BA: FIRST LINE OF DEFENSE AGAINST A SECURITY BREACH

Hans Eckman | EckmanGuides.com | @HansEckman
http://www.linkedin.com/in/hanseckman

Ground Rules

- This session is for you, so please participate.
- 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.
- No animals were harmed during the creation of this presentation, and please support pet rescue groups.

MoeMoe

Peanut

Oompa

Charlie

Charlie & Katy

Everything I Thought I Knew About Security

Source: Photo by Jordan Corrales from Pexels 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 July 2021

- Yahoo: 2013-14; 3 billion accounts
- Alibaba Date: November 2019 Impact: 1.1 billion pieces of user data
- LinkedIn Date: June 2021 Impact: 700 million users
- Sina Weibo (China Social Media) Date: March 2020 Impact: 538 million accounts
- Facebook Date: April 2019 Impact: 533 million users
- Marriott International (Starwood) Date: September 2018 Impact: 500 million customers
- Yahoo Date: 2014 Impact: 500 million accounts
- Adult Friend Finder Date: October 2016 Impact: 412.2 million accounts
- MySpace Date: 2013 Impact: 360 million user accounts
- NetEase Date: October 2015 Impact: 235 million user accounts
- Honorable mention: Sony Pictures Entertainment, 2014: Company's inner workings exposed

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

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

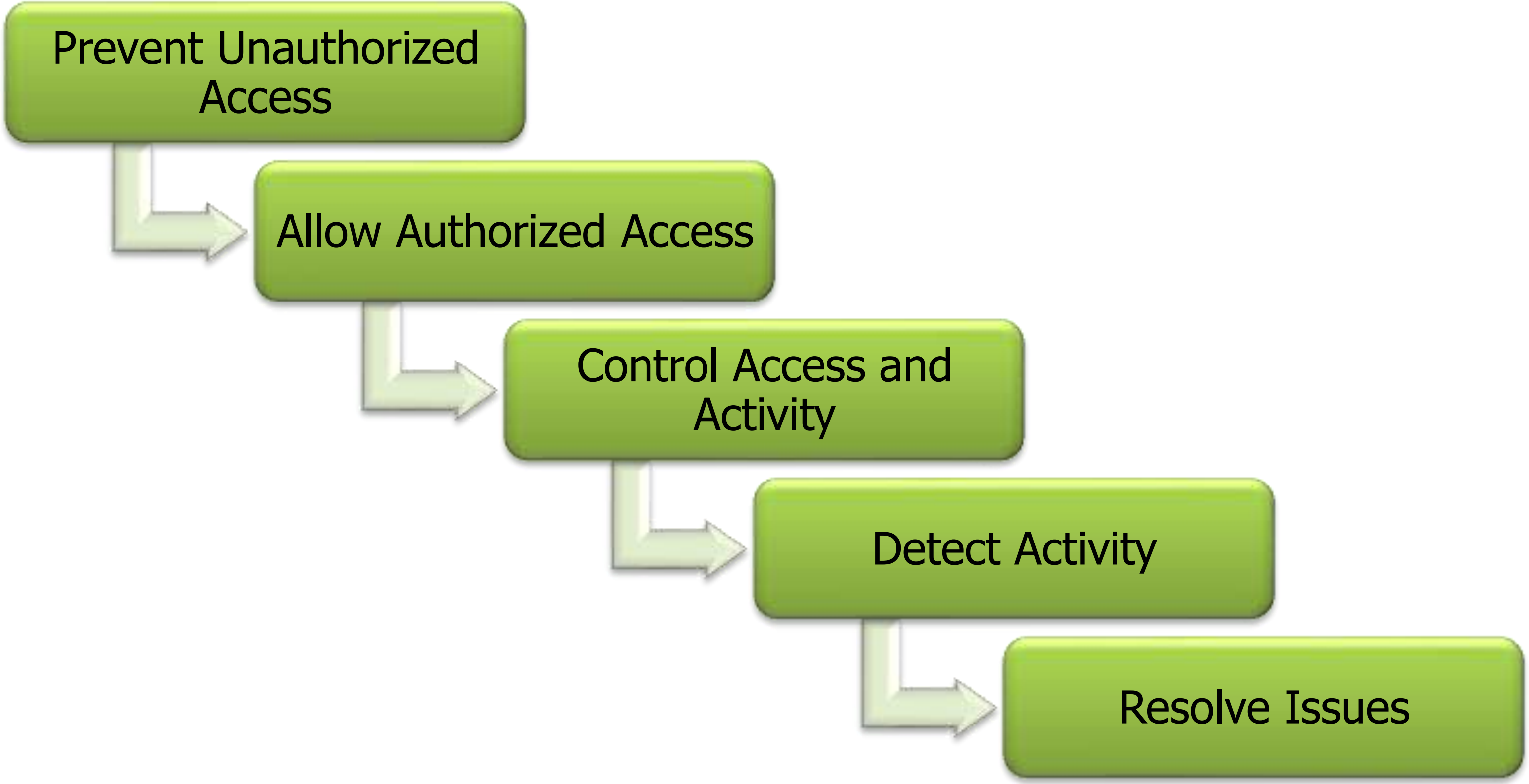
Source: http://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/

