END USER PRIVACY BREACHES

Rishi Narang
Vulnerability Research Analyst
Third Brigade Security Labs
rishi.narang (at) thirdbrigade.com
+91 988.6982.678

OWASP
06th September, 2007

The OWASP Foundation
http://www.owasp.org

HAWK'S EYE

- **Web Application Security**
  - 10 Steps to Secure
  - IE vs. Firefox Competition
- **Common User Behaviors**
  - Warnings & Error Messages
  - SURVEY: What End Users Say About Warnings
- **Security Products vs. Attacks**
  - Current Security Architecture
  - Security Myths
- **Ideal World vs. Real World**
  - Security Awareness (Geographically)
  - Plans & Actions + Prime Focus
- **Privacy Approach**
  - Data Gathering
  - Privacy Policies & Drives

WEB APPLICATION SECURITY

… lot many web apps, but are they secured ?? Can they live together ??

WEB 2.0 brings Threat 2.0

STEP 01. Policy: Fair policy @ every Gateway

STEP 02. Tuning the Policy: Tuning as per custom applications

STEP 03. Dealing with Malwares: HOST level protection against Malwares

STEP 04. Block Undesirable URLs: Block Black-Listed and undesirables

STEP 05. File Format Scans: Protection against malicious file downloads

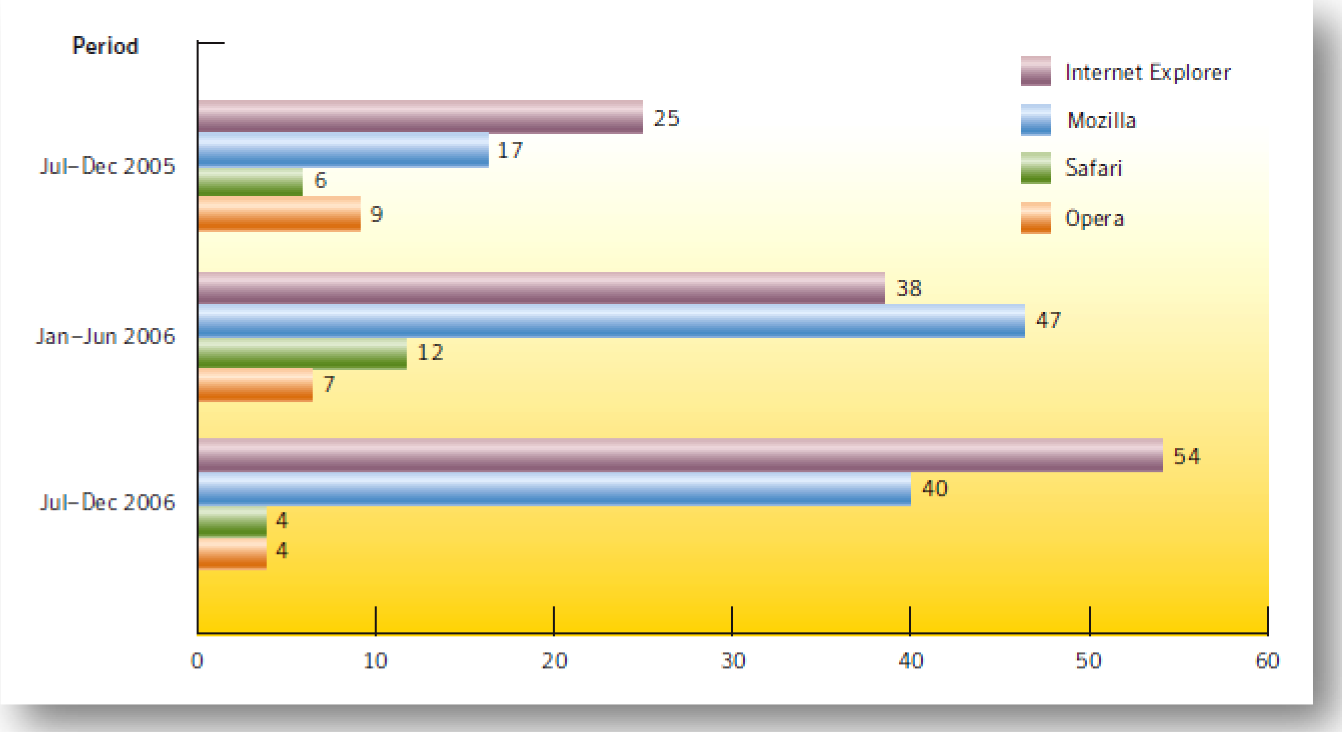
STEP 06. Upload Scans: Upload scan log for malicious activities

STEP 07. IM traffic scans: IM traffic scan for file sharing and scripts

STEP 08. Web Activity Monitoring: Passive monitoring for Anomalies

STEP 09. Policy Enforcements: User Education and simplified process

STEP 10. Emerging Web Activities: Keep an Eye on it !



Source: Internet Security Threat Report Volume XI, Symantec Corporation

IE & FIREFOX reported high number of vulnerabilities as compared to other browsers.

In the 2006 1st Quarter – IE reported: 38 & Firefox reported: 47

In the 2006 2nd Quarter – IE reported: 54 & Firefox reported: 40

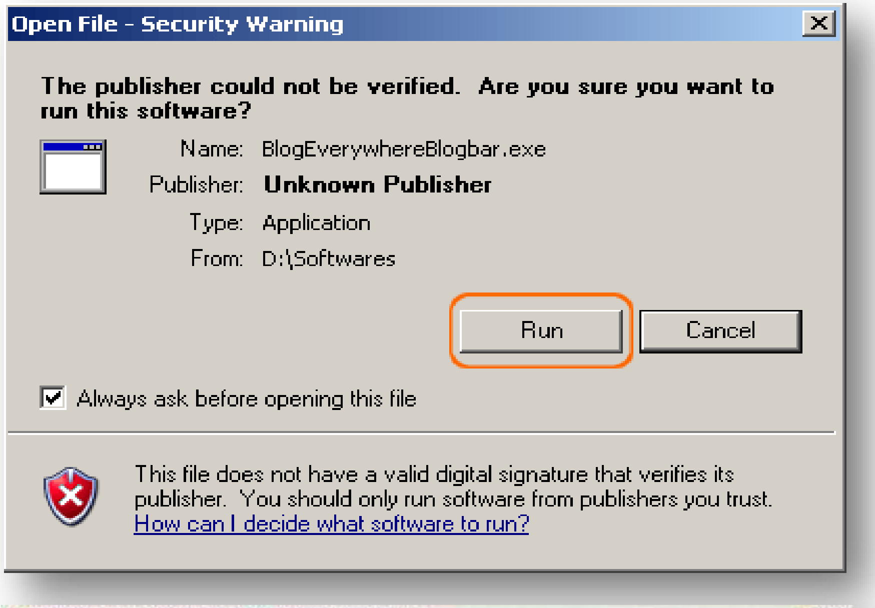
FIREFOXURL EXPLOIT DEMO

Common User Behaviors

1999 Randy Glasbergen. www.glasbergen.com
GLASBERGEN
"It's the latest innovation in office safety. When your computer crashes, an air bag is activated so you won't bang your head in frustration."

…99% of all problems sit between the keyboard and chair!

Common User Errors



The publisher could not be verified. Are you sure you want to run this software?

