Cyberthreats
Are we really prepared?

Something has changed… a lot.

Rise of the Cyber Attacks

Ref	Date	Author	Target	Description	Attack	Target Category	Attack Category	Country
1	Jan 16		Metropolitan State University	Minnesota-based Metropolitan State University notifies alerting faculty, staff and students that an attacker may have breached its web server to access a database that contained their personal information. 22,000 users are at risk. The attack happened in December and the alleged author is abdilo.	SQLi	Education	CC	US
2	Jan 16	?		LizardStresser[dot]ru, the "stresser service" (DDoS-for-hire) created by the infamous LizardSquad, is allegedly hacked, revealing the details of its 14,241 users.	Unknown	Org: Hackers	CC	N/A
3	Jan 16	?	UPI	A total of six fake messages are posted from the Twitter accounts of New York Post and United Press International (UPI) by unknown individuals	Account Hijacking	News	CC	US
4	Jan 16	?	grillparts.com	Barbecue Renew, which sells grill parts through its website grillparts.com, notifies an undisclosed number of individuals that their payment card data may have been compromised as a result of a series of cyber attacks on its web server.	Unknown	Industry: E-Commerce	CC	US
5	Jan 16	Team System DZ	Local Roots, Global Reach	Team System DZ, an Algerian pro-ISIS hacker defaces the Isle of Wight, Virginia, Website (co.isle-of-wight.va.us).	Defacement	Government	H	US
6	Jan 16			Smittenz hacks powerpulse.net and dumps **1,300** usernames and hashed passwords.	SQLi	News	CC	US
7	Jan 17	?	Outlook.com	Online censorship watchdog Greatfire.org receives reports related to a man-in-the-middle (MITM) attack against Outlook users in China.	MITM	Industry: Internet Services	CE	CN
8	Jan 17	?	Payivy	An unknown hacker hacks payivy.com (a virtual marketplace to sell products online) and dumps **10,000** users and clear text passwords.	SQLi	Industry: Internet Services	CC	US
9	Jan 17	p0lak & sh0utz		Two hackers called p0lak & sh0utz hack philsacra.ust.edu.ph and dump **5,100** usernames and hashed passwords.	SQLi	Education	CC	PH
10	Jan 19		Auwartravelcover	A hacker called abdilo (@abdilo_) claims responsibility for breaching the database of Australian travel insurer Aussie Travel Cover on December 18 last year. He claims to have exfiltrated **700,000** records and to have used the same technique to breach multiple government sites.	SQLi	Industry: Travel Insurance	CC	AU
11	Jan 19	Team Muslim Cyberforce		Two New Zealand non-profit websites tindall.org.nz and livefortomorrow.co.nz are defaced by a group calling themselves the Team Muslim Cyberforce.	Defacement	Org: Non-Profit	H	NZ
12	Jan 20	Master mind	topface	Russian dating site Topface is hacked and the username of 20 million visitors are offered for sale on a website. Few days after the hacked site buys back the records (officially "awards" the hacker for discovering the	Unknown	Dating	CC	RU

http://hackmageddon.com/

Organized cybercrime

Whistleblowers

Cyberintelligence or espionage?

