

# Data Platform Security

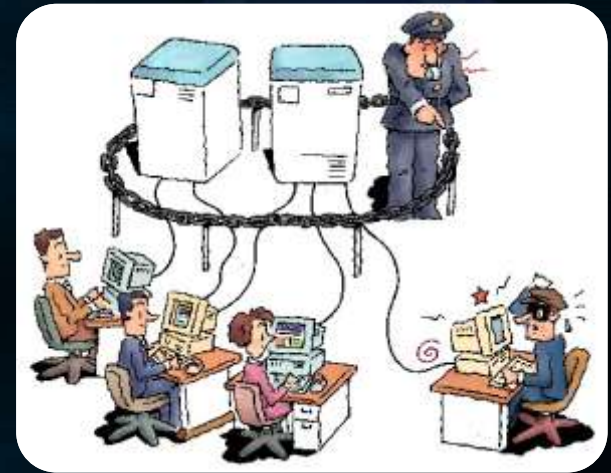


Vinod Kumar

Technology Evangelist

[www.ExtremeExperts.com](http://www.ExtremeExperts.com)

<http://blogs.sqlxml.org/vinodkumar>



# Agenda

- Problem Statement
- Security for Enterprise Security
- Defaults - Vulnerabilities
- Configurations - Vulnerabilities
- Securing Databases - Practices

# Tip for the Day !!!

HI, THIS IS YOUR SON'S SCHOOL. WE'RE HAVING SOME COMPUTER TROUBLE.



OH, DEAR - DID HE BREAK SOMETHING?  
IN A WAY - )



DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;-- ?



OH. YES. LITTLE BOBBY TABLES, WE CALL HIM.

WELL, WE'VE LOST THIS YEAR'S STUDENT RECORDS. I HOPE YOU'RE HAPPY.



AND I HOPE YOU'VE LEARNED TO SANITIZE YOUR DATABASE INPUTS.

# OWASP Top 10 Web Security Vulnerabilities

1. Unvalidated input
2. Broken access control
3. Broken account/session management
4. Cross-site scripting (XSS) flaws
5. Buffer overflows
6. (SQL) Injection flaws
7. Improper error handling
8. Insecure storage
9. Denial-of-service
10. Insecure configuration management

# Growing Problem: S/W Security

- *Survivability*: the capability of a system to fulfill its mission, in a timely manner, in the presence of attacks, failures and accidents. — Lipson, Howard and Fisher, 1999
- Survivability challenge
  - Previous focus primarily on S/W failure, human error and natural disaster
  - Primary security measure was physical
    - Keep external bad guys away
    - Protection against insiders primarily via legal protection and data isolation
- Industry shifts
  - Shift from mediated access to direct application access
    - Vendors, customers and partners
  - Shift from central administration to distributed administration
  - Shift from survivability focus largely ignoring security to security as the prime concern

