BA: First Line of Defense Against a Security Breach

1. 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.
- No animals were harmed during the creation of this presentation. Please support your local rescue groups.

2. Introduction

Video: 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.

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

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

- Heartland Payment Systems, 2008-2009: 130 million
- Target Stores, 2013: 110 million
- Sony online entertainment services, 2011: 102 million
- National Archive and Records Administration, 2008: 76 million
- Anthem, 2015: 69 to 80 million
- Epsilon, 2011: 60 to 250 million
- Home Depot, 2014: 56 million payment cards
- Evernote, 2013: More than 50 million
- Living Social, 2013: More than 50 million
- TJX Companies Inc., 2006-2007: At least 46 million
  Honorable mention: Sony Pictures Entertainment, 2014: Company's inner workings completely exposed

4. Data Breach Story – Target

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

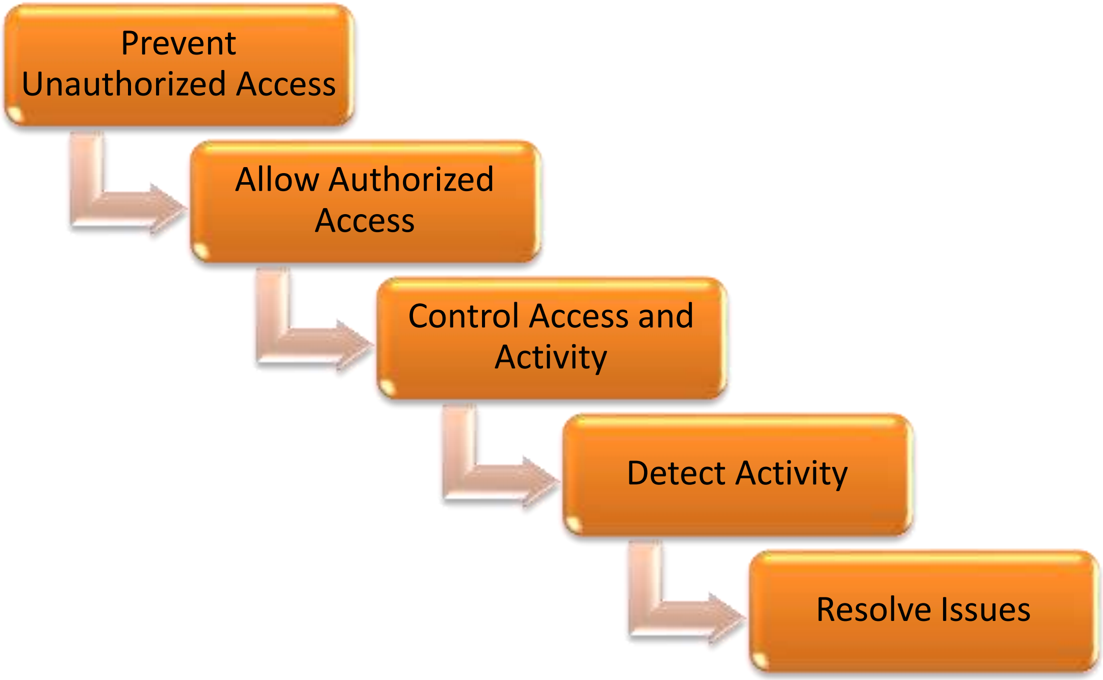
- November 27 to December 18 2013
  [Delayed discovery]
- Phishing email installed Citadel (Zeus variant) Fazio Mechanical (refrigeration contractor) computers.
  [Phishing, Inadequate Anti-virus]

- 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

5. 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

6. Tiers of Security



Prevent Unauthorized Access

Systems need to include measures for blocking all undesired access, both systems and people.

Allow Authorized Access

Blocking access is easy, recognizing and allowing desired access is much harder.

Control Access and Activity

Once in, ensure that users can only do what they are allowed to do.

