The Institute of
Internal Auditors
Indonesia

2014 ACIIA CONFERENCE BALI, INDONESIA

ASIAN CONFEDERATION OF INSTITUTE OF INTERNAL AUDITORS

The Stones Hotel - Legian, Bali

24 - 25 November 2014

Organized by:

Supported by:

Cybercrime and Security

State of the Nation

Pierre Noel

Asia Chief Security Officer

Microsoft

Why am I talking to you?

Over 1M Internet facing servers Worldwide

2nd most attacked organization, behind Pentagon

Trustworthy Computing, 11 years ago

Taking down bad people….

Security and privacy should be a top leadership concern

Managing risk in an increasingly connected world

security in terms of **new vulnerabilities**.

243

median # of days **attackers are present** on a victim network **before detection**

$ 3.5M

Average cost of a data breach to a company

15 % increase YoY

Security

is a

CEO

level issue

Job security

Customer loyalty

Implications

Brand reputation

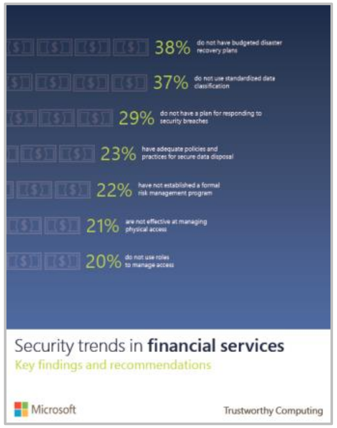
Legal liability

Intellectual property

Impact of cyber attacks could be as much as **$3 trillion** in **lost productivity and growth**

Market trends

Security trends report



38% do not have budgeted disaster recovery plans

37% do not use standardized data classification

29% do not have a plan for responding to security breaches

23% have adequate policies and practices for secure data disposal

22% have not established a formal risk management program

21% are not effective at managing physical access

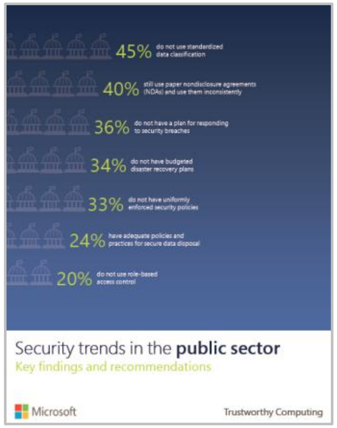
20% do not use roles to manage access

Security trends in **financial services**

Key findings and recommendations

Microsoft

Trustworthy Computing



45% do not use standardized data classification

40% still use paper nondisclosure agreements (NDAs) and use them inconsistently

36% do not have a plan for responding to security breaches

34% do not have budgeted disaster recovery plans

33% do not have uniformly enforced security policies

24% have adequate policies and practices for secure data disposal

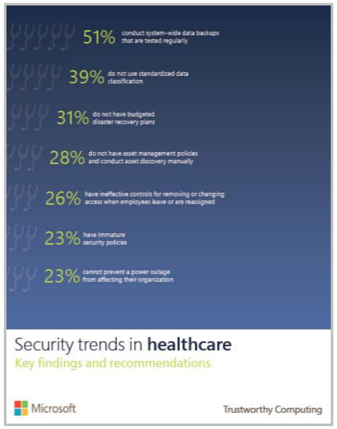
20% do not use role-based access control

Security trends in the **public sector**

Key findings and recommendations

Microsoft

Trustworthy Computing



51% conduct system-wide data backups that are tested regularly

39% do not use standardized data classification

31% do not have budgeted disaster recovery plans

28% do not have asset management policies and conduct asset discovery manually

26% have ineffective controls for removing or changing access when employees leave or are reassigned

23% have immature security policies

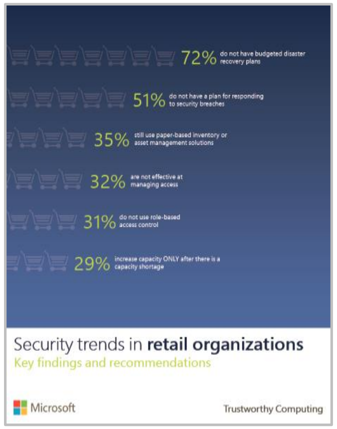
23% cannot prevent a power outage from affecting their organization

