THE ROLE OF RISK AND INSURANCE IN MANAGING VENDOR CYBER RISKS

Martha Jacobs
Healthcare Practice Leader

Adam Peckman
Cyber Risk Consulting Practice Leader

KEY TOPICS

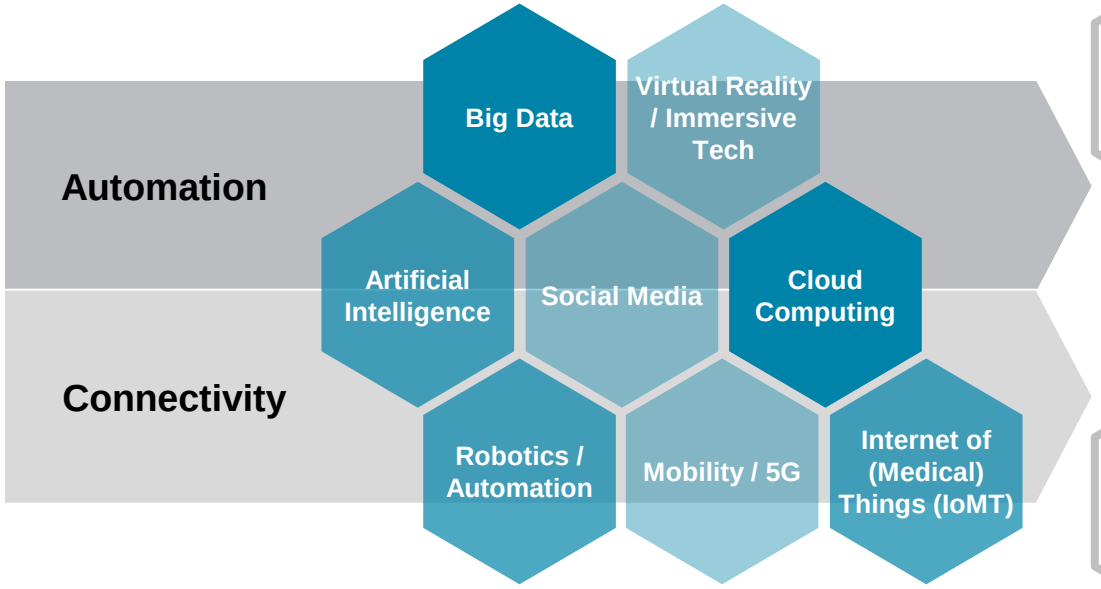
- Greater digital interconnectivity and technological dependencies created more complex aggregation and joint liability in the healthcare industry
- Emergence of vendor cyber risks
- Role of Risk teams in identifying and evaluate vendor cyber exposures
- Practical strategies can be adopted to improve vendor cyber readiness and financial resilience

THE EMERGENT RISK

INDUSTRY 4.0 IN HEALTHCARE

The increasingly application and dependency on technology in the Healthcare Sector has created more complex, and more impactful exposures to cyber events.

Economic Drivers **Technology Drivers** **Strategic Threats to Healthcare**



Disruption

- Attacks to disrupt critical information technology (i.e. networks, operating systems, and applications)
- Cyber manipulation or disruption to smart IoT building systems and web-enabled medical devices (MedTech)
- Encryption or destruction to time critical information (schedules, contracts, patient information)

Privacy

- Loss of internal financial data or intellectual property
- Loss of employee personal data (PII, PHI)
- Loss of patients medical records (PHI, PII)

Partners / Clients

- Data breach of patient personal data (PII, PHI) via partner failure
- Disruption of critical systems and services via partner failure
- Manipulation of critical patient care data (i.e. treatment, dietary, etc)

CAYMAN CAPTIVE FORUM 2018

CYBER RISKS FROM VENDORS

Dependencies

Growing technological dependency on vendors maintaining availability and integrity of critical system, services, and devices

Example: Downtime from ransomware to critical services vendors and FDA recall of a range of medical devices (insulin pumps / pacemakers)

Privacy

Increased outsourcing of data storage and processing activities to vendors

Example: 56% of companies suffer data breach via a vendor*

Regulatory

Growing scrutiny of privacy and security performance with greater punitive fines and joint liability between vendor and contracting entity

Example: GDPR fines of 4% of global turnover and joint liability

* Ponemon Institute Data Risk in the Third- Party Ecosystem study

THE NEED FOR A BETTER APPROACH

- **Some 75% of the IT professionals surveyed by the Ponemon Institute acknowledged that the risk of a breach from a third party is serious and increasing.**
- **Same survey indicated that 73% of IT professionals did not believe that a vendor would notify them if they encountered a data breach**

Some other findings:

- 58% are not confident in 3rd parties data safeguards, security policies and procedures
- Accountability is decentralized for managing third party risk - Only 31% rate their vendor risk management program as effective; 38% establish and track metrics of effectiveness
- Heavy reliance on contractual agreements and cyber insurance limits, versus security assessments and audits;
- Very limited visibility into Nth party vendors
- 20% know how information is being accessed or processed by vendors with whom they have no direct relationship, and rely on contractual agreements with direct vendors to monitor and mitigate exposure

ARE WE KEEPING PACE WITH CYBER RISK?

