Integrating Vulnerability and Patch Management into IT GRC

Thursday, September 20, 2012

3:15 – 4:15 PM

George G. McBride

Director, IT Risk Management Johnson & Johnson

IT Governance, Risk & Compliance

MIS TRAINING INSTITUTE

Agenda: Definition & Introduction

- Review Vulnerability and Patch Management
  - Highlight Differences
- Vulnerability Management Program (VPM)
- Patch Management Program
- Lessons Learned | War Stories
- Things To Apply At Work
- Additional Resources
- Questions | Comments | Thoughts

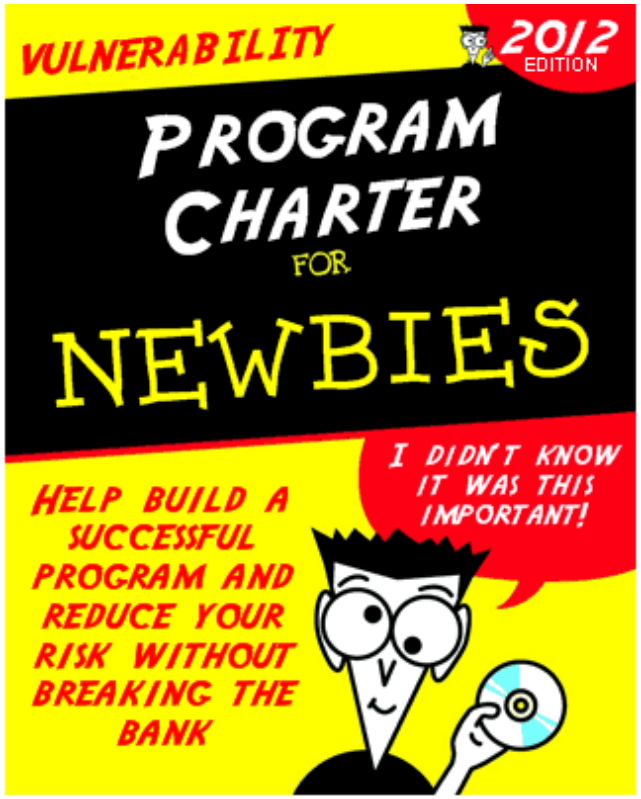
Vulnerability Management Components

Vulnerability Management Definition

- Industry Standard Security Practice
  - *That means you should be doing it!*
- Proactively reduce the risk of vulnerability exploitation
  - *So, you'll have to know the vulnerabilities and risks!*
- Should be staffed appropriately with the right tools
  - *HINT: It's more than just one person.*
- Should have a program around it (We'll talk about that)
  - *Helps to continue to evolve the program*
- Includes Patch Management as a solution

Program

- Charter:
  - Mission | People | Organization
- Funding
  - Tools, Payroll, Infrastructure
  - Service Providers
- Communications
  - Metrics, Awareness, Training
- Organization
  - Staffing Model



Policy, Procedures, Practices, etc.

- Vulnerability And Patch Management Policy
  - Memorializes the Program Charter
  - Get appropriate approval and awareness
- Standard Operating Procedures
  - How vulnerabilities are prioritized
  - How risk is measured
  - How interfaces to other groups (such as operations who may push the patches out)
  - And probably many others.

