BA: First Line of Defense Against A Security Breach

Building Business Capabilities

November 4-6, 2015

@BBCapability #BBC2015 | @HansEckman | #BAOT #PMOT

Disclaimers

- **Unless otherwise noted, all examples are from the Verizon "2015 Data Breach Investigations Report".**
- **The content in this presentation and discussion are the sole responsibility of Hans Eckman, and does not express the views SunTrust Bank.**
- **This presentation contains NO SunTrust Bank information, examples, policies or approaches.**

Welcome

- **This session is for you, so please participate.**
- **This is a high level introduction to general security terms and topics that business analysts should consider during a project.**
- **No animals were harmed during the creation of this presentation. Please support your local rescue groups.**

https://youtu.be/F7pYHN9iC9I

Why is the BA the First Line of Defense?

- **Requirements are the first opportunity to protect against errors and data breaches.**
- **Early discussions can save countless hours of rework.**
- **The BA must be the advocate for access control, data integrity and security, as well as for the business needs.**
  Security and Fraud Prevention are important business needs.

Data Breach Hall of Fame – Tom's Guide Top 10

1. **Heartland Payment Systems**, 2008-2009: 130 million
2. **Target Stores**, 2013: 110 million
3. **Sony online entertainment services**, 2011: 102 million
4. **National Archive and Records Administration**, 2008: 76 million
5. **Anthem,** 2015: 69 to 80 million
6. **Epsilon**, 2011: 60 to 250 million
7. **Home Depot**, 2014: 56 million payment cards
8. **Evernote**, 2013: More than 50 million
9. **Living Social**, 2013: More than 50 million
10. **TJX Companies Inc.**, 2006-2007: At least 46 million

- **Honorable mention: Sony Pictures Entertainment**, 2014: Company's inner workings completely exposed

Source: http://www.tomsguide.com/us/biggest-data-breaches,news-19083.html

Data Breach Story - Target

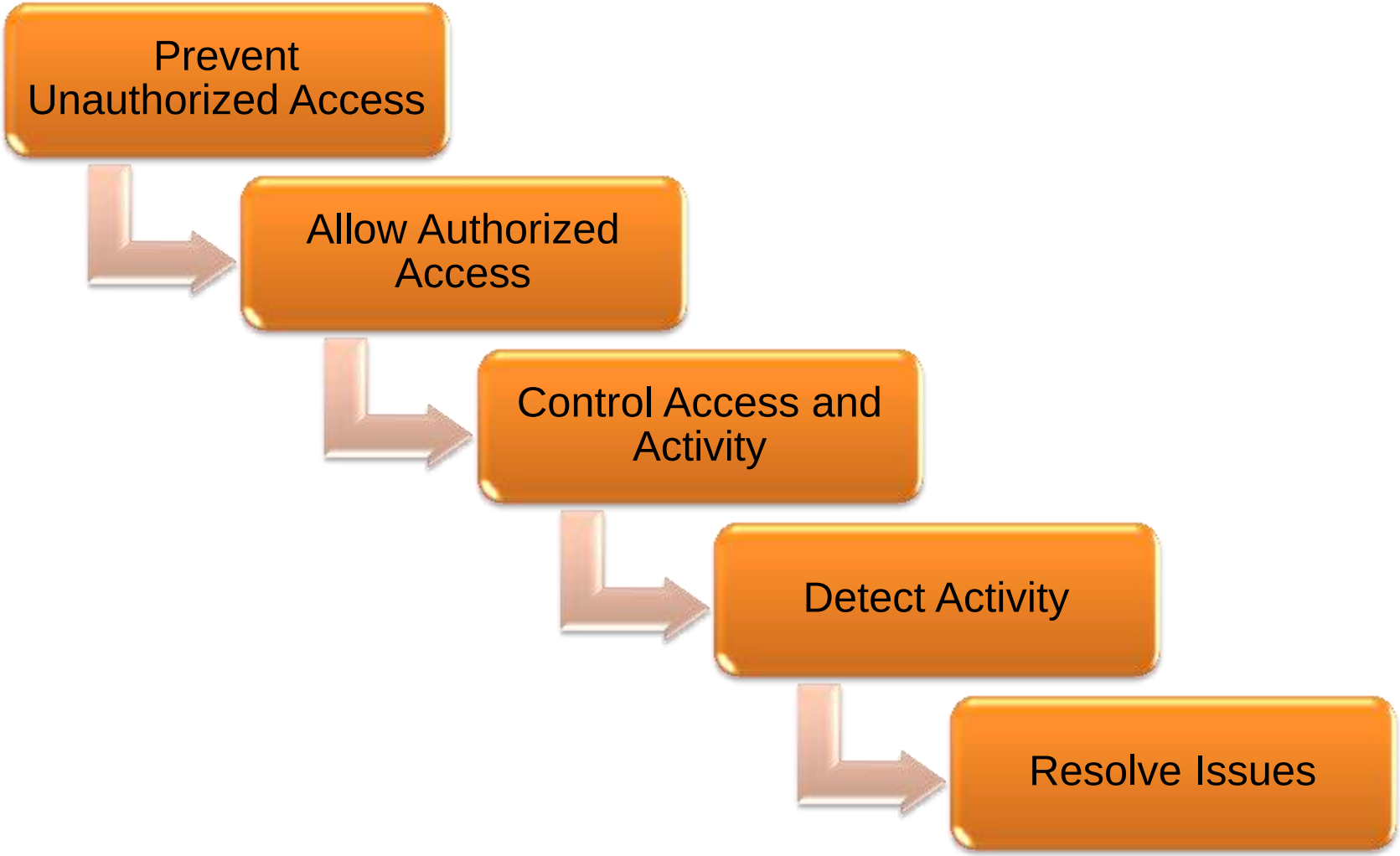
- **November 27 to December 18 2013**
  [Delayed discovery]
- **Phishing email installed Citadel (Zeus variant) Fazio Mechanical (refrigeration contractor) computers.**
  [Phishing, Inadequate Anti-virus]
- **Hackers used Fazio Mechanical's login to gain access through the Target's Ariba supplier portal.**
  [Single Factor Authentication]
- **Hackers exploited vulnerabilities in Windows servers.**
  [SQL injection attack]
- **Trojan.POSRAM used to copy credit/debit card from RAM on Target's POS system.**
- **$252 million cost to date**

