Main goals of Cyber Security ?

(what is this course about)

Learn why it is important to protect the CIA of data, and how to do it.

- Steganography
- Cryptography
- Access Control / Passwords
- Policy ...

$$$ is at the bottom line !!!

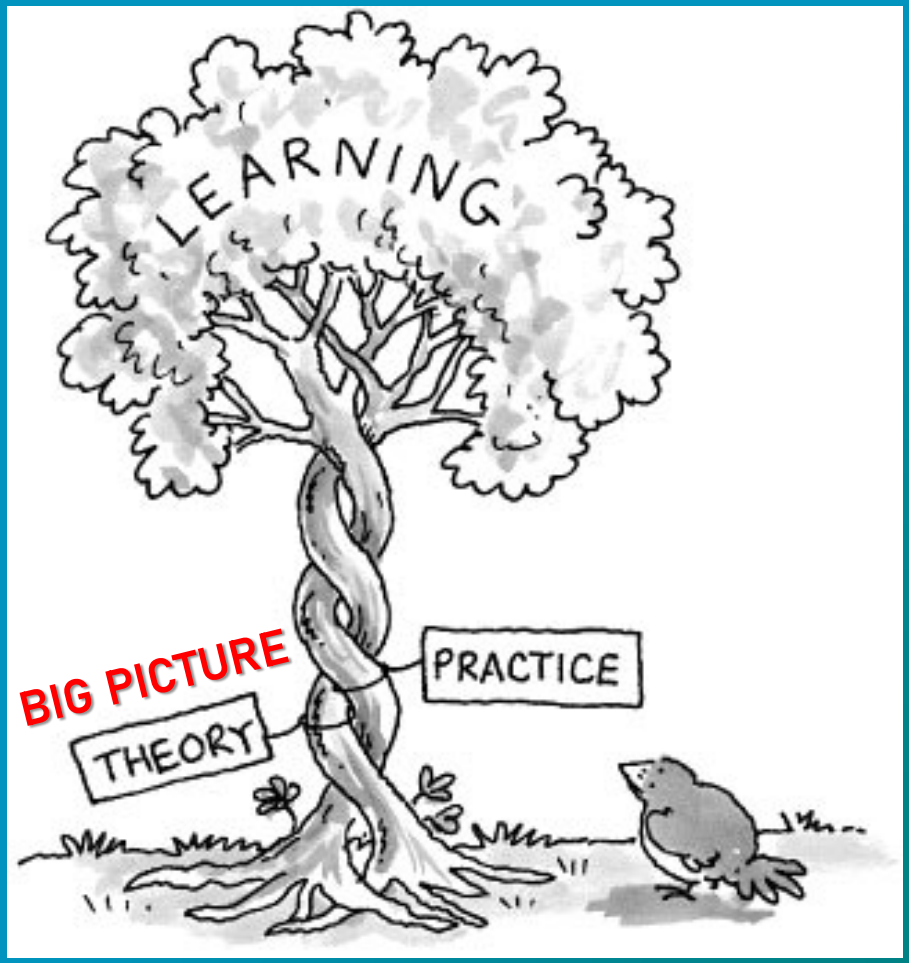
(prevent financial losses)

- IT Security Risk Management

What to expect from this course ?

(for CSec students)

1.



2.

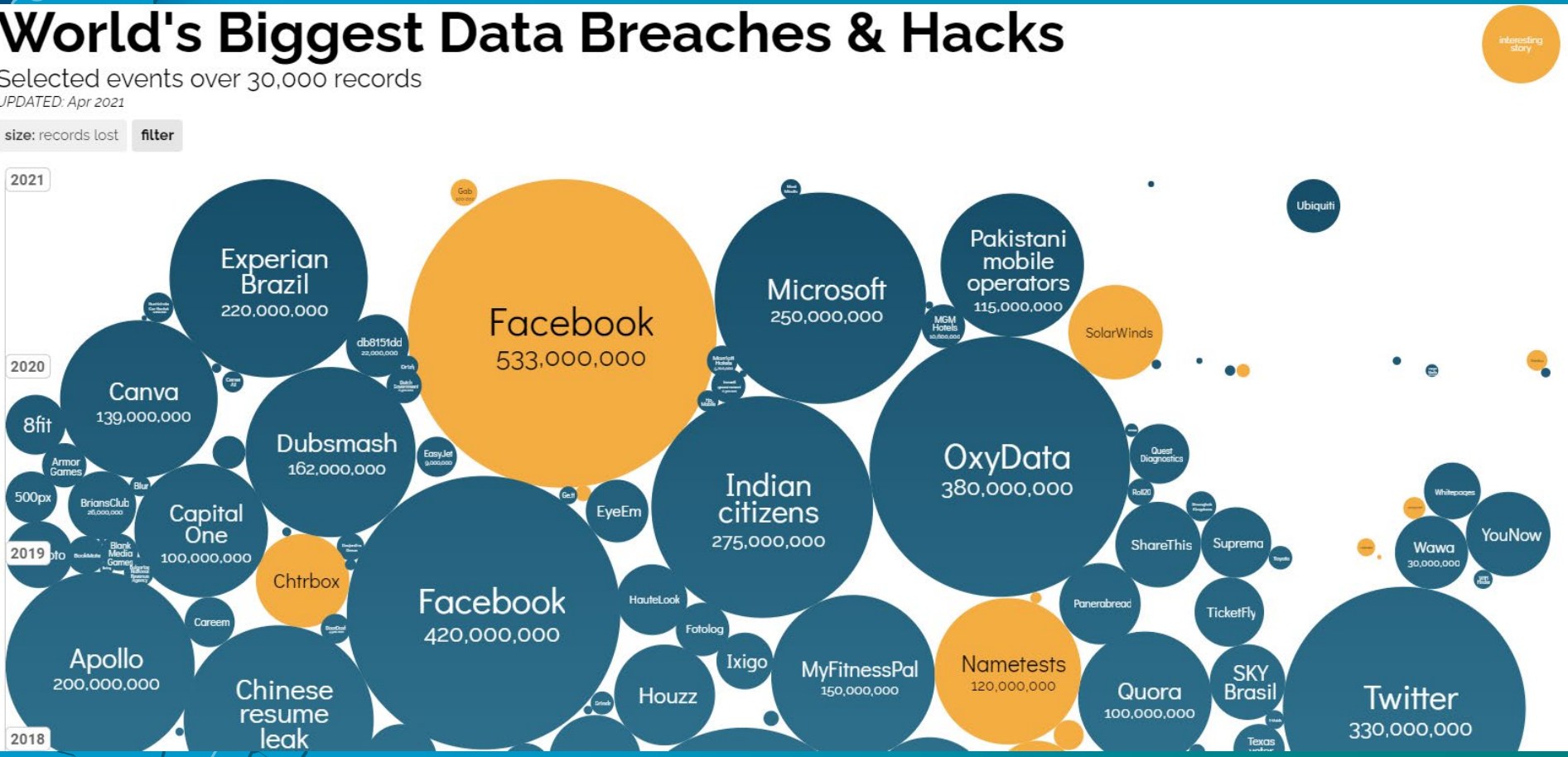
Cyber Security = cat vs. mouse (defender vs. offender) game that never ends …