Financial crisis

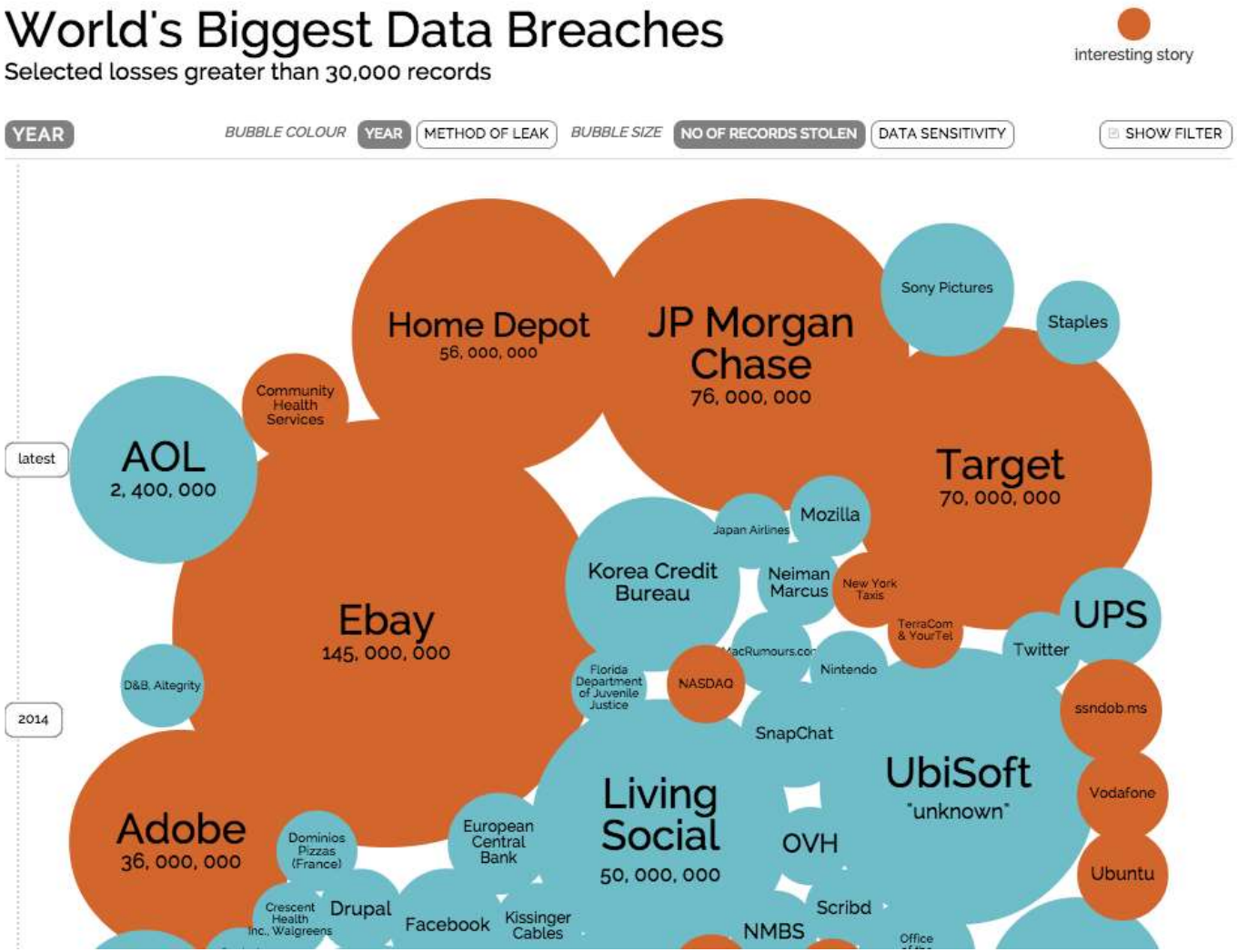
Outsourcing

The cloud

Corporate & Personal

Data breaches

Data breaches



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

Data breaches

Anthem BlueCross BlueShield

Cyber Attack Against Anthem

Dear Anthem Client,

We wanted to make you aware of a data breach that may have affected your personal health information and credit card data. The data which was accessed may impact clients who made credit or debit card payments for healthcare or who got treatment during the year 2014.

