COPING WITH CYBER RISK IN MANUFACTURING COMPANIES

12th Swiss Cyber Think Tank | 7 February 2019

Petra Wildemann | Carlos Arocha

AROCHA & ASSOCIATES

Agenda

BACKGROUND

COURSE OF ACTION

CONCLUSIONS

Cyber Threats

- It is more and more difficult to understand the difference of cyber threats between those to one's infrastructure and those being reported by the media

- Can we keep up to with all the potential cyber security threats that are emerging?
- Who are the experts we can follow to learn about the most recent trends in online attacks to be able to protect ourselves?
- Can we trust online software?

- It is vital to keep online presence and systems as secure as possible
- Cyber attacks have to be proactively understood
- Cyber threats need to be defended to ensure our systems retain their integrity

The main Cyber Threats

Phishing/ spear phishing attacks

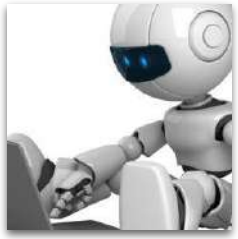
Misuse Of Employee Privileges

Password Cracking / Eavesdropping attack

Hacking (DDOS, Key Logging, Cookie Theft)

BYOD (Bring Your Own Device)

Ransomware



Bots / Credential Reuse

Cyber Security Mini Quiz

Man-in-the-middle (MitM) attack

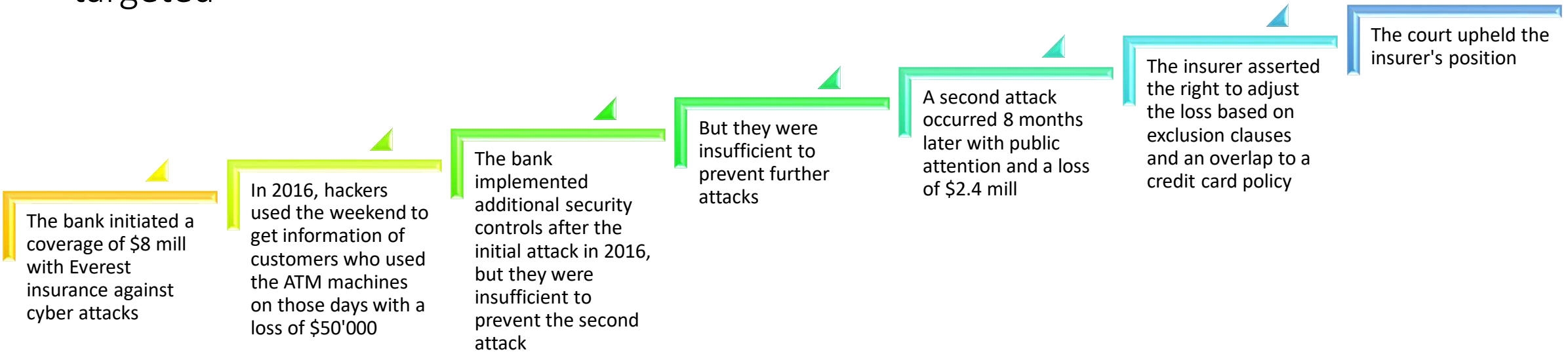
Compliance With Cyber Security Policies

Insufficient Recovery Planning

SQL injection attack

Use Case National Bank

- Attack against the National Bank in Virginia, USA was sophisticated and highly targeted

