Information Security is Foundational to Enterprise Risk Management

A Strategy for Effective and Sustainable Risk Management

~ The Genesis of a Patch and Vulnerability Group (The PVG) ~

Braun Tacon
ISSA Regional Meeting
Originally Presented April 13th 2006
Revised April 29th 2009

BraunsBlog.Com

Quick Bio

- **Who am I**? Braun Tacon. Over 25 years experience as a Strategist, Tactician, and Project Manager with an extensive background in Security, Process, and Documentation from both a Strategic and Tactical Point of View.
- **My Current Passion**: I have many passions, and one of them is writing. I have a blog, BraunsBlog, where I recently claimed that I would opine on the topic of Information Security. This seems as good of an opine as any.
- **Evolution of this Document**: This is a revised version of a presentation I gave three years ago on the topic of Enterprise Risk Management at the Information System Security Association (ISSA) NW Regional Conference, April 2006. View it in the past tense but I believe it is as valid today as it was then, perhaps more so.
- **My Current Interests**? To focus on People, Process and Technology as a Means of Delivering needed Innovation and Continual Service Improvement
- **My Current Focus**? Applying Strategic Vision with a Tactical Approach to Consistently Deliver Momentum and Closure for Large Scale Projects.

Agenda

- Key Presentation Objectives
- The Mission
- Current State
- How Did We Get Here
- Lessons Learned (and then some)
- The 4 P's
- Braun's Crystal Ball
- Summary/Recap

Key Presentation Objectives

1. Understanding why **Effective Vulnerability Management** is **Needed** in today's world and why it is a **Key Predecessor** for **Effective Information Security** and **Enterprise Risk Management** in a **Large Environment**
2. Seeing how a **Strategic Program** along with **Well Designed Reporting** goes **Hand in Hand** to **Deliver Successful** and **Sustainable Risk Management**
3. **Leveraging** our **Lessons Learned** to **Help** You **Improve** your **Overall Risk Management Posture**

The Mission

To **Increase** our **Security**, **ROI**, and **Operational Visibility** through the **Use** of **Tools**, **Process**, and **Reporting**

Current State – April 2006

- From the **Highest Level**, our **Global Patching Process** is as follows:
  - **Windows**-centric, both **Desktop** and **Server**
  - A **Defined Process**, **Repeated** on a **Monthly** cycle as driven by Microsoft Patching Notices, with timelines for patching completion
  - A **Defined Process** with **Prescribed Escalation** in the event that **Published Exploits** bring about an **Increased Risk Level** to our **Computing Systems**
  - A **Formal** and **Ongoing Process of Measurement** which **Gauges** both our **Current Risk Level**, and the **Success** of our **Patching Efforts**

How Did We Get Here

- **Begin with the end in mind**
  - Back in late 2002, my boss calls me into her office
  - She asks me if I'm familiar with the term, "Vulnerability Management"
  - I reply, "…nope, but I'll get familiar"

How Did We Get Here

- **When the truth hurts**
  - My first **Finding**, "…we **Aren't Patching**"
  - From peers and management alike: "We **Do Patch**. You **Are Mistaken**"
  - Service **Provider** says, "…**Patching BAD, Service Pack GOOD**"
  - SQL **Slammer Hits** the **Internet** in **January 2003**
  - We **Survive Unscathed** and in **Response**…there is a **Collective Yawn**

How Did We Get Here

- **Reality intrudes**
  - April 15th 2003
  - SQL Slammer
  - It's **NOT** a good day

How Did We Get Here

- **Ok…you've Got my Attention, now what?**
  - We need to do **SOMETHING**
  - Got any **Ideas**?
  - Let's **Not Reinvent** the **Wheel**

How Did We Get Here

- **Start from scratch? Not quite**
  - **From** the **Beginning** we wanted a **Standards Based Solution**
  - The **National Institute** of **Standards** and **Technology** (**NIST**) provides a multitude of **Standards** and **Guidelines** for use by **IT Professionals** in **Government** and **Business** alike
  - **NIST Special Publication 800-40** (now 800-40 v2) Creating a Patch and Vulnerability Management Program became our **Standard** (http://csrc.nist.gov/publications/nistpubs/)