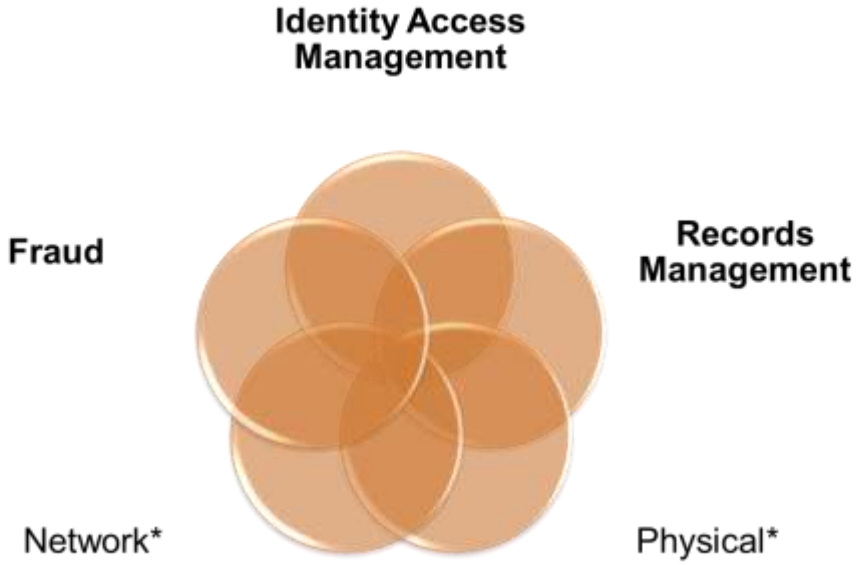
Detect Activity

Monitor all activities and transactions to detect changes and determine which are undesirable.

Resolve Issues

Use activity monitoring to respond to issues or concerns

7. Security Landscape



Your project needs a comprehensive approach to security, and to fit into your security programs. Your requirements need to account for not only the security and fraud aspects of your system, but risks from all interactions between systems. As a BA, you must be aware of how their system overlaps these areas to determine requirements and constraints.

How many people in your organization include physical security requirements into their software specifications?

Identity Access Management

Management of users and permissions

Records Management

Data capture, storage, access, encryption, transport and retention

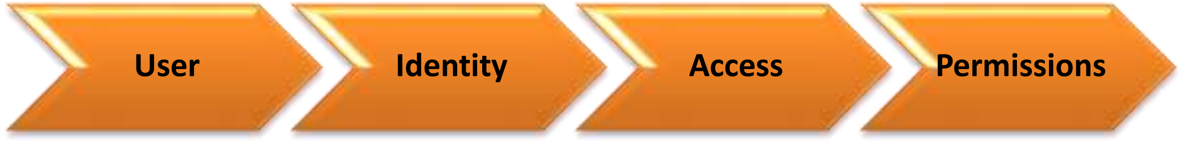
Network

Network security is typically used during infrastructure projects. Software project must account for system connectivity, protocols, FTP, etc.

Physical

Process and system controls around access to offices, data centers, computers or file storage. For example, if you capture paper applications, what happens to the paper after it has been processed?

8. 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

A user is mapped to one or more identities. Coarse grain entitlements determine which systems a user can access. Fine grain entitlements define what the user can do within the system.

Authentication

- Challenge response: User enters credentials (e.g. username/password) which are validated against stored values.
- Adaptive: Risk based approach to base access and entitlements.