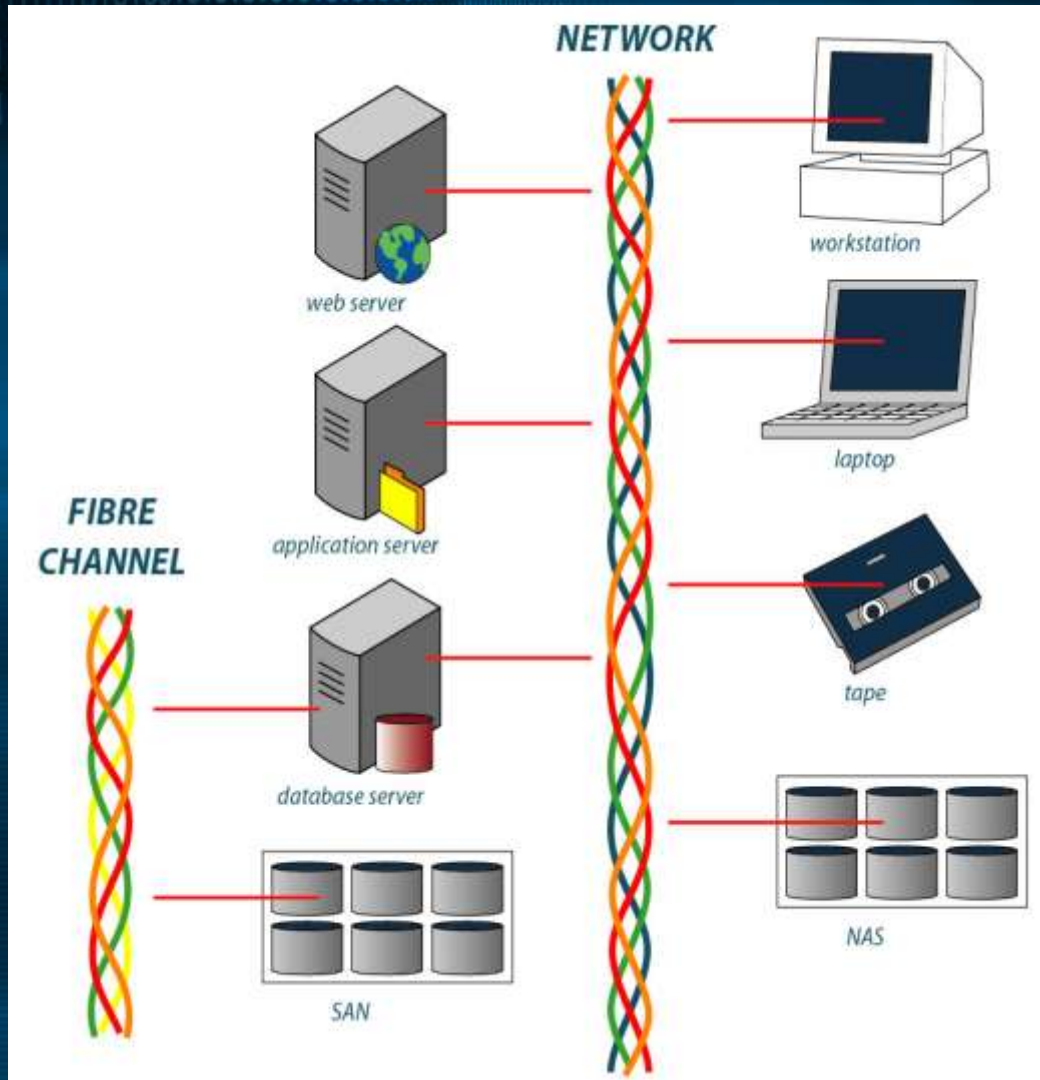
# Evolving Database Threat Environment

- A decade ago
  - Databases were physically secure
  - They were housed in central data centers — not distributed
  - External access was mediated through customer service representatives, purchasing managers, etc.
  - Security issues were rarely reported
- Now increasingly databases are externally accessible
  - Suppliers are directly connected
  - Customers are directly connected
  - Customers and partners are directly sharing data
- Data is most valuable resource in application stack
  - Value increases with greater integration and aggregation
  - Opportunities exist for data theft, modification or destruction
- Database security is a growing problem

