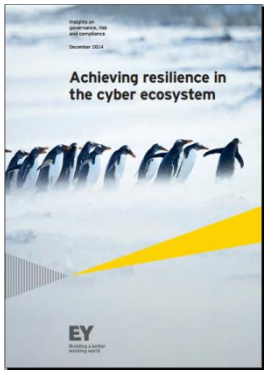
Mitigating Risk: Cyber Resilience

Heritage of culture: profession that brings value

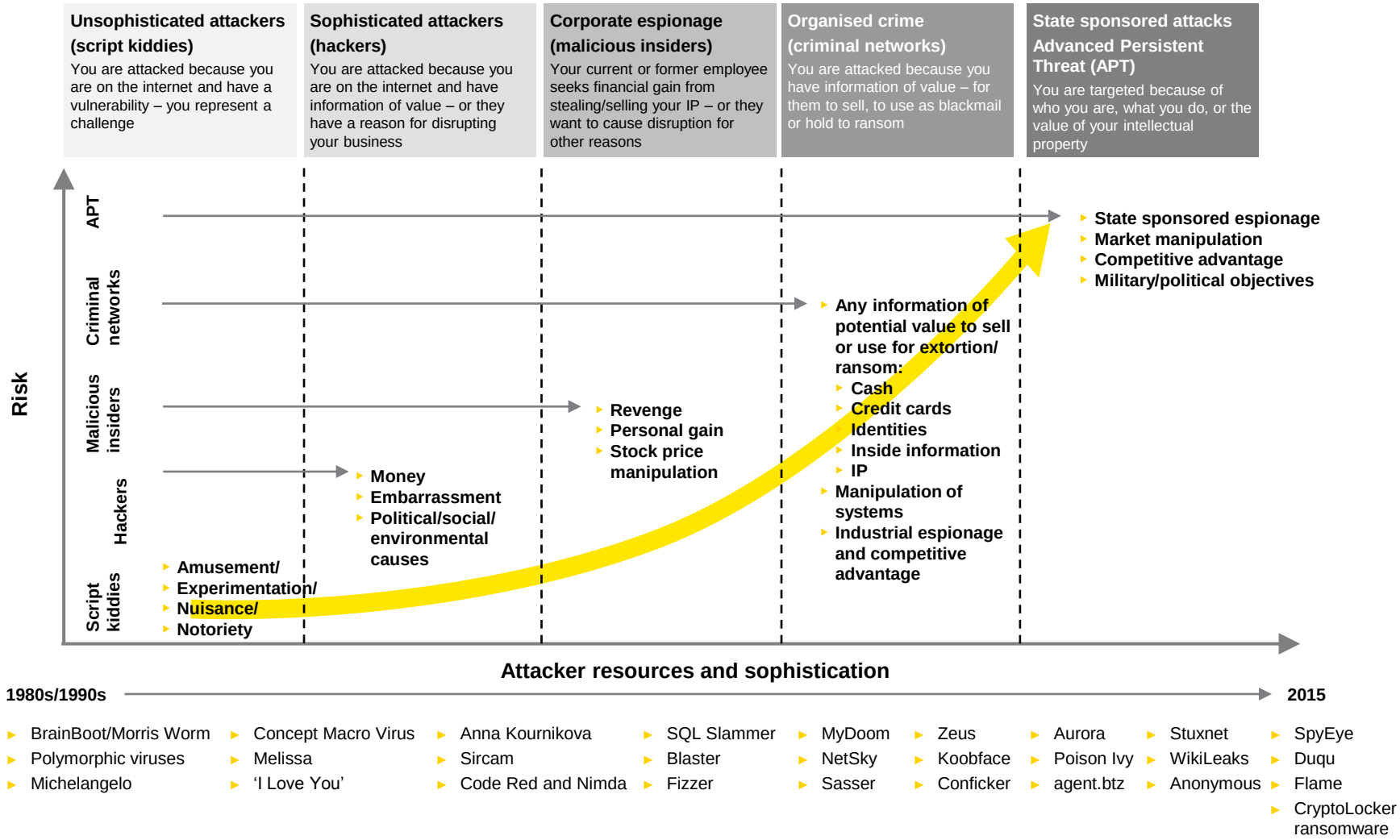
Isnaeni Achdiat
CISA, CISM, CGEIT, CIA
Partner of EY Indonesia
President ISACA Indonesia Chapter

