Career Talk
SCM and MSIM
Hang Seng Management College

Information/Cyber Risk Management

Micky Lo
Managing Director
AP Chief Information Risk Officer
BNY Mellon

Data Is Everywhere

Source: Alexa internet. http://www.alexa.com/topsites. Accessed May 9, 2014.

Data Is the Currency of Financial Services

The Digital Age

The Internet has brought new concerns about data protection for Financial Service companies.

WHAT HAS HAPPENED ?

System Outages

Source Code Theft

DDOS attacks have become "business as usual," but suspects there may be more to them than meets the eye.

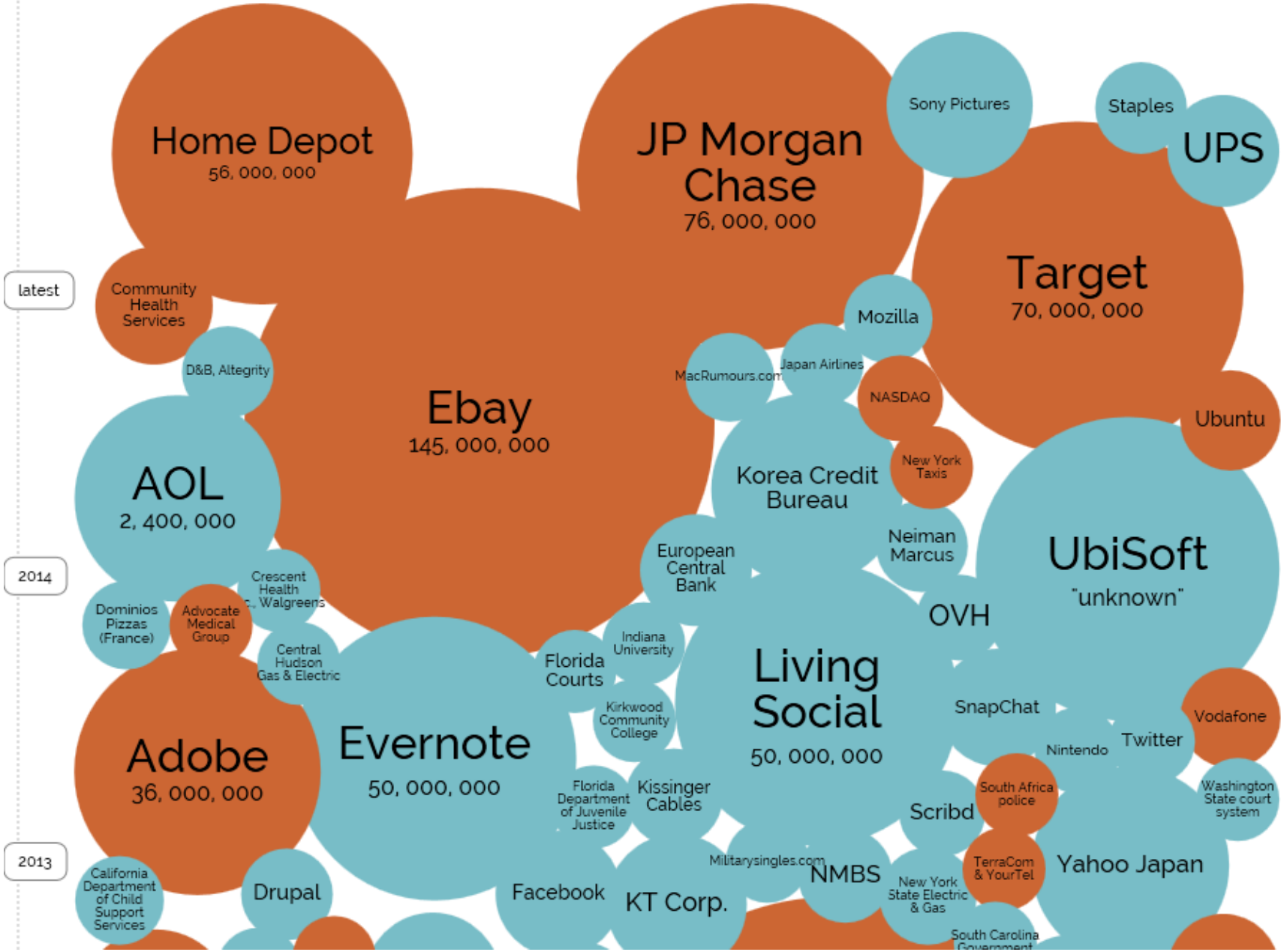
In terms of its potential impact, possibly the worst vulnerability found since commercial traffic began to flow on the Internet.

