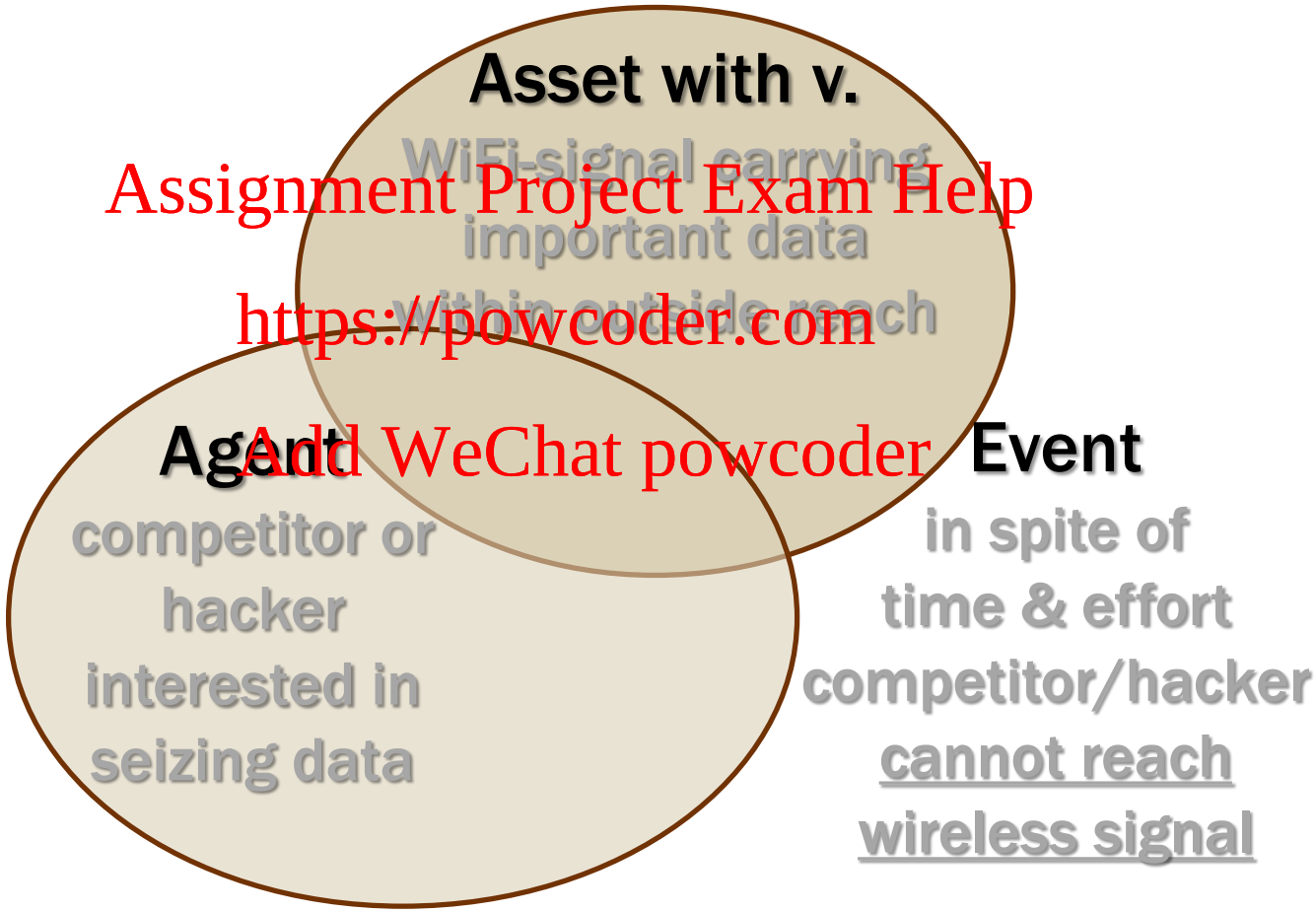
Threats (cont.)

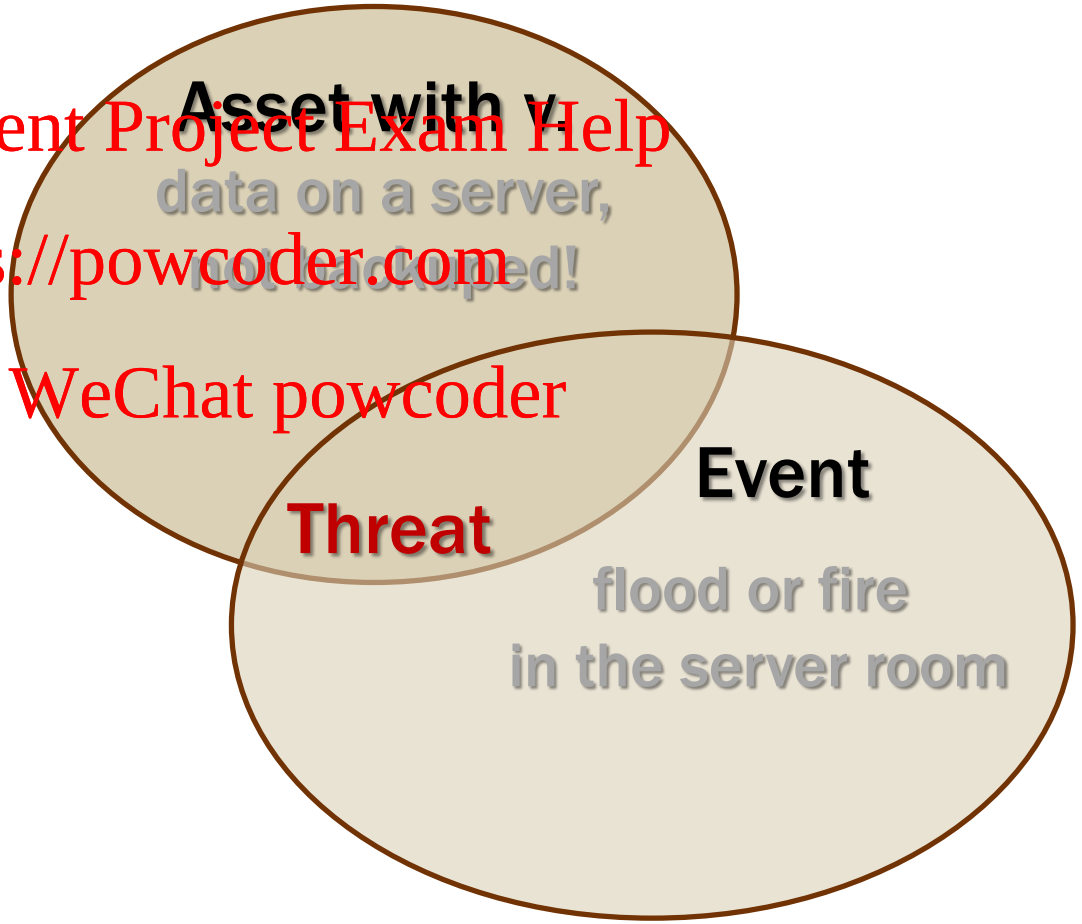
Example: Threat in WiFi network



NO EVENT ⇒ NO THREAT !!!