Fine grain entitlements management

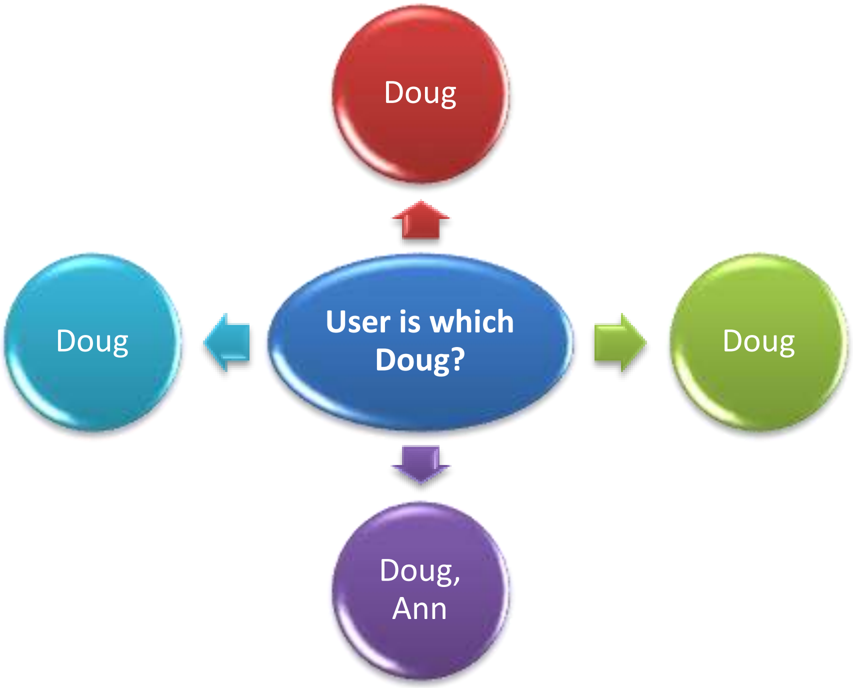
- Centralized: Organization uses a centralized repository for all permissions. Systems access the repository to determine fine grain entitlements. Advantage is that risk management can be centralized and updated across applications. Disadvantage is that any changes could impact other systems and increase risk.
- Distributed: Each application stores fine grain entitlements. Advantage is that the native security model can be leveraged, reducing development and risk within the application. Disadvantage is that risk management is spread across multiple applications allowing one system to increase risk to other systems.

9. Understanding Adaptive Authentication

- Risk based approach
    - Step-up authentication: Perform additional authentication steps when fine grain entitlement risk
- Multifactor examples
    - IP blocking: restrict access by provider and/or network
    - Location: Geo-blocking, Geo-profiling
    - Trusted device: Perform additional authentication steps to link a device to an account
    - Biometric: prints, facial, shake
    - Token: Time-based key

  - Temporary key: SMS, email, phone
  - User defined factor: User sets personally identifiable customizations to help differentiate real applications from a phishing site. (e.g. account image, nicknames)
  - CAPTCHA: Method of ensuring that the user entering the system is human.
- Third party identity

10. IAM – Mapping Identities



How many different logins do your teammates or clients maintain as part of their overall relationship? One of the greatest identity challenges a BA faces is managing multiple accounts for a user across multiple systems. If the BA works to define the identity management strategy upfront, the risk and work later can be dramatically reduced. Consider the cost and complexity of building teammate or client portals to unify the user experience when identity management is not determined upfront. Multi-user accounts must define requirements for managing fine grain entitlements where a user may not always be the primary account.

11. IAM – Password Risks

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

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

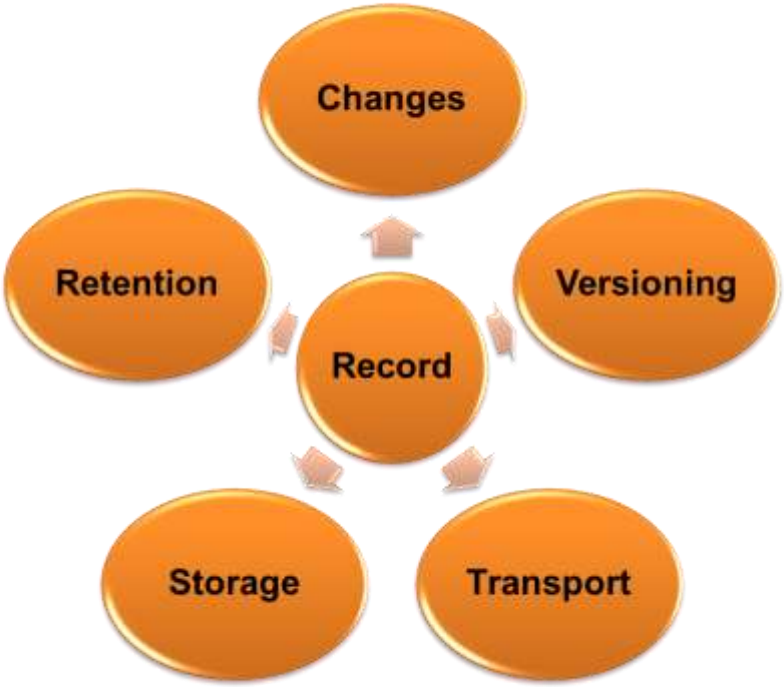
12. IAM – Entitlement Requirements

- 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): Which functions could increase risk or bypass controls if given to the same user? For example, a developer that can check in code (Developer) and promote code to production (Admin) has the ability to insert errors or malicious code into the application. This also applies to complex client systems with tiered permissions or multiple security groups.
  One of the most common ways to introduce SOD violations is from nested permission groups.
- Least Privileged Access: Minimum permissions and access required to complete approved processes.

