

# **BA: First Line of Defense Against A Security Breach**

**Hans Eckman | [EckmanGuides.com](http://EckmanGuides.com)**

**@HansEckman | #BAOT #PMOT**

## Everything I Thought I Knew About Security



Source: Photo by Jordan Corrales from Pexels

©2016-2018 Hans Eckman | @HansEckman | EckmanGuides.com

The tip of the volcano.

Throughout my career, I had a good handle on “all the basics” of security. I understood how to document permissions and build access control models. It wasn't until I managed delivery teams serving security, identity access management, information risk and data security, fraud, and audit remediation did I understand how little I really knew.

This presentation is designed to provide you with a high level landscape of everything I wish I had known. It's up to you to determine how wide and broad you want to stretch your knowledge.

## Ground Rules

- **Special thanks to [Verizon "2018 Data Breach Investigations Report"](#) and [CSO Online](#) for statistics and fun facts.**
- **These are tricks and tips that worked for me, but might not be right for everyone or every situation. Please consult a coach or physician to find a program that is best for you.**
- **The views and opinions expressed in this presentation are the sole responsibility of Hans Eckman.**
- **No animals were harmed during the creation of this presentation. Please support your local pet rescue groups.**



<https://youtu.be/F7pYHN9iC9I>



©2016-2018 Hans Eckman | @HansEckman | EckmanGuides.com

<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 Shame – CSO Online Top 17

1. **Yahoo:** 2013-14; 3 billion accounts
  2. **Adult Friend Finder:** October 2016; 412.2 million accounts
  3. **eBay:** May 2014; 145 million accounts
  4. **Equifax:** July 29 2017; 143 million consumers
  5. **Heartland Payment Systems:** March 2008; 134 million accounts
  6. **Target Stores: December 2013;** 110 million accounts
  7. **TJX Companies: December 2006;** 94 million credit cards
  8. **Uber; Late 2016:** 57 million users and 600,000 drivers
  9. **JP Morgan Chase: July 2014;** 76 mil customers; 7 mil businesses
  10. **US Office of Personnel Management (OPM):** 2012-14; 22 million current and former federal employees
- **Honorable mention: Sony Pictures Entertainment, 2014:**  
Company's inner workings completely exposed

Source: <https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html>

©2016-2018 Hans Eckman | @HansEckman | EckmanGuides.com

## Data Breach Story - Target

- **November 27 to December 18 2013**  
[Delayed discovery]
- **Phishing email installed Citadel (Zeus variant) in 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 direct cost, plus reputational loss**

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

©2016-2018 Hans Eckman | @HansEckman | EckmanGuides.com

1. Incident was not discovered for 3 weeks.
2. A contractor was the target of a phishing email and virus due to improperly updated and protected computers.
3. Virus allowed hackers to record the vendor's login to Target's Ariba supplier portal, which used LDAP for all internal and external users.
4. Hackers used LDAP account to install SQL on unpatched Windows servers, then used server access accounts to infect POS system.
5. Trojan.POSRAM copied credit/debit card information from active memory and before it was encrypted.



## Top 5 cybersecurity facts, figures and stats for 2018

- 1. Cybercrime damage costs to hit \$6 trillion annually by 2021**
- 2. Cybersecurity spending to exceed \$1 trillion: 2017 to 2021**
- 3. Cybercrime will more than triple the number of unfilled cybersecurity jobs, predicted to reach 3.5 million by 2021**
- 4. Human attacks to reach 6 billion people by 2022**
- 5. Global ransomware damage costs are predicted to exceed \$5 billion in 2017**

