Regional Forum on Cybersecurity in the Era of Emerging Technologies
&
the Second Meeting of the "Successful Administrative Practices"-2017
Cairo, Egypt 28-29 November 2017

Enforcing privacy: Regulatory & Legal approaches

Emadeldin Helmy, PhD, CRR-BC

Agenda

Definitions

What is the difference between the privacy and security of health information?

Regulatory & Legal

Approaches

Conclusions

Privacy

Just as you can look out a window, others can look in. Preventing unwanted eyes from looking in can be addressed by putting a drape, a curtain, or a shade inside of the window. This is privacy. Obscuring the view inside of your home also provides a little security as intruders may not be able to tell when you are home or see the things you own.

- What data should be collected?
- What are the permissible uses?
- With whom might it be shared?
- How long should the data be retained?
- What granular access control model is appropriate?

Privacy, security and business information

It is not much different in a business environment with regard to information. Security provides protection for all types information, in any form, so that the information's confidentiality, integrity, and availability are maintained. Privacy assures that personal information (and sometimes corporate confidential information as well) are collected, processed (used), protected and destroyed legally and fairly.

Just as the drapes on a window may be considered a security safeguard that also protects privacy, an information security program provides the controls to protect personal information. Security controls limit access to personal information and protect against its unauthorized use and acquisition. It is impossible to implement a successful privacy program without the support of a security program.

Just as the bars on a window help prevent intruders from entering into your home while allowing people to look inside, a security program can implement controls without regard for privacy. For example, a security program could require credentials to access a network without restricting access to personal information. You would have security but no privacy, as anyone with valid credentials can see all of the personal information your organization possesses.

What information does a privacy program protect?

A security program protects all the informational assets that an organization collects and maintains

One way to define personal information is to look at applicable laws and regulations. Often, in the U.S., statutes and regulations define personal information as first name or initial along with a government **issued identification number**, **financial account information, or health information**. While the protection of this type of information provides direct protection against identity theft, theft of funds and discriminatory acts, is this definition comprehensive?

Consider an email address. For many web sites, an email address is half of the credentials needed to sign in.

Also, if an email address for an individual is obtained from a particular business, it is easy to create a credible phishing campaign posing as providing a communication from that business.

If a legal definition for personal information is used, email address may not be protected adequately against unauthorized access nor will people be notified if their email address is lost in a data breach.

A privacy program needs to at least consider going beyond the legal definition of personal information

