A Little History

• The Pragmatic CSO debuted in 2007
• A few things have changed since then…
• A lot of things have not…
• Good management practices never go out of style
A Day in the Life of a CISO, as told by Shakespeare
6:30  Wake up
7:30  Get to Office
7:31  Fight Fires
9 AM
10 AM
11 AM
Noon
8:30
Take call from key supplier
9:00 Meet with CIO re: Audit
10:00 Investigate Possible Breach
11:00 Prepare Status Reports
Don't forget Bar Charts

(Don't forget bar charts)
Meet with VP, Development
Return call to Police

12:30
1:00

Brown Bag Lunch with Developers
re: BSIMM
Meet w/ GC re: Breach
<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Noon</td>
<td></td>
</tr>
<tr>
<td>1 PM</td>
<td></td>
</tr>
<tr>
<td>2 PM</td>
<td></td>
</tr>
<tr>
<td>3 PM</td>
<td>Vendor Briefing</td>
</tr>
<tr>
<td>4 PM</td>
<td></td>
</tr>
<tr>
<td>5 PM</td>
<td></td>
</tr>
<tr>
<td>6 PM</td>
<td></td>
</tr>
<tr>
<td>7 PM</td>
<td></td>
</tr>
</tbody>
</table>
3:00 Meet with CFO & CIO re: Budget
3:30

Order new iPad for VP Sales

http://www.flickr.com/photos/wader/4900313960/
Meet with Auditors
re: Compensating Control
Meet with Frank from Accounting

Clean Machine (again)
A Day in the Life

Thursday, Mar 1 2012

4 PM

5 PM

6 PM

Head home (Thanks the Gods)

7 PM

8 PM

9 PM

10 PM

6:00 Head Home.
Local Weather
Alpharetta

Phone

SIEM
Missed Call 8:47 PM

SIEM
Missed Call 8:47 PM

SIEM
Missed Call 8:47 PM

SIEM
Missed Call 8:46 PM

Messages

759-73 8:51 PM

Seriously, our email is being sent to Beijing right now.

759-73 8:51 PM

The APT is here. Call now!

Calendar
11:00 Go to Sleep
Wake Up.
Get to Office.
Fight Fires.

Wash. Rinse. Repeat.

Repeat.
No Wonder We’re Miserable
Security Folks = Junkies

- Addicted to the battle
- Addicted to the dysfunction
- Addicted to throwing products at the problem
- Addicted to fighting with the auditors
- You need a 12-step program
What is your job?
Your job is to protect the assets of the organization and ensure business can operate.
Why bother at all?

• The Reasons to Secure are about the business...
  – Maintain business system availability
  – Protect intellectual property
  – Limit corporate liability
  – Safeguard the corporate brand
  – Ensure compliance
Success
Security Success is…

• Being consulted about security issues BEFORE it’s too late
• (Largely) getting out of the day to day firefighting
• Understanding what NOT to get done
• Living to fight another day after an incident
• Understanding your progress based on data, not voodoo
• Turning the auditors into allies, instead of enemies
We can do this, right?
P-CSO: A 12-step Program for security pros...
Section 1: Plan to Be Pragmatic

Step 1: Assess the Value of Your Business Systems

Step 2: Baseline Your Environment

Step 3: Manage Expectations
Step 1: Assess the Value of Your Business Systems

- Business Systems vs. Assets
- Rankings
  - What does downtime cost?
  - Who uses the system?
  - How easy to replace?
  - Who gets fired if it goes down?
- Everything cannot be #1
- Your opinion doesn’t matter
Step 2: Baseline Your Environment

• Is your security effective?
  – How do you know?
  – Assess Maturity

• Current State
  – Technical tests
  – Incident review
  – Security awareness
  – Security perception

• Quantify where possible
  – Gives you a basis for comparison
Step 3: Manage Expectations

• It is what it is
  – Tactical security action plan

• The importance of buy-in
  – Fear vs. knowledge
  – Perception of Control
  – End-state maturity – where do you want to be?

• Educate about the program
  – 12 Steps
  – Reporting progress/milestones
  – Defining success
Section 2: Build a Pragmatic Security Environment

Step 4: Build Your Security Business Plan

Step 5: Sell the Story

Step 6: Procure the Solution
Step 4: Build Your Security Business Plan

- A business plan?
  - Positioning (why bother?)
  - Priorities (what to protect?)
  - Security architecture (how?)
  - Service levels (how much?)
  - Timelines and milestones (when?)

- Define future state

- Plan is a living document
Step 5: Sell the Story

• Estimate funding requirements
• Plays directly into end state maturity decision
• Build scenarios
  – Fully funded
  – Likely case
  – Worst case
• Be very clear about what WON’T get done at certain funding levels
Step 6: Get a Quick Win

• With funding, now you need to show value and earn credibility. Quickly.
• Choosing the project
  – Timeline
  – Chance of success
  – Impact to security posture
• Start slowly, make sure it works.
• Then beat the drum!
Section 3: Run Your Security Organization Pragmatically

Step 7: Operate/Monitor

Step 8: Contain the Problem

Step 9: Train the Users

Step 10: Assure your Defenses
Step 7: Operate/Monitor

- Prioritize fiercely
  - Security research/analysis
  - Vulnerability management evolution
- Security dashboard
  - Map/Attack paths
  - Thresholds (react faster)
  - Correlation?
- Manage to service levels
- Outsource non-strategic functions
Layered Defenses

- Pragmatic CSOs know there is no 100% security
  - You’ve been managing expectations accordingly, right?
- Layer controls and defenses to ensure no single point of failure
- Different controls for different valued assets (high-wall/lower-wall)
- Factor mobility and business partners into architecture
Step 8: Contain the Problem

- Incident response plan
  - Containment
  - Forensics/Investigation
    - Malware Analysis
  - Notification/disclosure (internal & external)
- Shared accountability driven by communications
- Come clean ASAP
  - The goal: Live to fight another day
Step 9: Train the Users

- Users first and last line of defense
- Carrot and stick – “Teaching moments”
- Consistency and perseverance (and kick butt content)
- The only way to fail at security awareness is to give up
Step 10: Assure Your Defenses

• Aggressive ongoing testing of business system security
  – Encompass apps, networks, data center, endpoints

• Tools vs. people

• Use of exploits

• Social engineering

• How to communicate the results
Section 4: Communicate Your Value

Step 11: Analyze Your Progress

Step 12: Comply without Going Nuts
Step 11: Analyze Your Progress

- Security metrics controversy
- What to measure?
  - Important to senior management
  - Important to running your business
- Relate back to business plan commitments
- Analytics
  - Big Data
  - Peer Groups
Step 12: Comply Without Going Nuts

- Good security = compliance (unless assessor is a dolt)
  - Not vice-versa
- Treat your auditor as a peer
  - On the same team
  - Can facilitate or impede your work
  - Understand their motivation
- Painless audits
  - Show that you listened
  - Present the business plan
  - Come clean about incidents
  - Give them what they want
Thank you!

P-CSO 2.0
August 2013

http://www.pragmaticcso.com

Register and get the Introduction
5 Tips to be a Better CSO
You are a business person, not a security person
Prioritize Fiercely
Stay Current
React Faster and Better
Plan for Problems