Cyberattacks Seem Meant to Destroy, Not Just Disrupt

Excessive Access Privileges

Target reported a 46 percent drop in net profit in the crucial holiday quarter and reported $61 million in costs related to the breach

Security companies recorded millions of attacks and probes related to the bug in the days following the disclosure.


latest
2014
2013
Home Depot
56, 000, 000
JP Morgan Chase
76, 000, 000
Sony Pictures
Staples
UPS
Target
70, 000, 000
Community Health Services
D&B, Altegrity
Ebay
145, 000, 000
Mozilla
MacRumours.com
Japan Airlines
NASDAQ
Ubuntu
New York Taxis
AOL
2, 400, 000
Korea Credit Bureau
Neiman Marcus
European Central Bank
UbiSoft
"unknown"
OVH
Crescent Health
Walgreens
Dominios Pizzas (France)
Advocate Medical Group
Central Hudson Gas & Electric
Florida Courts
Indiana University
Kirkwood Community College
Living Social
50, 000, 000
SnapChat
Vodafone
Twitter
Nintendo
Adobe
36, 000, 000
Evernote
50, 000, 000
Florida Department of Juvenile Justice
Kissinger Cables
South Africa police
Washington State court system
Scribd
Militarysingles.com
NMBS
TerraCom & YourTel
Yahoo Japan
California Department of Child Support Services
Drupal
Facebook
KT Corp.
New York State Electric & Gas
South Carolina

Challenging and Changing environment

In addition to a challenging environment …

- EU peripheral sovereign debt crisis

- Uncertain global economic recovery

- Dynamics in emerging markets

- Social unrest and political weaknesses

- Ecological disasters (Fukushima)

… banks face further sector specific challenges

Regulation

"The emergence of the regulator as a real force."

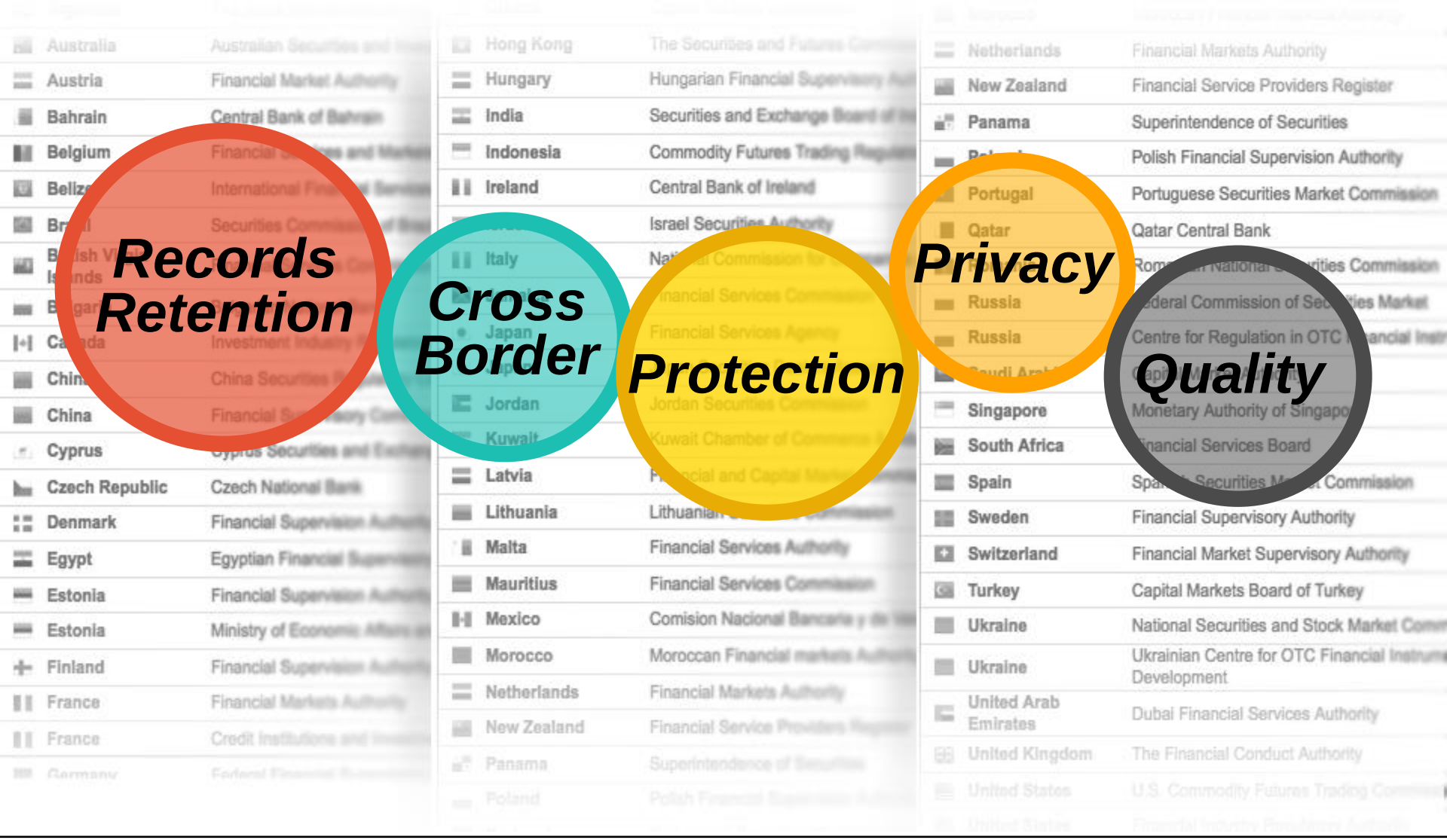
- Access Governance
- Vendor Governance
- Risk Reporting
- Living Wills