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

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

13. Records Management



BA must define what data or events are considered records. Records may have requirements similar to users to define all aspects.

Changes

Authorization to make changes (fine grain entitlements); Process to Add/Modify/Delete records

Versioning

Which records must retain versions; Number of versions; Full record or change only

Transport

Encryption; Allowed method of access and sharing; Physical records management

Storage

Location of records; Encryption; Compliance policies; Records in multiple places (man with two watches doesn’t know what time it is, systems of record, reporting/BI)

Retention

Minimum/maximum storage; Archival process; Record deletion; Compliance policies

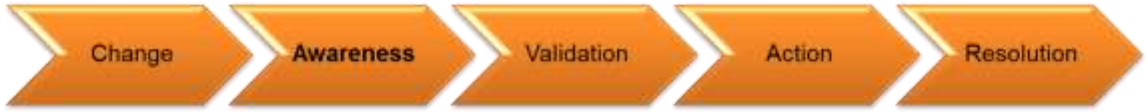
14. Record Management – Key Concerns

- Encryption
  - Only protects from a breach is outside your system
  - Should include seeding
  - Can be bypassed by repetitive data (e.g. password duplication)
  - Define in NFRs to ensure design coverage.
- 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?
  - BA will need to determine tiers based on system/data changes.

15. Record Management – Key Concerns

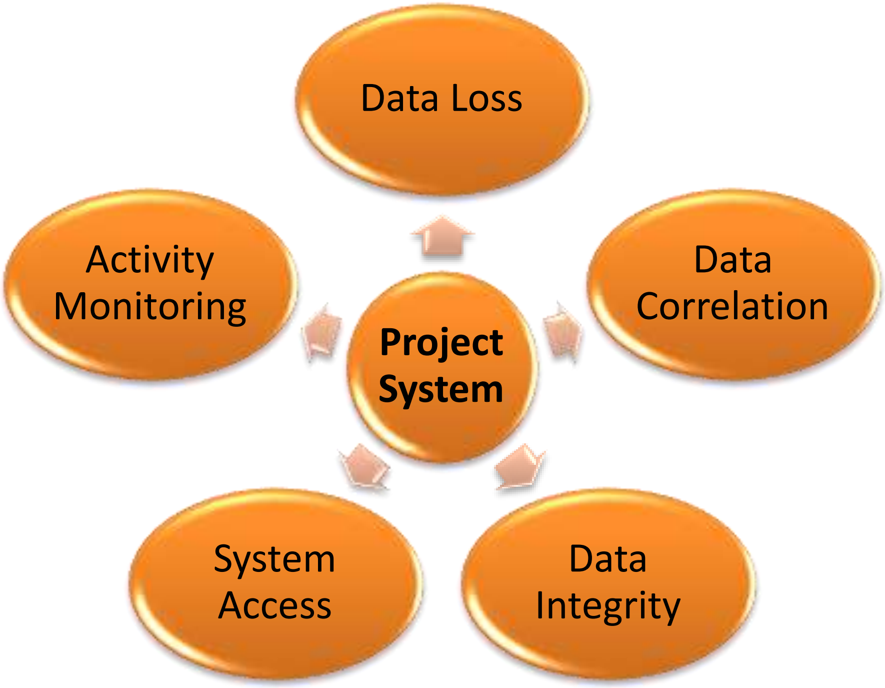
- Storage
  - Will the record be used by more than one system? BI applications?
  - If used outside the system of record, does the record bypass fine grain entitlements?
  - Relates to storage requirements, system of record, data synchronization and impact to project.
- Retention
  - Must comply with all corporate, compliance and regulatory requirements.
  - Keeping records longer than needed can cause more harm than deletion. (discovery)
  - Must be consistently applied.

16. Fraud Management



- Starts with a change or event: 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
- Resolution applies to the undesired change, but can also lead to enhancements to prevent future problems.