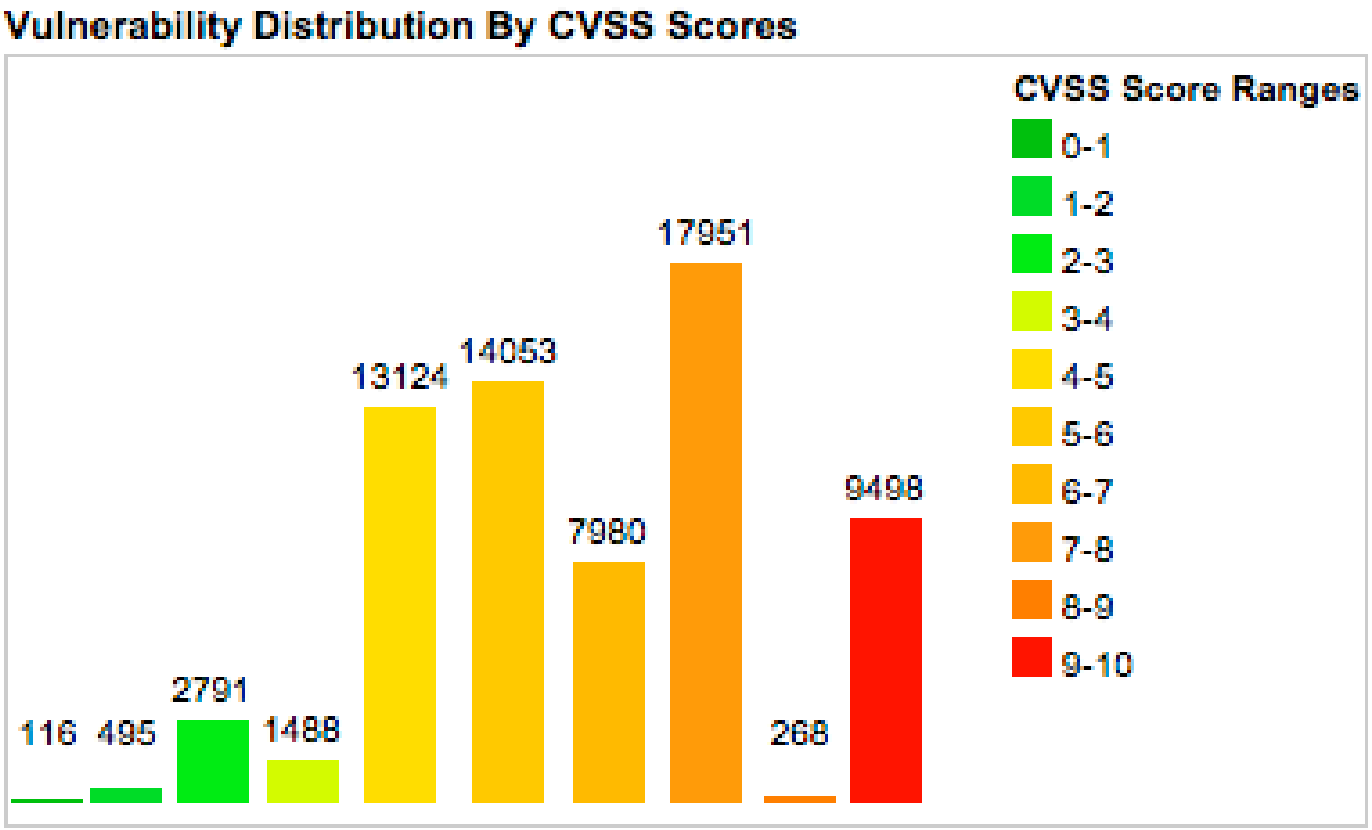
Your trust is a top priority for Anthem, and we deeply regret the inconvenience this may cause. The privacy and protection of our client's health care information is a matter we take very seriously and we are working diligently to resolve the incident.

To subscribe to a free year of credit card account protection please click on the link below and follow the instructions that will be required:

