

The Challenge of Global Compliance

- A Look at the Approach and Experience of Samsung Electronics -

SVP, Sang-joo Lee

Samsung Compliance Team



Samsung Compliance Activities

Prevention

Employee **education**, distribution of **manual on compliance Items**, system-based self-inspection, help desk, **staying up-to-date on** introduction/revision of **laws and regulations**

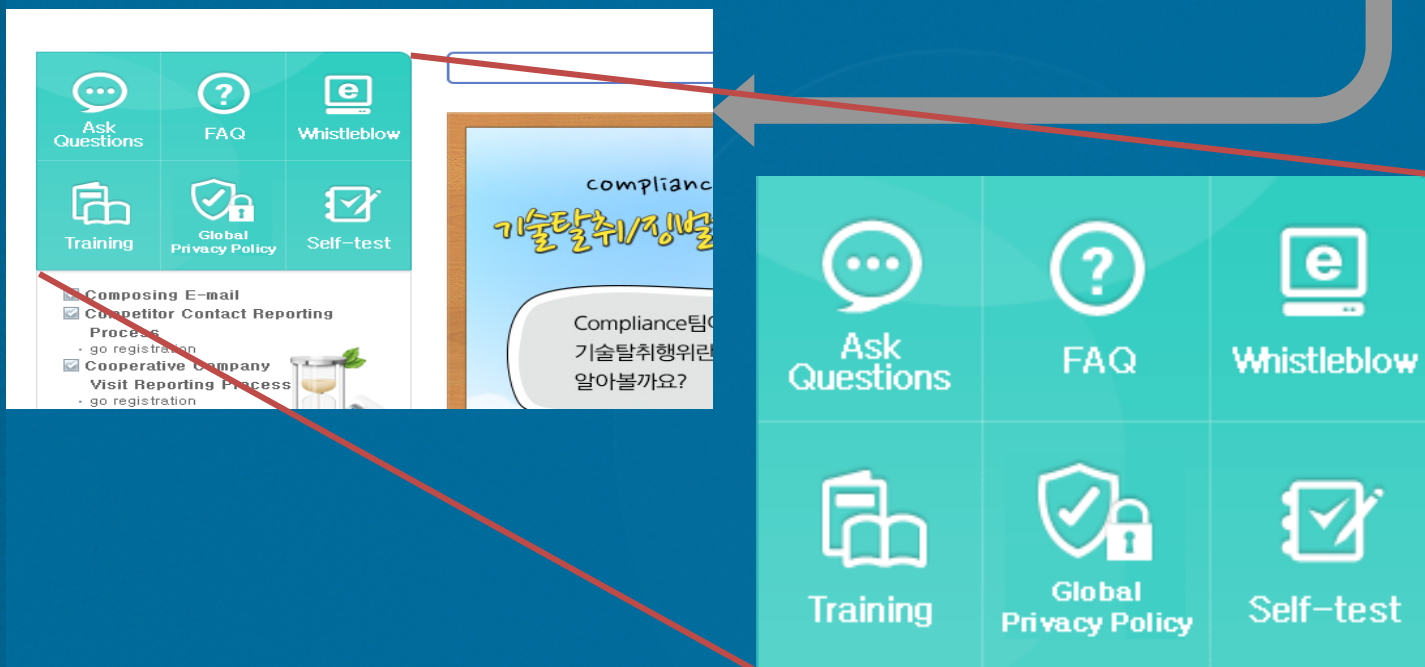
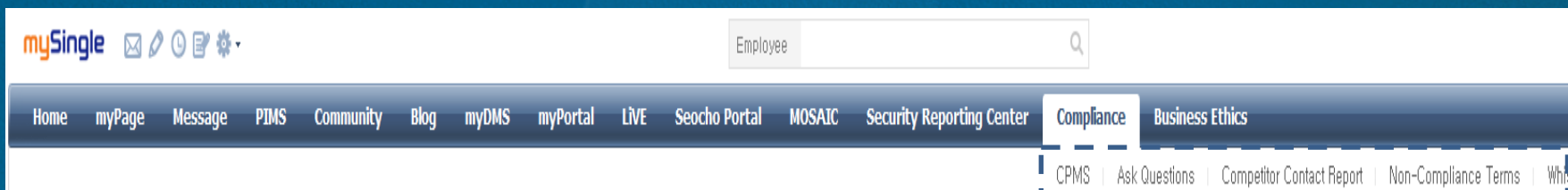
Monitoring