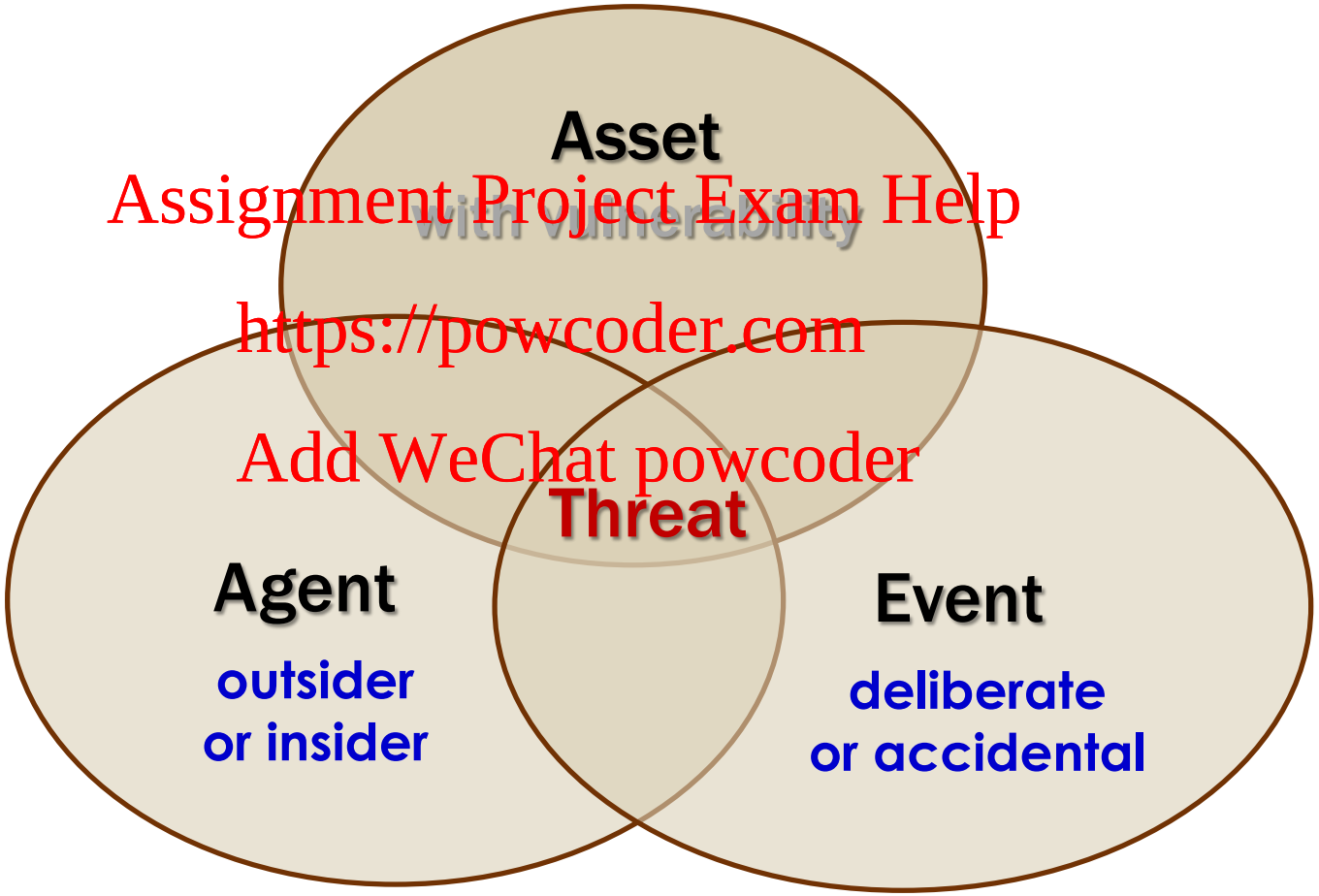
Threats (cont.)

Example: Threat without Agent



Threats (cont.)