Click Here To Get Your Free Year Of Credit Card Protection

Vulnerabilites

Vulnerabilities



http://www.cvedetails.com/

Mega-vulnerabilities

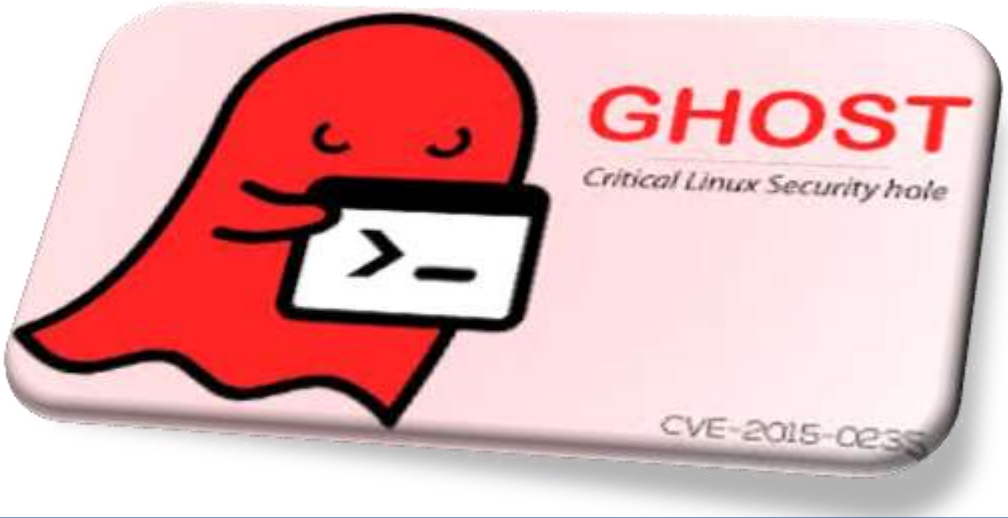
Heartbleed

Poodle

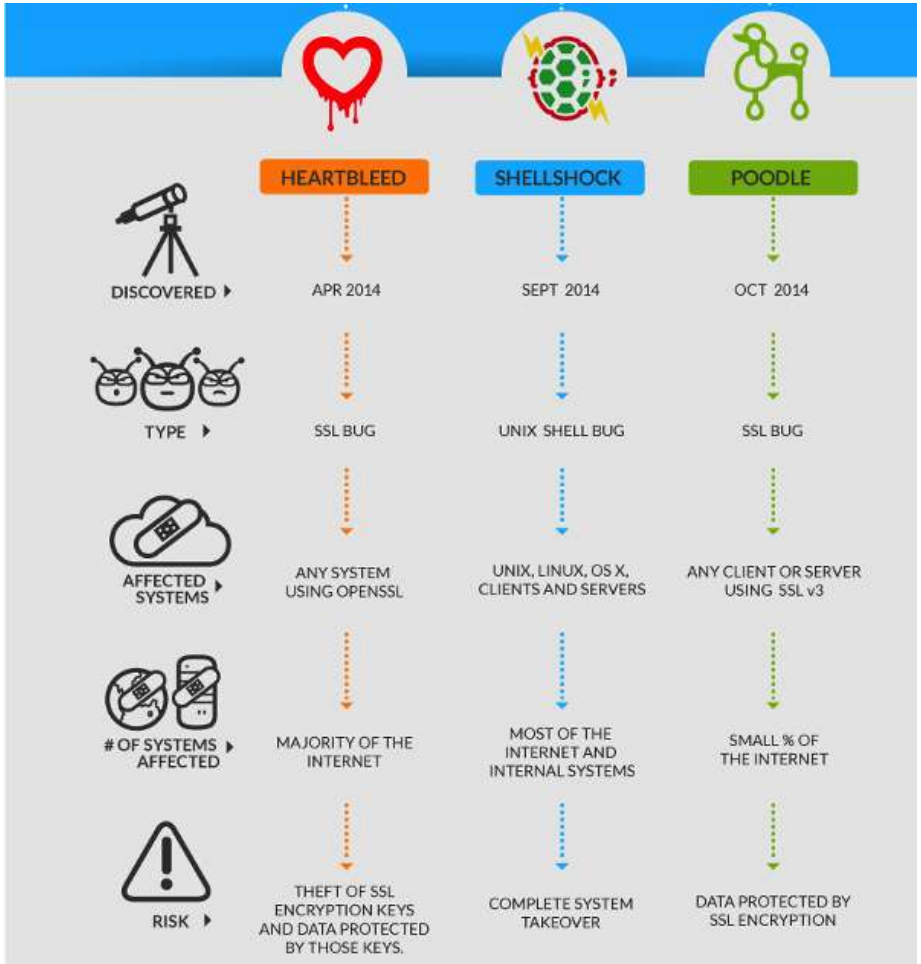
Mega-vulnerabilities

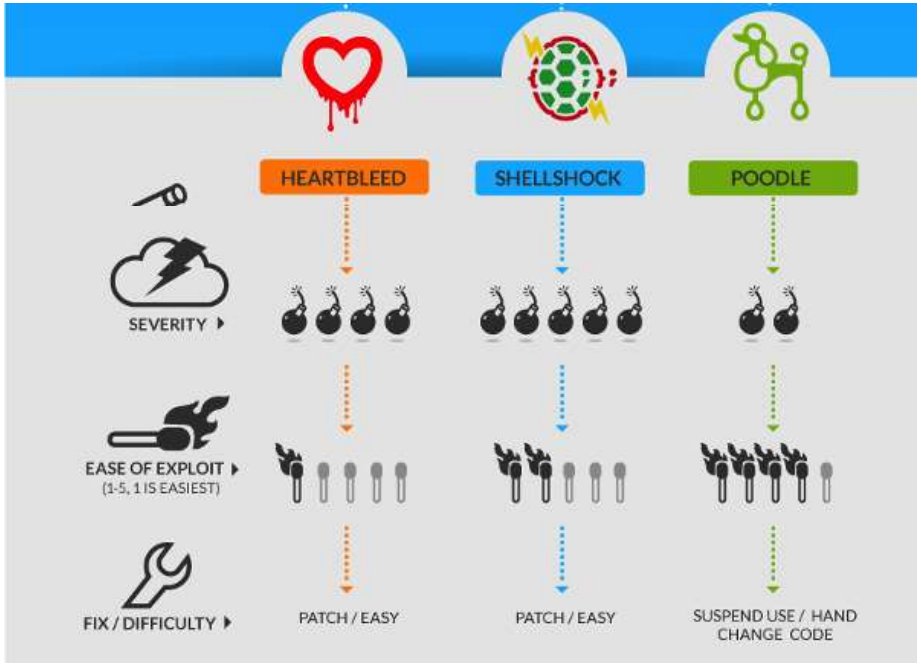
Shellshock

Ghost