Source: http://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/

What Happens When You Don't Take Action

- On average, 80% of breaches are from external.
- 23% of recipients now open phishing messages and 11% click on attachments. Nearly 50% open emails and click on phishing links within the first hour.
- 99.9% of the exploited vulnerabilities were compromised more than a year after the CVE (Common Vulnerabilities and Exposures) was published.
- Only 0.03% of all mobile devices are compromised.
- The forecasted average loss for a breach of 1,000 records is between $52,000 and $87,000.
- 55% of internal incidents were privilege abuse.
- Loss due to errors:
  - 30% Sensitive information reaching incorrect recipients
  - 17% Publishing nonpublic data to public web servers
  - 12% Insecure disposal of personal and medical data

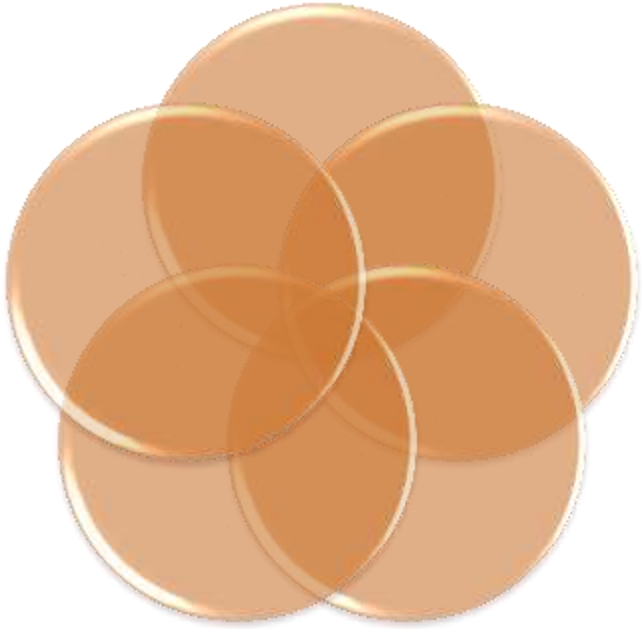
Tiers of Security



Security Landscape

Identity Access Management

Fraud



Records Management

Network*

Physical*

*Network and physical security are not typical requirements in software projects.

Identity Access Management (IAM)

Identity

- **Course grain entitlements**
- **Authentication method**
  - **Challenge response**
  - **Adaptive**

