



# Security, Privacy, Resiliency – “Are We Ready?”

Paul White  
Oracle Security Consultant

**ORACLE**

Copyright © 2016 Oracle and/or its affiliates. All rights reserved. |

Web Services  
Content Sharing

The internet of things (IoT)

Cloud  
Computing

Online  
Services

Exponential  
Growth of Data

Transformation

# MOST SIGNIFICANT IT Security Challenges IN 20 YEARS

Regulations &  
Compliance

Mobile  
Users

Mobile  
Devices

External  
Threats

# Security Challenges

# Government Data is Under Attack

The Washington Post

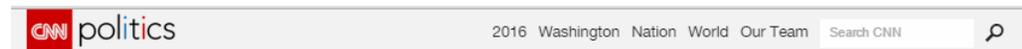
June 4, 2015

## Chinese breach data of four million federal workers

Hackers working for the Chinese state breached the computer system of the Office of Personnel Management in December, U.S. officials said Thursday, and the agency will notify about 4 million current and former federal employees that their personal data may have been compromised.

The hack was the largest breach of federal employee data in recent years. It was the second major intrusion of the same agency by China in less than a year...

ORACLE



## First on CNN: U.S. data hack may be 4 times larger than the government originally said

By [Evan Perez](#) and [Shimon Prokupecz](#), CNN  
Updated 10:59 PM ET, Tue June 23, 2015



Source: CNN  
U.S.: Hack of 18 million Americans came from China 01:13



# Data Breach: Office of Personal Management

- In June 2015, OPM announced that it had been the target of a data breach targeting the records of as many as four million people.
- Information targeted included SSNs, names, dates and places of birth, and addresses.
- Also likely involved the theft of detailed security-clearance-related background information.
- And even 5 million fingerprints.
- On July 9, 2015, the estimate of the number of stolen records was increased to 21.5 million.

## OPM says 5.6 million fingerprints stolen in cyberattack, five times as many as previously thought

“In the case of the OPM breaches, it turned out that a contractor’s compromised credentials were the key that provided attackers access to sensitive employee data held by the agency. In fact, the vast majority of government breaches we hear about involve the use of authentic user credentials. Because attackers are “trusted” once they are inside, they begin to create back doors to ensure they can get back in, should they so desire to do so”

## OPM Hack: Government Finally Starts Notifying 21.5 Million Victims

# Joint Chiefs of Staff Email Hack – August 2015



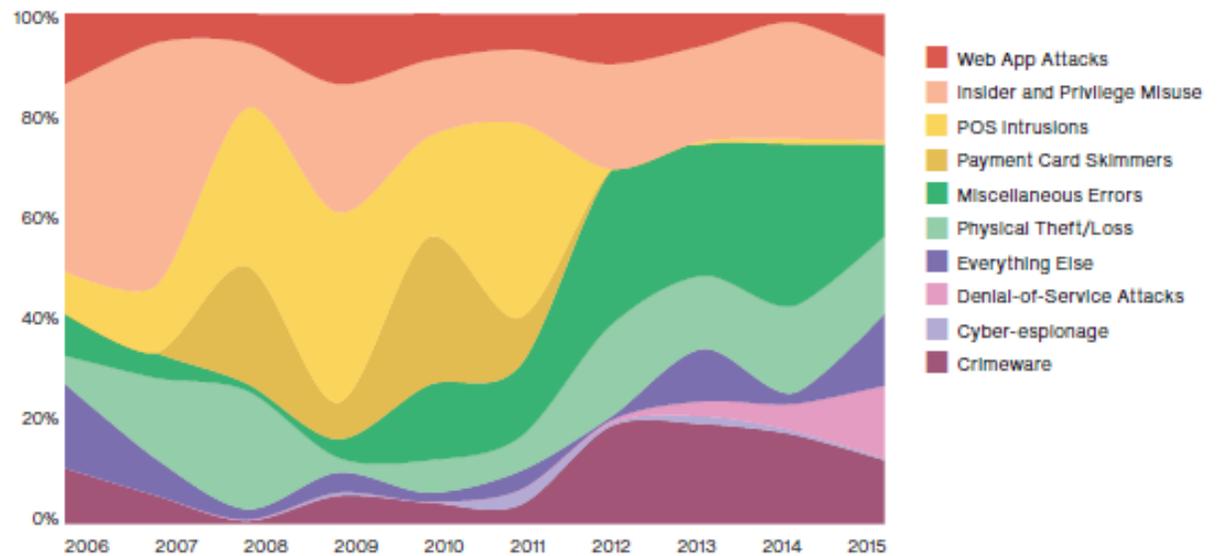
# Over 700 Million Records Breached in 2015