Source: <https://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics.html>

©2016-2018 Hans Eckman | @HansEckman | EckmanGuides.com



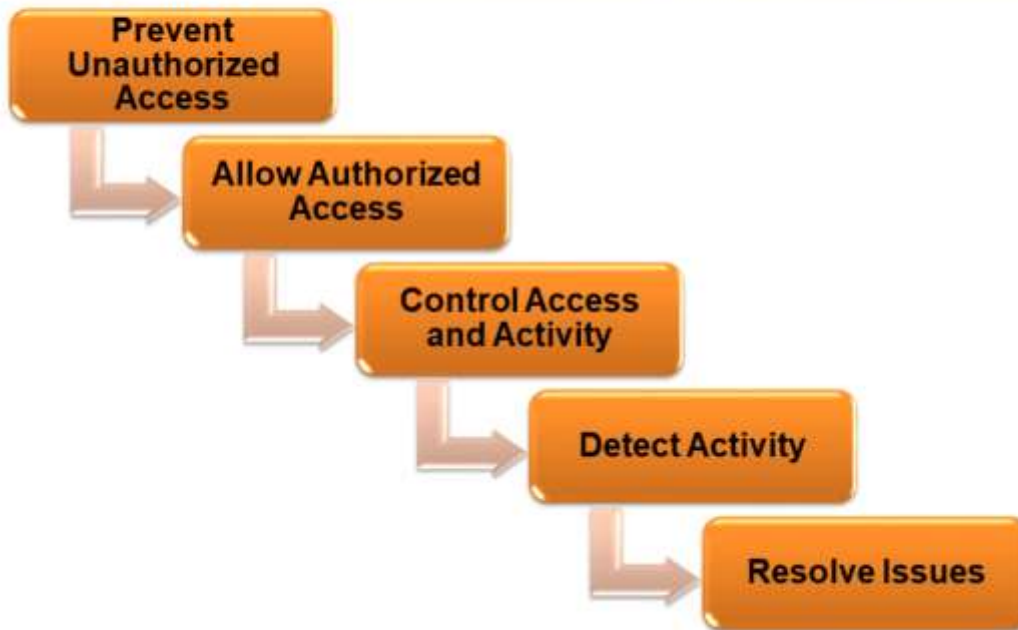
## What Happens When You Don't Take Action

- **73% of breaches are external**
- **50% organized crime and 12% government sponsored**
- **Tactics used: 48% hacking; 30% malware; 17% errors; 17% social; 12% privilege abuse; 11% physical**
- **Phishing/Pretexting: 13% of all breaches**
  - **22% of recipients now open phishing messages**
  - **Average first click in 16 minutes; first report 28 minutes**
  - **59% financial gain; 41% espionage**
- **Target of breach: 1. Web applications; 2. Errors; 3. POS systems; 4. Privilege misuse; 5. Espionage**

Source: [Verizon "2018 Data Breach Investigations Report"](#)