Security trends in **healthcare**

Key findings and recommendations

Microsoft

Trustworthy Computing



72% do not have budgeted disaster recovery plans

51% do not have a plan for responding to security breaches

35% still use paper-based inventory or asset management solutions

32% are not effective at managing access

31% do not use role-based access control

29% increase capacity ONLY after there is a capacity shortage

Security trends in **retail organizations**

Key findings and recommendations

Microsoft

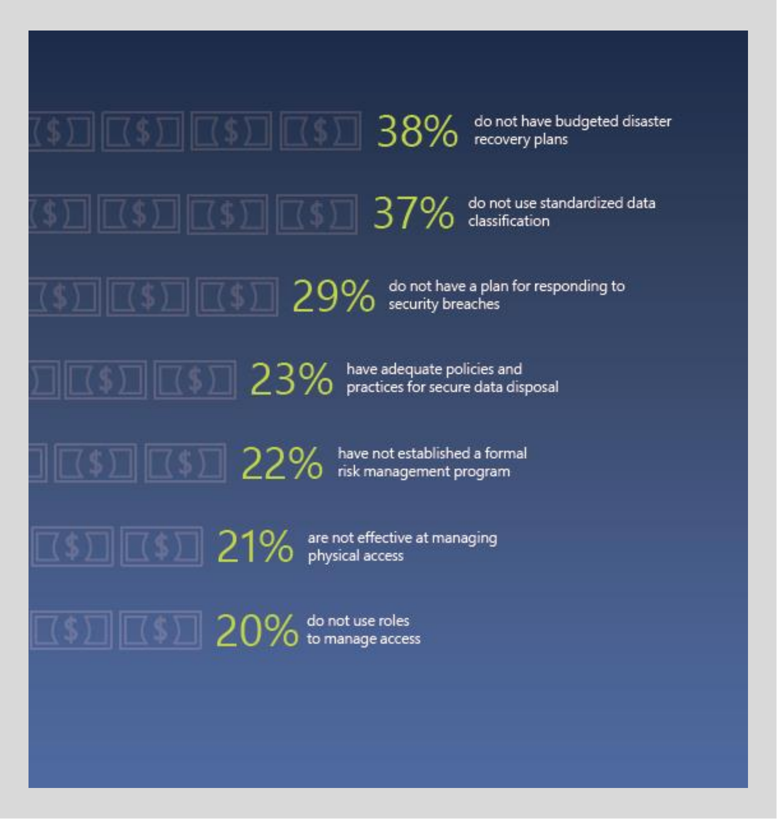
Trustworthy Computing

12,000 anonymized surveyed results

Cloud security readiness tool

Worldwide user base

Security trends for banking



38% do not have budgeted disaster recovery plans

37% do not use standardized data classification

29% do not have a plan for responding to security breaches

23% have adequate policies and practices for secure data disposal

22% have not established a formal risk management program

21% are not effective at managing physical access

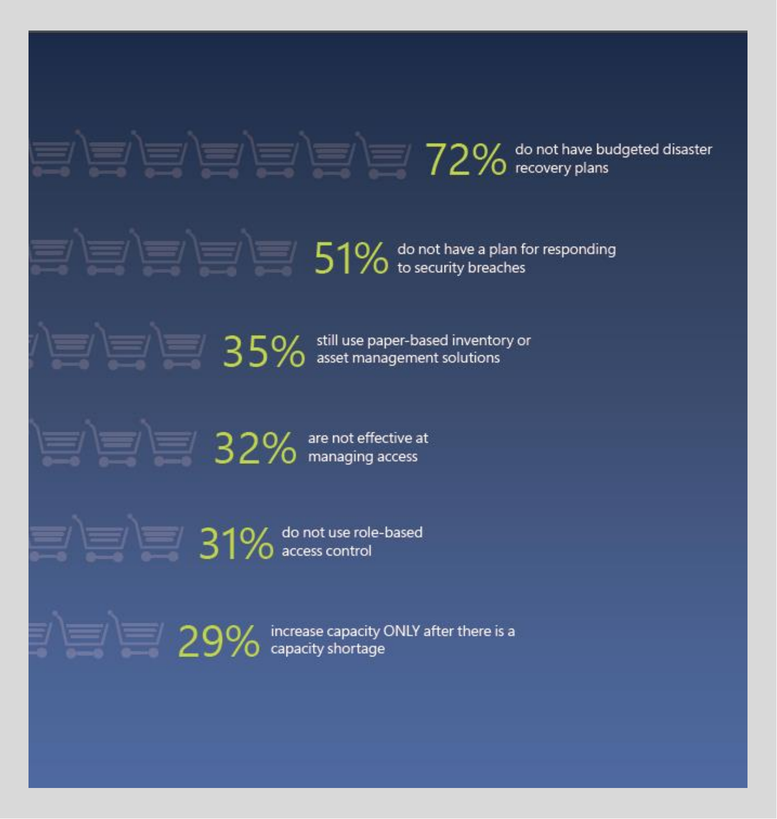
20% do not use roles to manage access

38% of surveyed financial organizations do not have budgeted disaster recovery plans

37% of surveyed financial organizations do not use standardized data classification

23% of surveyed financial organizations have adequate policies and practices for secure data disposal

Security trends for retail



72% do not have budgeted disaster recovery plans

51% do not have a plan for responding to security breaches

35% still use paper-based inventory or asset management solutions

32% are not effective at managing access

31% do not use role-based access control

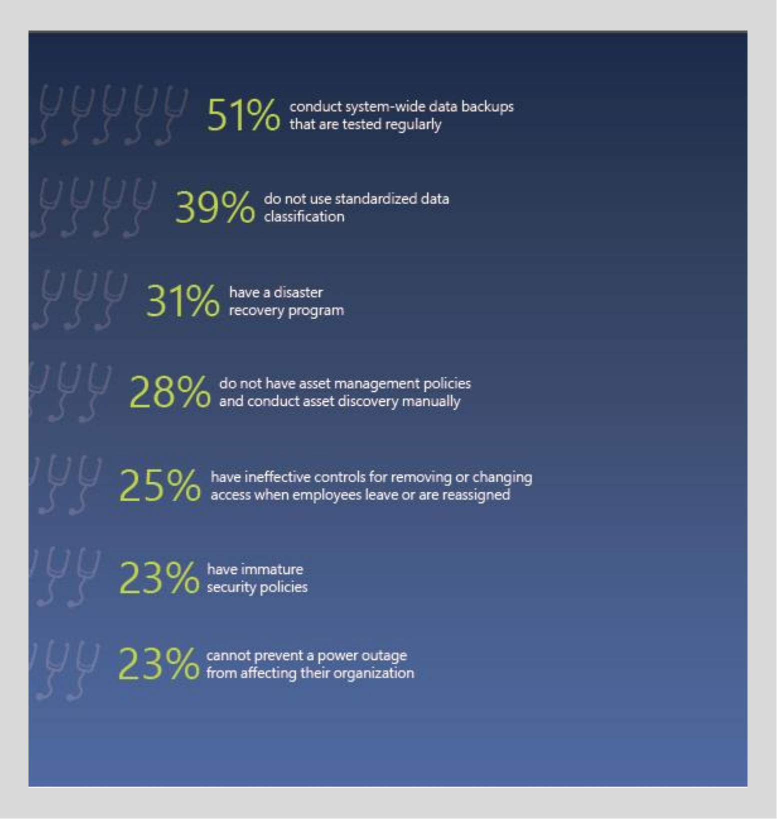
29% increase capacity ONLY after there is a capacity shortage

72% of surveyed retail organizations do not have budgeted disaster recovery plans

51% of surveyed retail organizations do not have a plan for responding to security breaches

31% of surveyed retail organizations do not use role-based access control

Security trends for healthcare



51% conduct system-wide data backups that are tested regularly

39% do not use standardized data classification

31% have a disaster recovery program

28% do not have asset management policies and conduct asset discovery manually

25% have ineffective controls for removing or changing access when employees leave or are reassigned

23% have immature security policies

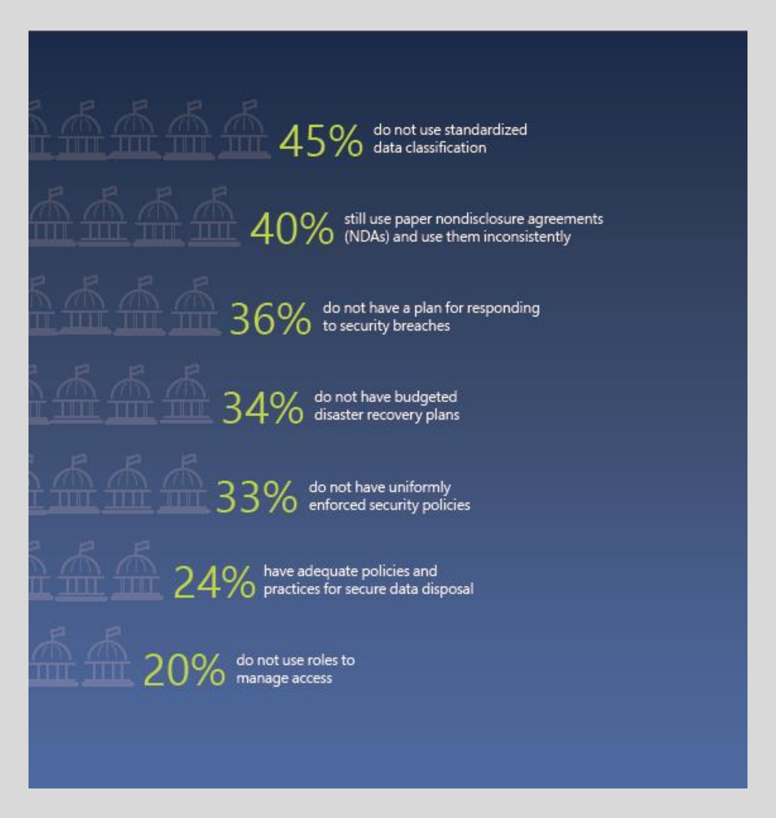
23% cannot prevent a power outage from affecting their organization

