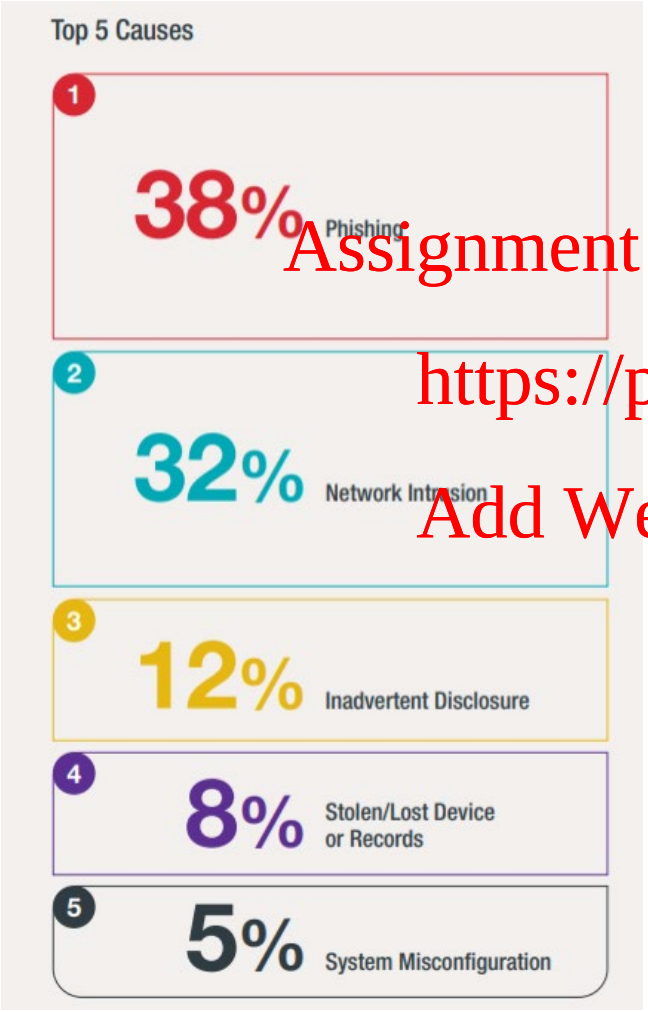
Introduction (cont.)

Causes of Incident Response in Cyber Security



Humans are the weakest link !!!

2020 BakerHostetler Data Security Incident Response Report
https://f.datasrvr.com/fr1/620/24943/2020_DSIR_Report_(003).pdf

Organization	Description of security breach	Number of identities exposed
Grays Harbor Pediatrics, WA	A backup tape, stolen from an employee's car, was used for storing copies of paper records; patients may have had their names, Social Security numbers, insurance details, driver's license information, immunization records, medical history forms, previous doctor records, and patient medical records stolen	12,000
Tulane University, LA	A university-issued laptop was stolen from an employee's car. It was used to process 2010 tax records for employees, students, and others; the information included names, Social Security numbers, salary information, and addresses	10,000
Seacoast Radiology, NH	Patient names, Social Security numbers, addresses, phone numbers, and other personal information were exposed by a security breach	231,400
Centra, GA	A laptop was stolen from the trunk of an employee's rental car that contained patient names and billing information	11,982
Stony Brook University, NY	Student and faculty network and student IDs were posted online after a file with all registered student and faculty ID numbers was exposed	61,001
deviantART, Silverpop Systems Inc., CA	Attackers exposed the e-mail addresses, usernames, and birth dates of the entire user database	13,000,000
Twin America LLC, CitySights, NY	An attacker inserted a malicious script on a Web server and stole the customer database that contained customer names, credit card numbers, credit card expiration dates, CVV2 data, addresses, and e-mail addresses	110,000
Ohio State University, OH	Unauthorized individuals logged into an Ohio State server and accessed the names, Social Security numbers, dates of birth, and addresses of current and former students, faculty, staff, University consultants, and University contractors	750,000
Gawker, NY	Attackers gained access to the database and accessed staff and user e-mails and passwords	1,300,000

Introduction (cont.)