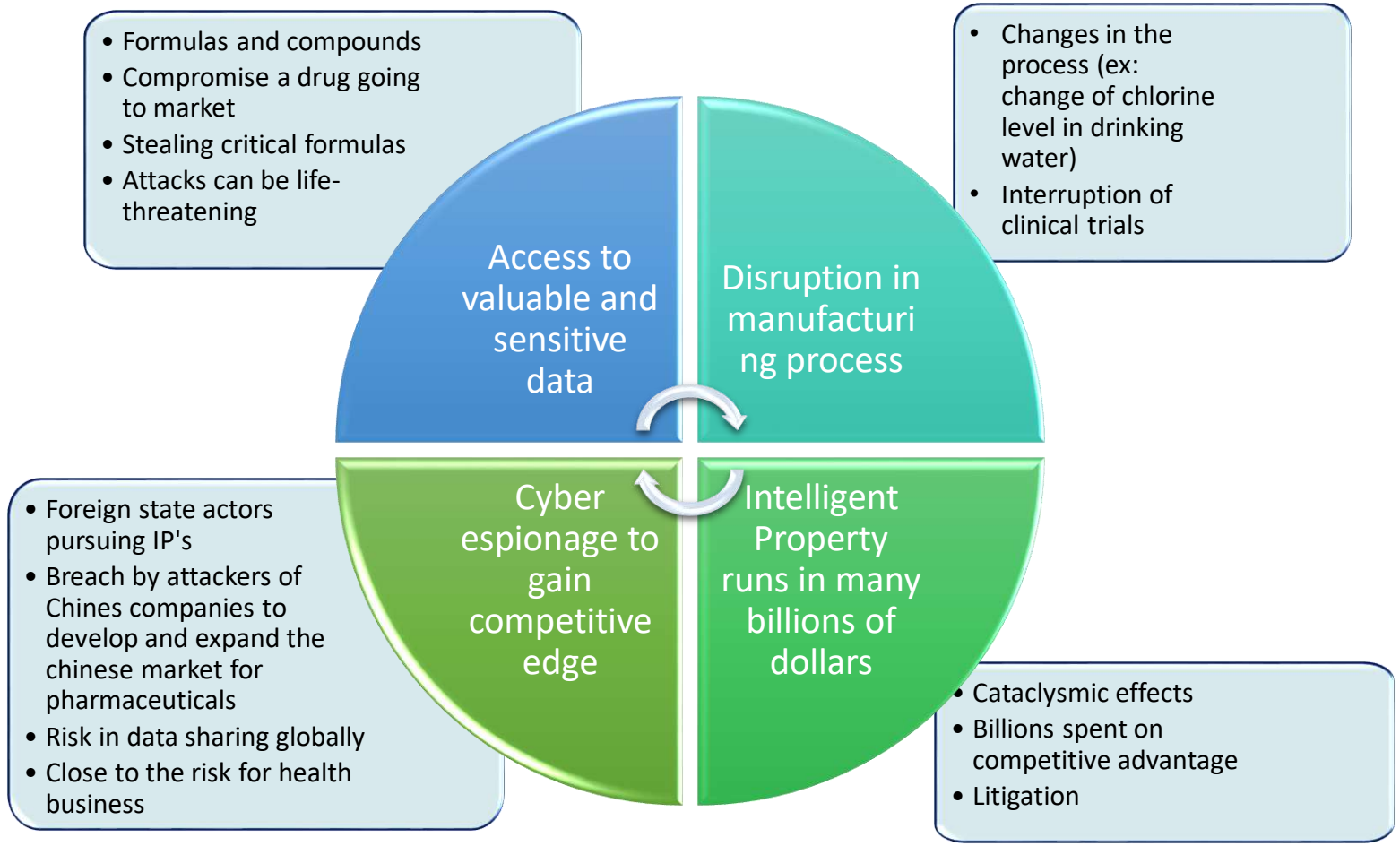


- It would be reasonable for the insurer to cooperate with the bank and to pay for the two claims, which represented 30% of the coverage
- Cases like this do not help the industry by mitigating the risk and using insurance coverages

Cyber security for the pharmaceutical companies

- Cyber threat for pharmaceutical organizations is real
- Prime target for cyber attacks
- Need for highest level of protection

- Any attack can threaten not only the company but also the lives of many customers
- Cybersecurity efforts must be a business initiative with people, process and technology efforts to combat the threat
- Regulations are only a single step toward addressing the issue



Agenda

BACKGROUND

COURSE OF ACTION

CONCLUSIONS

Sources of disruptive risks

EXTERNAL
- fragile economies
- populist agendas
- Brexit
- trade wars
- religious fundamentalism