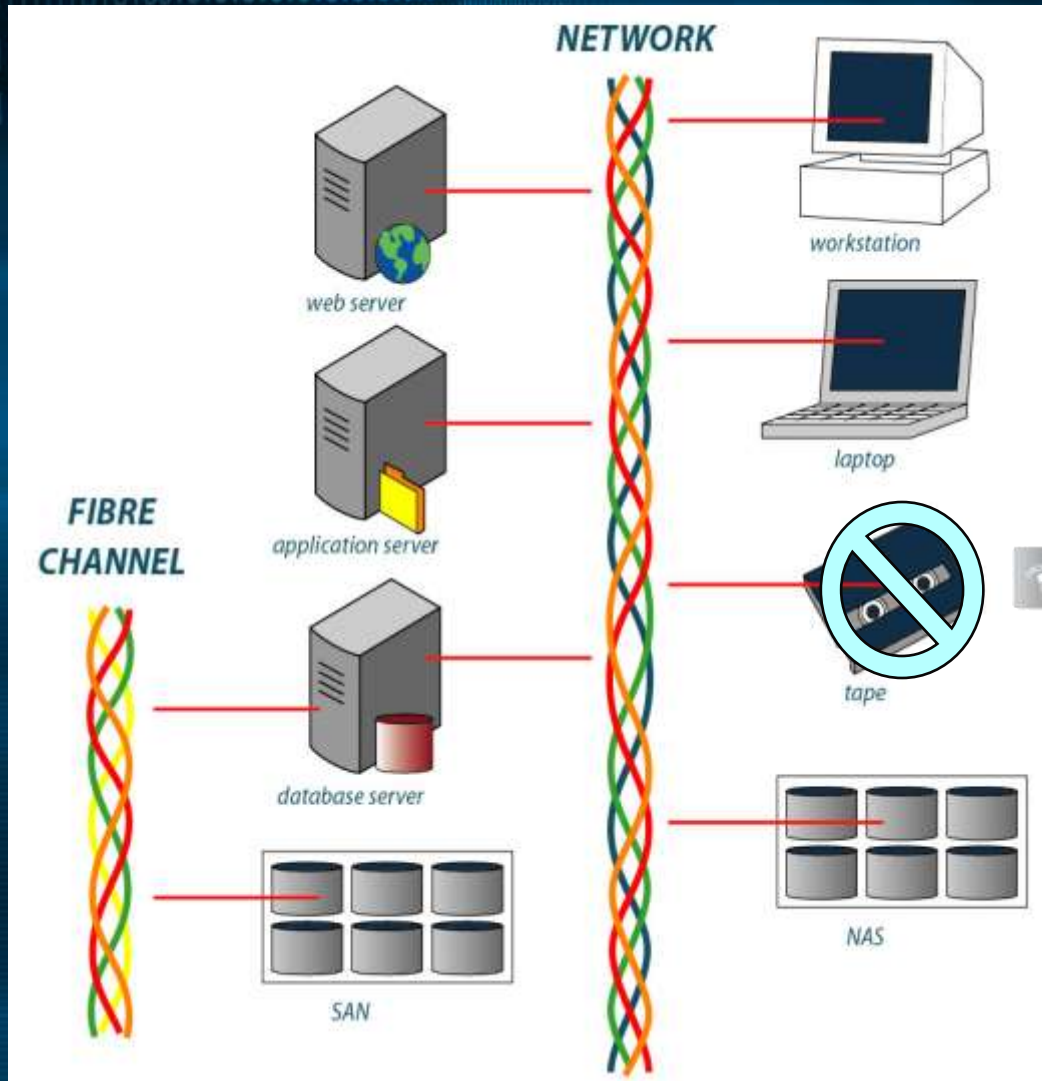
# Database Security: Shifting Ground

- Most applications of value have persistent data
- Data valuable to company, organization or even individual typically also has value to others
  - Information is becoming the most valuable asset in many industries; e.g., Charles Schwab and Wal-Mart both identify management of information assets as key competitive advantage
- Even ephemeral data has significant value, when trends analyzed and understood
  - Decreased storage and data management costs enable ephemeral data
  - Competitive pressure demands ephemeral data
- Where there is value, there are bad guys
  - And professional services guys, and press guys, and industry analysts ...

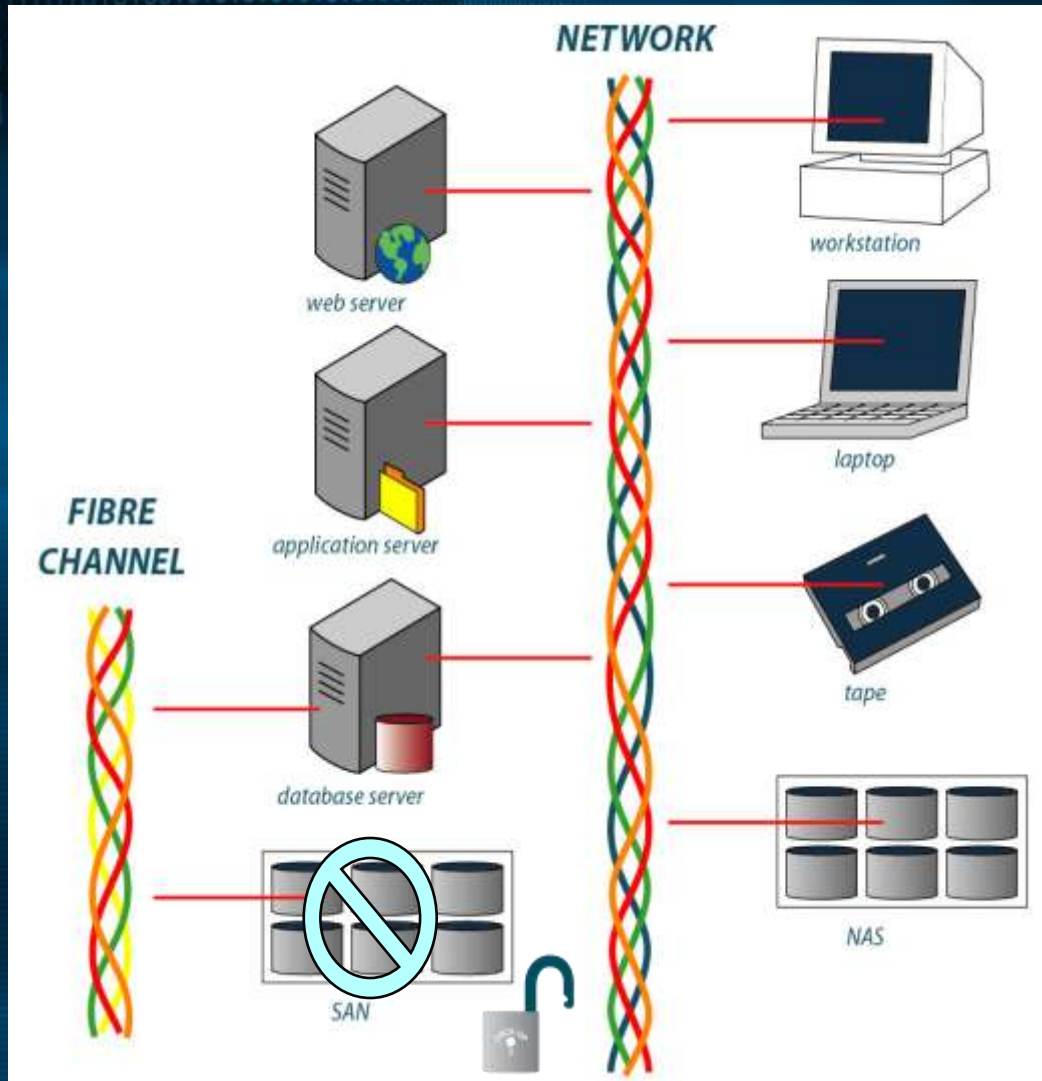
# Examples of bad things...



