OLIVER WYMAN

14TH ANNUAL ASIA DERIVATIVES CONFERENCE INTERNATIONAL REGULATORS' MEETING
CYBER WAR GAMES SIMULATION RECAP

TUESDAY, 27 NOVEMBER 2018

MARSH & McLENNAN COMPANIES

CONFIDENTIALITY

Contents

Section 1 | Cyber wargames recap

Simulation outcomes | Stage 1
Financial institutions and regulators have similar views on how to react when anomalies are detected in the system

Simulation context

- **Damage or losses:**
  - Flagged suspicious derivatives trade requests
- **Cyber security team response:**
  - Initial investigation
  - Compromised system
  - Suspected security breach
- **Financial institutions activities**
  - No comments from financial institutions nor regulators
- **Media activities:**
  - Rumor of potential losses of $20MN

Responses

- **Regulators (Audience)**
  - Prioritize mobilizing the incident response team and secure systems in order to contain breach
  - Identify scope of breach to consider cease trading
- **Clearing house**
  - Communicate to regulators, counterparty clearing (CCP) and exchange
  - Identify extent of breach to determine whether to turn exchange feed off
  - Set up crisis management team
- **Exchange**
  - Assess problem by reviewing and reconciling trade and data
  - Communicate how the clearing house will be impacted and consider taking extreme actions
- **Broker**
  - Formation of internal "Major Incident Group" and provide full access to bank resources
  - Communicate with regulators, clients, staff and group overseas

Key takeaways

Identify scope of breach

- Follow the pre-determined incident plan based on known situation
- Identify how broad the breach / incident is and consider what next steps must be taken

Communicate with relevant parties

- Regulators, Clearing house and exchange, clients, staff (media, internal, etc.) and group overseas

Set up incident response team in war rooms

- Mobilize incident response team and provide full access to bank resources

Simulation outcomes | Stage 2
The key for both institutions and regulators is to be well-prepared and utilize communication channels effectively

Simulation

- **Damage or losses:**
  - Not only financial loss and also sensitive data breach
- **Cyber security team response:**
  - Breach in clearing house's security systems
- **Financial institutions activities**
  - Fears due to similar modus operandi to other entities
- **Media activities:**
  - Threats of legal action to the players at fault for the breach

Responses

- **Regulator**
  - Communicate with cross-border entities (e.g. other governments)
  - Understand the fallback / contingency plans (e.g., when to segment systems, isolate entities)
- **Clearing house**
  - Focus on containment and recovery
  - Follow legal & compliance (data breach notification and cross jurisdiction)
  - Manage public sentiment (focus on reducing panic) by proving zero weaknesses and that the attacker is no longer present in the system
  - Consider taking extreme actions, if needed as part of containment / recovery
- **Exchange**
  - Have alternate infrastructures set up, if needed, to continue BAU processes
- **Broker Dealer**
  - Identify specific infrastructure affected and if there are any liquidity implications

Key takeaways

Be well prepared

- Having a response plan strategies / playbooks even in an unclear situation is critical to managing and recovering from an incident
- Be able to determine clearly what part of the infrastructure has been breached, and subsequent action plan

Communicate effectively

- Communicate timely to relevant cross-border parties to prevent further attacks
- Identify ways to promote confidence in the market / institutions

Act conservatively

- Contingency may require turning off clearing house to limit exposure / span of the attack
- Standardized daily reconciliation and market-wide simulated reconciliation as exercise

Section 2 | Actual results from session

The regulators would prioritize ceasing trading and share relevant information with the impacted market entities