Macros trends and metrics suggests that "cyber risk" is a top-of-mind issue for business leaders but this is not translating into any meaningful action

#4 ranked as a top enterprise risks to Healthcare leaders. #5 according to general industry 1400 business leaders. Up from #9 in 2015, #18 in 2013 (Aon GRMS 2017)

x2.5 more than other sectors and ransomware attacks on critical medical IT has increased +125% since 2010 (Ponemon 2015 research)

+$3bn of cyber related losses to large cap companies associated with the recent ransomware events (Aon Research 2017-18)

+$450bn of cyber related losses occurring globally (Aon analysis of McAfee, FTC, IP Commission, Insurance Information Institute, Lloyd's data)

However…

Only +$3.5bn premium is deployed to protect the balance sheet and only 5% of captives write cyber coverage (Aon Inpoint Analysis 2016-18)

WHAT ISN'T MEASURED…

The biggest challenge for managing Vendor Cyber Risk is to ensure consensus within the Leadership team as to the extent of the challenge. The risk is distributed throughout the organisation. Different functions have divergent approaches and metrics.

Only 38% of Risk Leaders are involved in assessing cyber risk, compared to 86% of Security Leaders.

29% of captive owners use any risk assessment to determine the cyber exposures to be covered

Leadership / Administrators

Focus on technology as an enabler of transformation and business strategy

CISO

Focus on safeguarding the information 'crown jewels'

CHRO

Focused on Human Capital, Employee Vetting, Engagement and Training

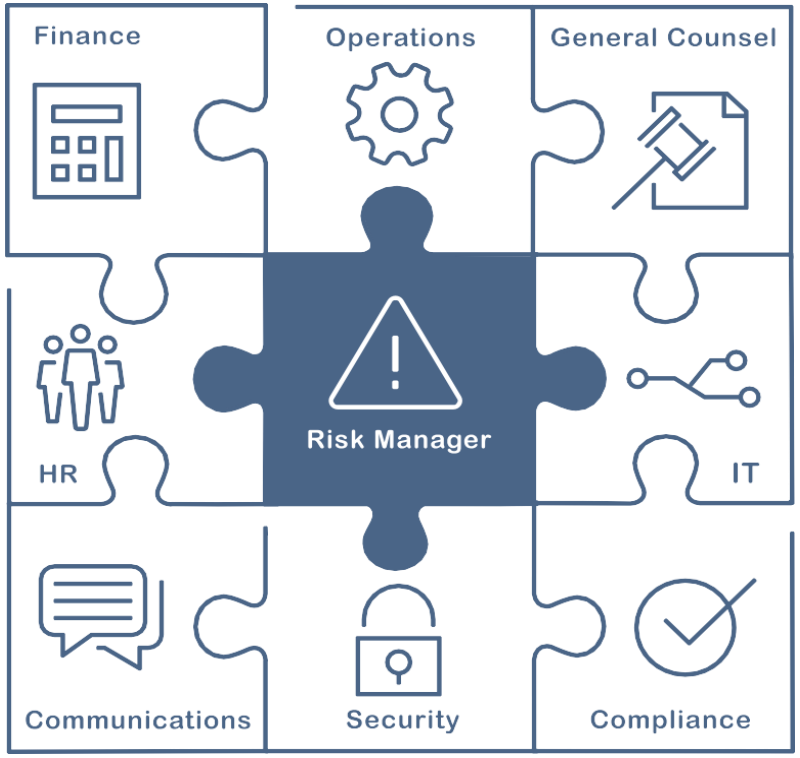
General Counsel

Focus on managing data privacy legal / regulatory position

CLOSING THE GAP

Transforming the Vendor Risk Management Approach to Cyber Risk

TRANSFORMING RISK MANAGEMENT



- Form a Security and Privacy Risk Committee
- Conduct an Enterprise Cyber Assessment of Vendor Risk
- Execute appropriate Risk Management and Financing

RISK DRIVEN STRATEGY

Vendor Risk Management Process

Assess Vendor Exposures

- Identify and map the cyber risks to the operations and technology profile of the parent company
- Employs best practice security and privacy risk frameworks (ISO, NIST, CSC)
- Facilitates establishing minimum security benchmarks for vendors
- Provide baseline underwriting information

Vendor Risk Quantification (VRQ)

- Management tool to support calculations of third party exposure from vendors
- Exposure analytics are based on breach scenarios (PII, PHI, PCI).
- Analytics leverages insights from vendor incidents, claims data, and heuristic analysis.