Competitive dynamics

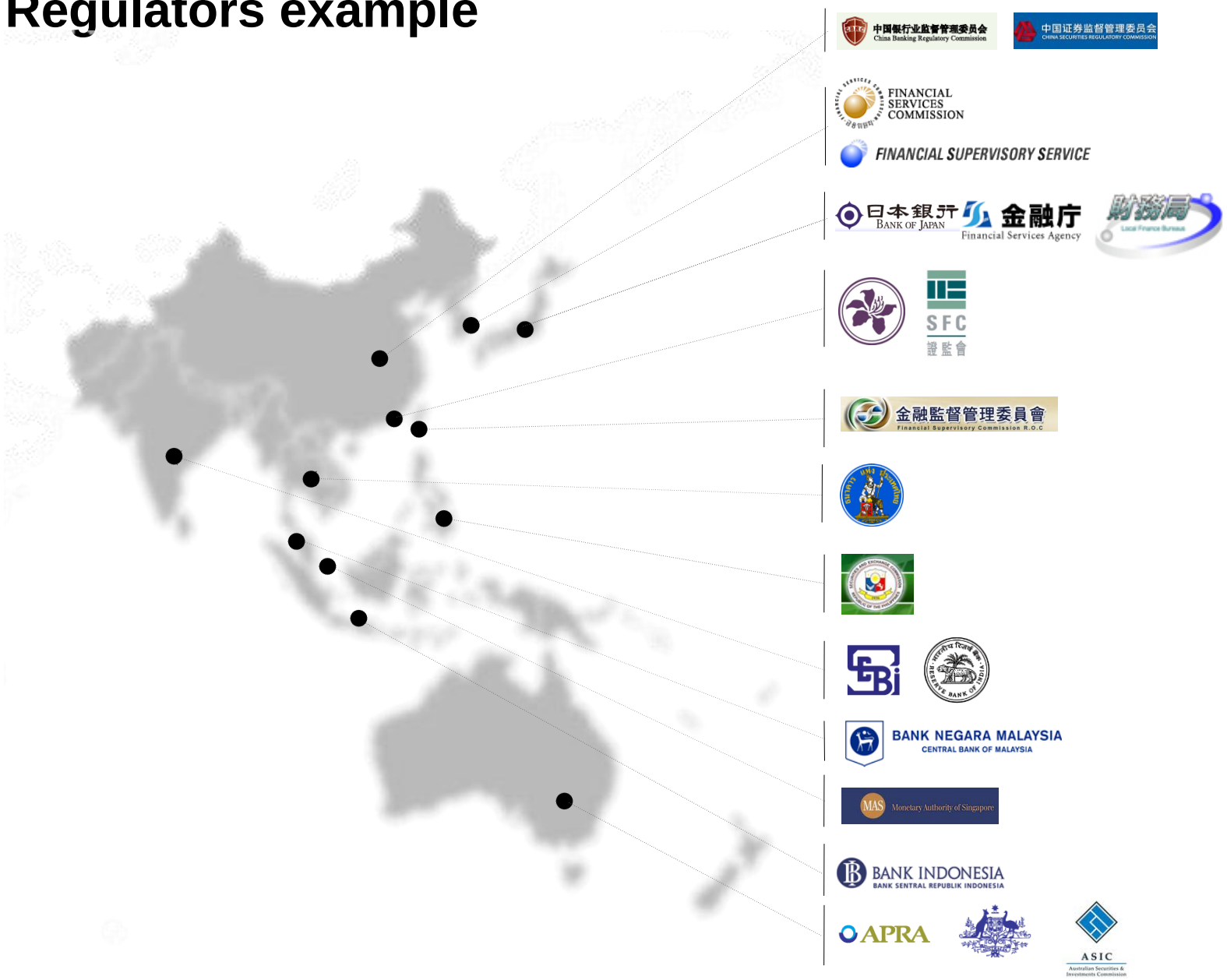
"Regulatory compliance will turn into competitive advantage."