©2016-2018 Hans Eckman | @HansEckman | EckmanGuides.com

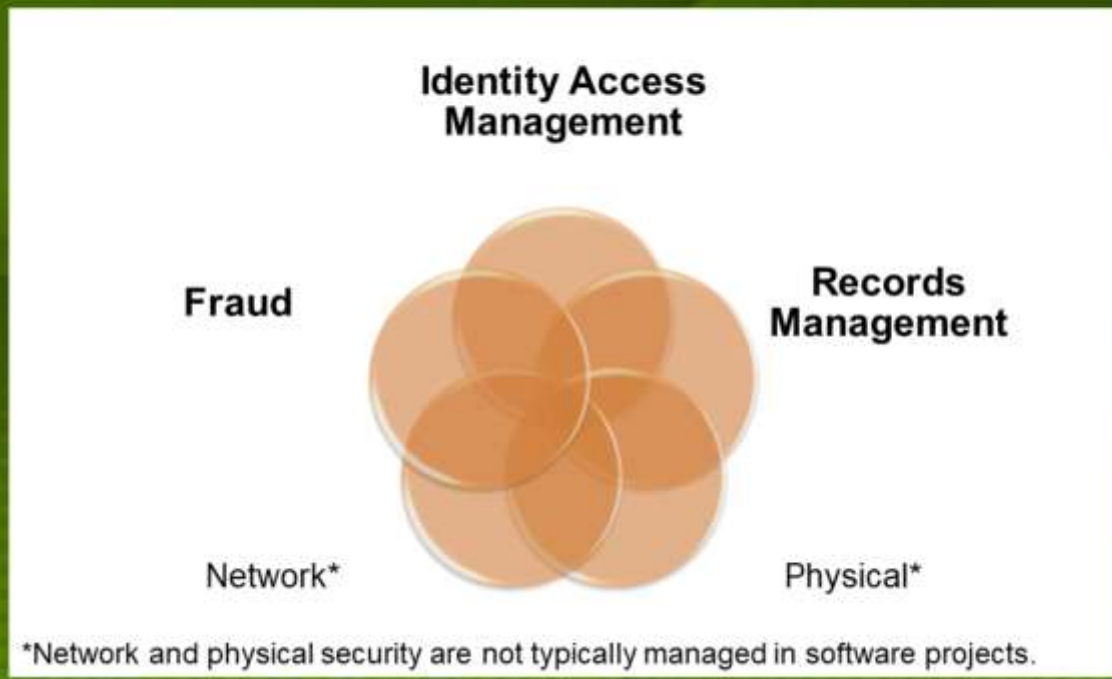
## Tiers of Security - From a Project Perspective



©2016-2018 Hans Eckman | @HansEckman | EckmanGuides.com

- **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
- Use credit card fraud protection as basic example of layers.

## Security Landscape



©2016-2018 Hans Eckman | @HansEckman | EckmanGuides.com

- Discuss five core areas of security that are part of a comprehensive strategy.
- Discuss how the BA must be aware of how their system overlaps these areas so that they can determine requirements and constraints.
- 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.
- Q: How many people include physical security requirements into their software specifications?
- Physical: 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?

## Identity Access Management (IAM)



### Identity - Who are you?

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

### Access - What can you do?

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

©2016-2018 Hans Eckman | @HansEckman | EckmanGuides.com

- Explain the difference between identity, authentication and access.
- Authentication: Difference between challenge response and adaptive
- Fine grain entitlements: Introduce centralized vs distributed management

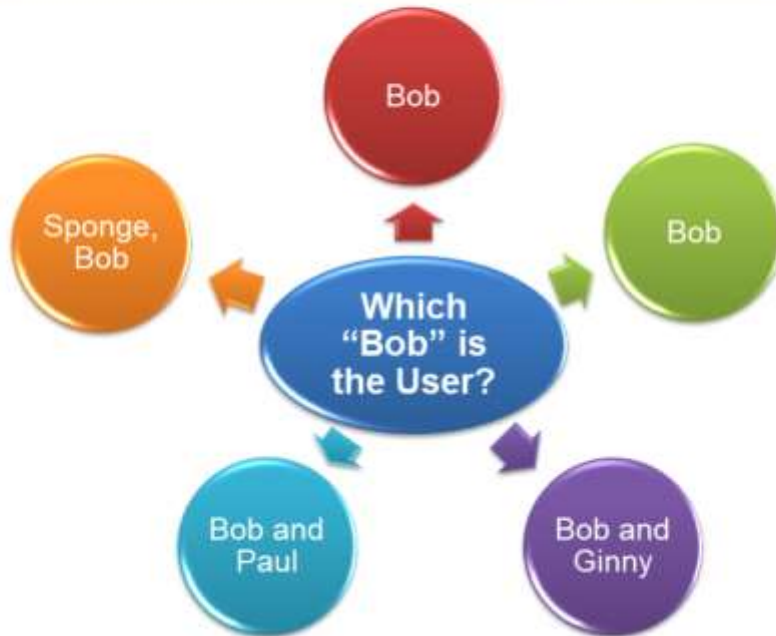
## Understanding Adaptive Authentication

- **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**

©2016-2018 Hans Eckman | @HansEckman | EckmanGuides.com

- Risk based: Discuss use of step up authentication tied to fine grain entitlements/action
- Multifactor: Overview of multifactor options
- Third Party: Discuss use of third party identities for authentication (Google, Facebook, LinkedIn, Apple, etc.)

