IBM Security
Intelligence. Integration. Expertise.

IBM

IBM Application Security Solution

Manage your application security risk

Charles Tostain
Application Security Sales Leader for Europe

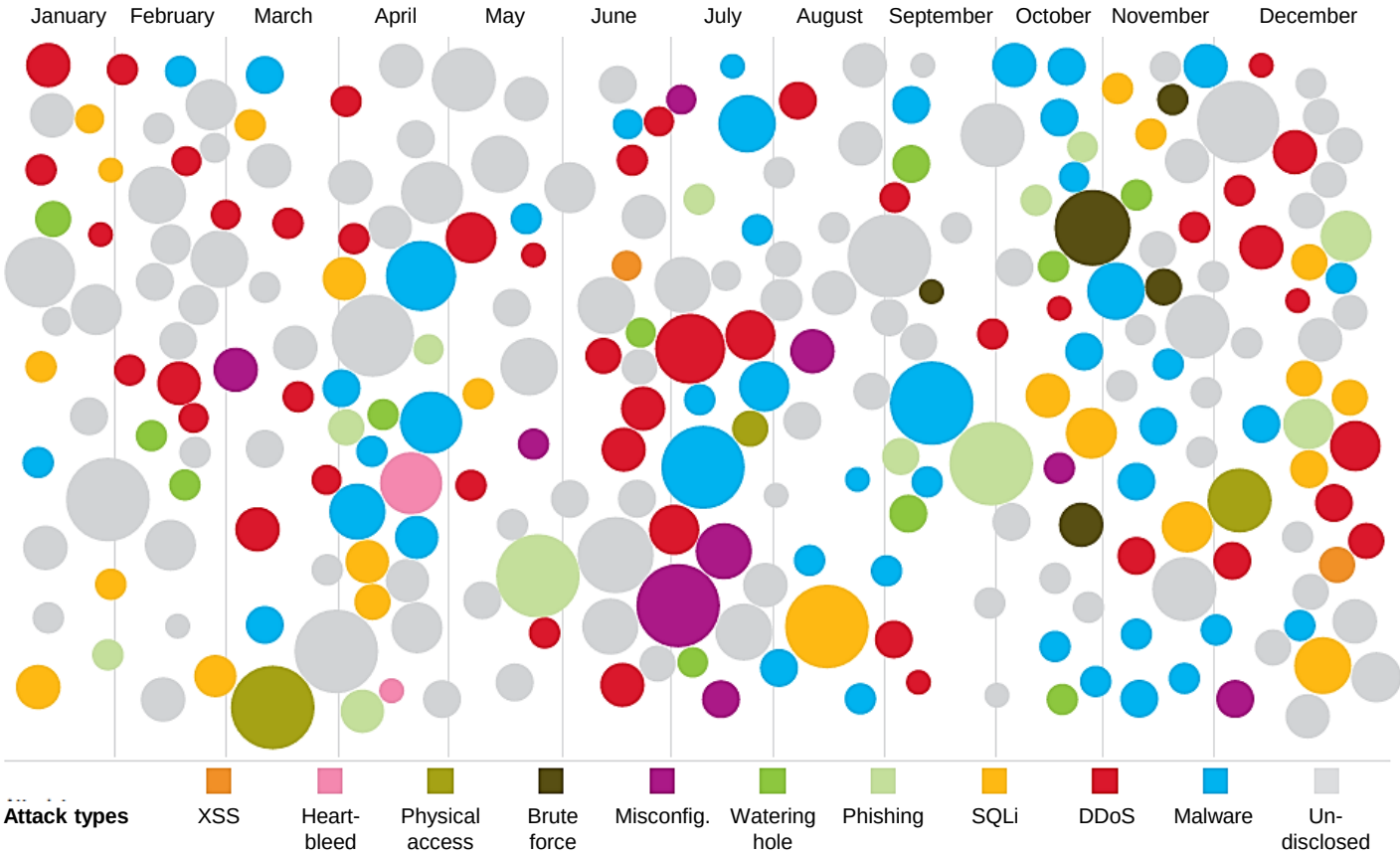
Victor Grane
Application Security Technical Specialist