OLIVER WYMAN

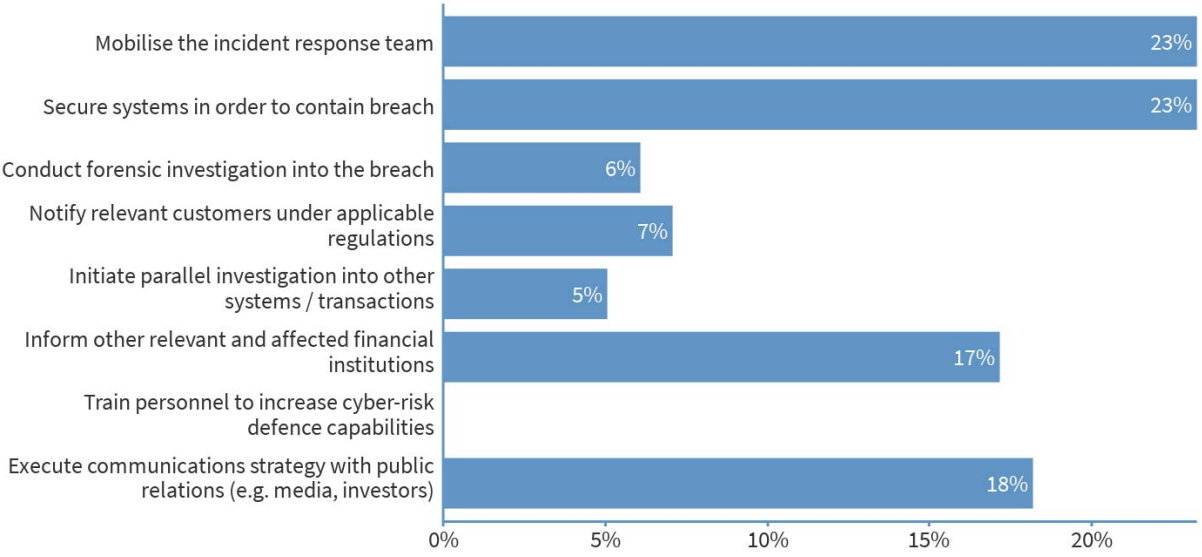
As the main regulator, what would be your priority action?

Poll locked. Responses not accepted.

The top 3 actions are mobilise the response team, contain the breach and communicate with relevant parties

What would be the top 3 actions that you would promote Financial Institutions to work on the first 24 hours of the alleged cyber-attack on Smart Clear?

Poll locked. Responses not accepted.



Top 3 stakeholders are national cyber agency, banking regulators and relevant industry participants

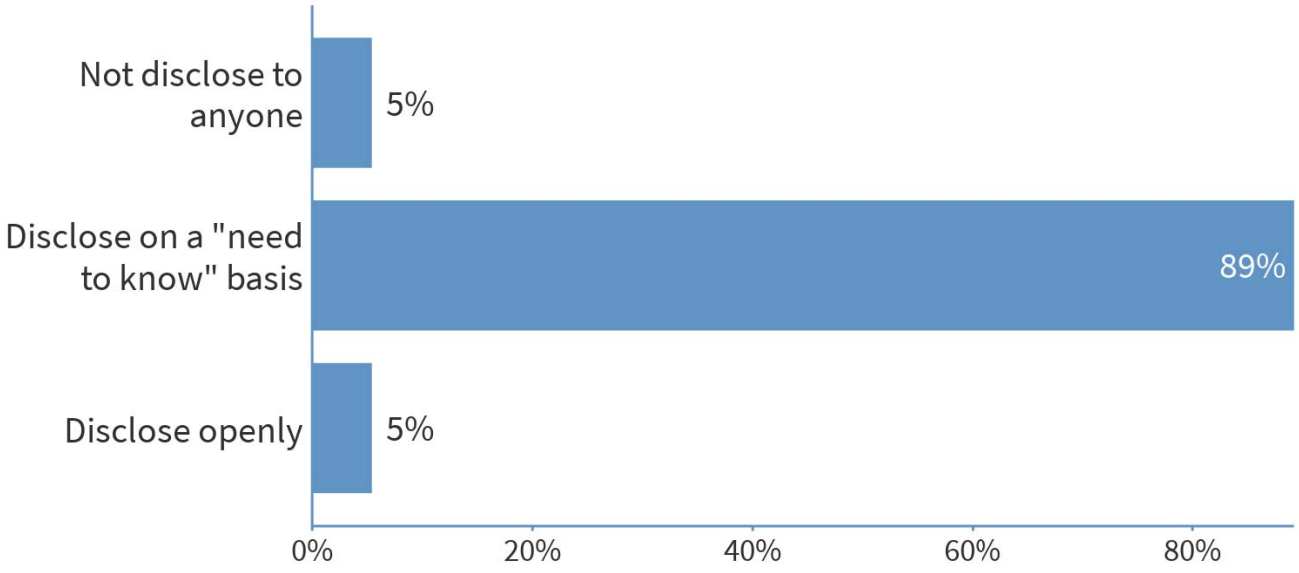
Who would be your top 3 stakeholders to engage and keep informed?