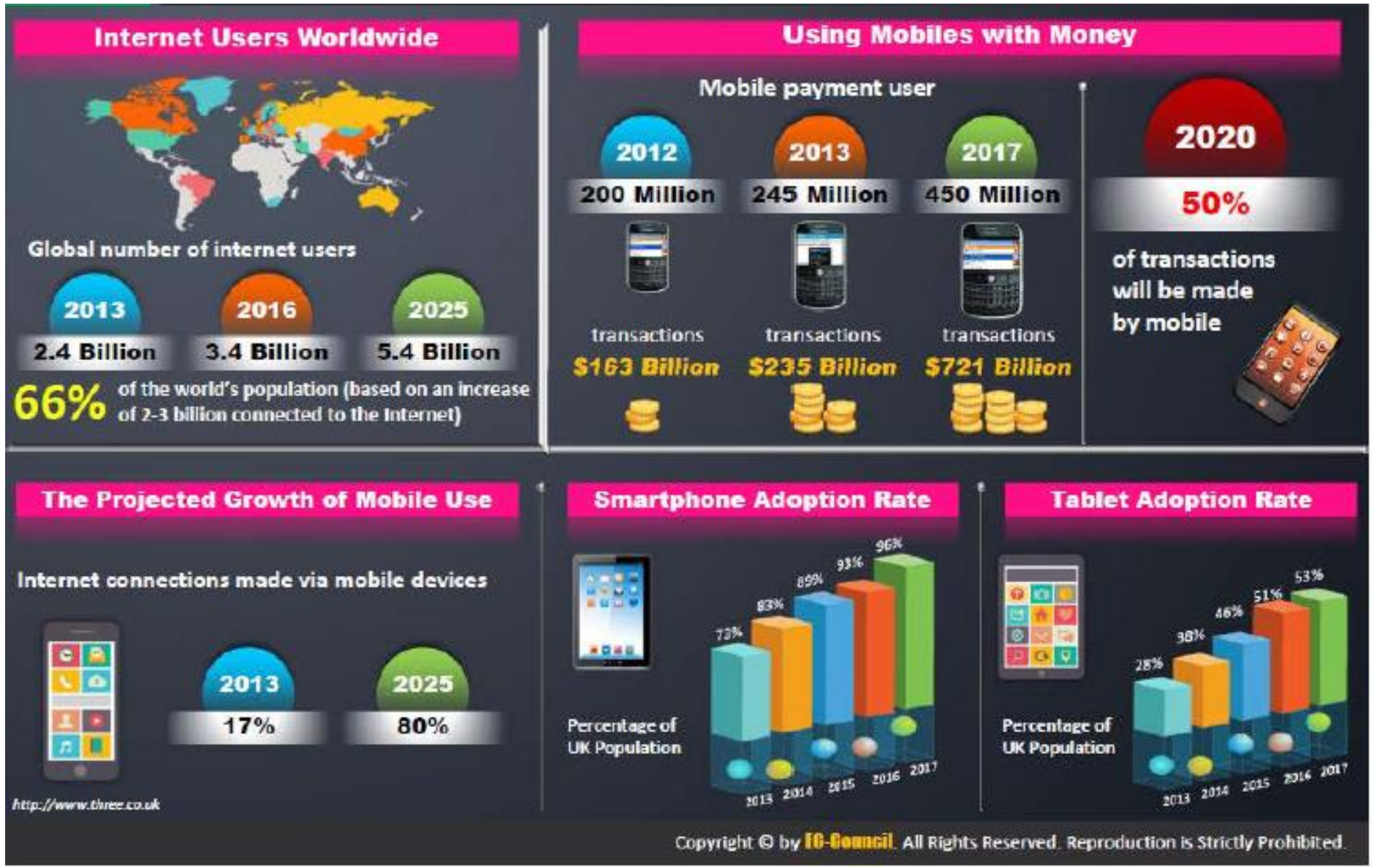
Protecting personal information

Given the organizational definition of personal information as a foundation, a privacy program needs to define the processing and protection requirements for personal information. The protection requirements include items such as what organizational roles have access to the information, when and how the information may be shared internally and externally, and when and how the information should be destroyed. These requirements should relate to personal information on any media, not just electronically stored.

These and similar privacy-related requirements are provided to the security program to implement appropriate protections and controls. It is not up to a privacy program to state the technology or processes to be used to protect personal information (though the privacy team may have valuable opinions); it is up to the security specialists to make this determination.