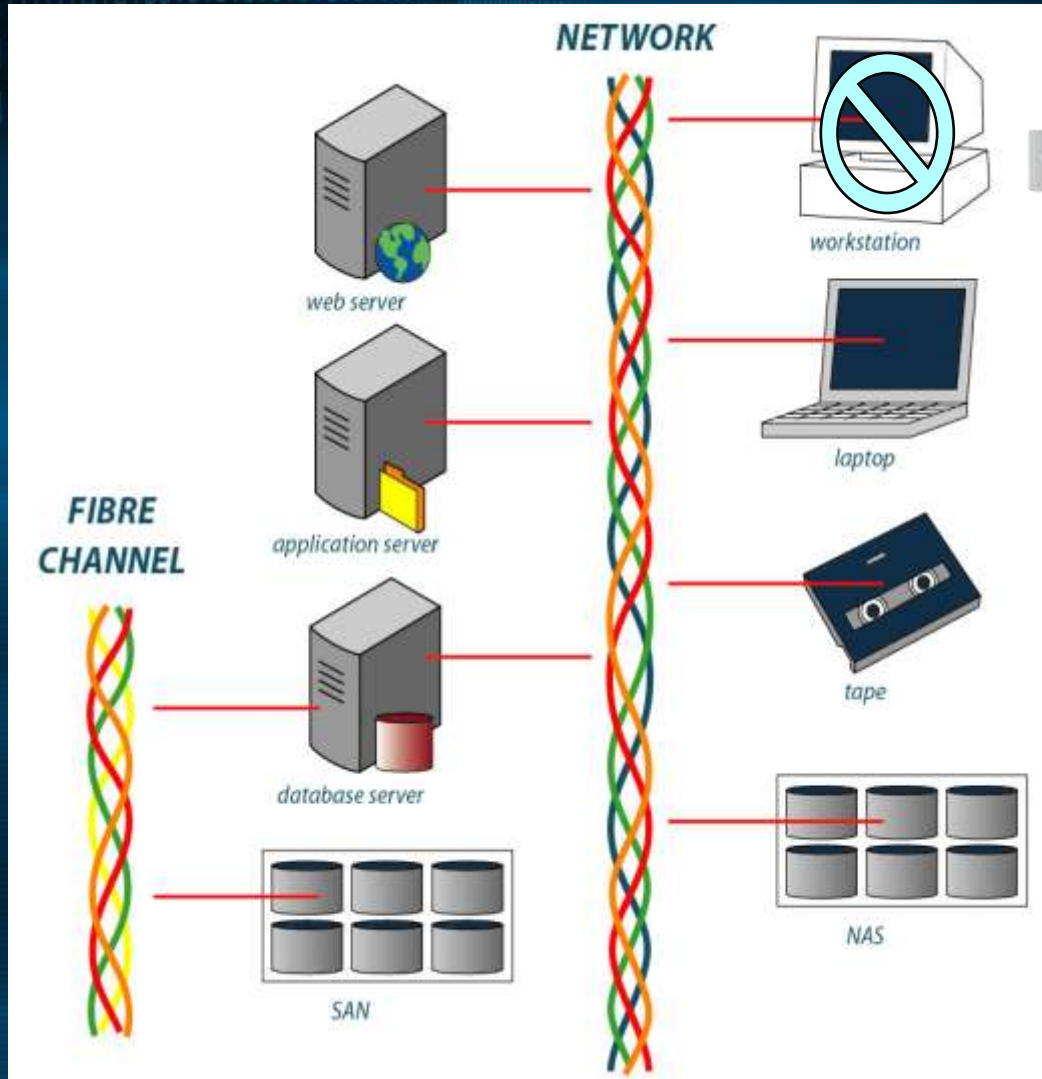
# Loss of backup



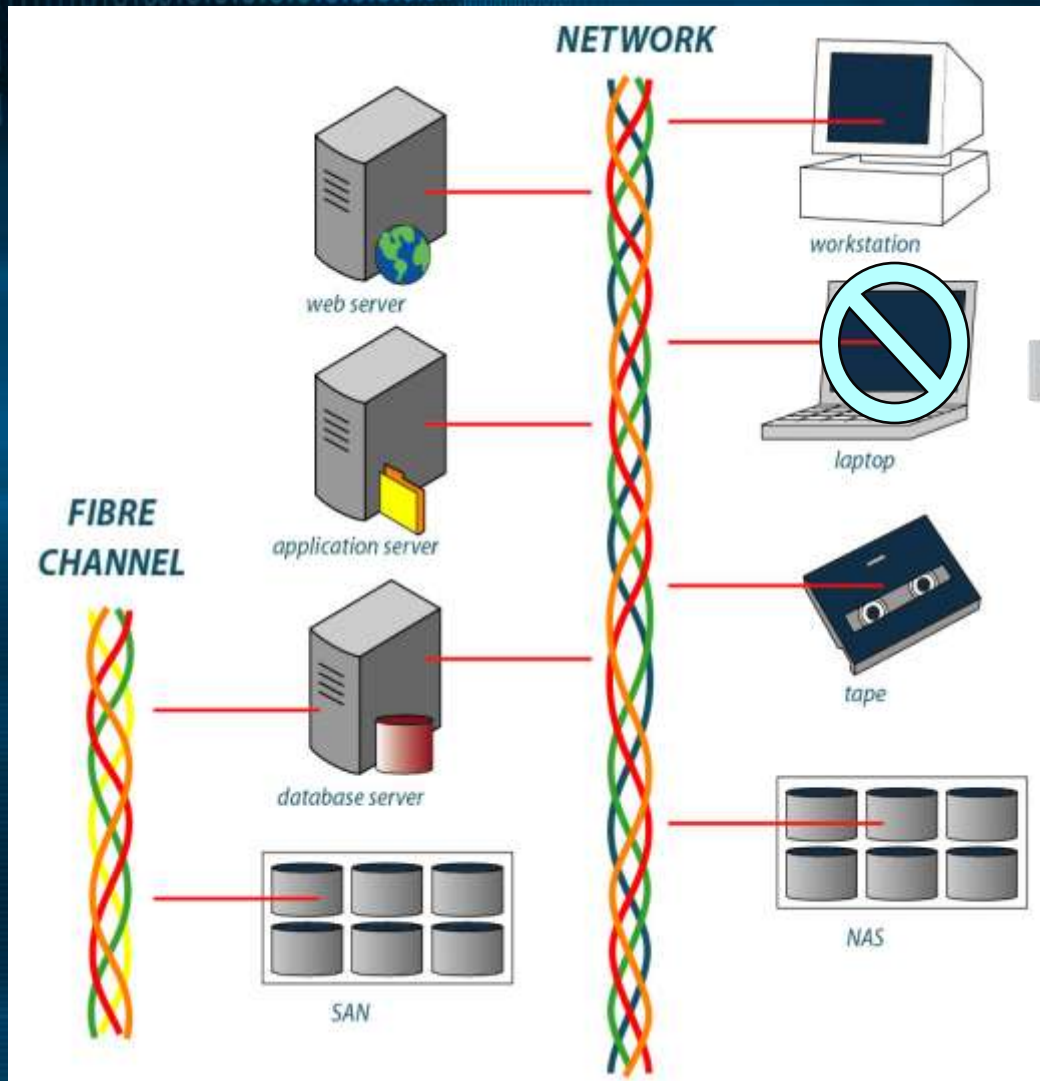
# SAN drive swapped out



# Pod slurping



# Examples of bad things...



# Some more Incidents as examples

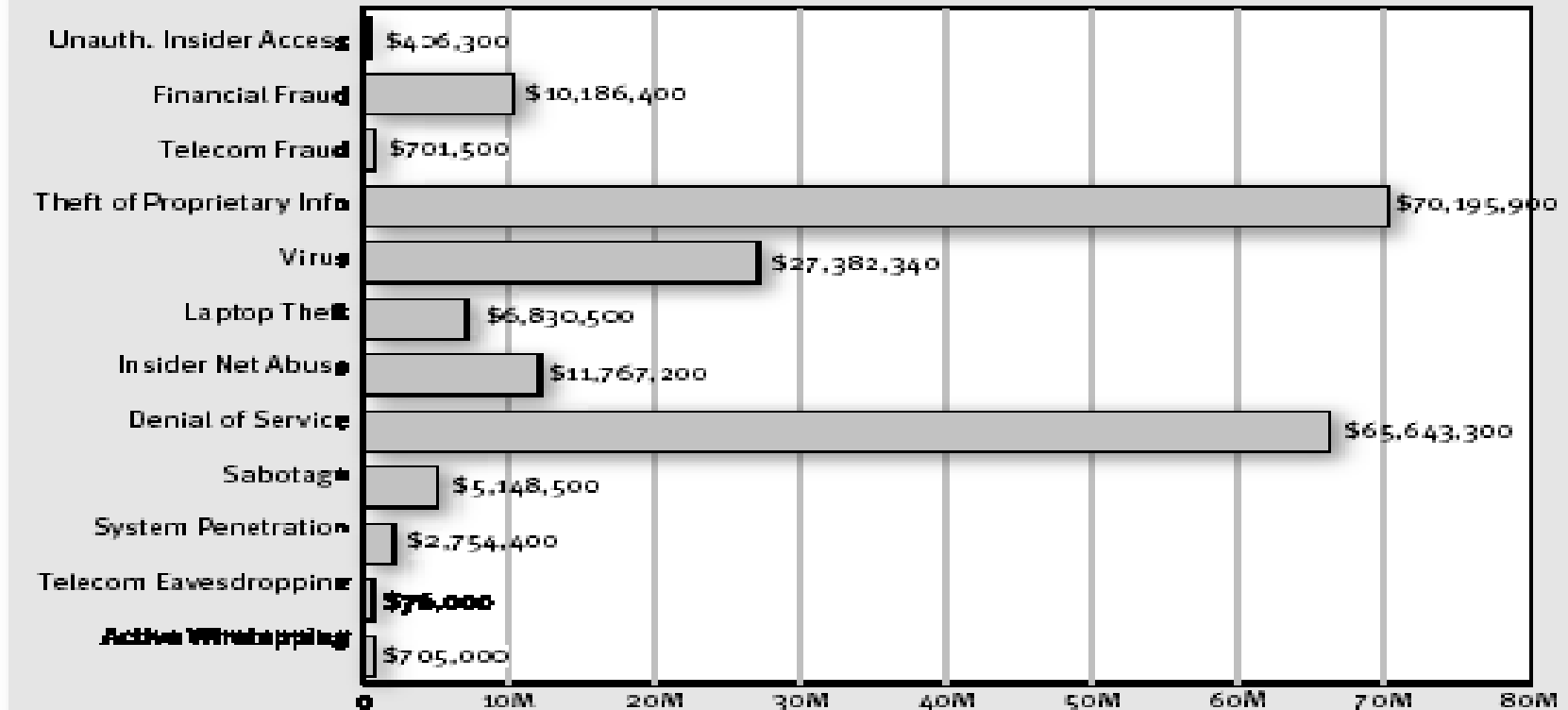
Company/Organization	# of Affected Customers	Date of Initial Disclosure
<u>Department of Energy's nuclear weapons</u>	1500	22-May-06
<u>Georgetown University</u>	41,000	5-Mar-06
<u>Misc retail debit card compromise (OfficeMax?)</u>	200,000	9-Feb-06
<u>Dept of Agriculture</u>	350,000	15-Feb-06
<u>Card Systems</u>	40,000,000	17-Jun-05
<u>Citigroup</u>	3,900,000	6-Jun-05
<u>DSW Shoe Warehouse</u>	1,400,000	8-Mar-05
<u>Bank of America</u>	1,200,000	25-Feb-05
<u>LexisNexis</u>	310,000	9-Mar-05
<u>Ameritrade</u>	200,000	19-Apr-05
<u>ChoicePoint</u>	145,000	15-Feb-05
<u>Etc, etc, etc.</u>		
<b># of customers affected</b>		<b>~50,000,000+</b>
Source: Privacy Rights Clearinghouse, <a href="http://www.privacyrights.org/ar/ChronDataBreaches.htm">http://www.privacyrights.org/ar/ChronDataBreaches.htm</a>		

