

CyberSecurity: State of the Nation(s)

Pierre Noel
Asia Chief Security Officer





Attackers are highly skilled, persistent, and very motivated at finding and exploiting new vectors

Over 2000 attacks recorded in 2014 alone !

Organizations with enormous security budgets and elite security analysts are **struggling** to address these modern threats

Traditional 'defense in depth' approach is not sufficient and typical breaches stay undiscovered for months

This is real

Cyber Security is like a virus outbreak. It must be treated with same answers and focus

Everyone is a target

Impacts are financial, operational and reputational

Basic hygiene and preparedness are essential

Rapid identification and containment

It begins by acknowledging the risk in everything you do, and build a **resilient infrastructure**

WHAT do

CYBERCRIME

HACKTIVISM

TERRORISM

Have in common?

NO RULES



HOW do the

CYBERCRIMINALS

HACKTIVISTS

TERRORISTS

See **US?**



Sobering statistics

200+

The median # of days that attackers reside within a victim's network before detection



76%

of all network intrusions are due to compromised user credentials



\$500B

The total potential cost of cybercrime to the global economy



\$3.5M

The average cost of a data breach to a company



The frequency and sophistication of cybersecurity attacks are getting worse.

Security



level issue



WE DO NOT FORGIVE WE DO NOT FORGET

File Edit Cyber

TIME Sub

SECTIONS

SOUTH KOR

ANONYMOUS
WE ARE LEGION

Most South Korean Credit Card Holders Have Details Stolen in Massive Breach

Air As

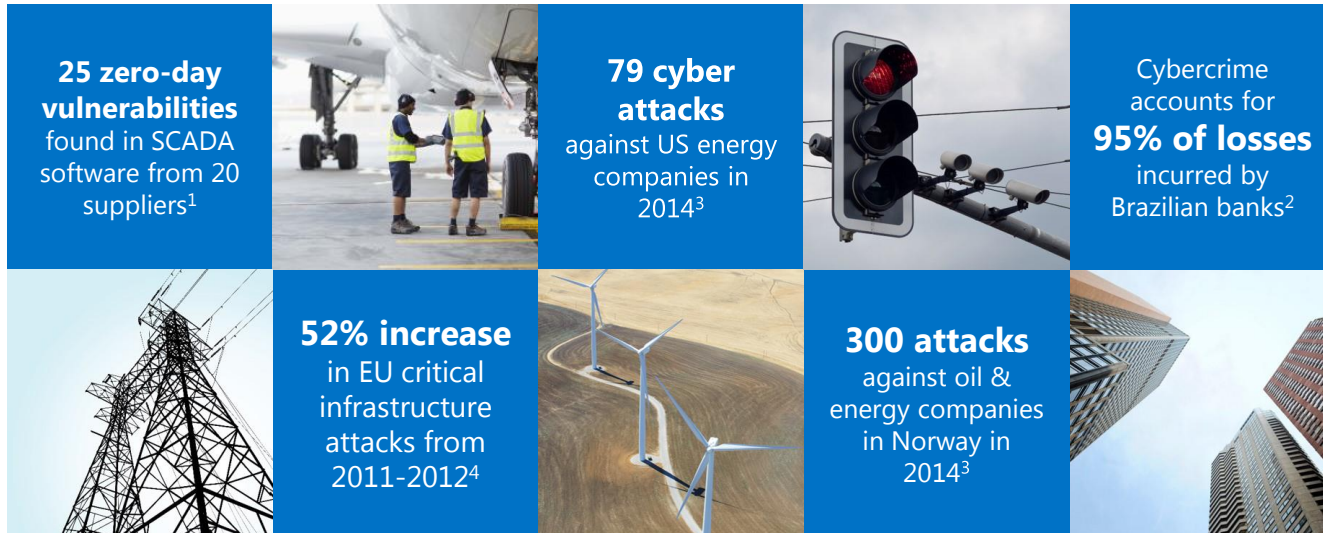
Cyber attacks are a global threat

2013 headlines from around the world



Infrastructure is a prime attack target

Statistics from the front lines



Sources:

¹ [Wired](#), 10-16-2014

² [New York Times](#), 7-2-2014

³ [Fox News](#), 11-25-2014

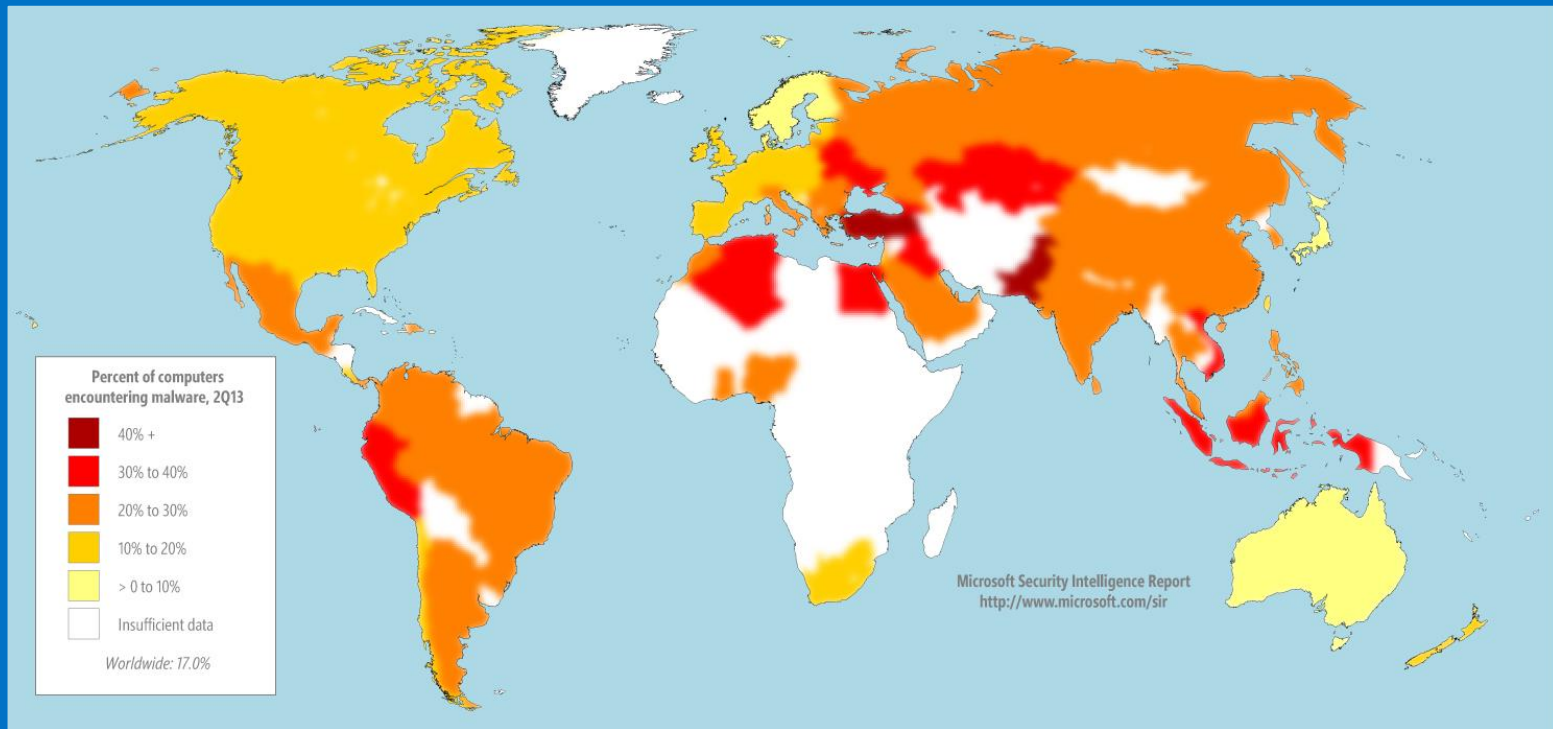
⁴ European Union Agency for Network and Information Security (ENISA), [Threat Landscape Report](#) 2013

State of the Nation

You think you live in a safe place? When you are on the Internet, your computer might as well be located in Syria or Afghanistan...