IBM Security

May 12, 2016

SQL injection: Still reliable for breaching applications

Sampling of security incidents by attack type, time and impact

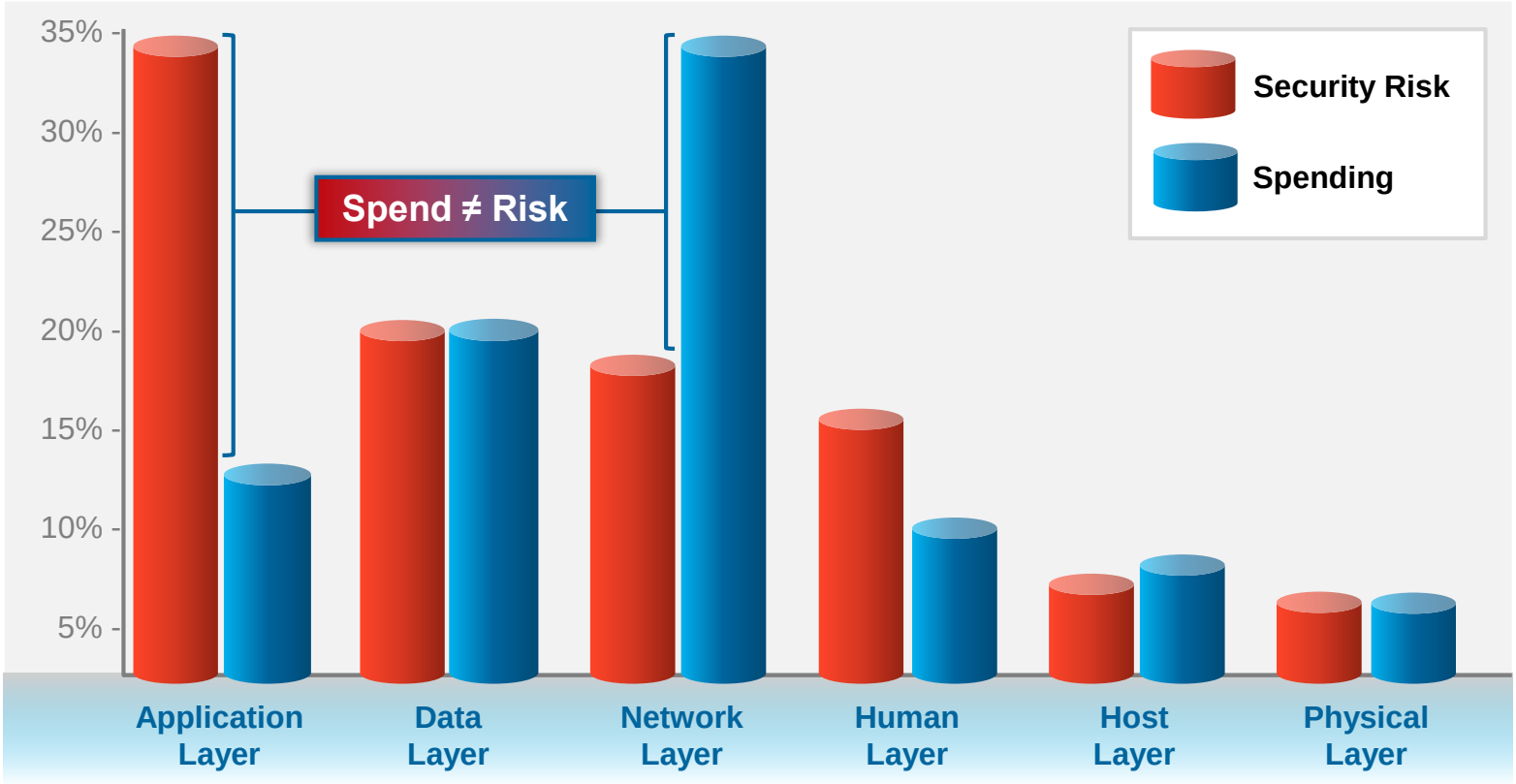


SQL injection accounted for 8.1% of attacks

Source: IBM X-Force Threat Intelligence Quarterly 1Q 2015

