The BotHerd is Coming: How Education & Technology Can Slow the Stampede!

Or…Dealing with a Series of Unfortunate Events

Copyright Martin Manjak 2006. This work is the intellectual property of the author. Permission is granted for this material to be shared for non-commercial, educational purposes, provided that this copyright statement appears on the reproduced materials and notice is given that the copying is by permission of the author. To disseminate otherwise or to republish requires written permission from the author.

Martin Manjak, ISO
Justin Azoff, Network Analyst
Background Info

- Marty - Director of ResNet since inception at U@A (1995), recently appointed ISO (2/06)
- Justin - Network Analyst, former student employee of Marty’s, reigning Nessus, Nmap, & Scripting guru.
Organizational Info

- ResNet & The Student Help Desk are part of Client Support Services, a division ITS
- Telecom-separate division of ITS
- Both report to Campus CIO
About UAlbany

- One of Four University Centers of SUNY
- 614 Full Time Faculty
- 311 Part Time Faculty
- 12,000 Undergrads
- 5,400 Grads
- 7,773 Residents
- 7,796 Fall ’06 System Registrations
Some History

- UAlbany Escaped!
- 2004: We started scanning and kicking
- All hell broke loose!!!!
Snapshot of September, 2004

- 486 systems booted from network
- At one point, over 800 systems suspended
- 1000+ open tickets first week of class
- Help Desk Hammered!
- 3 Week Wait for Remediation Appt.
- Parents calling CIO and President’s Ofc.
- Our fault: “Your network infected my machine!”
Never Again!

- “Today was the worst day in the history of the Internet.” –Justin L., Student Help Desk Shift Supervisor.
How Will We Prevent Reoccurrence?

- Technical Track
- Social Engineering Track
  - “More about people than technology.”
  - “Never stop working on awareness.”
    - Ced Bennett
We “social” you

- Obviously the message about securing your machine wasn’t getting through.
  - “Did you read the letter we sent?!”
  - “I don’t know much about computers.”

- Needed a different approach

- Technology, per se, is a turn off
People only do things for a reason.
The assumption that students would want to secure their machines was based on the premise that they understood the threats.
Painfully false!
Awareness needed to motivate “right” action
Focus shifts from “You need to do this,” to “Hey, did you hear the story about…?”
Craft a narrative where students can self-identify
Design is Key

- This approach requires first rate design and graphics.
- Pictures of people; not screen shots.
- Focus on behavior to elicit self recognition: “Gee, I do that.”
- Use behavior shift as key to implementation of safeguards.
Collect all Three and Trade Them with Your Friends.

- Created a series of brochures to spark interest in complete set
- Each brochure focused on one threat or behavior
- Allowed us to be more diverse in representing student body
- Created “buzz” for …
Coming soon…

- Network Survival Kit
- All brochures made reference to the kit in an attempt to create demand prior to arrival.
- Coordination with ResLife crucial to getting kit distributed on day one.
Orientation Indoctrination

- Redesigned IT presentation for summer orientation of incoming students
- Much more emphasis on security requirements
- Sanctions: loss of service, restoration fee
- Parents informed, too
No letter this time

- Letter was an abysmal failure to alert arrivals to security requirements and consequences
- Student employee suggested postcard
- Obvious advantages:
  - You don’t have to open it
  - Visually more interesting
  - Cheaper to mail (but more expensive to produce)
  - Can time arrival
Taking no chances…Security Quiz

- In past, all students required to take an online ethics quiz before they receive unrestricted IP
- For fall 05, security component added
- Students must pass through this gate
- Must get 10 out of 10 to pass
- Quiz based on our security requirements
No Excuses

- Using the network means you passed the quiz
- Which means you know about our security requirements
- Which means you can’t complain when we kick you off for failing to implement them
- Also works for DMCA violations
The Numbers, Please

- Tracker Statistics 08/18/2004 to 09/30/2004

<table>
<thead>
<tr>
<th>Ticket Counts</th>
<th>2004</th>
</tr>
</thead>
<tbody>
<tr>
<td>Worked on</td>
<td>3057</td>
</tr>
<tr>
<td>Opened</td>
<td>2967</td>
</tr>
<tr>
<td>Closed</td>
<td>2836</td>
</tr>
<tr>
<td>To Telecom</td>
<td>36</td>
</tr>
<tr>
<td>Email</td>
<td>2321</td>
</tr>
<tr>
<td>Phone/Walk in</td>
<td>646</td>
</tr>
</tbody>
</table>
**How did we do?**

- Tracker Statistics 08/18/2005 to 09/30/2005

<table>
<thead>
<tr>
<th>Ticket Counts</th>
<th>2004</th>
<th>2005</th>
</tr>
</thead>
<tbody>
<tr>
<td>Worked on</td>
<td>3057</td>
<td>1681</td>
</tr>
<tr>
<td>Opened</td>
<td>2967</td>
<td>1613</td>
</tr>
<tr>
<td>Closed</td>
<td>2836</td>
<td>1586</td>
</tr>
<tr>
<td>To Telecom</td>
<td>36</td>
<td>50</td>
</tr>
<tr>
<td>Email</td>
<td>2321</td>
<td>1073</td>
</tr>
<tr>
<td>Phone/Walk in</td>
<td>646</td>
<td>540</td>
</tr>
</tbody>
</table>
Comparisons

Registrations vs. Tickets

- Tickets
- Registrations
Benchmarking

- In 2004, 5787 machines registered
- In 2005, 7140 machines registered
- 23% Increase in registered systems
- 1376 fewer tickets; 45% decrease in tickets
And now, my esteemed colleague...

- XP SP2 played big role in reduction of hacked machines
- But they’re still out there, and patches can’t stop students from being click happy.
- New threat vectors emerging, i.e, IM
- How do we deal with these?