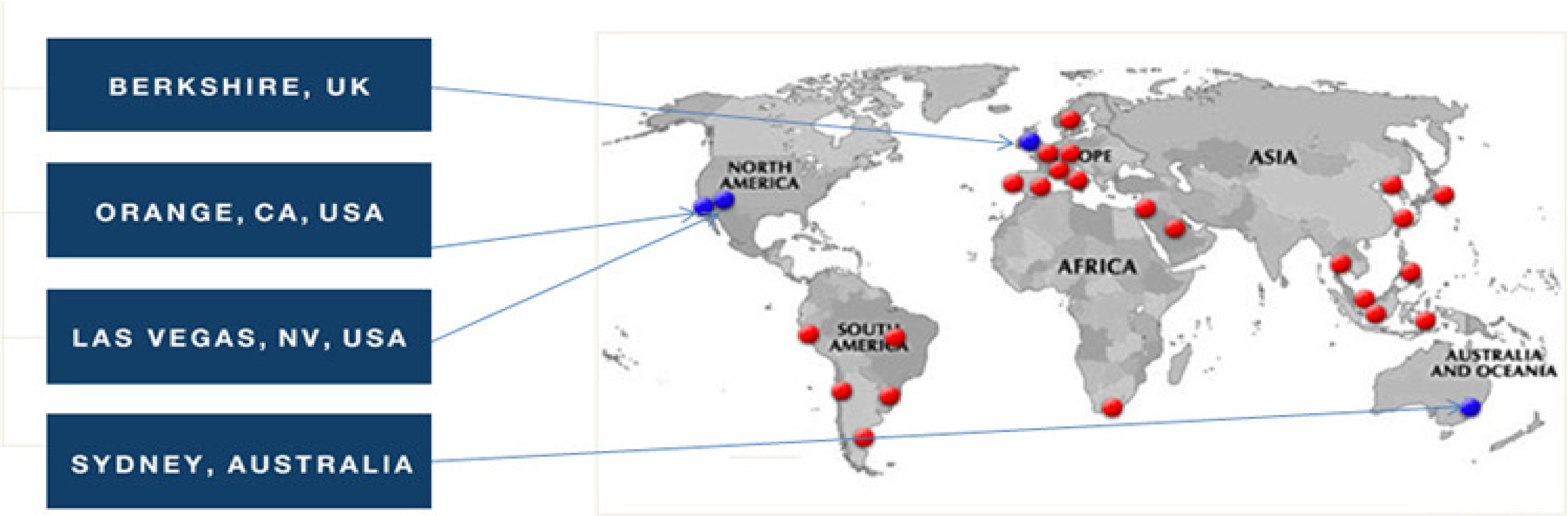
VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