How Did We Get Here

- **Enter the PVG**
  - **Core** to SP 800-40 is the **Concept** of the PVG, "Patch and Vulnerability Group". From the document's Executive Summary

    "Organizations should Create a Patch and Vulnerability Management Group (PVG) to Facilitate the Identification and Distribution of Patches Within the Organization"

  - The **Standard** defines 11 principle duties of a PVG. For our purposes, we chose 6
    - Inventory **Assets**
    - Monitor for **Threats**
    - Identify **Remediation** (patches) for organization
    - Maintain a **Database** of **Required Patches**
    - Understand **Risk**, **Vulnerability**, and **Remediation Requirements**
    - Monitor **Remediation** efforts and **Report** on **Progress**

How Did We Get Here

- **Enter the PVG**
  - The other **Core Concept** that **Drives** the **PVG Process**

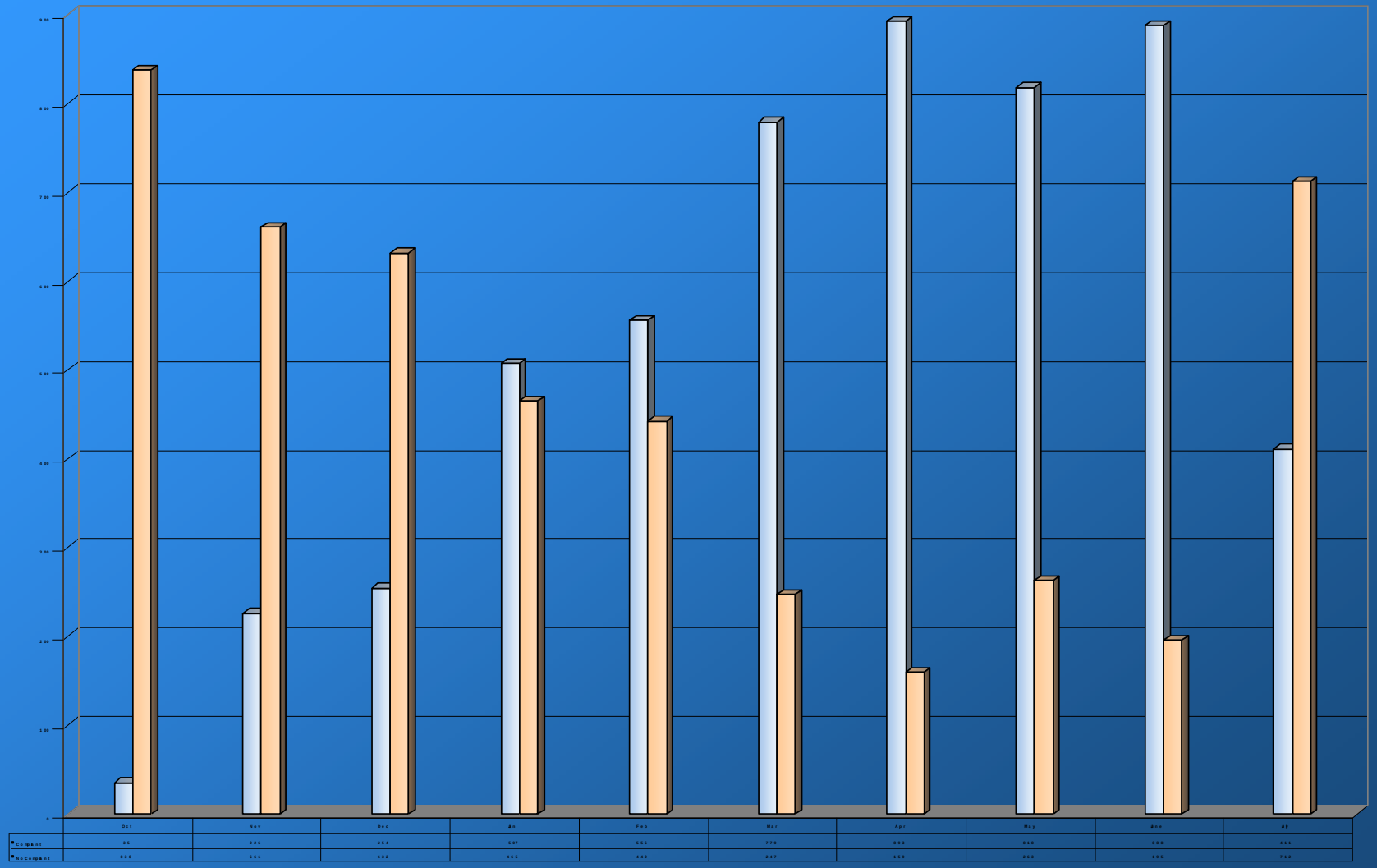
    "Organizations should Consistently Measure the Effectiveness of their Patch and Vulnerability Management Program and Apply Corrective Actions as Necessary"