Technical Scalability & Disaster Recovery more important than ever.

Regulation Increases Data Management Challenges



APAC Regulators example



What is Cyber Attack ?

Cyber attacks target computer information systems, computer networks and/or personal computer devices.

An anonymous source steals, alters or destroys a target by hacking into a system. Cyber attacks can be as harmless as installing spyware on a PC or as grand as affecting the infrastructure of entire corporations.

As the modern world becomes more reliant on computer systems, cyber attacks have become more sophisticated and dangerous.

Threat Landscape

Nation States

- Early understanding of strategic direction
- Intellectual property
- Cripple/disrupt services

Hacktivists

- Cripple/disrupt services; protest their cause and cause
- Humiliation and reputational damage

How They Do It:

Disruptive (D) DoS attacks

Insider-coordinated breach

Web facing application vulnerabilities compromised

Exploit internal and third party provider vulnerabilities

What They Get:

1. **Customer account information and credentials**
2. **Potentially sensitive information such as investment strategies and other confidential correspondence**
3. **Loss of confidence in financial institution**
4. **Disruption of services**
5. **Destruction of data and IT assets**

Introduction of destructive malware through phishing

Anonymous whistleblower, e.g., Wikileaks

Virus infection through email

Social engineering

Criminal Enterprises

- Financial

Insiders

- Financial
- Cripple/disrupt services

What is Risk

Risk is the possibility that an event will occur and adversely affect the achievement of objectives

Characteristics:

- Present due to uncertainties
- All entities face risks
- Some risks can be opportunities
- Risks can erode or enhance value
- Risks arise from “internal” and “external” environment
- Risks evolve

Mark Beasley, North Carolina State University

Information/Cyber Risk Management

Risk Assessment

- What are the risks in the business?
- What is the potential level of exposure?

Business Description

- What is the scope of the organization that is being evaluated?
- What are the operational processes?