Multi Factor Authentication – Security Beyond Usernames and Passwords

Brian Marshall
Vanguard Integrity Professionals
go2vanguard.com

About Vanguard

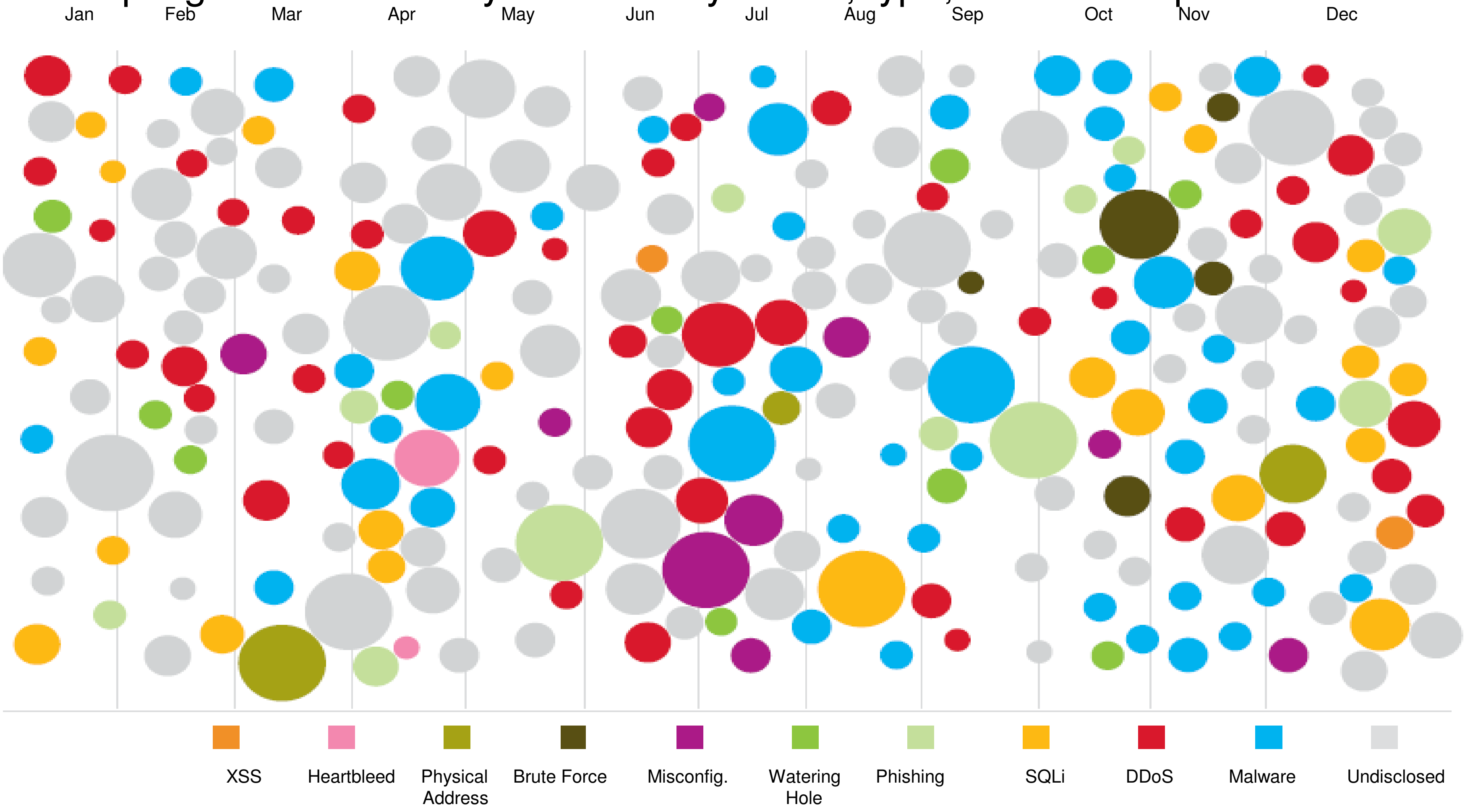
Founded:	**1986**
Business:	**Cybersecurity Experts for Large Enterprises** **Software, Professional Services, and Training**
Customers:	**1,000+ Worldwide**