  - **Continual Service Improvement** is **Key**, and is a great segue to the next slide

How Did We Get Here

- **Patching is *a Process, not an Event***
  - Began **Compliance Tracking** and **Reporting** in **Oct 2003**
  - **Servers** began at **5% Compliance**
  - In **6 months**, **Servers** were at **85% Compliance**

Windows 2000 Server Baseline - Critical and Regular Patches



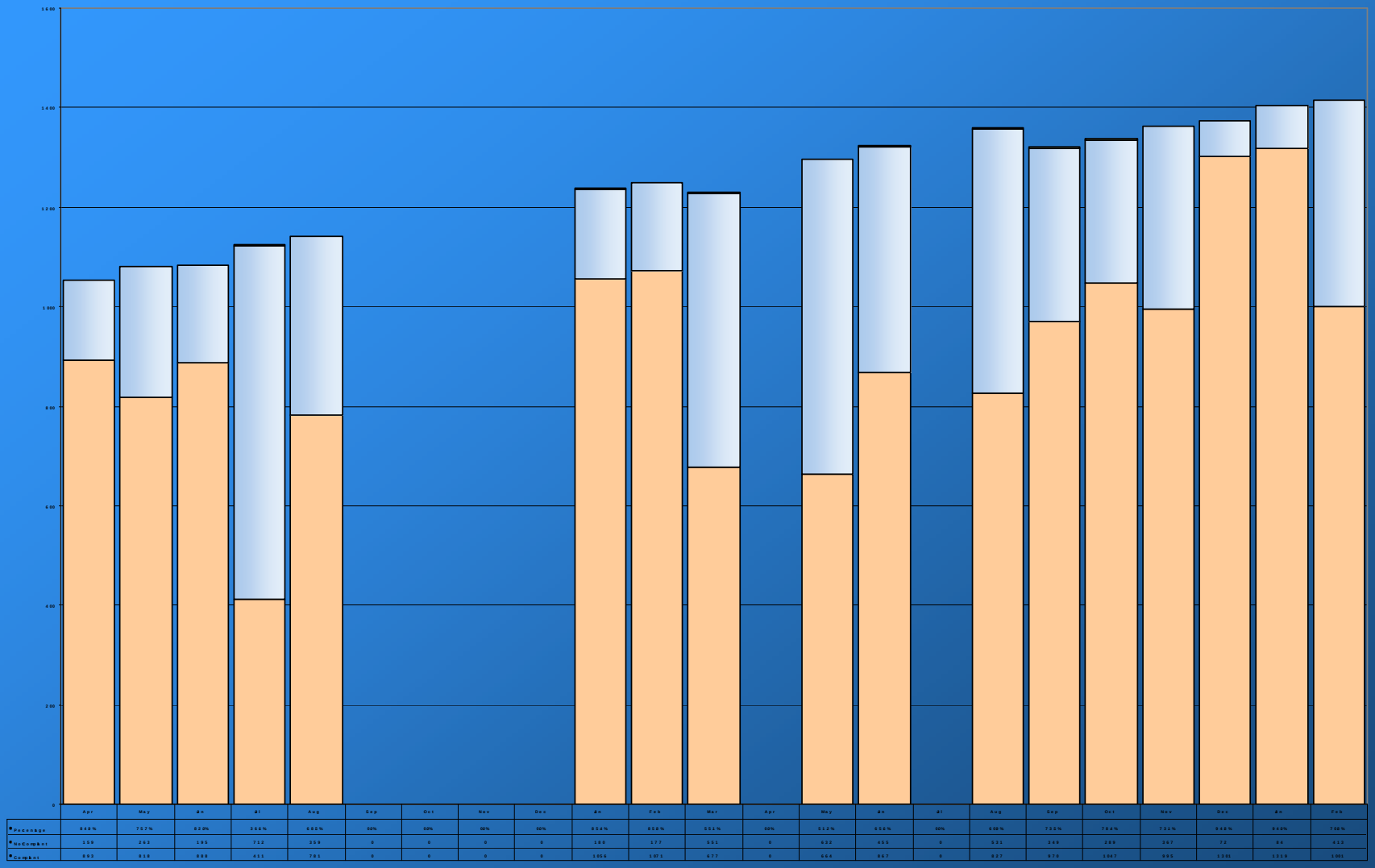
How Did We Get Here

- **Speed Bumps everywhere**
  - Scripts v SMS
    - At first we **Relied Completely** on **Scripts**
    - Unfortunately **Scripts** were very **Custom**; what was **Needed** was an **Automated Process** to **Identify** the **Risk** and **Manage** the **Work**
    - **SMS Won Out**, and we **Made** the **Change** in late **2004**

How Did We Get Here

- **Speed Bumps everywhere**
  - **Reporting** shows **Switching** to **SMS** caused us to **Loose Momentum**
    - We could not generate reports for a few months
    - Early reports were inaccurate, things are much better now
  - **SMS** is **Now Delivering** what **Information Security Needs**
  - **Remember…Patching is *a Process, not an Event***