Application security spending

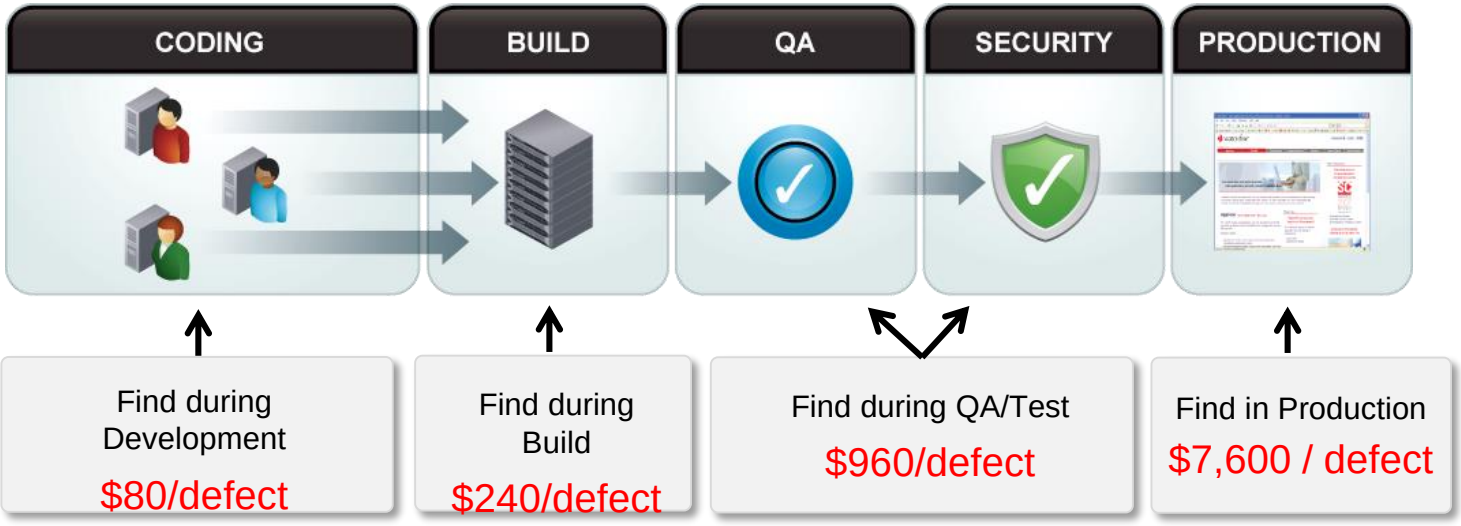
Where are your "security risks" versus your "spend"?



Many clients do not prioritize application security in their environments

Source: The State of Risk-Based Security Management, Research Study by Ponemon Institute, 2013