Name: BlogEverywhereBlogbar.exe

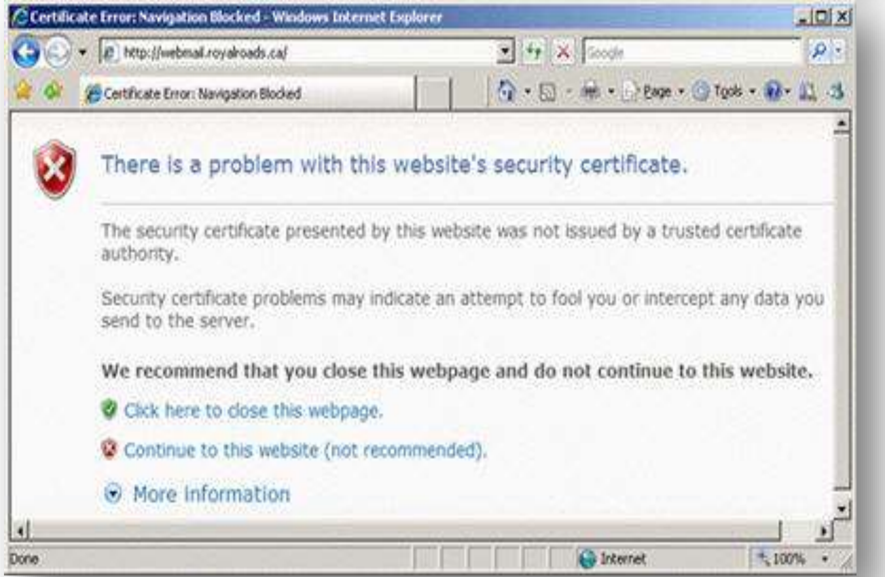
Publisher: **Unknown Publisher**

Type: Application

From: D:\Softwares

☑ Always ask before opening this file

This file does not have a valid digital signature that verifies its publisher. You should only run software from publishers you trust. How can I decide what software to run?



Certificate Error: Navigation Blocked - Windows Internet Explorer
http://webmail.royalroads.ca/
Google
Certificate Error: Navigation Blocked
Page
Tools
Done
Internet
100%

There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.

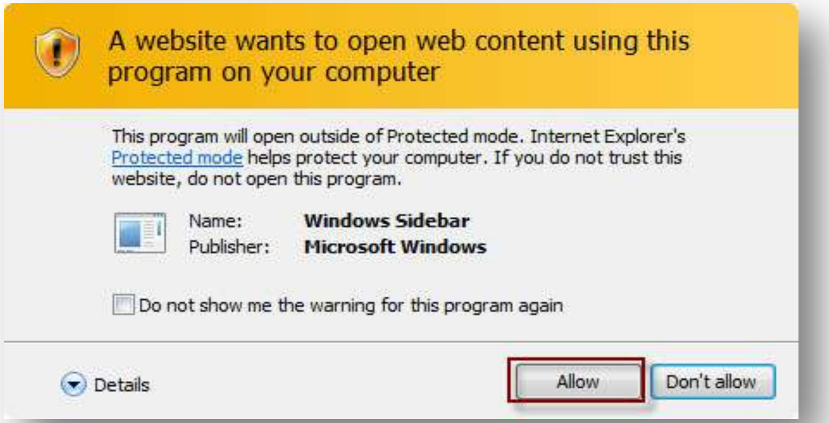
Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

More information



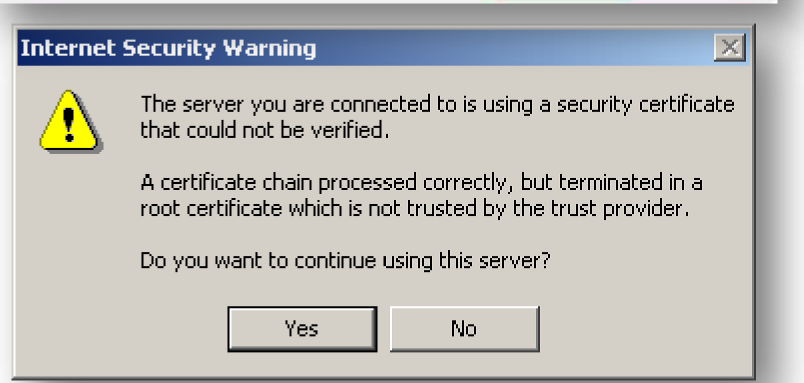
A website wants to open web content using this program on your computer

This program will open outside of Protected mode. Internet Explorer's Protected mode helps protect your computer. If you do not trust this website, do not open this program.

Name: **Windows Sidebar**

Publisher: **Microsoft Windows**

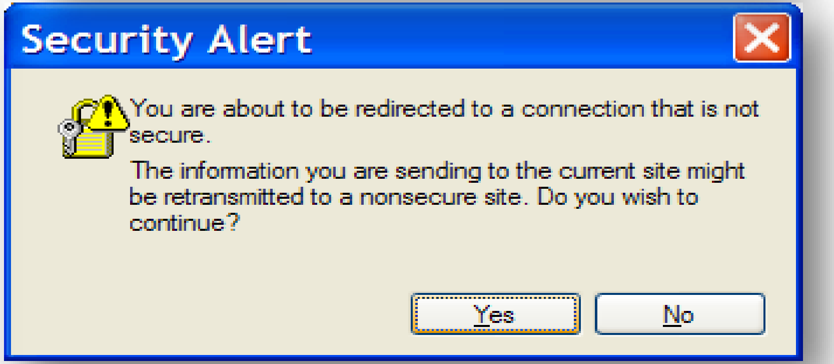
□ Do not show me the warning for this program again



The server you are connected to is using a security certificate that could not be verified.

A certificate chain processed correctly, but terminated in a root certificate which is not trusted by the trust provider.

Do you want to continue using this server?



You are about to be redirected to a connection that is not secure.

The information you are sending to the current site might be retransmitted to a nonsecure site. Do you wish to continue?

Q: Publisher could not be verified… will you continue ?

A: Sure, I need that application & I think that it just means I am installing something new and my Windows is old enough to recognize it. How come windows know that I wanted to install this application ??

Q: Website shows certificate was not issued by trusted authority…

A: Yeah, still click to continue as I want to check my mails/messages or I want to visit blogs. Rest, I don't know what a certificate has to do with this site (…its not a college degree site, then why any certificate etc.)

Q: Web browser lock icon. What is it ?

A: Oh! This I think it means I am secured; it symbolizes some kind of security, somehow, somewhere. And, I am protected and can't be hacked. Feels great!

Q: Web Site wants to open web content using this program…

A: I don't know whether to trust or not, but I will love this gadget on my sidebar. What harm can it do? We have big security appliances and servers in our company. huh !!

Q: You are about to be redirected to a connection that is not secured…

A: It means it is taking me to a new page, and there I can check my scraps or messages, and rest I never bothered about this as it pops daily, and see nothing has happened till now, so nothing will…

continued…

Q: Internet Explorer Web Site ActiveX Control installation warnings…

A: Yeah, I click install else the page will not load well. And, I know this because the site has listed it already. They knew that this warning will come and documented to click YES & INSTALL.

Q: To User: You surf and browse so many sites and links, what all you see to ensure security?

