Cybersecurity & Disruptive Technologies

Narudom Roongsiriwong, CISSP

NECTEC-ACE 2018, September 25, 2018

About Me

- Information Security since 1995
- SVP, Head of IT Security, Kiatnakin Bank
- Committee Member, Thailand Banking Sector Computer Emergency Response Team (TB-CERT)
- Vice President, OWASP Thailand Association
- Committee Member, Cloud Security Alliance (CSA), Thailand Chapter
- Committee Member, National Digital ID Project, Technical Team
- Chief Information Security Officer (CISO) of the Year 2017, NetworkWorld Asia

The Art of War

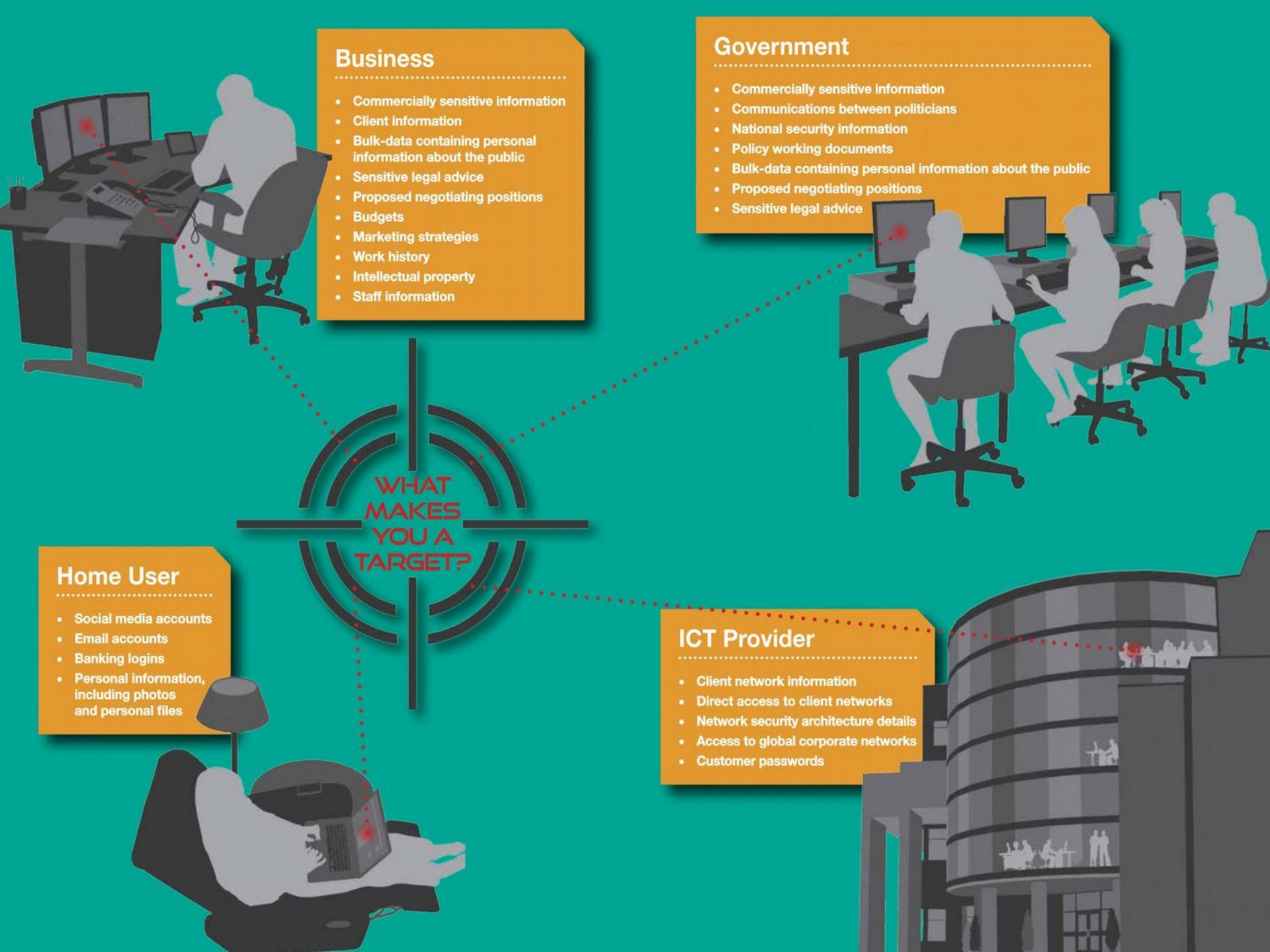
If you know the enemy and know yourself, you need not fear the result of a hundred battles.

If you know yourself but not the enemy, for every victory gained you will also suffer a defeat.

If you know neither the enemy nor yourself, you will succumb in every battle.