81%

Attackers are able to compromise an organization within minutes

69%

More than two-thirds of incidents that comprise the Cyber-Espionage pattern have featured phishing

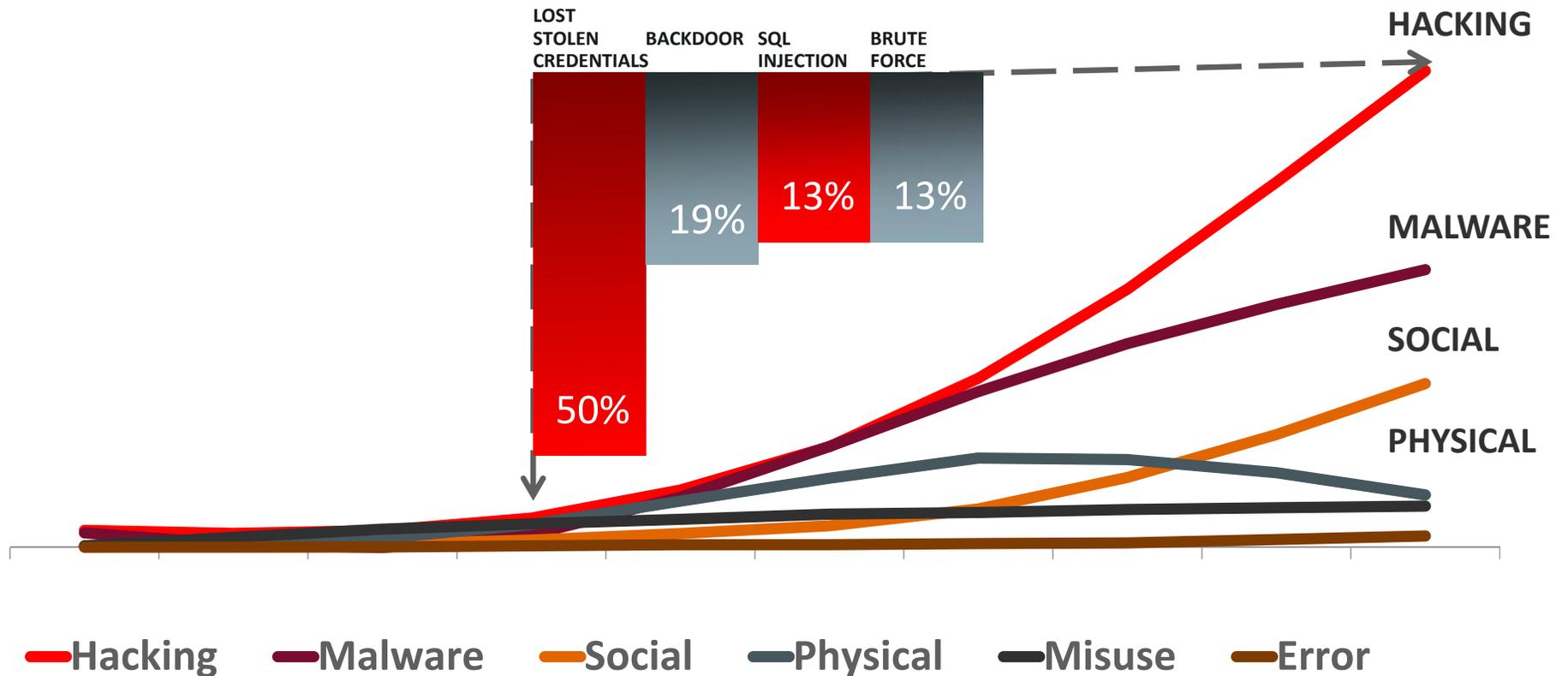


Frequency of incident classification patterns over time across security incidents