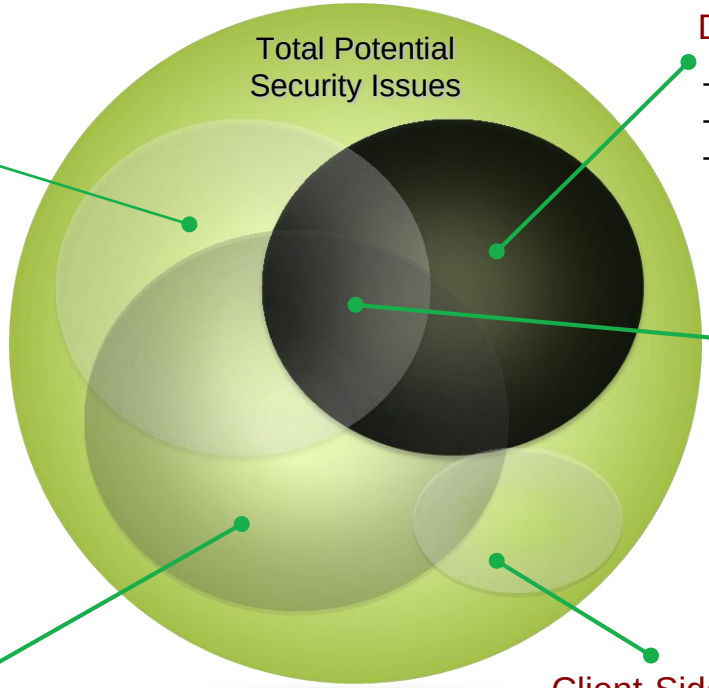
The Old Story – Still Valid But There's More….



* Source: National Institute of Standards and Technology

** Source: Ponemon Institute 2009-10

IBM AppScan uses various techniques to find vulnerabilities



Static Analysis

- Analyze Source Code
- Use during development
- Uses Taint Analysis / Pattern Matching

Dynamic Analysis

- Analyze Live Web Application
- Use during testing
- Uses HTTP tampering

Hybrid Analysis

- Correlate Dynamic and Static results
- Assists remediation by identification of line of code

Run-Time Analysis

- Combines Dynamic Analysis with run-time agent
- More results, better accuracy

Client-Side Analysis

- Analyze downloaded Javascript code which runs in client
- Unique in the industry

Flexible AppScan deployment solutions

Adopt individually or combine to meet your unique needs

SaaS	On-Premise	Managed Service
Testing focus	***Custom program***	***Program management***
• Simple • Self service • Quick results	• Scalable • Customizable • Comprehensive	• Skilled expertise • Guided remediation
IBM Application Security on Cloud	**IBM Security AppScan**	**IBM / Sogeti**

But analysis is not enough…

But analysis is not enough: It's all about managing risk…

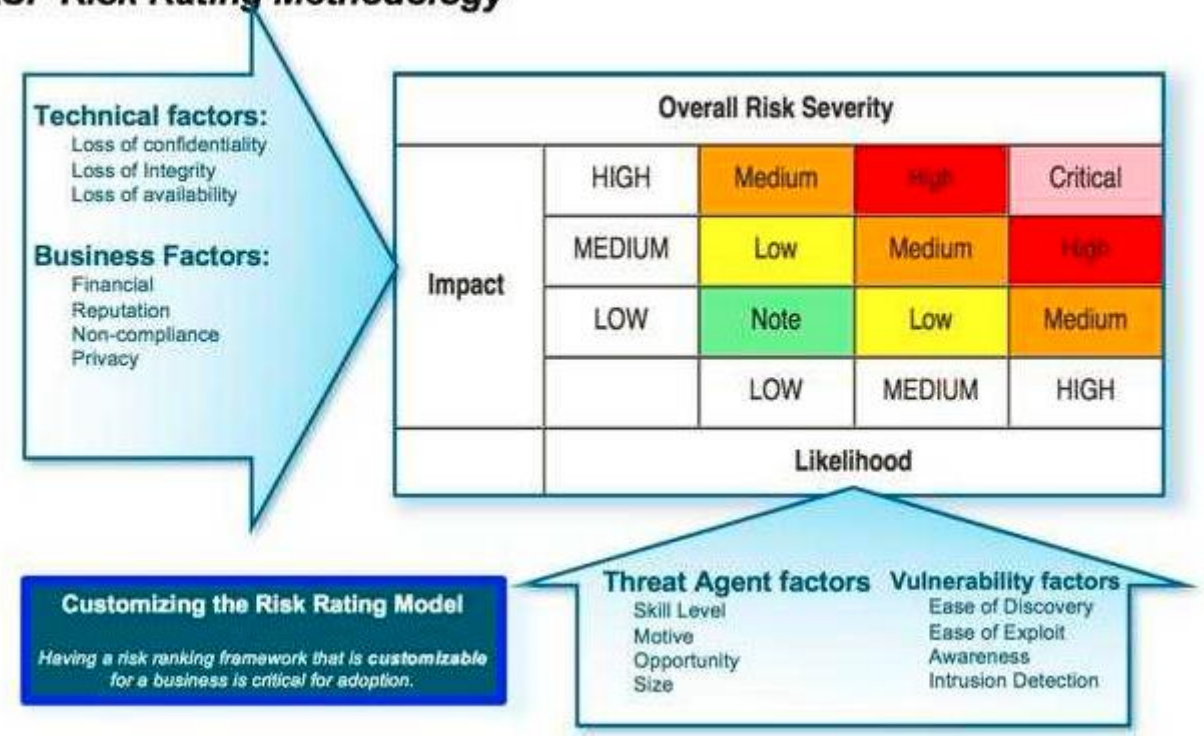
"Security has and will always be about understanding, managing, and mitigating the risk to an organization's most critical assets."