IAM – Mapping Identities




©2016-2018 Hans Eckman | @HansEckman | EckmanGuides.com

Discuss challenge of managing and mapping identities and permissions. Multi-user accounts must define requirements for managing fine grain entitlements across multiple systems where a user may not always be the primary account.



IAM – 2017 Common Passwords from Qizmodo



A Venn diagram with three overlapping circles. The top circle is light green and labeled 'Email'. The bottom-left circle is purple and labeled 'Accounts'. The bottom-right circle is teal and labeled 'Social Media'. The circles overlap in the center and at the intersections between two of them.

|              |              |
|--------------|--------------|
| 1. 123456    | 14. login    |
| 2. Password  | 15. abc123   |
| 3. 12345678  | 16. starwars |
| 4. qwerty    | 17. 123123   |
| 5. 12345     | 18. dragon   |
| 6. 123456789 | 19. passw0rd |
| 7. letmein   | 20. master   |
| 8. 1234567   | 21. hello    |
| 9. football  | 22. freedom  |
| 10. iloveyou | 23. whatever |
| 11. admin    | 24. qazwsx   |
| 12. welcome  | 25. trustno1 |
| 13. Monkey   |              |

Source: <https://qizmodo.com/the-25-most-popular-passwords-of-2017-you-sweet-misqu-1821425092>

©2016-2018 Hans Eckman | @HansEckman | EckmanGuides.com

Discuss risks of password reuse, extended risk when compromised, and common passwords. Risk of common passwords even when encryption is used without seeding.



## 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 (12% of incidents) was privilege abuse**

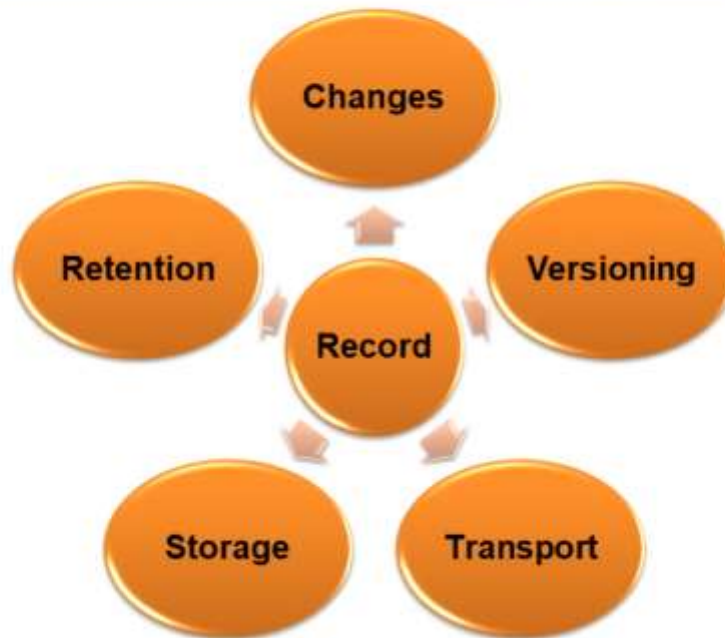
Source: [Verizon "2018 Data Breach Investigations Report"](#)

©2016-2018 Hans Eckman | @HansEckman | EckmanGuides.com

Discuss need and approach to defining entitlements in requirements.

- Unclear entitlements: The team must completely define all access requirements to avoid problems later.
- Least Privileged Access: A user should have the very least access needed to perform their job or task. Any additional access increases risk of error or abuse.
- The top action was privilege abuse: Whether error or theft, privileged access is the highest internal risk to an organization.