Example: Equifax (2017) - importance of good passwords

EDITOR'S PICK | 15,348 views | Oct 20, 2019, 10:41am

Equifax Lawsuit: 'Admin' As Password At Time Of 2017 Breach

That's according to a **class-action lawsuit launched against the company in the US**, claiming securities fraud by the company over the 2017 data breach that spilled information on **around 148 million accounts of people in the US, Canada and the UK**.

"Furthermore, Equifax employed the user name 'admin' and the password 'admin' to protect a portal used to manage credit disputes. This portal contained a vast trove of personal information."

But that is not all. The lawsuit also points out that Equifax was storing unencrypted user data on a public facing server–so it could have been viewed by any attacker who chose to compromise it.

https://www.forbes.com/sites/kateoflahertyuk/2019/10/20/equifax-lawsuit-reveals-terrible-security-practices-at-time-of-2017-breach/#25834c833d38

NEWS ANALYSIS

Attackers hack European Space Agency, leak thousands of credentials 'for the lulz'

A group of hackers operating under the Anonymous banner hacked the European Space Agency (ESA) and leaked the data for no reason other than for "lulz." Over 8,000 people will not find anything amusing about the breach since their names, email addresses and passwords were posted in one of three data dumps on JustPaste.it.

CSO's Steve Ragan analyzed the 8,107 passwords exposed, finding 39% (3,191) were three-character passwords, 16% (1,314) were eight-characters passwords which could have easily been cracked, and only 22 20-character passwords; the longest password had 24 characters with the rest of the leaked passwords falling somewhere in-between the extremes.

OFFICIAL! Good passwords more difficult than rocket science

https://www.computerworld.com/article/3014539/attackers-hack-european-space-agency-leak-thousands-of-credentials-for-the-lulz.html

https://nakedsecurity.sophos.com/2015/12/16/official-good-passwords-more-difficult-than-rocket-science/

C.I.A. of Information Security

- **C.I.A. Triangle** – 3 key characteristics of information that must be protected by information security:
  - **confidentiality** - only authorized parties can view private information
  - **integrity** - information is changed only in a specified and authorized manner (by authorized users)
  - **availability** – information is accessible to authorized users whenever needed

Different organizations may view one of the CIA components as being more important than others!!!

C.I.A. of Information Security (cont.)

Example: **DATA CONFIDENTIALITY**

Student grade – an information asset of high importance for student.

- In US, release of such information is regulated by **Family Educational Rights and Privacy Act** (FERPA).

  Grade information should only be available to students, their parents and employees that require this information to do their job.

- In Canada, the same issue is regulated by **Personal Information Protection and Electronic Documents Act** (PIPEDA).

Technology

Greenwich University fined £120,000 for data breach

21 May 2018

The University of Greenwich has been fined £120,000 ($160,000) by the Information Commissioner.

The fine was for a security breach in which the personal data of 19,500 students was placed online.

The data included names, addresses, dates of birth, phone numbers, signatures and - in some cases - physical and mental health problems.

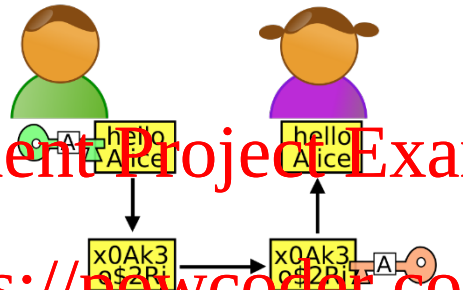
It was uploaded onto a microsite for a training conference in 2004, which was then not secured or closed down.

The Information Commissioner said Greenwich was the first university to receive a fine under the Data Protection Act of 1998 and described the breach as "serious".

C.I.A. of Information Security (cont.)

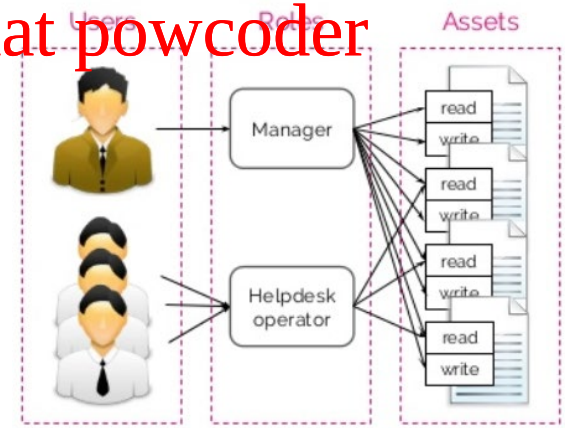
Example: How to ensure data confidentiality?