When poll is active, respond at **PollEv.com/cyberattack** Text **CYBERATTACK** to **+65 8241 0042** once to join

Transparency of shared information is recommended to disclose on a "need to know" basis

How transparent would you be with the information gathered from the investigation?

When poll is active, respond at **PollEv.com/cyberattack** Text **CYBERATTACK** to **+65 8241 0042** once to join



Panel had similar views on what are the priorities against cyber attacks

SmartClear CEO
- Communicate regulators, ccp participants, exchange
- Identify the extent of breach and communicate with counterparties
- Determine whether to turn exchange feed off

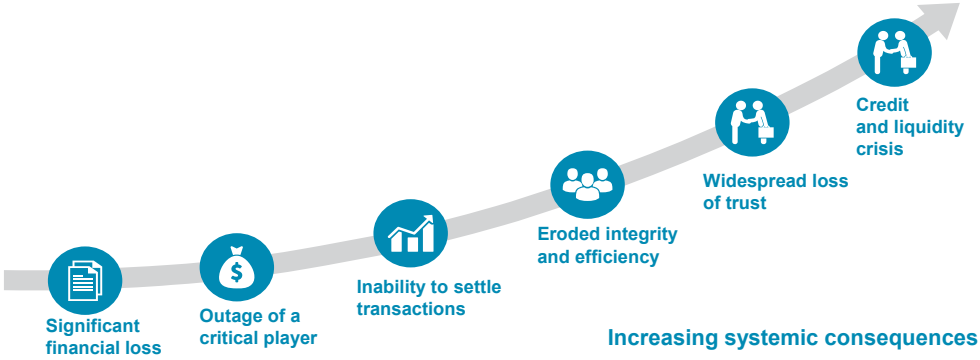
SmartClear COO
- Identification/Classification - What went wrong? Invoke forensics, security ops, last good data set, IOCs, affected party identification
- Set up crisis management team in war rooms
- Invoke pre-defined incident response playbook / comms plan (counsel, police, regulators, government, public affairs, peer group - WFE group (IOCs, general info), other participants, internal - upward, public

SmartEx CEO
- Assess whether the problem is with the Exchange by reviewing and reconciling trade and supervision data
- Ask SmartClear what they are doing about he problem and whether their service will be impacted in the coming hours - if so, consider closing the market
- Communicate with the regulator based on the above steps and avoid media speculation, but share operational consequence for the market

TradeCo
- Formation of our internal "Major Incident Group"; brings together TOP executives with full access to all bank resources.
- Communications to Regulator (escalated to clearing house no feedback yet and do you have any other reports), Clients (working with exchange will come back with details), staff (media direct to media team, working with clearing house) and group overseas
- Gathering information on risk exposure (clients, own, clearing house) and determining the origin of the problem

Section 3 | Cyber risk perspectives

Cyber attack can occur in several categories with increasing systemic consequences to market participants



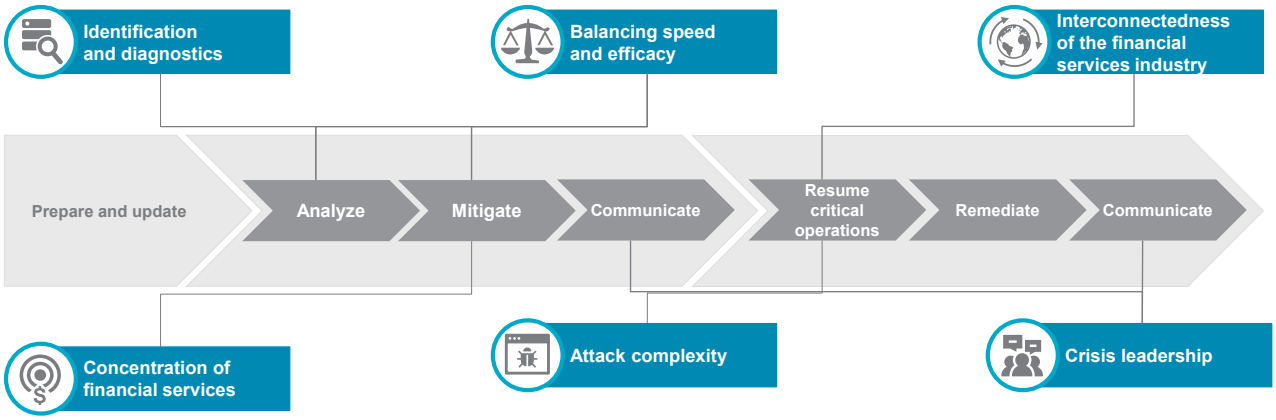
Cyber-attack categories	Significant financial loss	Outage of a critical player	Inability to settle transactions	Eroded integrity and efficiency	Widespread loss of trust	Credit and liquidity crisis
Deletion of critical data		✓	✓	✓	✓	✓
Manipulation of critical data		✓	✓	✓	✓	✓
Disruption of critical industry-wide services		✓	✓	✓	✓	✓
Fraudulent transactions	✓			✓	✓	
Theft of critical non-public information	✓			✓	✓	