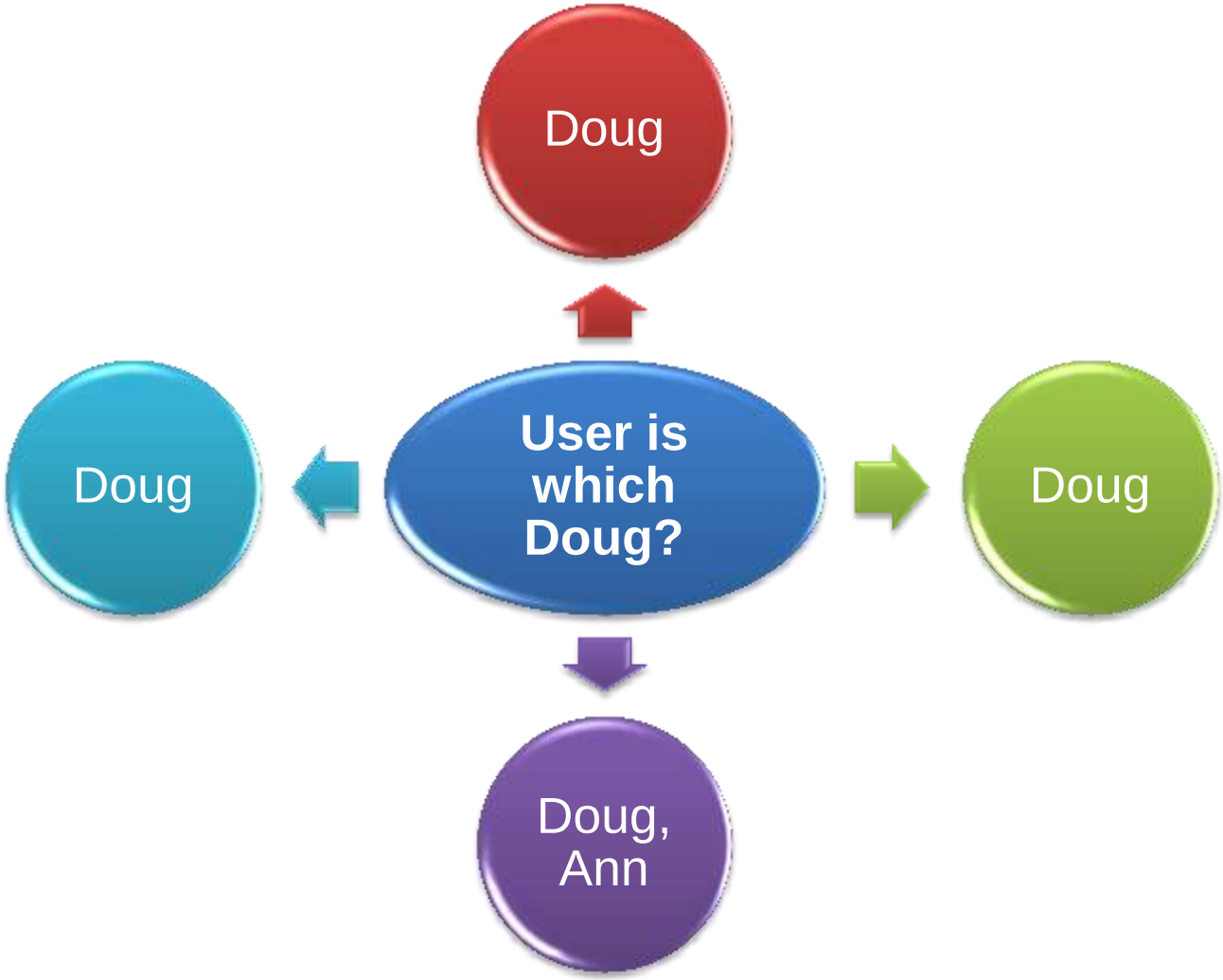
Access

- **Fine grain entitlements**
- **Where to manage**
  - **Centralized: shared repository**
  - **Distributed: within each application**

Understanding Adaptive Authentication

- **Risk based approach**
  - **Step-up authentication**
- **Multifactor examples**
  - **IP blocking: restrict access by provider and/or network**
  - **Location: Geo-blocking, Geo-profiling**
  - **Trusted device**
  - **Biometric: prints, facial, shake**
  - **Token: Time-based key**
  - **Temporary key: SMS, email, phone**
  - **User defined factor (e.g. account image, nicknames)**
  - **CAPTCHA**
- **Third party identity**

IAM – Mapping Identities



IAM – Password Risks

2014 Common Passwords:

1. 123456
2. password
3. 12345
4. 12345678
5. qwerty
6. 123456789
7. 1234
8. baseball
9. dragon
10. football
11. 1234567
12. monkey
13. letmein
14. abc123
15. 111111
16. mustang
17. access
18. shadow
19. master
20. michael
21. superman
22. 696969
23. 123123
24. batman
25. trustno1