Political challenges
Megatrends

Market deterioration
Industry disruption

EXTERNAL
- changing consumer behavior and attitudes
- new technologies
- new market entrants
- innovative business models

EXTERNAL
- natural catastrophes
- global warming
- terrorism
- cyber risk

Natural catastrophes
Man-made events

Business model failure
Erosion of corporate assets

INTERNAL
- faulty governance
- lack of strategy
- weak systems and processes
- lack of vision and mission
- lack of an enterprise-wide risk management program

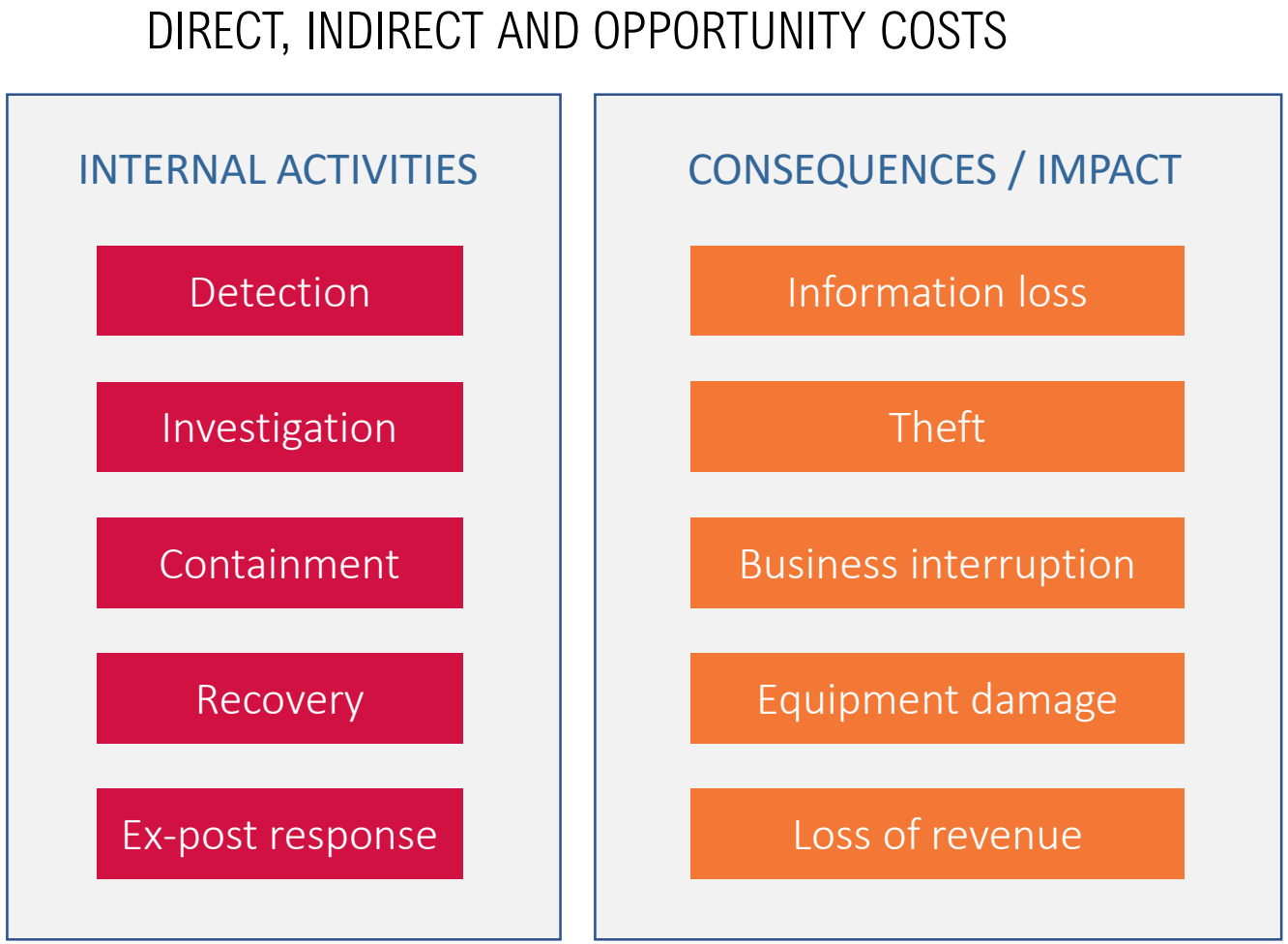
Categories of cyber risk*




ACTIONS OF PEOPLE	TECHNOLOGY FAILURE	FAILED PROCESSES	EXTERNAL
