2016 DATA PROTECTION CONFERENCE

BREAK-AWAY SESSION II

DATA PROTECTION & THE ONLINE ENVIRONMENT:

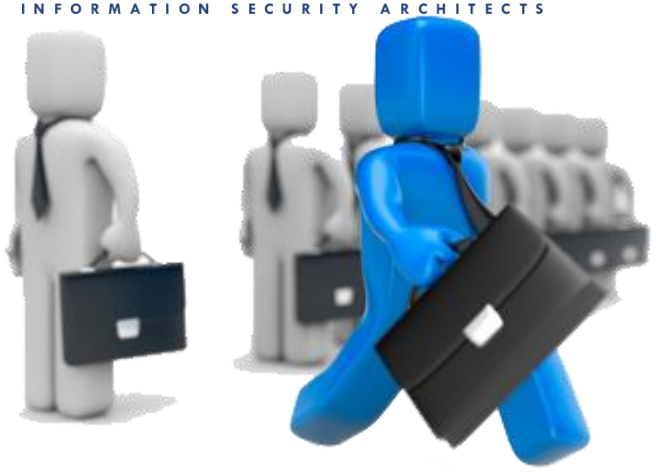
An IT Security Practitioner's Perspective

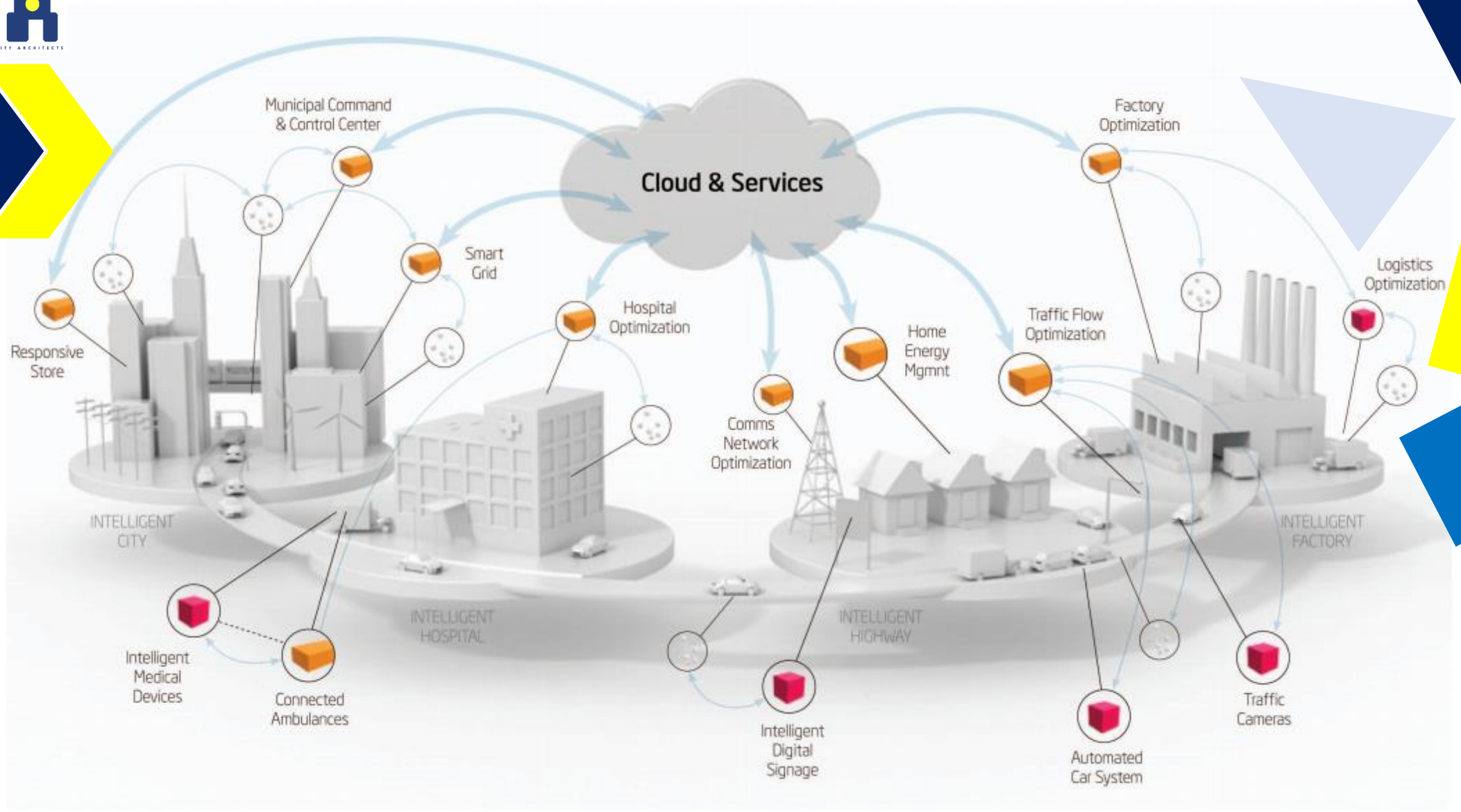
With references and Inspiration from:
Information Commissioners Office, UK

