



Challenging Information Systems Physical Access Controls

“And Sergeant, all you need to do to have an equal share of this money is crank this turret around a blow a hole in that door.”

(former) Lt. Kelly



©2005 The Hollis Group, Inc.

Slide 1



This Lecture's Agenda

- First, let's review the “three rings” concept
- Next, let's add a 0th ring – travel security
- Then, constrain ourselves to focus on threats / attacks against information assets
- To be rigorous, enumerate some threats
- Finally, DISCUSS techniques for defeating these defenses and workable tests
 - People-based attacks
 - Places-based attacks
 - Things-based attacks



©2005 The Hollis Group, Inc.

Slide 2

A Note On Style

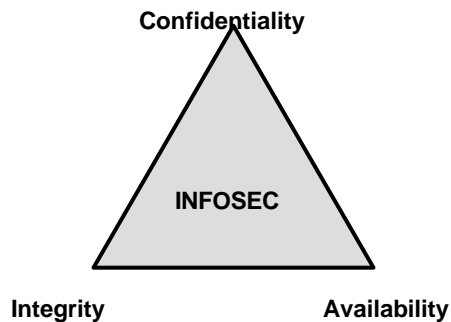
- ***“It is our goal to improve and extend information sharing between private industry and the government, particularly the FBI, when it comes to critical national infrastructures.”*** (InfraGard Mission Statement)
- **We’re going to emphasize the “sharing” by using a case study / discussion format**
- **The success of this format is largely dependent on YOUR contributions**



©2005 The Hollis Group, Inc.

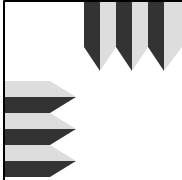
Slide 3

Continuing the Agenda, Three Targets for the Attack



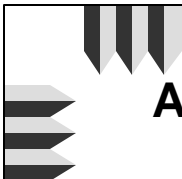
©2005 The Hollis Group, Inc.

Slide 4



So, Doing the Arithmetic

- **We have 36 penetration scenarios to do**
 - 4 rings of security to penetrate
 - times three vectors to follow
 - times three INFOSEC targets
- **Conceding that some might be “stretches”**
 - Such as an attack against the equipment (things) at the outermost ring to breach the confidentiality
 - Can’t anyone on the street see the fence?
- **Let’s treat this as a “red cell” exercise and solicit some of your ideas / war stories**



Also, Let’s Be Perfectly Clear CRIME IS AN OPTION!

- **Murder, attempted murder, kidnapping, arson**
- **Robbery (armed & strong-arm), smash-n-grab**
- **Carjacking, auto theft, burglary, theft**
- **Blackmail, extortion, coercion, intimidation**
- **Surveillance, eavesdropping, wiretapping**
- **Embezzlement, IP theft, staff raiding**



Three Rings of Security

- Let's use a case study company
- Mid-sized, high-tech manufacturing
- Corporate HQ and two remote locations
- R&D facilities at the HQ site
- And, some interesting additions...

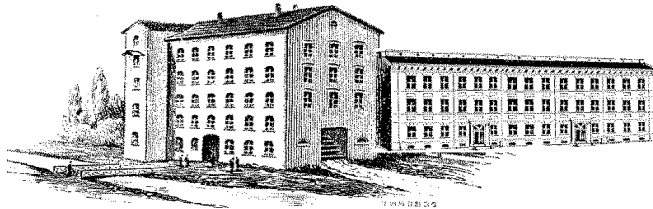


©2005 The Hollis Group, Inc.

Slide 7

Crockett Country Products, Inc. Murfreesboro, Tennessee

- 235,000 sq. ft. of facilities
- 40% prod., 25% dist., 20% admin, 15% R&D
- 705 employees / \$48 M in sales
 - (\$68K/employee)



©2005 The Hollis Group, Inc.

Slide 8



Crockett Country Products Company History

- **Ida May Crockett** (1884 - 1968)
 - Crockett Country Store, July 4, 1900
Cannon County, Tennessee, USA
- **April Crockett-Parsons** (1906 - 1973)
 - Crockett Country Products, Sept. '26 & Sept. '37
- **D. May Crockett** (1924 -)
 - Manager Manufacturing, 01/59
 - CEO, Crockett Country Products, Inc., Jan. '76
- **I. June Crockett** (1959 -)
 - Vice President, R&D, Mar. '90



©2005 The Hollis Group, Inc.