• unintentional • deliberate • lack of action	• hardware • software • systems	• process design and execution • process controls • supporting processes	• catastrophes • legal issues • business issues • service dependencies

(*) *Adapted from Cebula & Young (2010),* A Taxonomy of Operational Cyber Security Risks

Cost of Cyber Crime*



(*) *Adapted from Accenture, 2017 Cost of Cyber Crime Study*

Quantifying Cyber Risk

In general, cyber risk is difficult to quantify owing to

- nature of the risk
- interrelated losses
- lack of reliable data
- severe information asymmetries

Possible courses of action

To manage cyber risk and its threats, there are a few options

- purchase an insurance cover
- engineer resilient supply chains
- set up a captive operation
- embed a risk management culture
- establish an enterprise-wide risk management (ERM) program

Addressing the risks of operating complex supply chains

Resilient supply chains can address critical vulnerabilities, with a more targeted approach than attempting to predict and prepare for every risk type

A resilient supply chain balances risk and costs to prevent or recover quickly from a multitude of dynamic and simultaneous risk-related disruptions

This is achieved through visibility and transparency in the supply chain, flexibility in sourcing, collaboration within and outside of the organization, and a strong control environment

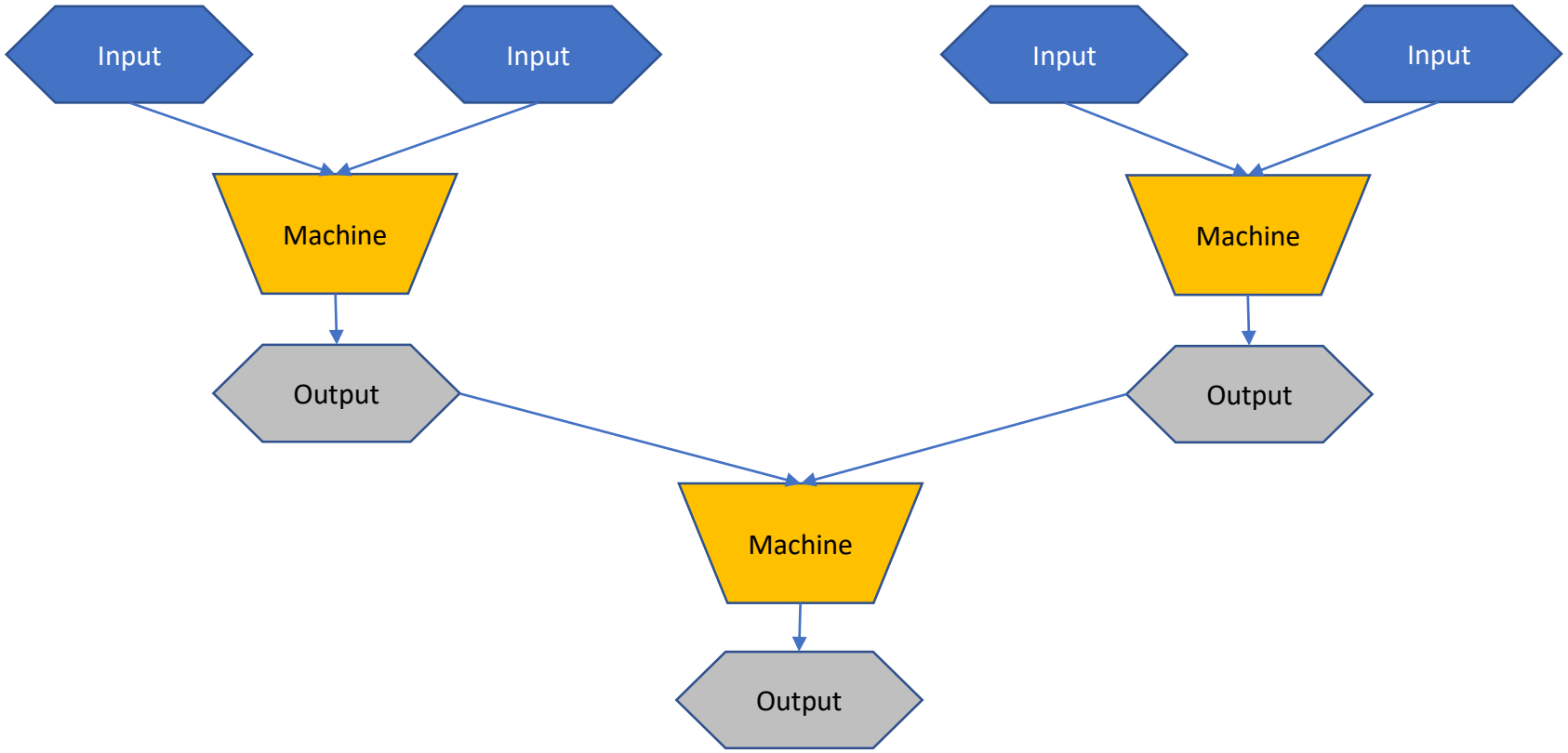
Internal Audit can play an important role in the supply chain processes