Response and recovery from a cyber attack can be challenging

- **Uncertainty around the origin, time and point of impact** of a cyber-attack
- Data sharing and **fast collection of relevant information** from a large number of partners

- **Lack of tailored requirements** and expectations for specific cyber-scenarios
- **Lack of fully effective industry-wide testing** may challenge fast industry-wide recovery

- **Connectivity of the financial system facilitates the spreading of a cyber-attack** across financial infrastructures, financial institutions and geographies



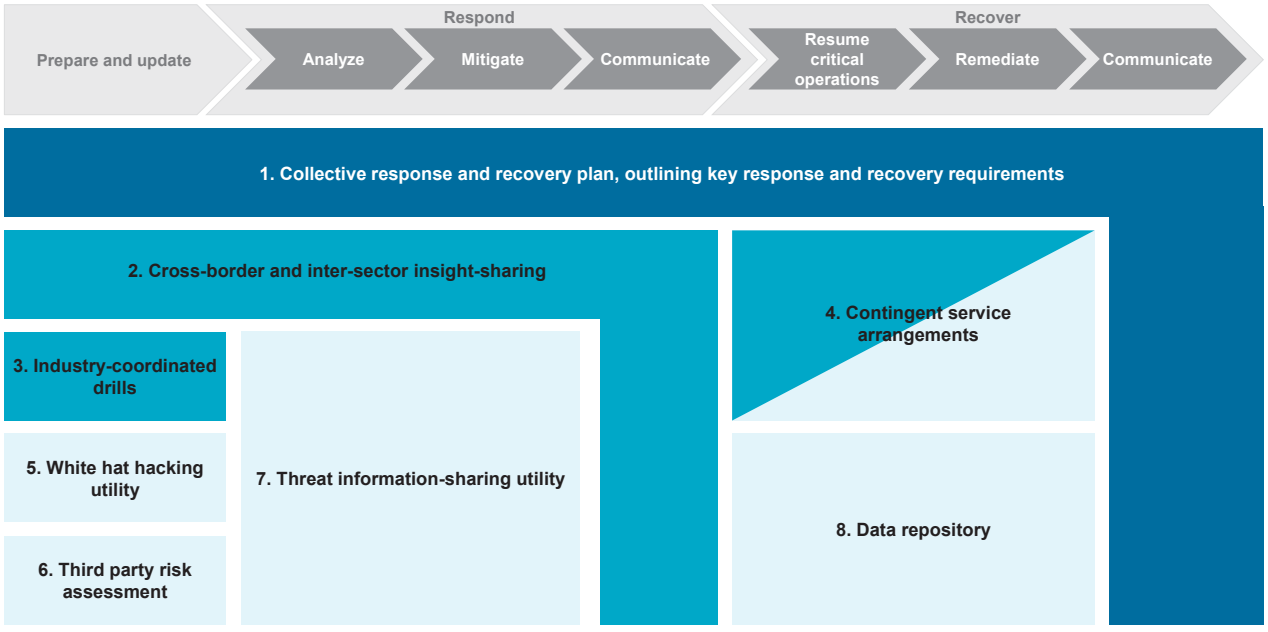
- **The increasing usage of cloud providers** could exacerbate the consequences of a successful large-scale cyber-attack