# SQL INJECTION & CREDENTIALS

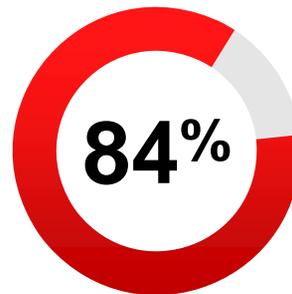
ARE IN THE TOP 3 INCIDENTS FOR HACKING



# SECURITY REQUIRES IDENTITY



Attacks target  
weak passwords



Target  
user interaction



Exploit stolen  
credentials

## MOST FREQUENT ATTACK VECTOR & POINT OF CONTROL

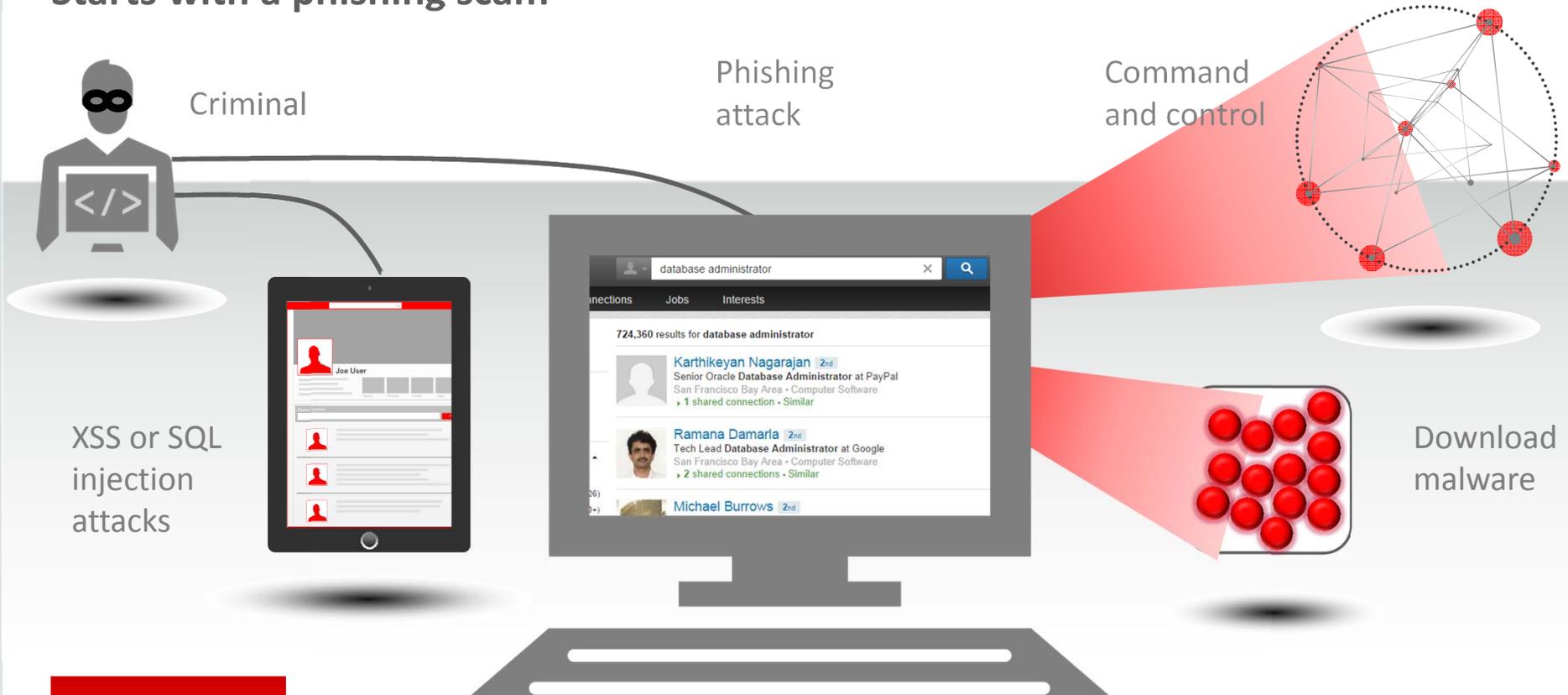
Source: 2013 Verizon Data Breach  
Investigations Report