51% of surveyed healthcare organizations conduct system-wide data backups that are tested regularly

31% of surveyed healthcare organizations have a disaster recovery program

23% of surveyed healthcare organizations cannot prevent a power outage from affecting their organization

Security trends for government



45% do not use standardized data classification

40% still use paper nondisclosure agreements (NDAs) and use them inconsistently

36% do not have a plan for responding to security breaches

34% do not have budgeted disaster recovery plans

33% do not have uniformly enforced security policies

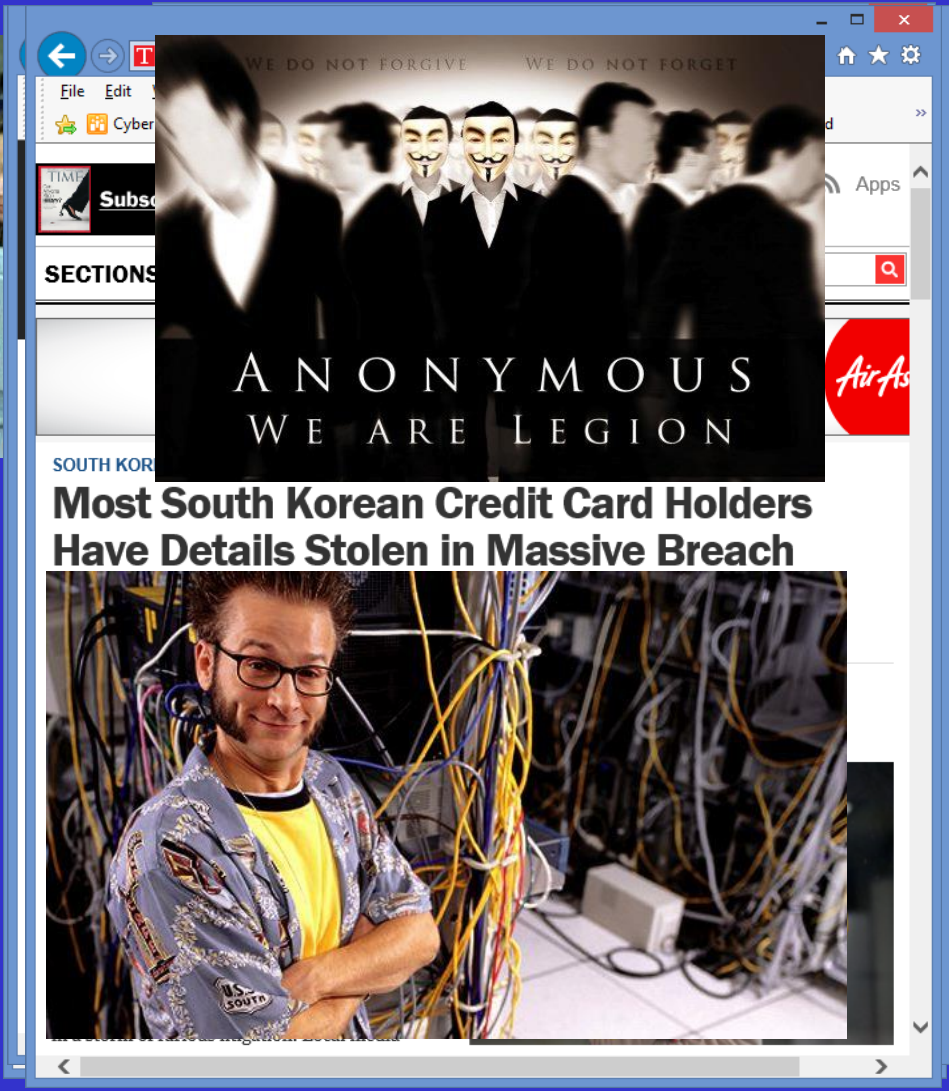
24% have adequate policies and practices for secure data disposal

20% do not use roles to manage access

45% of surveyed public sector organizations do not use standardized data classification

40% of surveyed public sector organizations still use paper Non-Disclosure Agreements (NDAs) and use them inconsistently

33% of surveyed public sector organizations do not have uniformly enforced security policies