Advanced Persistent Threat, Understanding the Danger and How to Protect Your Organization, by Dr. Eric Cole, SANS Institute

Internal / External / Sensitive data	**IT Help**	**Online Product Catalog**	**Employee Travel Site**	**Online Store**
Business Impact	Low	Medium	High	Critical
Vulnerabilities	(2) Medium Session identifier not updated	(2) High SQL injection	(1) Medium Open redirect	(1) High SQL injection
Application Security Risk	**LOW**	**HIGH**	**MEDIUM**	**VERY HIGH**

OWASP

OWASP Risk Rating Methodology



IBM Application Security Framework

Application Security Management

- Asset Inventory
- Business Impact Assessment
- Vulnerability Prioritization
- Status and Progress Measurement
- Compliance Determination

Test

Applications in Development

- Dynamic Analysis
- Static Analysis
- Interactive Analysis
- Mobile Application Analysis

Monitor and Protect

Deployed Applications

- Intrusion Prevention
- SIEM
- Database Activity Monitoring
- Web Application Firewall
- Mobile Application Protection

Utilize resources effectively to identify and mitigate risk

IBM Security

Intelligence. Integration. Expertise.

IBM

Looking at application security in the Cloud

IBM Application Security on Cloud

Easy as 1, 2, 3!

Simple

Does my application contain security vulnerabilities?

1

Enter URL / upload application

2

Scan the application

3

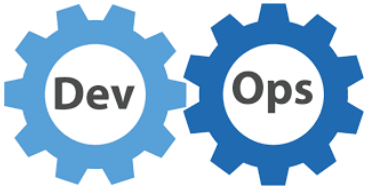
Review the report

Combine leading technology with the benefit of the cloud

EASY
(Simple configuration, Fast Scans, Easy integration)

IFA
(Intelligent Findings Analytics, reduce false positive)

IR
(Intermediate Representation, don't send your code to cloud)



SDLC
(Integration into SWG Dev Lifecycle)

IBM Application Security on Cloud – Analyzing a mobile application - Demo

IBM Application Security on Cloud - Video

IBM Security

Intelligence. Integration. Expertise.