You should be able to think like both !!!

3. World's Biggest Data Breaches & Hacks

Select losses greater than 30,000 records
Last updated: 11th May 2020

http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/



https://en.wikipedia.org/wiki/List_of_data_breaches

List of data breaches

From Wikipedia, the free encyclopedia

This is a list of **data breaches**, using data compiled from various sources, including press reports, government news releases, and mainstream news articles. The list includes those involving the theft or compromise of 30,000 or more records, although many smaller breaches occur continually. Breaches of large organizations where the number of records is still unknown are also listed. The various methods used in the breaches are also listed, with hacking being the most common.

Most breaches occur in North America. It is estimated that the average cost of a data breach will be over $150 million by 2020, with the global annual cost forecast to be $2.1 trillion.[1][2] It is estimated that in first half of 2018 alone, about 4.5 billion records were exposed as a result of data breaches.[3] In 2019, a collection of 2.7 billion identity records, consisting of 774 million unique email addresses and 21 million unique passwords, was posted on the web for sale.[4]

Entity	Year	Records	Organization type	Method	Sources
Ancestry.com	2021	300,000	web	poor security	[23]
Ankle & Foot Center of Tampa Bay, Inc.	2021	156,000	healthcare	hacked	[25]
AOL	2021	92,000,000	web	inside job, hacked	[28][29]
AOL	2021	20,000,000	web	accidentally published	[30]
Apple, Inc./BlueToad	2021	12,367,232	tech, retail	accidentally published	[32]
Apple	2021	275,000	tech	hacked	[33]
Apple Health Medicaid	2021	91,000	healthcare	poor security	[34]
T-Mobile	2021	45,000,000	telecom	hacked	[325]
Microsoft Exchange servers	2021	unknown		zero-day vulnerabilities	[396]
Health Service					[397]

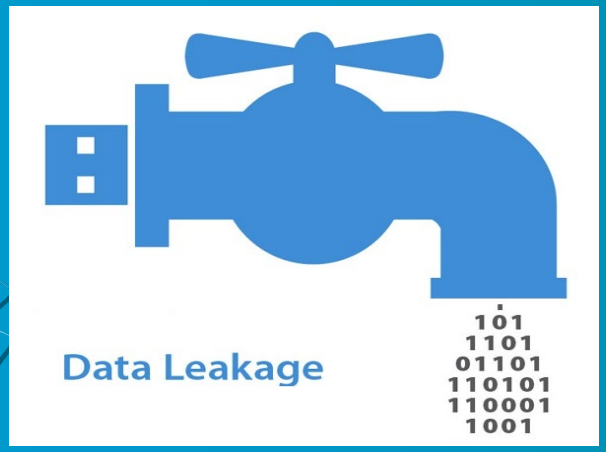
Data Breach vs. Hack

Are they the same thing ?

Are they related ?

Can one happen without the other ?

Data Breach
||
Data Leak vs. Data Loss



What is the relationship ?

Quiz 0:

What happens in the case of a ransomware attack ?

a) data loss only

Victim refuses to pay ransom.
Attacker destroys data without 'looking' or 'leaking' (honest hacker).

b) data leakage only

Victim pays ransom and gets data back – no data lost!
But, attacker 'looks at' or 'leaks' data to Dark Web (dishonest hacker).

c) both data loss and data leakage

Victim refuses to pay ransom.
Attacker destroys data & 'looks at' or 'leaks' data (vengeful hacker).

d) neither data loss nor data leakage

Victim pays ransom and gets data back – no data lost!
Attacker does not 'look at' or 'leaks' the data (very honest hacker ☺).

e) any of the above could happen

Data Breach

- data breach (data leak) = exposing of sensitive, confidential and/or protected data to someone who should not have access to that data

  * could be deliberate or unintentional !