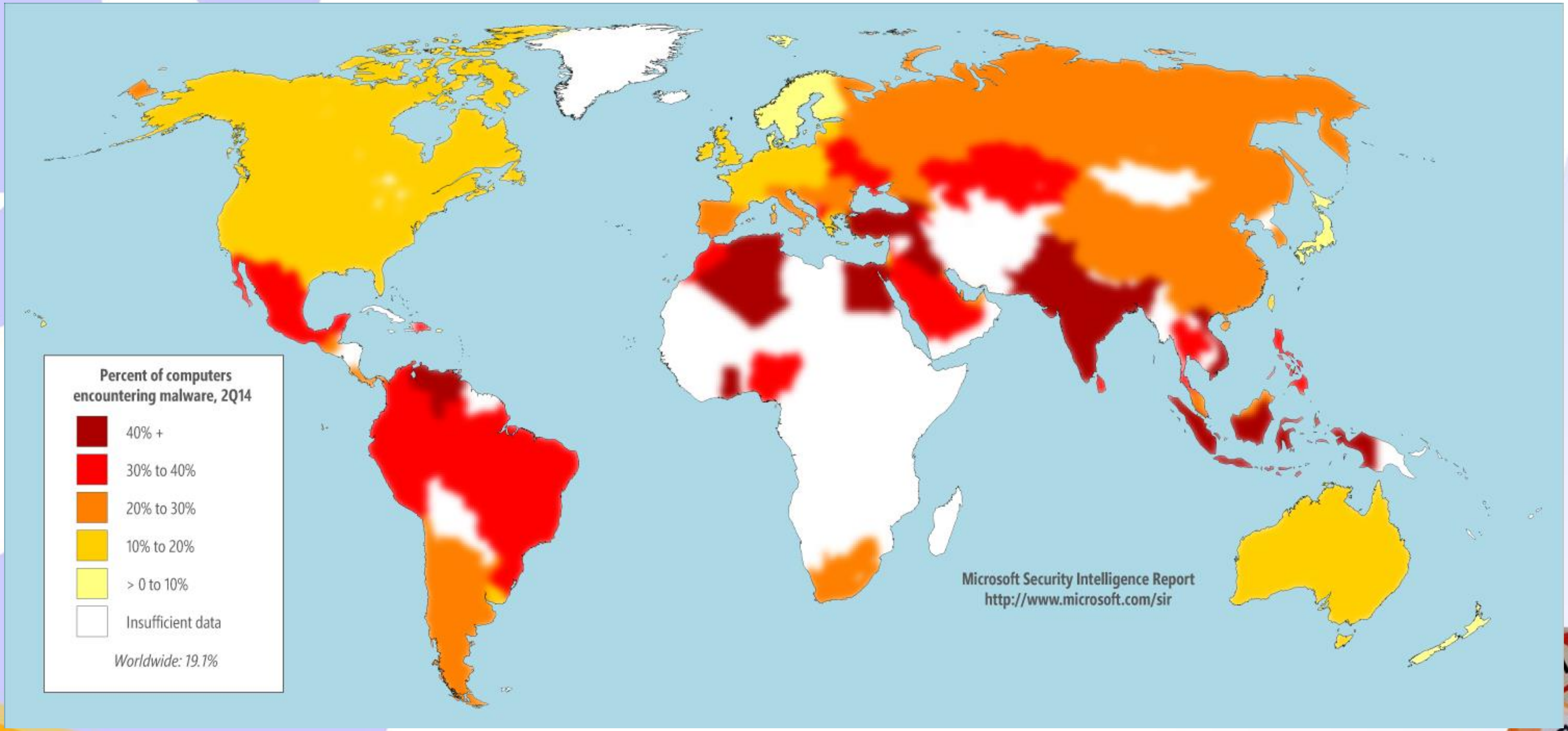
SOUTH KOR

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

State of the Nation

ER by country or region

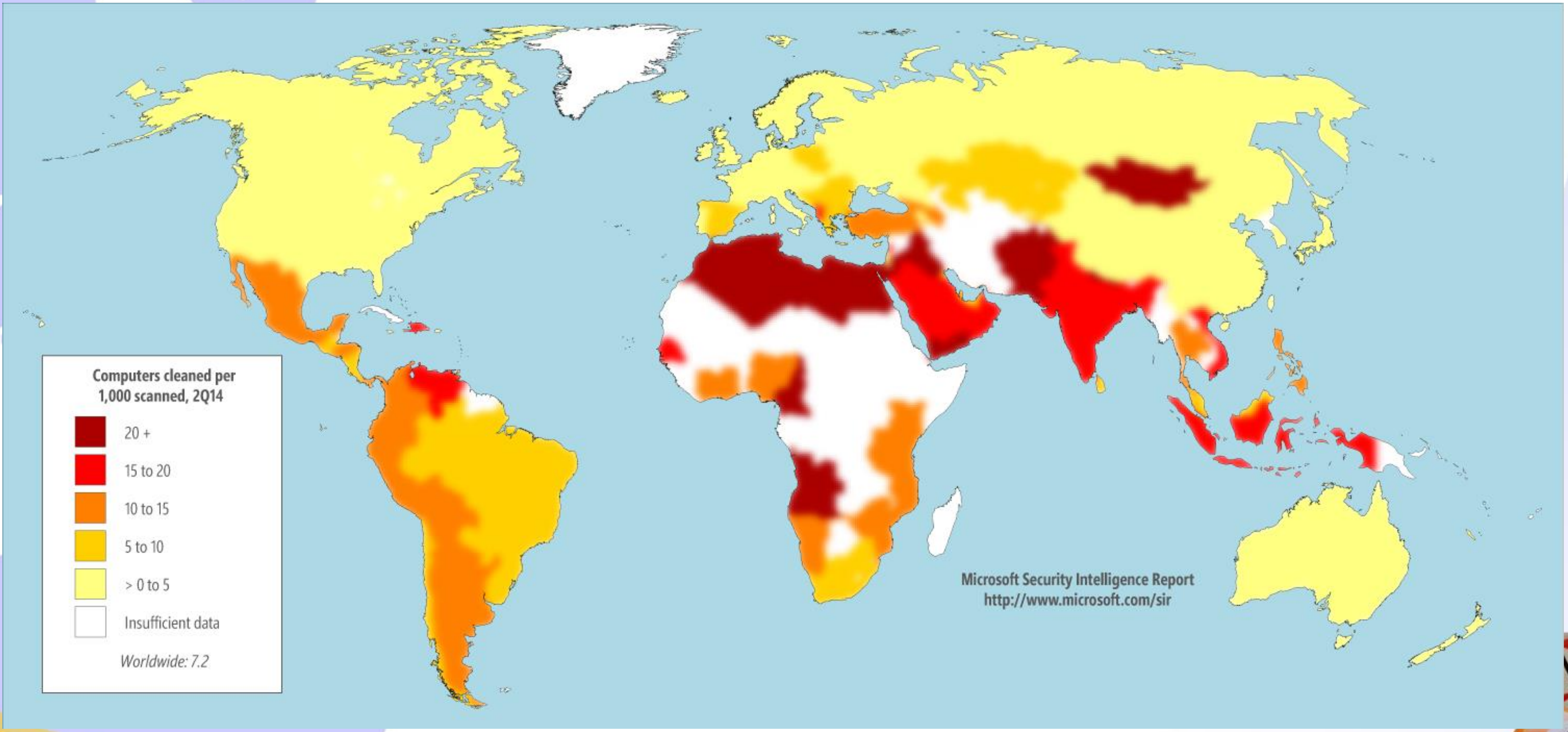
2Q14



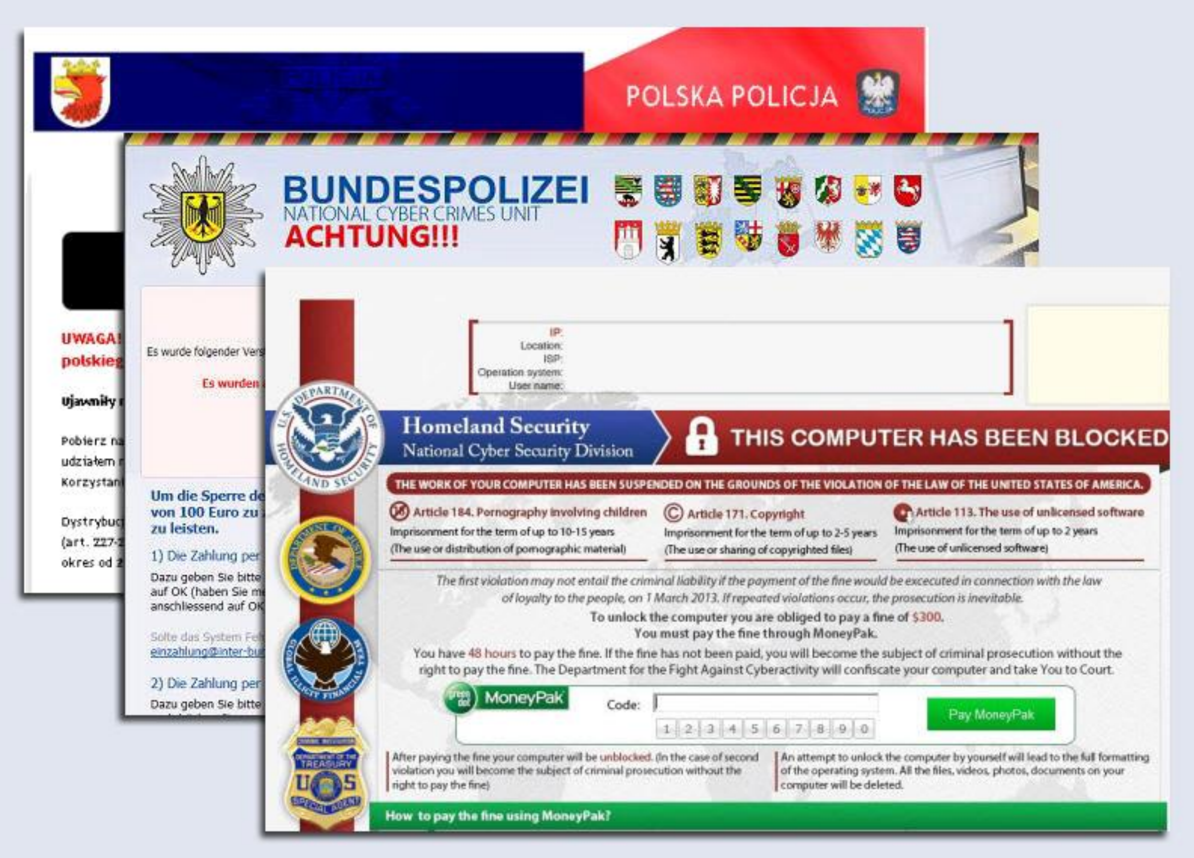
Microsoft Security Intelligence Report
http://www.microsoft.com/sir

CCM by country or region

2Q14


Computers cleaned per 1,000 scanned, 2Q14
20 +
15 to 20
10 to 15
5 to 10
> 0 to 5
Insufficient data
Worldwide: 7.2
Microsoft Security Intelligence Report
http://www.microsoft.com/sir

Ransomware



POLSKA POLICJA

UWAGA!
polskieg

Ujawniły r

Pobierz na
udziałem r
Korzystan

Dystrybuc
(art. 227-2
okres od 2

BUNDESPOLIZEI
NATIONAL CYBER CRIMES UNIT
ACHTUNG!!!

Es wurde folgender Vers

Es wurden

Um die Sperre de
von 100 Euro zu
zu leisten.

1) Die Zahlung per

Dazu geben Sie bitte
auf OK (haben Sie m
anschliessend auf OK

Solte das System Fe
einzahlung@inter-bu

2) Die Zahlung per

Dazu geben Sie bitte

IP:
Location:
ISP:
Operation system:
User name:

Homeland Security
National Cyber Security Division

THIS COMPUTER HAS BEEN BLOCKED

THE WORK OF YOUR COMPUTER HAS BEEN SUSPENDED ON THE GROUNDS OF THE VIOLATION OF THE LAW OF THE UNITED STATES OF AMERICA.