EY
Building a better working world

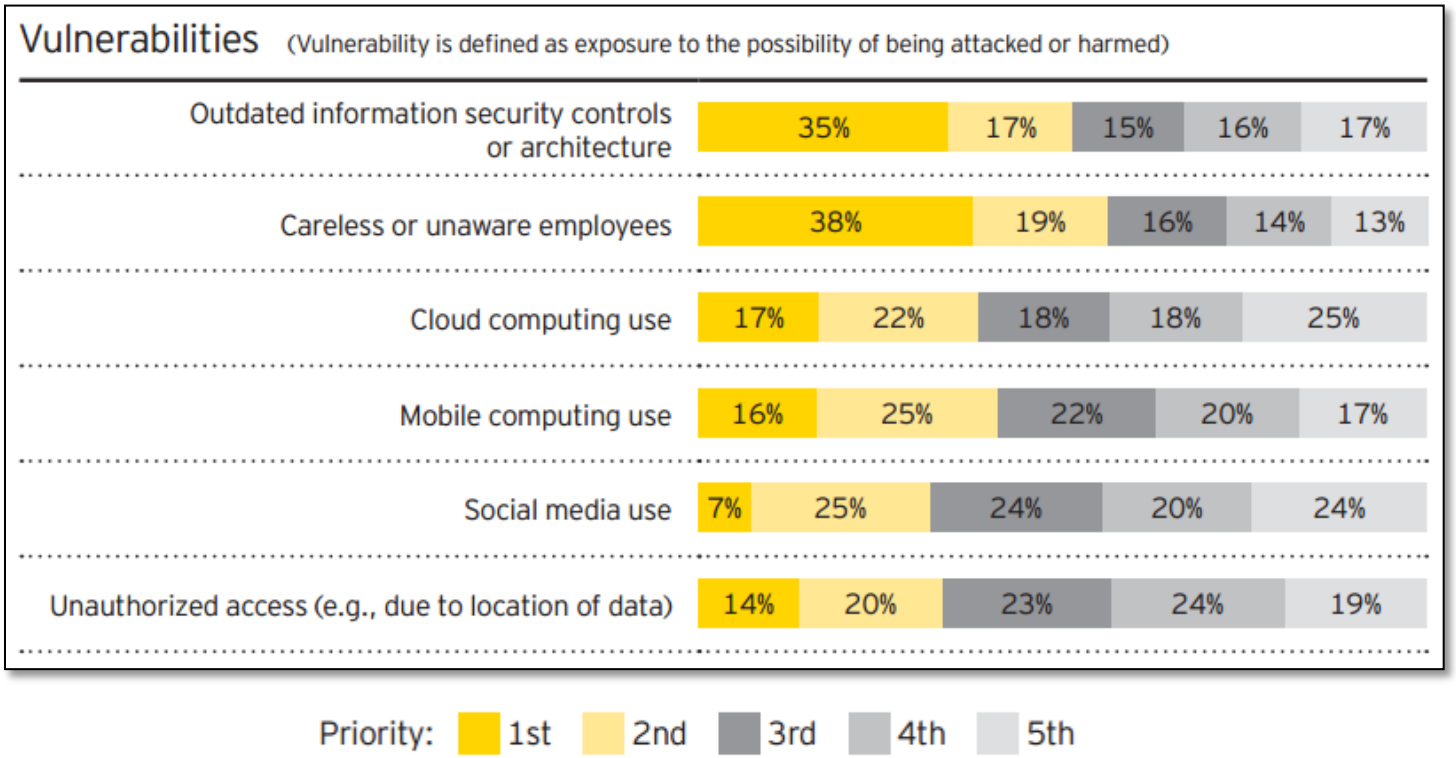
Contents



Cyber-threat growing as attacks become better funded and more sophisticated every year



Vulnerabilities have most increased risk exposure over the last 12 months



Threats have most increased risk exposure over the last 12 months

Threats (Threat is defined as the potential for a hostile action from actors in the external environment)

	1st	2nd	3rd	4th	5th
Cyber attacks to disrupt or deface the organization	25%	20%	21%	16%	18%
Cyber attacks to steal financial information (credit card numbers, bank information, etc.)	28%	23%	18%	19%	12%
Cyber attacks to steal intellectual property or data	20%	24%	22%	17%	17%
Espionage (e.g., by competitors)	16%	24%	20%	18%	22%
Fraud	19%	23%	22%	21%	15%
Internal attacks (e.g., by disgruntled employees)	11%	20%	23%	18%	28%
Malware (e.g., viruses, worms and Trojan horses)	15%	19%	24%	25%	17%
Natural disasters (storms, flooding, etc.)	15%	14%	16%	21%	34%
Phishing	17%	22%	21%	22%	18%
Spam	13%	18%	19%	20%	30%
Zero-day attacks	16%	20%	19%	20%	25%