## Records Management



©2016-2018 Hans Eckman | @HansEckman | EckmanGuides.com

- 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

## Record Management – Key Concerns

### ➤ 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?

### ➤ Encryption

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

©2016-2018 Hans Eckman | @HansEckman | EckmanGuides.com

- Encryption: Define in NFRs to ensure design coverage.
- Updates/Versioning: Discuss how BA will need to determine tiers based on system/data changes.

## 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.**

©2016-2018 Hans Eckman | @HansEckman | EckmanGuides.com

- Storage: Discuss storage requirements, system of record, data synchronization and impact to project.
- Retention: Discuss retention factors when no enterprise standard is present.

## Fraud Management



©2016-2018 Hans Eckman | @HansEckman | EckmanGuides.com

Overview of fraud process and impact to system requirements. How will fraud systems and teams be able to identify and validate when changes are fraud related? The gap between the change and where the organization becomes aware of the change is the highest risk area.

## Fraud Analytics



©2016-2018 Hans Eckman | @HansEckman | EckmanGuides.com

- **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

## Apply and Discuss



©2016-2018 Hans Eckman | @HansEckman | EckmanGuides.com



## Stay Connected

### ➤ Hans Eckman

- <http://EckmanGuides.com>
- [Hans@HansEckman.com](mailto:Hans@HansEckman.com)
- <http://www.linkedin.com/in/hanseckman>
- @HansEckman

### ➤ Twitter

- #BAoT – Business Analysis on Twitter
- #PMoT – Project Management on Twitter

# **Appendix: Interesting Facts**

## Cybercrime damage costs to hit \$6 trillion annually by 2021.

It all begins and ends with cybercrime. Without it, there's nothing to cyber-defend. The cybersecurity community and major media have largely concurred on the prediction that cyber crime damages will cost the world \$6 trillion annually by 2021, up from \$3 trillion in 2015. This represents the greatest transfer of economic wealth in history, risks the incentives for innovation and investment, and will be more profitable than the global trade of all major illegal drugs combined.

Source: <https://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics.html>

©2016-2018 Hans Eckman | @HansEckman | EckmanGuides.com

## Cybersecurity spending to exceed \$1 trillion from 2017 to 2021.

The rising tide of cyber crime has pushed information security (a subset of cybersecurity) spending to more than \$86.4 billion in 2017, according to Gartner. That doesn't include an accounting of internet of things (IoT), industrial IoT, and industrial control systems (ICS) security, automotive security, and other cybersecurity categories. Global spending on cybersecurity products and services are predicted to exceed \$1 trillion over five years, from 2017 to 2021.

Source: <https://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics.html>

©2016-2018 Hans Eckman | @HansEckman | EckmanGuides.com

**Cybercrime will more than triple the number of unfilled cybersecurity jobs, which is predicted to reach 3.5 million by 2021.**

Every IT position is also a cybersecurity position now. Every IT worker, every technology worker, needs to be involved with protecting and defending apps, data, devices, infrastructure and people. The cybersecurity workforce shortage is even worse than what the jobs numbers suggest. As a result, the cybersecurity unemployment rate has dropped to zero percent.

Source: <https://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics.html>

©2016-2018 Hans Eckman | @HansEckman | EckmanGuides.com



## Human attacks to reach 6 billion people by 2022.

As the world goes digital, humans have moved ahead of machines as the top target for cyber criminals. There were 3.8 billion internet users in 2017 (51 percent of the world's population of 7 billion), up from 2 billion in 2015. Cybersecurity Ventures predicts there will be 6 billion internet users by 2022 (75 percent of the projected world population of 8 billion) — and more than 7.5 billion internet users by 2030 (90 percent of the projected world population of 8.5 billion, 6 years of age and older). The hackers smell blood now, not silicon.