Article 184. Pornography involving children
Imprisonment for the term of up to 10-15 years
(The use or distribution of pornographic material)

Article 171. Copyright
Imprisonment for the term of up to 2-5 years
(The use or sharing of copyrighted files)

Article 113. The use of unlicensed software
Imprisonment for the term of up to 2 years
(The use of unlicensed software)

The first violation may not entail the criminal liability if the payment of the fine would be excecuted in connection with the law of loyalty to the people, on 1 March 2013. If repeated violations occur, the prosecution is inevitable.

To unlock the computer you are obliged to pay a fine of $300.
You must pay the fine through MoneyPak.

You have 48 hours to pay the fine. If the fine has not been paid, you will become the subject of criminal prosecution without the right to pay the fine. The Department for the Fight Against Cyberactivity will confiscate your computer and take You to Court.

MoneyPak Code:

1 2 3 4 5 6 7 8 9 0

Pay MoneyPak

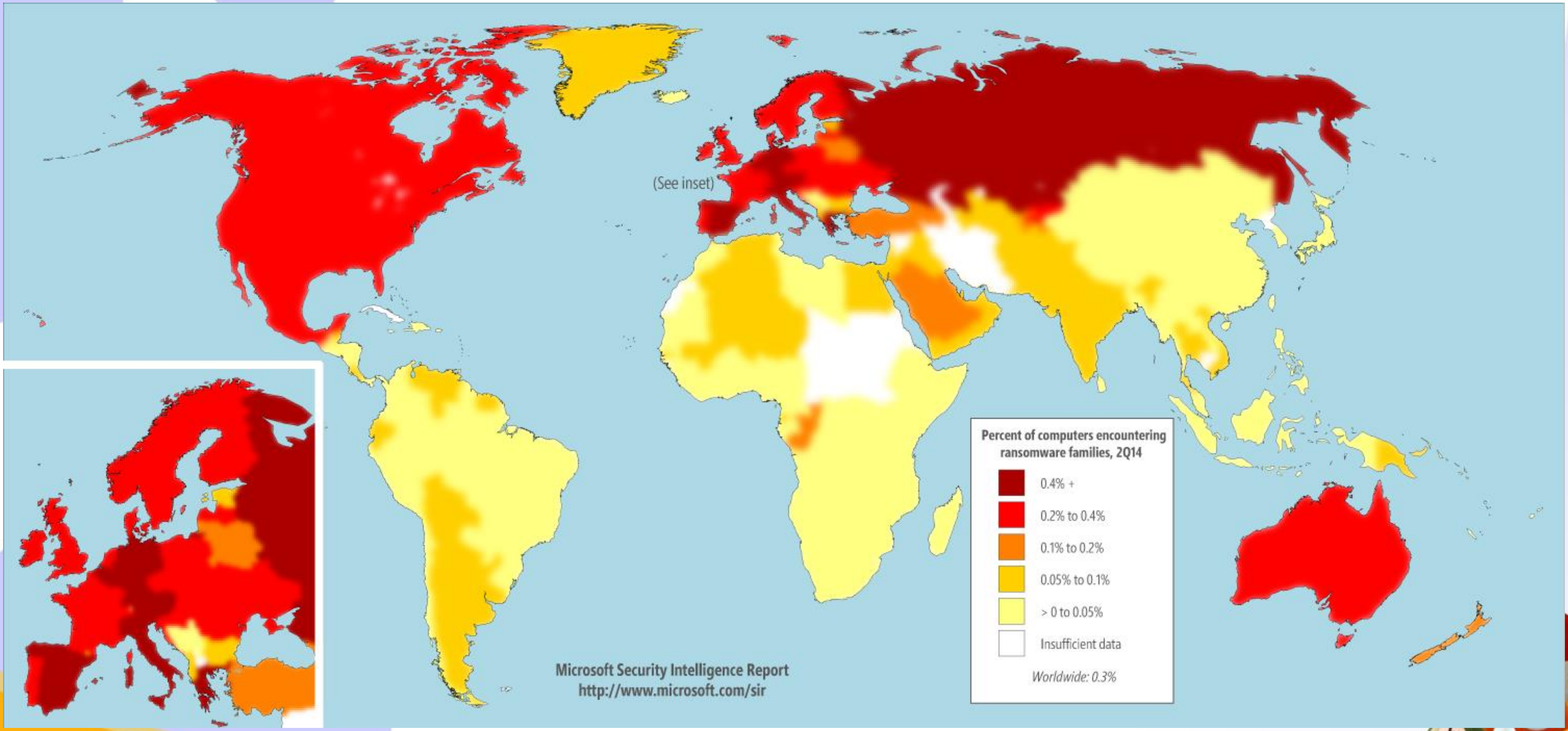
After paying the fine your computer will be unblocked. (In the case of second violation you will become the subject of criminal prosecution without the right to pay the fine)

