Your Talents Needed

Donald Dudenhoeffer,

Senior Information Technology Office, IAEA

Outline

Discuss 4 observations on computer security from developing programme guidance and from working with Member States

What are areas for improvement and how does this apply to you?

Observation 1: Knowing thy Enemy

The Threat – Adversary – Bad Guy

Most people have a hard time understanding the threat and thinking like the adversary.

Lone wolf?

Trusted Employee?

Dedicated group?

Who is the Adversary?

Threat Profiles and Classification

External and Internal threats	
Recreational Hackers	
Hacktivist	Social Activist
	Rogue Warriors
Disgruntled Individuals	Employees
	Contractors
	Third Parties
Terrorist	
Criminal Groups	
Nation States	

Motivation

Capability

Intention

Targets (People and Things)

Tactics

Observation 2: Often Fears <> Risk

Fears are not always aligned with the risk.

What do you fear in a cyber attack?

versus

What should you fear?

Fear versus Risk

Question asked during a Feb 2016 meeting on Cyber Threat:

Which of these animals do you fear the most?

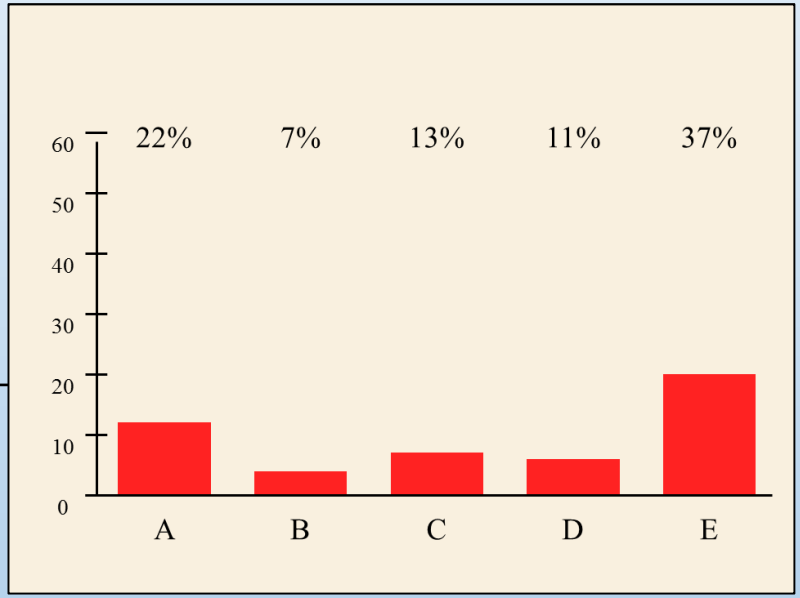
A.) Sharks

B.) Bees

C.) Spiders

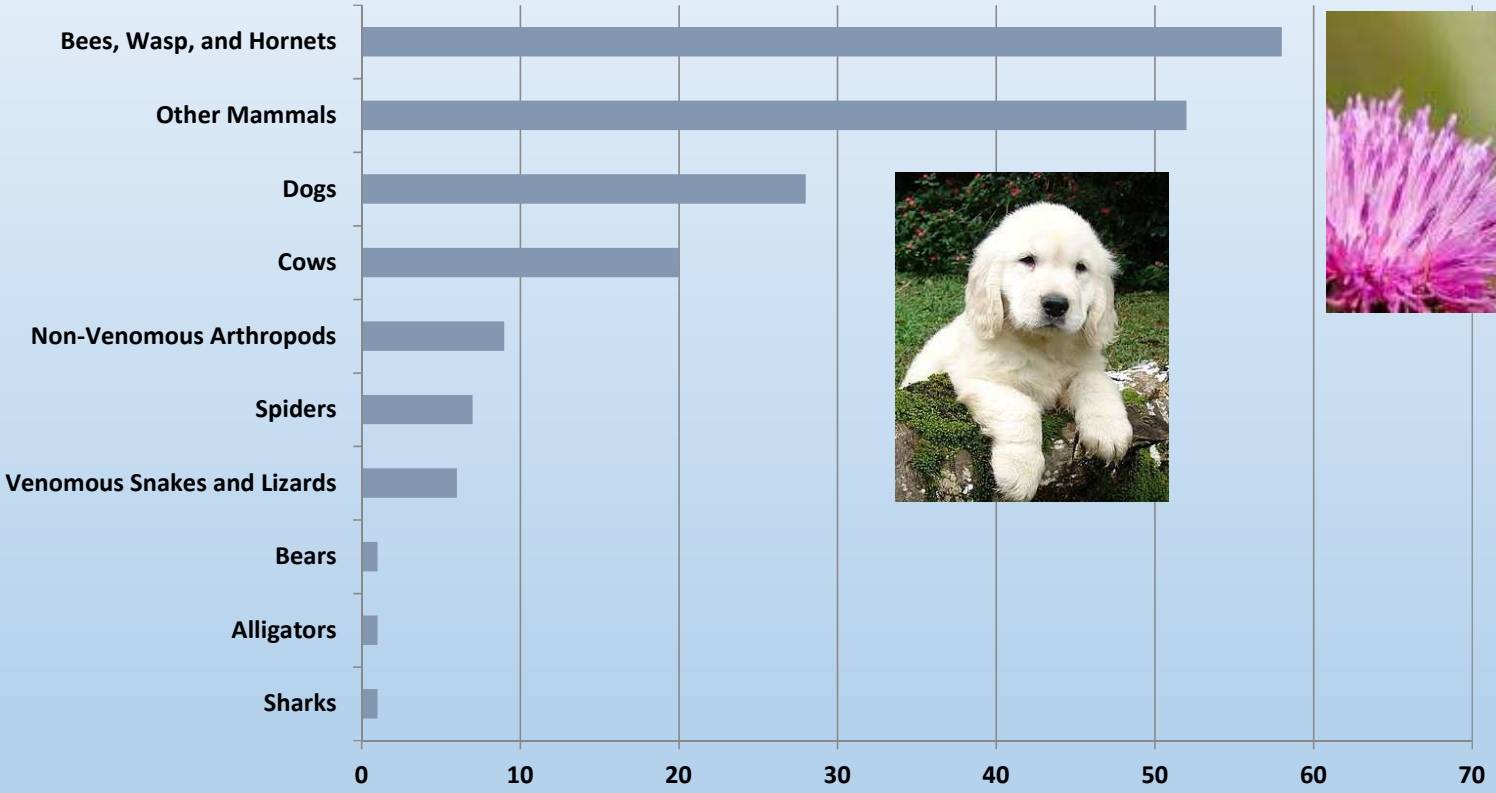
D.) Dogs

E.) Snakes



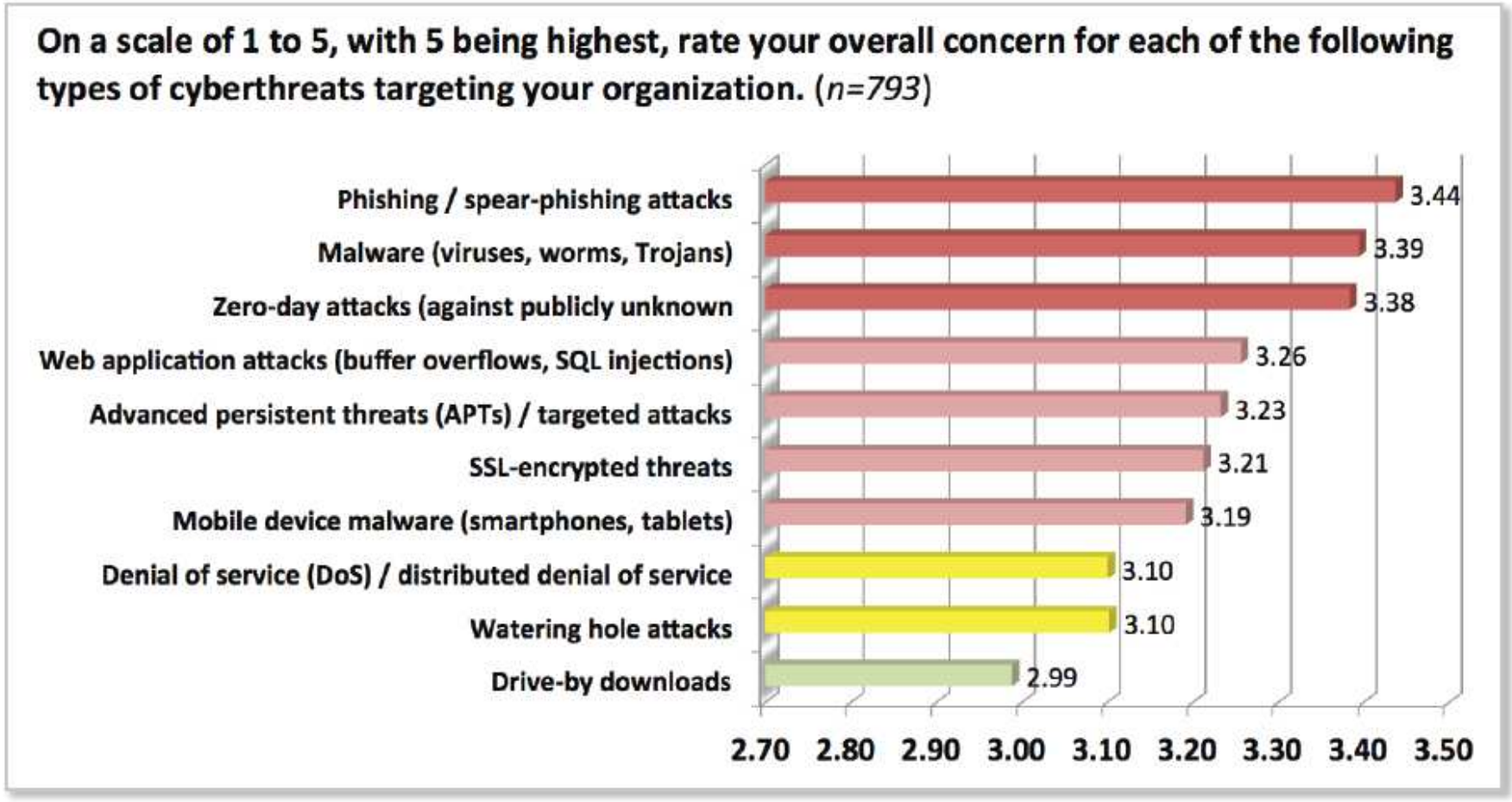
The animals that are most likely to kill you