Source: 2013 Verizon Data Breach  
Investigations Report

Source: 2013 Verizon Data Breach  
Investigations Report

# Anatomy of a Data Breach

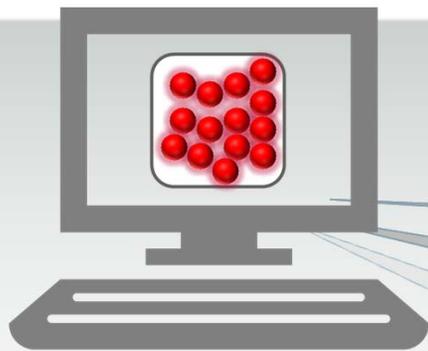
## Starts with a phishing scam



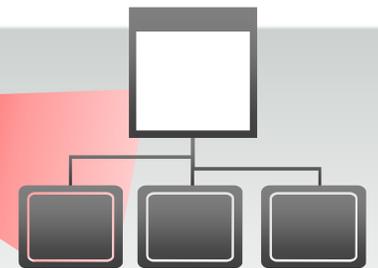
# Anatomy of a Data Breach

## Establish a foothold

Establish multiple  
backdoors

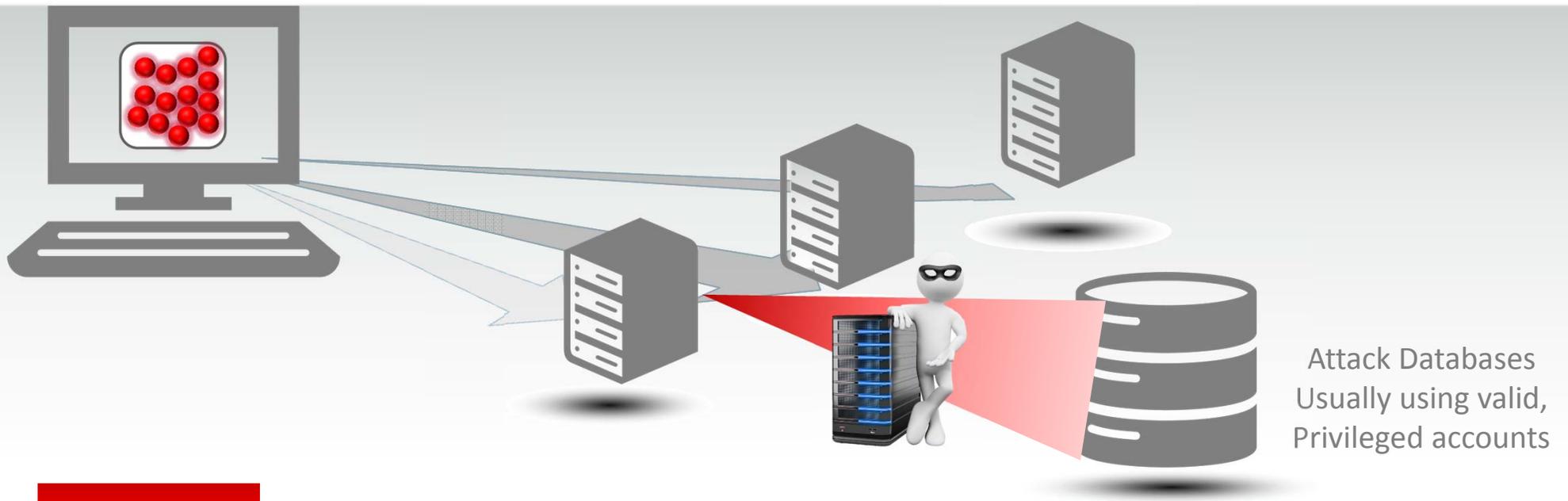


Dump passwords  
Domain controller



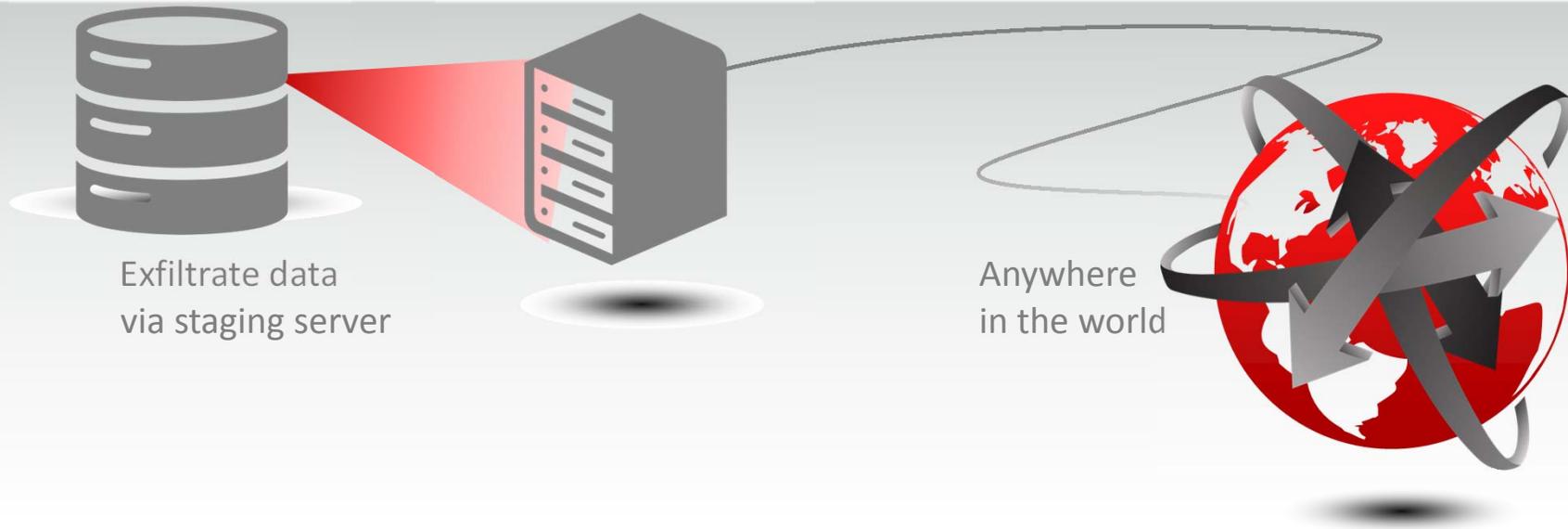
# Anatomy of a Data Breach

## Identify targets, probe for weaknesses



# Anatomy of a Data Breach

Exfiltrate data and cover tracks



# Prevention Is Futile in 2020: Protect Information Via Pervasive Monitoring and Collective Intelligence



🕒 30 May 2013 📄 G00252476

Analyst(s): [Neil MacDonald](#)

Free preview of Gartner research

## Summary

Advanced targeted attacks make prevention-centric strategies obsolete. Securing enterprises in 2020 will require a shift to information- and people-centric security strategies, combined with pervasive internal monitoring and sharing of security intelligence.

## Overview

### Key Challenges

Information security can no longer prevent advanced targeted attacks.

### Not a Gartner Client?

Want more research like this? Learn the benefits of becoming a Gartner client.

[CONTACT US ONLINE](#)

### RESEARCH [MORE](#)

🕒 30 January 2015  
**100 Information and Analytics Predictions Through 2020**  
Information and analytics are a priority across many IT and business...

🕒 5 January 2015  
**Agenda Overview for Security and Risk Management Leaders, 2015**  
Leaders must mind the gap between risk management necessities and business...