  * common type of leaked information:
    1. financial data (e.g., credit card numbers)
    2. medical or personal health information
    3. personally identifiable information (PII)
    4. intellectual property

Data Breach (cont.)

- most common causes / actors:

  * an accidental insider

    not problematic

    - e.g., an employee using a co-worker's computer & accessing files without having proper authorization, NO information is leaked outside the company

    problematic !

    - e.g., an employee fooled into disclosing data to a malicious actor – information leaked outside …

  * a malicious insider

    problematic !

    - e.g., an employee purposely accesses and/or shares data with the intent of causing harm to an individual or company – may have legitimate authorization

  * a malicious outsider

    problematic !

    - e.g., a hacker uses various attack vectors to gather information from a network or an individual (e.g., finds vulnerability in a server, gains access to net., …)

Data Breach (cont.)

Users / Customers

Should you (as an individual) worry about data breaches?

a) your university suffers a data breach

your PII compromised, your grades leaked
can lead to identity theft or blackmail …

b) your bank suffers a data breach

your online banking credentials stolen (user login, password)
your money gone …

c) your hospital suffers a data breach

your health information stolen
your chances of getting employed reduced …

Why should breached companies worry?

Data Breach (cont.)

- common costs / damages:

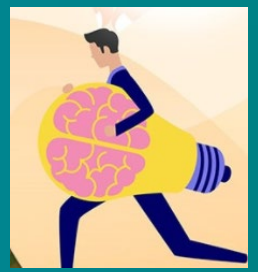
for company that suffered the breach

* direct, shorter term

1. operational disruption
2. cyber-security investigations
3. attorney fees
4. government fines
5. drop in stock price, …

* indirect, longer term

1. damage to brand and reputation
2. loss of intellectual property
3. increased insurance premium, …

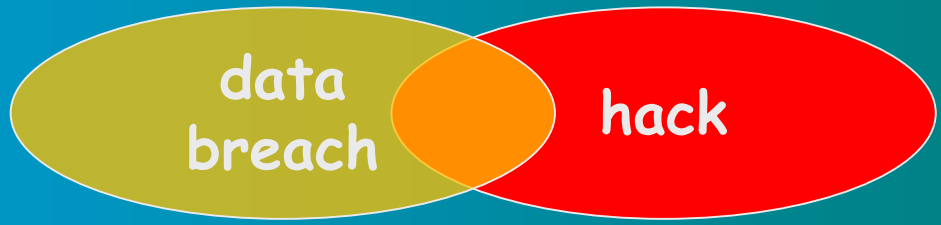


Hack

- hack = identification & exploitation of weaknesses in a computer system or a network in order to achieve a nefarious objective

  * an intentional attack typically conducted by a malicious outsider

  * could, but does not have to, result in a data breach / leak (e.g., DDoS, logic bomb)



Hack (cont.)

* weaknesses commonly exploited in a hack:

1. weak or compromised credentials
2. careless / untrained employees (social engineering)
3. missing or poor encryption
4. misconfiguration (e.g., in a firewall)
5. vulnerabilities (e.g., in servers or workstations)
6. third- or fourth- party vendors, …

Case Study 1: First American Financial (2019)

data breach (leak) but NOT hack

there was a weakness but was not intentionally or maliciously exploited

* First American is a leading insurance provider to the real estate and mortgage industries
* the company left unintentionally exposed 885 million digitized mortgage documents dating back to 2003
* the leak was not discovered by security researchers, nor did it appear on the dark web – it was discovered by a real estate developer Ben Shoval who noticed that simply changing a single digit in the document URL sent to him sensitive documents belonging to other people

https://www.cpomagazine.com/cyber-security/security-oversight-at-first-american-causes-data-leak-of-900-million-records/

Case Study 1: First American Financial (2019)

"There was no clear evidence that a malicious third-party gained access to files without permission."

https://www.forbes.com/sites/ajdellinger/2019/05/26/understanding-the-first-american-financial-data-leak-how-did-it-happen-and-what-does-it-mean/#4836aa17567f

* so, should anybody (company or consumers) worry about this leak?!

  - it's possible that information from First American could have been collected and indexed by bots over a period of time
  - someone could have performed a 'low-and-slow' attack to avoid detection (by requesting only a few documents at a time), and is willing to wait …

Case Study 2: Desjardins (2019)

Desjardins Insurance

data breach with(out) hack

* largest North Americ. federat. of credit unions
* in 2019 an ill-intended IT employee collected PII of more than 4.3 million people & businesses (> 40% of company's clients & members) and shared it with others outside the company
* suspected employee created a scheme to win trust of his colleagues, and then using their & his own access, collected and exfiltrated data