Sun Tzu

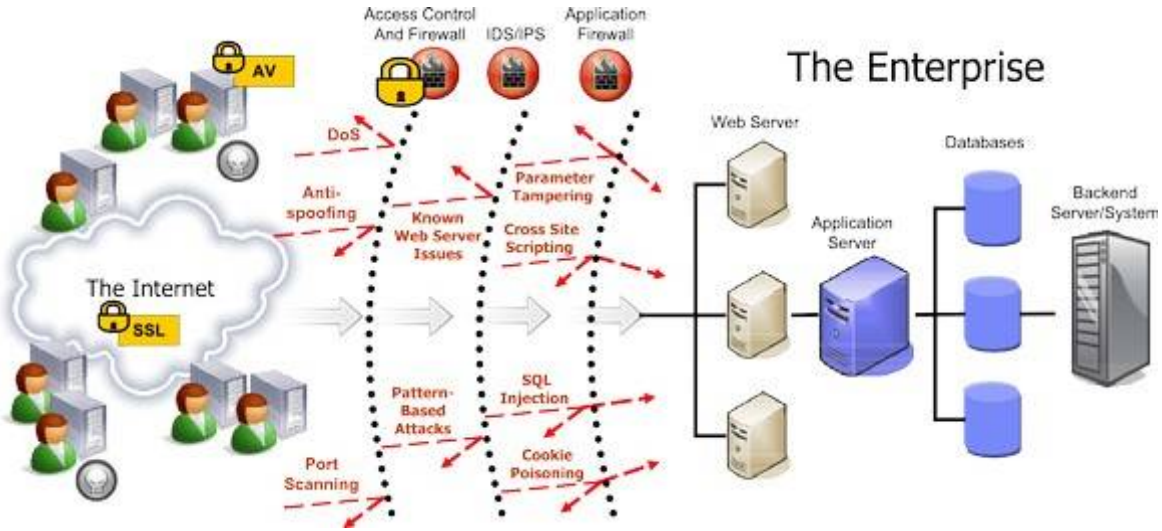

Know
Your
Enemies


Business
Commercially sensitive information
Client information
Bulk-data containing personal information about the public
Sensitive legal advice
Proposed negotiating positions
Budgets
Marketing strategies
Work history
Intellectual property
Staff information
Government
Commercially sensitive information
Communications between politicians
National security information
Policy working documents
Bulk-data containing personal information about the public
Proposed negotiating positions
Sensitive legal advice
WHAT MAKES YOU A TARGET?
Home User
Social media accounts
Email accounts
Banking logins
Personal information, including photos and personal files
ICT Provider
Client network information
Direct access to client networks
Network security architecture details
Access to global corporate networks
Customer passwords

Opportunistic vs Targeted Attacks

Opportunistic		Targeted
Many Try to attack as many users as they can.	Target	Few Focus on just one target with specific goal.
Old Use tried tested methods to exploit common vulnerability.	Tricks	New Use new, zero-day exploits on computer systems attackers might familiar with.
Make Money The prize is to make as much money as possible.	Intention	Do Damage The purpose is to steal or damage valuable data.
Don't Hide Often no point hiding the damage done	Covert	Silent But Deadly The aim is to leave little to no trace of entering the system.

How Attackers Do #1: Attacks Directly to Servers or Devices



Why Do Hackers Hack?

- Just for fun
- Steal the valuable protected information such as credit card or personal medical record information
- Perform unauthorized transactions
  - Money transfer
  - Goods shipping without payment
- Deploy malware to client machines those view these sites
- Use the hacked server or device for other purposes
  - Hacking their real target servers with scapegoat servers
  - Cryptocurrency Mining

Application Security

Percentage of web applications Trustwave application scanning services tested in 2017 that displayed at least one vulnerability