Windows 2000 Server Patch Baseline

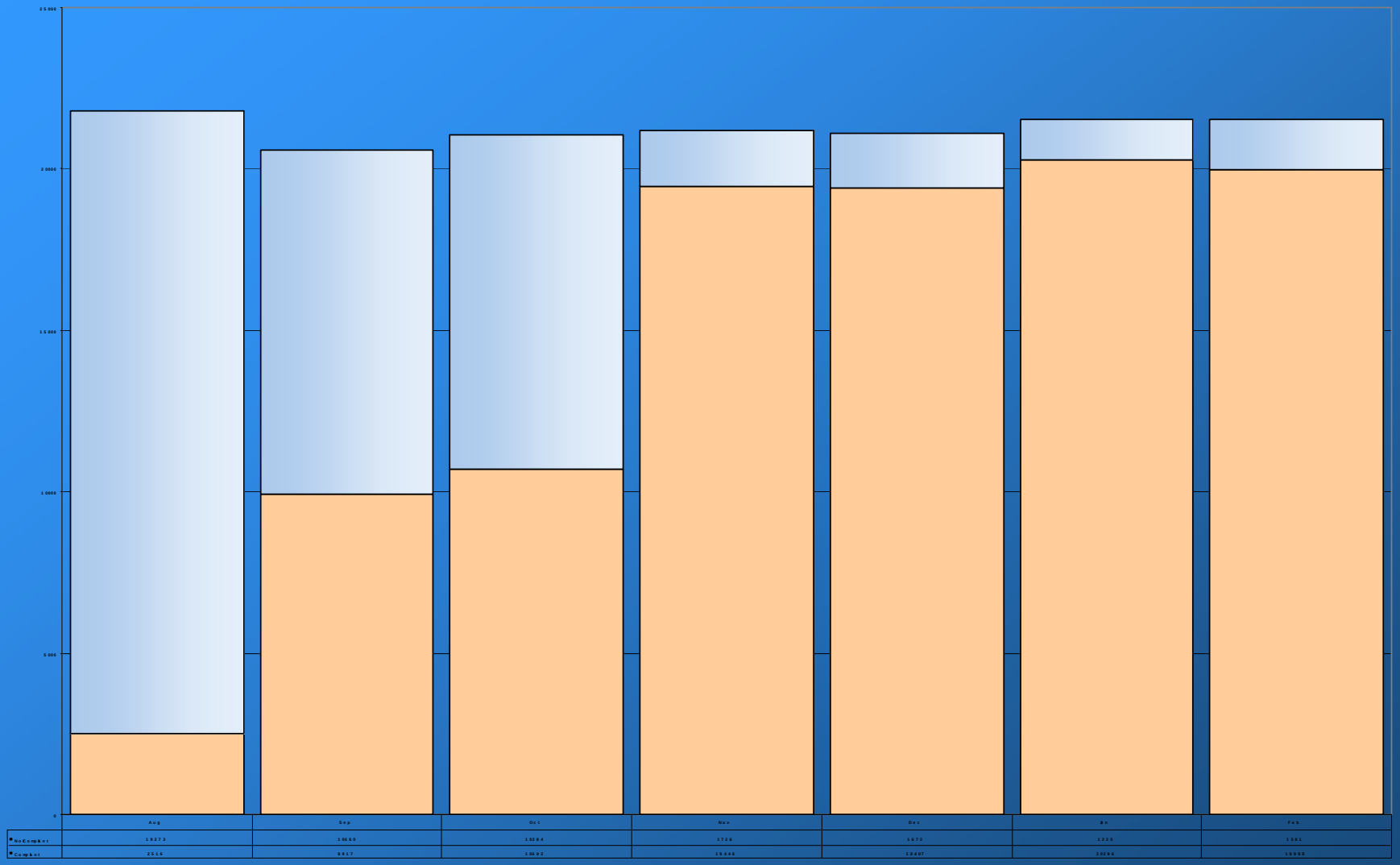


	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb
Percentage	849%	757%	820%	366%	685%	00%	00%	00%	00%	854%	858%	551%	00%	512%	656%	00%	630%	734%	784%	731%	948%	940%	700%
NoCompliant	159	263	195	712	359	0	0	0	0	180	177	551	0	632	455	0	531	349	269	367	72	94	413
Compliant	893	818	889	411	781	0	0	0	0	1054	1071	677	0	664	867	0	827	970	1047	995	1301	1319	1001

Lessons Learned

- **Utopia? Probably not, but with some effort you might get a little Nirvana**
  - That **85%** was for **Servers only**, **not Desktops**
  - We did a **Root Cause Analysis** and got **Pretty Good** at **Desktops** too
  - We now **Consistently Deliver 95% Compliance for Desktops**
  - **YMMV** (Your Mileage May Vary)

Windows Desktop Patch Baseline



More Lessons Learned

- **Just when you think everything is going along fine – Zotob**
  - **Zotob Attacks** within 3 days of Microsoft patch announcement
  - **Betting** the **Odds**, we **Work** the **Established Process**
  - Our **Luck Runs Out** 8 hours too soon
  - We **Experience Disruption**. Some **Cleanup** is **Needed**

Lessons Applied

- **Pick yourself up, dust yourself off, start all over again**
  - We **Gathered** the **Facts**
  - We **Learned** some **Lessons**
  - And finally, we **Made** some **Changes**
    - *Cut Desktop Patching time by half, and Made Application Mandatory*
    - *No change to Server Patching*