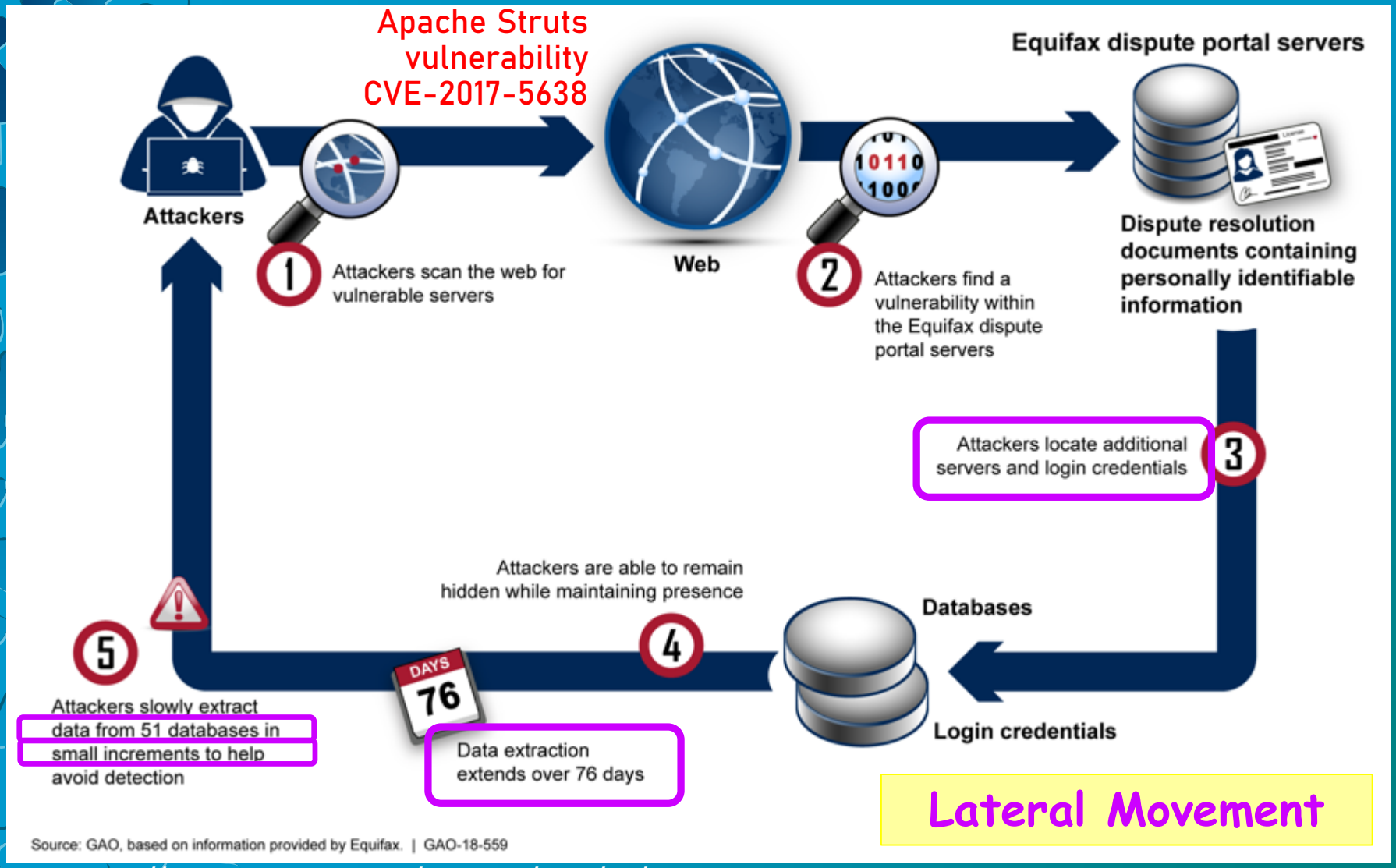
"… information was originally stored in two data warehouses to which the employee in question had limited access, the commissioner said.
However, other employees, in the course of their work, would regularly copy that information onto a shared computer drive. "
https://globalnews.ca/news/7520414/desjardins-data-breach-privacy-watchdog-probe/

Case Study 3: Equifax (2017)

data breach AND hack

* multinational consumer credit reporting agency
* on March 7, the Apache Software Foundation released a patch for Struts vulnerability; on March 9, Equifax administrators were told to apply the patch to any affected systems; the employee who should have done so didn't
* forensics analysis (after the fact) showed that the initial Equifax hack occurred on March 10
* from March to July 2017, outside attackers gained access to multiple Equifax databases and managed to exfiltrate PII of over 160 million people (more than 40% of USA population)

Case Study 3: Equifax (2017)



https://blogs.vmware.com/security/2019/03/equifax-data-breach-and-vmware-appdefense.html

Case Study 3: Equifax (2017)

Apache Struts is a free and open-source framework used to build Java web applications.

The Jakarta Multipart parser in Apache Struts 2 2.3.x before 2.3.32 and 2.5.x before 2.5.10.1 has incorrect exception handling and error-message generation during file-upload attempts, which allows remote attackers to execute arbitrary commands via a crafted Content-Type, Content-Disposition, or Content-Length HTTP header, as exploited in the wild in March 2017 with a Content-Type header containing a #cmd= string.