100%

11

Median number of vulnerabilities detected per application

Vulnerabilities Trustwave Managed Security Testing detected in 2017

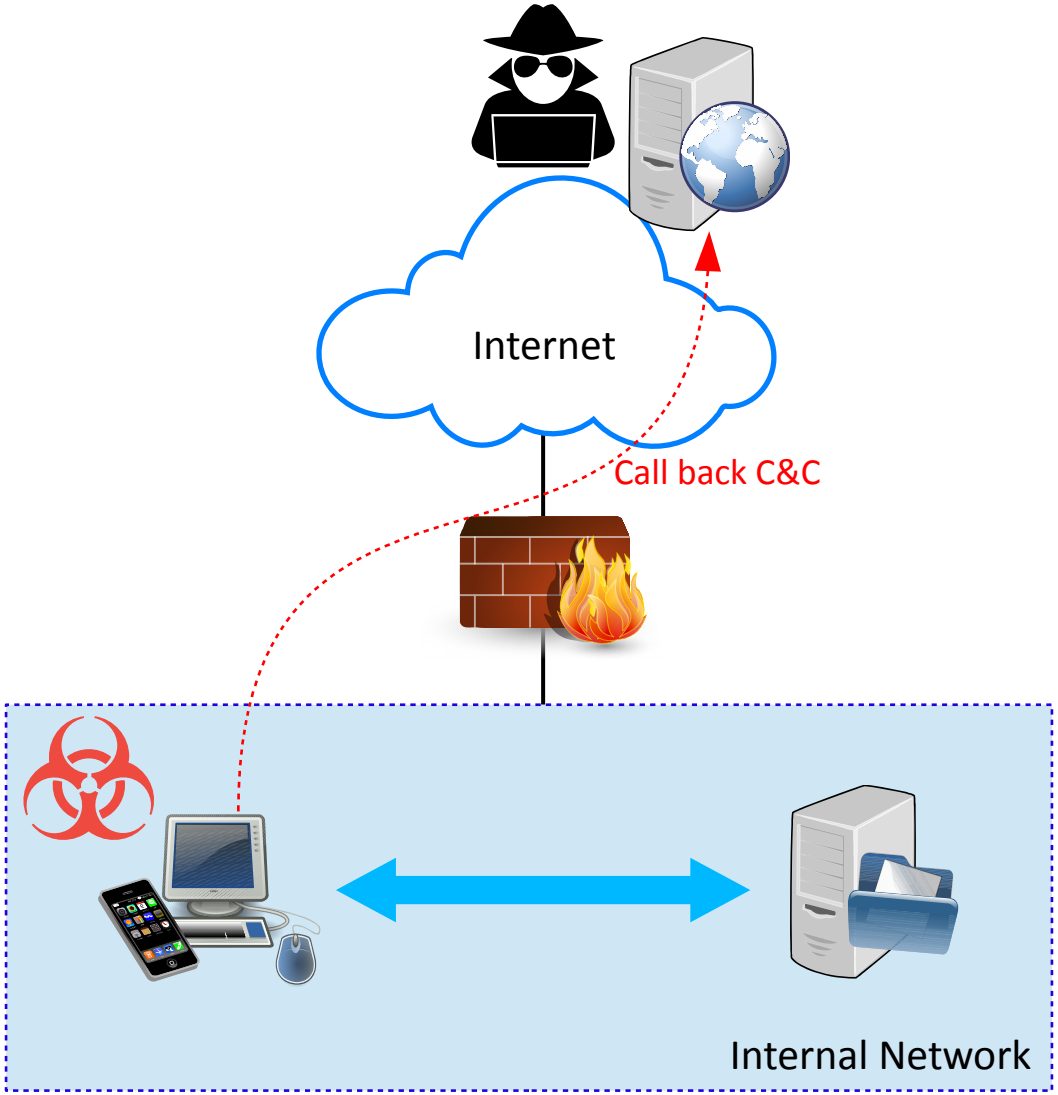
86%

involved session management

8%

were classif ed as high-risk or critical

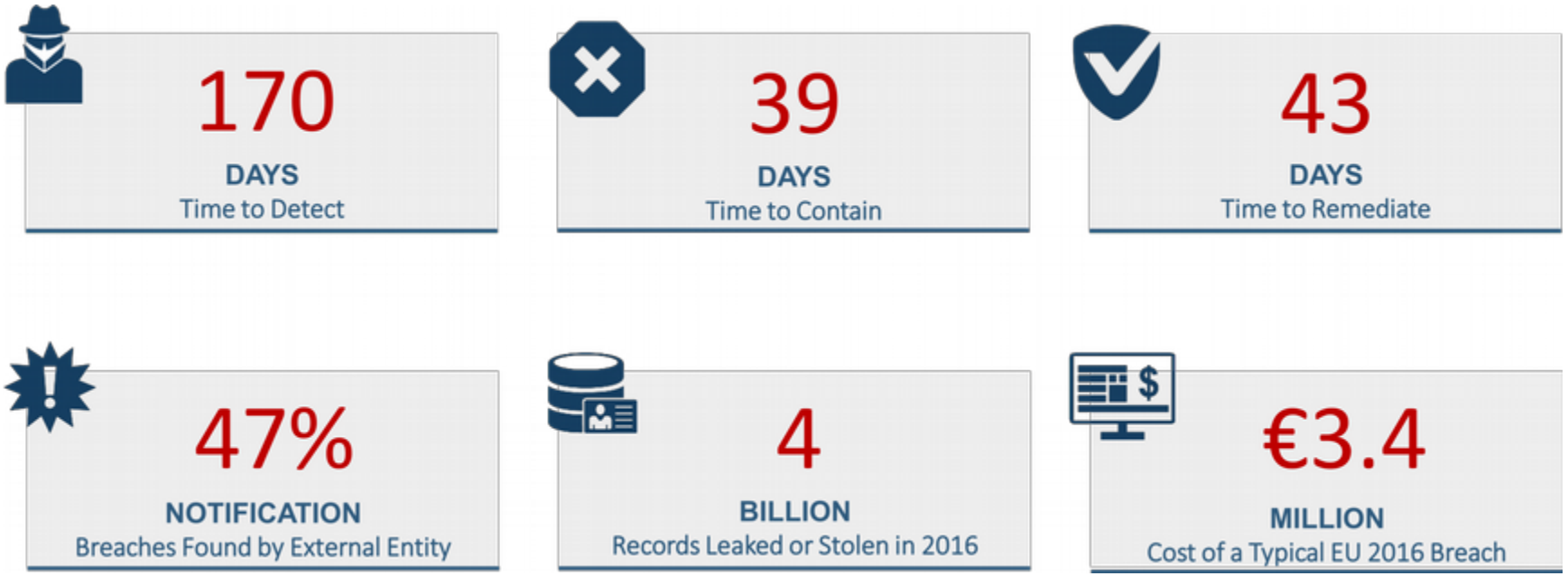
Know Your Enemies #2: Attacks with Malware