Top 10 cybersecurity facts, figures and stats for 2021

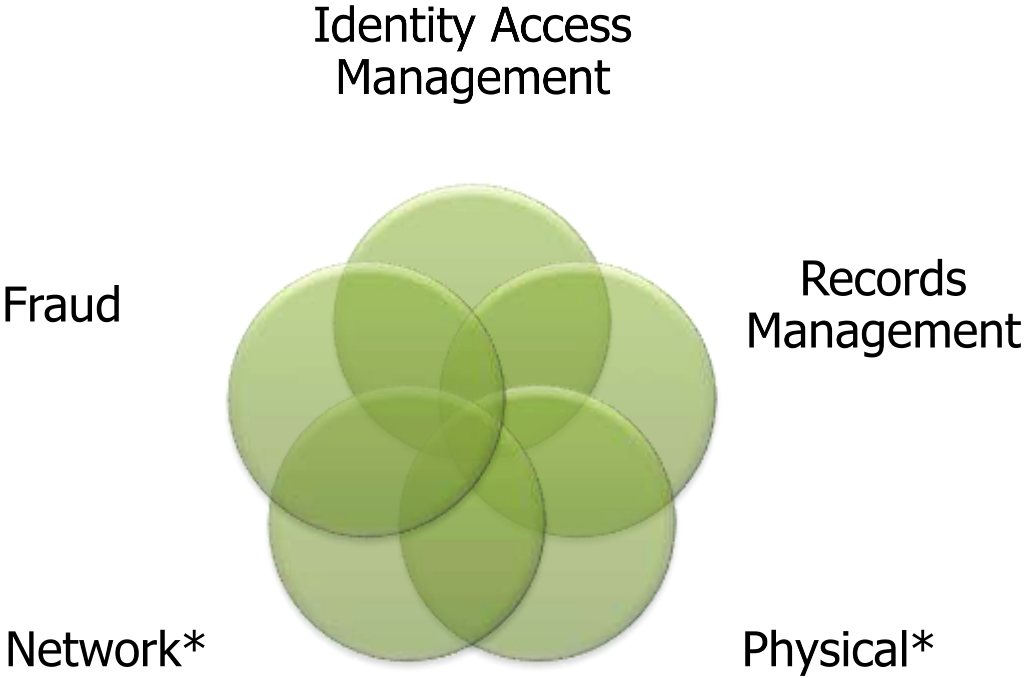
1. Small businesses are as likely of a target as corporations.
2. Phishing is still the #1 attack and up 34% in 2021
3. 75% of organizations were victims of ransomware attacks, up 61% since 2020.
4. Ransomware downtime costs an average of $250,000 per hour.
5. Employees are the leading barrier to IT security.
6. Tech fraud is up 137%.
7. Average cost of a breach in the US is $4.24 million USD.
8. It takes an average of 287 days to identify and contain a breach.
9. 18% of organizations have NOT increased cybersecurity budgets in 2021.
10. 72% of small businesses have no cybersecurity incident plan in place.

Source: https://www.gflesch.com/elevity-it-blog/cybersecurity-facts

BA Tiers of Security Awareness



Security Landscape



Identity Access Management

Records Management

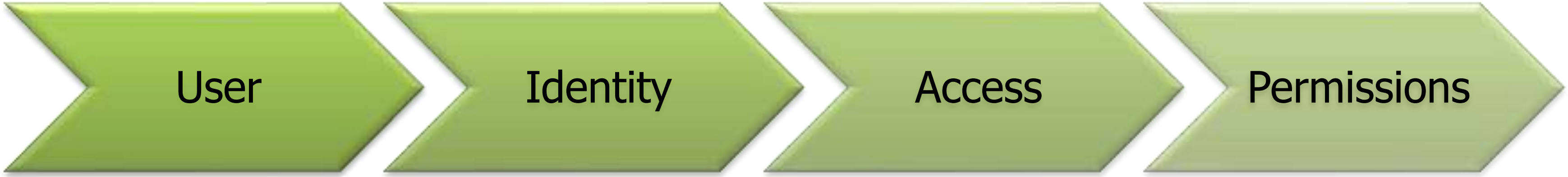
Physical*

Network*

Fraud

*Network and physical security are not typically defined in software projects.