Over 20 distributors/resellers serving 50+ countries worldwide

ATTACK STATISTICS

Sampling of 2014 security incidents by attack, type, time and impact



Source: IBM X-Force Threat Intelligence Quarterly, 1Q 2015

Data Breaches

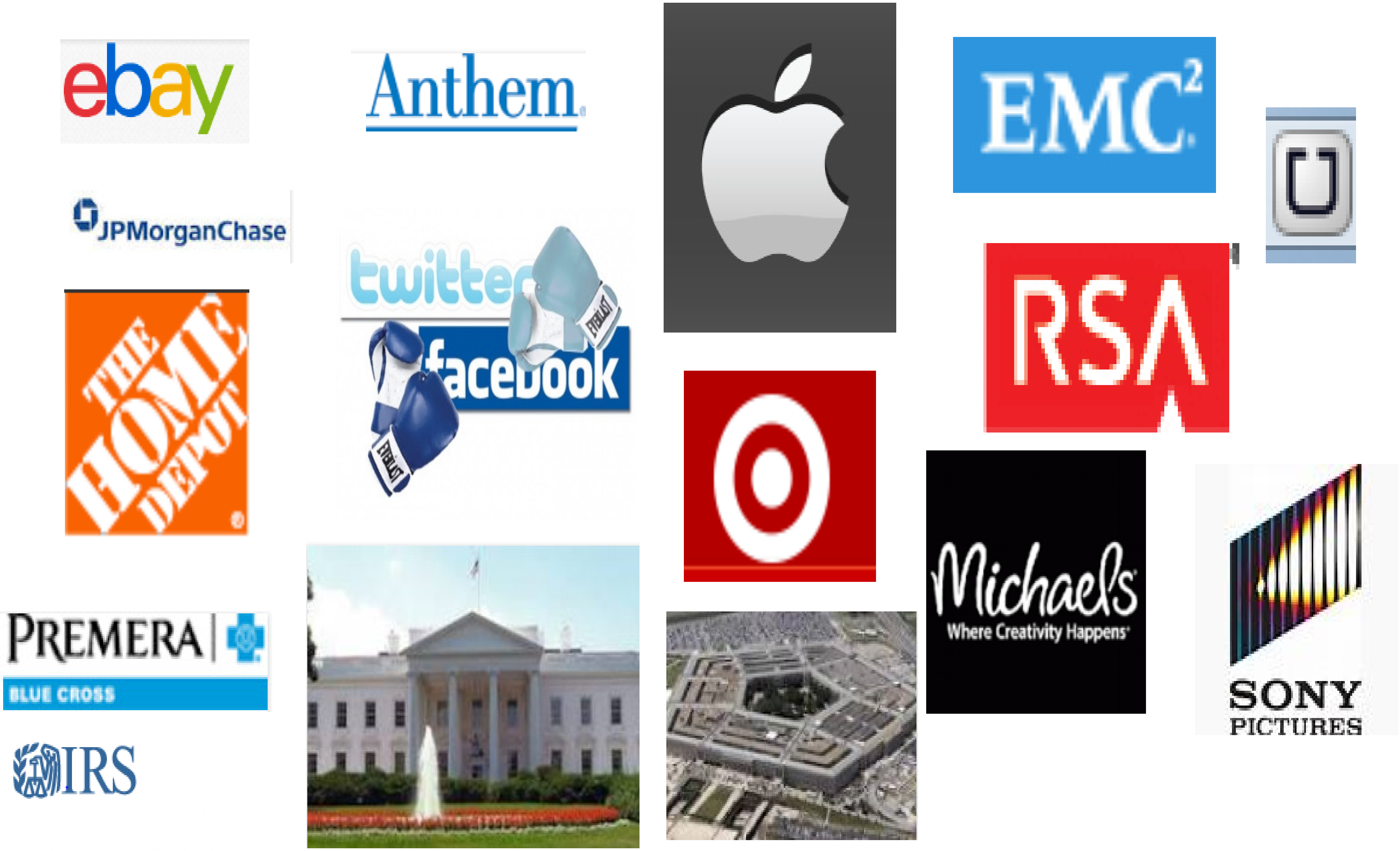
- Number of breaches and outside attacks increasing

- Continuing problem of insider - malicious or by accident

Tax Season Kicks Off with Scams
Haiti, World Cup Used to Trick
Criminals Infect Flash Drives
Cyber Crime:
Olympic Winter Games Attract Fraud
Online Crooks Romance Users with Valentine's Scams
Identity Thiefs Steal
Fake Security Software
Lured to Malicious Web Pages
Phishing Attacks Hit Twitter

Top Recent Breaches

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS



My Grandchildren

The Mainframe

ComputerWeekly.com

Mainframe at 50: Why the mainframe keeps on going

For the past 50 years, the mainframe has been the technological workhorse enab

In fact, 80% of the world's corporate data is still managed by mainframes.