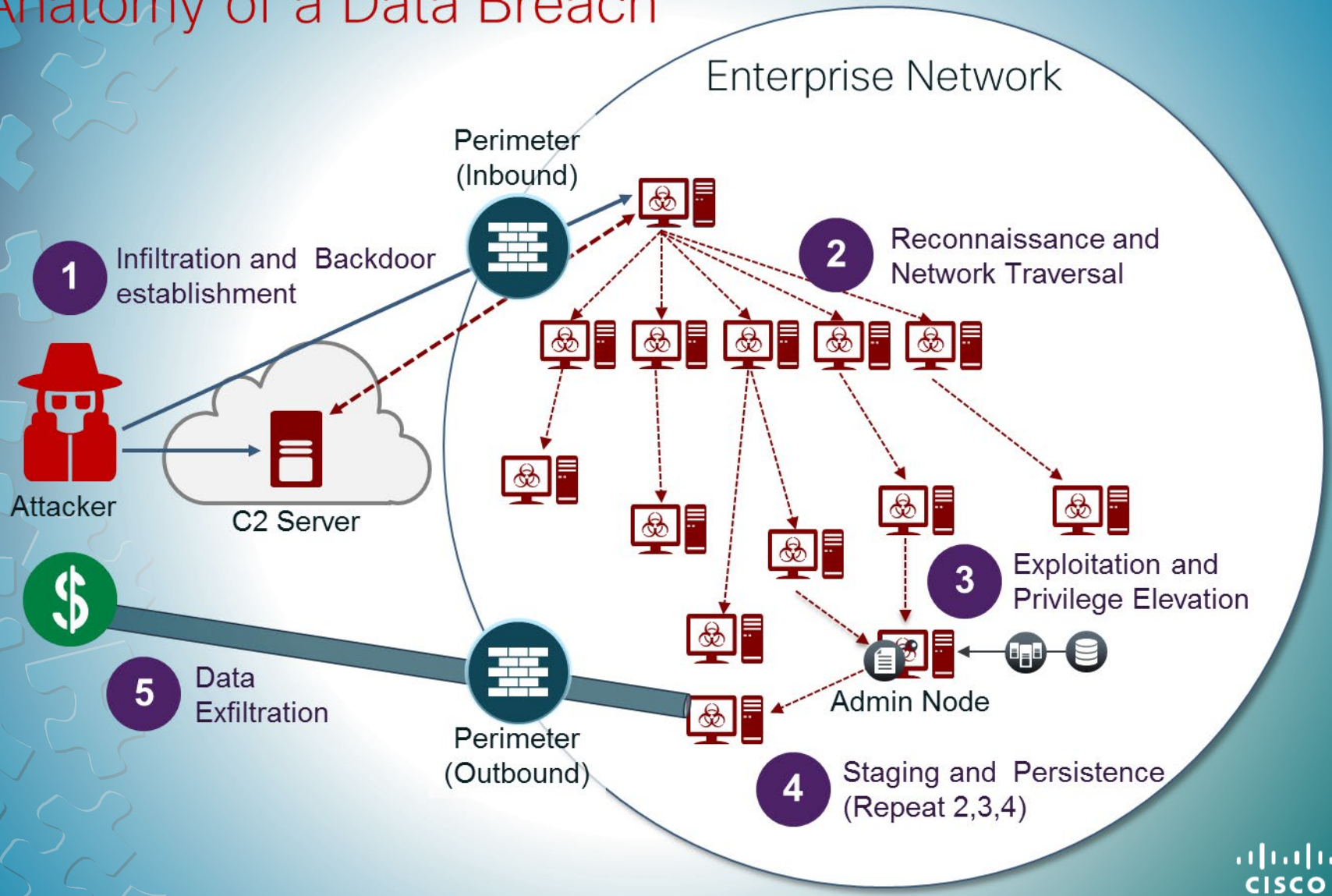
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5638

Who was responsible for the Equifax data breach?

As soon as the Equifax breach was announced, infosec experts began keeping tabs on dark web sites, waiting for huge dumps of data that might be connected to it. They waited, and waited, but the data never appeared. This gave rise to what's become a widely accepted theory: that Equifax was breached by Chinese state-sponsored hackers whose purpose was espionage, not theft.