Identity Access Management (IAM)



User → Identity → Access → Permissions

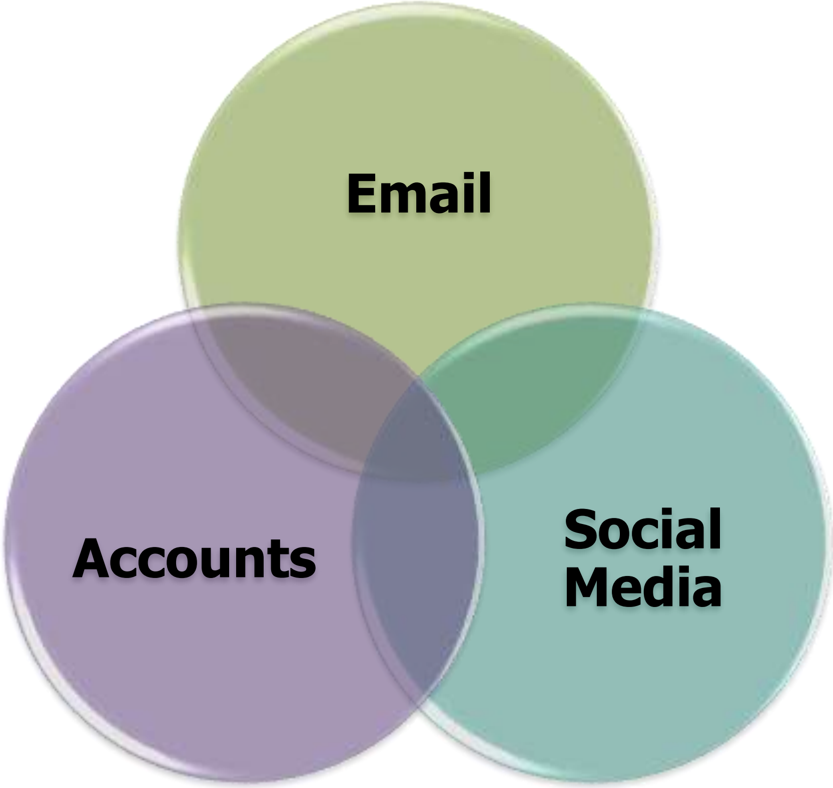
Identity - Who are you?

- 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

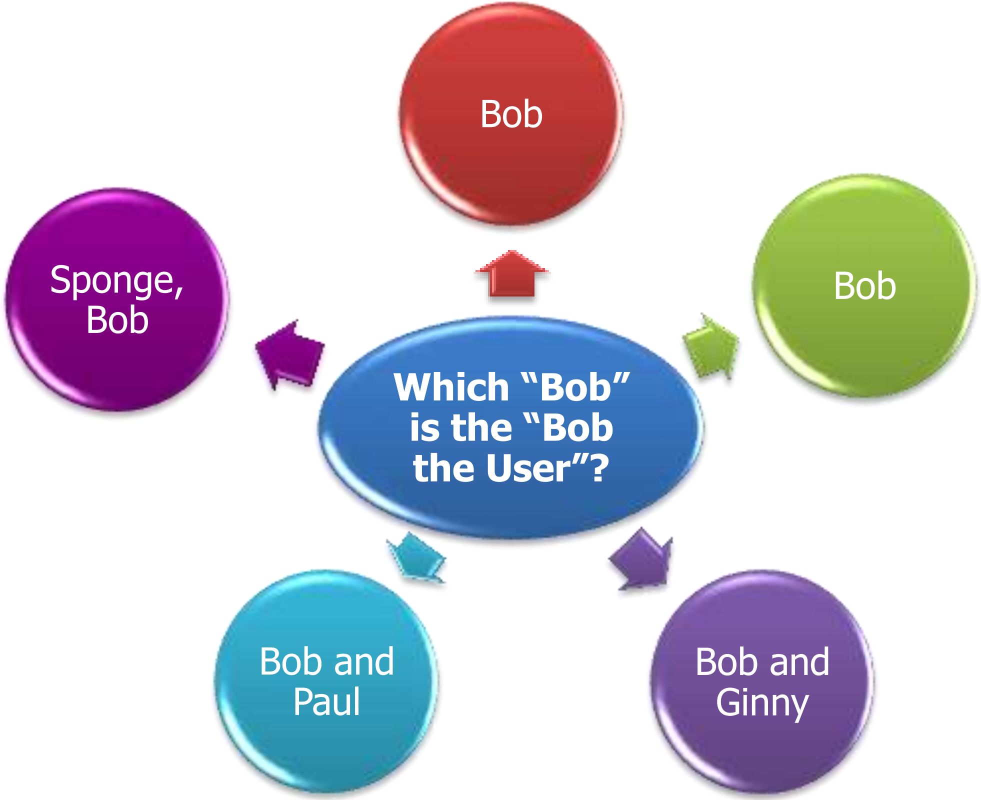
IAM – 2022 Common Passwords (Coarse Grain)