Priority: 1st 2nd 3rd 4th 5th

Losses regularly encompassing all data assets and forms of value loss

Direct financial loss

- Direct financial loss: money (e.g. CEO false money transfer).
- Higher capital requirement to cover operating risk due to large scale cyber attack or smaller repeated attacks
- Regulatory fines

Business continuity failures

- Customer service
- Denial of service
- Front and back office attacks impacting customer service (loss of data, flows…)

Owned and controlled data assets

Intellectual property

People information

Financial information

Business information

Impaired brand and trust

- Huge press coverage for a number of Cyber attack in 2014 capturing strong public interest
- Mistrust and potential loss of customers for firms operating in the financial services arena

Lost competitive advantage

- Loss of intellectual property, trade secrets, M&A information, technology
- Publication of sensitive information in public domain

Cybersecurity programs are not well positioned to deal with today's cyber risks

Fewer than 20% of organizations have real time insight on cyber risk readily available

Across almost every cybersecurity process **between 35% and 45%** correspondents rated themselves 'still a lot to improve"

56% of organizations say that it is unlikely or highly unlikely that their organization would be able to detect a sophisticated attack

Some top of mind questions for today's information security executives are:

- How does my information security program compare against those of my peers in the industry?
- Is my information security strategy aligned with business objectives?
- How well do we protect high-value information, especially given today's increasingly mobile workforce?
- Are we well prepared to monitor, detect, and respond to information security threats?
- Do we have the right people and skillsets?
- Are we spending on the right information security priorities?
- Am I or have I been the victim of an attack or a breach?

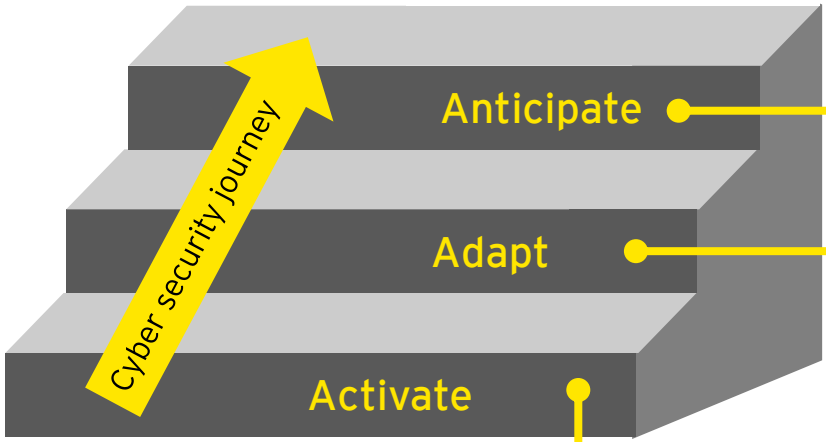
Source – Results from EY's Global Information Security Survey (GISS) 2014 captures the responses of 1,825 C-suite leaders and Information Security and IT executives/managers, representing most of the world's largest and most-recognized global companies.

Cybersecurity system building blocks

What it is	Cybersecurity system building blocks	Status
Anticipate is about looking into the unknown. Based on cyber threat intelligence, potential hacks are identified; measures are taken before any damage is done.	**Anticipate**	**Anticipate** is an emerging level. More and more organizations are using cyber threat intelligence to get ahead of cybercrime. It is an innovative addition to the below.
Adapt is about change. The cybersecurity system is changing when the environment is changing. It is focused on protecting the business of tomorrow.	**Adapt**	**Adapt** is not broadly implemented yet. It is not common practice to assess the cybersecurity implications every time an organization makes changes in the business.
Activate sets the stage. It is a complex set of cybersecurity measures focused on protecting the business as it is today.	**Activate**	**Activate** is part of the cybersecurity system of every organization. Not all necessary measures are taken yet; there is still a lot to do.

"We have found that organizations' responses to cybercrime fall into three distinct stages, and the aim should be to implement ever more advanced cybersecurity measures at each stage."