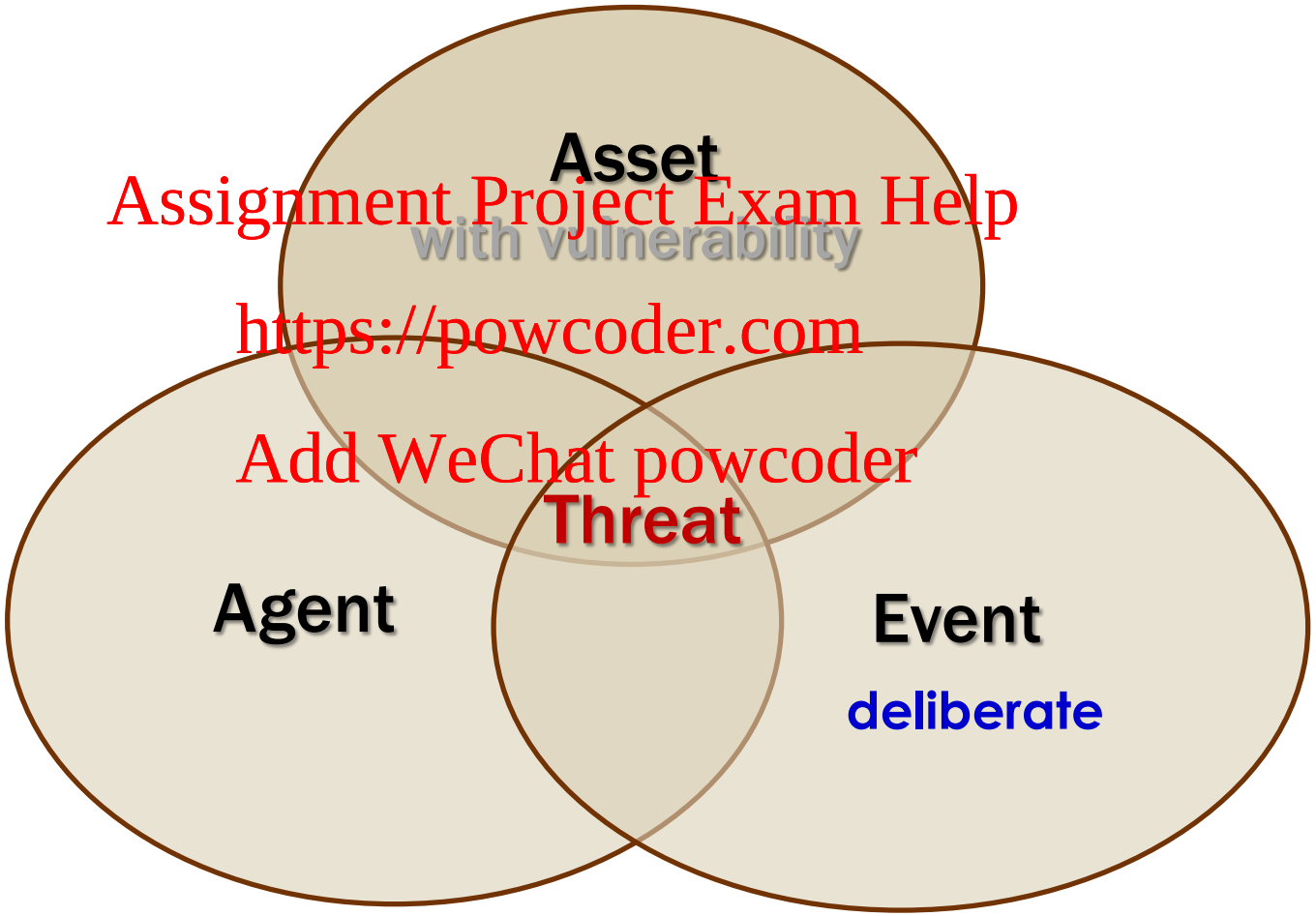
Example: outsider vs. insider, deliberate vs. accidental



Example of insider causing accidental threat: SysAdmin has added a new software to the system and has forgotten to change the password

Threats (cont.)

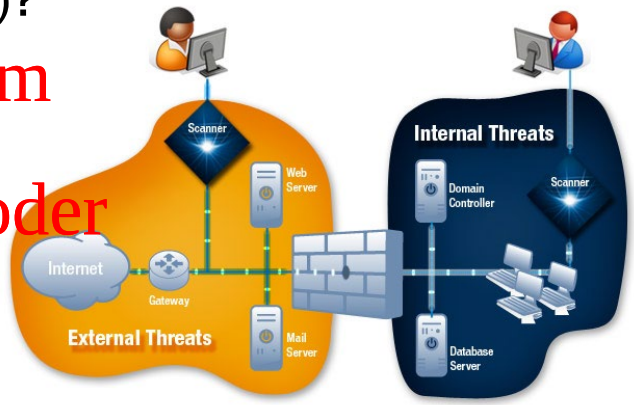
Example: attack definition



THREAT EVENT DELIBERATELY EXECUTED BY AGENT = ATTACK

Threats (cont.)

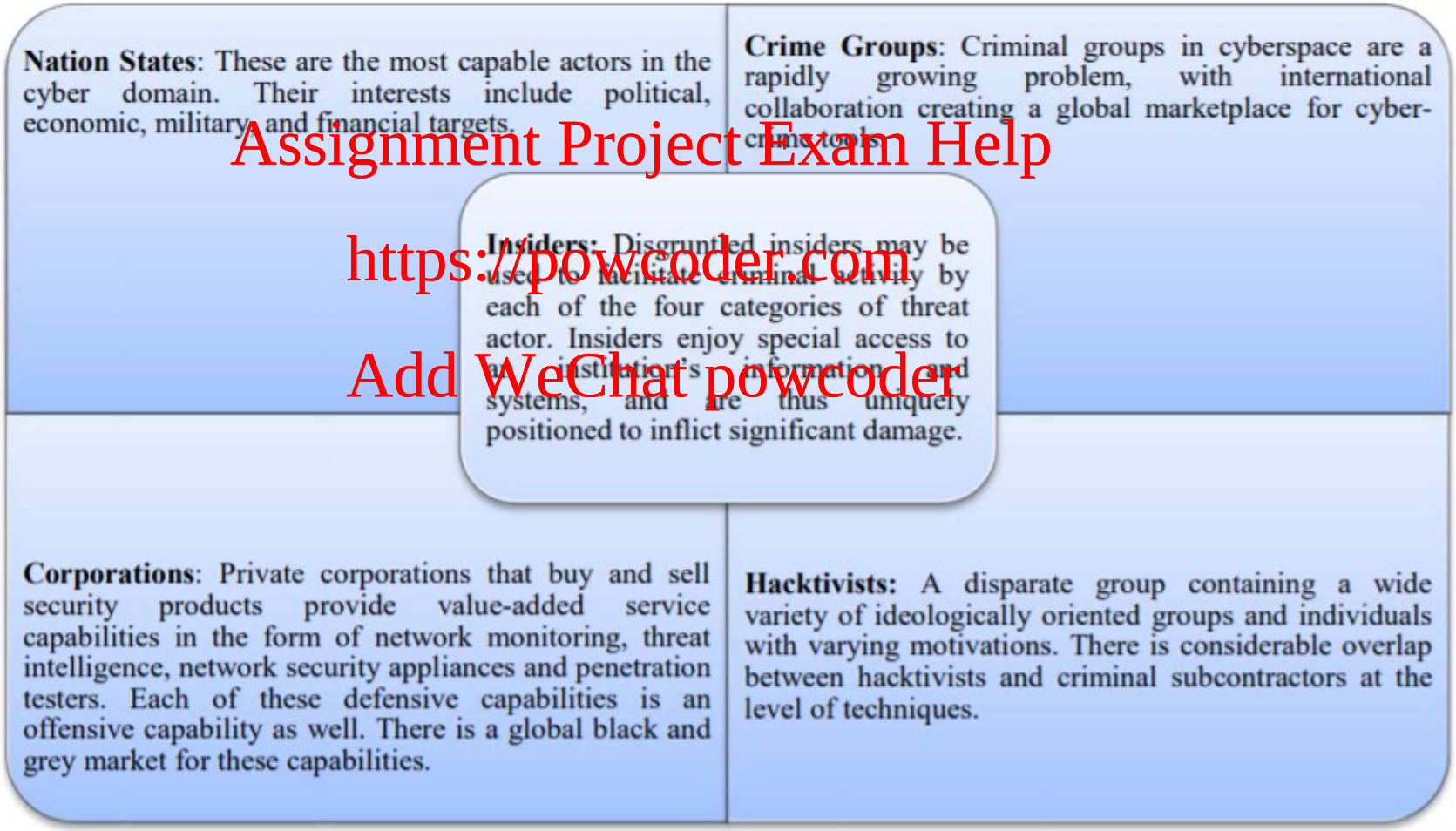
- Criteria for threat identification/prioritization :
  - asset identification
    - e.g. what are the company's main assets:
      (a) web servers (e-commerce company) or
      (b) workstations (software company)?