1. 123456
2. 123456789
3. qwerty
4. password
5. 12345
6. 12345678
7. 111111
8. 1234567
9. 123123
10. qwerty123
11. 1q2w3e
12. 1234567890
13. DEFAULT
14. 000000
15. abc123
16. 654321
17. 123321
18. qwertyuiop
19. Iloveyou
20. 666666

https://www.tomsguide.com/news/worst-passwords-2022

IAM – Mapping Identities (Coarse Grain)



Which “Bob” is the “Bob the User”?

Bob

Bob

Sponge, Bob

Bob and Paul

Bob and Ginny

Using Adaptive Authentication (Coarse Grain)

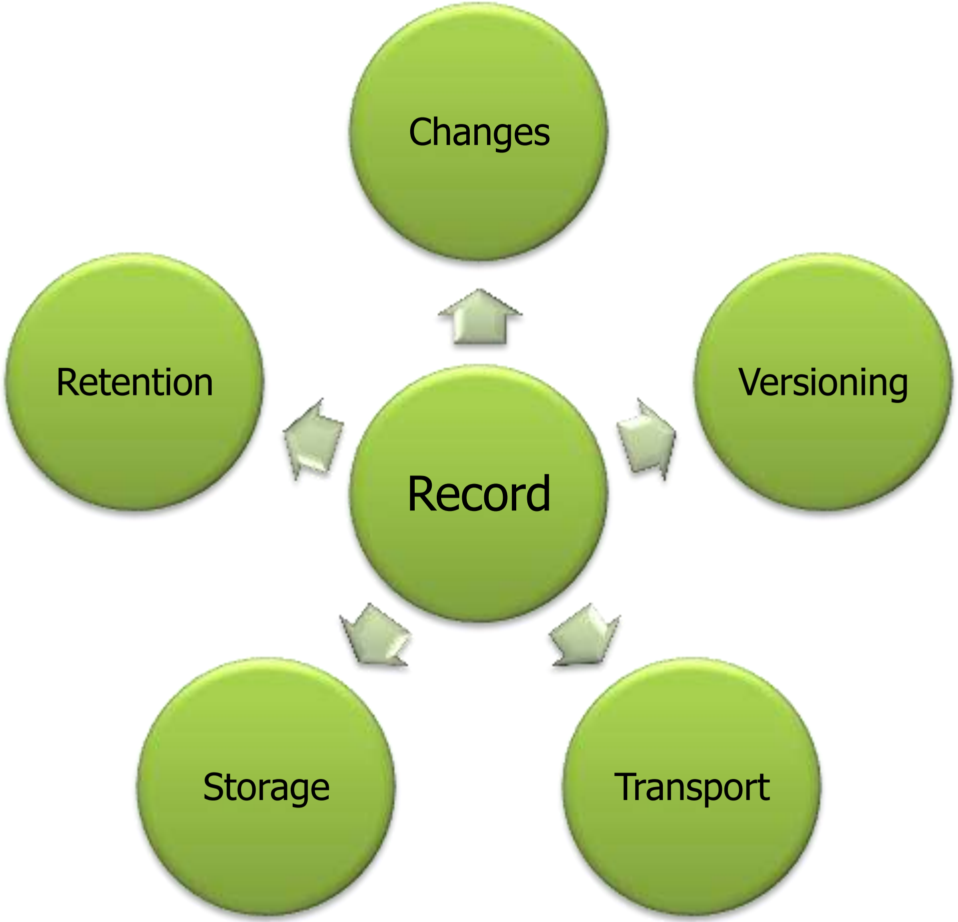
- Risk-based approach
  - Step-up authentication
- Multifactor examples
  - IP blocking: restrict access by a provider and/or network
  - Location: Geo-blocking, Geo-profiling
  - Trusted device
  - Biometric: prints, facial, shake
  - Token: Time-based key
  - Temporary key: SMS, email, phone
  - User-defined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

IAM – Entitlement Requirements (Fine Grain)

- 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"

Records Management



Copyright: wavebreakmediamicro - 123RF Stock Photo

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? For forensic analysis only?