" 80% of the world’s corporate data is still managed by mainframes."

In a video interview with Computer Weekly's Cliff Saran, IBM Hursley lab director
in computing paradigms and application systems, such as the move to the web and mobile technology.

"The platform is continually reinventing itself to remain relevant for cloud and mobile computing and to be able to run the most popular application server packages," he said.
Yet while it appears to be middle-aged technology, in terms of reach it seems the mainframe touches almost everything in modern life, according to Lamb.

“If you are using a mobile application today that runs a trans
another, there is a four in five chance that there is a mainfra

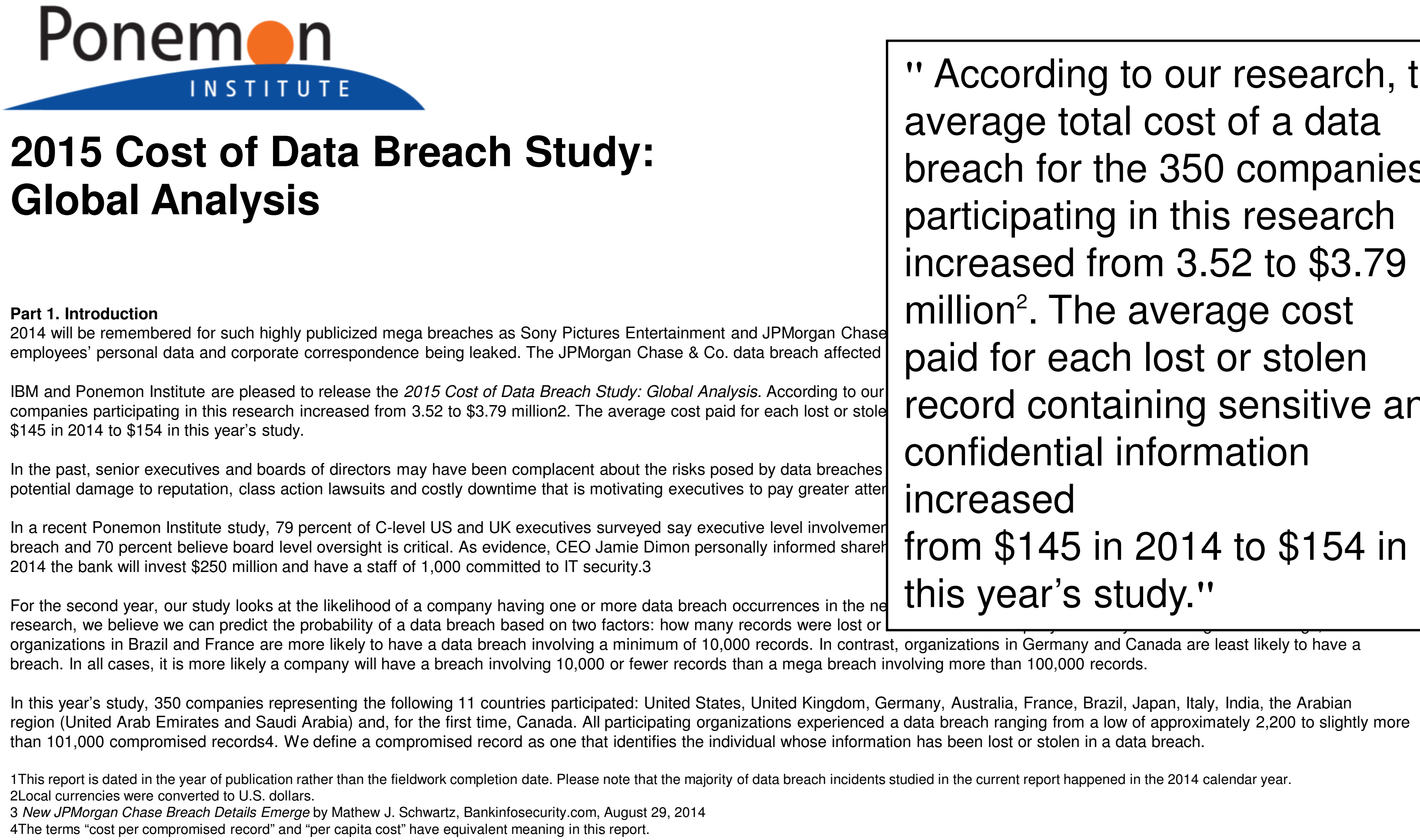
And the amount of processing run on the mainframe dwarfs
likes and 60,000 Google searches. But the CICs application
per second – that's 100 billion transactions a day," he said.