  - threat identification [asset-vulnerability, agent, event]
    - some assets have multiple vulnerabilities (e.g., web-server)
  - organizational strategy regarding risk
    - different threats pose different risks

Threat Agents

- **Main Categories of Threat Agents :**



https://www.iiroc.ca/industry/Documents/CybersecurityBestPracticesGuide_en.pdf

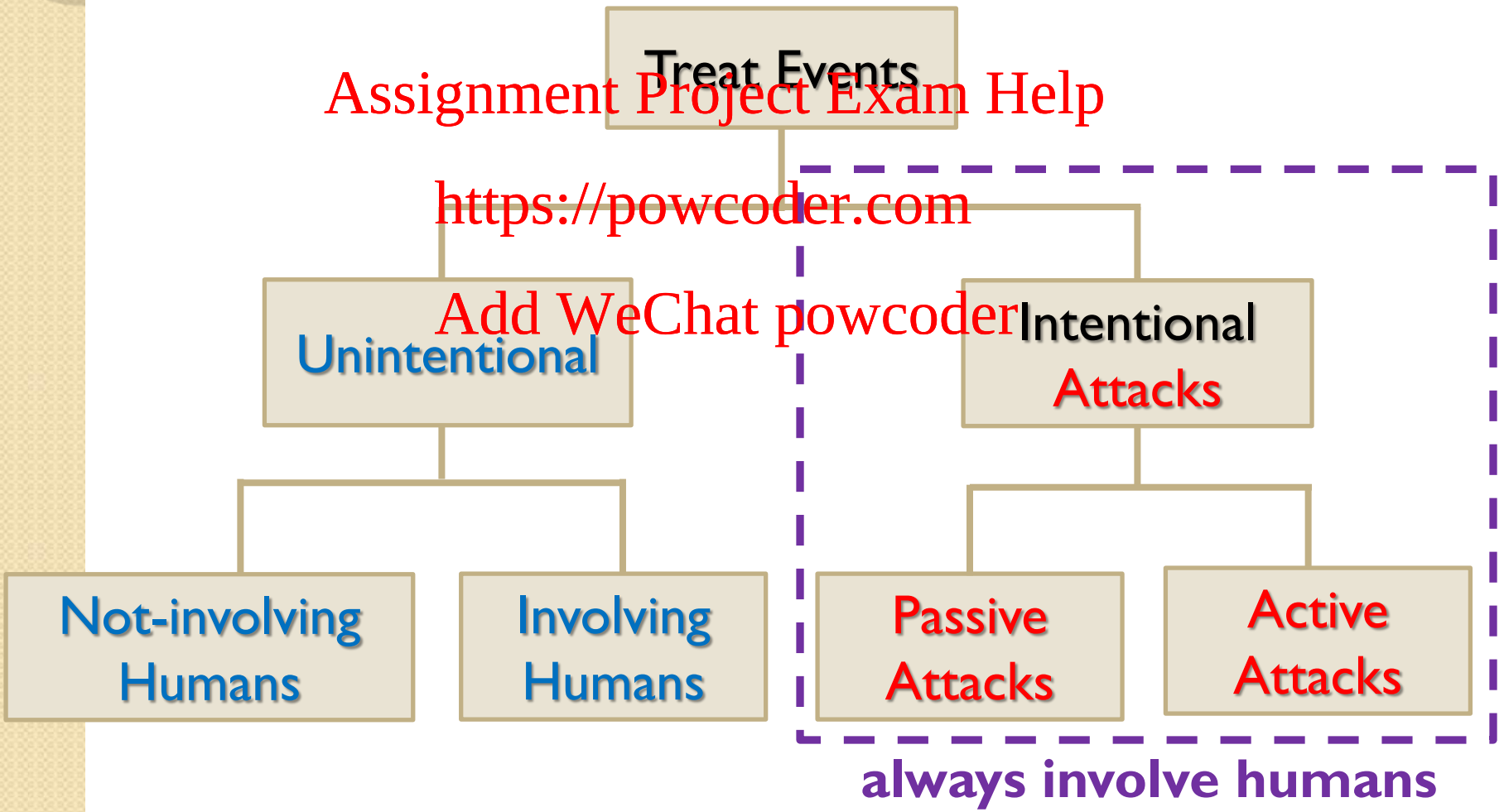
Threat Events

- **Main Groups of Threat Actions/Events :**

Threat	Example	
Act of human error or failure	Accidents, employee mistakes	with human agent
Compromises to intellectual property	Piracy, copyright infringement	with human agent ATTACKS
Deliberate acts of espionage or trespass	Unauthorized access and/or data collection	with human agent ATTACKS
Deliberate acts of information extortion	Blackmail for information disclosure	with human agent ATTACKS
Deliberate acts of sabotage or vandalism	Destruction of systems or information	with human agent ATTACKS
Deliberate acts of theft	Illegal confiscation of equipment or information	with human agent ATTACKS
Deliberate software attacks	Viruses, worms, macros, denial-of-service	with human agent ATTACKS
Deviations in quality of service by service provides	Power and WAN quality of service issues from service providers	with human agent
Forces of nature	Fire, flood, earthquake, lightning	no human
Technical hardware failures or errors	Equipment failure	no human
Technical software failures or errors	Bugs, code problems, unknown loopholes	no human
Technological obsolescence	Antiquated or outdated technologies	no human

Threat Events (cont.)

- **Categories of Threat Events** :



Threat Events (cont.)