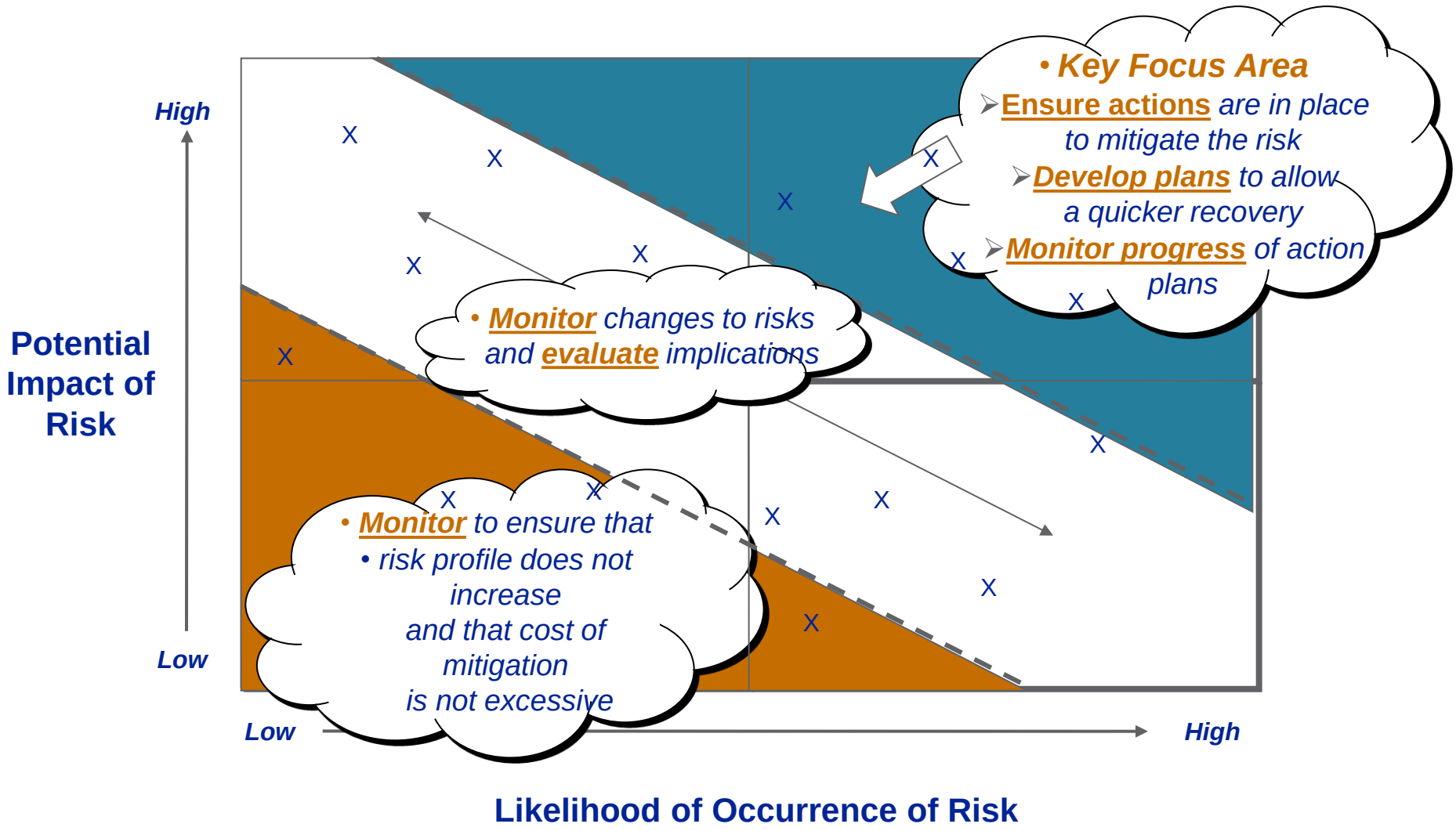
Control Activities

- What controls are there to mitigate these risks?
- How effective are the current controls?
- Are there any gaps?

Monitor Information & Communication

- What management mechanisms are in place to receive timely information about the quality of current controls?
- How are potential control breakdowns escalated?

Risk Profile Matrix



Types of Risk

Information Risk – 3 pillars

Confidentiality is the property of information being secret or private within a predetermined group

Integrity is the property of information being a correct and representation if an authorized business process. Integrity has 3 aspects :

- Completeness
- Accuracy
- Validity

Availability is the property of information being accessible and useable by the business. It has 2 aspects :

- Response time
- Up time

What to do in such a complex environment?