Protecting personal data in online services: learning from the mistakes of others
May 2014 Whitepaper

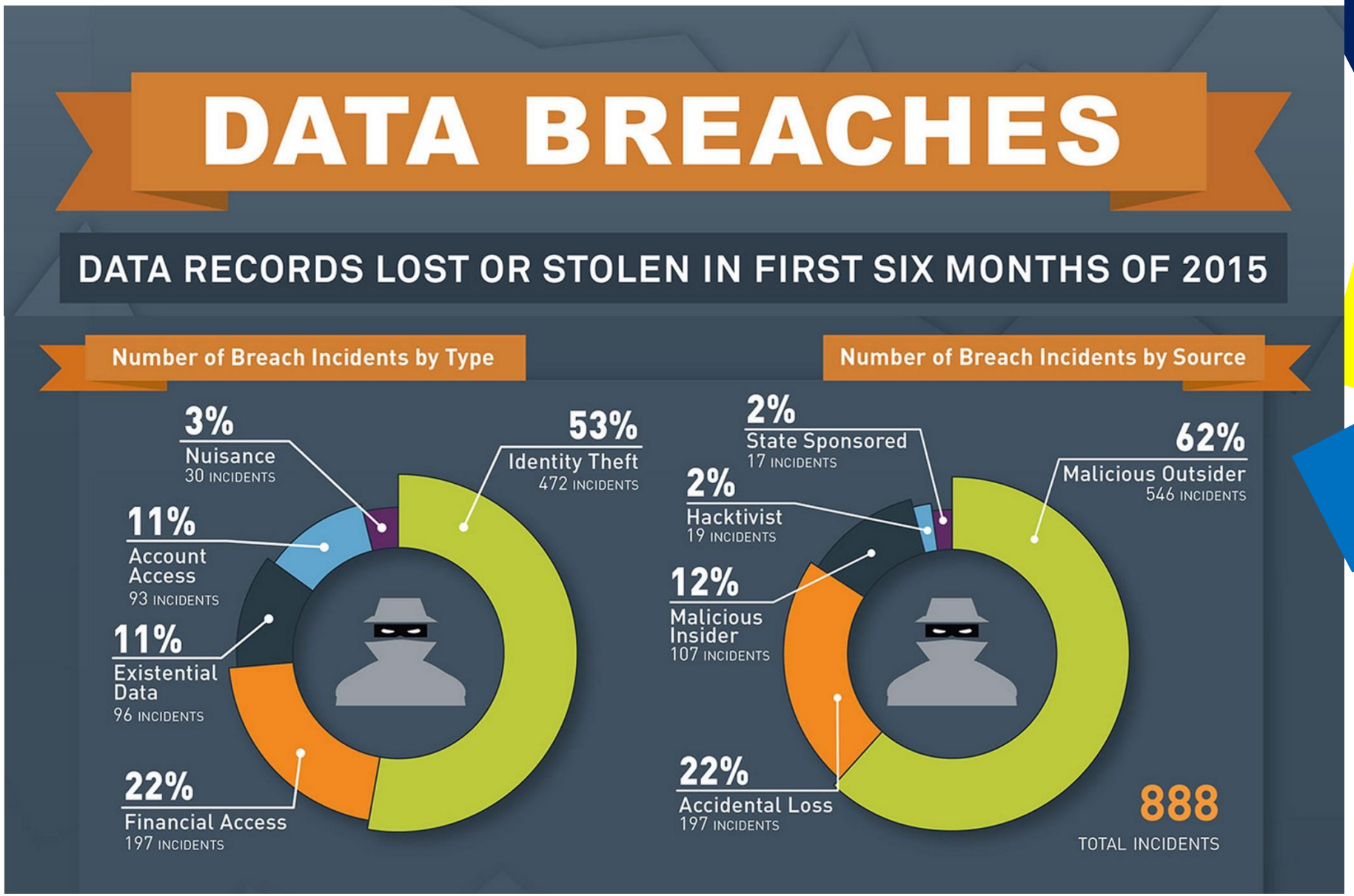
Who am I?