Source: <https://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics.html>

©2016-2018 Hans Eckman | @HansEckman | EckmanGuides.com

**Global ransomware damage costs are predicted to exceed \$5 billion in 2017.**

That's up from \$325 million in 2015 — a 15X increase in two years and expected to worsen. Ransomware attacks on healthcare organizations — the No. 1 cyber-attacked industry — will quadruple by 2020. Cybersecurity Ventures expects ransomware damage costs will rise to \$11.5 billion in 2019 and that a business will fall victim to a ransomware attack every 14 seconds by that time.

Source: <https://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics.html>

©2016-2018 Hans Eckman | @HansEckman | EckmanGuides.com



Verizon “2018 Data Breach Investigations Report”

**73% of breaches are external**

Source: [Verizon “2018 Data Breach Investigations Report”](#)

©2016-2018 Hans Eckman | @HansEckman | EckmanGuides.com

Verizon "2018 Data Breach Investigations Report"

**73% of breaches are external**

Source: [Verizon "2018 Data Breach Investigations Report"](#)

©2016-2018 Hans Eckman | @HansEckman | EckmanGuides.com

Verizon “2018 Data Breach Investigations Report”

**50% organized crime and 12%  
government sponsored**

Source: [Verizon “2018 Data Breach Investigations Report”](#)

©2016-2018 Hans Eckman | @HansEckman | EckmanGuides.com

## Verizon "2018 Data Breach Investigations Report"

### Tactics used:

- **48% hacking**
- **30% malware**
- **17% errors**
- **17% social**
- **12% privilege abuse**
- **11% physical**

Source: [Verizon "2018 Data Breach Investigations Report"](#)

©2016-2018 Hans Eckman | @HansEckman | EckmanGuides.com

## Verizon "2018 Data Breach Investigations Report"

### **Phishing/Pretexting:**

- **13% of all breaches**
- **22% of recipients now open phishing messages**
- **Average first click in 16 minutes; first report 28 minutes**
- **59% financial gain; 41% espionage**

Source: [Verizon "2018 Data Breach Investigations Report"](#)

©2016-2018 Hans Eckman | @HansEckman | EckmanGuides.com

Verizon "2018 Data Breach Investigations Report"

**58% of victims are small businesses**

Source: [Verizon "2018 Data Breach Investigations Report"](#)

©2016-2018 Hans Eckman | @HansEckman | EckmanGuides.com

## Verizon "2018 Data Breach Investigations Report"

### **Targets of a breach:**

- 1. Web applications**
- 2. Errors**
- 3. POS systems**
- 4. Privilege misuse**
- 5. Espionage**

Source: [Verizon "2018 Data Breach Investigations Report"](#)

©2016-2018 Hans Eckman | @HansEckman | EckmanGuides.com



## Verizon “2018 Data Breach Investigations Report”

### Who's behind the breaches?



Source: [Verizon “2018 Data Breach Investigations Report”](#)

©2016-2018 Hans Eckman | @HansEckman | EckmanGuides.com

## Verizon “2018 Data Breach Investigations Report”

### What tactics are utilized?



Source: [Verizon “2018 Data Breach Investigations Report”](#)

©2016-2018 Hans Eckman | @HansEckman | EckmanGuides.com

## Verizon "2018 Data Breach Investigations Report"

### Top 20 action varieties in incidents



### Top 20 action varieties in breaches



Source: [Verizon "2018 Data Breach Investigations Report"](#)