# Top 5 Issues in Enterprise Security

- Attackers have gone pro
  - Want personal data they can sell – Personal data like credit card and social security numbers are relatively easy to monetize
- Attacks are moving to the source
  - Why pull a single credit card via compromising the network? It's relatively hard with a meager pay off. Instead, take over the corporate database and get them ALL
- The perimeter provides little defense
  - Insiders don't go through the firewall thus perimeters provide no protection from this growing source of risk
- Everyone is watching
  - Everyone is very-much clued in to the increased threats against personal data. Any mistakes are likely to be very public

# CSI/FBI Computer Security Survey

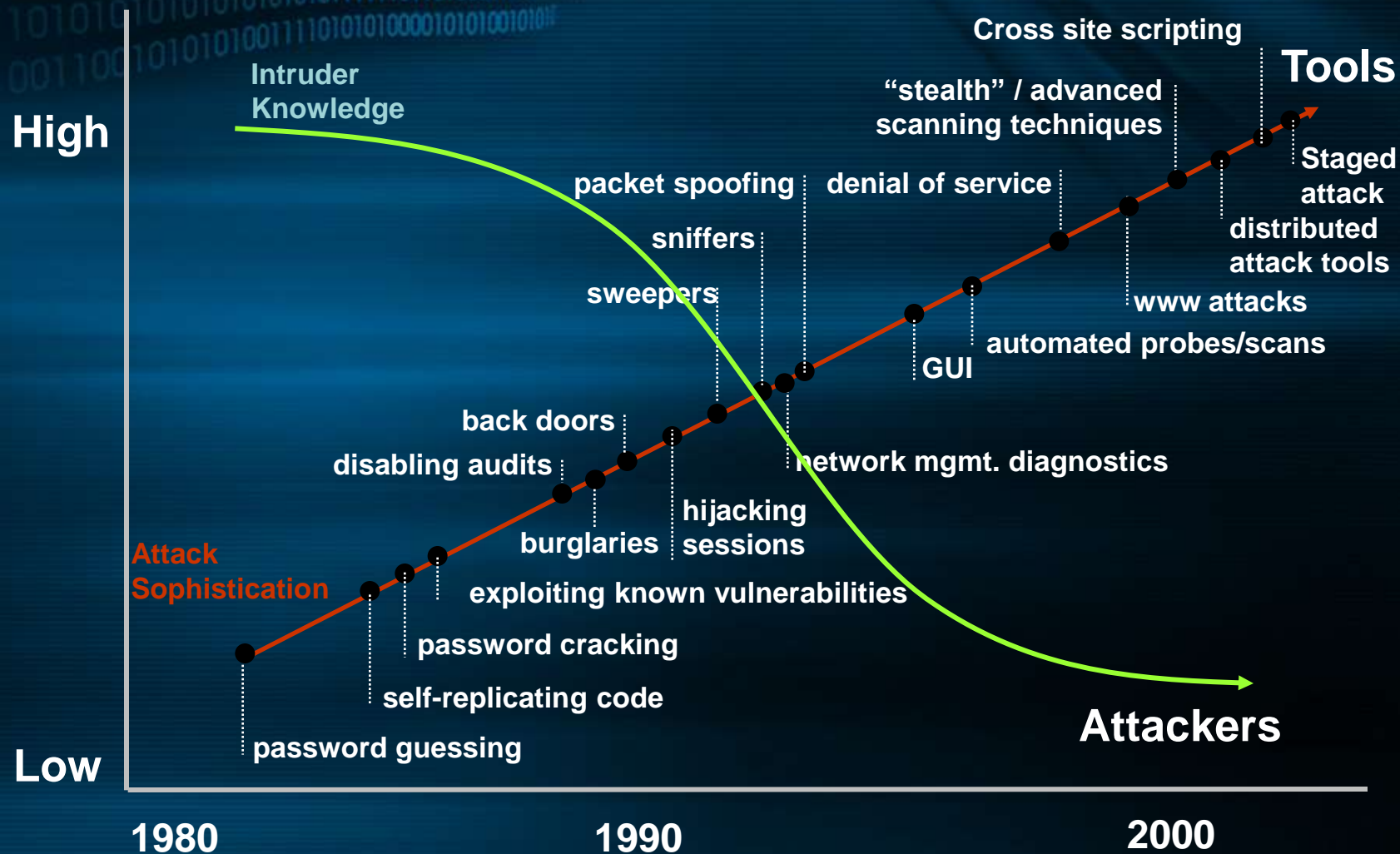
## Dollar Amount of Losses by Type



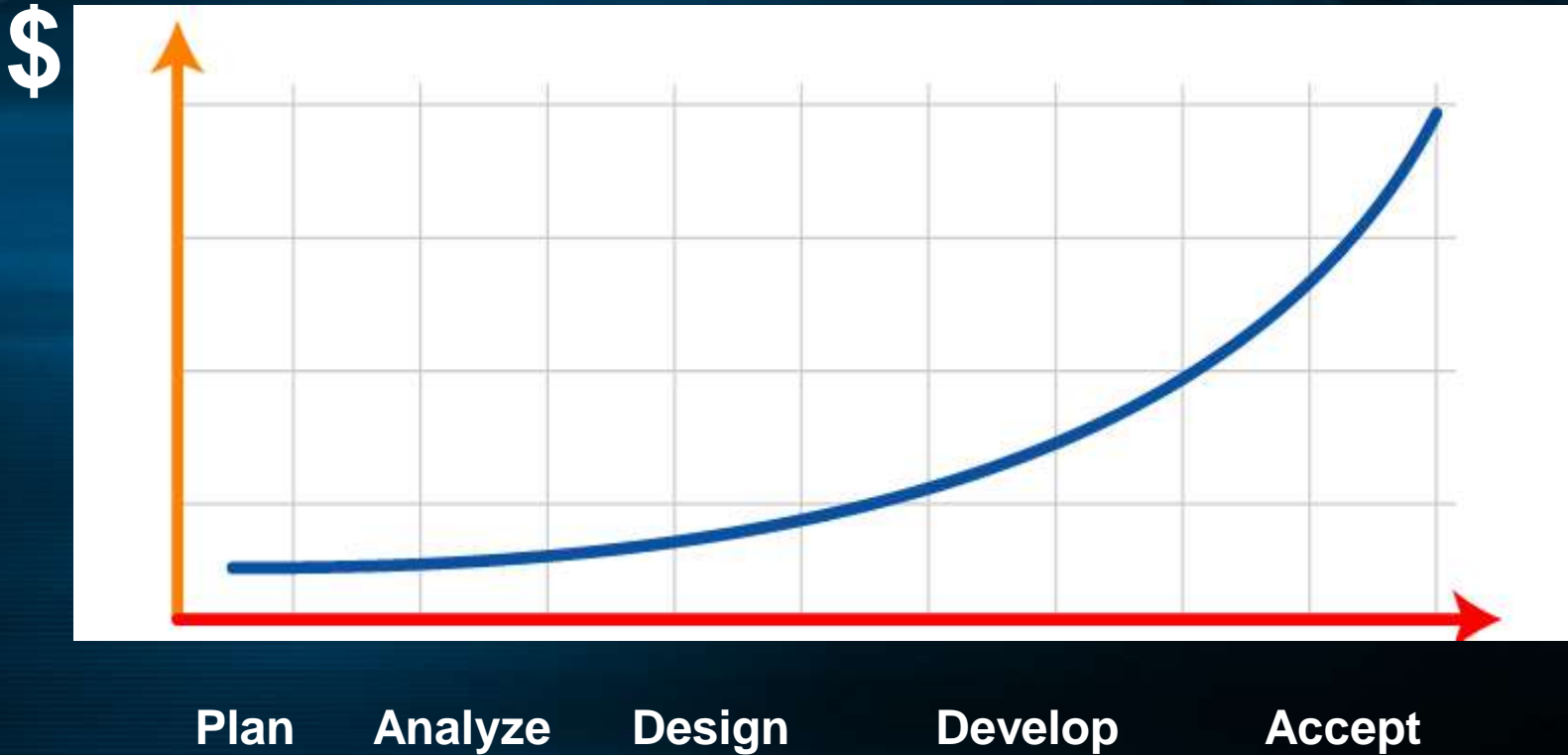
CSI/FBI 2003 Computer Crime and Security Survey  
Source: Computer Security Institute

2003: 251 Respondents / 47%

# Attack Sophistication vs. Intruder Technical Knowledge

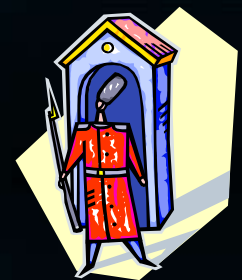


# How Expensive to repair



# Outsider vs. Insider Attack

- Most security schemes address outsider attack
- Have password to database? Can update anything
  - Bypassing all application level security measures
    - More people with access → more danger
- Application program has database password
- Great deal of trust in people who manage databases
  - Risk of compromise greater with value of data
  - Happened with auto-rickshaw registration in New Delhi





# How would you react?

## Email from your IT department

- Time for the annual password change
- Please reply with your new password
- Must be exactly 8 characters
- Must not contain special characters (e.g. \$ @)