A: Foremost, I see my back to ensure boss or mentor is not here. And, then I sometimes see https to see its secured and I click the links that my good friends send, else mostly I don't click.
See, I am smart indeed !!

Q: Are you sure of security and are a smart user? and is there any corporate policy to block sites ?

A: Yes I am secured, as our company has big servers, security policies and 4-5 administrators and a separate IT support team. Yes, our company block sites too, but we are smart users, we use proxy to bypass and as soon as anyone comes to know something new, he/she sends a mail to us on how to open blocked sites.

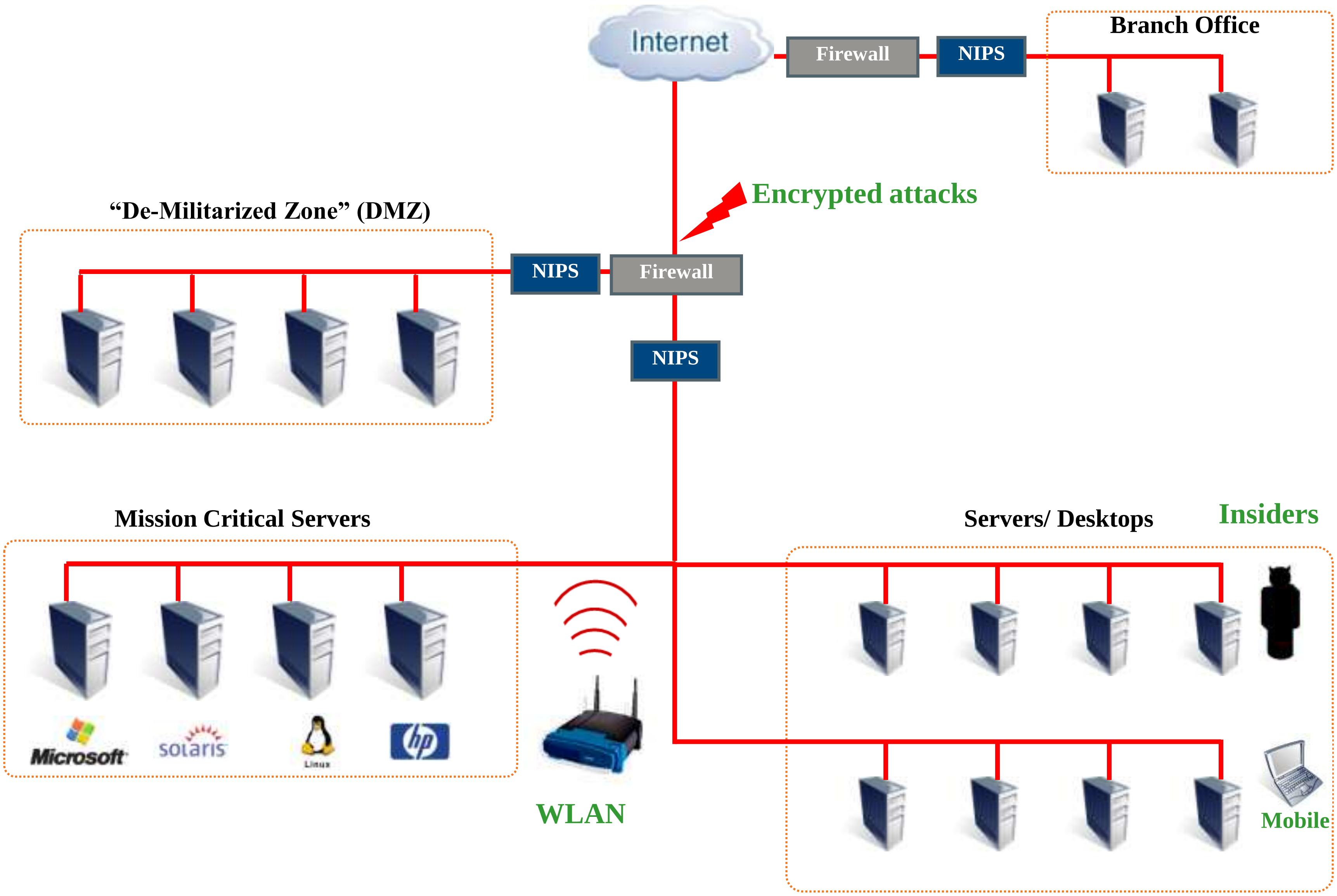
CONCLUSIONS

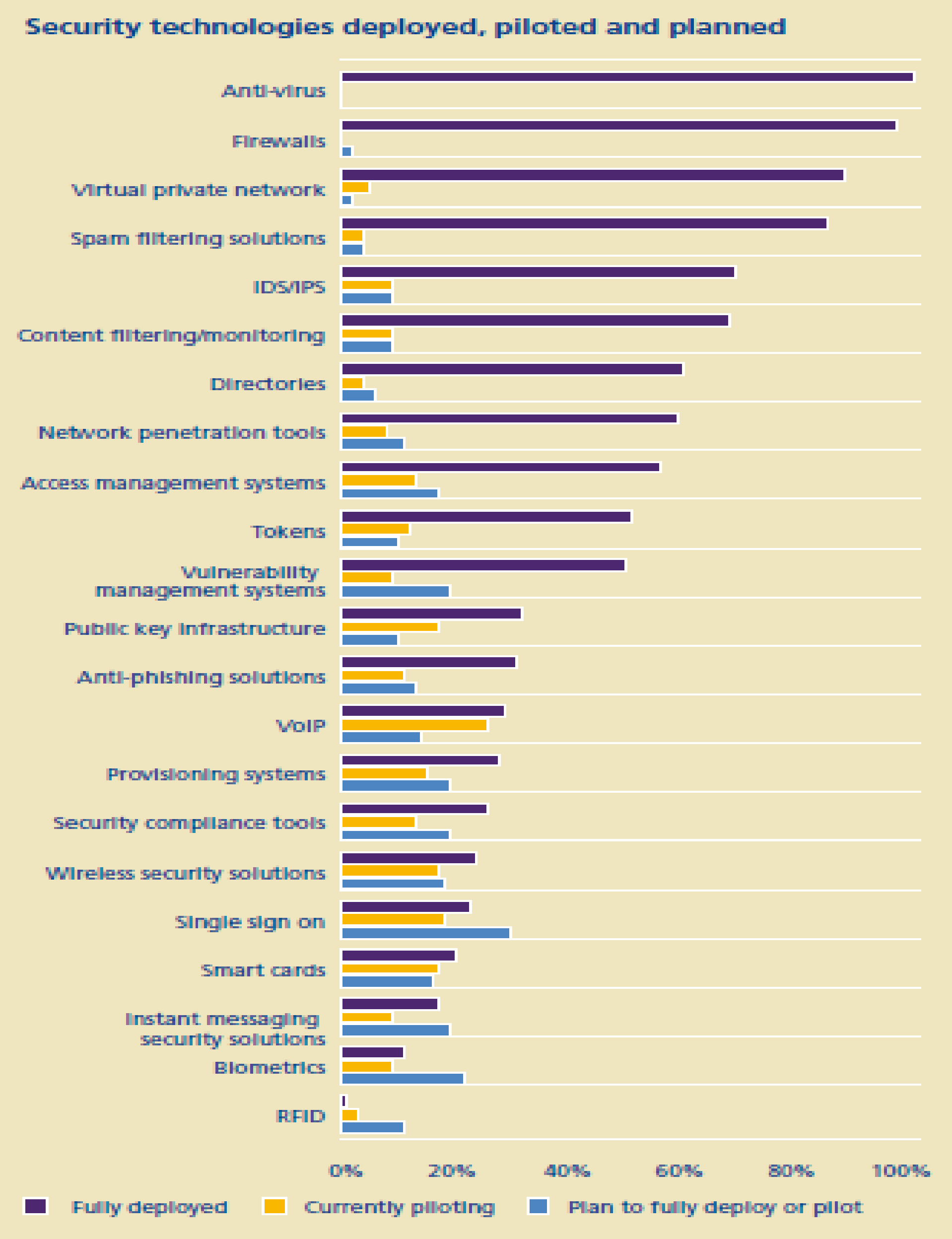
** Temptations
** Lack of awareness
** False Sense of Security
** Carelessness
** Curiosity
** Past Experiences