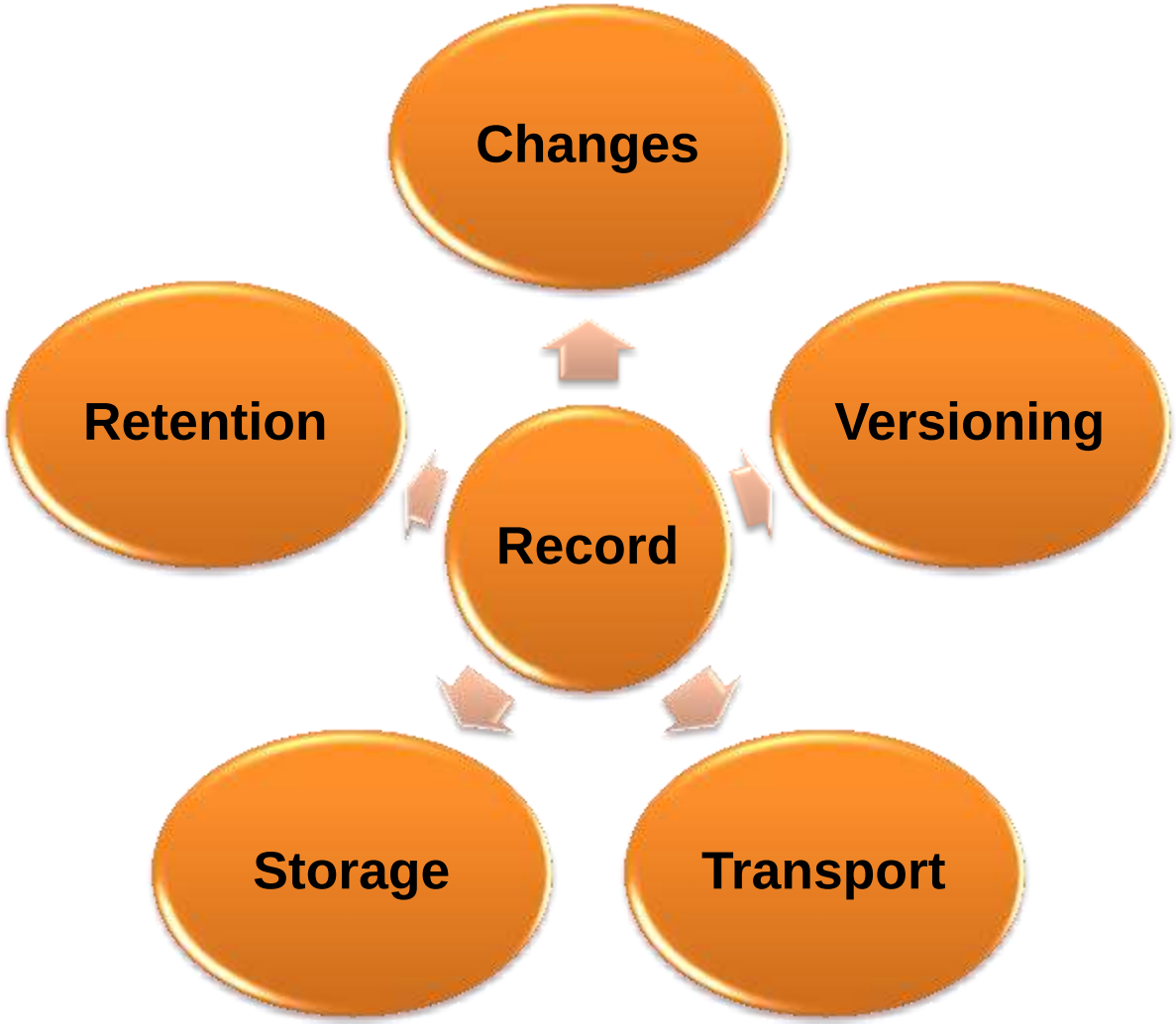
Source: http://gizmodo.com/the-25-most-popular-passwords-of-2014-were-all-doomed-1680596951

IAM – Entitlement Requirements

- **Unclear entitlements**
  - **What can a user actually View/Modify/Delete?**
  - **Embedded groups/inherited permissions**
  - **Assumed requirements or constraints that aren't adequately documented**
- **Segregation of Duties (SOD)**
- **Least Privileged Access**

- ***The top action (55% of incidents) was privilege abuse***
- ***Financial gain and convenience being the primary motivators (40% of incidents)***

Records Management



Record Management – Key Concerns

- **Encryption**
  - **Only protects from a breach is outside your system**
  - **Should include seeding**
  - **Can be bypassed by repetitive data (e.g. password duplication)**

- **Updates and Versioning**
  - **Tied to fine grain entitlements**
  - **Do you care who/how data was changed? Updated?**
  - **How will versions be used? Forensic analysis only?**