Activities during the journey



- Design and implement a cyber threat intelligence strategy
- Define and encompass the organization's extended
- Take a cyber economic approach
- Use forensics and analytics
- Ensure everyone understands what's happening

- Conduct security assessment and roadmap
- Get Board-level support for a security transformation
- Review and update security policies, procedures and supporting standards
- Establish a Security Operations Center (SOC)
- Design and implement cyber security controls
- Test business continuity plans and incident response procedures

- Design and implement a transformation program
- Decide what to keep in-house and what to outsource
- Define a RACI matrix for cybersecurity
- Define the organization's ecosystem
- Introduce cyber security awareness training for employees

Resilience cycle

How an organization responds to cybercrime (pre, during, and post disruption) **depends** on their stages (activate / adapt / anticipate).

Resilience is the **strategic** organizational capability to **resist** and **react** to disruptive and destructive threats, reshape environments, and **survive** both foreseen and unforeseen risks.

This requires them to learn and adapt through the key resilience phases:

- During ***pre-disruption***, through an ability to better sense and resist security threats, including advanced capabilities to scan internal and external environments, and eliminate vulnerabilities
- During ***disruption***, by reacting rapidly to sudden events that threaten the organization; leveraging non-routine leadership and mobilizing effective responses that minimize impacts
- During ***post-disruption***, by absorbing shocks while continuing to achieve strategic security goals and reshaping and reconstructing the operating environment in ways that eliminate future sources of disruption threat

Implementing cyber resilience

Understanding your cyber ecosystem

Mapping the relationships

The organization must understand its internal and external environments and determine its “crown jewels” of information, where they exist and how they flow across this system.

Determining the risk factors

Performing a risk assessment on the organization’s “cyber presence” in the ecosystem, by looking at information assets, interdependencies with other organizations, threats, vulnerabilities, cybersecurity controls, and security testing activities.

Establishing control in your cyber ecosystem

A detailed risk assessment will identify what risks exist across the cyber ecosystem and determine which security measures will provide with control. In order to both establish these security measures and to assess the change in the status of identified risks, the organization should consider to establish a Security Operations Center (SOC).

Taking a risk-based approach

With any risk-based approach that seeks to focus on tackling the “right risks” in the “right way,” organizations must make tough, evidence-based decisions. Organizations must seek to take into account the connections, transactions and relationships that exist between entities within their cyber ecosystem.

Developing resilience attributes

While certainly not easy to define or track as directly as investments in the latest security-related hardware, **organizations should nevertheless aim to track and assess resilience attributes**. These attributes provide a key element of the flexibility with which organizations that demonstrate the ability to "anticipate" security threats.

Key resilience attributes

Resilient leadership

- The visionary, executive-led commitment to establishing resilient organizations.
- Non-routine management styles are consultative but enable rapid, decisive and compassionate decision making during disruptive circumstances.

Resilient culture

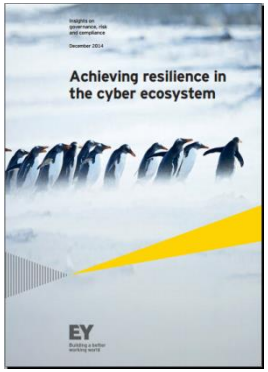
- Supports a "one-in, all-in" approach embraced across an organization and encourages resilient behaviors of collaboration, vigilance, proactivity, and the preparedness to learn from failure and disruption.

Resilient networks

- Establishes and strengthens trust-based relationships with third parties (including business partners, customers and other stakeholders) to maximize the ability to withstand and recover rapidly from disruptive threats.