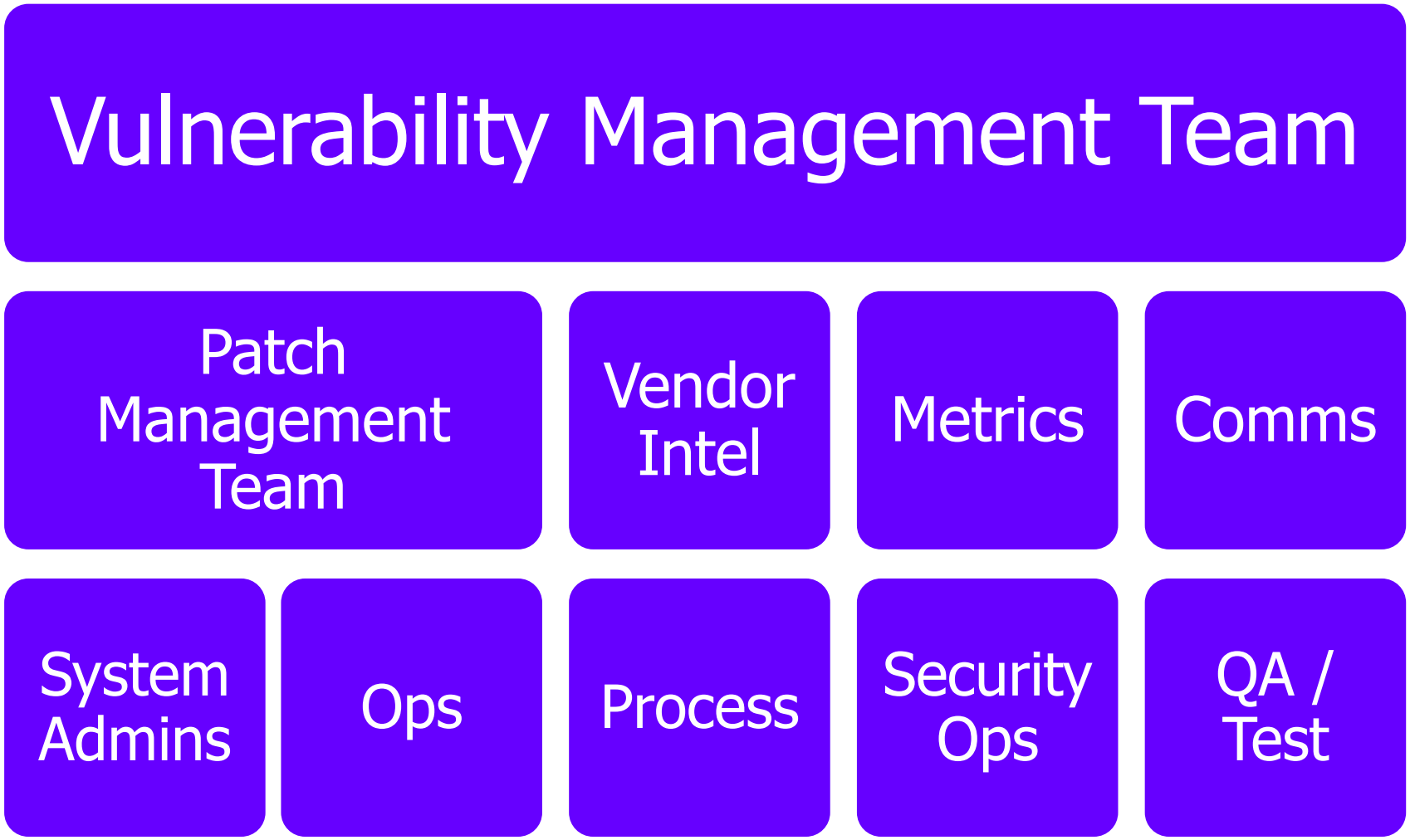
Policy, Procedures, Practices, etc. (2)

- Standards
  - Documents the solutions (tools) in place and their versions and configurations
- Practices:
  - How vulnerability intel comes in to the organization
- Consider the Audit Program
  - Partner with the Audit team to develop 'auditable' documents
  - Validate with the subject matter experts on the team
  - Don't over-engineer or over-comply

What Assets Are In Scope?