Average annual animal-caused fatalities in the US 2001 - 2013



- https://www.washingtonpost.com/news/wonk/wp/2015/06/16/chart-the-animals-that-are-most-likely-to-kill-you-this-summer/

Survey –Cyber Fears?



Ref: 2015 Cyberthreat Defense Report:
North America & Europe
CyberEdge Group

Observation 3: Understandability

Fog of Complexity

- Digital I&C Architectures
- The Threat
- Attack Impact

Physical World – Well defined

Service history	
In service	1949–present
Designer	Mikhail Kalashnikov
Designed	1944–1947
Manufacturer	Izhmash
Number built	approximately 75 million AK-47 100 million AK-type rifles[
Specifications	
Weight	4.78 kg (10.5 lb) with a loaded magazine AKM weight with unloaded magazine 3.1 Kg.
Length	880 mm (35 in) fixed wooden stock 875 mm (34.4 in) folding stock extended 645 mm (25.4 in) stock folded
Barrel length	415 mm (16.3 in)
Cartridge	7.62×39mm M43/M67[
Action	Gas-operated, rotating bolt
Rate of fire	Cyclic rate of fire is 600 rounds/min[Semi-auto rate of fire is 40 rounds/min[Full-auto burst rate of fire is 100 rounds/min[
Muzzle velocity	715 m/s (2,350 ft/s)[
Effective range	350 metres (380 yd)
Feed system	Standard magazine capacity is 30 rounds. There are also 10, 20, 40, 75, or 100-round detachable box and drum style magazines.
Sights	Adjustable iron sights with a 378 mm (14.9 in) sight radius: AK-47 has 100–800 meter adjustments AKM has 100–1000 meter adjustments