Security Products vs. Attacks

…in the dust of web, is security just a myth ??

Current Security Architecture





Security technologies deployed, piloted and planned

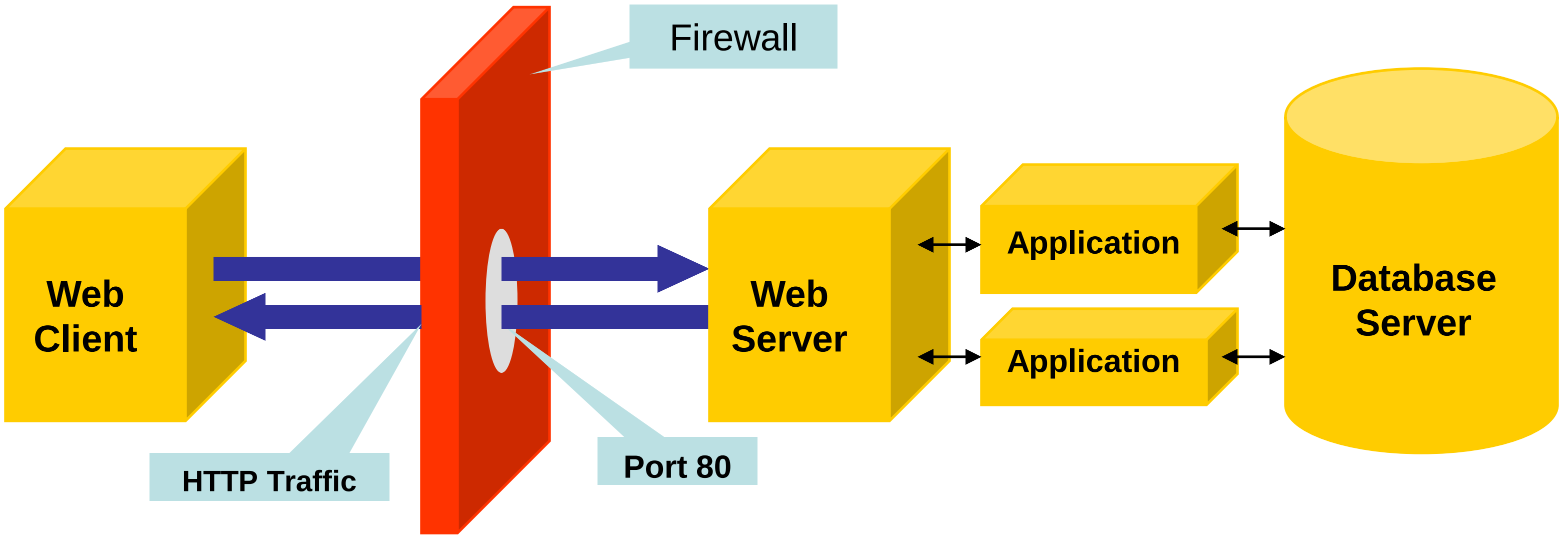
… in spite of so many security devices deployed or piloted, security awareness is the need of the hour as –

- **Companies are not even aware that their systems have been compromised.**

- **If aware, companies don't want to admit that their systems have been breached.**

- **Companies don't know what to do, or what is their Plan of Action after they get to know.**

- **Companies don't want to incur the expenses necessary to rectify the problem or breach.**



1. **Firewall protects Web Server & Database: Ports – 80, 8080, 443**

   - Firewall can't protect or look into the allowed traffic through HTTP ports that can be malicious and can exploit systems and networks. e.g. MPACK

   - Web Server or Web Apps Vulnerabilities may allow entry to Internal Network

2. **IDS/IPS protects Web Server & Database**

   - protection is based on signatures/filters of well known attacks not every 0-days

   - doesn't protect custom applications

   - heuristic protection/proactive web defense may result in False Positives on servers

3. **SSL Layer and protection to Web pages**

   - protects the packets transfer between server and client, thus Man in Middle attacks