17. Fraud Analytics



Data Loss

Deletion or corruption of data

Data Correlation

Ability to correlate data/changes to determine risk potential.

Data Integrity

Confidence that the data is correct and reliable. Risk due to unintended data changes or even ability to change data outside of controls. (SOX implications)

System Access

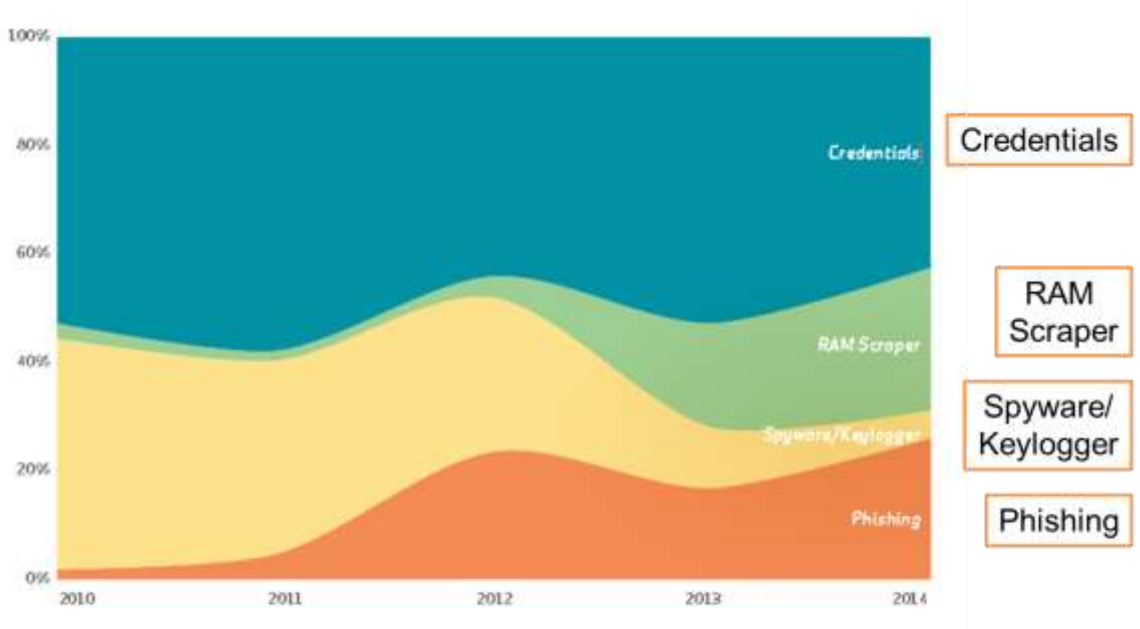
Role of authentication and authorization in data integrity.

Activity Monitoring

Ability to monitor changes

Appendix
Verizon "2015 Data Breach Investigations Report"
Interesting Facts

- ~80% of breaches are external.
- In 60% of cases, attackers are able to compromise an organization within minutes.



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.
- 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.

Common Vulnerabilities and Exposures (CVE)

- 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.