Record Management – Key Concerns

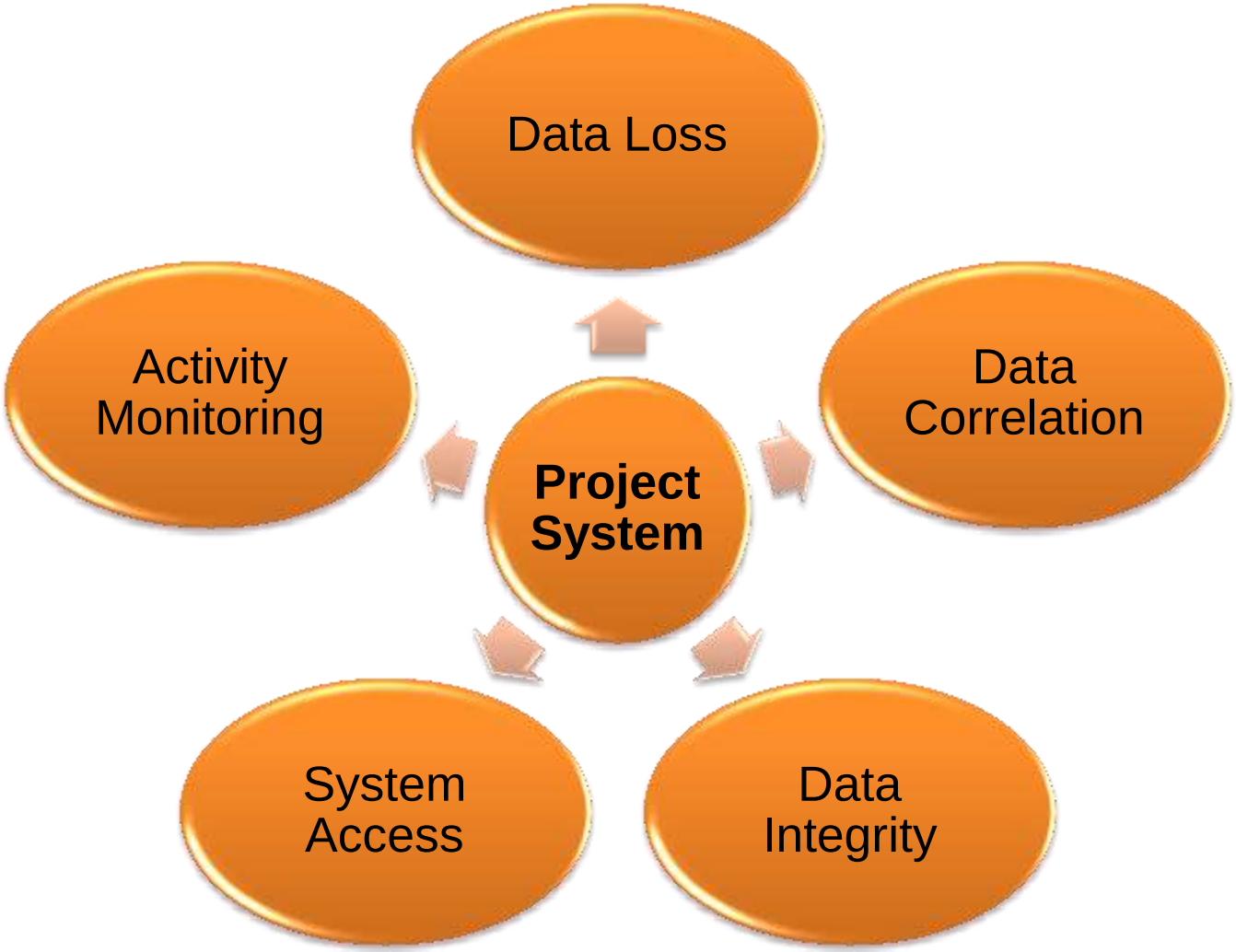
- **Storage**
  - **Will the record be used by more than one system? BI applications?**
  - **If used outside the system of record, does the record bypass fine grain entitlements?**

- **Retention**
  - **Must comply with all corporate, compliance and regulatory requirements.**
  - **Keeping records longer than needed can cause more harm than deletion. (discovery)**
  - **Must be consistently applied.**

Fraud Management

- **Starts with a change: access, record, config**
- **System or user must be aware of change to determine risk**
- **Validate if change exceeds risk tolerance**
- **If action is required, remediation process must be defined**

Fraud Analytics



Stay Connected

- **Building Business Capability -**
  - **@BBCapability**
  - **#BBC2015**

- **Hans Eckman - HansEckman.com**
  - **Hans@HansEckman.com**
  - **http://www.linkedin.com/in/hanseckman**
  - **@HansEckman**

- **Twitter**
  - **#BBC2015**
  - **#BAoT**
  - **#PMoT**

Appendix

Verizon "2015 Data Breach Investigations Report"