Presented By:
Desmond Israel (LLB| BSC | CASP | CCNSP | QCS-VM)
Enterprise IT Security Practitioner
Executive Director & Consulting Partner
Information Security Architects Ltd
8 Lomo Adawu Street, La – Accra, Ghana
desmond@isa.com.gh
+233233333163




Cloud & Services
Municipal Command & Control Center
Factory Optimization
Smart Grid
Hospital Optimization
Home Energy Mgmnt
Traffic Flow Optimization
Logistics Optimization
Responsive Store
Comms Network Optimization
INTELLIGENT CITY
INTELLIGENT HOSPITAL
INTELLIGENT HIGHWAY
INTELLIGENT FACTORY
Intelligent Medical Devices
Connected Ambulances
Intelligent Digital Signage
Automated Car System
Traffic Cameras

What we mostly do....


DATA BREACHES
DATA RECORDS LOST OR STOLEN IN FIRST SIX MONTHS OF 2015
Number of Breach Incidents by Type
3%
Nuisance
30 INCIDENTS
53%
Identity Theft
472 INCIDENTS
11%
Account Access
93 INCIDENTS
11%
Existential Data
96 INCIDENTS
22%
Financial Access
197 INCIDENTS
Number of Breach Incidents by Source
2%
State Sponsored
17 INCIDENTS
62%
Malicious Outsider
546 INCIDENTS
2%
Hacktivist
19 INCIDENTS
12%
Malicious Insider
107 INCIDENTS
22%
Accidental Loss
197 INCIDENTS
888
TOTAL INCIDENTS

An idea of what we should do....

- What the DPA says

- Software security updates
- SQL injection
- Unnecessary services
- Decommissioning of software or services
- Password storage
- Configuration of SSL or TLS
- Inappropriate locations for processing data
- Default credentials

Where the law aligns .....

- The Data Protection Act 2012
- Centered on eight (8) principles for good information handling
- Give specific rights to data subjects
- Provides obligations for data subjects and processors
- We focus on the 7th principle intended to informed about appropriate safeguard measures to protect personal data.
- Online services is our focus.

What's up with software updates

- Software updates policy for all software used for processing personal data. Cover OS, apps, libs and dev frameworks in policy
- There may be good reasons not to apply all available updates as soon as possible. Your policy can take into account these reasons.
- When there is no compelling reason to delay, you should apply security updates as soon as is practical.

The SQL Injection dose...

- Be aware of all of your assets that might be vulnerable to SQL injection.
- Can affect applications that pass user input into a DB. [E.g Web sites/apps]
- Presents a high risk of compromising significant amounts of personal data. Must have high priority for prevention, detection and remediation.

The SQL Injection dose...

- Happens from coding flaws – coders (develop and maintain codes). You will need to rely on to prevent SQL injection or fix SQL injection flaws if they are found.
- Independent security testing (penetration testing, vulnerability assessment, or code review, as appropriate). Do this before the application goes live. It is good practice to periodically test live applications.
- When remediating an SQL injection flaw, use parameterised queries where possible, and ensure that all similar input locations are also checked and remediated.

3

Unnecessary services? Really?

- Completely decommission any service that is not necessary.
- Avoid high risk services such as telnet, ftp, smtp etc
- Ensure that services intended for local use only are not made publicly-available.
- Use periodic port-scanning to check for unnecessary services which have been inadvertently enabled.
- Maintain a list of which services should be made available.
- Periodically review the list to see whether any services have become unnecessary, and restrict or decommission them as appropriate.