Extended role of Internal Audit	• Assessment of related regulations across jurisdictions • Monitoring global processes • Evaluation of import and export processes • Assessment of third-party risks • Consideration of risk management framework, methodology and tools

Other areas to consider include measurement techniques for monitoring supplier performance, availability and delivery of materials, and risk sensing analytic capabilities established by the business to monitor risk exposures within the supply chain

Addressing the risks of operating complex supply chains

Similar questions from a strategic and risk management perspective apply.
The difficulty resides in reproducing the whole production process and derive answers to “what-if” questions on the potential issues that could arise from the production plans. This will improve the risk management of the company.



ERM is the process by which companies identify, measure, manage and disclose all key risks to increase value to stakeholders.

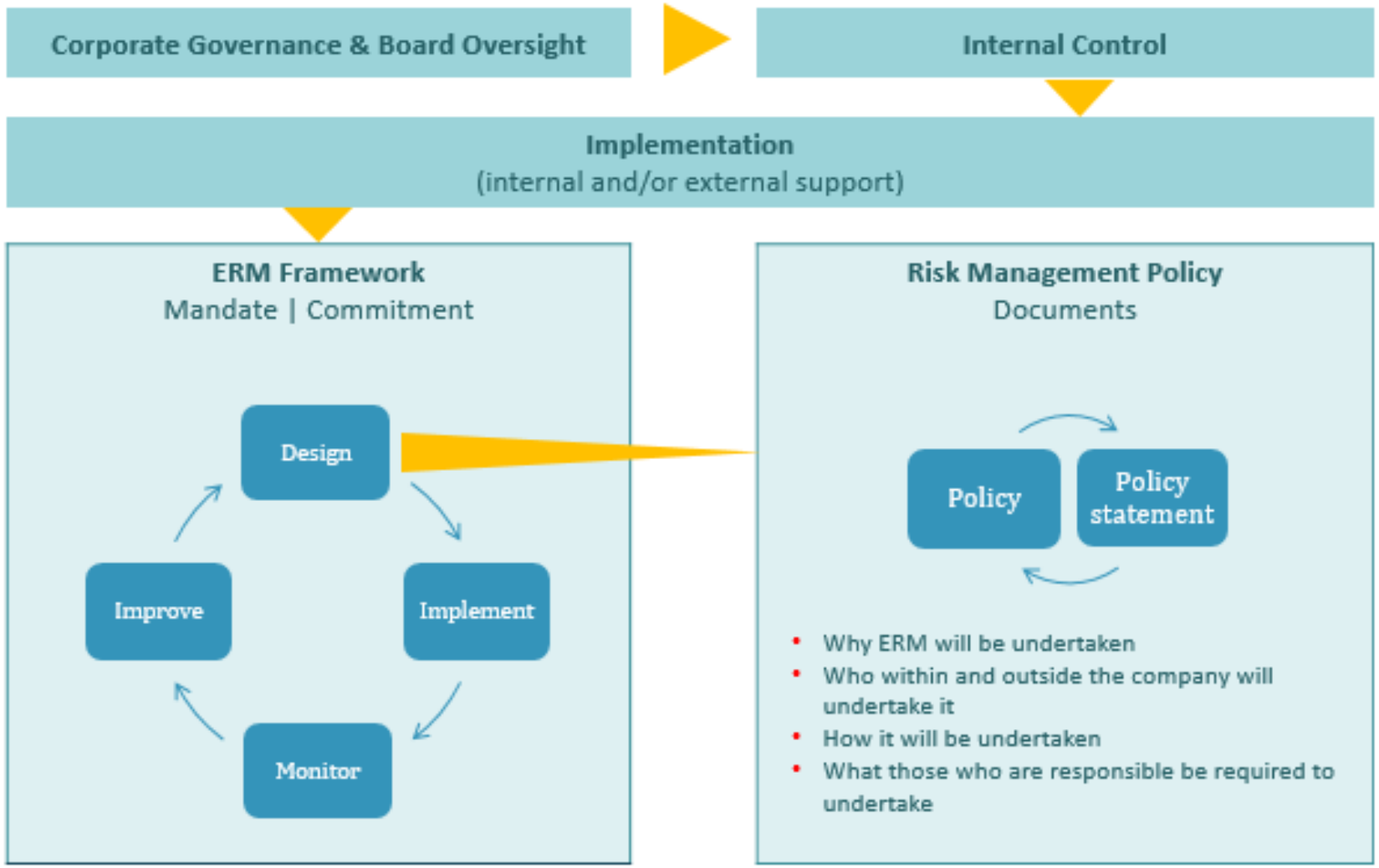
Alternatively,

it’s the ability to capture and manage all necessary risk-related data.

Components of an Enterprise Risk Management program

1 Risk architecture	Specification of roles, responsibilities, communication and risk reporting structure
2 Risk strategy	Risk appetite, attitudes and philosophy defined in a Risk Management Policy
3 Risk protocols	Risk guidelines, including rules, procedures, methodologies, tools and techniques