# Take Away - Assume Breach!

“Assuming the breach” has been a point of contention within the IT and cloud security community, with some seeing it as a defeatist attitude, but that's a misconception. It's really about shift the focus from a one-side purely preventative strategy to include more emphasis on breach detection, incident response, and effective recovery when a breach does (almost Inevitably) occur.”

*David Cross, Microsoft Azure Security GM*

# Privacy Challenges



# European Union Safe Harbor

- US-EU Safe Harbor was a process for US companies to voluntarily comply with the EU Directive 95/46/EC
- Protection of individuals with regard to the processing of personal data and on the free movement of such data
- Data can only be transferred to countries with an “adequate level of protection” of personal data

# Max Schrems vs Irish Data Protection Commissioner

- Max Schrems, an Austrian citizen, was a user of Facebook
- Claimed his privacy was violated when data from Facebook subsidiary in Ireland was transferred to Facebook server in the US
- Schrems was concerned in light of the 2013 Snowden release of NSA surveillance data that no real protection was provided by data transferred to the US
- Irish lower courts refused to rule on the matter
- Appealed to High Court of Ireland, who sought the European Court of Justice (ECJ) opinion

# ECJ Decision

- “...the law and practice of the United States allow the large-scale collection of the personal data of citizens of the Union which is transferred under the safe harbour scheme, without those citizens benefiting from effective judicial protection.”
- “...access enjoyed by the United States intelligence services to the transferred data therefore also constitutes an interference with the fundamental right to protection of personal data guaranteed in Article 8 of the Charter.”

[Teachprivacy.org](http://Teachprivacy.org)

# EU – US Privacy Shield

**Strong obligations on companies handling Europeans' personal data and robust enforcement:**

- U.S. companies wishing to import personal data from Europe will **need to commit to robust obligations on how personal data is processed and individual rights are guaranteed**. The Department of Commerce will monitor that companies publish their commitments, which makes them **enforceable under U.S. law by the US. Federal Trade Commission**. In addition, any company handling human resources data from Europe has to commit to comply with decisions by European DPAs.

[http://europa.eu/rapid/press-release\\_IP-16-216\\_en.htm](http://europa.eu/rapid/press-release_IP-16-216_en.htm)

# EU – US Privacy Shield

## Clear safeguards and transparency obligations on U.S. government access:

- For the first time, the US has given the EU written **assurances that the access of public authorities for law enforcement and national security will be subject to clear limitations, safeguards and oversight mechanisms.** These exceptions must be used only to the extent necessary and proportionate. **The U.S. has ruled out indiscriminate mass surveillance on the personal data transferred to the US under the new arrangement.** To regularly monitor the functioning of the arrangement **there will be an annual joint review**, which will also include the issue of national security access. The European Commission and the U.S. Department of Commerce will conduct the review and invite national intelligence experts from the U.S. and European Data Protection Authorities to it.

[http://europa.eu/rapid/press-release IP-16-216 en.htm](http://europa.eu/rapid/press-release_IP-16-216_en.htm)

# EU – US Privacy Shield

## Effective protection of EU citizens' rights with several redress possibilities:

- Any **citizen who considers that their data has been misused** under the new arrangement will have several redress possibilities. **Companies have deadlines to reply to complaints.** European DPAs can refer complaints to the Department of Commerce and the Federal Trade Commission. In addition, Alternative Dispute resolution will be free of charge. For complaints on possible access by national intelligence authorities, a new Ombudsperson will be created.

[http://europa.eu/rapid/press-release IP-16-216 en.htm](http://europa.eu/rapid/press-release_IP-16-216_en.htm)

# Take Away – Privacy is the great unknown!

- Important to security professionals, because of the technical connection to security controls, privacy usually ends up on their plate
- Because of the Schrems case, the privacy goal posts will be moving to the right for US companies
- While that is not public-sector relevant on it's face, Congress has given assurances that SEC, FCC, FTC & Commerce will provide privacy guidelines & controls. As in the past (breach notification, Chip & PIN, Cybersecurity Framework) the government will 1) promulgate those standards/controls through NIST & 2) be the first industry to mandate “eating their own dog food.”

