MARSH

Navigating a World of Elevated Risk:

Implications for Cyber Risk Management

October 27, 2020

MARSH & McLENNAN COMPANIES

Navigating A World of Elevated Risk
Implications for Cyber Risk Management

1. Current risk context: An illustration
2. New world of elevated risk: Impact of technology & COVID-19
3. Changes to cybersecurity and cyber risk environment
4. Changes to cyber insurance markets / policies / buying considerations
5. Looking ahead: The new normal

Our Speakers

Thomas Fuhrman
Managing Director, Advisory
Marsh

Paul Mee
Cyber Practice Lead
Oliver Wyman

Bob Parisi
Cyber Product Leader
Marsh

Poll #1

1. Which of the following rank among your top 5 risk concerns for 2021 (excluding cyber threats)? (Multiple choice)

Financial stability / performance	71%
Political / social unrest	56%
Climate change / weather events	30%
Regulation	28%
Workforce morale / productivity	45%

A Context Setting Story

A Cyber Exercise in an Environment of Heightened Risk Realization

Major US Fortune 50 corporation
Practical cyber exercise scope

Progressive Ransomware

Protests abroad

Blockade

Hurricane

A Cyber Exercise in an Environment of Heightened Risk Realization

Major US Fortune 50 corporation
Practical cyber exercise scope

Progressive Ransomware

Protests abroad

Blockade

Hurricane

Meanwhile in the ‘real world’…

Two hurricanes

Protests domestically

COVID Pandemic

Extensive wildfires

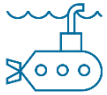
Persistent attacks
on third parties

Elevated Risk Manifestation

Increasing Use of Digital Tech is Fueling Cyber Risk Conditions

Seamlessness (eg Heath, Travel)

Internet of things



Autonomous transport

Advanced computing (eg cloud, 5G, quantum,)

Robotics

Biometrics

Artificial intelligence

Open APIs/Microservices

COVID Has Created an Environment of Greater Exploitation

- Alternate modes of working
- Different technology utilization
- Less familiar modes of data movement and exchange
- Rebalancing of supply chain dynamics and third-party reliance
- Facility access and collaboration constraints
- Management and staff distraction
- Rogue actor motivation

148%

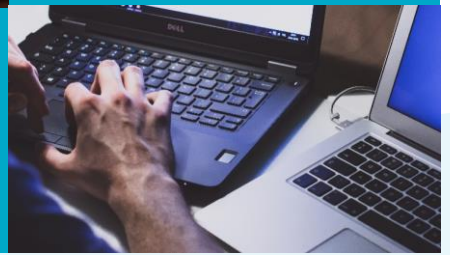
Increase in ransomware attacks versus 2019