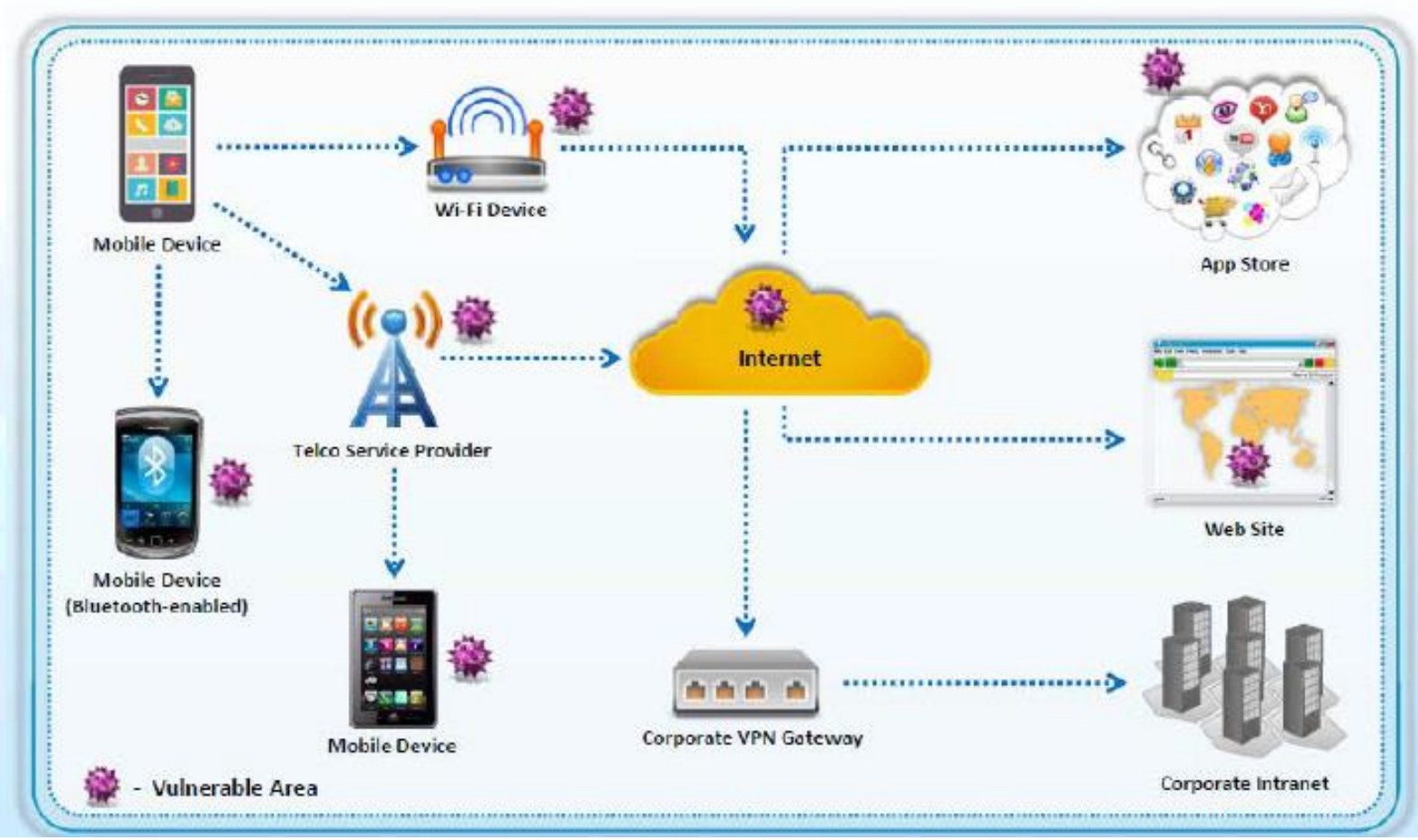
Therefore, a privacy program is dependent upon a security program. This creates a necessity to establish a cooperative, interdependent relationship be established between the teams (and the Chief Privacy Officer and Chief Security Officer).

Mobile Future



Vulnerable Areas in Mobile Business Environment

اين توجد الثغرات فى خدمات المحمول



Anatomy of a Mobile Attack

NTRA
National Telecom Regulatory Authority
الجهاز القومي لتنظيم الإتصالات

ITUWTDC
BUENOS AIRES 2017
9-20 October

5 WAYS

Your Vendor Risk Management Program Leaves You In The Dark

(& What You Can Do About It)

ITU-D 1992 2017
CELEBRATING 25 YEARS OF ACHIEVEMENTS

Here are a few commonly-used methods that are conducted in random:

1 **Questionnaires** are a typical standby for measuring vendor risk. They can be hundreds of questions long, and they ask the vendor questions like, “Do you have antivirus software installed?” or “Have you properly implemented SSL?” However, do those questions actually help you understand their long-term security risk? Unfortunately they only give you part of the picture as they assess which controls are in place, not the effectiveness of those controls.

2 Asking vendors to **send documentation**, like their last audits, allows you to see what they’ve done in the past. But, it doesn’t give you an indication of where they’ll be in the future (making these reports obsolete rather quickly).

3 A **desk assessment**—which takes place over the phone—is often the next step. This allows both parties to discuss and review the questionnaire.

4 Sending one of your team members to the vendor for an **on-site visit** is another common VRM protocol. This, however, is costly and time-consuming.

5 Finally, a **penetration test** can be performed, either on- or offsite.

Penetration tests enable you to identify vulnerabilities in the vendor's network security. Unfortunately, vulnerabilities change rapidly, so the test results are only valid for the time they are run. That means tests have to be run again to ensure the issues have been resolved.


ITUWTDC
BUENOS AIRES 2017
9-20 October

Thank You


ITU-D
1992
2017
CELEBRATING
25YEARS
OF ACHIEVEMENTS