IBM will be formally celebrating the 50th anniversary of the S

"If you are using a mobile application today that runs a transaction to check your bank balance or transfer money from one account to another, there is a four in five chance that there is a mainframe behind that transaction."

Source: Computer Weekly; Interview with Rob Lamb, IBM Hursley lab director, March 24, 2014

Cost of a Data Breach



Ponemon INSTITUTE

2015 Cost of Data Breach Study: Global Analysis

Part 1. Introduction
2014 will be remembered for such highly publicized mega breaches as Sony Pictures Entertainment and JPMorgan Chase
employees' personal data and corporate correspondence being leaked. The JPMorgan Chase & Co. data breach affected

IBM and Ponemon Institute are pleased to release the *2015 Cost of Data Breach Study: Global Analysis.* According to our
companies participating in this research increased from 3.52 to $3.79 million2. The average cost paid for each lost or stole
$145 in 2014 to $154 in this year's study.

In the past, senior executives and boards of directors may have been complacent about the risks posed by data breaches
potential damage to reputation, class action lawsuits and costly downtime that is motivating executives to pay greater atter

In a recent Ponemon Institute study, 79 percent of C-level US and UK executives surveyed say executive level involvemer
breach and 70 percent believe board level oversight is critical. As evidence, CEO Jamie Dimon personally informed shareh
2014 the bank will invest $250 million and have a staff of 1,000 committed to IT security.3

For the second year, our study looks at the likelihood of a company having one or more data breach occurrences in the ne
research, we believe we can predict the probability of a data breach based on two factors: how many records were lost or
organizations in Brazil and France are more likely to have a data breach involving a minimum of 10,000 records. In contrast, organizations in Germany and Canada are least likely to have a breach. In all cases, it is more likely a company will have a breach involving 10,000 or fewer records than a mega breach involving more than 100,000 records.

In this year's study, 350 companies representing the following 11 countries participated: United States, United Kingdom, Germany, Australia, France, Brazil, Japan, Italy, India, the Arabian region (United Arab Emirates and Saudi Arabia) and, for the first time, Canada. All participating organizations experienced a data breach ranging from a low of approximately 2,200 to slightly more than 101,000 compromised records4. We define a compromised record as one that identifies the individual whose information has been lost or stolen in a data breach.