   - fails to protect Web Server and its Applications' Vulnerabilities

4. **Secured Web Apps and HTTP Requests**

   - every HTTP request is not valid, still almost all Web Apps accept it

5. **Encryptions and Hash: File level Security (hide data, data integrity)**

   - server backup files, conf. files & admin dir. usually unattended & default

CONCLUSIONS

** Awareness & Responsibility

** Improved Practices

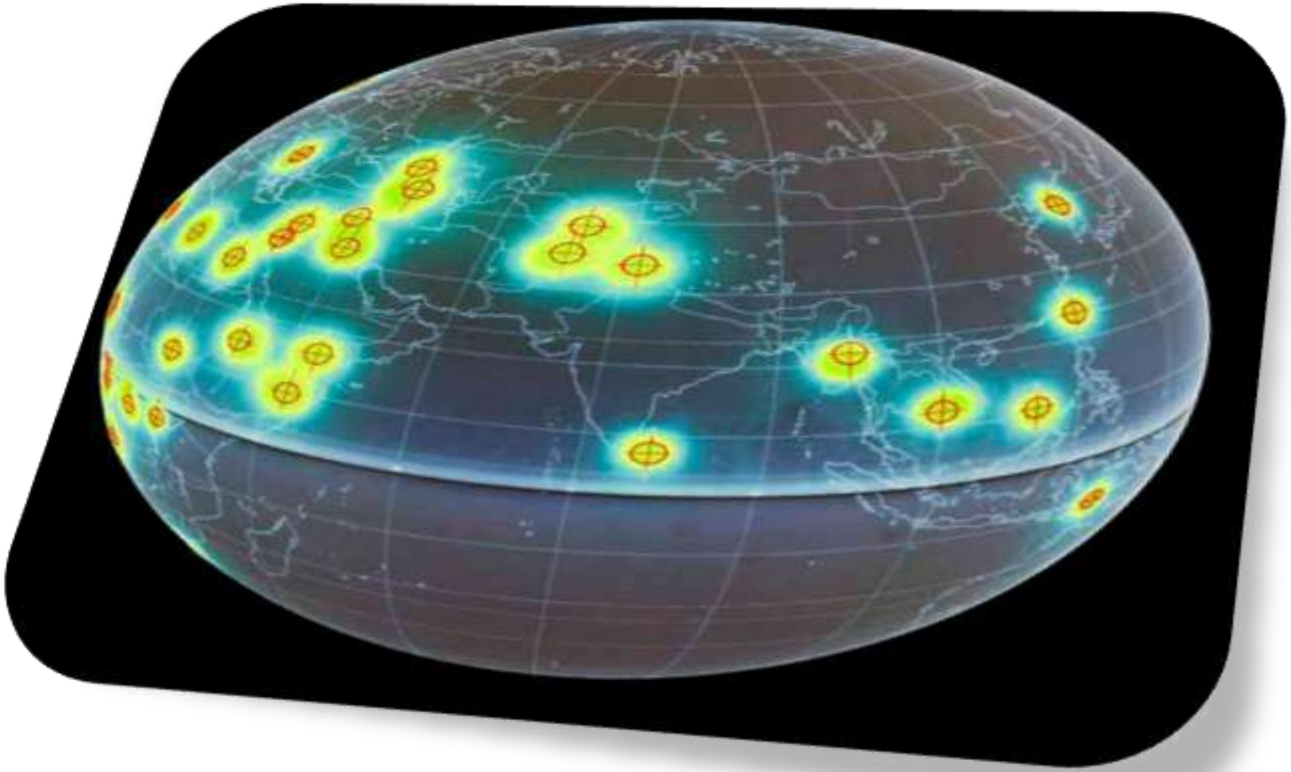
** Web Application Security

** Security Policies

** Host Applications' Security

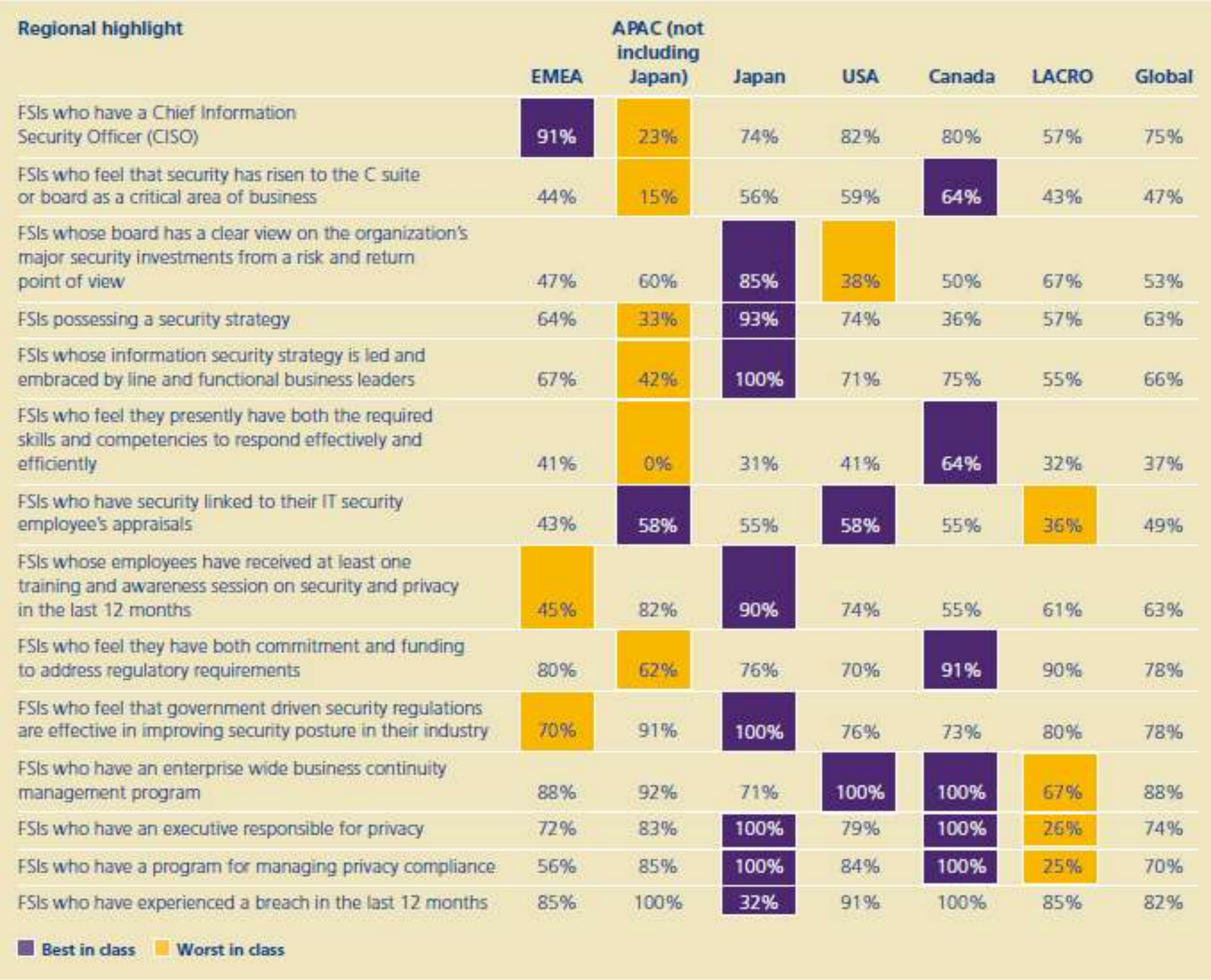
** Latest Security updates

Ideal World vs. Real World



…will the two sides of the same coin ever meet ??

FSIs Security: Geographic Distributions



Regional highlight	EMEA	APAC (not including Japan)	Japan	USA	Canada	LACRO	Global
FSIs who have a Chief Information Security Officer (CISO)	🟪 91%	🟨 23%	74%	82%	80%	57%	75%
FSIs who feel that security has risen to the C suite or board as a critical area of business	44%	🟨 15%	56%	59%	🟪 64%	43%	47%
FSIs whose board has a clear view on the organization's major security investments from a risk and return point of view	47%	60%	🟪 85%	🟨 38%	50%	67%	53%
FSIs possessing a security strategy	64%	🟨 33%	🟪 93%	74%	36%	57%	63%
FSIs whose information security strategy is led and embraced by line and functional business leaders	67%	🟨 42%	🟪 100%	71%	75%	55%	66%
FSIs who feel they presently have both the required skills and competencies to respond effectively and efficiently	41%	🟨 0%	31%	41%	🟪 64%	32%	37%
FSIs who have security linked to their IT security employee's appraisals	43%	🟪 58%	55%	🟪 58%	55%	🟨 36%	49%
FSIs whose employees have received at least one training and awareness session on security and privacy in the last 12 months	🟨 45%	82%	🟪 90%	74%	55%	61%	63%
FSIs who feel they have both commitment and funding to address regulatory requirements	80%	🟨 62%	76%	70%	🟪 91%	90%	78%
FSIs who feel that government driven security regulations are effective in improving security posture in their industry	🟨 70%	91%	🟪 100%	76%	73%	80%	78%
FSIs who have an enterprise wide business continuity management program	88%	92%	71%	🟪 100%	🟪 100%	🟨 67%	88%
FSIs who have an executive responsible for privacy	72%	83%	🟪 100%	79%	🟪 100%	🟨 26%	74%
FSIs who have a program for managing privacy compliance	56%	85%	🟪 100%	84%	🟪 100%	🟨 25%	70%
FSIs who have experienced a breach in the last 12 months	85%	100%	🟪 32%	91%	100%	85%	82%

🟪 Best in class 🟨 Worst in class

FSI
Financial Services Institutions

EMEA
Europe, Middle East & Africa

APAC
Asia Pacific

LACRO
Latin America & Caribbean

IDEAL WORLD

- Security thought out at the beginning of the project and throughout
- Security requirements exist, security policy is defined
- Threat Modelling is used to discover threats.
- Developers trained in application security, a security specialist is on board.
- Code reviews and assessment.