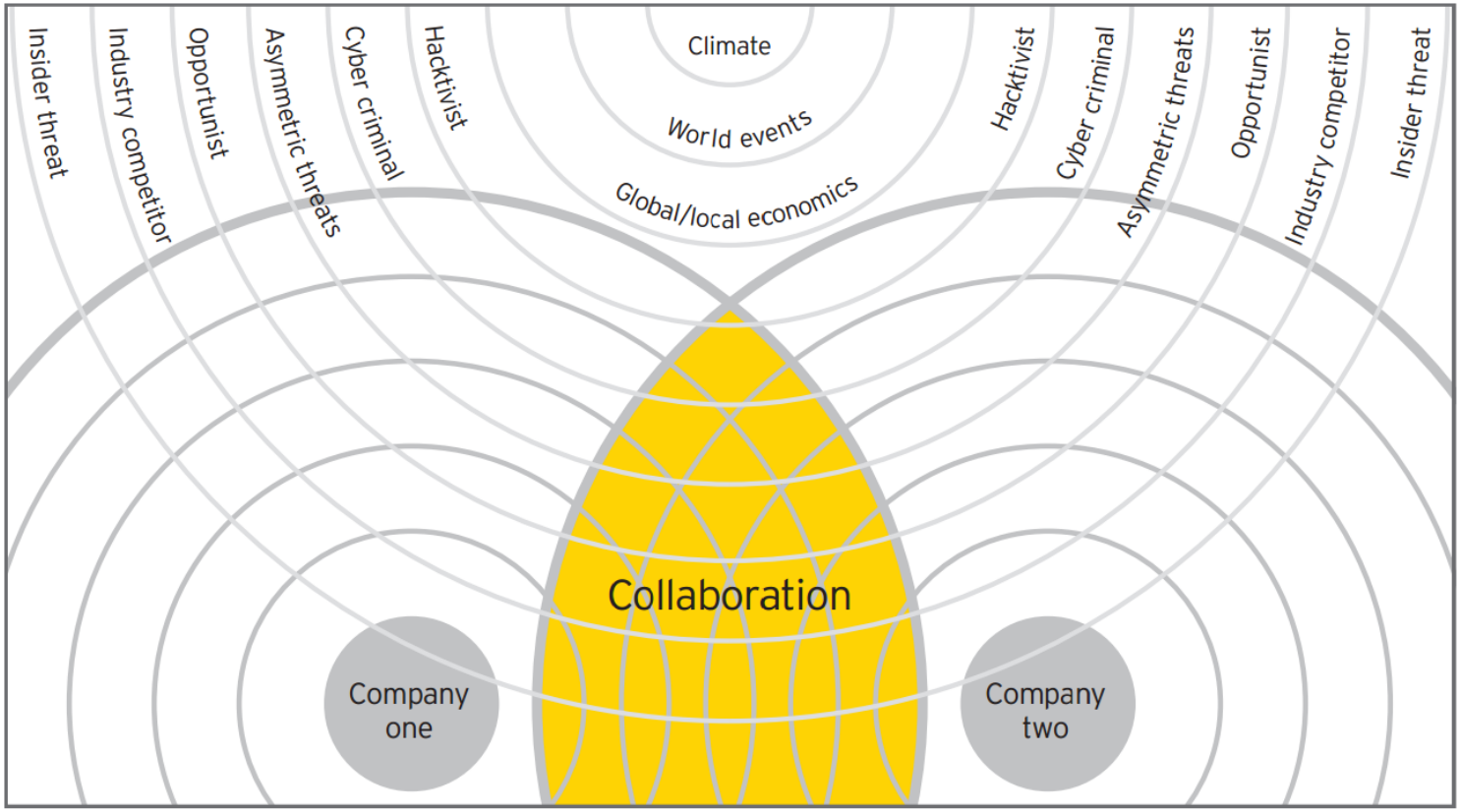
Resilient change-readiness

- The readiness of teams enabled with training, tools and techniques to rapidly detect, respond to and adapt security responses in an ever-changing security context.