Mega-vulnerabilities



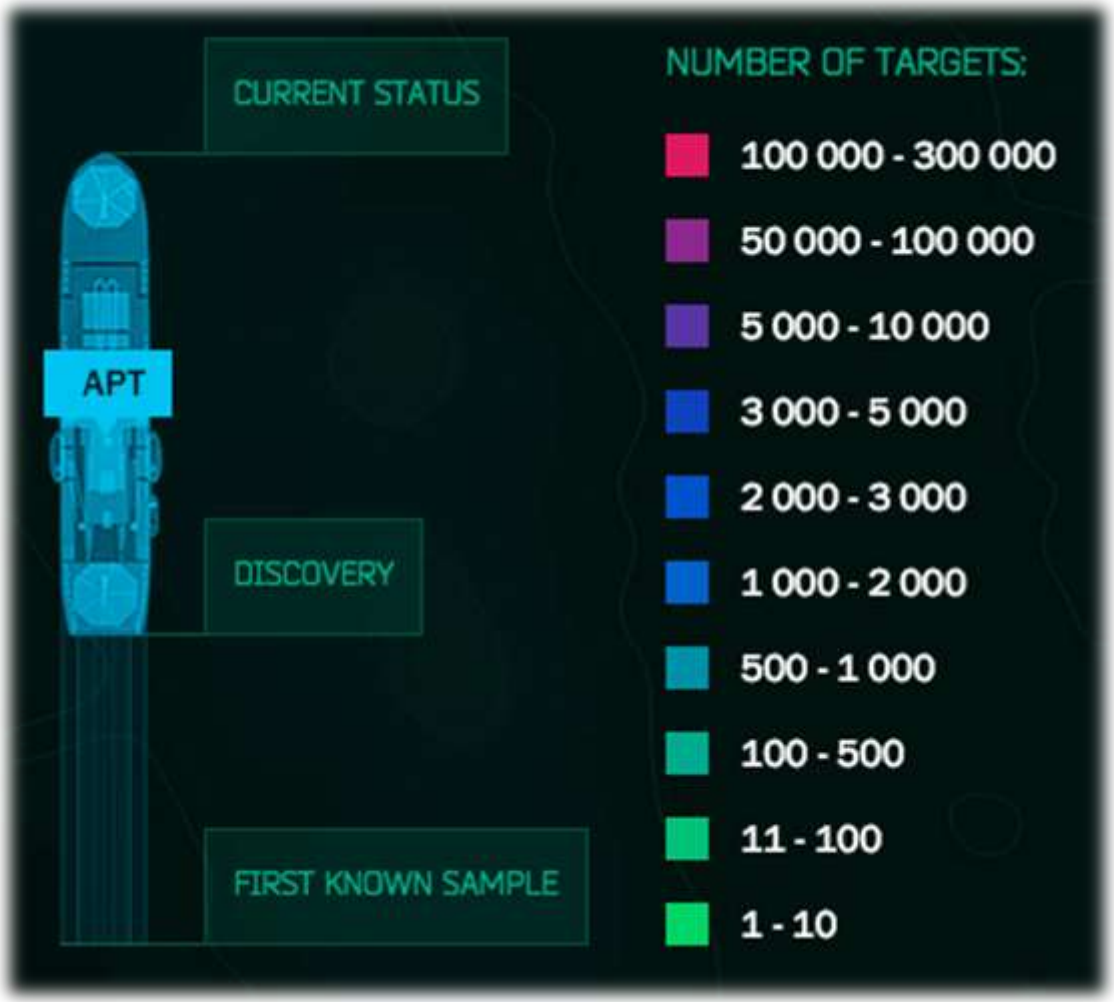


http://www.incapsula.com/blog/2014-mega-vulnerabilities.html

Malware

Advanced Persistent Threats

Advanced Persistent Threats



https://apt.securelist.com/

Trojan horses

All together

Denial of Service

Hacktivism & Cyberwar

http://map.ipviking.com/

And… ransomware!