REAL WORLD

- Applications are insecure.
- Trivial vulnerabilities demonstrate serious lack of understanding of the web programming model.
- Users want features; security is an afterthought.
- Anyone with a browser can break in.
- Confident on Application Security & market it.

POINTS TO PONDER

- If you can **improve the software** – do it!
- Put **insecure applications** into **secure environments**.
- Use **threat modelling** for deployment, to determine the threats.
- **Correct architectural issues** if that can be corrected.
- Use **network design tools** to increase security by limiting exposure.
- Dissolve the myth "**It will not happen to us**". It can happen to anyone, anywhere and there are many vectors to support it.

PRIME FOCUS

- **Assessment**: Discover problems before attackers do.
- **Monitoring**: Know what happened. Monitor Logs, files, captures etc.
- **Detection**: Know when you are being attacked.
- **Prevention**: Stop attacks before they succeed. Secure your web applications.

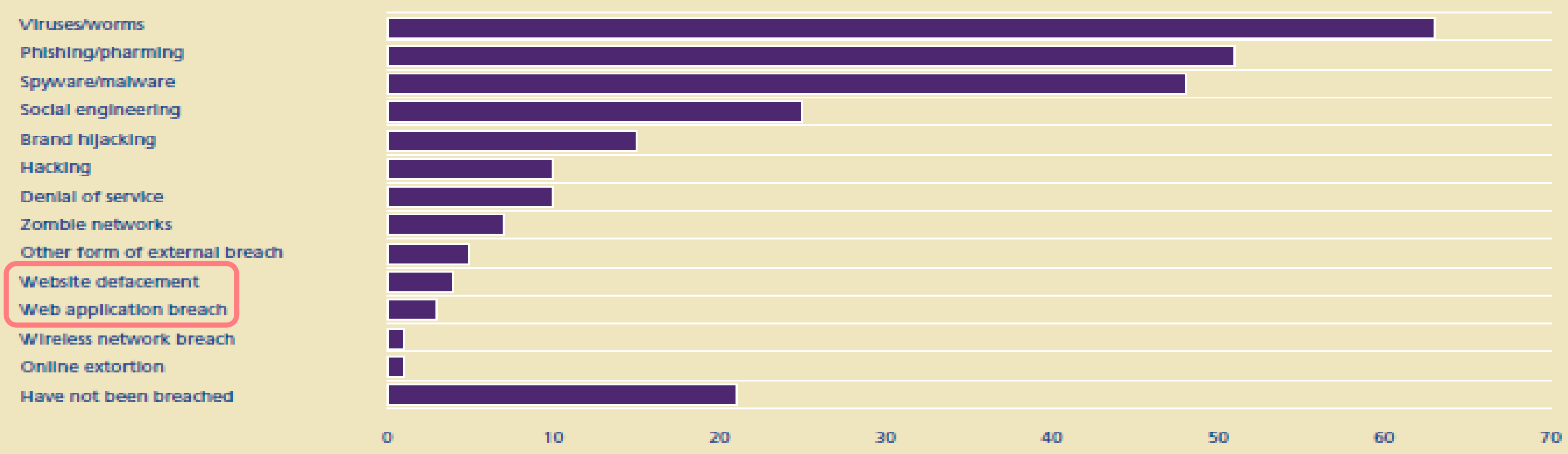
APPROACH TO PRIVACY

'Information sharing' - you tell me everything about yourself and I'll tell you when to stop.
CHRIS

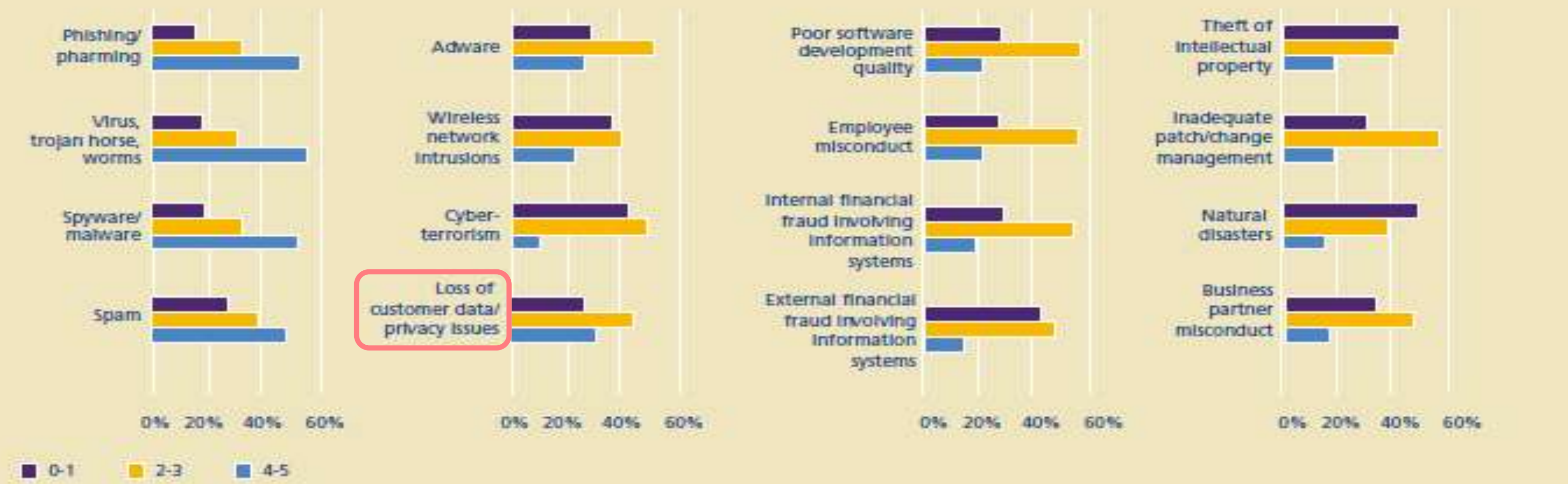
... the intersection of privacy and the internet requires a rule book that has yet to be written