- **cryptography**



What is a potential drawback of protecting confidentiality through encryption?!

- **strong access control**

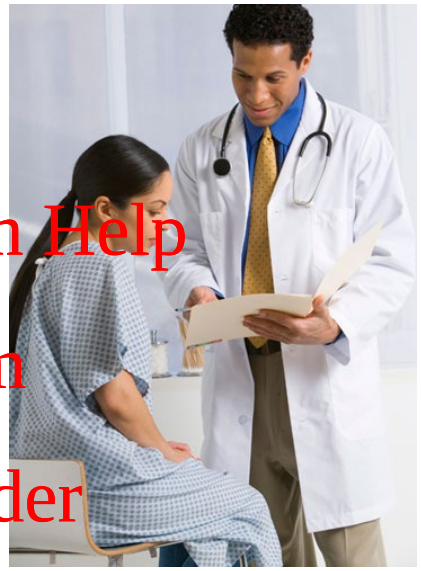


- **limiting number of places where data can appear**
  (e.g., cannot be stored on an USB)

C.I.A. of Information Security (cont.)

Example: **DATA INTEGRITY**

Patient information in a hospital – the doctor should be able to trust that the information is correct and current.



Inaccurate info could result in serious harm to the patient and expose the hospital to massive liability.

- In US, **Health Insurance Portability and Accountability Act** (HIPAA) regulates the collection, storage, and transmission of sensitive personal health care information.

  Hospital is responsible for safeguarding patient information against error, loss, defacing, tampering and unauthorized use.

  (Ontario's Personal Health Information Protection Act - PHIPA)

C.I.A. of Information Security (cont.)

Cottage Health, Touchstone Medical Imaging, and University of Rochester Medical Center (URMC): $3 million each

2019 saw three large HIPAA violations; $3 million each for Cottage Health & Touchstone Medical Imaging.

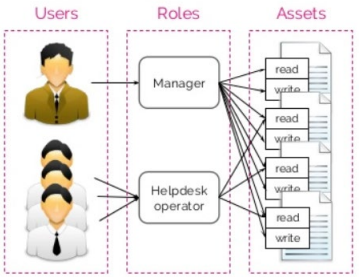
Cottage health was fined for two breaches — one in 2013 and another in 2015 — resulting in electronic protected health information (ePHI) affecting over 62,500 individuals being leaked. Both incidents involved servers holding ePHI being accessible over the internet.

Tennessee-based Touchstone Medical Imaging was fined after leaving the protected health information (PHI) of over 300,000 patients available online through an exposed FTP server. Touchstone was notified about this exposure by the FBI in 2014 but claimed no patient PHI was exposed.

https://www.csoonline.com/article/3410278/the-biggest-data-breach-fines-penalties-and-settlements-so-far.html

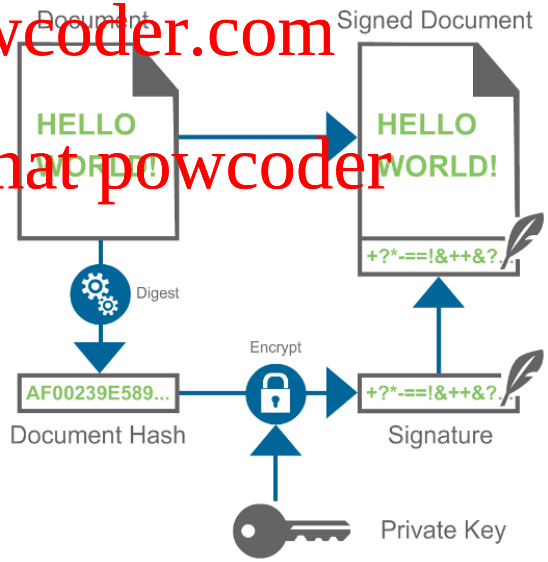
C.I.A. of Information Security (cont.)

