Cyber Crimes
the Good, the Bad, and the Ugly

Mohd Serieh
QCB Information & Security Conference
November 2017
"I have internet access but I don’t shop online, this means I won’t become a victim of Cyber Crime."

Is this statement True or False?

FALSE
Knowledge check

“Cybercrime is limited to any criminal act dealing with computers and networks”

Is this statement True or False?

TRUE
Knowledge check

“Cybercrime includes only traditional crimes conducted through the internet”

Is this statement True or False?

TRUE
Knowledge check

“70% of fraud is cyber enabled”

Is this statement True or False?

TRUE
The good
The average total cost of data breach decreased by 11% this year.

The average cost for each lost or stolen record containing sensitive and confidential information also significantly decreased 12% this year.

Source: 2017 Cost of Data Breach Study: Global Overview
Ponemon Institute, June 2017
2. More corporates are starting to rely on cloud security

- No plans yet: 11%
- Putting plans together, unsure when will deploy: 17%
- Putting plans together, deployment end of year: 28%
- Pilot deployment in place: 18%
- A full-service deployment in place: 19%
- Several services are in place, fairly mature: 9%

Source: Amazon estimates based on 1000 compute cycles (300 compute cycles, 700 peak cycles) and data transfer (3000 GB of In data and 6,000 GB of “out” data).

Source: Gartner, “Private Cloud Matures, Hybrid Cloud Is Next,” Thomas J. Bittman,
3. Year-end cybercrime update 2016

• The hacker behind JPMorgan Chase Hack, world’s largest-ever bank hack, arrested in Russia;
• Hacker Gets 4 Years in Prison for Selling Stolen Bank Accounts on the Dark Web;
• Teen Behind Titanium DDoS Stresser Pleads Guilty in London: used to launch over 1.7 million DDoS attacks;
• FBI Arrests Customer of Xtreme Stresser DDoS-for-Hire Service;
• Joint Cyber Operation Takes Down Avalanche Criminal Network Servers Enabled Nefarious Activity Worldwide;
• Hacker known as Guccifer sentenced to 52 months in prison;
• And the list goes on...
The bad
Cybercrime trends are higher than any other category

There were almost 6M incidents of fraud and cybercrime last year, according to the 2016 Crime Survey for England and Wales- more than any other category of crime, and almost as much as all the other categories measured in the survey when added together.

Source: million incidents
And so are the costs

Worldwide security spending ($bn)

- 2016: 80
- 2017: 86
- 2018: 93

Source: Gartner
Furthermore, highly regulated industries have the highest per-record data breach costs

- Healthcare: $359
- Education: $294
- Pharmaceutical: $227
- Financial: $206
- Consumer: $155
- Energy: $141
- Hospitality: $122
- Retail: $105

*Currencies converted to US dollars
Source: 2014 Cost of Data Breach Study: Global Analysis, Ponemon Institute, sponsored by IBM
And the ugly
Most enterprises lack security capabilities

Source: McKinsey Cyber Risk Maturity Survey (CRMS)
And they know it!

How prepared is your company for a cyber event? KPMG research

Are we prepared? Seventy-two percent of CEOs say they are not fully prepared for a cyber event, 50% more than 2015

Can you be fully prepared? CEOs frequently said: “we are as prepared as we can be” or “you can never be fully prepare”

How to prepare? By practicing the ability to respond to cyber events. Companies need an ability to be agile and deal with the unexpected
There are only two types of companies: Those that have been hacked and those that don’t know they have been hacked.

Robert S. Mueller, III, Director FBI
Just like infections, there is an incubation period for hacks

Incubation period in weeks

Chicken pox  Ebola  Rabies  HIV

People know they are infected, WHEN the symptoms start showing. NOT when they are infected.

Hacking is like infection, Your systems do not know they are hacked until it is too late.
Scared Yet?

- Hardware and software keep getting cheaper;
- Combine the Internet and a global scope, the potential for attacks is limitless;
- Security will always be breached;
- Even when laws are passed to increase technological safeguards, new technology will always outstrip legislation.
What are you going to do about it?
Here are the questions any CISO want to be able to answer...

|--------------------------|--------------------------|---------------------------|---------------------|------------------------|----------------|
| Identify what needs to be defended or observed as well as formulate a risk profile to detect abnormalities  
- Who are the attractive targets?  
- Which applications to defend?  
- What is the normal behavior profile for users, assets, and application | Gain awareness of a motivated/incentivized attacker attempting to hide/disguise the attack  
- Which assets are already compromised?  
- Which external domain may be the source of attacks?  
- Are there any low profile network traffic elements that might signal an ongoing imminent attack? | Identify or warn of users within the organization who may be inclined to perform actions that are detrimental to the organization’s operations  
- What data is being leaked or lost and by whom?  
- Who internally has the motivation to compromise the cyber operation?  
- Who is exhibiting abnormal usage behavior? | Alert to a possible attack from groups that sympathize with causes that are contrary to the interests  
- Which controversial issues may trigger a negative sentiment about the organization?  
- How to identify and monitor intentions?  
- How does publicity of the company in the media impact risk? | Inform of an impeding or ongoing attack by criminal groups  
- Which geographical region may be the origin of an attack?  
- Which hacking tools maybe used and who is gaining access to them?  
- Are there symptoms of an attack underway or being planned manifesting themselves as support issues? | Surface new or existing fraud methods that may compromise its compliance with regulations or cause significant losses to its financial operations  
- How can the organization identify a fraudulent activity?  
- Which users have compromised identities that may lead a fraudulent activity?  
- Can well known fraud attempts have patterns can either be detected or even anticipated? |
And no one knows backdoor answers, like our good old friend The Hacker
What is a hacker?