Interesting Facts

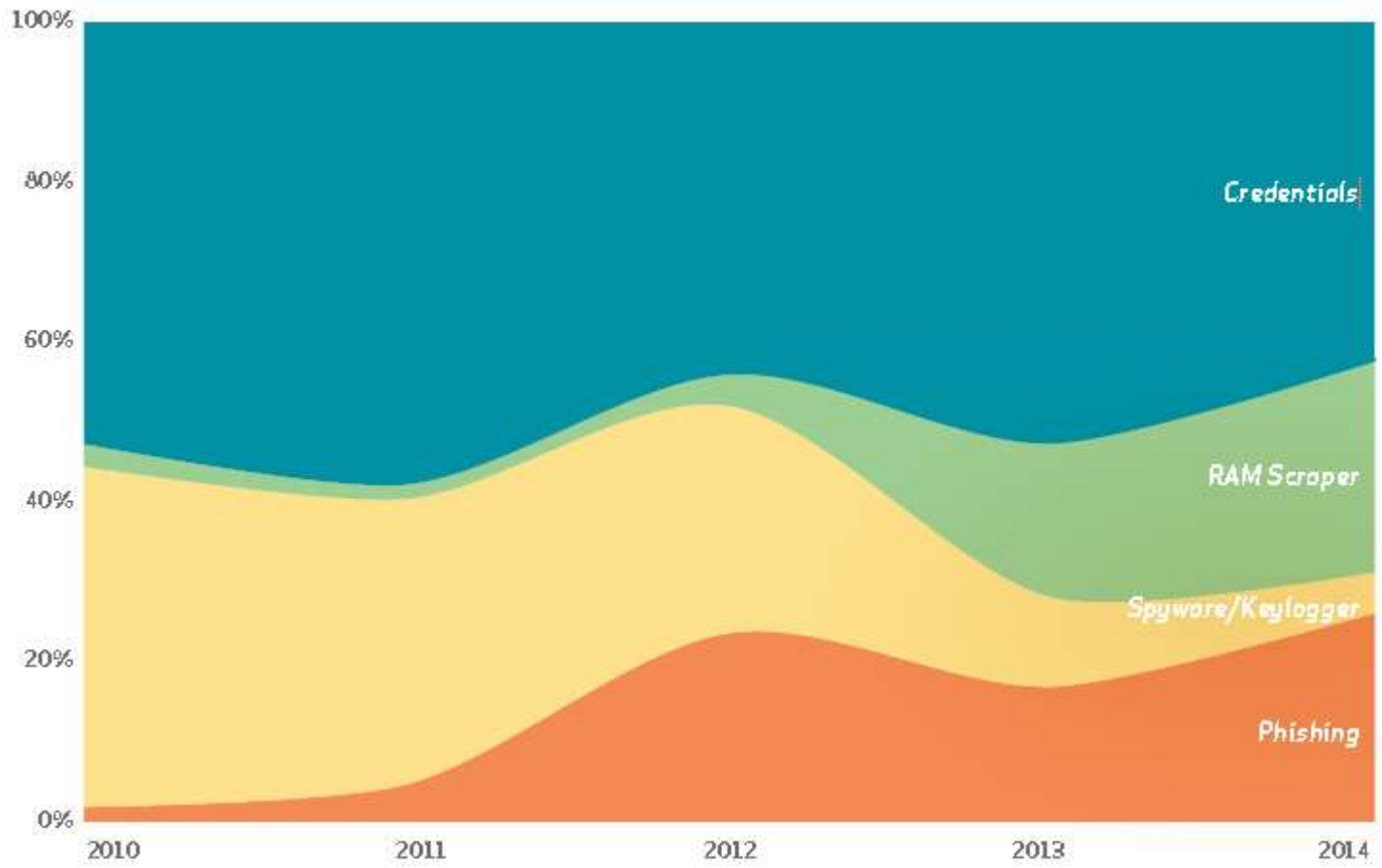
Verizon “2015 Data Breach Investigations Report”

~80% of breaches are external.

Source: Verizon “2015 Data Breach Investigations Report”

HANS·ECKMAN

Verizon "2015 Data Breach Investigations Report"



Credentials

RAM Scraper

Spyware/ Keylogger

Phishing

Source: [Verizon "2015 Data Breach Investigations Report"]

Verizon "2015 Data Breach Investigations Report"

In 60% of cases, attackers are able to compromise an organization within minutes.

Source: Verizon "2015 Data Breach Investigations Report"

Verizon "2015 Data Breach Investigations Report"

Phishing Attacks

23% of recipients now open phishing messages and 11% click on attachments.

Nearly 50% open emails and click on phishing links within the first hour.

Source: Verizon "2015 Data Breach Investigations Report"

Verizon "2015 Data Breach Investigations Report"

For two years, more than two-thirds of incidents that comprise the Cyber-Espionage pattern have featured phishing.

Over 9,000 domains and 50,000 phishing URLs tracked each month.

Source: Verizon "2015 Data Breach Investigations Report"

Verizon "2015 Data Breach Investigations Report"

99.9% of the exploited vulnerabilities were compromised more than a year after the CVE (Common Vulnerabilities and Exposures) was published.

Ten CVEs account for almost 97% of the exploits.

Half of the CVEs exploited in 2014 fell within two weeks.

Source: Verizon "2015 Data Breach Investigations Report"

Verizon "2015 Data Breach Investigations Report"

Mobile Malware

I got 99 problems and mobile malware isn't even 1% of them.

0.03% out of tens of millions of mobile devices, the number of ones infected with truly malicious exploits was negligible.