https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html

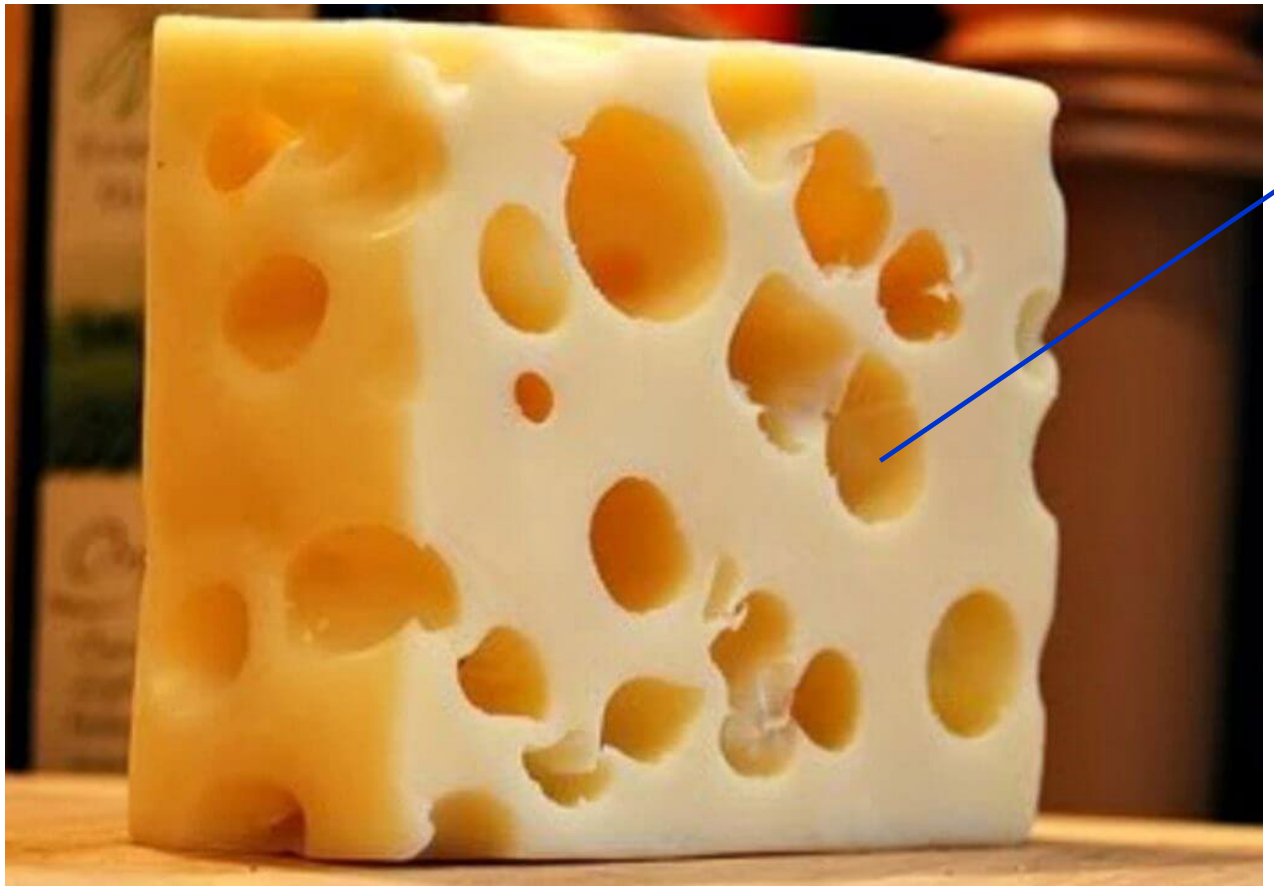
Anatomy of a Data Breach



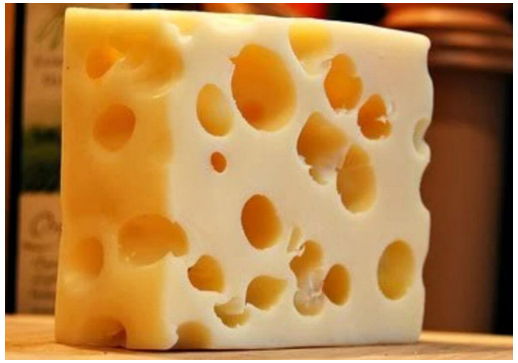
https://news-blogs.cisco.com/networking/149268

Security of the Internet and its components:

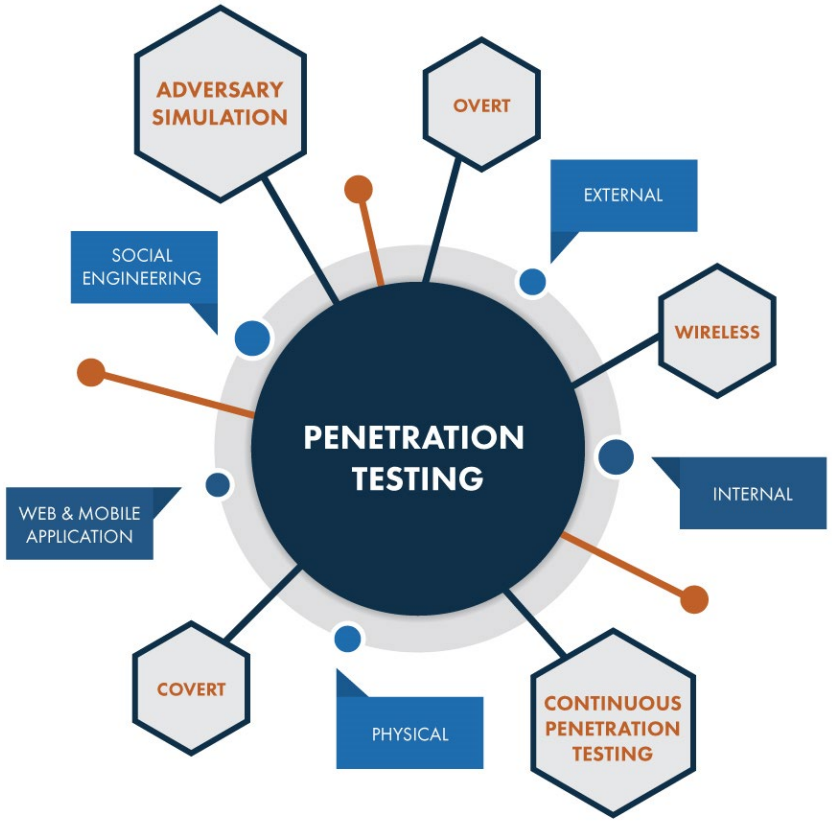
How are the 'holes' identified ???