And now?

Criminal mindset

Weakest link

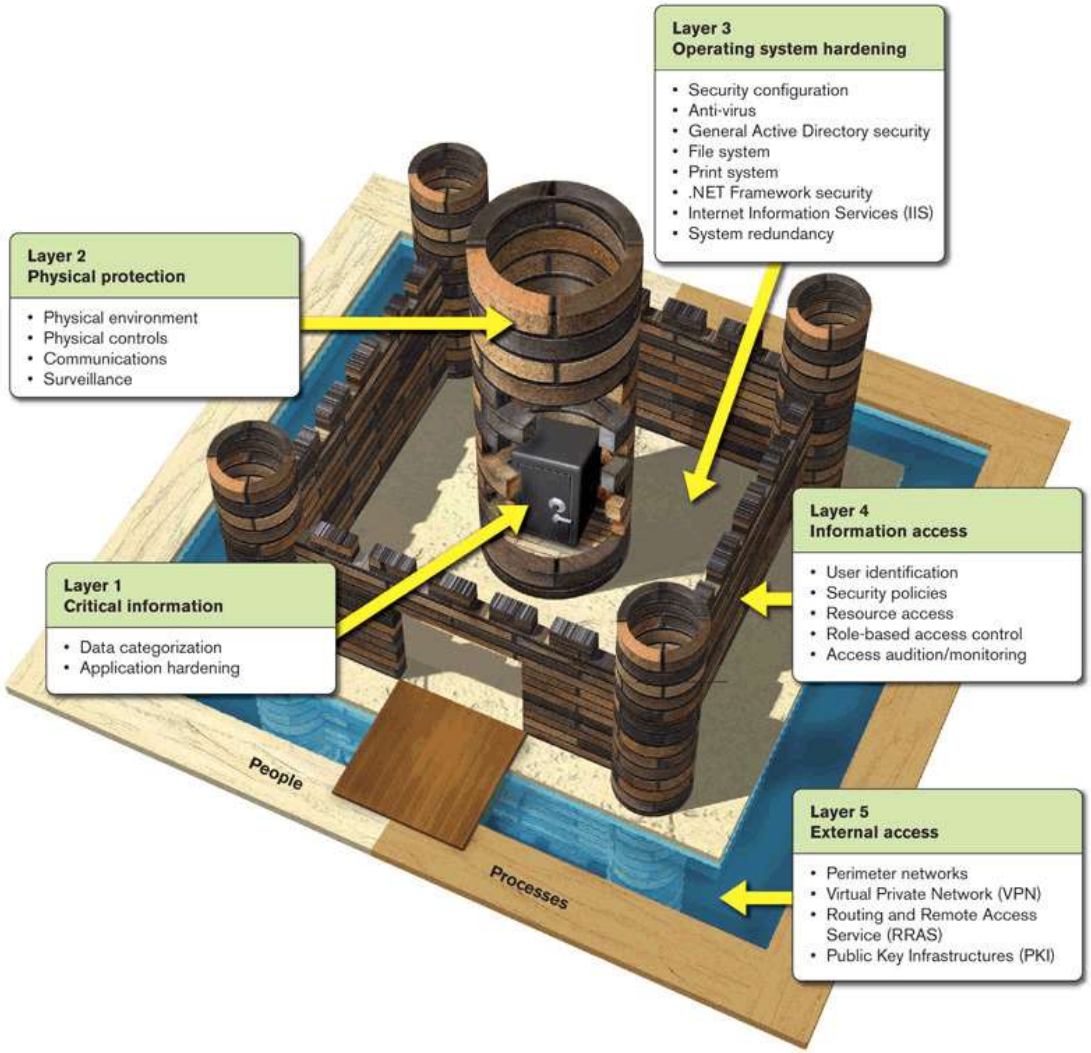
PCs are compromised

Smartphones are compromised

Apps are compromised

Protect everything

Security in depth



Monitor everything

Know yourself…

… and know your enemy

Forensics readiness

Event correlation

Big data and prediction

Cybersecurity Readiness

QUESTIONS