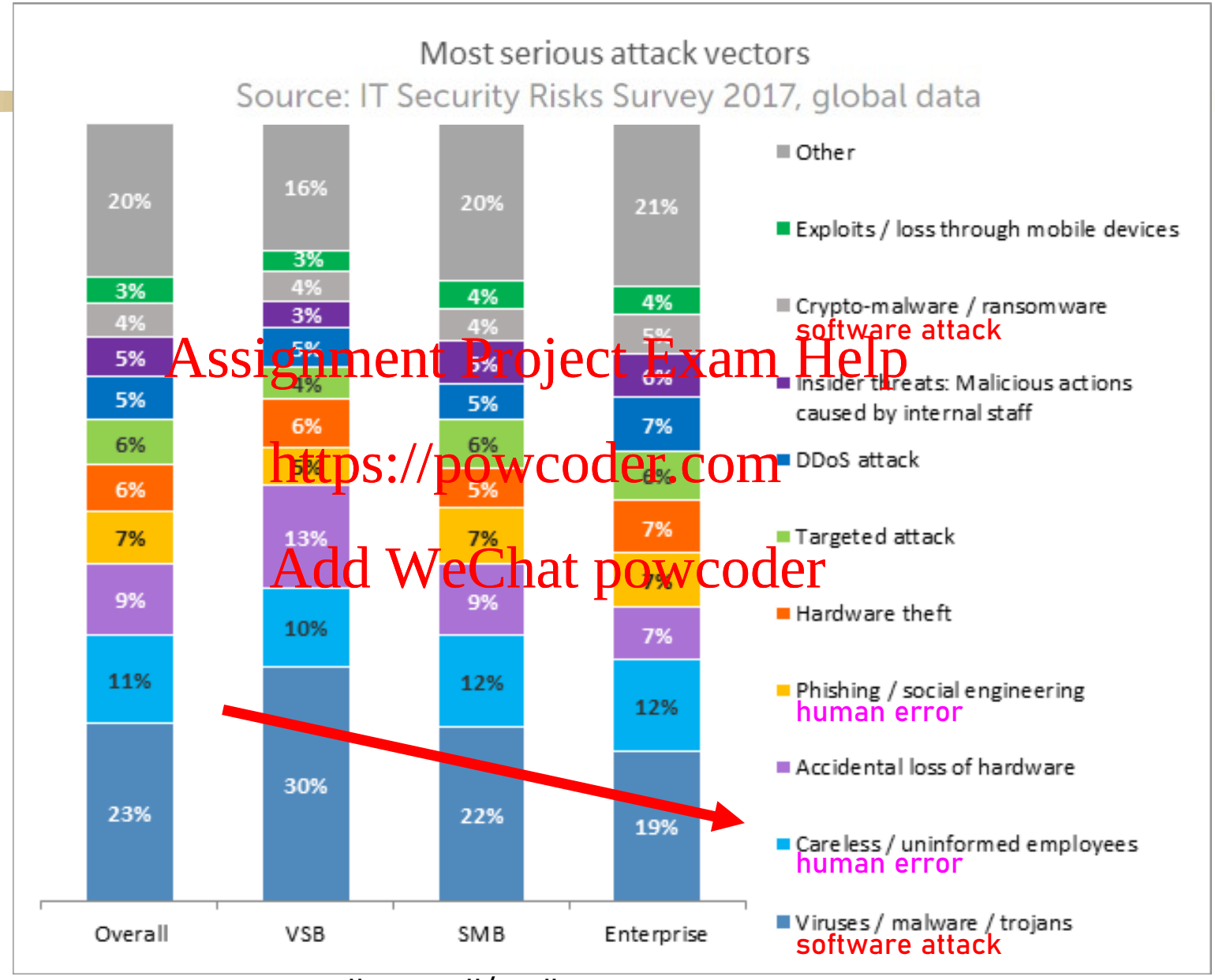
- **Top Threat-Driven Expenses (C-ACM study)**

2012 JISSec Ranking	Categories of Threats	Rate	Rank	Combined	2003 CACM Rank
1	Espionage or trespass	3.52	462	16.35	4
2	Software attacks	4.00	306	12.24	1
3	Human error or failure	4.30	222	9.55	3
4	Theft	3.61	162	5.85	7
5	Compromises to intellectual property	3.59	162	5.82	9
6	Sabotage or vandalism	3.11	111	3.45	5
7	Technical software failures or errors	3.17	105	3.33	2
8	Technical hardware failures or errors	2.88	87	2.51	6
9	Forces of nature	2.76	81	2.24	8
10	Deviations in quality of service from service providers	2.88	72	2.07	10
11	Technological obsolescence	2.66	57	1.52	11
12	Information extortion	2.68	18	0.48	12

Rating of different threat events based on their frequency and significance.

kaspersky daily

https://www.kaspersky.com/blog/the-human-factor-in-it-security/



Threat Events: Unintentional & No Human

- **Forces of Nature**
  - fire, flood, earthquake, hurricane, tsunami, dust contamination, …
  - cannot be predicted/prevented
  - organization must implement controls to limit damage as well as develop incident response plans and business continuity plans

Hurricane Harvey, for instance, put Houston data centers to the test. Edward Henigin, CTO of Data Foundry Inc. in Austin, said their North Houston data center is a "purpose-built facility designed to withstand Category 5 hurricane wind speeds." Just before Hurricane Harvey last year, the company brought on additional staff to maintain the data center throughout the emergency and provided food, showers, cots, books and video games for employees who remained at work five straight days. The major data center providers in Houston reported that there was no interruption of service during the emergency. This is impressive, as Hurricane Harvey damaged 203,000 homes and cost at least $125 billion in reparations.

https://www.idexpertscorp.com/articles/data-security-and-natural-disasters/

Threat Events: Unintentional & No Human

- **Hardware and Software Failures and Errors**
  - cannot be fully controlled/prevented by the organization
  - causes of hardware failures: wear, tear, age, operating environment (e.g., high temperature, moisture, dust), …
  - best defences against hardware failures:
    - redundancy (e.g., backup servers)
    - continuous monitoring of hardware devices
  - causes of software failures: difficulty of testing software for all possible inputs & all possible operating conditions; OS evolutions and software incompatibilities …
  - best defences against software failures:
    - keep up-to-date with software updates and vulnerabilities
    - continuously monitor and maintain software system