90%

Cybersecurity professionals working overtime

4.83M

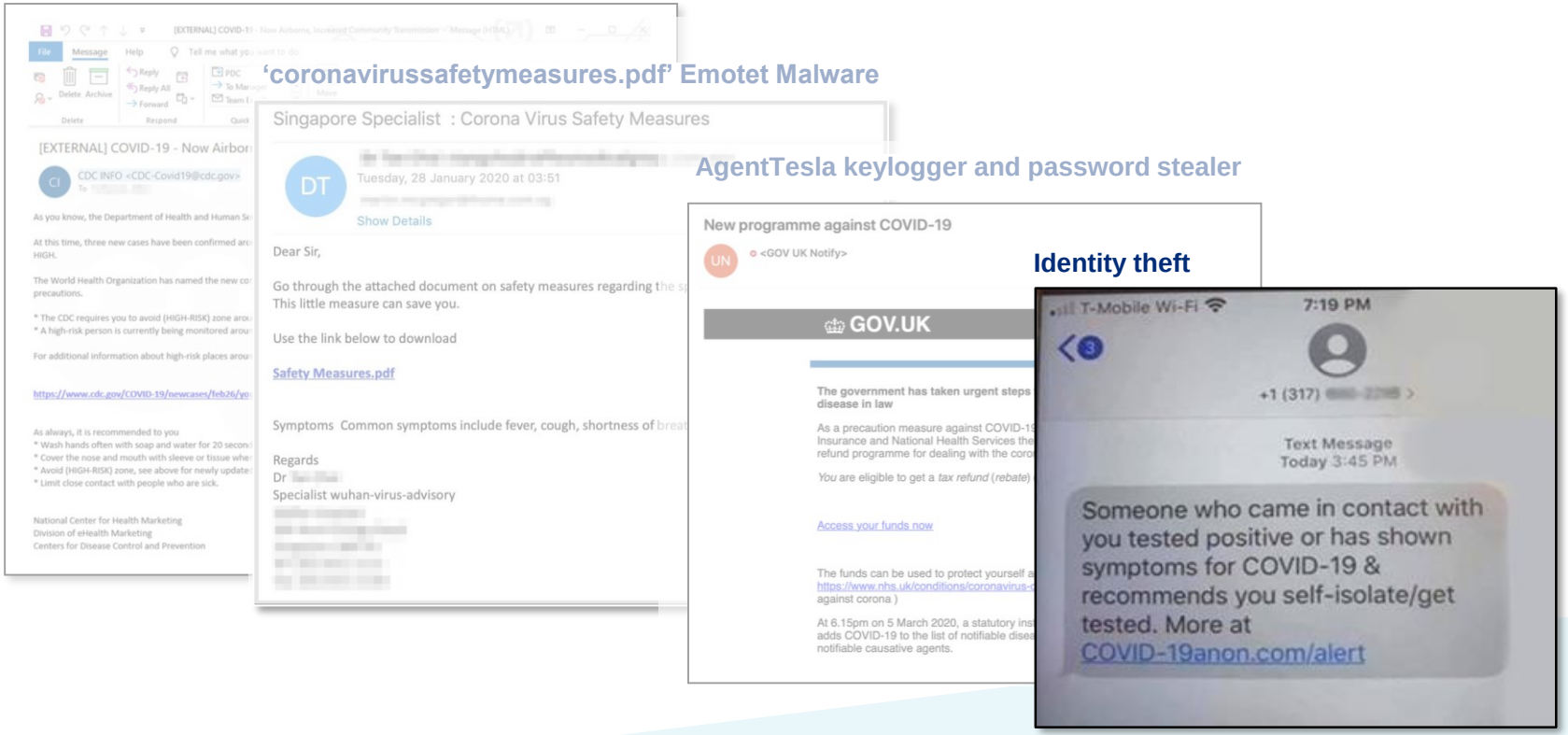
DDOS attacks since COVID prevalent in the West, up +25% vs. 2019



Sources: VMWare Carbon Black; NetScout

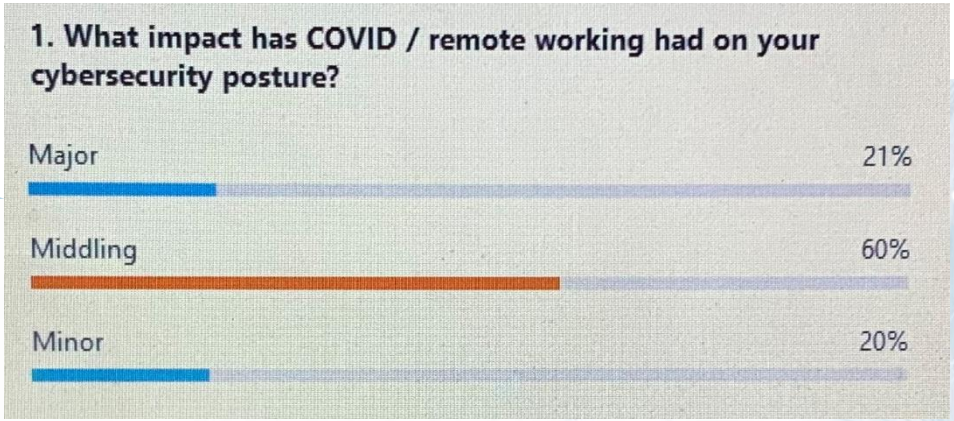
COVID Oriented Cyber Exploitation Examples