Design the Strategy

Evaluate the coverage for vendors

Evaluate the viability of captive utilisation and ensure the risk financing strategy reflects the complexity and materiality of the cyber exposures (limits/coverage)

Alignment on Vendor Cyber Risk

Executive Leadership | CTO/CSO/CISO | General Counsel | Risk Officer

MAP RISKS AND EXPOSURES

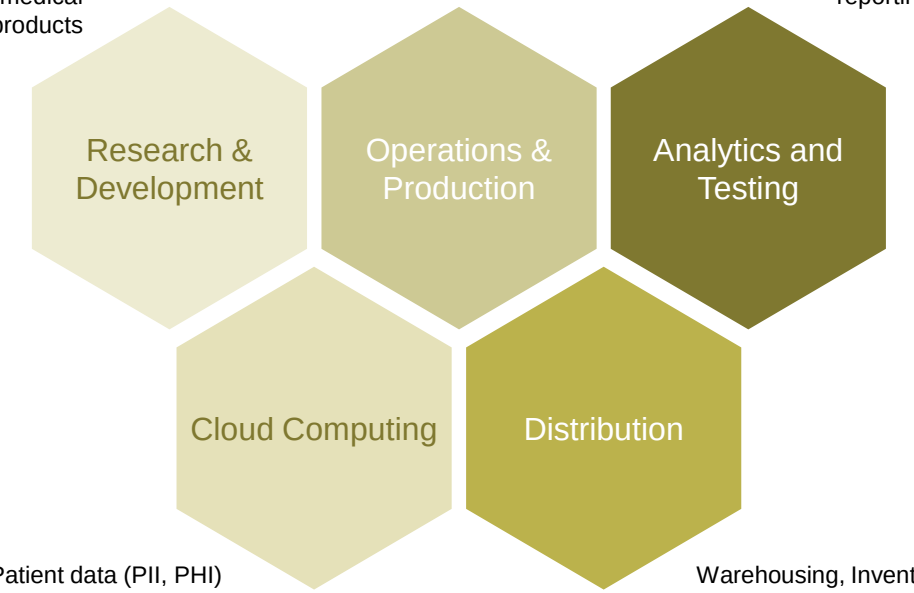
Healthcare Value Chain & Vendor Profile

Building technology, Access Controls, HVAC, Environmental Controls, Quality Control (QC)

Network Infrastructure

R&D data relating to new medical products

Medical testing and reporting (PII, PHI)



Patient data (PII, PHI)

Warehousing, Inventory, and Logistics Systems (ERP)

Vendor Cyber Threats

- Loss of Intellectual Property Commercially Sensitive Data
- Disruption to Production and Supply Chain processes (internal, vendor operations, and critical IT vendors)
- Contamination and sabotage of product integrity
- Disclosure of sensitive data (employees, trial participants, and customers)
- Industry and Data Protection Regulatory fines and actions (i.e. EU GDPR, FDA, HIPAA)

BUILDING A FINANCIAL MODEL

Existing management responses for each cyber event is mapped through the established cost framework

Drivers of Financial Loss:

- Digital forensics (RCA) to determine impact and containment
- IT/OT incident response operations to contain and remediate event
- Crisis communications to clients and public

- Operational business continuity activation
- IT backup and recovery activities and tools

- Net Income Loss associated with disrupted business operations and termination of customer contracts (abnormal churn)

- Legal defence costs from impacted customers

- Local Regulatory fines
- HIPAA (US)
- FDA (US)
- GDPR fines (EU)

- Client injury associated with revenue loss, remediation, and bodily injury (

TRANSLATING INSIGHT TO ACTION

Stress Testing Insurance Strategies

Stress Testing Security Strategies

Improved Financial Resilience to Cyber

Improved Operational Resilience to Cyber

Efficient and consistent approach to monitor contingent cyber exposures and establish cyber insurance requirements for Vendors

CAYMAN CAPTIVE FORUM 2018

BUILDING CYBER RESILIENCE FROM VENDORS

Consensus View on the Financial Exposure from Vendors

Leadership

- Improved Governance / Fiduciary Duty
- More efficient Capital Allocation to Vendor Risk

CISO

- Report technical risks to Leadership in a meaningful way that highlights financial exposures and associated ROSI to unlock additional CAPEX
- Prioritize security assessments, testing, and improvement activities that will have greatest risk reduction

Risk Manager

- Position ‘Cyber’ from Vendors as a ‘Business Risk’
- Make more informed recommendations to Leadership on optimal Risk Financing & Insurance Strategy (i.e. Limits and Coverage)

General Counsel

- Understand financial exposure emanating from Vendors, Data Breaches, Customer Liability, and Regulatory matters that are triggered by a cyber event
- Ensure contract risk management philosophy is appropriate to risk appetite and materiality of exposures

NEXT STEPS

UNLOCKING THE VALUE OF THE CAPTIVE

- **Formalize the an appropriate Decision Committee and define the relevant Process/Decision Making Process**
- **Leverage a common strategic risk management tool**
- **Integration of Cyber Risk into the broader risk financing framework**
  - Captive growth is accelerating +263% to grow to 20% of captives by 2020
  - Only 30% of clients currently utilize the Captive as a strategic risk management measure for Cyber Risk

THANK YOU

Martha Jacobs
martha.jacobs@aon.com

Adam Peckman
adam.peckman@aon.com

www.caymancaptive.ky

CAYMAN CAPTIVE FORUM 2018