Threat Events: Unintentional & No Human

Backblaze Q2 2020 Annualized Hard Drive Failure Rates

Reporting period: April 1, 2020 through June 30, 2020 inclusive

Hitachi

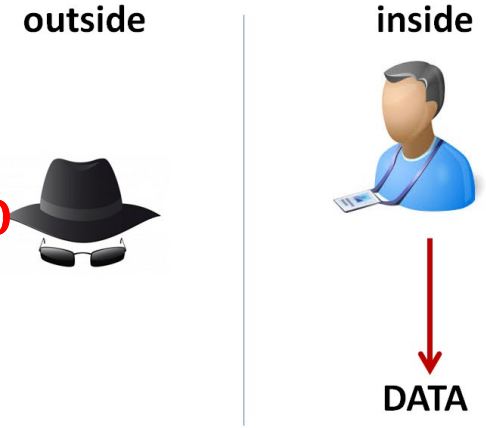
MFG	Model	Drive Size	Drive Count	Drive Days	Drive Failures	AFR
HGST	HMS5C4040ALE640	4TB	2,952	266,200	1	0.14%
HGST	HMS5C4040BLE640	4TB	12,739	1,159,472	9	0.28%
HGST	HUH728080ALE600	8TB	1,200	97,600	0	0.00%
HGST	HUH721212ALE600	12TB	2,600	200,188	3	0.55%
HGST	HUH721212ALN604	12TB	10,846	986,674	19	0.70%
Seagate	ST4000DM000	4TB	19,093	1,739,577	49	1.03%
Seagate	ST6000DX000	6TB	886	80,626	0	0.00%
Seagate	ST8000DM002	8TB	9,705	890,937	17	0.70%
Seagate	ST8000NM0055	8TB	14,462	1,316,313	33	0.92%
Seagate	ST10000NM0086	10TB	1,200	109,200	2	0.67%
Seagate	ST12000NM0007	12TB	35,095	3,319,854	82	0.90%
Seagate	ST12000NM0008	12TB	15,543	1,279,568	27	0.77%
Seagate	ST12000NM001G	12TB	4,799	137,929	8	2.12%
Seagate	ST16000NM001G	16TB	59	5,431	1	6.72%
Toshiba	MD04ABA400V	4TB	99	9,009	0	0.00%
Toshiba	MG07ACA14TA	14TB	8,699	663,647	20	1.10%
		TOTALS	**139,867**	**12,255,625**	**271**	**0.81%**

https://www.backblaze.com/blog/backblaze-hard-drive-stats-q2-2020/

BACKBLAZE

Threat Events: Unintentional With Human

- **Act of Human Error or Failure**
  - organization's own employee's are one of its greatest threats
  - examples:
    - revelation of classified data (e.g., phishing)
    - accidental deletion or modification of data
    - failure to protect data
    - storing data in unprotected areas
    - entry of erroneous data



Much of human error or failure can be prevented!

- preventative measures:
  - training and ongoing awareness activities
  - enhanced control techniques:
    - require users to type a critical command twice
    - ask for verification of commands by a second party

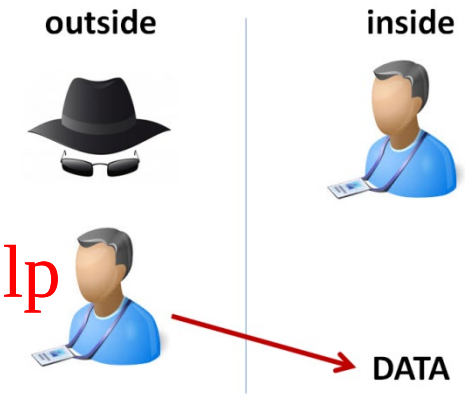
Threat Events: Unintentional With Human

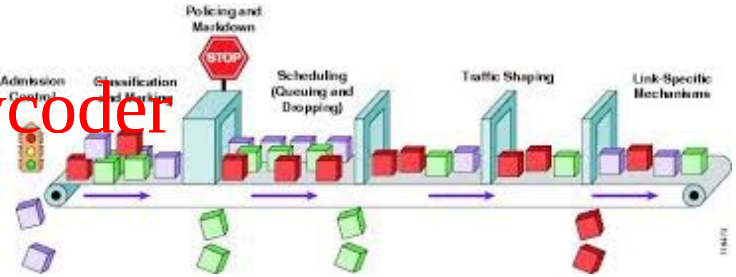
Example: Is this a cyber-security threat event? Justify your answer.

You are depositing $500 cash at your bank.
The bank clerk types/enters into the system $5,000 as the deposit amount.

Threat Events: Unintentional With Human

- **Deviations in Quality of Service**
  - in organizations that relies on the Internet and Web, irregularities in availability bandwidth can dramatically affect their operation
    - e.g. employees or customers cannot contact the system