Example: How to ensure data integrity?



- **strong access control** - good at preventing attacks on data integrity

- **cryptography (hashing)**
  - detects attacks on data integrity



- **documenting system activity (logging) - who did what and when** - detects attacks on data integrity

C.I.A. of Information Security (cont.)

Example: **DATA AVAILABILITY**

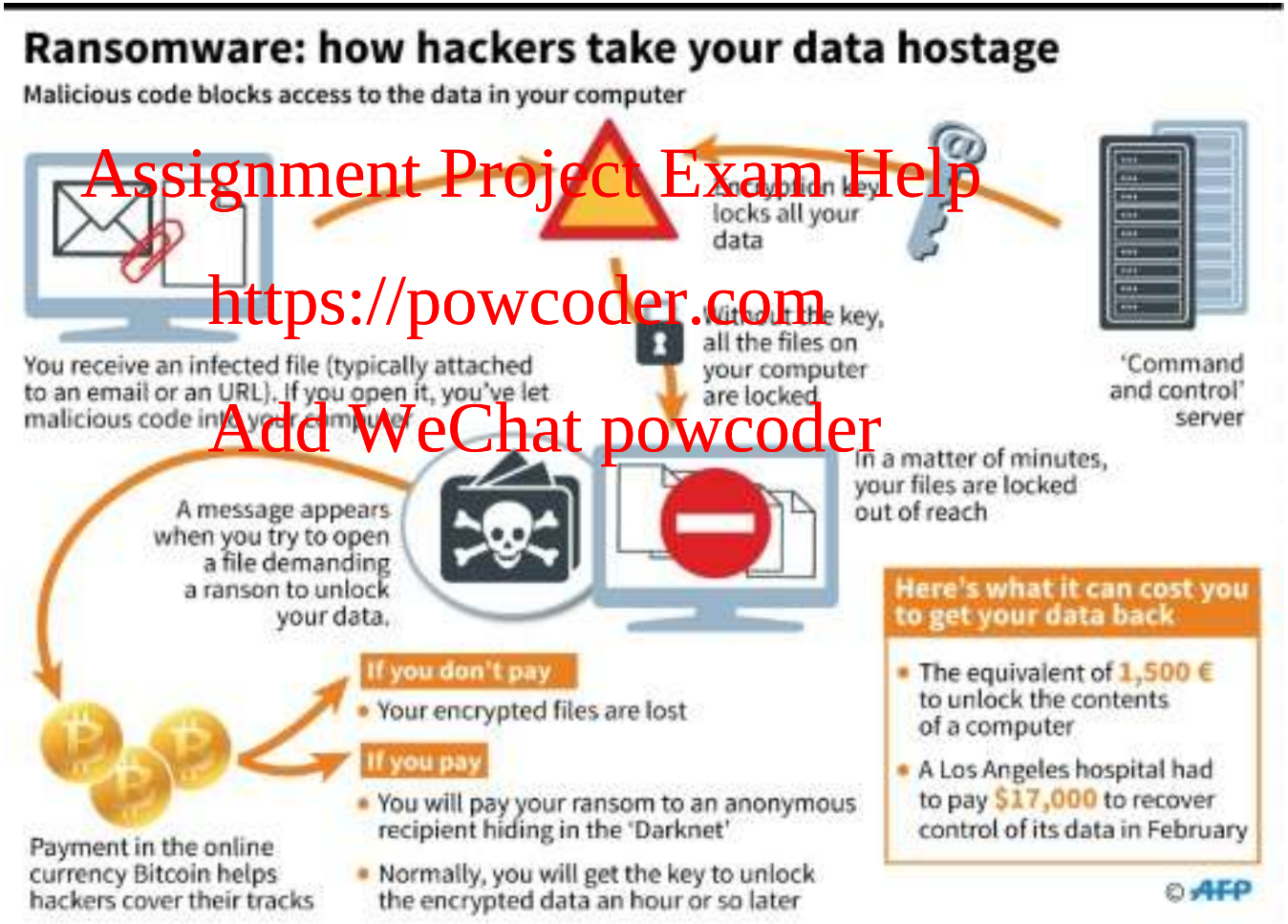
Accessible and properly functioning web site – a key asset for an **e-commerce company**.