Adapted Phishing



Sources: Recorded Future, Cofense, IBM, IssueMakersLab, Proofpoint

Poll #2


1. What impact has COVID / remote working had on your cybersecurity posture?
Major
21%
Middling
60%
Minor
20%

Changes to Cybersecurity & Cyber Risk

Changes to Cybersecurity and Cyber Risk

Restructured work patterns and changing business models define the landscape:

- **High level of remote working**

- **Changing business models**
  - Decentralizing operations
  - Continued adoption of cloud services
  - More eCommerce
  - Long-term impact on cybersecurity approaches
  - Hybrid working becomes the norm
  - ‘Emotionally impacted’ and displaced workers
  - Personal data collection for COVID (e.g., temperature, personal/health info)

Poll #3


1. Where do you plan a material change in your cyber risk spending next year? (Multiple choice)
Cybersecurity technology 62%
Consultants / advisors 16%
Hiring / staffing 9%
Employee education / training 52%
Insurance 21%
Other 3%
We plan no material spending changes 14%

Changes in Cyber Insurance

Changes in Cyber Insurance

Insurers' Biggest Risk Concerns

- Ransomware
- Pandemic/Remote Connectivity

Pricing

- Insurers responding to increased losses from ransomware

Coverages

- Cyber Extortion and Business Interruption coming under increased scrutiny

Underwriting Questions

- Supplemental ransomware applications

Buyers' Behaviors

- Increased demand for coverage and higher limits driven by:
  - Awareness of the risk
  - Silent Cyber initiatives

Cyber Insurers' Biggest Risk Concerns

Ransomware attacks are increasing in both frequency and severity as it grows more lucrative

Attacks are becoming more **frequent**, aided by new types of ransomware and malware.

COVID-19-related topics in phishing emails are targeting remote workers.

With more people working in **less secure cybersecurity environments**, attacks are more successful.

Cybercriminals are increasingly targeting ransomware attacks to **enterprises, governments, and healthcare organizations.**

239% increase in ransomware attacks reported by Beazley clients between 2018 and 2019.

Operational and financial **severity** are rising sharply: ransom demands, related costs, and operational downtime are all growing exponentially.

Average ransomware payments were up **60%** in Q2 2020, reaching **$178,254**.

Downtime from ransomware events now averages **16 days**: more than 2 weeks of business impairment and disruption.

The **complexity and cost of remediation** are growing, with ransomware proving increasingly damaging and expensive.

Average ransom demanded in Maze ransomware attacks is **6 times** the overall average.

Bad actors prey on pandemic conditions: virtual work environments, changes to business operations, distracted workforces, and individuals' anxiety

Cyber Insurance Changes: Coverage Issues

Cyber Extortion/Ransomware

- Recent regulatory activity:
  - Calls into question propriety of ransomware payments, citing OFAC
  - Takes novel approach of applying OFAC restrictions to individuals and organizations allegedly responsible for ransomware
- Ransomware payments have caused insurers to take a hard look at this coverage grant
- Increased underwriting scrutiny: many insurers now insist policyholders complete special ransomware supplemental applications
- Not yet implemented, some insurers suggest they may begin sub-limiting Cyber Extortion coverage