An attempt to unlock the computer by yourself will lead to the full formatting of the operating system. All the files, videos, photos, documents on your computer will be deleted.

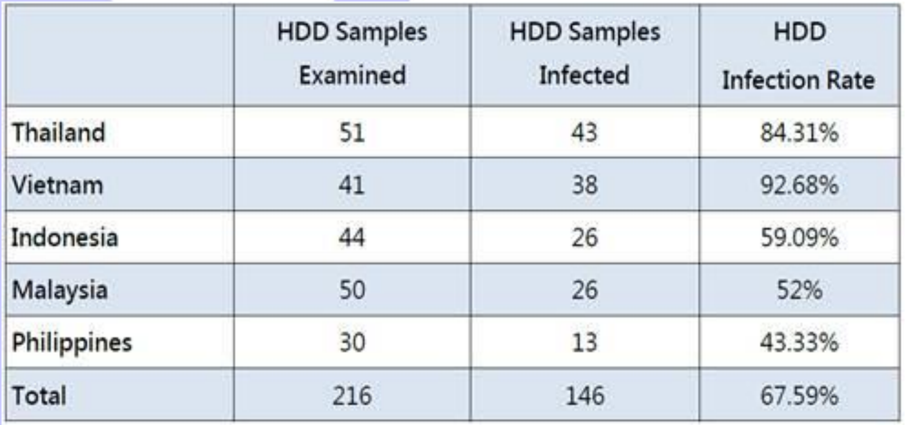
How to pay the fine using MoneyPak?

Ransomware by country or region

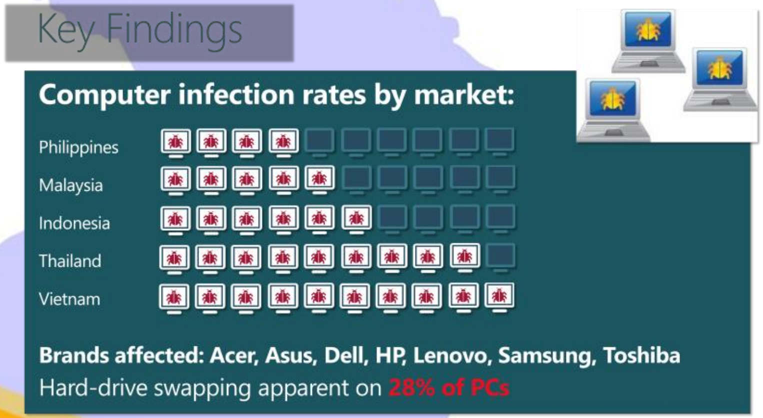
2Q14


(See inset)
Percent of computers encountering ransomware families, 2Q14
0.4% +
0.2% to 0.4%
0.1% to 0.2%
0.05% to 0.1%
> 0 to 0.05%
Insufficient data
Worldwide: 0.3%
Microsoft Security Intelligence Report
http://www.microsoft.com/sir

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%

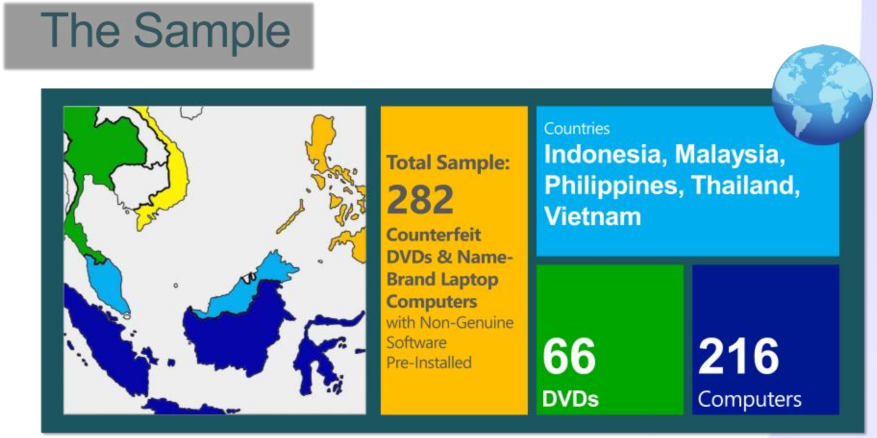


Key Findings

Computer infection rates by market:

Brands affected: Acer, Asus, Dell, HP, Lenovo, Samsung, Toshiba

Hard-drive swapping apparent on 28% of PCs



The Sample

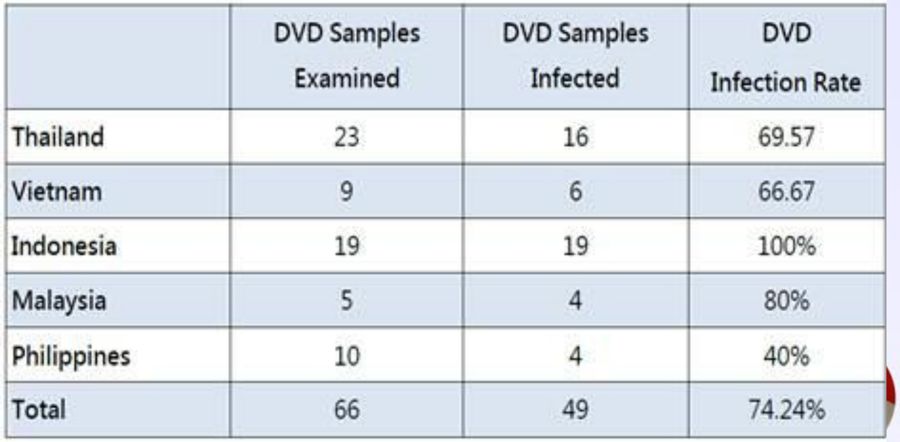
Total Sample: 282 **Counterfeit DVDs & Name-Brand Laptop Computers** with Non-Genuine Software Pre-Installed

Countries

Indonesia, Malaysia, Philippines, Thailand, Vietnam

66 DVDs

216 Computers



	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%

Advanced Persistent Threat (APT)

August 2012
Saudi Aramco

30,000 computers down for two weeks

"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)

It all starts with *Data Classification*

KNOW WHAT YOU ARE DEALING WITH

↑HBI HIGH Business Impact

- HBI information is usually labeled Confidential or HBI.
- Unauthorized disclosure of HBI would cause severe or catastrophic material loss.
- Examples of common forms of sensitive information include (without limitation)
  - social security numbers,
  - credit card numbers,
  - username and password combinations.
- In many cases this data is encrypted.