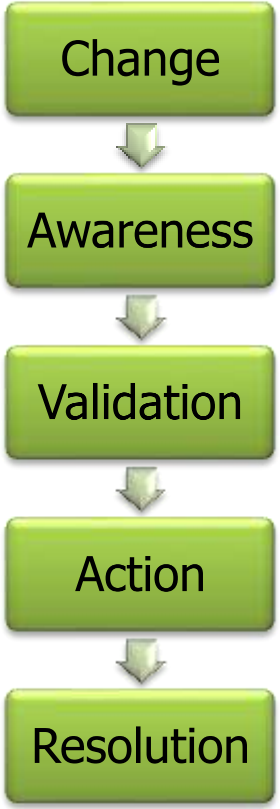
- Encryption
  - Only protects from a breach is outside your system
  - Should include seeding
  - Can be bypassed by repetitive data (e.g., password duplication)

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?

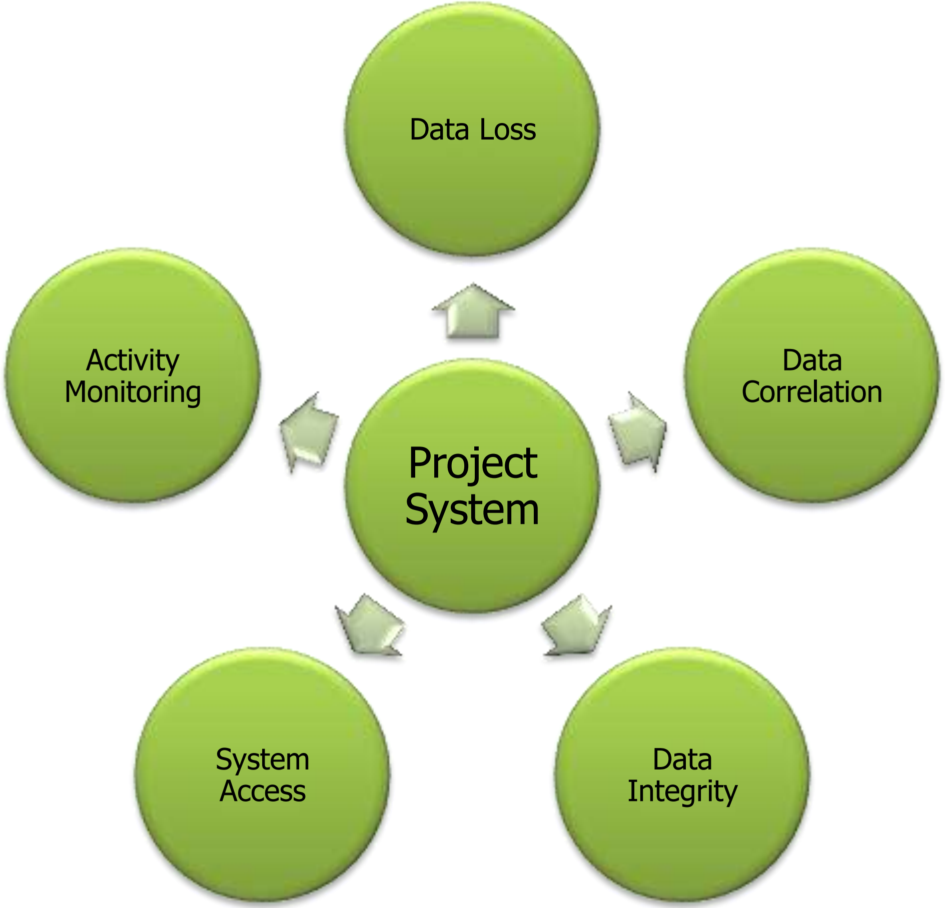
- Retention
  - Must comply with all corporate, compliance, and regulatory requirements.
  - Keeping records longer than needed can cause more harm than deletion. (e.g., legal discovery)
  - Must be consistently applied.