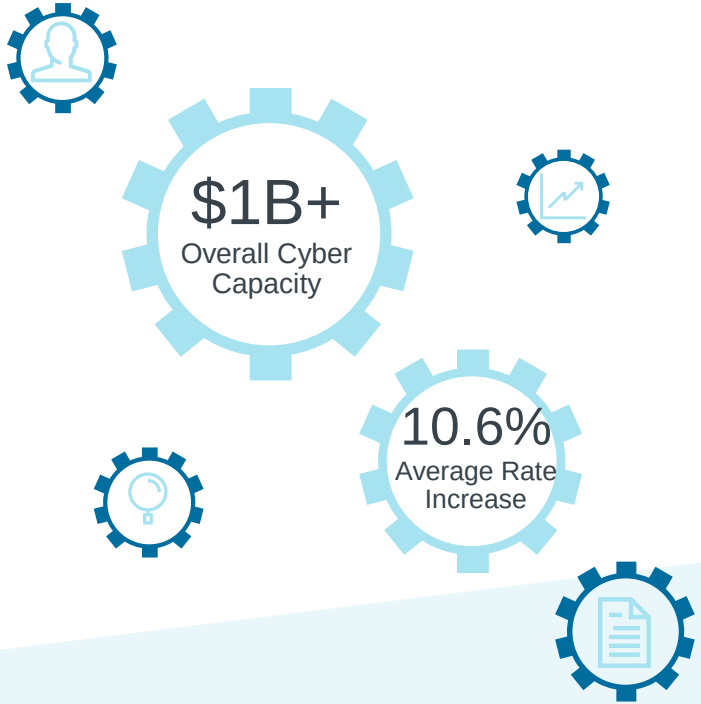
Remote Engagement

- Insurers have clarified and/or expanded existing definitions (i.e. computer system)

US Cyber Insurance Q3 Market Update

- Q3: Total program cyber rates increased by 10.6% average, all industries.
- Q2: Primary cyber rates increased by 6.4% average, all industries.
- Primary rate increases were lower than total program increases: excess pricing is increasing more quickly than primary.
  - Consistent with the prior three quarters.
- Acceleration of rate increases is largely a response to significant increases in frequency and severity of ransomware and business interruption claims.
  - Uptick has particularly affected primary insurers in SME segment.
- Capacity remains ample, with largest programs exceeding US $700 million.
- Larger programs: Some tightening of capacity as many insurers manage limit deployment to coincide with global aggregation strategies.

Cyber Insurance Market



Looking Ahead

Poll #4

1. Are you changing your overall risk management practices to address the new / elevated risk landscape?

Yes significantly	19%
Yes in minor ways	59%
Not materially	22%

Looking Ahead
New Normal: Cybersecurity & Cyber Risk Management

Re-evaluating risk and building resiliency

- Tighten the strategic management of cybersecurity as an enterprise risk
  - ✓ Coordinate roles and processes from Board of Directors through IT/cybersecurity operations
  - ✓ Refresh the cyber risk register
- Focus on cyber resiliency
  - ✓ Integrate cybersecurity and business continuity plans and processes
  - ✓ Build on inherent resilience of decentralized workforce
  - ✓ Improve operational readiness in cybersecurity – event detection and response

Looking Ahead
New Normal: Cyber Risk Transfer & Coverage

Markets: Flight to Quality

- Capacity remains robust and sufficient to meet demand.

Pricing

- Expectation that rates will increase.
- Insureds can still differentiate themselves to mitigate premium increases.
- Insurers offering discounts and reductions for active loss prevention.

Coverages

- Cyber Extortion coverage will be continued to be scrutinized by insurers.
- Market faces challenges as Silent Cyber muddies the waters in P&C market.

Underwriting Questions

Increased scrutiny around:

- Ransomware.
- Vendor risk.
- Business Interruption.

Buyers' Behavior

- Demanding higher limits and broader solutions.

Looking Ahead
New Normal: Changes in Overall Risk Management

Arguably, these elevated longer-tail risks have always been out there – but for now and looking forward they feel more real, more present, and more dangerous.

Risk Management Imperatives

- Understand the nature of risks you face, especially considering current circumstances and environment.
- Be prepared to understand threats and associated exposure.
- Confirm mitigation, plans & practicalities (eg., BCP, supply chain risk).
- Explore opportunities for risk transfer (eg., enhanced, revised insurance).
- Conduct practical exercises for most present risks (eg., ransomware).

MARSH

Navigating a World of Elevated Risk:

Implications for Cyber Risk Management

October 27, 2020

MARSH & McLENNAN COMPANIES