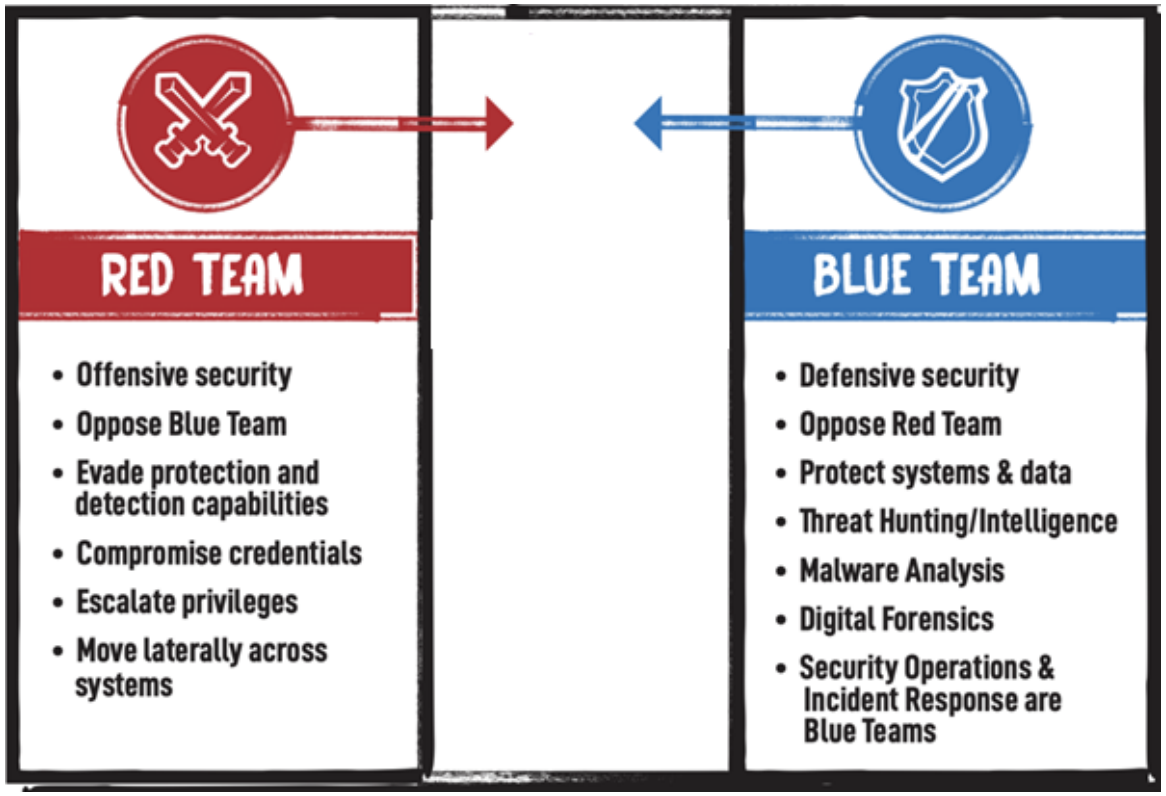
Could be identified by 'bad' guys or 'good' guys.



‘Smart’ companies are wiling to pay specialized (trusted) teams
to try to hack them.



https://www.synercomm.com/network-penetration-testing/



https://pentestmag.com/red-teaming-10000-feet/

Both pentesting and 'red-team/blue-team' exercises happen only periodically (over limited period of time).

(curious) security researchers

regulated vulnerability disclosure

organization

Security researchers should keep looking for various vulnerabilities in various 'components' of the Internet.

Security researchers should know that poking around a software or software system could put them in trouble.

'Smart' organization should know that it is impossible to build a bulletproof software or software-system.

'Smart' organization should incentivize security researchers to discover and report vulnerabilities in their software products and systems => **Bug Bounty !!!**

OWASP (Open Web Application Security Project):
Vulnerability Disclosure Cheat Sheet

https://cheatsheetseries.owasp.org/cheatsheets/Vulnerability_Disclosure_Cheat_Sheet.html

Organisations should:

- Provide a clear method for researchers to securely report vulnerabilities.
- Clearly establish the scope and terms of any bug bounty programs.
- Respond to reports in a reasonable timeline.
- Communicate openly with researchers.
- Not threaten legal action against researchers.
- Request CVEs where appropriate.
- Publish clear security advisories and changelogs.
- Offer rewards and credit.

OWASP = online community that produces freely-available articles, methodologies, documentation, tools, and technologies in the field of web application security.

https://www.securitymagazine.com/articles/89372-bug-bounty-programs-an-emerging-best-practice

Cyber Security News | Cyber Tactics | Cyber

Bug Bounty Programs: An Emerging Best Practice

Google Application Security

Google Vulnerability Reward Program (VRP) Rules

We have long enjoyed a close relationship with the security research community. To honor all the cutting-edge external contributions that help us keep our users safe, we maintain a Vulnerability Reward Program for Google-owned web properties, running continuously since November 2010.

Qualifying vulnerabilities

Any design or implementation issue that substantially affects the confidentiality or integrity of user data is likely to be in scope for the program. Common examples include:

- Cross-site scripting,
- Cross-site request forgery,
- Mixed-content scripts,
- Authentication or authorization flaws,
- Server-side code execution bugs.

Why is this important ??

Reward amounts for security vulnerabilities

New! Vulnerabilities in the Google Cloud Platform are also eligible for additional rewards under the GCP VRP Prize. The total prize money is $313,337 including a top prize of $133,337. See our announcement and the official rules for details and nominate your vulnerability write-ups for the prize here.