- Platforms:
  - Servers | Workstations | Virtual Machines | Blades
  - Mobile
  - Printers | Copiers
  - VoIP Phones
  - DVR/CAMS
  - Remote Monitoring Sensors, DVRs, IP Cameras
  - SCADA
  - Infrastructure

Organizational Chart



Organization - Roles & Responsibilities

- Should consider the following roles at a minimum:
  - Tools / Admins – keeps things running and focuses on specialty tools and infrastructure
  - Inventory team – keeps the inventory up to date
  - Vulnerability team – maintains current state of vulnerabilities
  - Build Teams – may develop or package patches
  - QA Teams – tests the builds and develops fail plans
  - Vendor Management – relationships with key vendors

User Awareness and Training

- Training in the VPM Team
  - Tools, Processes, Awareness of policies, standards, etc.
  - Cross-training and exposure to other areas
- Training in the extended VPM Team
  - Understand expectations, interfaces, roles and responsibilities, and communications protocols
- Training across the organization
  - End user expectations, awareness, support

Basic Components

People

- Formal organization structure
- Adequately staffed with trained and experienced individuals
- Interfaces to other organizations defined.

Process

- Process workflow designed and tested
- Standards, Policies, Procedures documented and available

Technology

- Vulnerability Management Workflow
- Interfaces between inventory and vulnerability tools
- Vulnerability Management Tools

Governance

- A linkage mechanism that supports alignment between the VPM and business and IT strategy and direction.
- Defines the outcomes of the programs
  - Builds a path to those outcomes
- Ensure appropriate visibility and awareness of the program
  - Metrics, communications, awareness tools
- Continually inspects and improves upon the program
- Includes the program structure and charter

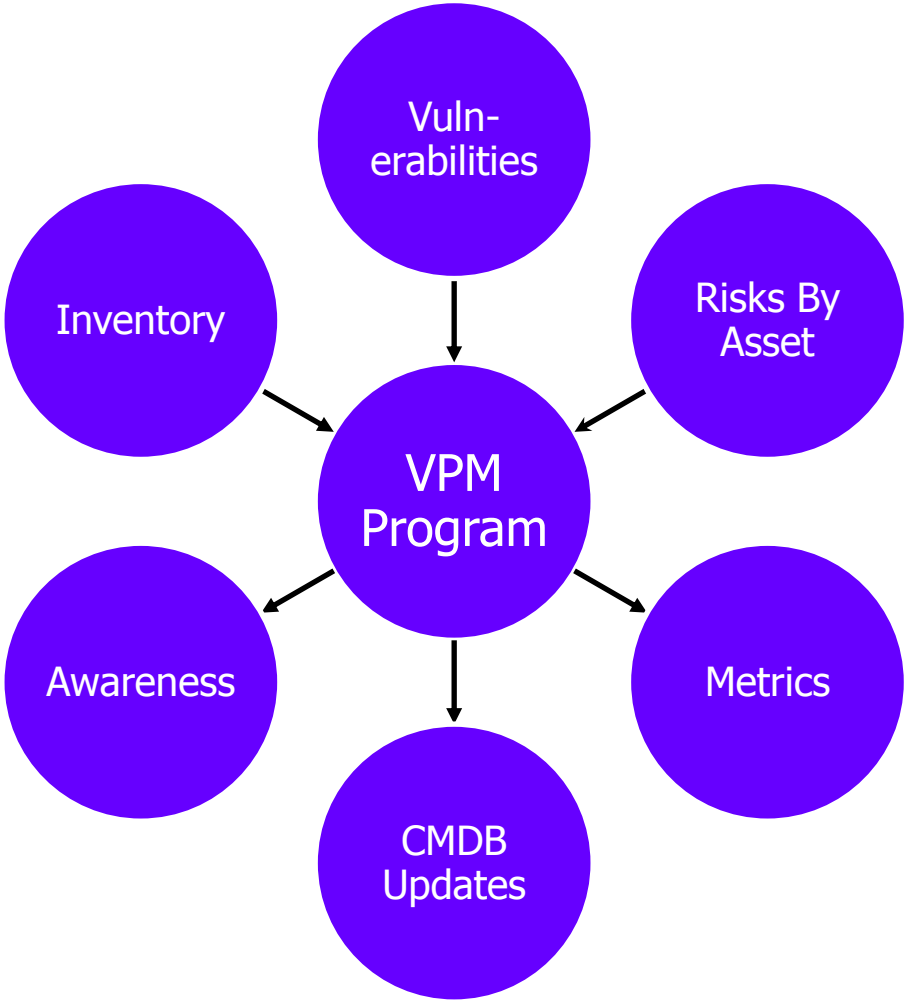
Monitoring and Auditing

- Auditing against the plan
  - Are you doing what you said that you would do?
- Comparing to Industry Leading Practices
  - Are you doing good things like your competitors?
- Optimizing The Program
  - Do you know the program weak areas?
  - Are you getting better?
- Sending the right message?
  - Are your metrics capturing the right information?