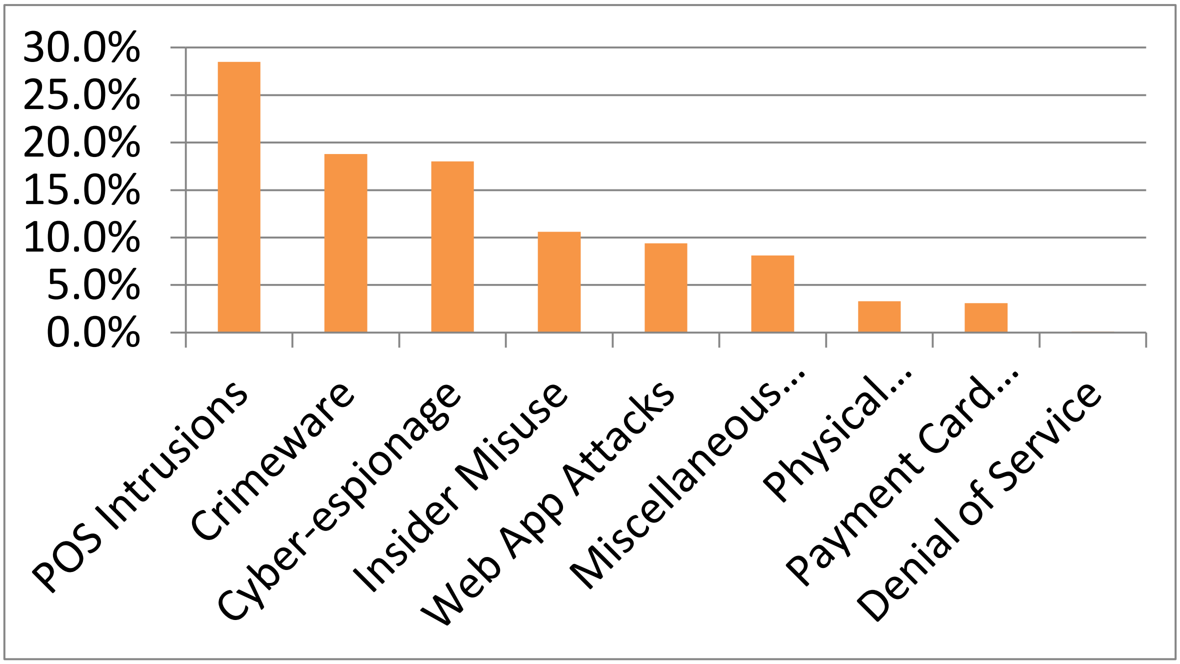
Mobile Malware

- 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.

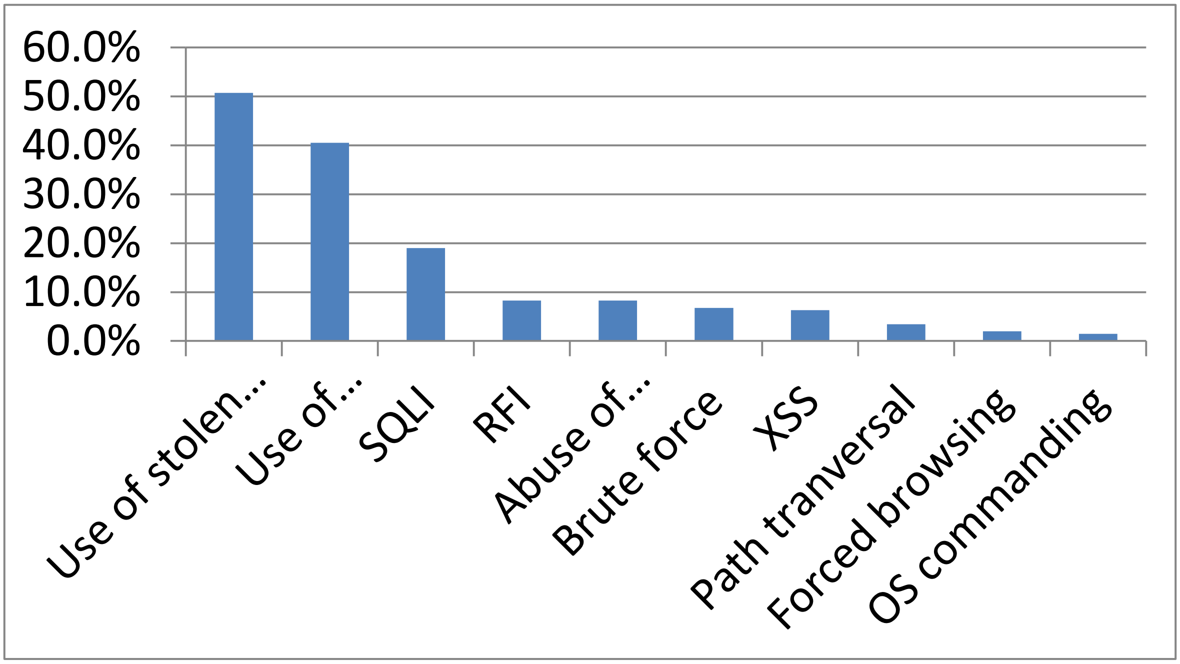
Cost of Data Breaches

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

Incident Classification - Confirmed Data Breaches



Web App Attacks



Insider Misuse

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

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

Top 2014 Breaches by Month

- 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

Internet of Things

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