1. Creates and modifies computer software and computer hardware;
2. Exploits systems and gains unauthorized access through clever tactics and detailed knowledge;
3. Computer enthusiast/person who enjoys learning programming languages;
4. Someone who breaks into computers;
5. Can make a computer do what they want;
6. Anyone who ‘breaks open’ code and manipulates it in a clever or original;
7. Not necessarily illegal.
Kevin Mitnick (AKA The Darkside Hacker)

The US Department of Justice called him “the most wanted computer criminal in US history”

After serving a year in prison for hacking into the Digital Equipment Corporation’s network, he was let out for three years of supervised release. But near the end of that period, he fled and went on a 2.5-year hacking spree that involved breaching the national defense warning system and stealing corporate secrets.
He infiltrated 97 US military and NASA computers, by installing virus and deleting a few files.

All the efforts to satisfy his curiosity.
Part of hacking group called lulzSec who
Gained credentials for hacking into Sony,
News International, CIA, FBI, Scotland Yard,
and several noteworthy accounts. So
notorious was the group that when it hacked
into News Corporations account, they put
across a false report of Rupert Murdoch
having passed away.
Topiary also an associate of Anonymous
Adrian Lamo

Hacked into Yahoo!, Microsoft, Google, and The New York Times. This, although culminated into his arrest, it later helped him gain the batch of an American Threat Analyst. A guy who would hack into top-notch accounts sitting in the spacious and comforting cafeterias, libraries, internet cafes, soon turned Wikileaks suspect Bradley Manning over to FBI. While Manning was arrested for leaking several hundred sensitive US government documents, Lamo went hiding or should we presume, undercover?
Targeting the over-sensitive nerves, what Mathew Bevan along with his alleged partner Richard Pryce did, could have triggered great many issues between USA and North Korea. The duo hacked the US military computers and used it as a means to infiltrate the foreign systems. The crucial contents of Korean Atomic Research Institute were dumped into USAF system. However, the contents were majorly relevant to South Korea and hence, less volatile. But this, nonetheless, could have led to a huge international issue.
Hector Monsegur (AKA Sabu)

An American computer hacker and co-founder of the hacking group LulzSec.

He later turned informant for the FBI, working with the agency for over ten months to aid them in identifying other hackers from LulzSec and related groups.

LulzSec intervened in the affairs of organizations such as News Corporation, Stratfor, UK and American law enforcement bodies and Irish political party Fine Gael.
Jan Krissler used high resolution photos, including one from a government press office, to successfully recreate the fingerprints of Germany’s Defence Minister, Ursula von der Leyen.
So what are you going to do about it??
“Hire the hacker!”

Underworld investigator Journalist Misha Glenny
Big companies do that already

George Hotz
His famed PlayStation 3 and Apple phone hacks served as resume fodder to his current employer.

Peter Hajas
Peter Hajas is the creator of uber-popular iOS jailbreak app MobileNotifier.

Jonny Lee
Famously hacked a Nintendo Wiimote using a few ballpoint pens and infrared lights.

Jeff Moss
AKA "Dark Tangent" the founder of Black Hat and the annual DefCon computer hacker conference.

Chris Putnam
Created an XSS-based worm on Facebook and modified infected pages to look just like MySpace profiles.
“What I did in my youth is hundreds of times easier today. Technology breeds crime.”

Frank Abagnale
Types of hackers

**White Hat**

- White Hat”- hired by large corporations, or governments Usually as a “Tiger Team”
- Tiger Team is a team that is hired to test the security of networks/find flaws or loopholes
- Will snoop around networks, trying to find loopholes
- If such loophole(s) is/are found – report created explaining how hack was achieved

**Grey Hat**

- Unhired, People who break into networks for fun, Usually don’t intentionally cause harm (following hacker ethic). Enjoy doing this, Perceived as challenge. Want to “test security to prevent such attacks in future”

**Black Hat**

- Stereotypical hacker you hear about in the media, Break into systems and damage them
- May write things like “you just got served by X group” May delete files, erase portions of code, etc.”
Why you should consider legal hacking

01. You need experienced security professionals, People who know how to defend networks, systems, Innovation, forward thinking

02. Penetration testing is part of the (larger) security auditing/analysis process

03. To perform comprehensive security analysis process takes into account many other aspects (e.g., source code analysis, policy analysis, social engineering

04. You want somebody who can find problems before the bad guys do
Only the paranoid survive

Andrew S. Grove, the President and CEO of Dell
Thank you

mohd.serieh@vodafone.com