PAST & FUTURE THREATS

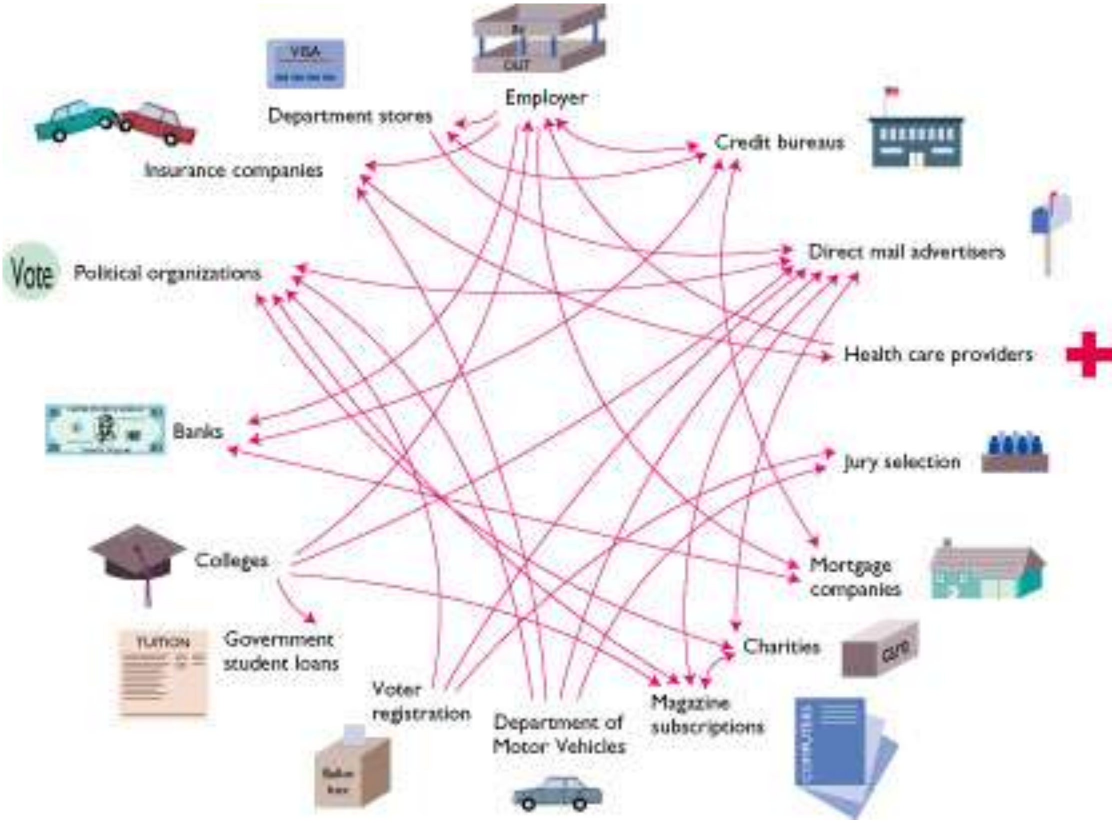
External breaches over the past 12 months



Threats envisioned over the next 12 months



Using a scale from 0-5 (0 being a non threat to 5 being a major threat) respondents rated the intensity of the following threats they envision over the next 12 months



01. Loans
02. Charge accounts
03. Orders via mail
04. Magazine subscriptions
05. Tax forms
06. Applications for schools, jobs, clubs

07. Insurance Claims
08. Hospital Stays
09. Sending checks
10. Funds raisers
11. Advertisers
12. Warranties

P3P: W3C Platform for Privacy Preferences (P3P) Project
W3C: World Wide Web Consortium

- **Collection of Personally Identifiable Information (PII)**
  Type of data collected through on-line forms
  Security of data collection

- **Visitor tracking**
  Provision of data to 3rd parties via cookies and web beacons

- **Adoption of Privacy Policies and posting of Privacy Statements**

- **Ensuring compliance with Privacy Policies**

- **P3P is a set of specifications for expressing a Web site's online privacy policy in machine interpretable way**

- **The standardized P3P format allows a web browser (or other user agent) to quickly evaluate a Web site's privacy**

- **Why is this important?**
  - Internet Explorer 6.0 (IE6), utilizes P3P to evaluate a Web site's privacy practices
  - IE6 automatically takes various actions on cookies based on the P3P policy (accept, leash, deny, downgrade)

P3P Deployments

P3P policies can be applied broadly or narrowly

- As broad as an entire site
- As narrow as a single URL on a site

P3P policies are applied to "HTTP entities"

- That is, URLs, not pages
- A page is typically many "entities" (frameset, framed content, graphics, style sheets, ...)

P3P uses a policy reference file (PRF) which:

- Lists the P3P policies used by the site
- States what parts of the site and what cookies are covered by each policy

A PRF can only cover resources on that domain

- Each domain needs its own policy reference file
- The policies themselves can be on another host & can be fetched

PRF File Contents

Allow specification of which policy applies:

<EXPIRY>: Determines how long PRF is valid

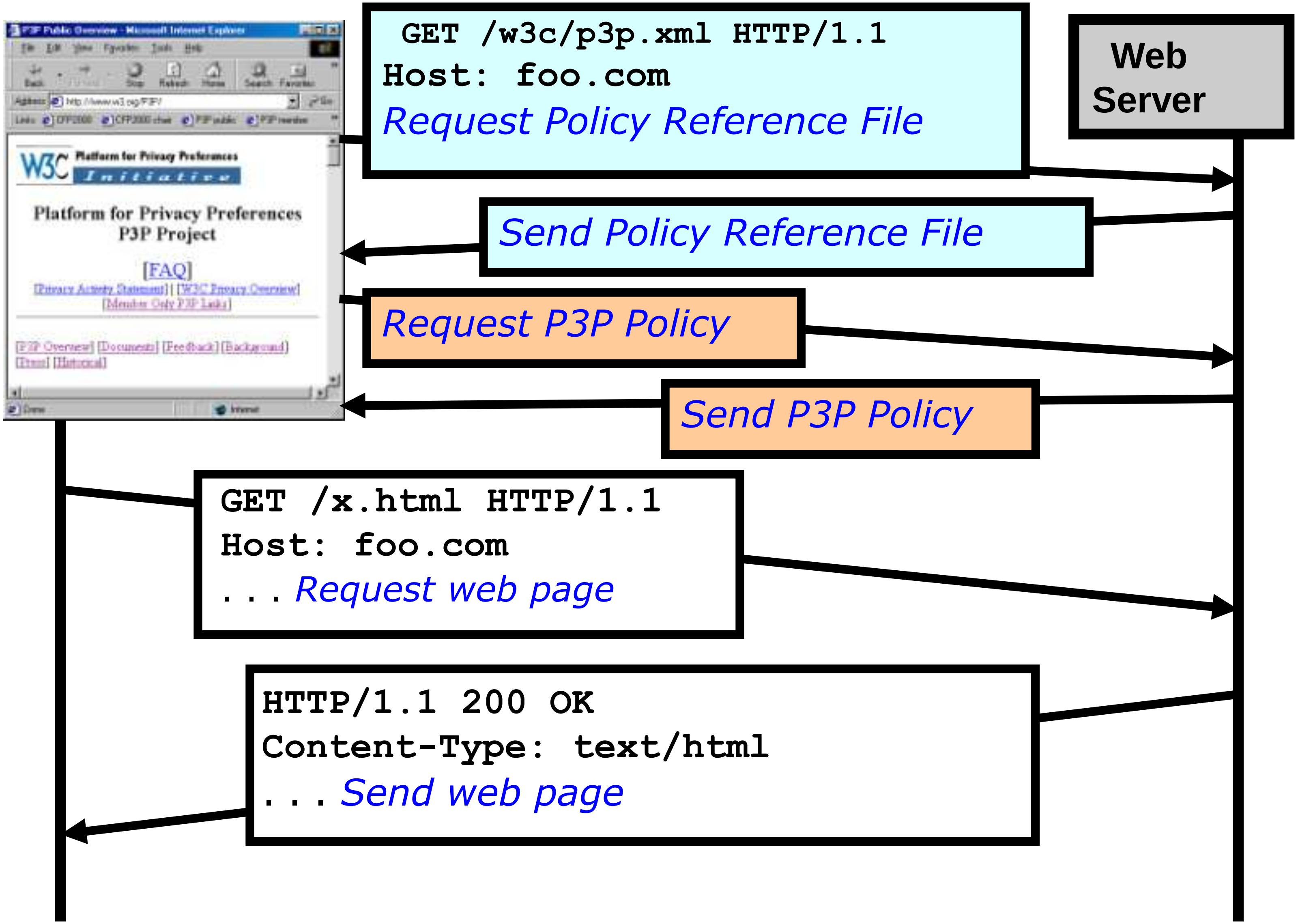
<POLICY-REF>: URL of policy

<INCLUDE>, <EXCLUDE>: URL prefixes (local) to which policy applies or doesn‵t apply