- **Difficulty in defining adequate response and recovery strategies** given the broad scope of potential impacts of cyber-attacks (e.g. compromise of backups, coordinated attacks on multiple sectors)

- **Insufficient clarity around leadership** may hinder key decision-making and coordinated communication to the public

Tackling cyber attacks - Initiative 1: Industry collaboration

As cyber threats tend to be more systemic in nature, drafting responses to such threats presents an opportunity for enhanced industry collaboration

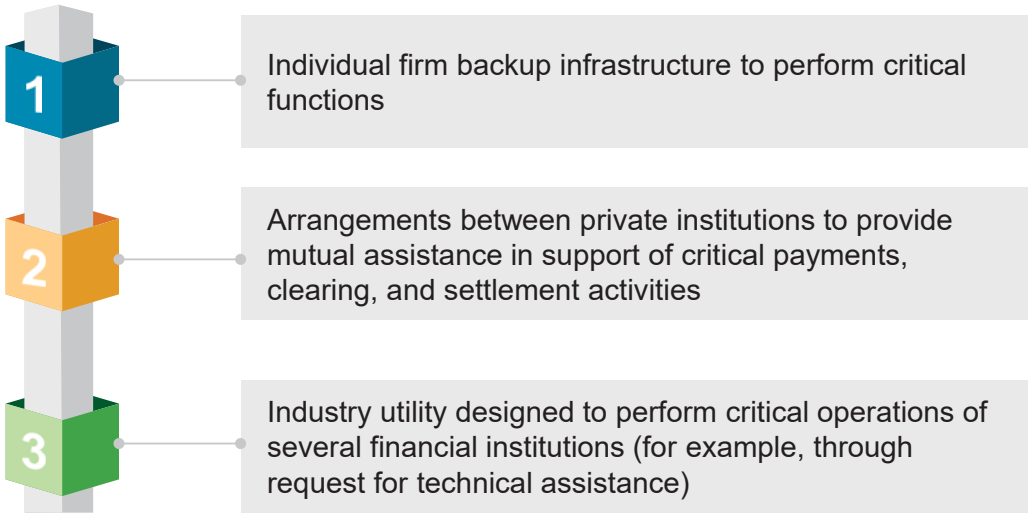


1. [7] Sheltered Harbor is a voluntary industry initiative for secure storage and rapid reconstitution of retail bank customer account data. Data is stored in a distributed fashion in a Sheltered Harbor specified data vault, it is kept private by each institution and is encrypted.

Tackling cyber attacks - Initiative 2: Contingent Service Agreement

Irrespective of preparedness to protect against cyber threats, FIs should have contingent service agreements, given scale and complexity of cyber attacks

Candidate operating models for contingent service agreements



Section 4 | Credentials

Oliver Wyman is part of Marsh & McLennan Companies (MMC), the premier global professional services firm

MARSH & McLENNAN COMPANIES

- Revenue 2016: Over US$13 BN
- Staff: 60,000
- Clients in more than 130 countries
- Listed on the New York Stock Exchange

OLIVER WYMAN | Marsh Inc. Risk and Insurance | Guy Carpenter Re-Insurance Advisors | Mercer Human Capital

Industry knowledge

With more than 40 years of experience in consulting with leading companies in following industries

- Automotive
- Aviation, Aerospace and Defence
- Communication, Media and Technology
- Energy
- Financial Services
- Health and Life Sciences
- Industrial Products
- Retail and Consumer Products
- Distribution and Wholesale
- Surface Transportation
- Public Sector
- Surface transportation
- Business Services
- Travel and Leisure

Capabilities

Broad expertise in functional areas

- Strategy and Growth
- Marketing and Client Relationship management
- **Risk Management**
- Mergers and Acquisitions, Capital Markets
- Cost Efficiency and Operations
- R&D and Innovation Excellence
- **Digital**
- **Strategic Information Technology**
- Restructuring
- Procurement and Supply Chain
- Organisation and Processes