Please let us know if you have  
any questions or concerns,

Regards,

Network Security & Operations

# Attitude towards the Users



# World of Default Passwords !!!

# Database Vulnerabilities

## Default Passwords

- Oracle Defaults (Over 200 of them)
  - User Account: internal / Password: oracle
  - User Account: system / Password: manager
  - User Account: sys / Password: change\_on\_install
  - User Account: db snmp / Password: db snmp
- IBM DB2 Defaults
  - User Account: db2admin / Password: db2admin
  - User Account: db2as / Password: ibmdb2
  - User Account: dlfm / Password: ibmdb2

# Database Vulnerabilities

## Default Passwords

- MySQL Defaults
  - User Account: root / Password: null
  - User Account: admin / Password: admin
  - User Account: myusername / Password: mypassword
- Sybase Defaults
  - User Account: SA / Password: null
- Microsoft SQL Server Defaults (Till SQL 2000)
  - User Account: SA / Password: null

# Misconfigurations & Resource Privileges

## Misconfigurations Can Make a Database Vulnerable

### Oracle

- External Procedure Service
- Default HTTP Applications
- Privilege to Execute UTL\_FILE

### Microsoft SQL Server

- Standard SQL Server Authentication Allowed
- Permissions granted on xp\_cmdshell and xp\_regread

### Sybase

- Permission granted on xp\_cmdshell

### IBM DB2

- CREATE\_NOT\_FENCED privilege granted
  - This privilege allows logins to create stored procedures

### MySQL

- Permissions on User Table (mysql.user)

# How are search engines used for attacks?

- First thing an attacker needs is information
  - Where to attack
  - What a site is vulnerable to
- Search engine is a large repository of information
  - Every web page in your application
  - Every domain on the Internet
- Search engines provide an attacker:
  - Ability to search for attack points on the Internet
  - Ability to search for an attack point in a specific website
  - Ability to look for specific URLs or files

# Securing Databases - Practices

# Secure Installation

- Physical security
  - Protect all related systems, media, backups, etc
- Never place database unprotected on public net
  - Or on unprotected private net
  - Firewall protected
  - S/W mediating database access
- Install on NTFS file system
  - This allows securing the files appropriately
- Do not install on a domain controller
- Choose weak service account
  - Do not choose LocalSystem, box admin or domain admin
  - Cracked database won't get access to rest of enterprise
- Latest code is most secure code

# Configuration Options

- Authentication mode
  - Use Integrated Security
    - More secure protocols (Kerberos and NTLM)
    - Kerberos allows for delegation
    - Allows for password policy enforcements
    - Typically does not require application to store passwords
  - If using Mixed mode (Standard SQL Authentication)
    - Use SSL to encrypt network traffic
    - Use strong passwords
    - Never use blank passwords
- Login auditing
  - Audit failed login attempts at the very least
- Disallow ad hoc queries
- Choose static ports for named instances

# Secure Operation

- Understand the security model
- Only configure and run needed features
- Smallest possible administrator groups
  - Don't put all enterprise/box administrators in one group
- Changing service accounts
  - Use Enterprise Manager
  - [KB article Q283811](#)
- Disallow direct catalog updates
- Know encryption nuances and options !!!

# Application Best Practices

- Use weak access accounts
  - Only capable of actions needed to run application
  - Use different account for administration
- Use Windows auth rather than SQL Auth
  - Easier to secure
  - No password storage required
  - If using SQL auth, use SSL
- Turn on encryption for sensitive data
- Use roles for permissions and ownership
  - Ease of management
  - Objects owned by roles, need not be dropped/renamed when user dropped
  - Do not grant permissions to public
- Don't show “developer quality” error messages to users
  - Can reveal information to attackers in multiphase attacks

# SQL Injection

- Why SQL injection works?
  - Connection made in context of higher-privileged account
  - Application accepts arbitrary user input
- Mitigating SQL injection
  - Validate all user input
    - Define set of valid input, accept only that
    - Reject all invalid input
  - Avoid using dynamic SQL in stored procs
  - Run applications in minimally privileged contexts
    - Never run as sysadmin

# Summary

- Look to secure both Physically and Logically the applications data
- Know all the paths the databases would be accessed
- Turn Off by Default – This must be true for your application too
- Reduce remote access to database
- Be on the latest patch and control direct access into database

# Resources

- [Security Awareness Toolkit](#)
- [Security Considerations for SQL Server](#)
- [Securing Data in Hosted Applications](#)
- [Building Secure ASP.NET Applications: Data Access Security](#)
- [Operating System Vulnerability Scorecard](#)
- [SQL Server 2005 Security Best Practices - Operational and Administrative Tasks](#)
- [SQL Server 2005 Deployment Guidance for Web Hosting Environments](#)
- [CIS security lockdown guide for SQL Server 2005](#)

Questions?

[www.ExtremeExperts.com](http://www.ExtremeExperts.com)

<http://blogs.sqlxml.org/vinodkumar>



**Microsoft<sup>®</sup>**

*Your potential. Our passion.<sup>™</sup>*

101000100100101001010100110011  
10101010010101010101010101010101  
1010101010101111011010000101011  
10100010010010010101010100110011  
10101010010101010101010101010101  
1010101010101111011010000101011