People

Awareness
Skills

Process

Policies &
Standards
Governance

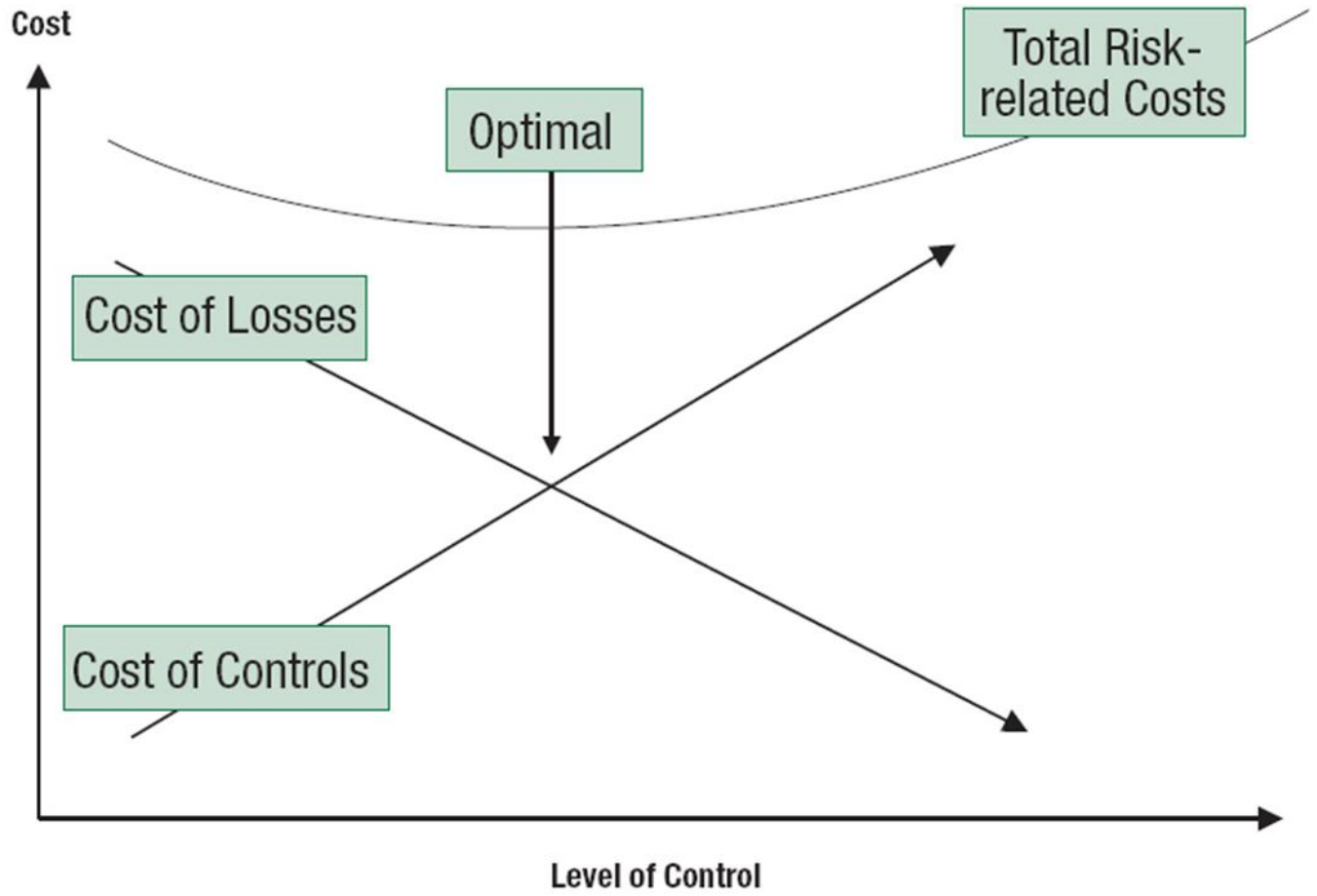
Technology

Automation
Innovation

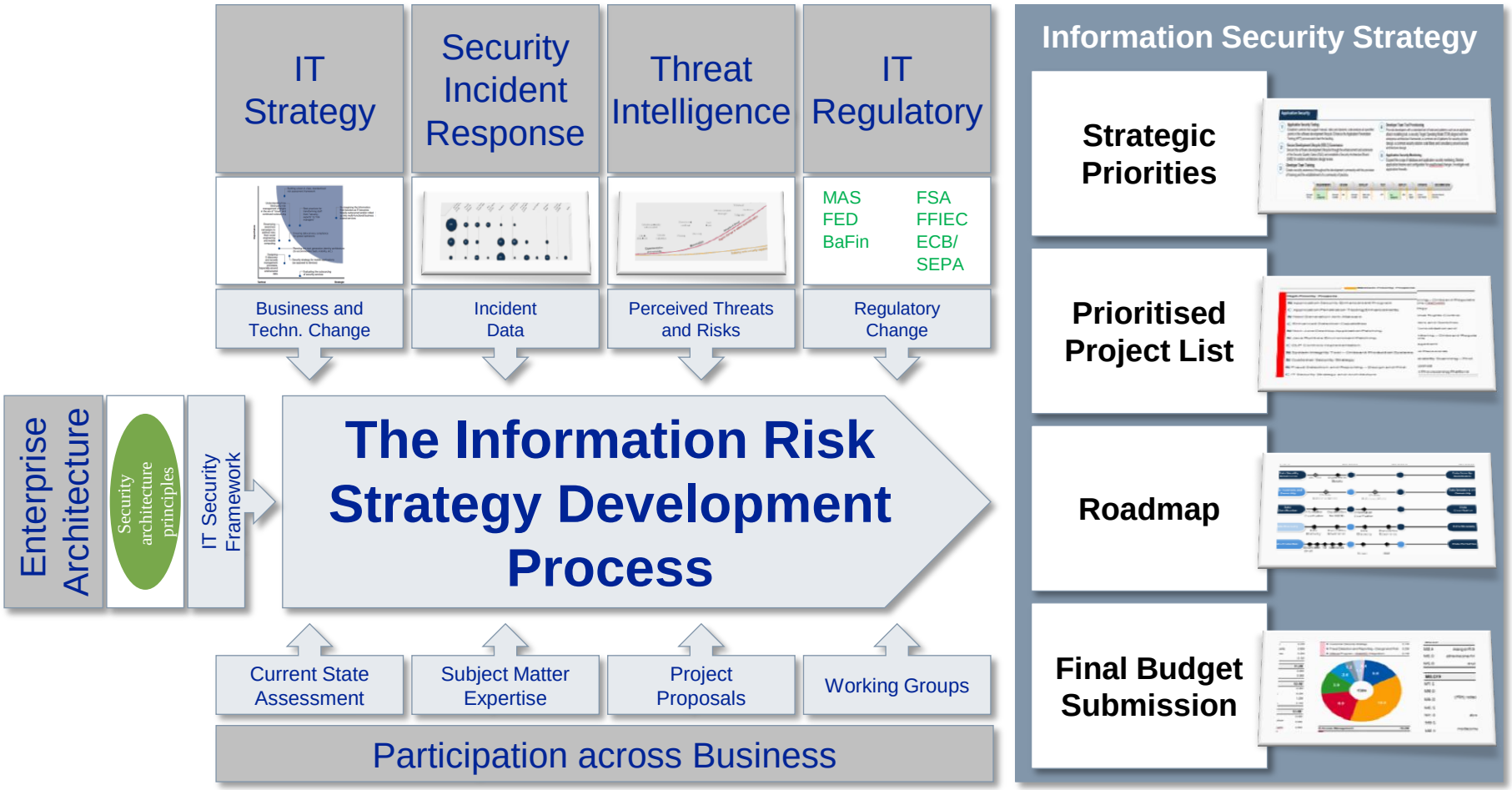
Synthesize and analyze multiple data streams.