Presence

US$1.8 BN revenue
Staff of 4,500 in 50+ cities across nearly 30 countries

- Abu Dhabi
- Atlanta
- Bangalore
- Barcelona
- Beijing
- Berlin
- Boston
- Chicago
- Columbus
- Dallas
- Detroit
- Dubai
- Dusseldorf
- Frankfurt
- Hamburg
- Hamilton
- Hong Kong
- Houston
- Istanbul
- Keller
- Leatherhead
- Lisbon
- London
- Los Angeles
- Milan
- Madrid
- Melville, NY
- Mexico City
- Milwaukee
- Montreal
- Moscow
- Munich
- Mumbai
- New Delhi
- New York
- Ottawa
- Paris
- Philadelphia
- Pittsburgh
- Portland
- Princeton
- Reston
- Riyadh
- San Francisco
- Sao Paulo
- Seoul
- Shanghai
- Singapore
- Stockholm
- Sydney
- Tokyo
- Toronto
- Washington DC
- Wilmslow
- Zurich

Source: Oliver Wyman

Oliver Wyman and MMC integrated capabilities cover the full NIST Cyber security framework

Understand Cyber Risk Exposure (Oliver Wyman Group, Marsh)

- Cyber risk management framework
- Industry and sector benchmarking exercises
- Risk quantification, mapping and modelling

Strengthen Internal Capabilities (Marsh, Mercer)

- Endpoint security assessment and review
- Attract and retain cybersecurity experts and talent management

Enhance Cyber Analytics (Marsh, Marsh Risk Consulting)

- Enhance threat intelligence (in partnership with FireEye)
- Vulnerability management

Manage Business Continuity Plans (Marsh/Marsh Risk Consulting, Oliver Wyman)

- Crisis management and business continuity

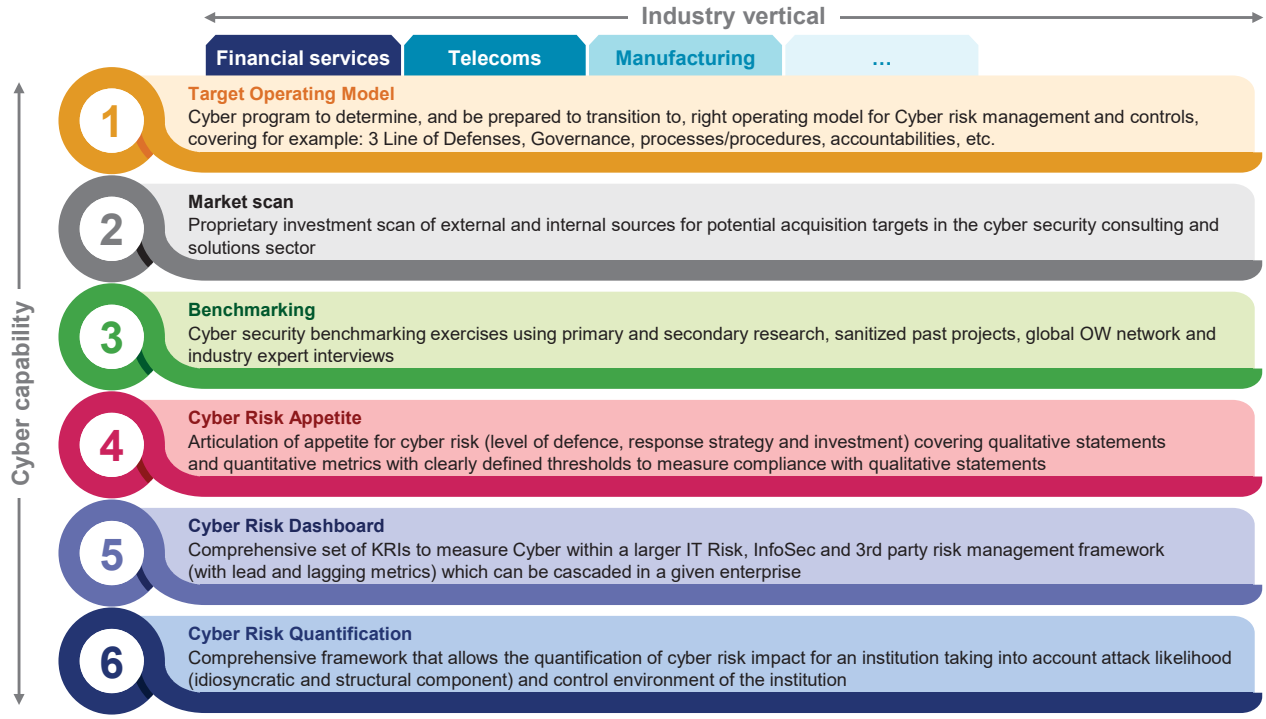
Strategize Risk Transfer Solutions (Marsh, Guy Carpenter)