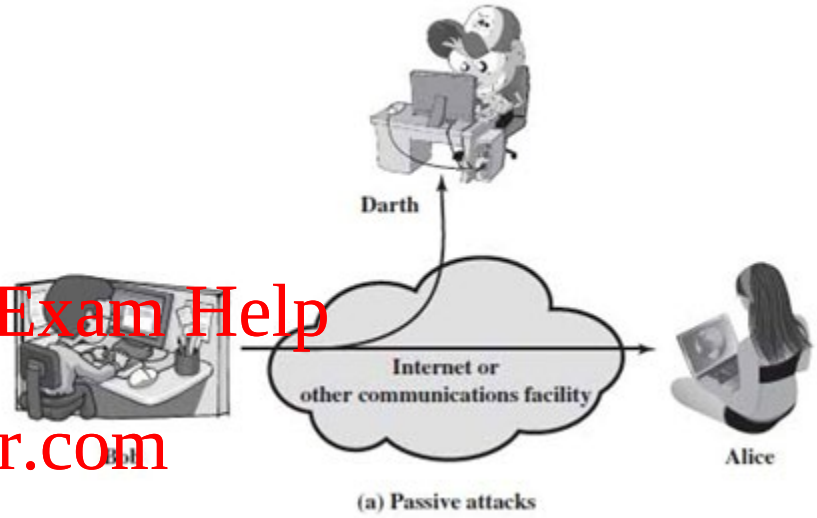




  - possible 'defence': backup ISP or backup power generator

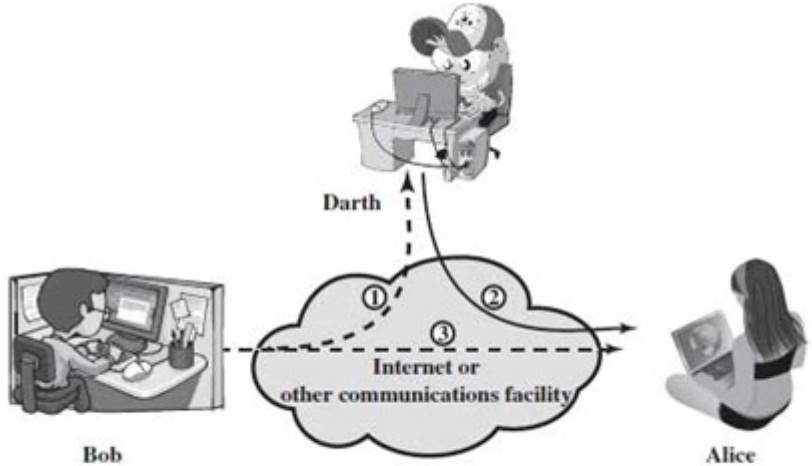
Threat Events: Intentional Attacks

- **Passive Attack** - attempts to learn or make use of info. from the system but does not affect system resources
  - compromises **Confidentiality**
  - generally hard to detect
  - examples: traffic sniffing



(a) Passive attacks

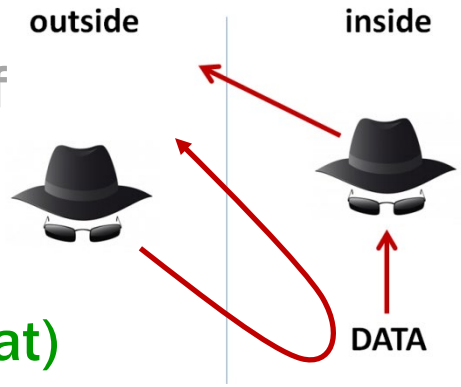
- **Active Attack** - attempts to alter system resources or affect their operation
  - compromises **Integrity** or **Availability**
  - examples: masquerade, data/packet injection and DoS



(b) Active attacks

Threat Events: Intentional Attacks (cont.)

- **Compromise to Intellectual Property (IP)**
  - IP = any intangible asset that consist of human knowledge & ideas – creations of the mind (copyright, patent, trade secret)
  - any unauthorized use of IP constitutes a security threat (MS Office, Adobe Acrobat)
  - defense measures:
    - use of digital watermarks and embedded code



Example: Peter Morch story – compromise to IP by insider

In 2000, while still employed at Cisco Systems, Morch logged into a computer belonging to another Cisco software engineer, and obtained (burned onto a CD) proprietary information about an ongoing project.

Shortly after, Morch started working for Calix Networks – a potential competitor with Cisco. He offered them Cisco's information.

Morch was sentenced to 3 years' probation.

APPLE \ TECH \ TRANSPORTATION

FBI charges former Apple employee with stealing trade secrets from self-driving car project

The employee was allegedly trying to get a job at Alibaba-backed Xiaopeng Motors

By Sean O'Kane | @sokane1 | Jul 10, 2018, 5:19pm EDT

Xiaolang Zhang, who worked for Apple from December 2015 until May 2018, has been charged in federal court with stealing trade secrets, and faces 10 years imprisonment and a $250,000 fine. Zhang was arrested trying to leave the country this past weekend. The news was first reported by The Mercury News.

Once Zhang told his Apple supervisor about his intentions, and after "feeling that he had been evasive," according to the filing, a member of Apple's New Product Security Division joined the meeting and had Zhang turn in his two work phones and his laptop. After the meeting, Apple reviewed Zhang's past network activity, performed a forensic analysis on his work devices, as well as his "activities on the Apple campus," including swipe badge access and closed circuit TV footage.

The company's security team discovered that Zhang's network activity "increased exponentially compared to the prior two years of his employment" in the days before his attempted resignation, and that the majority of that activity was "bulk searches and targeted downloading copious pages of information" from confidential databases that he had access to. The CCTV footage that Apple reviewed showed, according to the complaint, Zhang leaving the company's autonomous vehicle lab on April 28th (during time when he was supposed to be on leave) carrying a "computer keyboard, some cables, and a large box."

https://www.theverge.com/2018/7/10/17556034/fbi-apple-trade-secrets-xpeng-self-driving

Protecting intellectual property from insider threat

By Josh Lefkowitz June 12, 2019

A company's IP is estimated to represent as much as 70% of its market value.

Unfortunately, the value of IP is often only understood once it has been stolen and commercialised. When copycat products start appearing, or unique features pop up in competitor designs, the loss becomes apparent. By that point, the damage has been done, and recourse is limited to patent infringement courts.

Employees with a grievance against their employer could to punish them by sharing sensitive information for personal profit. Another scenario might see an employee tempted by a high-salary position with a competitor in return for stealing corporate secrets prior to leaving their current role.

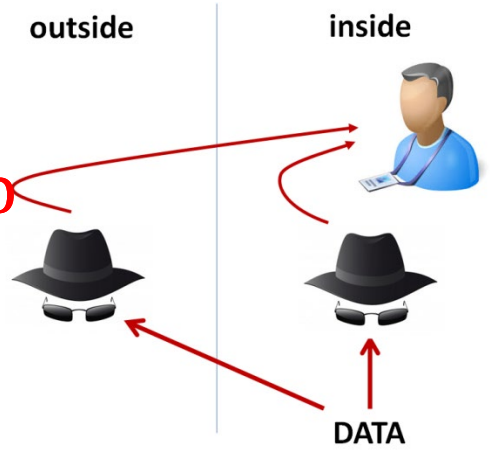
Employees don't always deliberately reveal secrets; they can simply be targets of malicious activity themselves. They may be recruited by bad actors using an apparently legitimate front, such an invitation to an overseas academic conference, and manipulated into divulging trade secrets.

Finally, we see bad actors take roles within target organisations with the sole aim of accessing and exfiltrating trade secrets.

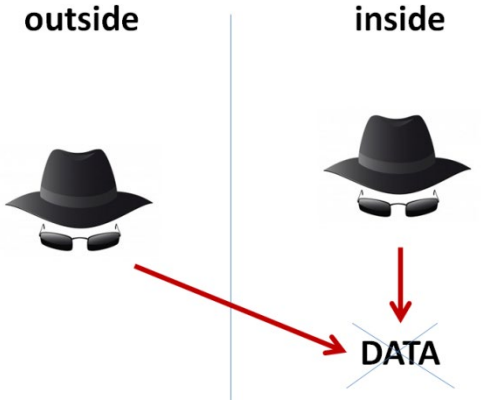
https://www.techradar.com/news/protecting-intellectual-property-from-insider-threat

Threat Events: Intentional Attacks (cont.)