Outsourcing VS In-House

- Is this your core competency? Something critical to your operations? Do you need to control this process?
- How much do you want to outsource?
- Service Providers Specialize In This Area
  - Cost benefits – Economies of Scale
  - Vulnerability and Patch information from other clients can help optimize your program
  - May have limited insight and input when needed
  - Is getting metrics and reports good enough?
- Do you want to make the investment to build this out?

Fundamental Communications



Inventory

- How is this managed?
  - How is this updated?
  - Do updates trigger the Vulnerability Management program?
- Do you have any isolated or segmented networks?
  - How do you discover them?
- Integration with other enterprise inventory systems and tools
- Previous audits and assessments

Change Management

- Build an interface between the inventory and scanning tools.
- Ensure that the Configuration Items (CI)s in the CMDB are changed to reflect the current configuration as the systems are patched.
  - Helps business case and ROI
- Changes to the VMP Program:
  - Change policies, practices, standards, procedures
  - Training programs

Prioritize Inventory

- Baseline the inventory:
  - Does the program scope need to change?
    - Are there things you hadn't thought of?
  - Are known critical assets included?
  - Leverage Business Impact Analysis (BIA)s
  - Business Critical Application Lists
  - Network Diagrams – Extranets, DMZ Systems
  - Business functional groups – Treasury, R&D, etc.

Identify Vulnerabilities

- More tools than you need to automate the vulnerability scanning
- The challenge and big differentiator is in how the tool manages, reports, and exports the information.
- Has to integrate to the enterprise inventory system (or vice-versa).
- Refresh network vulnerability scanning basics before scanning!
  - Notification, hours, awareness, when things fail, small pilot

Calculate Risk

Whether you calculate risk as:

$$R = \frac{\text{Threat X Vulnerability}}{\text{Countermeasures}} \quad \textit{or} \quad \text{Likelihood X Impact}$$

- Calculate risk for each of the assets
  - Qualitative vs. Quantitative
- Prioritizes the deployment
- May be matrix based – not formula bases

Patch Management

- One way to mitigate vulnerabilities
- What Else Is There?
  - Compensating Controls
  - Layered / Defense In Depth
  - Reduction of Attack Surface
  - Monitoring (Intrusion Detection / Database)
  - Decommission systems

Patches

- Patches May Be Deployed To Systems at many levels:
  - Firmware/BIOS,
  - Anti-Virus/Malware/Spyware,
  - Software Applications that are either commercial or proprietary, and
  - Operating Systems.
- Patches can be deployed as a black box or with complete transparency
  - Be prepared for both instances
    - And associated challenges