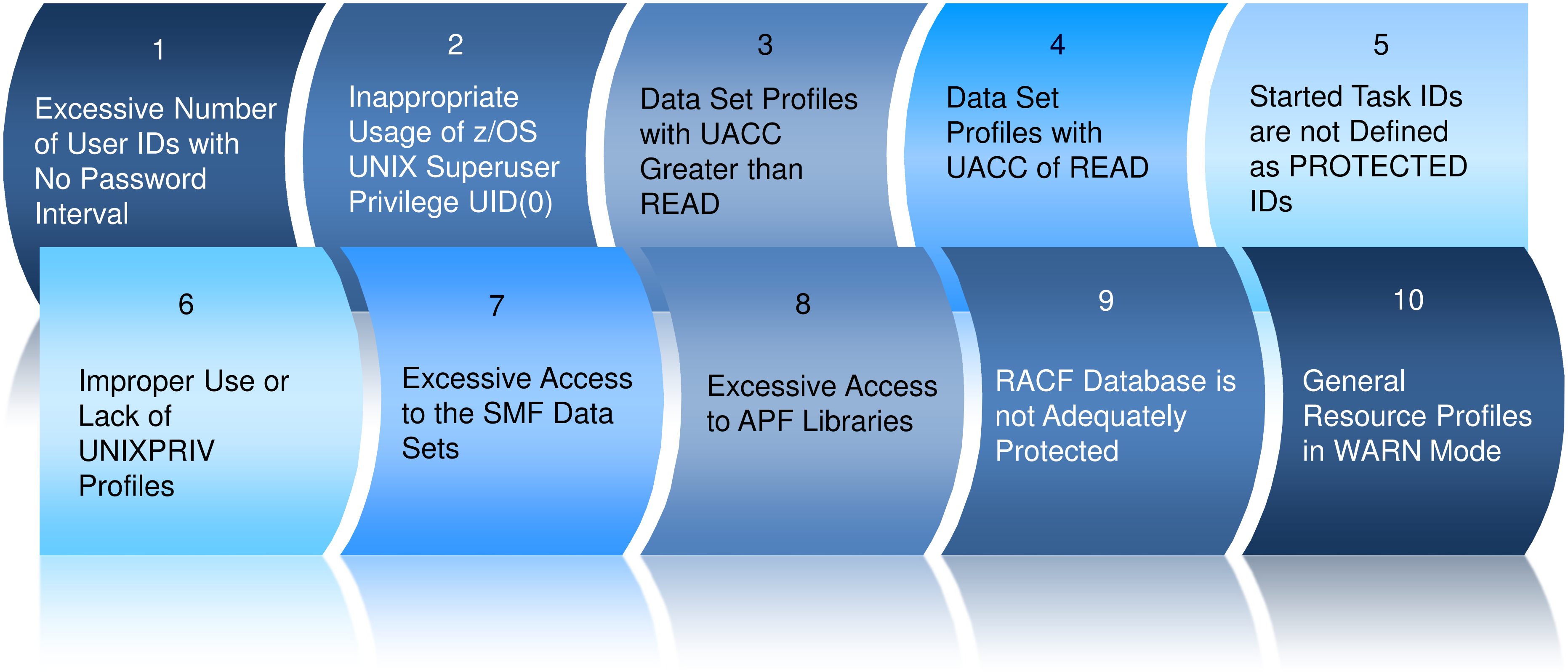
1This report is dated in the year of publication rather than the fieldwork completion date. Please note that the majority of data breach incidents studied in the current report happened in the 2014 calendar year.
2Local currencies were converted to U.S. dollars.
3 *New JPMorgan Chase Breach Details Emerge* by Mathew J. Schwartz, Bankinfosecurity.com, August 29, 2014
4The terms "cost per compromised record" and "per capita cost" have equivalent meaning in this report.

" According to our research, the average total cost of a data breach for the 350 companies participating in this research increased from 3.52 to $3.79 million[2]. The average cost paid for each lost or stolen record containing sensitive and confidential information increased
from $145 in 2014 to $154 in this year's study."