Regular and non-regular monitoring by pertinent organization units or persons

Follow-up

Identifying the cause of a problem via **analysis** of process and outcome, improvement activities, **preventing recurrence** through case studies

Compliance Program Management System



Supporting Languages : Korean, English, Chinese and Japanese

Compliance Desk

Compliance Guide

Competitor Contact
Composing Email(CPGS)
성희롱 방지

- Anti-corruption
- Ask Questions
- Whistleblow
- Self-test
- FAQs
- Training
- Notices

Competitor Contact Reporting Process

In order to protect employees from the risks of antitrust violations that could arise from **contact with employees of competitor companies**, Compliance Team is operating "Competitor Contact Reporting Process."



Scheduled meeting
with competitor companies
Must proceed self-check
after the meeting

Prior-meeting



Spontaneous meeting
with competitor companies

Post-meeting

The employees who follow the above process will be able to minimize the risk of being subject to an antitrust violation associated with contact with ECC.

[View FAQ](#)

[View System Manual](#)

Compliance Risks need to be covered

Personal Data Protection

Anti-corruption

Trade Secrets

Fair Labeling and Advertising

Fair Competition

HR related issues, etc.

Compliance Risks need to be covered

Personal Data Protection

Anti-corruption

Trade Secrets

Fair Labeling and Advertising

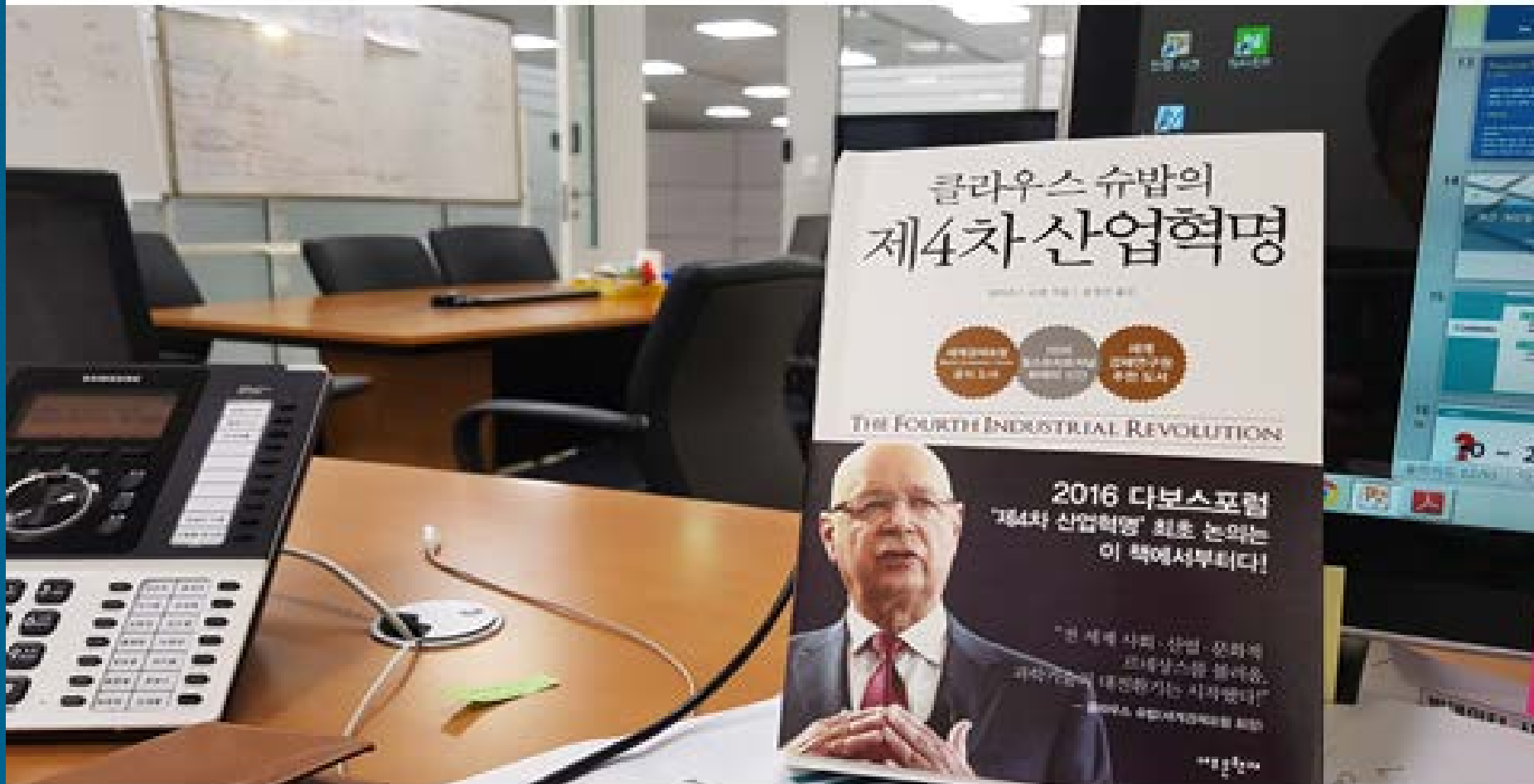
Fair Competition

Lawful Use of Software

Compliance Risks: personal data protection



The 4th industrial revolution, Klaus Schwab



The 4th industrial revolution



AI

Big data

IoT, VR, Robot, Gene sequencing...

Three major elements of AI

- ✓ Computing power
- ✓ Algorithm
- ✓ Data

Global Trends in Data Protection Regulation

Compliance Risks: personal data protection



▪ EU GDPR, effective May, 2018

(general data protection regulation)

- explicit consent
- data transfers allowed by “adequacy” decision
- 20,000,000 EUR or 4% of the worldwide annual turnover

Compliance Risks: **personal data protection**



Russia

- **Amendments on “Personal Data Act” Sep, 2015**
- database to be localized in Russia.