Overall structure of ERM



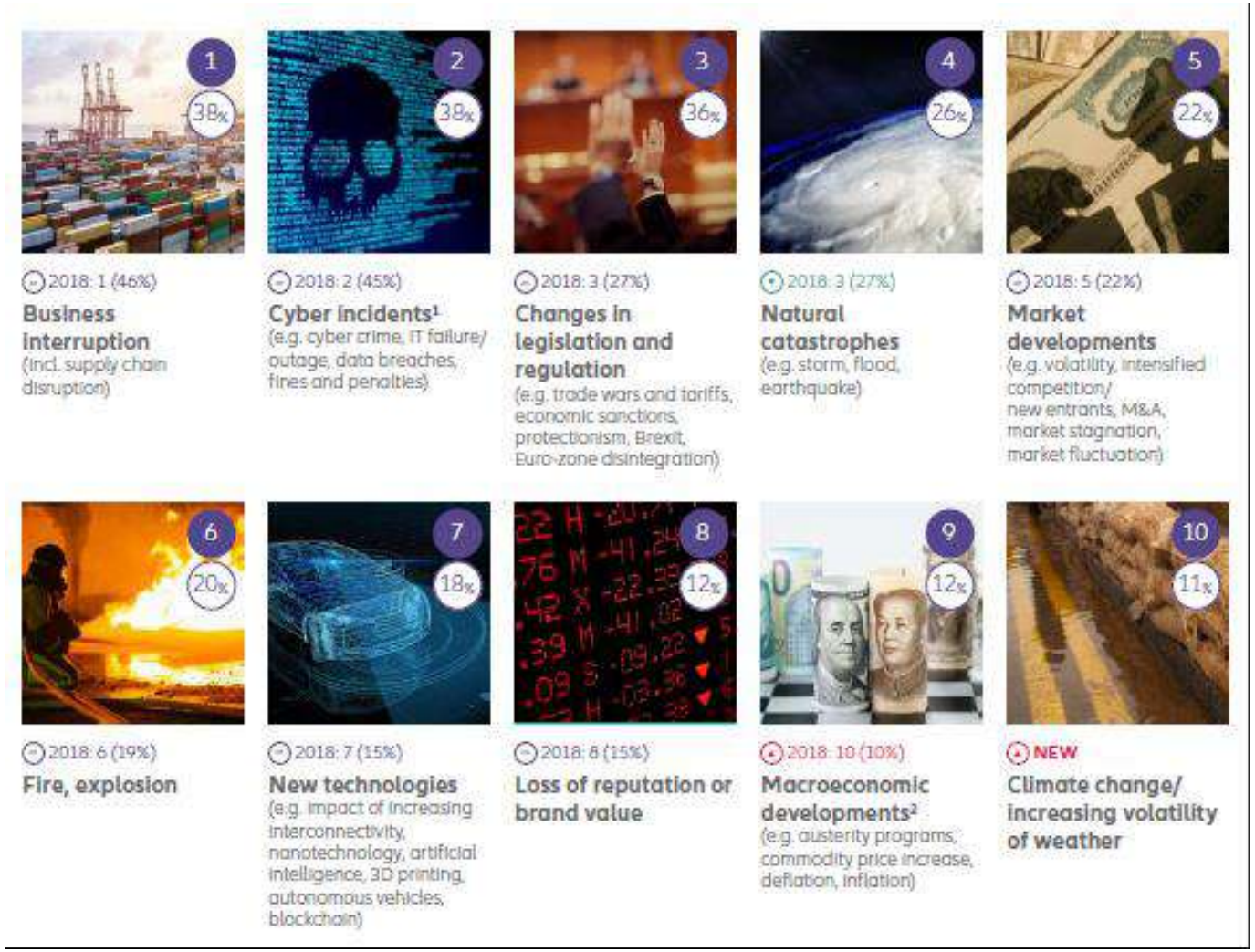
Agenda

BACKGROUND

COURSE OF ACTION

CONCLUSIONS

Top business risks in Europe*



(*) Allianz Risk Barometer (2019), *Allianz Global Corporate & Specialty*

Top business risks: manufacturing & pharmaceutical*

MANUFACTURING

1. Business interruption
2. Natural catastrophes
3. Cyber incidents
4. Fire, explosion
5. Product recall, quality management

PHARMACEUTICAL

1. Business interruption
2. Cyber incidents
3. Changes in legislation and regulation
4. Market developments
5. Product recall, quality management

(*) *Adapted from* Allianz Risk Barometer (2019), *Allianz Global Corporate & Specialty*

Top initiatives funded in cyber budgets*

MANUFACTURING COMPANIES

1. Application security
2. Anti-virus software
3. Security consultants
4. Hardware and infrastructure
5. Cyber studies and research costs
6. Incident response
7. Security Operations Center (SOC)
8. Infrastructure protection devices/products
9. Privacy
10. Enterprise Risk Management

(*) *Adapted from Deloitte (2017),* Cyber risk in advanced manufacturing

Conclusions

- Making supply chains resilient is a real need
- Adoption/overhaul of an enterprise risk management framework should be evident in light of volatility, uncertainty, complexity and ambiguity
- ERM should be viewed as a process that is unique to the company
  - an ongoing process
  - effected by people
  - applied in strategic setting
  - designed to identify potential events and to manage risk within the company's risk appetite
  - must provide reasonable assurance to senior management
  - geared to the achievement of corporate objectives