Slide 9



CCPI Product Lines

- **Plowder's Home Remedies**
 - OTC, personal care, cosmetics, toiletries
- **Granny's Candies**
 - confections, ice cream, & toppings
- **Ida May's Cannings**
 - jams, jellies, preserves, condiments
- **Crockett's Country Store Products**
 - dry goods, crafts, specialty foods
- **Nathaniel Crockett Homestead**
 - general store, crafts community, B & B



©2005 The Hollis Group, Inc.

Slide 10



Crockett Country Products - Confections Division

- **Manufactures products for:**
 - **Granny's Candies**
 - confections, ice cream, & toppings
 - **Ida May's Cannings**
 - jams, jellies, preserves
 - **Crockett's Country Store Products**
 - general store brand
 - **Nathaniel Crockett Homestead**
 - retail store & resort brand
- **Co-located with Plowder's Home Remedies**
 - Which has a minor problem



©2005 The Hollis Group, Inc.

Slide 11



CCPI's Minor Problem

- **Recently, a graduate project established the effectiveness of Granny's Hair Tonic**
- **FDA claims that it is a pharmaceutical, while CCPI claims that it is a "natural" product**
- **The proprietary product formula has been unchanged since 1899**
- **CCPI's operations are not CGMP compliant**
- **Increased capacity will be in production (pending FDA approval) in 10 months**



©2005 The Hollis Group, Inc.

Slide 12

CCPI's Unique Solution

- **Establish Canon Pharmaceuticals, Inc.**
 - Granny's Hair Tonic, biotech research
- **Conduct an accelerated, compassionate trial to establish GHGF's effectiveness**
- **Manufacture clinical lots of GHGF in a GMP-grade manufacturing facility**
- **Build a new GHGF production / research facility in Murfreesboro, TN**

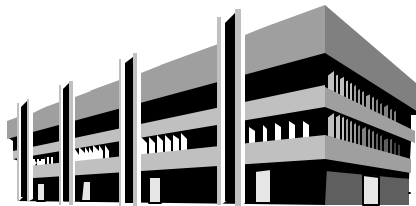


©2005 The Hollis Group, Inc.

Slide 13

Canon Pharmaceuticals, Inc. Murfreesboro, Tennessee

- **245,000 sq. ft. of facilities under construction**
- **50% prod., 5% dist., 5% admin, 40% R&D**
- **35 employees,
\$0 M in sales**
- **Projected sales next
year (US & EU) for
GHGF-derivatives
of \$(US) 206 M**



©2005 The Hollis Group, Inc.

Slide 14

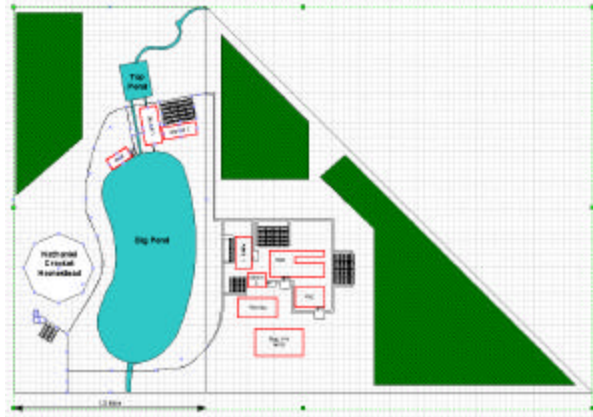
CCPI Property



©2005 The Hollis Group, Inc.

Slide 15

CCPI Site Plan – HQ

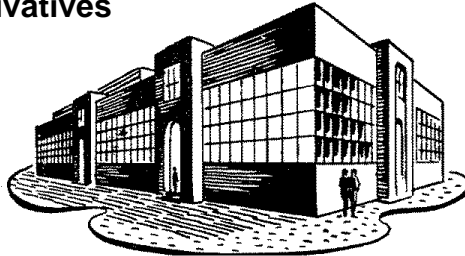


©2005 The Hollis Group, Inc.

Slide 16

Canon Pharmaceuticals, Inc. Malvern, PA, USA

- 52,000 sq. ft. of facilities (leased facility)
- 60% prod., 15% dist., 15% admin., 10% R&D
- 122 direct employees, 16 temporary staff
- \$(US) 2.6 M in sales (US & EC)
of GHGF-derivatives



©2005 The Hollis Group, Inc.

Slide 17

Quaker Holistic Medical Center, Gettysburg, Pennsylvania

- 150 bed community medical center
- Holistic wellness unit specializing in alternative healthcare
 - Chelation therapies
 - Herbal medicine
 - Midwifery
 - Magnetics
 - Accupuncture
- Experienced with outpatient, practice-based (i.e., at the doctors' offices) clinical trials



©2005 The Hollis Group, Inc.