Turkey

- **‘Data Protection Law’ enacted in April, 2016**
- explicit consent.
- Cross-border data transfer resembles EU model

Compliance Risks: **personal data protection**



New regulations under consideration

China : A draft of 'Cyber Security Law'

- Data to be localized

Brazil : A draft of 'Data Protection Law'

- Restriction from transferring personal data to countries that do not provide similar levels of data protection.
- fines, prohibition of processing personal data for 10 years.

Action Plans #1

- ✓ **IDC, HR data server within the EU**
- ✓ **Onward transfer: DTAs and BCRs.**

Action Plans #2

- ✓ **Continued monitoring of local laws regarding cross border data transfers**
- ✓ **Coordination between HQ and subsidiary.**

Triage based on Severity of Local Laws

- ✓ **1st Tier: Strict compliance is required. (EU, Singapore, Russia)**
- ✓ **2nd Tier: Ongoing monitoring is required. (China, Brazil, Turkey)**
- ✓ **3rd Tier: Other countries**

Data Privacy Laws of Korea

- Structure and Enforcement -

Personal Information Protection Act (PIPA)

- ✓ **Information Communication Network Act**
- ✓ **Location Information Act**
- ✓ **Credit Information Act**

Personal Information Protection Act

- ✓ **Consent regime**
- ✓ **Ministry of the Interior**
- ✓ **Personal Information Protection Commission**

Information Communication Network Act

- ✓ **Consent regime**
- ✓ **Communications Commission**

Location Information Act

- ✓ **Consent regime**
- ✓ **Communications Commission**

Credit Information Act

- ✓ **Consent regime**
- ✓ **Restrictions on sharing with a third party**
- ✓ **Financial Services Commission,
Financial Supervisory Service**

Criminal Enforcement

- ✓ **PIPA,
Information Communication Network Act,
Location Information,
Credit Information Act**
- ✓ **Potentially strong deterrent against would-be violators**

Civil Lawsuits

Recent legislative efforts:

incentivizing civil lawsuits

- ✓ **Punitive damages**
- ✓ **Statutory damages**
- ✓ **“Group lawsuit”**

Administrative measures

Personal Information Protection Commission

- Various authorities

Ministry of the Interior

- administrative fines or order corrective measures. etc.