Encountered Malware by Region — 4Q14

source: Security Intelligence Report (www.microsoft.com/sir)

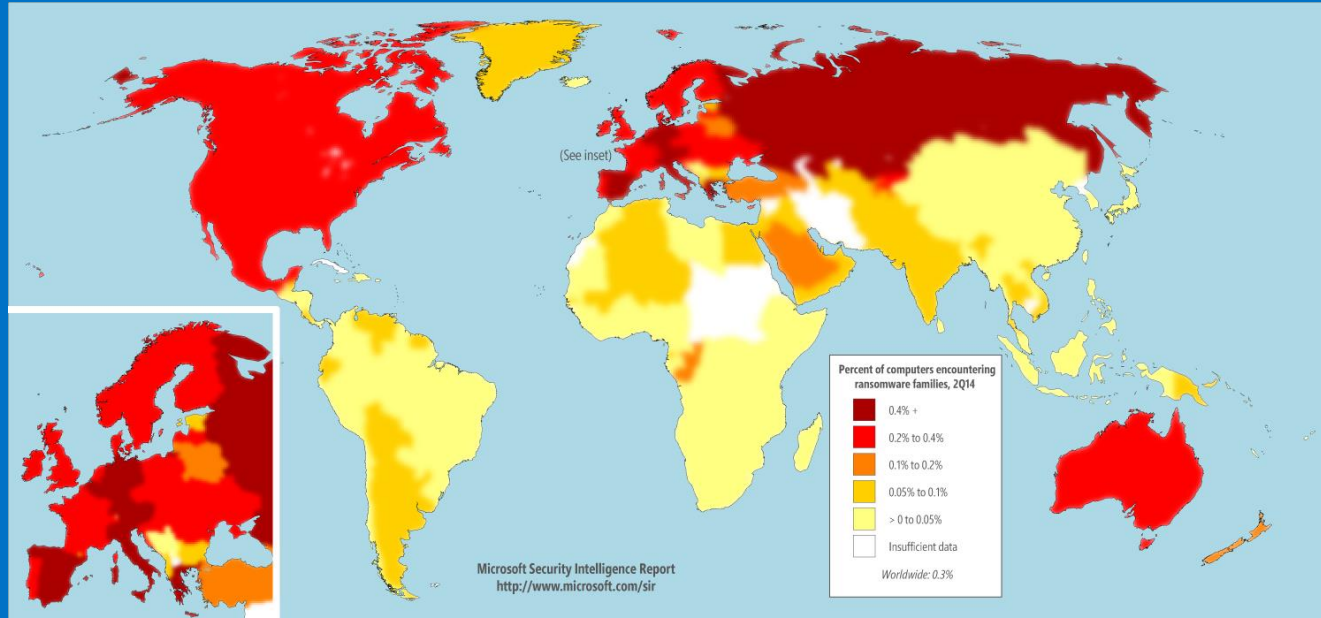


Ransomware



Ransomware by country or region

2H14



Where are my risks? Search no further....

	HDD Samples Examined	HDD Samples Infected	HDD Infection Rate
Thailand	51	43	84.31%
Vietnam	41	38	92.68%
Indonesia	44	26	59.09%
Malaysia	50	26	52%
Philippines	30	13	43.33%
Total	216	146	67.59%

Key Findings

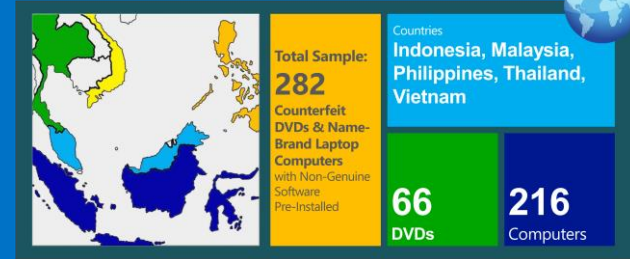
Computer infection rates by market:



Brands affected: Acer, Asus, Dell, HP, Lenovo, Samsung, Toshiba
Hard-drive swapping apparent on **28% of PCs**



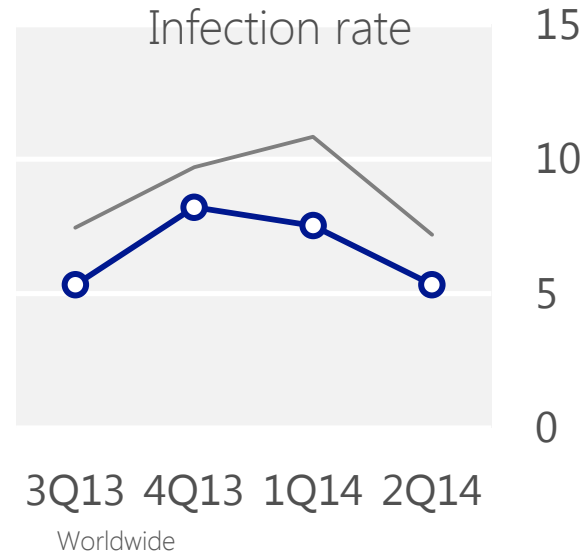
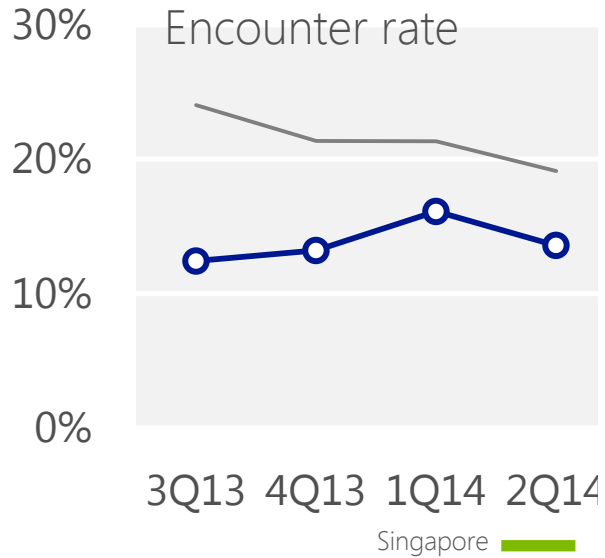
The Sample



	DVD Samples Examined	DVD Samples Infected	DVD Infection Rate
Thailand	23	16	69.57
Vietnam	9	6	66.67
Indonesia	19	19	100%
Malaysia	5	4	80%
Philippines	10	4	40%
Total	66	49	74.24%

Malware encounters and infections

Singapore



What IS Working

What it takes



Governance

Accountability

Compatible with
the Culture

Dynamic Risk
Management

Data classification is core to security



Growing data sources

- Data classification and metadata
- Archival, retention, and disposal
- Policies and tools

Managing at the individual level

- Employees, partners, and customers
- Permeate access policies across the org

Various access points

- Secure access to data on personal or company devices
- Manage access points

Do's and Don'ts

Do not fight the corporate culture

Someone must be ultimately responsible

"If you protect your paper clips and diamond with equal vigor, you will soon have more paper clips and fewer diamonds"

Dean Rusk (USA Secretary of States 1961 – 1969)

Start with simple data classification

Know your risks. What are they, where are they?

Behind every security problem is a human being

Do have anti virus on every machine

Systems must be Resilient And Managed

Australia's Top 35



Australia's Top 4

Patching applications and using the latest version of an application

Patching operating systems

Keeping admin right under strict control
(and forbidding the use of administrative accounts for email and browsing)

Whitelisting applications

CyberSecurity: State of the Nation(s)

Pierre Noel
Asia Chief Security Officer