Source: Verizon "2015 Data Breach Investigations Report"

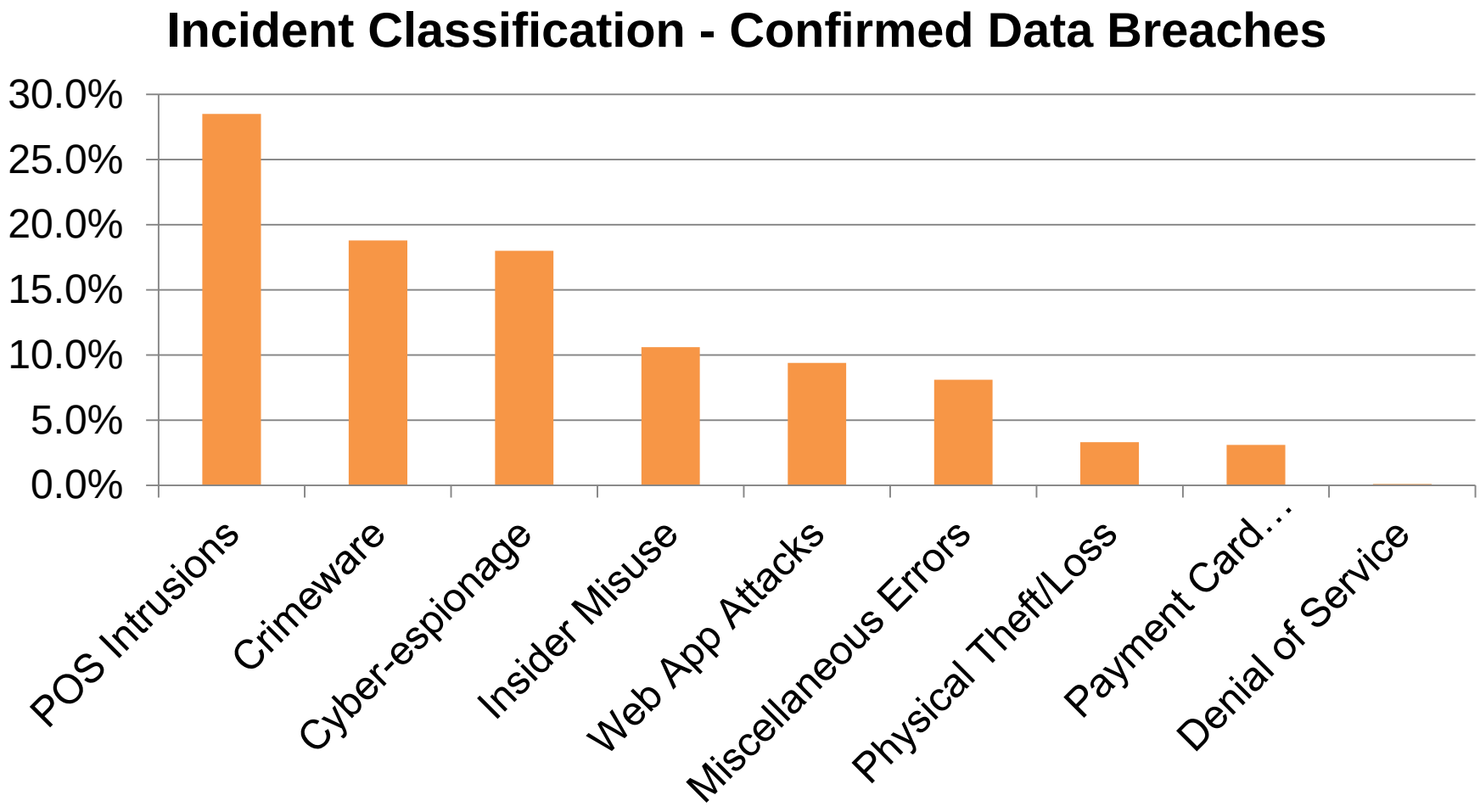
Verizon "2015 Data Breach Investigations Report"

Cost of Data Breaches

The forecast average loss for a breach of 1,000 records is between $52,000 and $87,000.