# Resiliency Challenges

PadCrypt 2.0 (Not Responding)

## Your files and documents have been encrypted!



**Price will multiply on**  
01/01/1970

**Time Left**  
00 : 00 : 00 : 00

[Live Chat](#)  
[Decrypt Help](#)  
[Encrypted Files](#)

### What happened to my files?

Your photos, documents, and videos on this computer have been encrypted with AES-256. To get your files back you will need to purchase your encryption key within the set date, failing to pay will result in the destruction of your key.

### How do I obtain my key?

The key produced for your computer is stored on our server. To obtain the unique key for your computer, which will decrypt and recover your encrypted files, you will need to pay a fee in Bitcoin/UKash/PSC prior to the key destroy date. After that your key will be destroyed and nobody will ever be able to recover your files.

### Payment Method

Bitcoin (Cheapest Option) 0.8 BTC

Next

# What is Ransomware?

“Ransomware is a type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files unless a ransom is paid. More modern ransomware families, collectively categorized as crypto-ransomware, encrypt certain file types on infected systems and forces users to pay the ransom through certain online payment methods to get a decrypt key.”

<http://www.trendmicro.com/vinfo/us/security/definition/ransomware>

A recent U.S. Government interagency report indicates that, on average, there have been 4,000 daily ransomware attacks since early 2016 (a 300% increase over the 1,000 daily ransomware attacks reported in 2015).

*United States Government Interagency Guidance Document, How to Protect Your Networks from Ransomware available at <https://www.justice.gov/criminal-ccips/file/872771/download>.*

The US Department of Health and Human Services recently released a fact sheet titled:  
**FACT SHEET: Ransomware and HIPAA**

# Is Ransomware a Security Incident?

“The presence of ransomware (or any malware) on a covered entity’s or business associate’s computer systems is a security incident under the HIPAA Security Rule. A security incident is defined as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. See the definition of security incident at 45 C.F.R. 164.304. **Once the ransomware is detected, the covered entity or business associate must initiate its security incident and response and reporting procedures.** See 45 C.F.R. 164.308(a)(6).”

<http://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf>

# Is Ransomware a HIPAA data breach?

- HIPAA defines a breach as:

“...the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI.”

*See 45 C.F.R. 164.402*

# Is Ransomware a HIPPA data breach?

When electronic protected health information (ePHI) is encrypted as the result of a ransomware attack, a breach has occurred because the ePHI encrypted by the ransomware was acquired (i.e., unauthorized individuals have taken possession or control of the information), and thus is a **“disclosure”** not permitted under the HIPAA Privacy Rule.

*<http://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf>*

# Is Ransomware a HIPPA data breach?

Unless the covered entity or business associate can **demonstrate that there is a “...low probability that the PHI has been compromised,”** based on the factors set forth in the Breach Notification Rule, **a breach of PHI is presumed to have occurred.** The entity must then comply with the **applicable breach notification provisions, including notification to affected individuals without unreasonable delay, to the Secretary of HHS, and to the media** (for breaches affecting over 500 individuals) in accordance with HIPAA breach notification requirements. See 45 C.F.R. 164.400-414.

*<http://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf>*

# Four Factors to determine “low probability”

A risk assessment considering at least the following four factors (see 45 C.F.R. 164.402(2)):

- The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification
- The unauthorized person who used the PHI or to whom the disclosure was made
- Whether the PHI was actually acquired or viewed
- The extent to which the risk to the PHI has been mitigated

<http://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf>

## Take Away – Resilience is a core competency given the breadth of threats to the enterprise

- Overall assumption that the Cyber discipline **MUST** assume incidents **WILL** happen and have contingency/recovery plans in place and test them, are now required
- The inclusion of Cyber activities & outcomes in NIST guidance that focus on (even at the highest level of guidance) “Respond” & “Recover” practices, punctuates this need
- This is not so much an indictment of threat intelligence, a worthy consideration in security planning, but a **wholesale increase in the likelihood that valuable assets will be compromised** by “dumb tools” through lateral infection, sheer number of automated attacks or because “**important but not critical**” assets hadn’t made it to the top of the threat intelligence pyramid yet

# Questions