- Bespoke (re)insurance coverage optimization and enhancement

1. Published in 2014 by National Institute of Standards & Technology (NIST) based on foundations introduced by Obama administration to Improve critical infrastructure Cyber security

Oliver Wyman helps clients enhance their Cyber risk management capabilities across multiple industries

OLIVER WYMAN



Oliver Wyman has successfully delivered a broad range of Cyber projects across industries (recent examples)

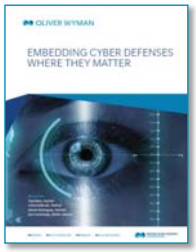
Client	Goal and outcome of the project
Scandinavian universal bank	• Assessment of existing cyber security roadmap and target operating model design
Leading US Bank	• Assessment of cyber security roadmap framework, identification of weaknesses, cyber risk strategy framework implementation
Leading US Utility	• Assessment and prioritization of reactive and preventive cyber risk mitigation and information protection measures with workshops on investment prioritisation
UK municipal institution	• Assessment of status quo, future developments and impact of cyber trends to Financial Services industry in a certain region and creation of a report on an action plan and roadmap
Leading German Car Manufacturer	• Assessment of existing cyber security roadmap and identification of weaknesses for the development of a framework to continuously adapt the information security infrastructure of the company
Leading North American consumer lender	• Assessment of the cyber risk program based on NIST Cybersecurity Framework and the creation of a roadmap for changes in cybersecurity policies and their incident response plans
Leading Consumer Lender	• Assessment of the technical controls and risk approach for the development of a risk-based approach to assess the technical controls and cyber risk processes
National financial institution	• Ongoing Cyber Security Program Assessment
International financial institution	• Assessment of the potential cyber risks that could affect the business which resulted in the creation of a transition risk governance program and the creation of an effective link between IT Risk and Group Risk Management
Defence technology firm	• Assessment of the clients current state security situation after a suspected data breach which resulted in the client attaining a better transparency of their security risks and an implementation outline to solve deficiencies
Global provider of secure messaging services	• Definition of a Cyber Counterparty Risk Management framework to implement a counterparty-relationship assessment that incorporates risk, business and mitigating factors
Leading online discount stock brokerage	• Assessment of the impact of a recent organisational change on the cyber security of the client which resulted in the creation of a target state model for the client and the development of high-level initiatives to address issues
Leading online brokerage firm	• Design of a digital Cyber Dashboard to support board and management analytics and decision making across cyber risk topics

Other Cyber Risk Publications

Oliver Wyman regularly publish leading industry insights on a wide range of cyber-related topics

- Not exhaustive -

Embedding Cyber Defences Where They Matter



Equifax major data breach implications

Deploying a Cyber Risk Strategy: Five key moves

Cyber Risk Management: Why hackers could cause the next global crisis

Closing the Door to Cyber Attacks: How enterprises can implement comprehensive information security

Taming Cyber: Quantifying cyber risk using a structured scenario approach

Evolving Challenges in Cyber Risk Management: Protecting assets and optimizing expenditures

Cyber Risk in Asia Pacific: The case for greater transparency

Section 5 | Contacts

Oliver Wyman expert panel

Jacob Hook
Head of APR
Jacob.Hook@oliverwyman.com

Christian Pedersen
Head of Finance & Risk practice
Christian.Pedersen@oliverwyman.com

Tim Colyer
Head of Indonesia
Tim.Colyer@oliverwyman.com

Anutosh Banerjee
Corporate & institutional banking practice
Anutosh.Banerjee@oliverwyman.com

Vadim Kosin
Head Digital, Technology and Analytics
Vadim.Kosin@oliverwyman.com

Jayant Raman
Non Financial Risk practice
Jayant.Raman@oliverwyman.com

Alon Cliff-Tavor
Digital, Technology and Analytics, and
Corporate & institutional banking practice
Alon.CliffTavor@oliverwyman.com

OLIVER WYMAN