Communications Commission

Financial Services Commission

- fines up to 3 % of the relevant sales revenue

Data Breach

Korean Data Breach Status

뉴스 > 사회 > 뉴스라인



개인 정보 유출 1초에 1건...피해도 급증

입력 2015.12.23 (23:03) | 수정 2015.12.24 (00:51) | 276

뉴스라인

표준 화질

고화질

키보드 컨트롤



Total Data Breach Cases (`11.10.1 ~ `15.12.31)



67 Cases
130 million People

Market rates for Personal Data In Korea



\$ 0 ~ 2

Market Rates for Unlawfully Attained Personal Data 1/2

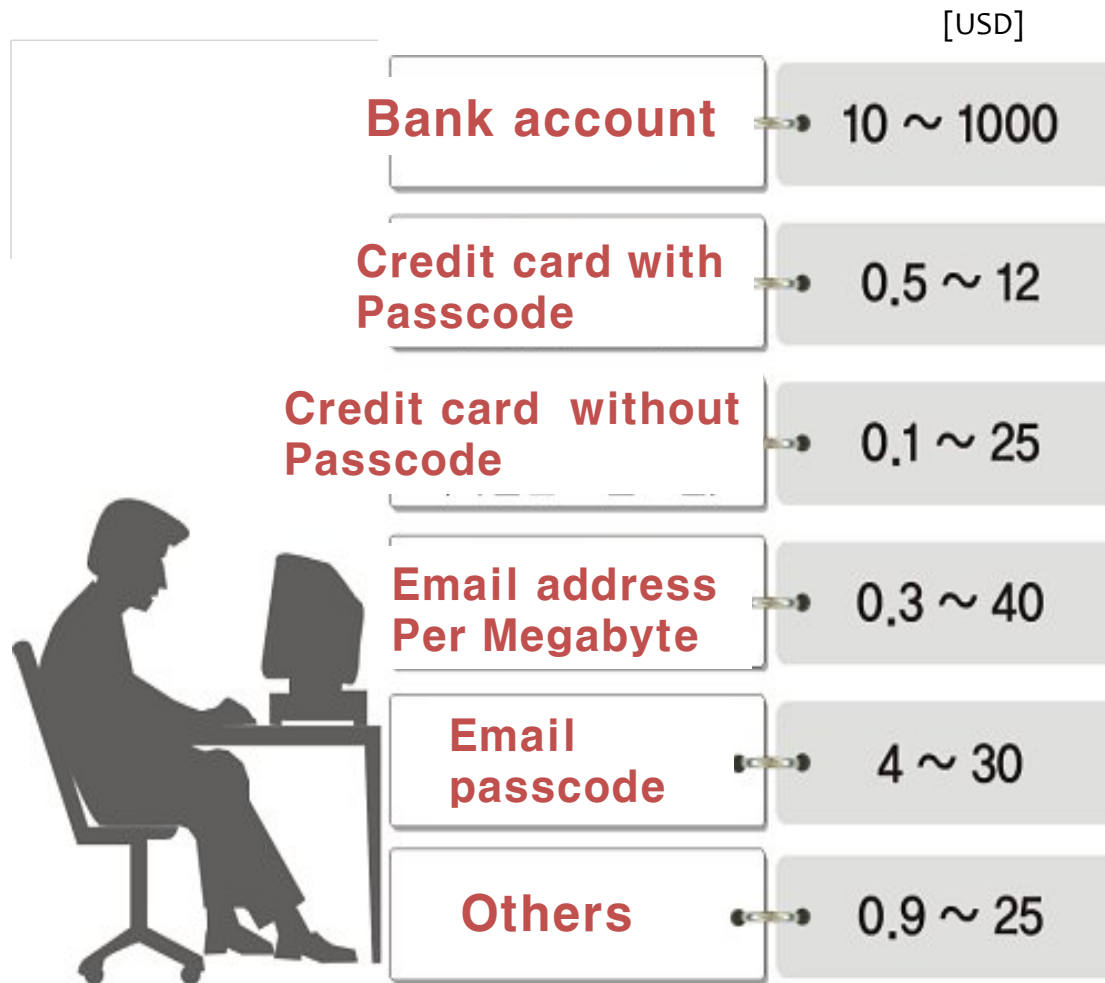
□ Price of credit card data (as of Oct. 2015)

[USD]

Categories*	US	UK	Canada	Australia	EU
Basic Card Information	5~8	20~25	20~25	21~25	25~30
+ Account Number	15	25	25	25	30
+ Date of Birth	15	30	30	30	35
Cumulative Card Data	30	35	40	40	45

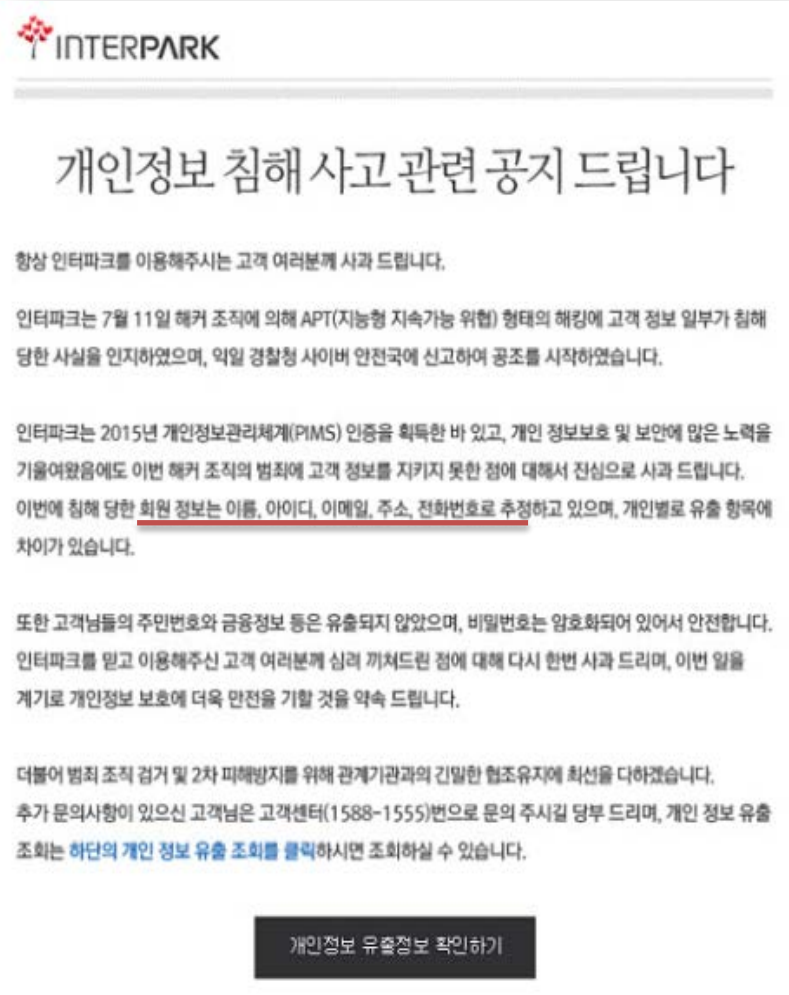
* InfoSec Megafee Research Center

Market Rates for Unlawfully Attained Personal Data 1/2



자료: 이코노미스트

Recent Data Breach Case - 1. Interpark



INTERPARK

개인정보 침해 사고 관련 공지 드립니다

항상 인터파크를 이용해주시는 고객 여러분께 사과 드립니다.

인터파크는 7월 11일 해커 조직에 의해 APT(지능형 지속가능 위협) 형태의 해킹에 고객 정보 일부가 침해 당한 사실을 인지하였으며, 익일 경찰청 사이버 안전국에 신고하여 공조를 시작하였습니다.

인터파크는 2015년 개인정보관리체계(PIMS) 인증을 획득한 바 있고, 개인 정보보호 및 보안에 많은 노력을 기울여왔음에도 이번 해커 조직의 범칙에 고객 정보를 지키지 못한 점에 대해서 진심으로 사과 드립니다. 이번에 침해 당한 회원 정보는 이름, 아이디, 이메일, 주소, 전화번호로 추정하고 있으며, 개인별로 유출 항목에 차이가 있습니다.

또한 고객님들의 주민번호와 금융정보 등은 유출되지 않았으며, 비밀번호는 암호화되어 있어서 안전합니다. 인터파크를 믿고 이용해주신 고객 여러분께 심려 끼쳐드린 점에 대해 다시 한번 사과 드리며, 이번 일을 계기로 개인정보 보호에 더욱 만전을 기할 것을 약속 드립니다.

더불어 범칙 조직 검거 및 2차 피해방지를 위해 관계기관과의 긴밀한 협조유지에 최선을 다하겠습니다. 추가 문의사항이 있으신 고객님은 고객센터(1588-1555)번호로 문의 주시길 당부 드리며, 개인 정보 유출 조치는 하단의 개인 정보 유출 조회를 클릭하시면 조회하실 수 있습니다.

[개인정보 유출정보 확인하기](#)

26,658,753

※ Active User, Past Users, Dormant Users

Data Breach Details

User Categories		Data Types	No.
Active Users	Interpark	ID, encrypted passwords, name, sex, DOB, telephone numbers, email, addresses	10,947,544
	Partners	ID	2,454,348
Past Users		ID	1,734,816
Dormant Users		ID, encrypted passwords	11,522,045
Total			26,658,753

Recent Data Breach Case- - 2. Yahoo

Expected Damages from Data Breach



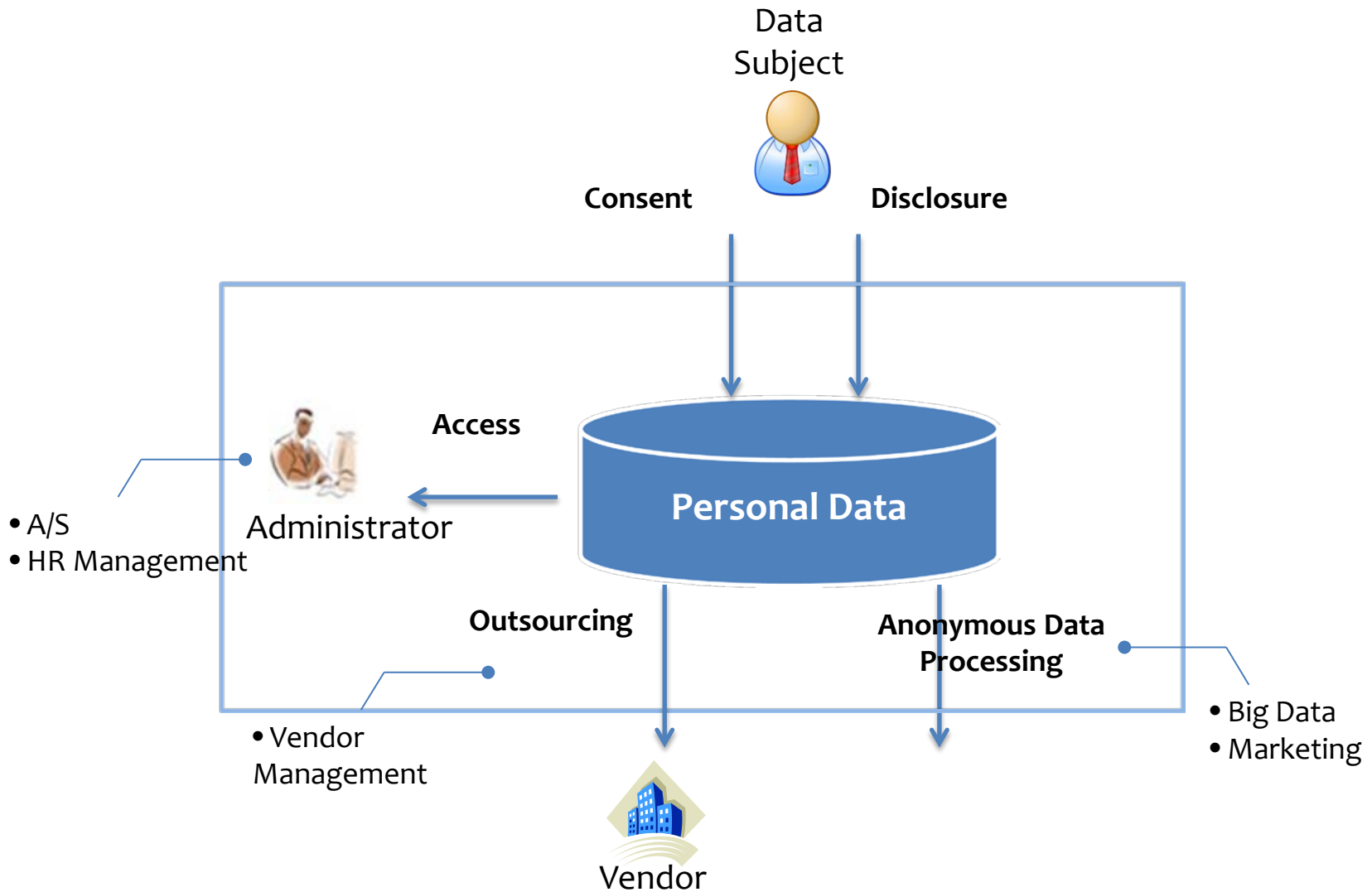
An Important Message About Yahoo User Security

By Bob Lord, CISO

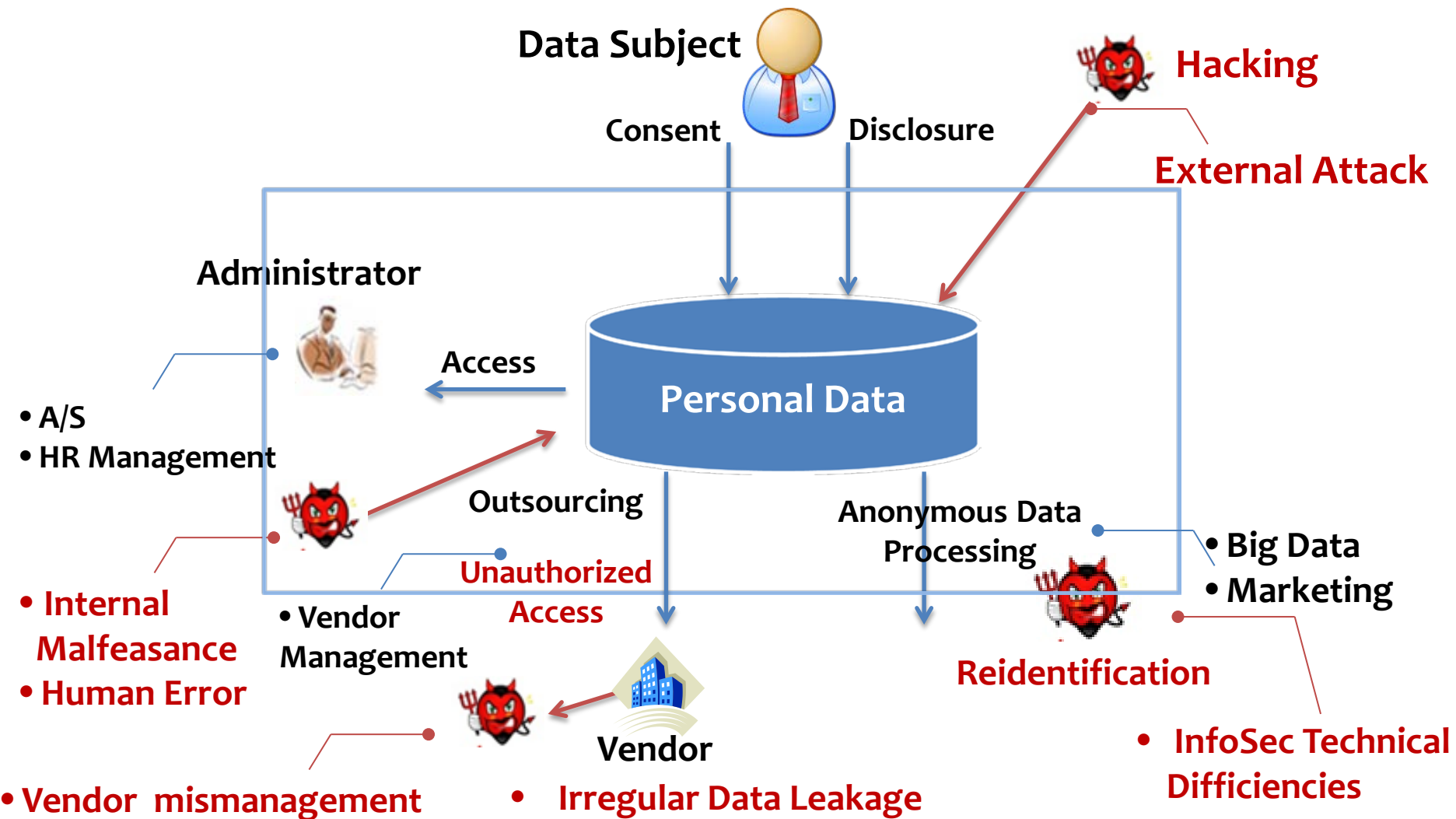
A recent investigation by Yahoo has confirmed that a copy of certain user account information was stolen from the company's network in late 2014 by what it believes is a state-sponsored actor. **The account information may have included names, email addresses, telephone numbers, dates of birth, hashed passwords (the vast majority with bcrypt) and, in some cases, encrypted or unencrypted security questions and answers.** The ongoing investigation suggests that stolen information did not include unprotected passwords, payment card data, or bank account information; payment card data and bank account information are not stored in the system that the investigation has found to be affected. Based on the ongoing investigation, Yahoo believes that information associated with at least 500 million user accounts was stolen and the investigation has found no evidence that the state-sponsored actor is currently in Yahoo's network. Yahoo is working closely with law enforcement on this matter.