Source: Ponemon Institute® Research Report, May, 2015

Vulnerability Assessment Findings

Scope: Vanguard Top 10 z/OS Risks Identified in Client Security Assessments



1 Excessive Number of User IDs with No Password Interval

2 Inappropriate Usage of z/OS UNIX Superuser Privilege UID(0)

3 Data Set Profiles with UACC Greater than READ

4 Data Set Profiles with UACC of READ

5 Started Task IDs are not Defined as PROTECTED IDs

6 Improper Use or Lack of UNIXPRIV Profiles

7 Excessive Access to the SMF Data Sets

8 Excessive Access to APF Libraries

9 RACF Database is not Adequately Protected

10 General Resource Profiles in WARN Mode

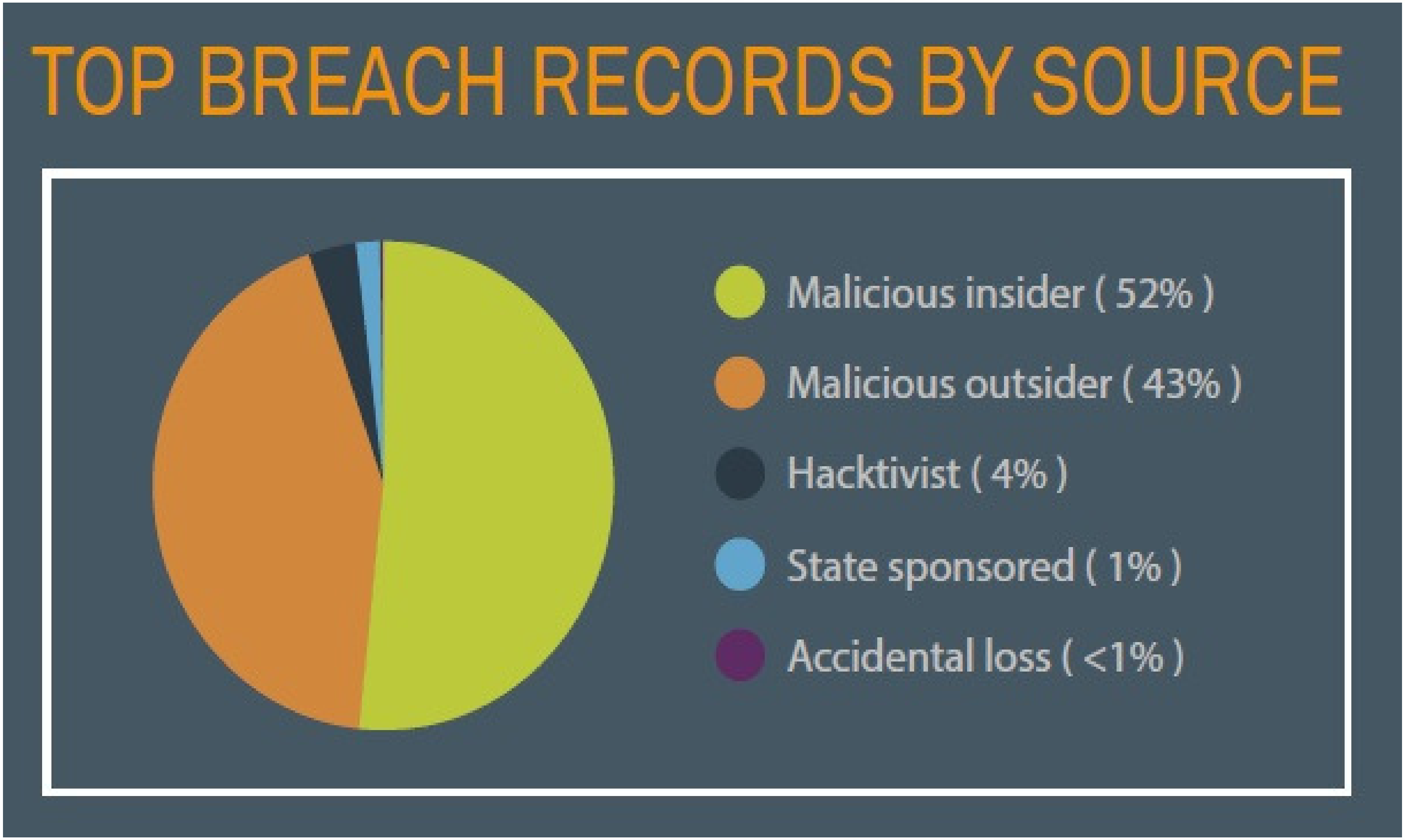
Note: Data collected from hundreds of security assessments performed by Vanguard Integrity Professionals.