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



Copyright: alphaspiri - 123RF Stock Photo

Info-Tech Research Group Security Blueprints

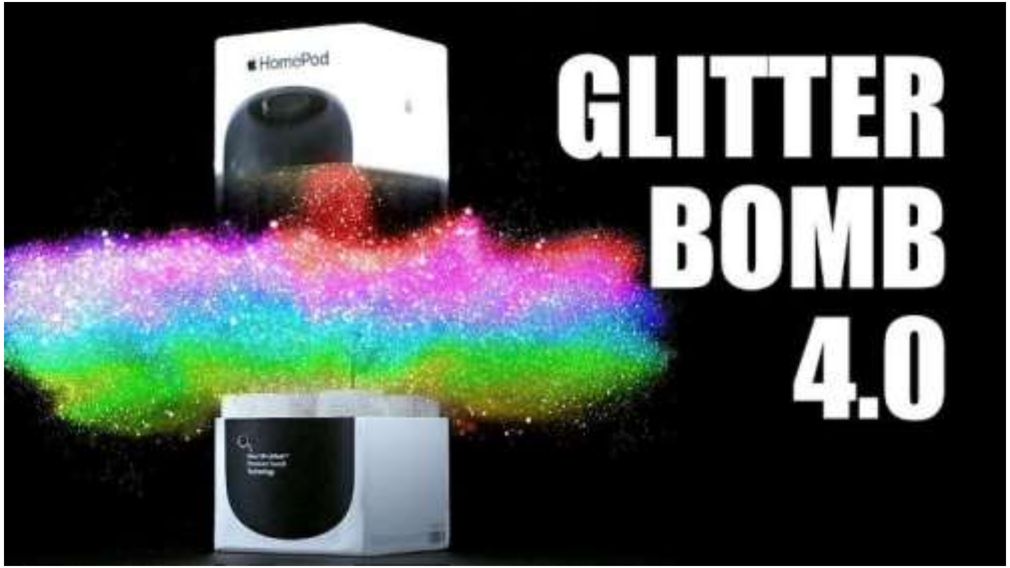
- Build an Information Security Strategy
  - Create value by aligning your strategy to business goals and business risks.
- Develop and Deploy Security Policies
  - Enhance your overall security posture with a defensible and prescriptive policy suite.
- Simplify Identity and Access Management
  - Leverage risk- and role-based access control to quantify and simplify the IAM process.
- Mature Your Identity and Access Management Program
  - Securely manage identities and their access from identity creation to deactivation.
- Embed Security Into the DevOps Pipeline
  - Shift security left to get into DevSecOps

Learn more at https://www.infotech.com/browse/security

Revenge Against the Scammers on YouTube

- Mark Rober - Pranks Destroy Scam Callers- GlitterBomb Payback

- Trilogy Media
- Jim Browning



EXPLODING Glitter Bomb 4.0 vs. Package Thieves - YouTube

Apply and Discuss

Stay Connected - Phone a Friend!

- http://EckmanGuides.com
- http://www.linkedin.com/in/hanseckman
- https://www.youtube.com/channel/UCVcJ70vc3COPzwFneWL2kqA
- https://www.facebook.com/EckmanGuides/
- https://twitter.com/hanseckman
- Hans@HansEckman.com

Scan for LinkedIn

Data Breach Hall of Shame – CSO July 2021

- Yahoo: 2013-14; 3 billion accounts
- Alibaba Date: November 2019 Impact: 1.1 billion pieces of user data
- LinkedIn Date: June 2021 Impact: 700 million users
- Sina Weibo (China Social Media) Date: March 2020 Impact: 538 million accounts
- Facebook Date: April 2019 Impact: 533 million users
- Honorable mention: Sony Pictures Entertainment, 2014: Company's inner workings exposed

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

“Top 10 List of Cybersecurity Facts for 2022”

Small businesses are as likely of a target as corporations.

Source: https://www.gflesch.com/elevity-it-blog/cybersecurity-facts

“Top 10 List of Cybersecurity Facts for 2022”

Phishing is still the #1 attack and up 34% in 2021.

Source: https://www.gflesch.com/elevity-it-blog/cybersecurity-facts

“Top 10 List of Cybersecurity Facts for 2022”

75% of organizations were victims of ransomware attacks, up 61% since 2020.

Source: https://www.gflesch.com/elevity-it-blog/cybersecurity-facts

“Top 10 List of Cybersecurity Facts for 2022”

Ransomware downtime costs an average of $250,000 per hour.

Source: https://www.gflesch.com/elevity-it-blog/cybersecurity-facts

“Top 10 List of Cybersecurity Facts for 2022”

Employees are the leading barrier to IT security.

Source: https://www.gflesch.com/elevity-it-blog/cybersecurity-facts

“Top 10 List of Cybersecurity Facts for 2022”

Tech fraud is up 137%.

Source: https://www.gflesch.com/elevity-it-blog/cybersecurity-facts

“Top 10 List of Cybersecurity Facts for 2022”

Average cost of a breach in the US is $4.24 million USD.

Source: https://www.gflesch.com/elevity-it-blog/cybersecurity-facts

Stay Connected - Phone a Friend!