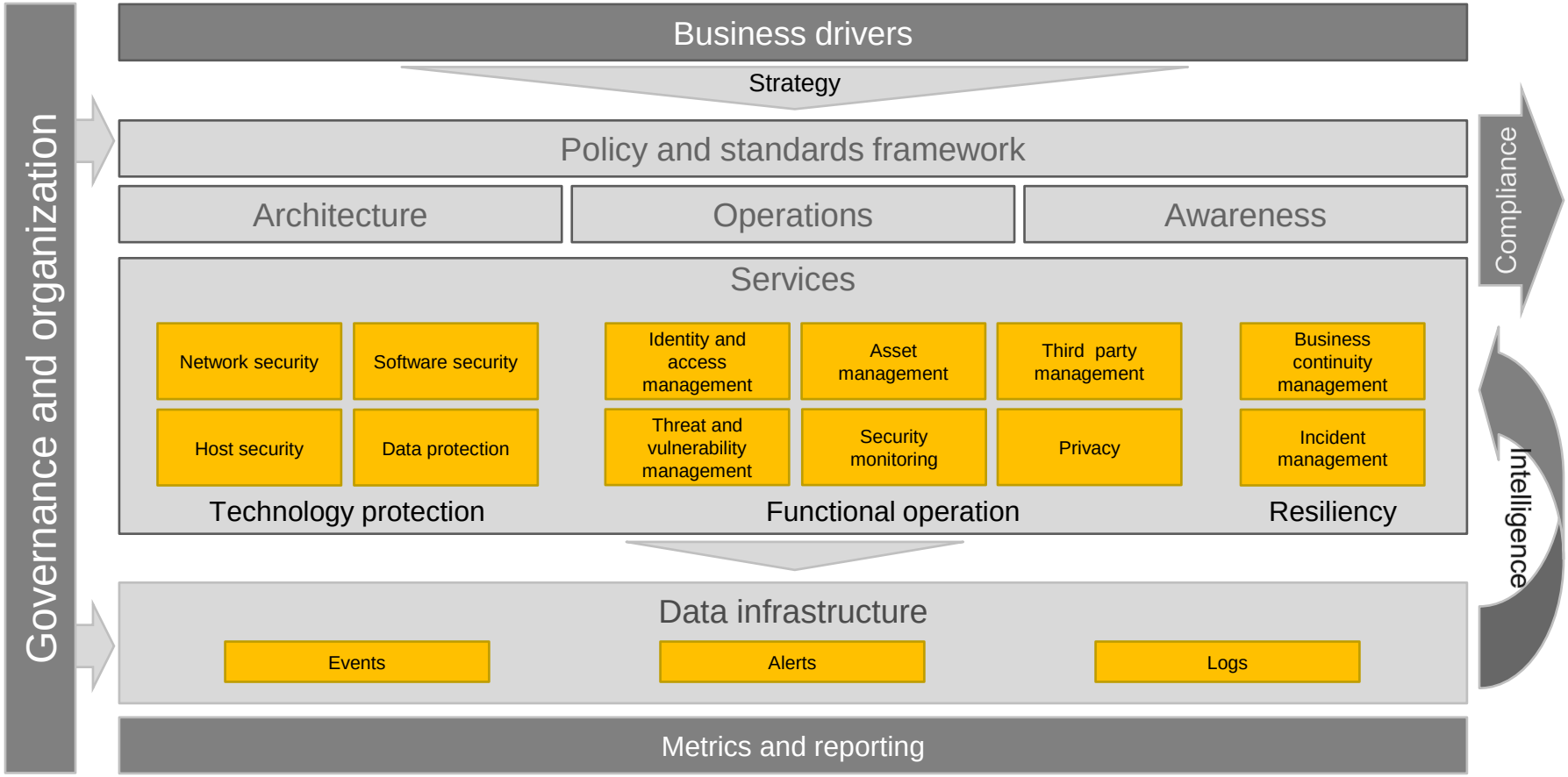
Potential collaboration within the ecosystem

The organization needs to **increase** the **level of collaboration** (rather than just monitoring) of their ecosystem, working more closely with others in the industry, competitors and governments to combat the threats that face them all as a team.



Cyber Program Management

Cyber Program Management (CPM) is a **holistic framework** for **identifying and addressing security risks** within the cyber ecosystem. CPM also aligns with industry standards and regulations, and will help us **assess** and **improve** the organization's **information security program**.



Key takeaways

- It is **no longer possible to prevent all attacks** or breaches. The focus needs to shift to prevention, detection, containment & response
- Cybersecurity is increasingly being recognized as a **key business risk**. This requires new skill sets to identify and manage the emerging risk. The issue is increasingly cyber risk, not cybersecurity
- You **cannot protect everything**. The sophistication and targeted nature of the cyber attacks makes it increasingly difficult to mitigate against the attacks. The key issue is to identify and protect the key information assets.
- Cybersecurity risk needs **to be mitigated**, **not eliminated**
- Alignment with the business. The role of the security function increasingly is to **assist the business** to achieve its objectives
- Cybersecurity requires shift in leadership mindset **from defense to detection**

EY GRC insights

Identity and access management: beyond compliance

www.ey.com/IAM

Cyber threat intelligence – how to get ahead of cybercrime

www.ey.com/CTI

Get ahead of cybercrime: EY's 2014 Global Information Security Survey 2014

www.ey.com/GISS

Cyber Program Management: identifying ways to get ahead of cybercrime

www.ey.com/CPM

Security Operations Centers – helping you get ahead of cybercrime

www.ey.com/SOC

Maximizing the value of a data protection program

www.ey.com/dataprotect

Insights on governance, risk and compliance is an ongoing series of thought leadership reports focused on IT and other business risks and the many related challenges and opportunities. These timely and topical publications are designed to help you understand the issues and provide you with valuable insights about our perspective. Please visit our Insights on governance, risk and compliance series at **www.ey.com/GRCinsights**

EY | Assurance | Tax | Transactions | Advisory

About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization and may refer to one or more of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

In line with EY's commitment to minimize its impact on the environment, this document has been printed on paper with a high recycled content.

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, or other professional advice. Please refer to your advisors for specific advice.

ey.com/id

EY

Building a better working world