Complexity of Attack Examples

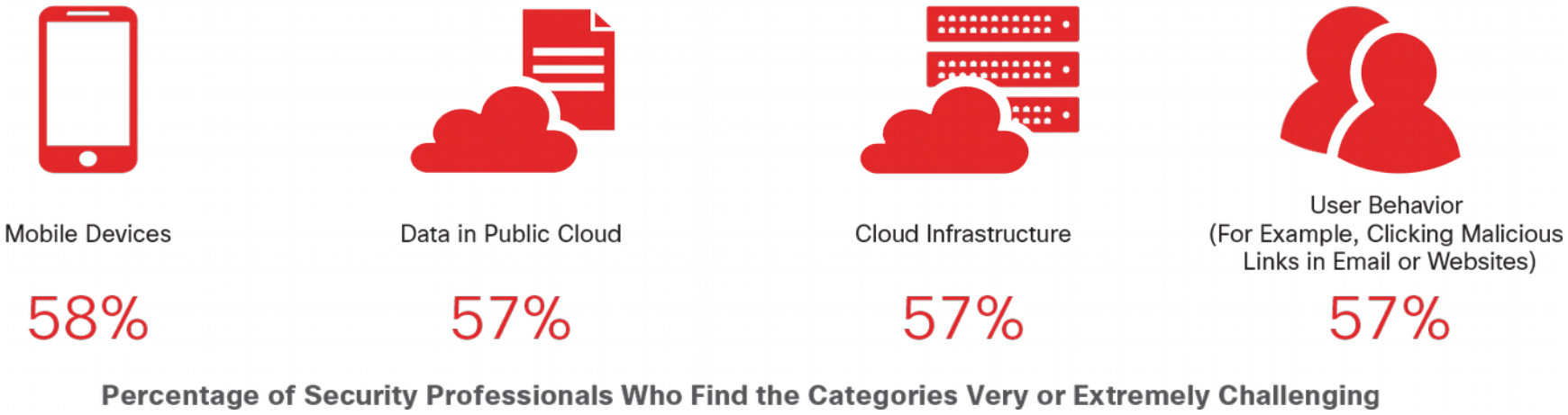

Google
Sag "Ok Google"...
17:09
Hangouts
Twitter
Instagram
Facebook
Play Musik
Google+
Spotify
Fotos
Play Spiele
Know
Yourself

Compromise and Data Breach Statistics



Source: IBM Security

Security Professionals Biggest Sources of Concern Related to Cyber Attacks



Source: Cisco 2017 Security Capabilities Benchmark Study

The 25 Most Common Passwords of 2017

1	123456	6	123456789	11	admin	16	starwars	21	hello
2	password	7	letmein	12	welcome	17	123123	22	freedom
3	12345678	8	1234567	13	monkey	18	dragon	23	whatever
4	qwerty	9	football	14	login	19	passw0rd	24	qazwsx
5	12345	10	iloveyou	15	abc123	20	master	25	trustno1

Source: SplashData Annual Report

THE IMPORTANCE OF MOBILE SECURITY IN TWENTY SEVENTEEN

80% of the adults on **earth** will have a smartphone by 2020.

Source: World Bank, GSMA, a16z

75% or more mobile apps will **fail** basic security tests

11% of all apps leak **sensitive data** over the network

35% of communications sent by mobile devices are **unencrypted**

24% of mobile applications have at least **one high risk** security flaw

50% of popular apps send your **data** to an ad network including, but not limited to: phone numbers, IMEI numbers, call logs, location coordinates and more…

So what can you do to **protect** yourself?


Q&A