Data Breach Scenario



Data Breach Scenario



Lessons Learned



Measures to secure personal data

개인정보보호법

제29조(안전조치의무) 개인정보처리자는 개인정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 안전성 확보에 필요한 기술적·관리적 및 물리적 안전조치에 관한 **최소한의 기준**을 정하는 것을 목적으로 한다.

개인정보보호법 시행령

제30조(개인정보의 안전성 확보조치) ① 개인정보처리자는 법 제29조에 따라 다음 각 호의 안전성 확보 조치를 하여야 한다.

- 개인정보의 안전한 처리를 위한 **내부 관리계획의 수립·시행**
- 개인정보에 대한 **접근 통제 및 접근 권한의 관리** 조치
- 개인정보를 안전하게 저장·전송할 수 있는 **암호화** 기술의 적용 또는 이에 상응하는 조치
- 개인정보 침해사고 발생에 대응하기 위한 **접속기록의 보관** 및 위조·변조 방지를 위한 조치
- 개인정보에 대한 **보안프로그램**의 설치 및 갱신
- 개인정보의 안전한 보관을 위한 보관시설의 마련 또는 잠금장치의 설치 등 **물리적 조치**
- 개인정보처리자가 **개인정보 파기 시 조치**

③ 제1항에 따른 안전성 확보조치에 관한 세부 기준은 행정자치부장관이 정하여 고시한다.

▶ **개인정보의 안전성 확보조치 기준 (행정자치부 고시 제2016-35호) 2016년 9월 1일 개정 고시 및 시행**

구분	주요내용
(제 3조) 안전조치 기준 적용 (신설)	<ul style="list-style-type: none"> 개인정보 처리자 유형 및 개인정보 보유량에 따른 안전조치 기준 차등 적용
(제 4조) 내부관리계획 수립·시행	<ul style="list-style-type: none"> 보호책임자 지정 및 역할과 책임, 유출사고 대응계획(신설), 재해재난 대비(신설) 등 연 1회 이상 내부 관리계획 이행실태 점검 (신설)
(제 5조) 접근 권한의 관리	<ul style="list-style-type: none"> 업무수행에 필요한 최소한의 범위로 차등 부여, 취급자별 계정 발급 권한 부여기록은 최소 3년 보관, ID/비밀번호 일정횟수 잘못 입력시 접근제한 (신설)
(제 6조) 접근통제	<ul style="list-style-type: none"> 방화벽 등 접근통제시스템 설치·운영, 외부 접속시 안전한 접속 및 인증 수단 적용 고유식별정보 수집 홈페이지 취약점 점검 1회/년 이상 일정시간 업무처리하지 않을시 자동 시스템 접속 차단(신설)
(제 7조) 개인정보의 암호화	<ul style="list-style-type: none"> 암호화 대상 : 고유식별정보, 비밀번호, 바이오정보 전송시 및 저장시 암호화 (비밀번호는 저장시 일방향 암호화) 안전한 암호화 키 생성, 이용, 보관, 배포 및 파기 (신설)
(제 8조) 접속기록의 보관 및 점검	<ul style="list-style-type: none"> 최소 6개월 이상 보관, 반기별 1회 이상 점검
(제 9조) 악성프로그램 등 방지	<ul style="list-style-type: none"> 백신 등 보안프로그램 설치, 자동 또는 일 1회 이상 최신 업데이트
(제10조) 관리용 단말기 안전조치 (신설)	<ul style="list-style-type: none"> 인가받지 않은 사람의 관리용 단말기 임의 조작 방지, 악성프로그램 감염 방지
(제 11조) 물리적 안전조치	<ul style="list-style-type: none"> 물리적 보관장소 출입통제, 보조저장매체 반·출입 통제 절차 등
(제 12조) 재해재난 대비 안전조치(신설)	<ul style="list-style-type: none"> 재해재난 발생시 대응절차의 마련 및 정기점검 실시
(제 13조) 개인정보의 파기	<ul style="list-style-type: none"> 개인정보 완전파기 및 부분파기

미조치에 따른 유출 시

2년 이하 징역 또는 2천만원 이하 벌금

보호조치 미비

3천만원 이하 과태료

Thank you

A stylized white line-art illustration of a city skyline with various skyscrapers and buildings, positioned behind the word 'Thank you'.

SVP, Sang-joo LEE

SAMSUNG

The Samsung logo, consisting of the word 'SAMSUNG' in a white oval with radiating lines, positioned in the bottom right corner.