Why Multi-Factor Authentication?

“Target was certified as meeting the standard for payment card industry (PCI DSS) in September 2013. Nonetheless, we suffered a data breach…”

now ex-chairman, ex-president, and ex-CEO of Target Corporation, Gregg Steinhafel (http://buswk.co/1lT9j0X)

Data Breaches



Data Breaches

Mandiant: 2014 Data Breach Report

100% of breaches examined included an exploitation of a user id and password that was compromised.

DATA BREACHES

Not My House

MULTI FACTOR AUTHENTICATION TYPES

- – Two-Factor Authentication
- – Two-Step Verification
- – Strong Authentication

MULTI FACTOR AUTHENTICATION

- **An Industry full of often confused terms**
  - Multi-Factor Authentication is a method of requiring factors from the following three categories;
    - Knowledge Factors
    - Possession Factors
    - Inherence Factors

MULTI FACTOR AUTHENTICATION

Knowledge Factors

- Password
- PIN Number
- Mothers Maiden Name
- Favorite Potato Chip

MULTI FACTOR AUTHENTICATION

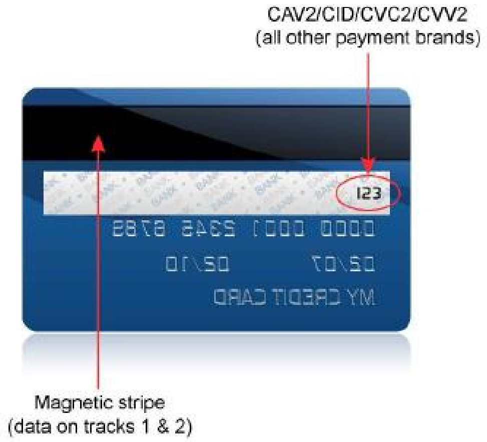
Possession Factors

- Disconnected (RSA, ActivID, etc)
  - – Sequence-Based Tokens – Singular button, multiple depresses
  - – Time-Based Tokens – Change Every ‘x’ Seconds typically
  - – Challenge-Based Tokens – Small keypad to enter challenge code
  - – HOTP - HMAC-Based One-Time Password Algorithm (RFC 4226)
  - – TOTP – Time-based One-time Password Algorithm (RFC 6238)

MULTI FACTOR AUTHENTICATION

Possession Factors

- *Connected*
  - Magnetic Strip – ATM Card, etc
  - Contacts – SmartCard, EMV Credit Cards,
  - USB Keys, RSA SecureID800
  - Wireless – RFID, Bluetooth, Proximity
  - Other – Audio Port, iButtons, etc



MULTI FACTOR AUTHENTICATION

Mobile Phones

- Soft Token
- SMS one-time password

Get the **multi-factor authentication** you need to protect against today's threats without the hassle and cost of yesterday's technology.

- Easy to set up, manage, and use
- Out-of-band and OATH methods
- Adds a critical second layer of security
- Cost-effective to deploy and support

MULTI FACTOR AUTHENTICATION

Inherence Factors

- Fingerprint
- Hand Topography
- Eye (Iris)

Exposure Issues

- – Phishing/Man-In-The-Middle
- – Malware
- – Session Hijacking
- – Lost/Stolen
- – Over the shoulder
- – Sniffers

MULTI FACTOR AUTHENTICATION

US based Regulation and Guidance

- NIST FIPS 201/HSPD-12
- HIPPA
- NERC CIP
- NIST SP 800-63-2
- PCI DSS
- FFIEC
- SOX

MULTI FACTOR AUTHENTICATION FOR Z

Come see a Presentation on our products

In Washington 4 @ 5:30 for 30 mins

ANY Questions?

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS