CLOSING THE DOOR ON DATA THEFT

Craig Guiliano

18 MAY 2016

TSC ADVANTAGE

Securing the Enterprise

| 962 Wayne Ave | 9th Floor suite 900 | Silver Spring , Maryland 20910 | 202-629-1960

22nd April 2016

USA Risk

Miller Cyber Captive Solutions

Miller Cyber

Introduction

- Miller's experienced cyber-risk specialists have been active in the market since 1997 and are proficient in the design and placement of bespoke solutions.

- The Miller cyber team has strong commercial relationships with an array of insurers in the London market, including Lloyd's largest capacity providers, members of the company market and specialised MGAs.

- At Miller, we understand that cyber threats cannot always be mitigated by risk transfer alone and have therefore established strong relationships with a number of law firms, forensics specialists and other service providers who share our values and ethos.

Miller Cyber

Breadth of Coverage

Cyber

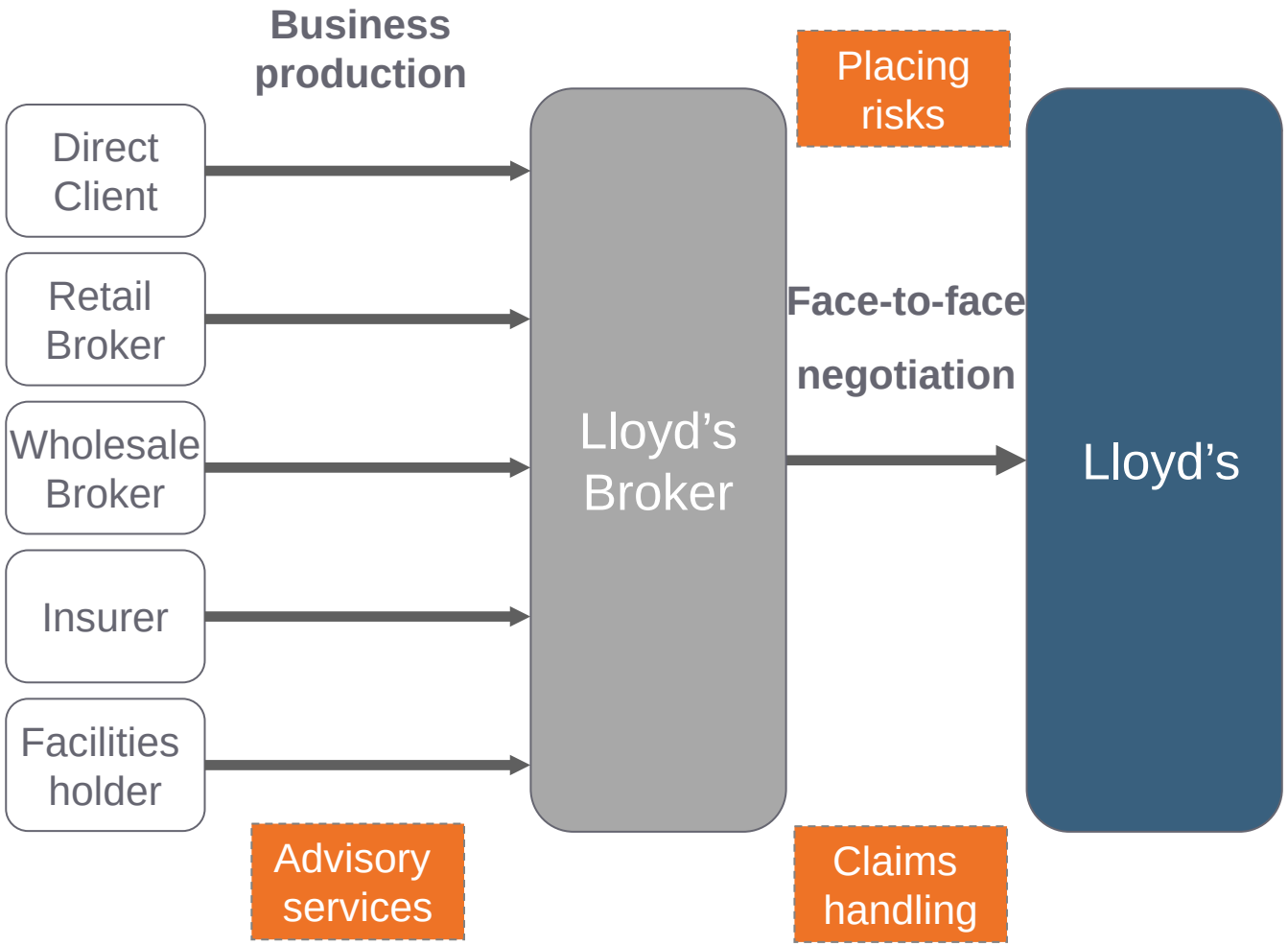
- Privacy Liability / Employee Liability
- Regulatory Defence & Civil Penalties
- Media Liability
- Business Income Loss
- Notification, Credit Monitoring & Crisis Management
- Data Asset Restoration / Forensics
- Cyber Extortion

Technology Liability

- Technology Errors & Omissions
- Financial loss
- Intellectual Property Infringement
- Cyber Perils

The Traditional Route to Market

Option 1



Embedded Beazley Product

Option 2

- A complete privacy breach response management and information security insurance solution tailored to the needs of small businesses.

- Extensive Coverage
  - Information Security and Privacy Liability
  - Regulatory Defence and Penalties
  - Website Media Content Liability
  - PCI Fines and Penalties
  - Cyber Extortion
  - Enhanced First Party Computer Security Coverage

- Privacy Breach Response Services - Forensics, Notification, Legal

- Access to Risk Management Portal

Embedded Beazley Product

Option 2

- Beazley will seek to embed the product fully in to the partner's coverage so that it forms part of their core offering.
- Beazley set limits, rates and retentions based on the exposure that they believe the client's portfolio presents.
- All claims handled by Beazley's dedicated breach response team in Philadelphia, San Francisco or New York.
- Beazley will reinsure the coverage 100% on a quota share basis.

Bespoke Captive Reinsurance

Option 3

- Miller has its own dedicated binding authority backed by Lloyd's underwriters.
- Can accept reinsurance of up to 100% for captives.
- Over the last six months, Miller has been working on the development of a fully integrated incident response service with a number of cyber industry experts. It will provide cyber policy holders with an all-encompassing service that manages the immediate aftermath of a cyber-breach through a fully coordinated suite of service providers.

Miller Cyber team

Nick Fearon

T +44 20 7031 2498
E nick.fearon@miller-insurance.com

Nick joined Miller in 2013. He primarily works with North American brokers and is a specialist producer and broker of professional lines including; professional indemnity, medical malpractice, financial institutions, directors and officers, cyber and technology errors & omissions. Before joining Miller he held the position of Senior Vice-President - Executive Risk at Paragon and before that; Divisional Director - Casualty at RK Harrison.

Tom Quy

T +44 20 7031 2694
E tom.quy@miller-insurance.com

Tom joined Miller in 2013 and begun his insurance career in 2007. He is a producer of cyber, professional indemnity and technology risks, primarily for Fortune 500 multinationals. He previously worked at Paragon International Insurance Brokers Ltd. where he was a vice president of the executive risk team.

Simon Milner

T +44 20 7031 2506
E simon.milner@miller-insurance.com

Simon began his insurance career in 1984. He has specialised in designing and broking cyber and technology risks since 1997 and is recognised to be one of the first in the market to do so. He began his career with Alexander Howden where he became an Associate Director before joining Jardine Lloyd Thompson in 1991 where he was a Partner prior to joining Miller.

Miller Cyber team

Dan Westinghouse

T +44 20 7031 2806
E dan.westinghouse@miller-insurance.com

Dan began his insurance career in 2001 and spent 10 years working for Marsh, some of which was spent in their New York office. He has also spent time working in Hong Kong for Jardine's affiliated companies. Dan is a specialist in North American lawyers', miscellaneous and cyber/privacy liability coverage.

Adam Kleinman

T +44 20 7031 2846
E adam.kleinman@miller-insurance.com

Adam joined Miller in 2013 in a production and broking role. He specialises in US lawyers' professional liability and has underwritten D&O, EPL, LPL, as well as a many other classes of E&O. At Miller, he works on producing lawyers' business. Adam began his career in 1992 and has previously worked for Marsh, AIG and joined Miller from Swiss Re. He has also spent time working in New York, Bermuda and Zurich.

Daniel Leahy

T +44 20 7031 22310
E daniel.leahy@miller-insurance.com

Daniel joined Miller on the graduate Programme in September 2014. Prior to joining he studied Law at Exeter University, with a year abroad studying German and International Business Law at Bucerius Law school in Hamburg. He is fluent in German.

Thank you

miller-insurance.com

“Cyber attacks have become an ever-increasing threat. The F.B.I. now ranks cybercrime as one of its top law enforcement activities, and President Obama’s recently proposed budget would sharply increase spending on cybersecurity to $14 billion”

KEVIN GRANVILLE NY TIMES

TSC ADVANTAGE
Securing the Enterprise

Who We Are

TSC Advantage delivers proactive and holistic defense of trade secrets, intellectual property, and other sensitive information from current and emerging threats to an organization's innovation, execution and reputation.

Data Security
- Network Architecture
- Endpoint protection
- Configuration Management
- Intellectual Asset Identification

Internal Business Operations
- Governance/Strategy
- Cyber Risk Profile
- Incident Response Approach
- Business Continuity, Disaster Recovery Plans

External Business Operations
- Product/Systems Development Lifecycle
- Supply Chain Risk Management
- Procurement/ Contracts

Insider Threat
- Access Control
- Training/Awareness
- Hiring/Firing Practices
- Digital Asset Monitoring

Physical Security
- Defense in Depth
- Visitor Policies and Procedures
- Facilities Security
- Guards, Gates, Guns

Mobility
- Mobile Device Management
- Travel Security Procedures
- Remote Access

Understanding Malicious Threats – the 5 C's of Cyber

Hackers and cyber criminals have a variety of motives for engaging in malicious cyber attacks. Understanding these motives can help understand the risks to your company.

	Description	Example
Convenience	**Attacks against open vulnerabilities**	Company with open ports, unencrypted data
Circumstance	**Threats introduced via business dependencies (partners, suppliers, etc)**	Suppliers with vulnerabilities or are high-value targets
Consequence	**Specific high- target and high-value industries**	Banking, retail, healthcare
Conflict	**Military, political, terrorists, nation-state targets & business competitors**	Critical infrastructure
Conscience	**Social protesters or "hacktivists", motives are cause vs financial gain**	Ashley Madison, VIP/Political targets

Recent Cyber Events:

MedStar

- Insider Threat/EBO
- Ransomware

Primera / Anthem

- Phishing/Malware
- Same Attackers

Sony

- Phishing Attack

Ukrainian Power Company

- Nation-State

Target

- Third-Party Vendor

TSC Cyber Security: Findings and Trends

- There is an upward trend in the resources applied to cyber security programs from 62% (2014) to 86% (2015)

- Only half of the organizations assessed had fully documented crisis communication plans for a breach or a disaster event

- The vast majority of organizations have not identified where their most valuable information assets reside.

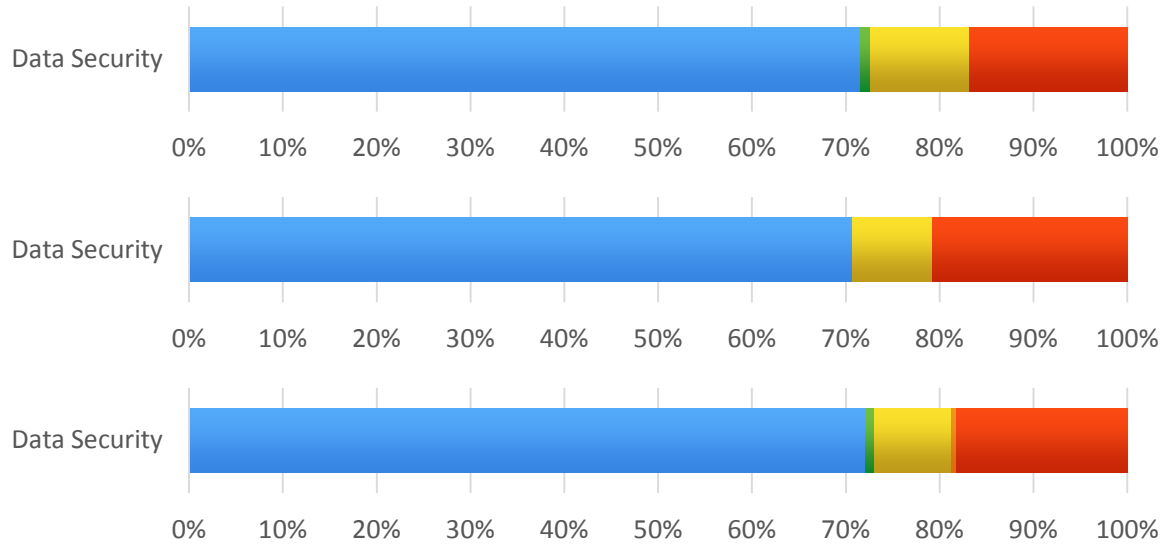
Diminishing Returns

Investments in Data Security VS. Risk Profile

CRP
74.08
out of 100

CRP
52.61
out of 100

AVERAGE



Back to Basics

- **The most basic cyber hygiene controls are not being followed:**
  - Strict Password Management
  - Enforce Least Privilege
  - Multifactor Authentication

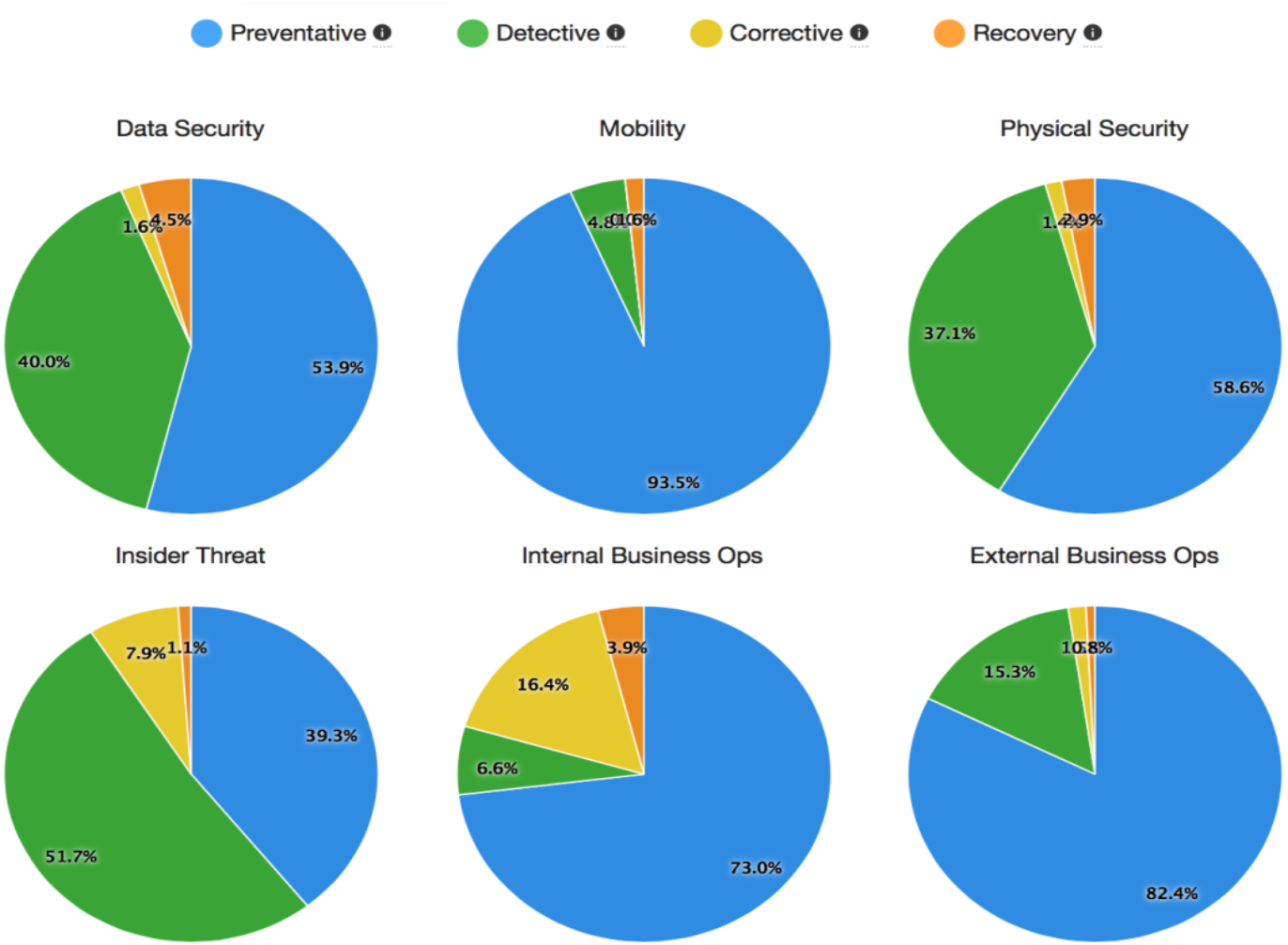
- **Compliance is NOT Security**
  - HIPAA
  - PCI-DSS
  - NERC-CIP

Resiliency

- **Not Just About Preventative Measures – Most Companies Dedicate Their Resources Solely Focused on Prevention**
  - Detect
  - Correct
  - Recover

- **Cyber Security + Cyber Resiliency = Cyber Maturity**
  - Prevent & Detect + Correct & Recover

Resiliency


Preventative
Detective
Corrective
Recovery
Data Security
1.6%
4.5%
40.0%
53.9%
Mobility
93.5%
Physical Security
37.1%
58.6%
Insider Threat
7.9%
1.1%
39.3%
51.7%
Internal Business Ops
3.9%
16.4%
6.6%
73.0%
External Business Ops
15.3%
82.4%

Transfer Risk

- **Understand Your Exposure and Risk**
  - Physical Damage from Cyber
  - Regulatory Regimes & Fines
  - Third Party Exposure
  - Reputation
  - Business Loss

- **Insurance Policies**
  - Know the Limits and Exclusions
  - Based on Industry

QUESTIONS?