©2016-2018 Hans Eckman | @HansEckman | EckmanGuides.com

## Verizon "2018 Data Breach Investigations Report"

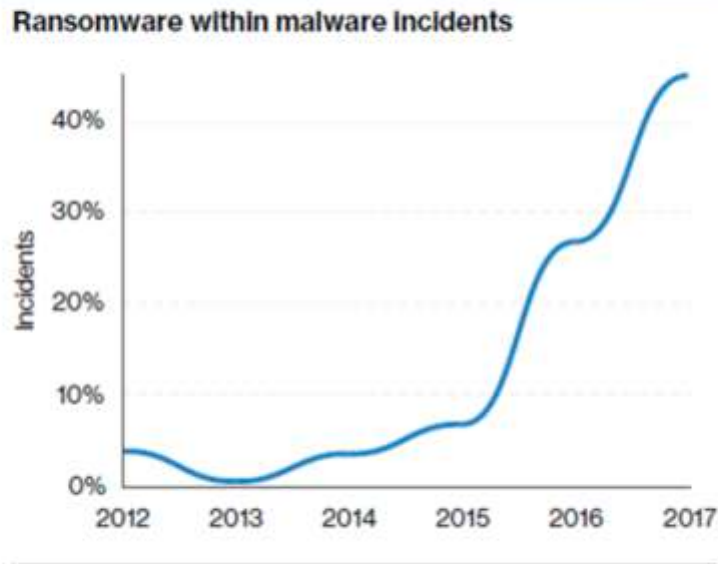


Figure 15. Ransomware within malware incidents over time

Source: **Verizon "2018 Data Breach Investigations Report"**

©2016-2018 Hans Eckman | @HansEckman | EckmanGuides.com

## Verizon "2018 Data Breach Investigations Report"

### Frequency of malware vectors

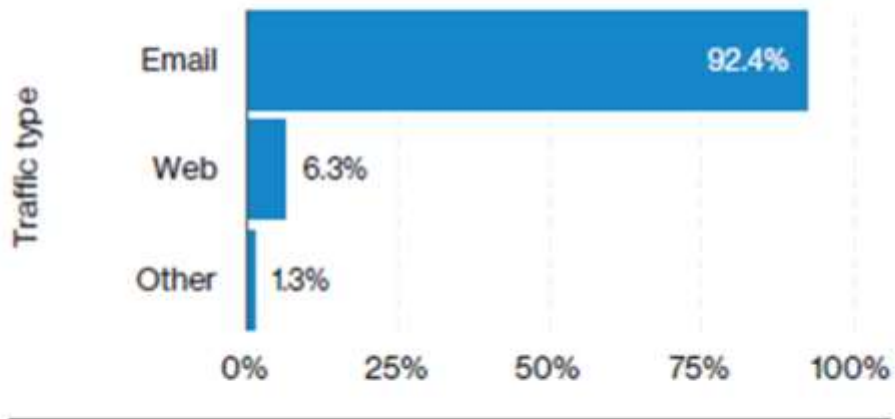


Figure 21. Frequency of malware vectors within detected malware (n=58,987,788)

Source: [Verizon "2018 Data Breach Investigations Report"](#)

©2016-2018 Hans Eckman | @HansEckman | EckmanGuides.com

## Verizon "2018 Data Breach Investigations Report"

Frequency of malware file types

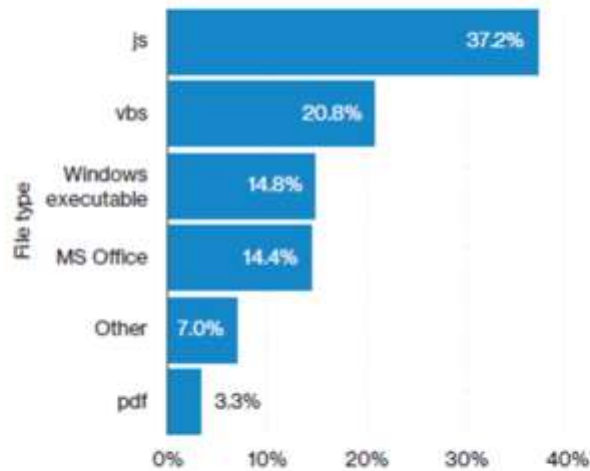


Figure 22. Frequency of malware file types within detected malware (n=436,481,686)

Source: [Verizon "2018 Data Breach Investigations Report"](#)

©2016-2018 Hans Eckman | @HansEckman | EckmanGuides.com



Verizon "2018 Data Breach Investigations Report"