↑MBI MODERATE Business Impact

- MBI information is usually labeled Confidential or MBI.
- Only specific groups of employees, or approved non-employees with a legitimate corporate business need, have access to MBI content.
- Unauthorized disclosure may cause
  - serious material loss due to identity or brand damage,
  - operational disruption,
  - damage to corporations reputation,
  - legal or regulatory liability.

↓LBI LOW Business Impact

- LBI information carries no or little risk of impact to the corporation if lost or stolen.
- Released financials, Public Relations campaigns and released product information are examples of LBI.

Bring Your Own Device (BYOD)

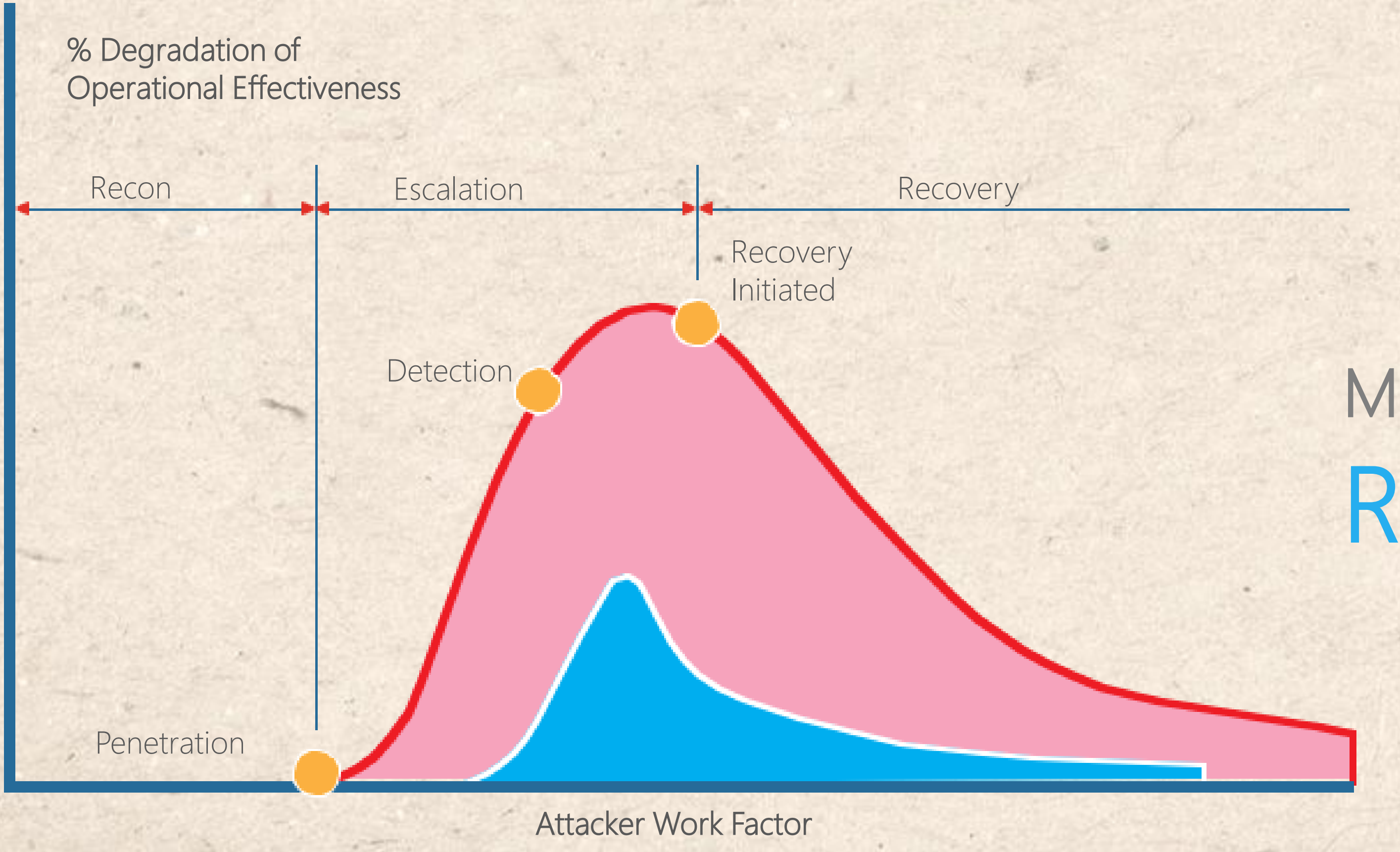
Resilience

"The bamboo that bends is **stronger** than the oak that resists."