E.g., a **DDoS attack** could make the site unavailable and cause significant loss in revenue and reputation.

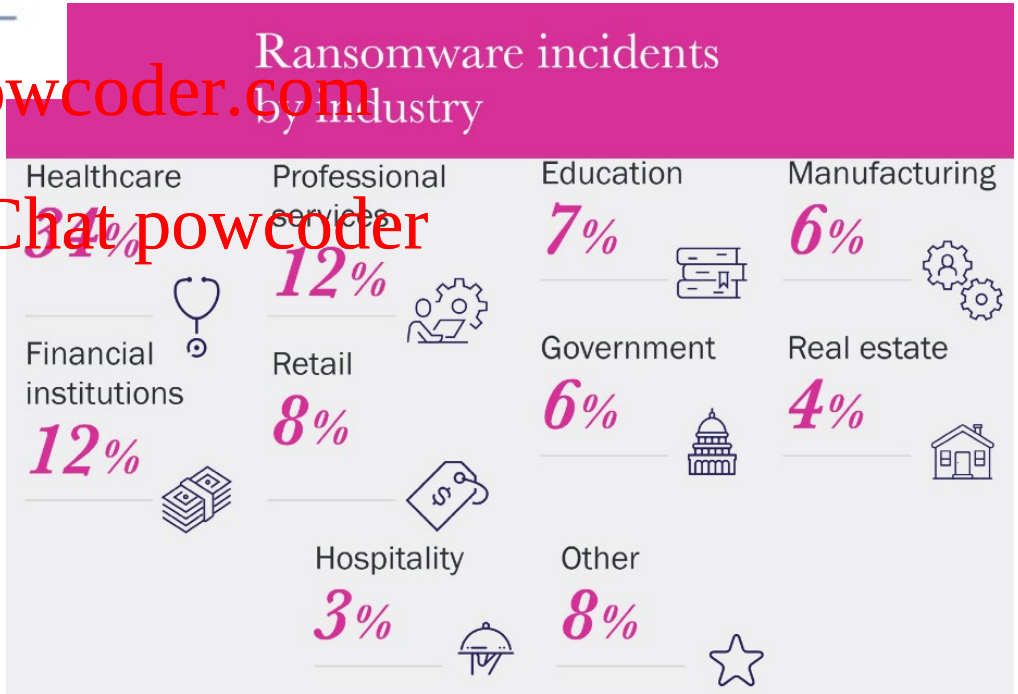
- In US, **Computer Fraud and Abuse Act** (CFAA) applies to DoS-related attacks.
- In Canada, DoS activities are regulated under **Criminal Code of Canada, Section 342: Unauthorized Use of Computer**

C.I.A. of Information Security (cont.)

- besides DoS, ransomware is another way to attack data availability



https://phys.org/news/2017-05-alarm-global-ransomware.html



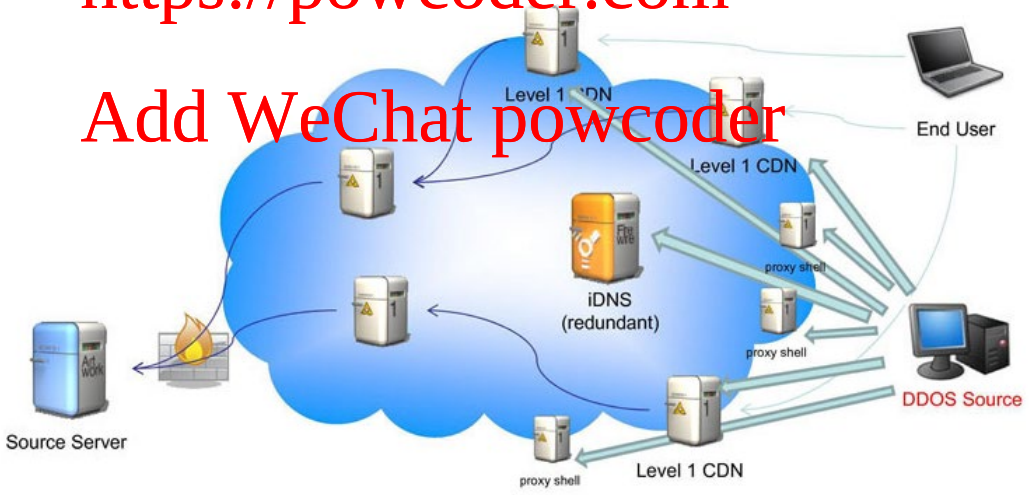
https://www.bleepingcomputer.com/news/security/70-percent-of-ransomware-attacks-targeted-smbs-bec-attacks-increased-by-130-percent/

C.I.A. of Information Security (cont.)