- **Deliberate Act of Info. Extortion / Blackmail**
  - hacker or malicious insider steals information & demands compensation for its return or non-disclosure
  - example:
    - theft of data files containing customer credit card information



- **Deliberate Act of Sabotage or Vandalism**
  - hacker or malicious insider destroys an asset in order to cause financial loss or damage the organization's reputation
  - example:
    - hackers accessing a system and damaging or destroying critical data



Threat Events: Intentional Attacks (cont.)

Example: Two Kazakhstan employees story –
info. extortion by insider

In 2002, two employees in a company in Kazakhstan allegedly got access to Bloomberg L.P.'s financial information database because their company was an affiliate of Bloomberg.

They allegedly demanded $200,000 from Bloomberg to reveal how they got access to the database.

Bloomberg opened an offshore account with $200,000 balance, and invited the pair to London to personally meet with Michael Bloomberg. The meeting was recorded. Soon after the two were arrested ....

In the end, there were sentences to 51 months in prison.

NOTE: finding a vulnerability and requiring payment to learn about it may be considered extortion.

http://www.cybercrime.gov/zezevIndict.htm

Threat Events: Intentional Attacks (cont.)

Example: Maxus story – info. extortion by outsider

In 2000, a mysterious hacker identified as Maxus demanded $100,000 from CDUniverse company in exchange for not releasing the names and credit card numbers of over 350,000 customers he had obtained from the company website.

After CDUniverse failed to pay him, Maxus decided to set up the site, titled Maxus Credit Cards Datapipe, and to give away the stolen customer data. He announced the site's presence Dec. 25th on an Internet Relay Chat group devoted to stolen credit cards.

Soon after launching his site, Maxus said it became so popular among credit card thieves that he had to implement a cap to limit visitors to one stolen card at a time.

The case remains unsolved, as Maxus moved online using stolen accounts and relayed his emails through other sites to conceal the originating IP address …

www.nytimes.com/2000/01/10/business/thief-reveals-credit-card-data-when-web-extortion-plot-fails.html
www.cyberagecard.com/news/?page=2

Threat Events: Intentional Attacks (cont.)

Which type of attack is 'ransomware' ???

- ransomware, most commonly, is 'extortion by an outsider'
- though, in some cases it is also a simple act of 'vandalism' or 'sabotage'

Threat Events: Intentional Attacks (cont.)

Example: Patrick McKenna story – information vandalism by insider

In 2000, McKenna was fired by Bricsnet (software company).

As a revenge, he remotely accessed his former employer's computer server, and:

1) deleted approximately 675 computer files;
2) modified computer user access levels;
3) altered billing records;

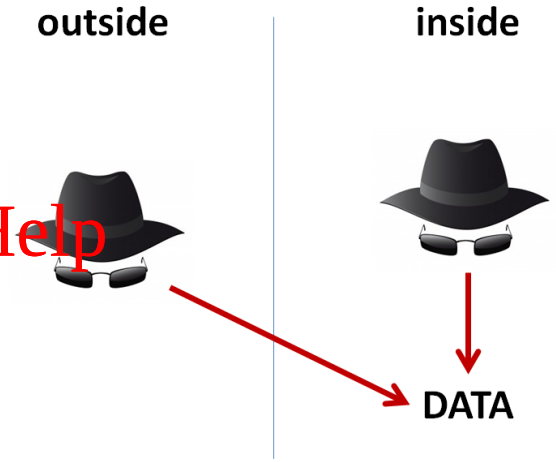
4) sent emails, which appeared to have originated from an authorized representative of the victim company to over 100 clients. Emails contained false statement about business activities of the company.

He was sentenced to 6 months in prison, followed by 2-years of supervised release. He was also ordered to pay $13,614.11 for caused damages …

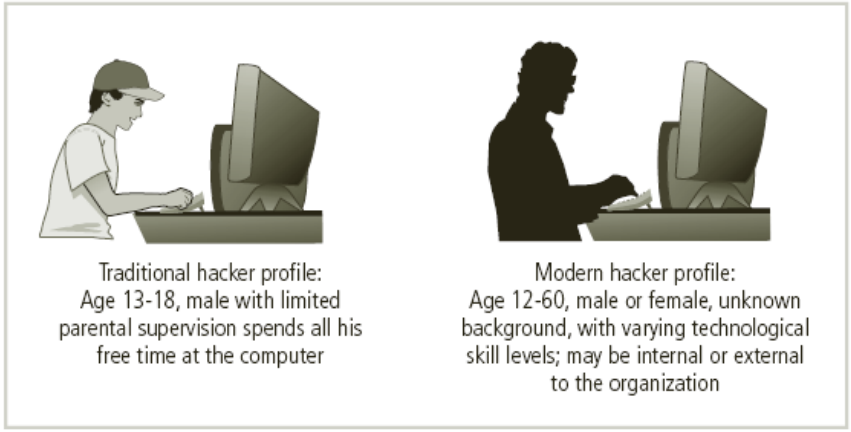
http://www.cybercrime.gov/McKennaSent.htm

Threat Events: Intentional Attacks (cont.)

- **Deliberate Act of Trespass**
  - unauthorized access to info. that an organization is trying to protect (e.g., through stolen passwords)
  - low-tech e.g.: shoulder surfing
  - high-tech e.g.: hacking

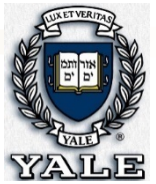


shoulder surfing



hacker profiles

Threat Events: Intentional Attacks (cont.)



Example: Princeton vs. Yale – trespass by outsider

Yale University's admission created a web-based system to enable applicants to check the status of their application on-line. To access the system, the applicants had to prove their identity by answering questions regarding their name, birth date, SIN.

Many of these students also applied to other top universities.

At Princeton, Associate Dean and Director of Admissions - Stephen LeMenager - knew that the private information that Yale used to control access was also in the applications that candidates submitted to Princeton. He used this information to log into the Yale system several times as applicants.

When the word got out, he admitted doing the break-ins but said that he was merely testing the security of the Yale system. Princeton put him on administrative leave.

NOTE: The case emphasizes that information used to control access must not be generally available ...