4

Retiring ...software & services

- Be aware of all the components of a service so that you can make sure they are all decommissioned.
- Make a record of any temporary services which you will eventually need to disable.
- Thoroughly check that the decommissioning procedure has actually succeeded.
- Use systematic tools such as port scanners to do this where possible.
- Do not forget to arrange for proper disposal of any hardware, as appropriate.
- Refer the ICO guidance on IT disposal it helps a lot.

5

Password storage... do it well

- Don’t store passwords in plain text, nor in decryptable form.
- Use a hash function. Only store the hashed values.
- Hash functions with appropriate strength to make offline brute-force attacks difficult.
- Use salting to make offline brute-force attacks less effective.
- Periodically review the strength of the hash function.
- keep up to date with advances in computing power, use password hashing scheme with a configurable work factor(KDF).
- Use a combination of password strength requirements and user-education.
- Have a plan of action in case of a password breach.

6

Cyphering online traffic.. SSL

- Ensure that personal data (and sensitive information generally) is transferred using SSL or TLS where appropriate.
- Use SSL or TLS for all data transfer in order to reduce complexity.
- Any included content such as images, javascript or CSS should also be provided over SSL or TLS in order to avoid 'mixed content' warnings.
- Ensure that SSL or TLS is set up to provide encryption of adequate strength.
- Ensure that every SSL or TLS service uses a valid certificate, and schedule renewal of all certificates before they expire to ensure the services remain secure.
- Obtain an Extended Validation (EV) certificate if assurance of identity is of particular importance.
- Do not encourage users to ignore SSL or TLS security warnings.

QUALYS® SSL LABS

Home Projects Qualys.com Contact

You are here: Home > Projects > SSL Server Test > (

SSL Report: ebank. .com (( ))

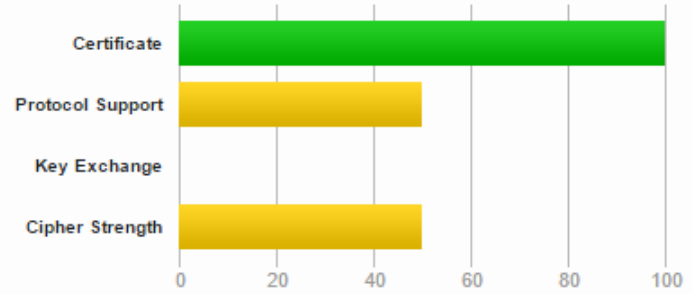
Assessed on: Fri, 29 Jan 2016 01:38:30 UTC | Clear cache

Scan Another »

Summary

Overall Rating

F



Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server supports insecure Diffie-Hellman (DH) key exchange parameters (Logjam). Grade set to F. MORE INFO »

Certificate has a weak signature and expires after 2015. Upgrade to SHA2 to avoid browser warnings. MORE INFO »

The server supports only older protocols, but not the current best TLS 1.2. Grade capped to C. MORE INFO »

This server accepts RC4 cipher, but only with older protocol versions. Grade capped to B. MORE INFO »

The server does not support Forward Secrecy with the reference browsers. MORE INFO »

7

Inappropriate data processing..

- Ensure testing or staging environments are segregated from the production environment.
- Segmenting network according to function and in accordance with your data protection policies.
- Network architecture accounts for functions such as backups and business continuity.
- Policies for how, when and where personal data will be processed.
- Consider all the services you are running, how they are accessible, and whether they comply with your policies.
- Ensure any web servers are exposing only the intended content. Where necessary, apply specific access restrictions.
- Do not rely merely on obscurity to prevent access.

Default credentials.. Huh?

- Change any default credentials as soon as possible.
- When changing default credentials, remember to follow good practice on password choice.

- Ensure that credentials are not hard-coded into any of your software.
- Ensure that credentials are not transmitted in plain text.

THANK YOU
FOR STAYING …

Try me ….

desmond@isa.com.gh
+233233333163

KEEP IT SECURE
Preferred Partner

DEMOS & QUESTIONS