~ Japanese proverb

Microsoft

Defining **Resilience** | Profiling a Resilient Information System

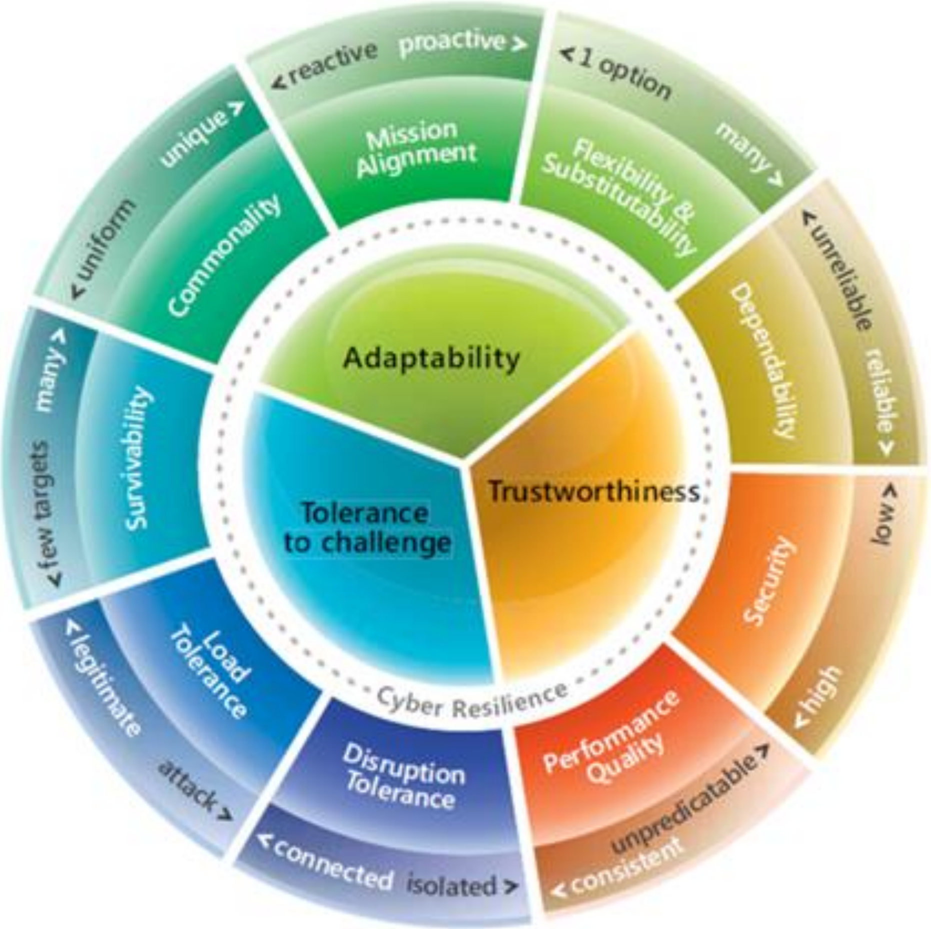


Making it

Resilient

Microsoft

Evaluating Resilience



Microsoft

The Impact of Security Standards

JAB
FedRAMP
Provisional ATO

AICPA Service Organization Control Reports
AICPA
SERVICE ORGANIZATIONS
SOC
aicpa.org/soc
Formerly SAS 70 Reports

CSA cloud security alliance℠

pci DSS COMPLIANT

SYSTEM CERTIFICATION
ISO/IEC 27001 SGS

HIPAA

G-Cloud Accredited
IL2

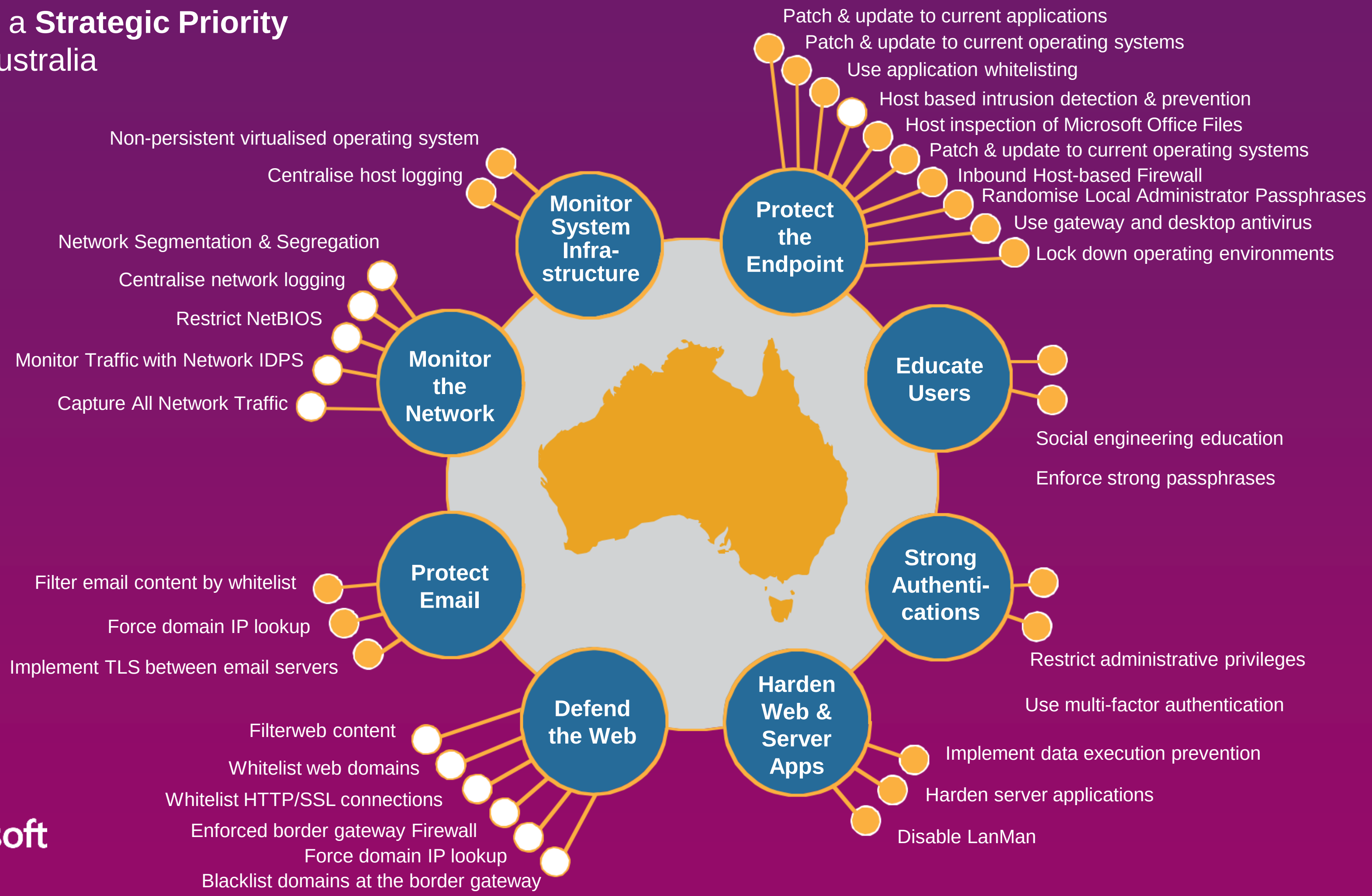
Case Study:

Australia

Collaboration between Microsoft and the Australian government resulted in a series of implementations across local government agencies to provide better resilience to cyber incidents.

Microsoft

Resilience as a **Strategic Priority**
Microsoft + Australia



Monitor System Infra-structure

Non-persistent virtualised operating system

Centralise host logging

Protect the Endpoint

Patch & update to current applications

Patch & update to current operating systems

Use application whitelisting

Host based intrusion detection & prevention

Host inspection of Microsoft Office Files

Patch & update to current operating systems

Inbound Host-based Firewall

Randomise Local Administrator Passphrases

Use gateway and desktop antivirus

Lock down operating environments

Monitor the Network

Network Segmentation & Segregation

Centralise network logging

Restrict NetBIOS

Monitor Traffic with Network IDPS

Capture All Network Traffic

Educate Users

Social engineering education

Enforce strong passphrases

Protect Email

Filter email content by whitelist

Force domain IP lookup

Implement TLS between email servers

Strong Authenti-cations

Restrict administrative privileges

Use multi-factor authentication

Defend the Web

Filterweb content

Whitelist web domains

Whitelist HTTP/SSL connections

Enforced border gateway Firewall

Force domain IP lookup

Blacklist domains at the border gateway

Harden Web & Server Apps

Implement data execution prevention

Harden server applications

Disable LanMan

Microsoft

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

Cybercrime and Security
State of the Nation

Pierre Noel

Asia Chief Security Officer

Microsoft