- http://EckmanGuides.com
- http://www.linkedin.com/in/hanseckman
- https://www.youtube.com/channel/UCVcJ70vc3COPzwFneWL2kqA
- https://www.facebook.com/EckmanGuides/
- https://twitter.com/hanseckman
- Hans@HansEckman.com

Scan for LinkedIn

“Top 10 List of Cybersecurity Facts for 2022”

It takes an average of 287 days to identify and contain a breach.

Source: https://www.gflesch.com/elevity-it-blog/cybersecurity-facts

“Top 10 List of Cybersecurity Facts for 2022”

18% of organizations have NOT increased cybersecurity budgets in 2021.

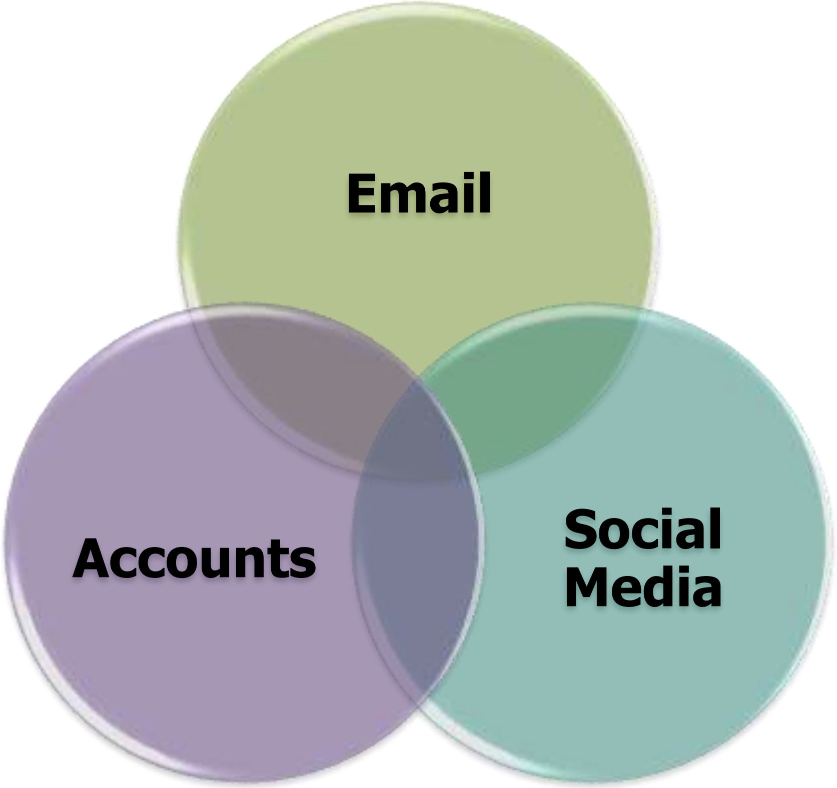
Source: https://www.gflesch.com/elevity-it-blog/cybersecurity-facts

“Top 10 List of Cybersecurity Facts for 2022”

72% of small businesses have no cybersecurity incident plan in place.

Source: https://www.gflesch.com/elevity-it-blog/cybersecurity-facts

IAM – 2022 Common Passwords (Coarse Grain)



- 123456
- 123456789
- qwerty
- password
- 12345
- 12345678
- 111111
- 1234567
- 123123
- qwerty123

11. 1q2w3e
12. 1234567890
13. DEFAULT
14. 000000
15. abc123
16. 654321
17. 123321
18. qwertyuiop
19. Iloveyou
20. 666666

https://www.tomsguide.com/news/worst-passwords-2022

Cybersecurity facts and figures for 2022, statistics, and trends

Opinion poll: Cyber threats will not only continue to massively attack organizations after 2022, but they will also increase in strength.

Source: https://www.ecsoffice.com/cybersecurity-statistics-and-trends/

Cybersecurity facts and figures for 2022, statistics, and trends

Ransomware will continue to exist despite the vast availability of deterrent resources. Attacks could become more sophisticated, targeting companies of all sizes.

Actual losses can be deplorable. Behind this type of attack is an organized and professional criminal network developer.

Source: https://www.ecsoffice.com/cybersecurity-statistics-and-trends/

Cybersecurity facts and figures for 2022, statistics, and trends

It is much easier to get someone to install spyware without realizing their mistake than to look for technical vulnerabilities. Therefore, phishing campaigns will be quite common in 2022.

Source: https://www.ecsoffice.com/cybersecurity-statistics-and-trends/

Cybersecurity facts and figures for 2022, statistics, and trends

Cybercriminals will target virtual currencies as they continue to grow in popularity and active demand around the world. With the increase in asset holders, cryptocurrency wallet management solutions and transactions, this is like a personal invitation for hackers.