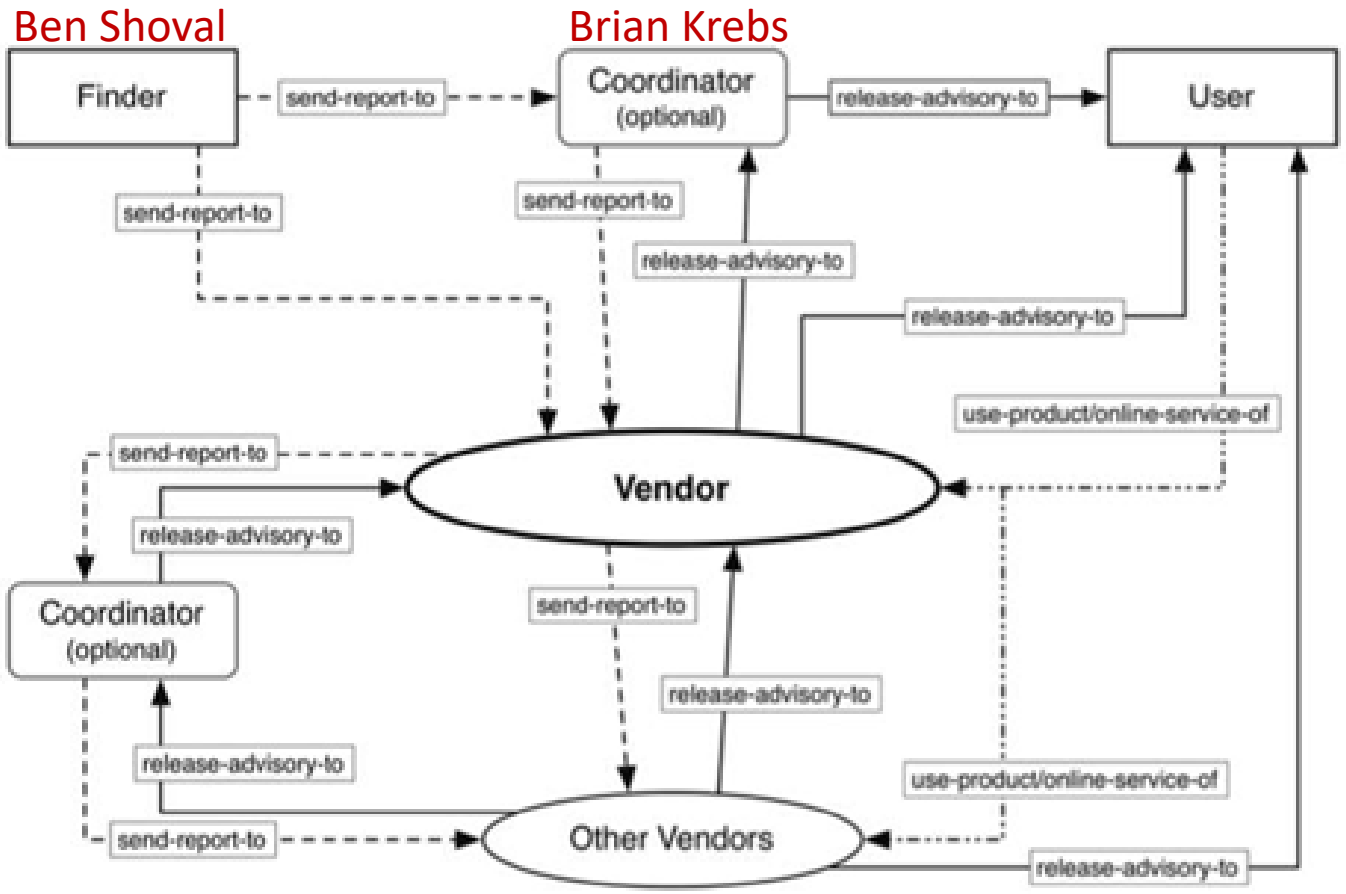
OWASP (Open Web Application Security Project):
Vulnerability Disclosure Cheat Sheet

https://cheatsheetseries.owasp.org/cheatsheets/Vulnerability_Disclosure_Cheat_Sheet.html

Researchers should:

- Ensure that any testing is legal and authorised.
- Respect the privacy of others.
- Make reasonable efforts to contact the security team of the organisation.
- Provide sufficient details to allow the vulnerabilities to be verified and reproduced.
- Not demand payment or rewards for reporting vulnerabilities outside of an established bug bounty program.

ISO/IEC 29147 and ISO/IEC 30111: Vulnerability Disclosure & Handling Standards for Vendors



The standard provides guidance to vendors on how to disclose vulnerabilities in products and services. The goal is to reduce the risk associated with exploiting vulnerabilities.

https://www.first.org/global/sigs/vulnerability-coordination/multiparty/FIRST-Multiparty-Vulnerability-Coordination.pdf

OWASP (Open Web Application Security Project):
Vulnerability Disclosure Cheat Sheet

Methods of Disclosure

Private Disclosure

In the private disclosure model, the vulnerability is reported privately to the organisation. The organisation may choose to publish the details of the vulnerabilities, but this is done at the discretion of the organisation, not the researcher, meaning that many vulnerabilities may never be made public. The majority of bug bounty programs require that the researcher follows this model.

Full Disclosure

With the full disclosure approach, the full details of the vulnerability are made public as soon as they are identified. This means that the full details (sometimes including exploit code) are available to attackers, often before a patch is available. The full disclosure approach is primarily used in response of organisations ignoring reported vulnerabilities, in order to put pressure on them to develop and publish a fix.

Question:

Is ‘private disclosure’ the best way to go??

Think of:

- Vulnerability may be ‘quietly’ patched, without publicizing the scale and severity – the public still ‘in the dark’ …

- Companies may refuse to address/patch every vulnerability …

Methods of Disclosure

Responsible or Coordinated Disclosure

Responsible disclosure attempts to find a reasonable middle ground between these two approaches. With responsible disclosure, the initial report is made privately, but with the full details being published once a patch has been made available (sometimes with a delay to allow more time for the patches to be installed).

In many cases, the researcher also provides a deadline for the organisation to respond to the report, or to provide a patch. If this deadline is not met, then the researcher may adopt the full disclosure approach, and publish the full details.

Google's Project Zero adopts a similar approach, where the full details of the vulnerability are published after 90 days regardless of whether or not the organisation has published a patch.