Slide 18



CPI's Internet-Based GHGF Accelerated Clinical Study

- **A web-based study of GHGF efficacy in breast cancer chemotherapy follow-up**
- **The system will be designed so that study participants will fill in their own CRF's**
- **The system will include screens for the physician, the participant, and a "partner"**
- **The system will operate at the participant's home, or at the physician's office**



©2005 The Hollis Group, Inc.

Slide 19



Canon Pharmaceuticals, Inc. INFOSEC Challenges

- **Several agencies and consultants have advised CCPI of an international threat**
 - **Specifically an Asian multinational is trying to "duplicate" the GHGF active ingredient**
- **Also, one of the participating clinics has had a serious incident regarding patient records**
 - **For posting on the Internet**
- **Lastly, two of the participating physicians have "borrowed" some clinical supplies**



©2005 The Hollis Group, Inc.

Slide 20

Some Specific Data Security Needs for the I-Trial System:

- **Confidentiality**
 - Protection against surveillance
- **Integrity**
 - Protection against alteration
- **Availability**
 - Protection from loss
- **Quality**
 - Facilitation of participant compliance
- **Authenticity**
 - Demonstration of signer's identity



Negative and Positive Ways to Motivate (Compromise) People

- This concept is familiar to those from the law enforcement and intelligence communities
- The mnemonic usually taught to categorize these motivations is "MICE – PERSON"
- **Money, Ideology, Compromise, and Ego,**
 - The negative motivational factors
- **Professionalism, Ethics, Responsibility, Service, Operations, and Nomenclature**
 - The positive motivational factors



The Outer Ring – Targets

- **What can compromise:**
 - Confidentiality?
 - Integrity?
 - Availability?
 - Quality?
 - Authenticity?
- **What can we compromise to gain an alternate target or a higher level of compromise?**
- **What's the sequence?**



The Outer Ring – Attacks

- **People attacks**
 - Attack 1
 - Attack 2
- **Places attacks**
 - Attack 1
 - Attack 2
- **Things attacks**
 - Attack 1
 - Attack 2



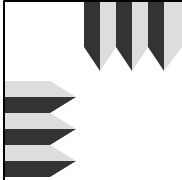
The Middle Ring – Targets

- **What can compromise:**
 - Confidentiality?
 - Integrity?
 - Availability?
 - Quality?
 - Authenticity?
- **What can we compromise to gain an alternate target or a higher level of compromise?**
- **What's the sequence?**



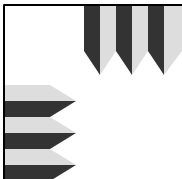
The Middle Ring – Attacks

- **People attacks**
 - Attack 1
 - Attack 2
- **Places attacks**
 - Attack 1
 - Attack 2
- **Things attacks**
 - Attack 1
 - Attack 2



The Inner Ring – Targets

- **What can compromise:**
 - Confidentiality?
 - Integrity?
 - Availability?
 - Quality?
 - Authenticity?
- **What can we compromise to gain an alternate target or a higher level of compromise?**
- **What's the sequence?**



The Inner Ring – Attacks

- **People attacks**
 - Attack 1
 - Attack 2
- **Places attacks**
 - Attack 1
 - Attack 2
- **Things attacks**
 - Attack 1
 - Attack 2





Defending the Laptop – Targets

- **What can compromise:**
 - Confidentiality?
 - Integrity?
 - Availability?
 - Quality?
 - Authenticity?
- **What can we compromise to gain an alternate target or a higher level of compromise?**
- **What's the sequence?**



Defending the Laptop – Targets

- **People attacks**
 - Attack 1
 - Attack 2
- **Places attacks**
 - Attack 1
 - Attack 2
- **Things attacks**
 - Attack 1
 - Attack 2

How Did We Do?

$$\text{RISK} = \sum_{\text{Threat \# 1}}^n \text{Scope} * \text{Probability}$$

- Masqueraders?
- Inside thieves?
- Malicious vandals?
- The “Agency”?
- General mishaps?
- Communication errors?
- Viruses and colds?
- Armed robbery?



©2005 The Hollis Group, Inc.

Slide 31

Questions and Discussion

Pierre de Hail, President
Risk Management Intl.
1118 Merrybrook Rd.
Suite 200
Collegeville, PA 19426
v - 610-584-8816
e - pdehail@comcast.net

Thomas Quinn, President
The Hollis Group, Inc.
PO Box 187
Paoli, PA 19301
v - 610-889-7350
f - 610-296-2339
e - tquinn@hollisgroup.com
www.hollisgroup.com



©2005 The Hollis Group, Inc.

Slide 32