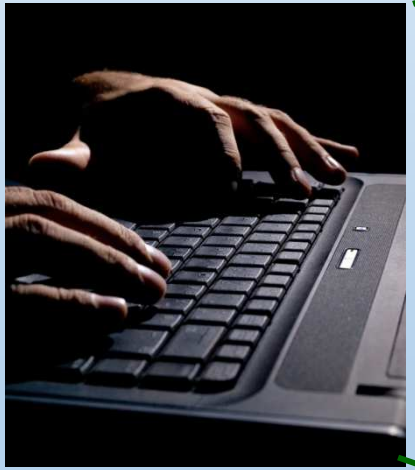
Impacts well understood

7.62×39mm		
Specifications		
Case type	Rimless, bottleneck	
Bullet diameter	7.92 mm (0.312 in)	
Neck diameter	8.60 mm (0.339 in)	
Shoulder diameter	10.07 mm (0.396 in)	
Base diameter	11.35 mm (0.447 in)	
Rim diameter	11.35 mm (0.447 in)	
Rim thickness	1.50 mm (0.059 in)	
Case length	38.70 mm (1.524 in)	
Overall length	56.00 mm (2.205 in)	
Case capacity	2.31 cm^3 (0.0356 gr H_2O)	
Rifling twist	240 mm (1 in 9.45 in)	
Primer type	Boxer Large Rifle	
Maximum pressure	355.00 MPa (51,488 psi)	
Filling	SSNF 50 powder	
Filling weight	18.21 gr	
Ballistic performance		
Bullet weight/type	**Velocity**	**Energy**
123 gr (8 g) Full metal jacket	731.5 m/s (2,400 ft/s)	2,073.6 J (1,529.4 ft·lbf)
154 gr (10 g) Spitzer SP	641.3 m/s (2,104 ft/s)	2,056.3 J (1,516.6 ft·lbf)
123.5 gr (8 g) Full metal jacket	804.7 m/s (2,640 ft/s)	2,460 J (1,810 ft·lbf)
123 gr (8 g) Full metal jacket	738 m/s (2,420 ft/s)	2,179 J (1,607 ft·lbf)
Test barrel length: 415 mm *Source(s): Wolf Ammo*[1] *Omar* [2] *Sellier & Bellot* [3]		

The Cyber Threat

How does one characterize the threat?

We can talk about Operational Characteristics of computers

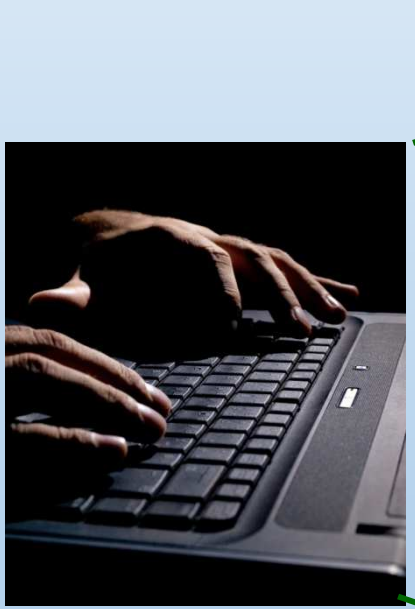


Processor
Intel® Core™ i7-2640M Dual Core (2.80GHz,4M cache,)
Operating System
Windows 7 Professional, No Media, 64-bit
Display
17.3" UltraSharp™ FHD(1920x1080) Wide View Anti-Glare LED-backlit
Memory
4GB3 DDR3 SDRAM at 1333MHz
Hard Drive
750GB 7200rpm Hard Drive
Video Card
AMD® FirePro® M8900 Mobility Pro Graphics with 2GB GDDR5
Optical Drive
8X DVD+/-RW
System Weight
7.77 lbs

The Cyber Threat

How does one characterize the threat?

But how does one characterize the range of attack vectors – targets and methods, impacts?



Culture

Observation 4: Culture is key.

Security is a people issue, not just a technical issue

- Without good training, technology cannot be effective
- Attacks against organizational staff including directed attacks are a common tactic by adversaries
- Over half of all computer security compromise results from or are complicated by human error
- People can be the strongest asset or your weakest link in security

Placing a Man on the Moon

President John F. Kennedy was visiting NASA headquarters for the first time, in 1961. While touring the facility, he introduced himself to a janitor who was mopping the floor and asked him what he did at NASA.

The janitor replied, “I’m helping put a man on the moon!”

Obviously, the janitor understood the importance of his contribution. He truly felt he was a valuable part of something bigger than himself, and his attitude created a feeling of self-confidence in his mission. He wasn’t merely a janitor; he was a member of the 1962 NASA Space Team!

How to we empower and motivate each employee to be part of the Security Team.

Ref: http://www.tlnt.com/2012/06/07/company-goals-do-your-employees-have-a-line-of-sight-to-them/

Conclusions

Greater awareness and understanding of computer security is needed at all levels

- Cyber adversaries continue to advance at a rapid pace
- Attack methods may be sophisticated, but also they often take advantage of human failure
- Everyone is a target of attack
- Talent is needed across many disciplines and levels.

Questions

Donald D. Dudenhoeffer
Nuclear Security Information Officer
International Atomic Energy Agency
Vienna International Centre
A-1400 Wien
Austria
Tel: +43 (1) 2600-26424
Fax: +43 (1) 2600-29299
d.dudenhoeffer@iaea.org