Push enterprise connectivity to new levels.

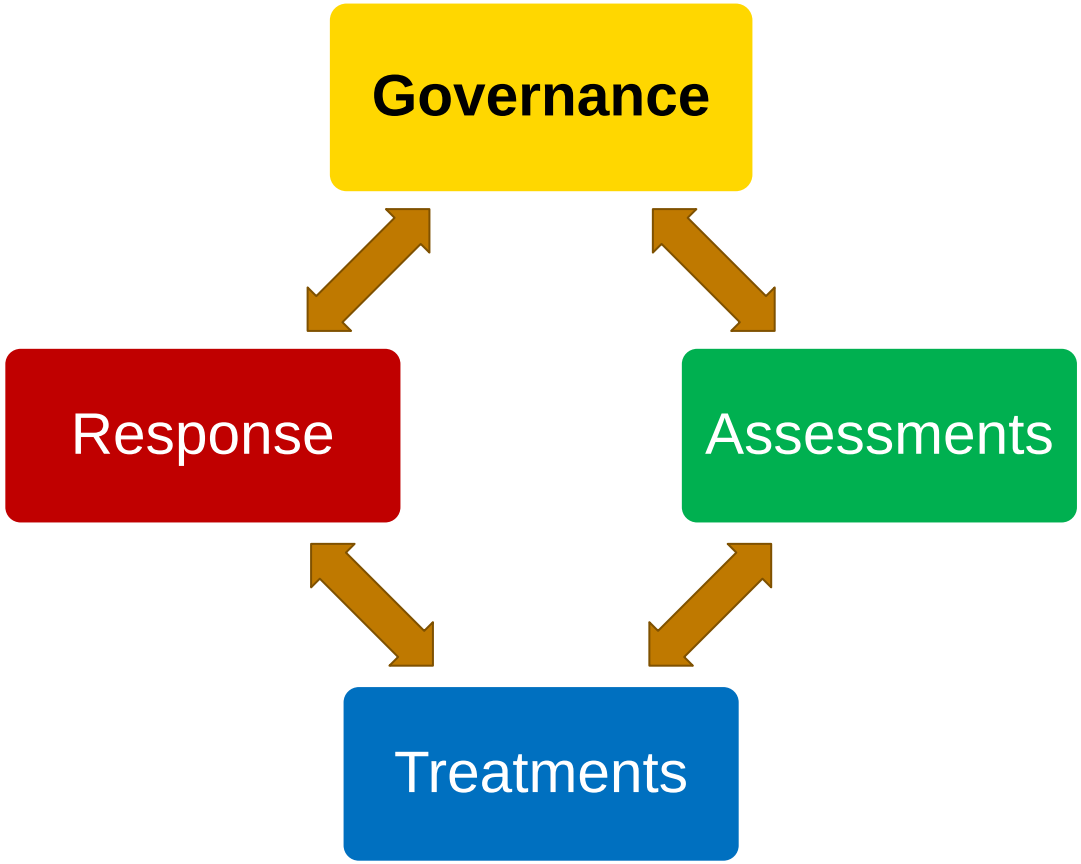
Optimizing Risk Costs



Risk Strategy Development Model



Information Risk Management Services



Three Lines of Defense

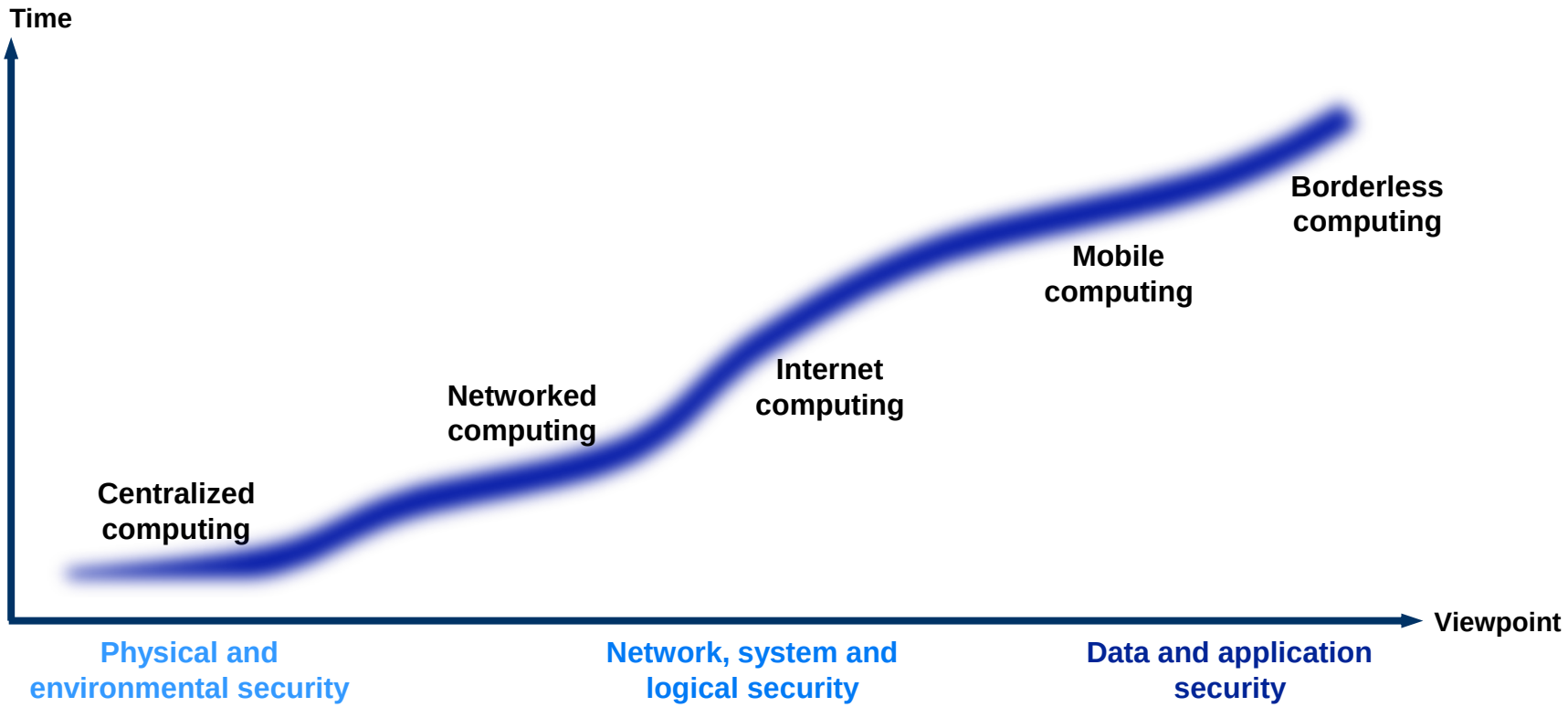
Enterprise Risk

The **First Line of Defence** is managers and employees at the business or, in some cases, business partner level. They own the risks associated with their business activities, and they manage the risks and the related control processes and procedures on a day-to-day basis.

The **Risk Management and Compliance** functions are the **Second Line of Defence**. They own the enterprise-wide risk management framework and provide independent oversight of the First Line of Defence. This also includes Corporate Security, Business Continuity, Financial Management and Analysis within Finance, Human Resources and Legal.

The **Third Line of Defence** is **Internal Audit**, which maintains independence from the first two and provides our Board of Directors and senior management with the assurance that our governance structures, risk management and internal controls are effective.

Summary



As the threat landscape is rapidly changing, so too must the capability and maturity of Information Risk/Security

The notion that any organization can be 100% secure is unrealistic in today's borderless environment.

The question is not are we secure, but is the data that matters most secure enough?

The goal is to…

Make data available.

Ensure its integrity.

Protect its confidentiality.


MERCI!
どうもありた
Todah!
多謝
Thank You!
Dank Je Wel!
Merci!
GRACIAS!
Thank you!
Gracias!
感謝
ありがとうございました
Danke!
Todah!
Dank Je Wel!
謝謝
ThAnK YoU!
Merci!
どうもありがとうございました
Todah!
MERCI!
DANKE!
GRACIAS!
Thank you!