    - *Defined our Escalation Criteria*
    - *Defined our Escalation Roles*
    - *Defined our Escalation Communication Paths*

The 4 P's

- **If you want to have Success, you have to Write it Down**
  - The **4 P's** – **Policy**, **Process**, **Procedure** and **People**
  - Many **Folks Confuse** these **Terms**…**Remember**
    - ***Policy*** – *Clearly states our goals and objectives*
    - ***Process*** – *What we need to do*
    - ***Procedure*** – *How we do it*
    - ***People*** – *Define your roles*

PVG/PATCH MANAGEMENT

PVG/Patch Management (Patch and Vulnerability Group) Process and Procedures

Overview

From the highest level, XXXX's current PVG patching process is as follows:

- Windows-centric, both desktop and server
- A defined process, repeated on a monthly cycle as driven by Microsoft Patching Notices, with timelines for patching completion
- A defined process for timeline escalation in the event that published exploits bring about an increased risk level to XXXX computing systems
- A formal and ongoing process of measurement which gauges both our current risk level, and the success of our patching efforts

Roles and responsibilities

The XXXX Global IT Security Operations Manager (GITSOM) will be responsible for the oversight of the vulnerability management process, as well as tracking of and reporting of any patch initiatives sponsored by the Patch and Vulnerability Group (PVG).

