling around with your system, if you don't have the configuration documented?

This sounds like basic Blocking & Tackling, but it is frequently overlooked. (Alligator Fighting)

Documenting your configuration will save you hours of downtime!

You need a process to make changes in a controlled manner

Ideally you would have an automated system to detect changes to a configuration

-Tripwire (linux-based tool – creates a MD5 Hash of selected filed and stores it as a snapshot in a database)

-Batch File

-RSGaurdian

The need for formalizing CM increases as you have more people involved in supporting the Plant Floor

How Well Do Your Plant Floor Work Practices Scale?

Favorite Tools

- DamewareNT – Enterprise Remote Control
- What's Up Gold - Uptime Monitoring
- Arpwatch – Detect new MAC Addresses (Linux)
- Knoppix – Bootable Linux CD
- NMAP – Scanner & Network Mapping Tool
- Nessus – Remote Agent Security Scanner
- MSBA – Microsoft Baseline Security Analyzer
- Dumpel - Dumps event logs to a text file
- MoveIT Freely – Command Line FTPS
- Logparser – Read/Analyze any log format

The only secure computer is one that's disconnected from all networks – especially power…

Mike Meyer

Don't be a security Nazi!

Take Prudent Measures but balance business needs

Business Unit Manager: "Never let a nerd shut you down"