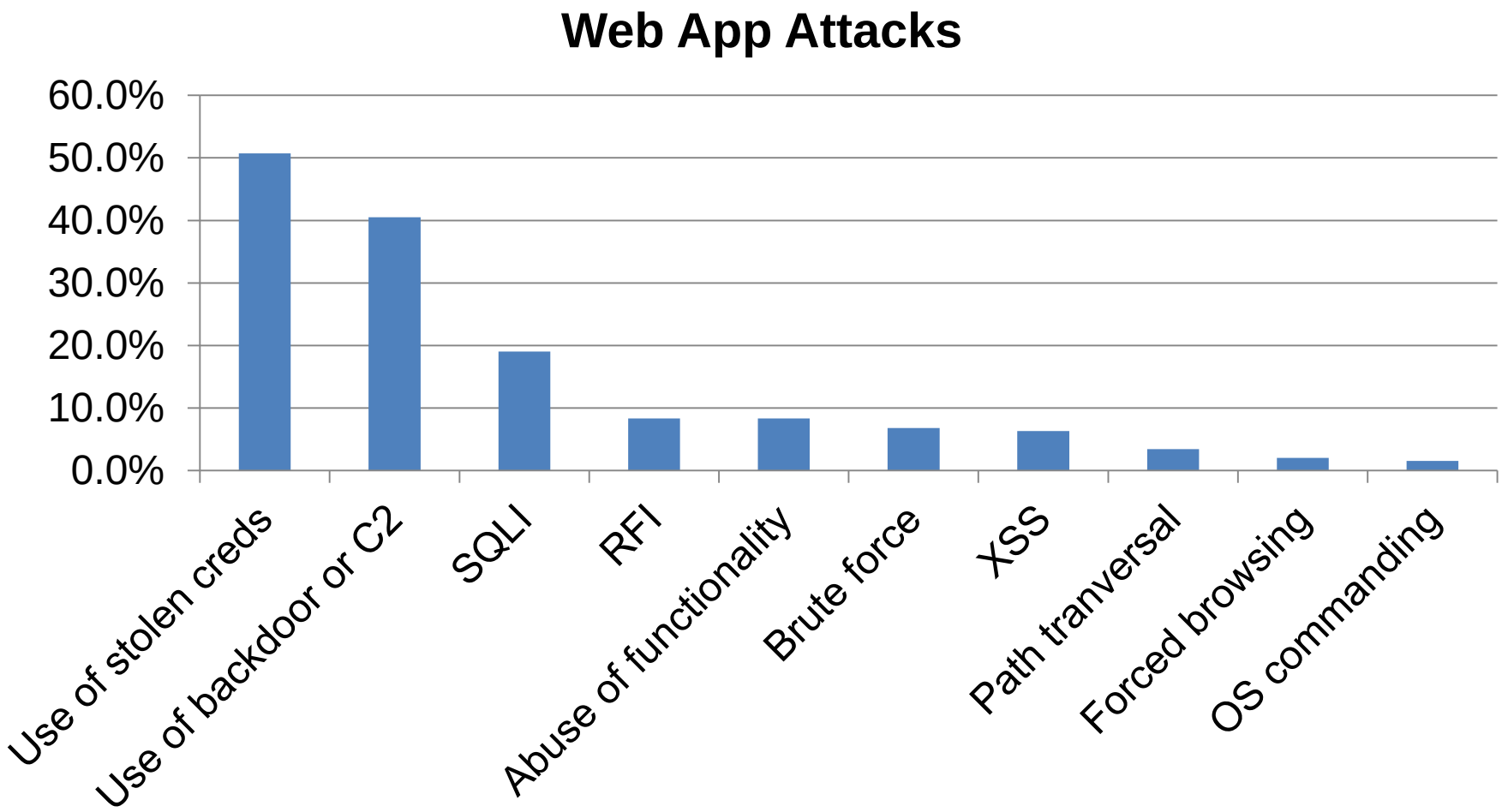
Source: Verizon "2015 Data Breach Investigations Report"

Verizon "2015 Data Breach Investigations Report"



Source: Verizon "2015 Data Breach Investigations Report"

Verizon "2015 Data Breach Investigations Report"



Source: [Verizon "2015 Data Breach Investigations Report"]

Verizon "2015 Data Breach Investigations Report"

Insider Misuse

The top action (55% of incidents) was privilege abuse

Financial gain and convenience being the primary motivators (40% of incidents)

Source: Verizon "2015 Data Breach Investigations Report"

Verizon "2015 Data Breach Investigations Report"

Miscellaneous Errors

System administrators were the prime actors in over 60% of incidents.

- **Sensitive information reaching incorrect recipients 30% of incidents**
- **Publishing nonpublic data to public web servers 17% of incidents**
- **Insecure disposal of personal and medical data 12% of incidents**

Source: Verizon "2015 Data Breach Investigations Report"

Verizon "2015 Data Breach Investigations Report"

JAN: SNAPCHAT

- 4.5 million compromised names and phone numbers

FEB: KICKSTARTER

- 5.6 million victims

MAR: KOREAN TELECOM

- One of the year's largest breaches affected 12 million customers

APR: HEARTBLEED

- First of three open-source vulnerabilities in 2014

MAY: eBAY

- Database of 145 million customers compromised

JUN: PF CHANG'S

- Most high-profile breach of the month

JUL: ENERGETIC BEAR

- Cyberspying operation targeted the energy industry

AUG: CYBERVOR

- 1.2 billion compromised credentials

SEP: iCLOUD

- Celebrity accounts hacked

OCT: SANDWORM

- Attacked a Windows vulnerability

NOV: SONY PICTURES ENTERTAINMENT

- Highest-profile hack of the year

DEC: INCEPTION FRAMEWORK

- Cyber-Espionage attack targeted the public sector

Source: Verizon "2015 Data Breach Investigations Report"

Verizon "2015 Data Breach Investigations Report"

Internet of Things

Verizon experts predict that there will be over 5 billion IoT devices by the end of this decade.

Source: Verizon "2015 Data Breach Investigations Report"