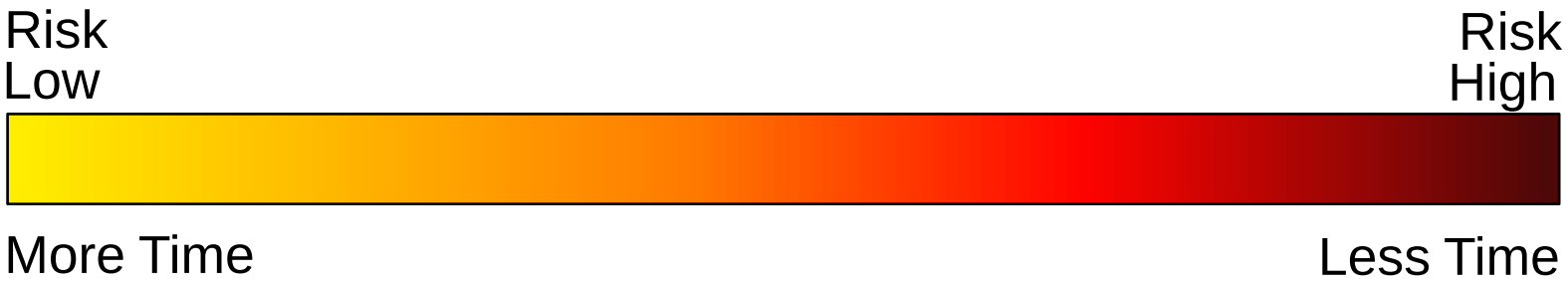
Patch Prioritization

- May be tough when you don't know what the patch does!

Bulletin ID	Vulnerability Title	CVE ID	Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Key Notes
MS12-008	Keyboard Layout Use After Free Vulnerability	CVE-2012-0154	1 - Exploit code likely	1 - Exploit code likely	Not Applicable	(None)
MS12-008	GDI Access Violation Vulnerability	CVE-2011-5046	2 - Exploit code would be difficult to build	2 - Exploit code would be difficult to build	Permanent	This vulnerability has been publicly disclosed.
MS12-009	AfdPoll Elevation of Privilege Vulnerability	CVE-2012-0148	1 - Exploit code likely	3 - Exploit code unlikely	Permanent	x64 is exploitable, x86 is not.
MS12-009	Ancillary Function Driver Elevation of Privilege Vulnerability	CVE-2012-0149	Not Affected	1 - Exploit code likely	Permanent	Only Windows Server 2003 is affected.
MS12-010	HTML Layout Remote Code Execution Vulnerability	CVE-2012-0011	1 - Exploit code likely	1 - Exploit code likely	Temporary	(None)
MS12-010	Null Byte Information Disclosure Vulnerability	CVE-2012-0012	3 - Exploit code unlikely	Not Affected	Not Applicable	This is an information disclosure vulnerability.

Testing Patches

- If you have to compromise a portion of this program, this is where it always happens.
- Should have established time limits.
  - 2 Days for Critical Patches?
  - Race against the clock. Consider off-shore efforts?
- You shouldn't be testing the distribution mechanism during an emergency patch push.



Deploying Patches

- Test on a smaller department or location
- Inputs:
  - Tested Package(s)
  - Timeframes
  - Prioritization
  - Hot Patch vs. Reboot Patches
- Outputs:
  - Statistics / Errors
  - Systems not on-line or reachable – or new systems?

Patch Distribution Tools

- Automated Tools
  - May help package
  - Manage deployment
    - Errors / Re-tries
    - Statistics
- Manual – Not Very Practical – but sometimes required.
- Proprietary – May work well

NETWORKING & SECURITY
GFI LANguard
Network Security Scanner and Patch Management

altiris

bmcsoftware

ORACLE
ENTERPRISE MANAGER
OPS CENTER

Windows Server
Update Services

Patch Roll-Back Procedures

- Develop a plan to roll-back the patch.
  - Before you deploy.
  - Test It. Test Again. Involve the QA Team.
- Roll back the entire deployment or specific systems?
  - How long do you wait before you roll it back?
- Communications is key when rolling the patch back

Patch Validation and Verification

- Did the patch install properly?
  - Do systems need to be rebooted?
- Does the patch do what you expected?
  - Do you know what it was supposed to do?
  - Is the vulnerability mitigated?
    - Vulnerability Scanning
    - Penetration Testing
  - Are there any other issues?