IBM

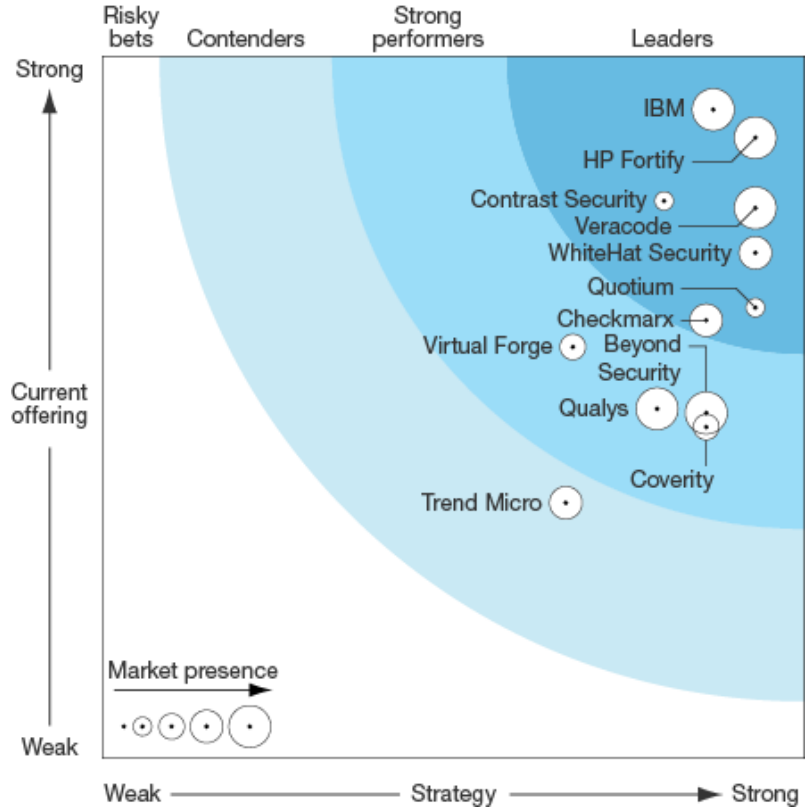
Summary of Application Security at IBM and Sogeti

IBM positioned in “Leaders” category in The Forrester Wave™

FORRESTER®

The Forrester Wave™:
Application Security,
Tyler Shields

“IBM’s focus on the developer integration leads to exceptional results. The IBM product offering provides extensive general features on both on-premises and on-demand application security solutions, depending on customer needs.”



The benefits of IBM and Sogeti application security in three points

- Save IT resources – Optimize the security work of Developers, QA and Security Analysts thus lowering development cost
- Business Operation Efficiency – Reduce the risk of application outages and loss of critical information
- Flexible solutions – Take advantage of solutions delivered as On-premises, Cloud and/or Managed Services

IBM Security

Intelligence. Integration. Expertise.

IBM

Test Data Management and Service Virtualization

Test data Management

Service Virtualization

Test Virtualization Server

Simulate interfaces so you can test when you want.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

THANK YOU

www.ibm.com/security

IBM Security

Intelligence. Integration. Expertise.

Legal notices and disclaimers

U.S. Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM.

Information in these presentations (including information relating to products that have not yet been announced by IBM) has been reviewed for accuracy as of the date of initial publication and could include unintentional technical or typographical errors. IBM shall have no responsibility to update this information. THIS document is distributed "AS IS" without any warranty, either express or implied. In no event shall IBM be liable for any damage arising from the use of this information, including but not limited to, loss of data, business interruption, loss of profit or loss of opportunity.

IBM products and services are warranted according to the terms and conditions of the agreements under which they are provided.

Any statements regarding IBM's future direction, intent or product plans are subject to change or withdrawal without notice. Performance data contained herein was generally obtained in a controlled, isolated environments. Customer examples are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual performance, cost, savings or other results in other operating environments may vary. References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business.

Workshops, sessions and associated materials may have been prepared by independent session speakers, and do not necessarily reflect the views of IBM. All materials and discussions are provided for informational purposes only, and are neither intended to, nor shall constitute legal or other guidance or advice to any individual participant or their specific situation.

It is the customer's responsibility to insure its own compliance with legal requirements and to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products in connection with this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products. IBM does not warrant the quality of any third-party products, or the ability of any such third-party products to interoperate with IBM's products. IBM EXPRESSLY DISCLAIMS ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents, copyrights, trademarks or other intellectual property right.

Other company, product, or service names may be trademarks or service marks of others. A current list of IBM trademarks is available at "Copyright and trademark information" www.ibm.com/legal/copytrade.shtml