<COOKIE-INCLUDE>, <COOKIE-EXCLUDE>Associates or disassociates cookies with policy

<METHOD>: Methods to which policy applies

PRF Request in Action



```
 GET /w3c/p3p.xml HTTP/1.1
Host: foo.com
```

Request Policy Reference File

Send Policy Reference File

Request P3P Policy

Send P3P Policy

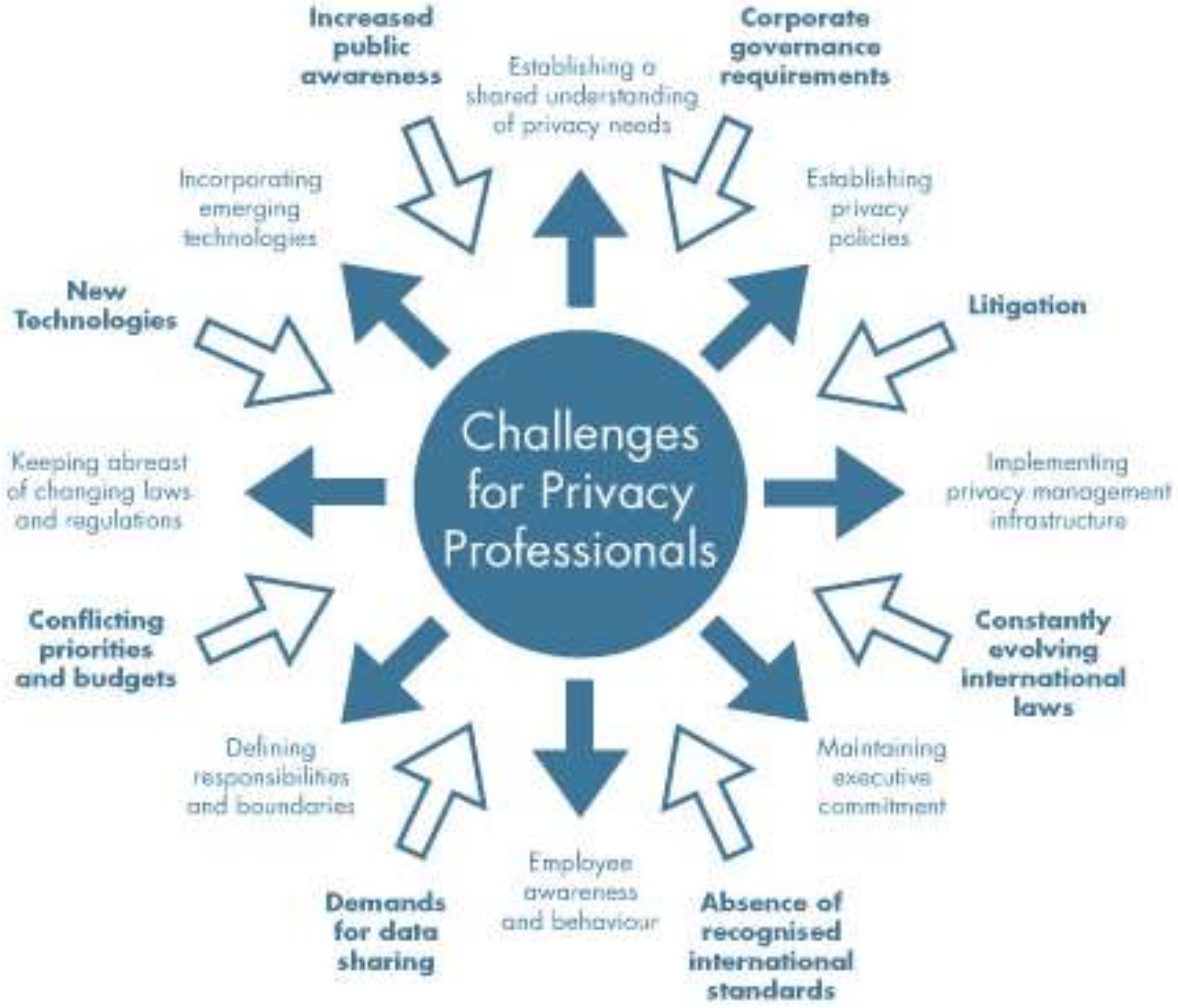
```
GET /x.html HTTP/1.1
Host: foo.com
```

. . . *Request web page*

```
HTTP/1.1 200 OK
Content-Type: text/html
```

. . . *Send web page*

Web Server
P3P Public Overview - Microsoft Internet Explorer
Platform for Privacy Preferences
Initiative
Platform for Privacy Preferences
P3P Project
[FAQ]



Challenges for Privacy Professionals

Increased public awareness

Establishing a shared understanding of privacy needs

Corporate governance requirements

Incorporating emerging technologies

Establishing privacy policies

New Technologies

Litigation

Keeping abreast of changing laws and regulations

Implementing privacy management infrastructure

Conflicting priorities and budgets

Constantly evolving international laws

Defining responsibilities and boundaries

Maintaining executive commitment

Demands for data sharing

Employee awareness and behaviour

Absence of recognised international standards

- increased media and public awareness of privacy issues & demands for correct use of personal information

- increased litigation arising from privacy-related incidents; demands for good corporate governance and social responsibility driven by emerging legislations

- the need to meet ever-changing national & international legal and regulatory requirements that impose different demands in different countries

- an absence of recognized international standards for privacy management

- the emergence of new technologies that are invariably a lightning rod for privacy-related problems as new risks are identified

- conflicting priorities for organizations that divert executive priorities away from privacy-related issues

- business pressures for greater sharing of personal information within and between organizations

Resources

- Cartoon Images: images (dot) google (dot) com
- Current Security Architecture: Third Brigade Inc.
- Statistical Chart and Graphs: 2006 Global Security Report (Finance Services Institutions) Deloitte
- 10 Steps to Secure: ZDNET White Paper
- Ideal World vs. Real World: ThinkingStone
- Privacy Approach: Joshua Freed, NETED
- securityfocus.com
- secunia.com
- symantec.com
- google.com

MEET ME

Rishi Narang
Vulnerability Research Analyst
Third Brigade Security Labs, Bangalore (INDIA)
_ official: rishi.narang (at) thirdbrigade (dot) com
_ personal: x72.x6e (at) gmail (dot) com
_ mobile: +91 988.6982.678

THANK YOU