**JavaScript (.js), Visual Basic Script (.vbs), MS Office and PDF10 tend to be the file types found in first-stage malware. They're what sneaks in the door. They then drop the second-stage malware. In this case, it's predominantly Windows executables.**

Source: [Verizon "2018 Data Breach Investigations Report"](#)

©2016-2018 Hans Eckman | @HansEckman | EckmanGuides.com

Verizon "2018 Data Breach Investigations Report"

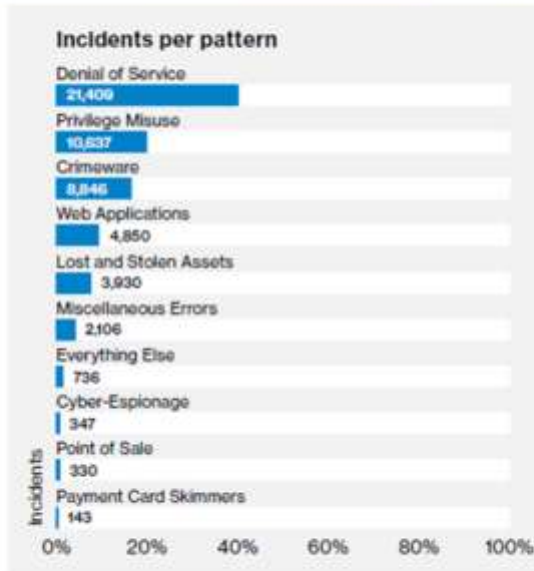


Figure 26. Percentage and count of incidents per pattern (n=53,308)

Source: [Verizon "2018 Data Breach Investigations Report"](#)

Verizon "2018 Data Breach Investigations Report"

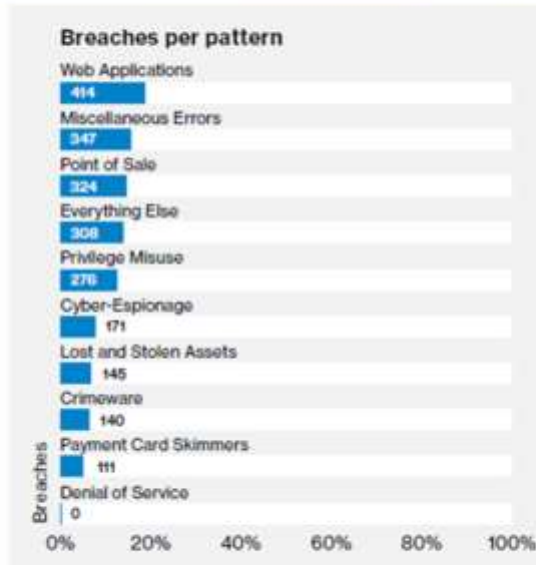


Figure 27. Percentage and count of breaches per pattern (n=2,216)

Source: [Verizon "2018 Data Breach Investigations Report"](#)

Verizon "2018 Data Breach Investigations Report"

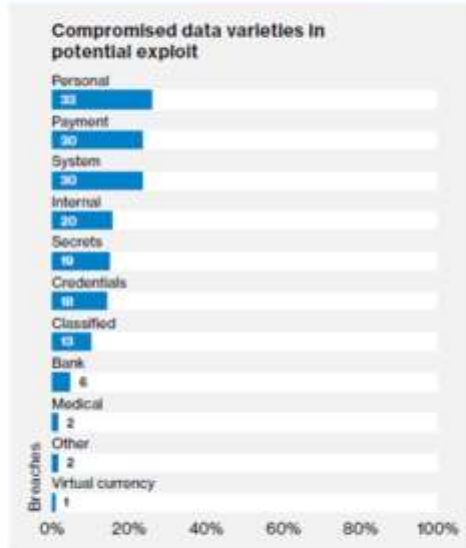


Figure 46. Compromised data varieties within potential exploit breaches (n=128)

Source: [Verizon "2018 Data Breach Investigations Report"](#)