The PVG Review Team will be comprised of both XXXX and XXX members who will consider and approve any escalation to the normal patching process, as the risk level dictates.

XXX will manage the patching of XXXX systems as defined by contract. Groups that maintain their own patching infrastructure, i.e. EMEA, Memphis, Retail and Subs will be responsible for insuring the patching of their infrastructure as defined.

Process

1. On the second Tuesday of each month, Microsoft will announce and release a set of patches that they deem applicable for that monthly patch cycle.

PATCH MANAGEMENT

Procedures

1. Microsoft Patch Announcements shall be sent to XXX and the PVG PatchNotification Mailbox
2. XXX shall deliver recommendations in a document which contains the following information at a minimum for each published vulnerability (**bolded** text):

   Bulletin: MS05-0XX
   Description: Vulnerability in the Windows FTP Client Could Allow File Transfer Location Tampering (QNumber)
   Vendor Severity Rating: Moderate
   Bulletin URL: http://www.microsoft.com/technet/security/bulletin/ms05-0XX.mspx
   Summary: A tampering vulnerability exists in the Windows FTP client. This vulnerability could allow an attacker to modify the intended destination location for a file transfer, when a client has manually chosen to transfer a file by using FTP. This vulnerability could allow the attacker to write the file to any file system that is located on an affected system.
   Desktop Recommendation:
   Test and apply to all WinXP SP1 machines and Win2k SP4 machines with IE 6 SP1
   Server Recommendation:
   Test and apply to all Windows 2003 servers and any Windows 2000/SP4 server with IE 6/SP1
3. PVG shall review, accept or reject any or all of the XXX recommendation and make them available in the Regular Patch Notification as a linked document called PVG Patch Notification Details. This document shall contain the following information at a minimum:

   Executive Summary *1*
   Patch Summary *1*
   Patch Schedule *1*
   Microsoft Special Comments *1*
   XXX Recommendations *2*
4. PVG shall maintain at a minimum the following e-mail lists in Outlook: Lst-PVG.ReviewTeam, Lst-PVG.Patchnotification.All , Lst-PVG.RTM, and Lst-PVG.SMSTeam. IOS shall maintain at a minimum the following e-mail list in Outlook:

Braun's Crystal Ball

- **Bottling the Egg. How does all of this fit in with Enterprise Risk Management**
  - **Enterprise Risk Management Allows** the **Business** to **Make Informed Choices** about **Acceptable Risk** in order to **Meet Specific Business Goals**
  - A **Principle Pillar** of **ERM** is **Information Security**
  - An **Essential Component** of **Information Security** is **Vulnerability Management**
  - **Information Security** is **Only One** of the **Many Disciplines** that **Support ERM**

Braun's Crystal Ball

- Here are some **Other Examples** of **Disciplines** that might be **Found Supporting Enterprise Risk Management**
  - **Compliance**
  - **Change Management**
  - **Finance**
  - **Legal**
  - **HR**
  - **Business Continuity and Recovery**
  - **Incident Response**
  - **Crisis Management**
  - **Loss Prevention (Fraud)**
  - **Health & Safety**
  - **Liability**

Braun's Crystal Ball

Each of these **Discipline Contribute** uniquely to **Ensure Enterprise Risk** is **Managed** so that it **Protects** the **Enterprise** from **Undue Harm**, but at the same time **Allows** the **Business** to **Function…as a Business**

Braun's Crystal Ball

- As stated earlier, **Vulnerability Management** is essential to **Information Security** and **Foundational** to **Enterprise Risk Management**
  - There is "**No One Standard**" for **Vulnerability Management**
  - It should be **Tailored** to your **Industry** and **Needs**
  - Whatever **Path** you take you should **Strive** for **Consistency**, **Clarity**, and **Sustainability** in your **4 P's**

Summary/Recap

- **ERM** is a **Enterprise Strategy** for **Managing** the **Risk Appetite** of an **Organization**
- The **PVG** is an **Example** of one **Approach** to **Meet** those **Goals**; by one **Discipline**
- **Similar Approaches** can be used by other **Disciplines Across** the entire **Risk Management Portfolio**