Example: How to ensure data availability?

- **anti-DDoS system** (in case of attack that attempt to prevent access by blocking the bandwidth/server):

e.g., content distribution networks, scrubbing centers



- **well established backup procedure** (in case of attacks that prevent access by encrypting or destroying data)

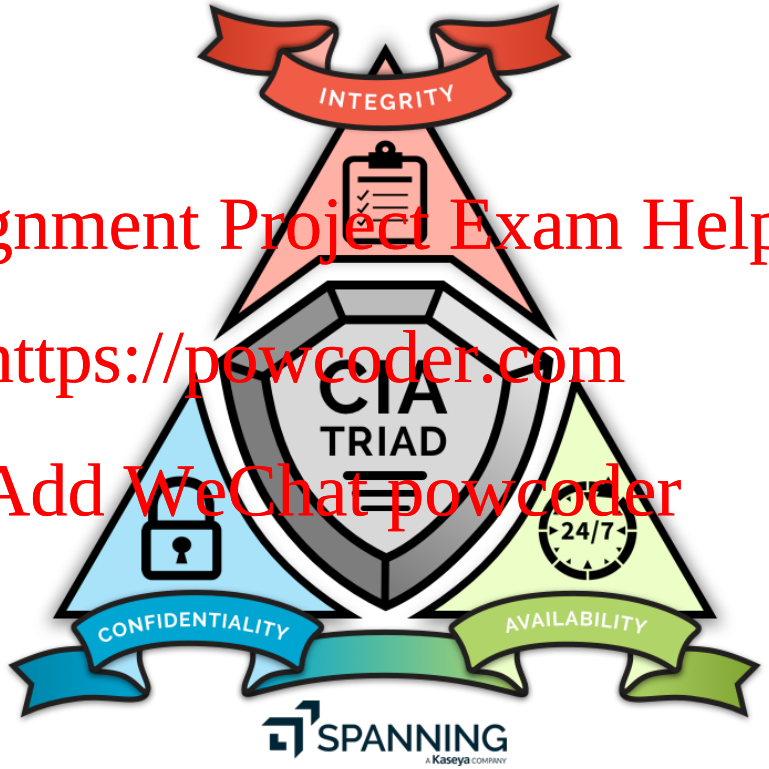
C.I.A. of Information Security (cont.)

Example: CIA of different IT components

	Availability	Confidentiality	Integrity
Hardware	Equipment is stolen or disabled, thus denying service.	An unencrypted CD-ROM or DVD is stolen.	
Software	Programs are deleted, denying access to users.	An unauthorized copy of software is made.	A working program is modified, either to cause it to fail during execution or to cause it to do some unintended task.
Data	Files are deleted, denying access to users.	An unauthorized read of data is performed. An analysis of statistical data reveals underlying data.	Existing files are modified or new files are fabricated.
Communication Lines and Networks	Messages are destroyed or deleted. Communication lines or networks are rendered unavailable.	Messages are read. The traffic pattern of messages is observed.	Messages are modified, delayed, reordered, or duplicated. False messages are fabricated.

Table 1.3 Computer and Network Assets, with Examples of Threats.

C.I.A. of Information Security (cont.)



Is there anything else to protect / add ???

https://securityboulevard.com/2019/08/cia-triad-best-practices-for-securing-your-org/

C.I.A. of Information Security (cont.)

- **Extended C.I.A. Triangle** – some security experts feel that additional concept need to be added to the CIA triad:
  - **authenticity** – being able to verify that users are who they claim to be, and that each data input has come from a trusted source
  - **accountability** – being able to trace actions of an entity uniquely to that entity

Single log-file/system may not be enough!