Monitor and Repeat The Process

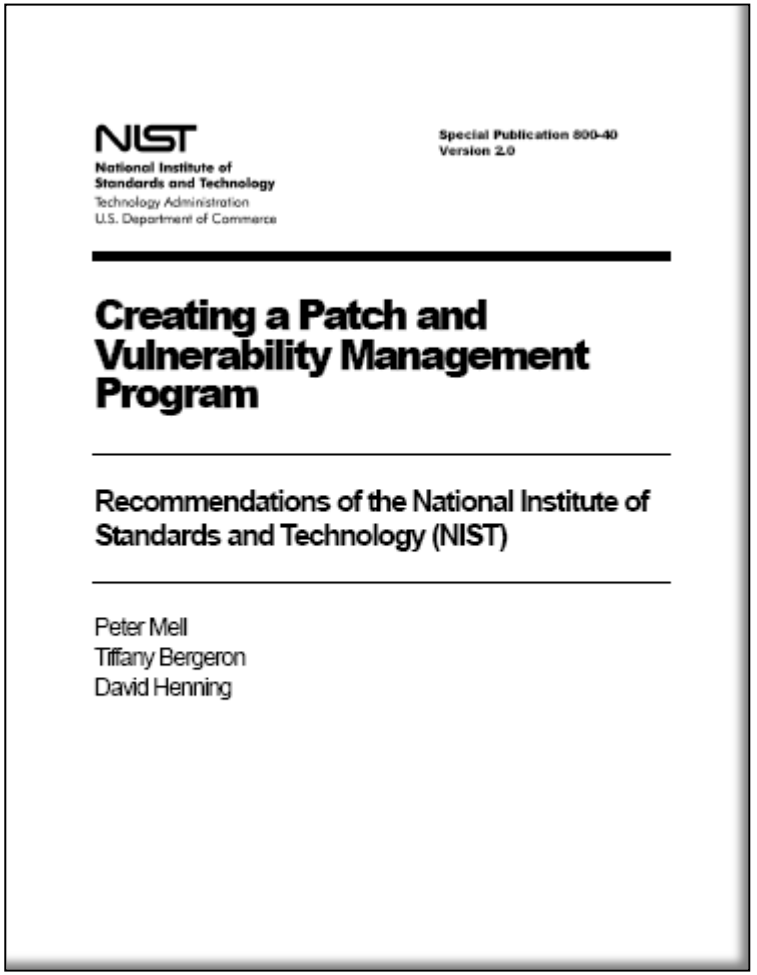
- Don’t rely on the audit group to find issues.
  - Review and act upon the metrics that you have built.
- You’ll have a lot of lessons learned after the first patch deployment
- Celebrate the success; fix the failures.
- Continuously improve effectiveness and efficiency.
- Refine the prioritization and scheduling of patch deployment.

Lessons Learned

- Look at what is already in place. Don't reinvent anything that you don't have to.
- Build a program that is auditable. Especially the policies and roles and responsibilities.
- Have insight into what your vendor does. If you don't know, ask. If you want to, assess and audit.
- Plan ahead with the budget. Anticipate program, scope, and company growth.
- Don't always expect to know that the patches do.
- Don't expect everything to be patched. You've got more segmentation / isolation than you though!

Tools and Resources - NIST, SANS, Vendor Presentations

- SANS Reading Room
- NIST-800-40 v2
- A number of vendors in the GRC and Vulnerability and Patch Management space
- Forrester Research and Gartner have some great articles as well
- Your company policies



NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Special Publication 800-40
Version 2.0

Creating a Patch and Vulnerability Management Program

Recommendations of the National Institute of Standards and Technology (NIST)

Peter Mell
Tiffany Bergeron
David Henning

Summary

- This is an enterprise wide effort.
- Leverage your audit team whose findings can be inventory inputs or business case drivers
- Build it so that it operates as a business function that enables the business –
  - Not as security function that restricts growth or operations.
- You have to have a charter and a program to be effective.
- Start small. Grow the function organically.

Questions / Comments / Thoughts

- What's left?
- What's next?
- Questions? Comments? Thoughts?

Johnson & Johnson

INFORMATION TECHNOLOGY

George G. McBride

Director, IT Security Risk Management

Johnson & Johnson

1003 US Route 202, Raritan, NJ 08869 USA

T: +1.908.655.3915 M: +1.732.312.8354

gmcbri32@its.jnj.com www.jnj.com