Source: https://www.ecsoffice.com/cybersecurity-statistics-and-trends/

Stay Connected - Phone a Friend!

- http://EckmanGuides.com
- http://www.linkedin.com/in/hanseckman
- https://www.youtube.com/channel/UCVcJ70vc3COPzwFneWL2kqA
- https://www.facebook.com/EckmanGuides/
- https://twitter.com/hanseckman
- Hans@HansEckman.com

Scan for LinkedIn

Cybersecurity facts and figures for 2022, statistics, and trends

In 2020, 97% of companies face mobile threats using multiple attack vectors highlighted this trend. Not to mention, the remote operation has led to an increase in the attack surface. Every available device offers an entry point.

Source: https://www.ecsoffice.com/cybersecurity-statistics-and-trends/

Cybersecurity facts and figures for 2022, statistics, and trends

While the cloud has many benefits, it is also becoming increasingly standardized. This is a boon for cybercriminals, who can more easily test their attacks against precisely standardized solutions. In addition, vulnerabilities in the cloud make massive attacks possible.

Source: https://www.ecsoffice.com/cybersecurity-statistics-and-trends/

Cybersecurity facts and figures for 2022, statistics, and trends

Deepfake technology is one of the top riskiness for 2022. It's about video or audio recordings made or altered by artificial intelligence that can create false content made of credible. Aimed at manipulating, misinforming and discrediting populations and organizations, Deepfake can lead to the worst fears of international destabilization.

Source: https://www.ecsoffice.com/cybersecurity-statistics-and-trends/

Cybersecurity facts and figures for 2022, statistics, and trends

Attacks on the supply chain are likely to continue. A sector undergoing a powerful digital transformation has become a target for hackers. Rather than confronting large security-equipped companies, they are targeting suppliers who are likely to have sensitive data (accountants, lawyers, etc.).

Source: https://www.ecsoffice.com/cybersecurity-statistics-and-trends/

Cybersecurity facts and figures for 2022, statistics, and trends

Cybercriminals will continue to use them to infiltrate organizations through fake profiles. Misinformation and fake news campaigns will continue to be a source of mass phishing or fraud. We saw this in the example of fake vaccination certificates this year.

Source: https://www.ecsoffice.com/cybersecurity-statistics-and-trends/

Cybersecurity facts and figures for 2022, statistics, and trends

In December 2021, cybercriminals stole over 35 million euros from a French real estate developer. This is just the latest in numerous cyberattacks around the world that are affecting a growing number of businesses and organizations.

Source: https://www.ecsoffice.com/cybersecurity-statistics-and-trends/

Cybersecurity facts and figures for 2022, statistics, and trends

The National Agency for Information Systems Security (ANSSI) found a 255% increase in ransomware attacks on organizations in 2020 compared to 2019.

Source: https://www.ecsoffice.com/cybersecurity-statistics-and-trends/

Cybersecurity facts and figures for 2022, statistics, and trends

A business interruption after a cyberattack has a significant impact on a company's annual turnover. In the time to restore a computer system and restore backup data (if any), a company loses an average of 27% of its annual revenue.

Source: https://www.ecsoffice.com/cybersecurity-statistics-and-trends/

Stay Connected - Phone a Friend!

- http://EckmanGuides.com
- http://www.linkedin.com/in/hanseckman
- https://www.youtube.com/channel/UCVcJ70vc3COPzwFneWL2kqA
- https://www.facebook.com/EckmanGuides/
- https://twitter.com/hanseckman
- Hans@HansEckman.com

Scan for LinkedIn

Cybersecurity facts and figures for 2022, statistics, and trends

60% of SMBs attacked do not recover and file for bankruptcy within 18 months of the attack.

Source: https://www.ecsoffice.com/cybersecurity-statistics-and-trends/

Cybersecurity facts and figures for 2022, statistics, and trends

Half of the U.S. companies affected by the cyberattack have refused to file a complaint. The other 50% are prepared for upcoming hacker attacks.

Source: https://www.ecsoffice.com/cybersecurity-statistics-and-trends/

Cybersecurity facts and figures for 2022, statistics, and trends

Nearly half of employees have been duped by phishing attempts while working from home.

Source: https://www.ecsoffice.com/cybersecurity-statistics-and-trends/

Cybersecurity facts and figures for 2022, statistics, and trends

Ransomware continues to grow at an alarming rate, accounting for at least 79% of all reported cyberattacks, according to Sophos. According to the latest ANSSI data, Ransomware attacks increased by 60% in the first six months of 2021, after 255% in 2020.

Source: https://www.ecsoffice.com/cybersecurity-statistics-and-trends/