ASMGi

Quantifying Cyber Risk: Real or Hocus Pocus?

Presented by ASMGi and TowerStreet

Feb 28, 2019

Today's Webinar
Quantifying Cyber Risk: Real or Hocus Pocus?

- Why is it so important for companies to quantify their cyber risk in dollar terms?
- What are the limitations of the current qualitative measurement methodology?
- What are the benefits of a quantitative measurement and methodology?
- Is quantifying Cyber Risk Real or Hocus Pocus?

ASMGi is …

Global Technology Services and Consulting company focused on **Total Solutions** that provide immediate positive impact to your business

Total Solutions = People + Process + Technology

We deliver IT, Software and Cyber Security solutions from our headquarters in Cleveland, OH by helping our customers Plan, Manage and Execute:

- *Strong programs as a foundation to meet compliance requirements as well as foster best practices across the enterprise*
- *Best-in-Class platforms and tools to drive value thru adoption and shorter time to value*
- *A security eco-system model to ensure tools work together*
- *Achieve Results:*
  - ONEteam "XaaS" capabilities to ensure you maximize adoption – *Benefits without the Burden*!
  - "Fill the gap" approach to leverage your existing resources and complement/ supplement where needed
  - Action = Results -> Orchestrated Action = Great Results!

Over 400 CISOs polled ….

- More than half fear for their jobs as cyber-attacks threaten their organizations
- More than half feel they don't have adequate budget or resources to deal with growing threat landscape
- All are working long hours
- 60% believe their CEOs agree a breach is inevitable
- More than half believe a lack of resources is holding back an effective security posture
- 65% believe lack of senior buy-in to the problem is a barrier

Current State of Risk-Based security

- Everything is a risk, so how do you prioritize?
- Constant flow of new technology / rate of change increasing
- CISO and practitioners are overwhelmed and often can't get staff or budget to accomplish their goals
- Fragmented Approach / Point Solutions = Over spending + under adopting = no ROI = wasted $

What if there was a better way to orchestrate your resources?

Quantifying Cyber Risk

- Move Security “closer” to the business
- Change the discussion with the business
- Stop Guessing! Prioritize roadmap by “financial impact”
- Align security budgets with financial outcomes

Managing Risk is a 3-Step Process

1. Identify / Assess/ Rate risks
2. Leverage a platform to track and prioritize risks
3. Remediate, Accept or Transfer risks

Today we will focus on ASSESS RISKS, and touch on the other areas

Quantifying Cyber Risk: Real or Hocus Pocus?

I am excited about today's webinar!

- We've been trying to make IT/Security more "proactive" and less "reactive" for decades – we need to tie **Risk to Dollars** for this to happen
- Most wouldn't argue the challenges, so how do you actually **change the game**?
- Our goal is to help you succeed – how can we best position you to move closer to the business, have more meaningful discussions and get what you need to drive the results the business wants?

Tower Street

Quantifying Cyber Risk – Real or Hocus Pocus?

Steve Roesing, CEO ASMGi
Jeffrey Sirr, President Tower Street
Webinar February 28th, 2019

The Cyber Risk **Management Conundrum**

Challenges:

→ Current risk assessments are qualitative

→ Credibility challenge on cyber budget requirements and application

→ CEO and Board usually don't have in-depth understanding of cyber

→ Inability to assimilate into organization's enterprise risk management (ERM)

Resulting in:

→ Difficulty in determining balance sheet impact

→ Arduous discussions for CISO when substantiating needs

→ CISO role not widely accepted as a strategic function

→ Exclusion of critical risk from enterprise wide risk integration management

At the Center of the Cyber Risk Management Conundrum
is the Lack of CISO, CFO & CEO Synchronicity

Risk Assessment with Financial Quantification

NEXT LEVEL OF CYBER RISK MATURITY

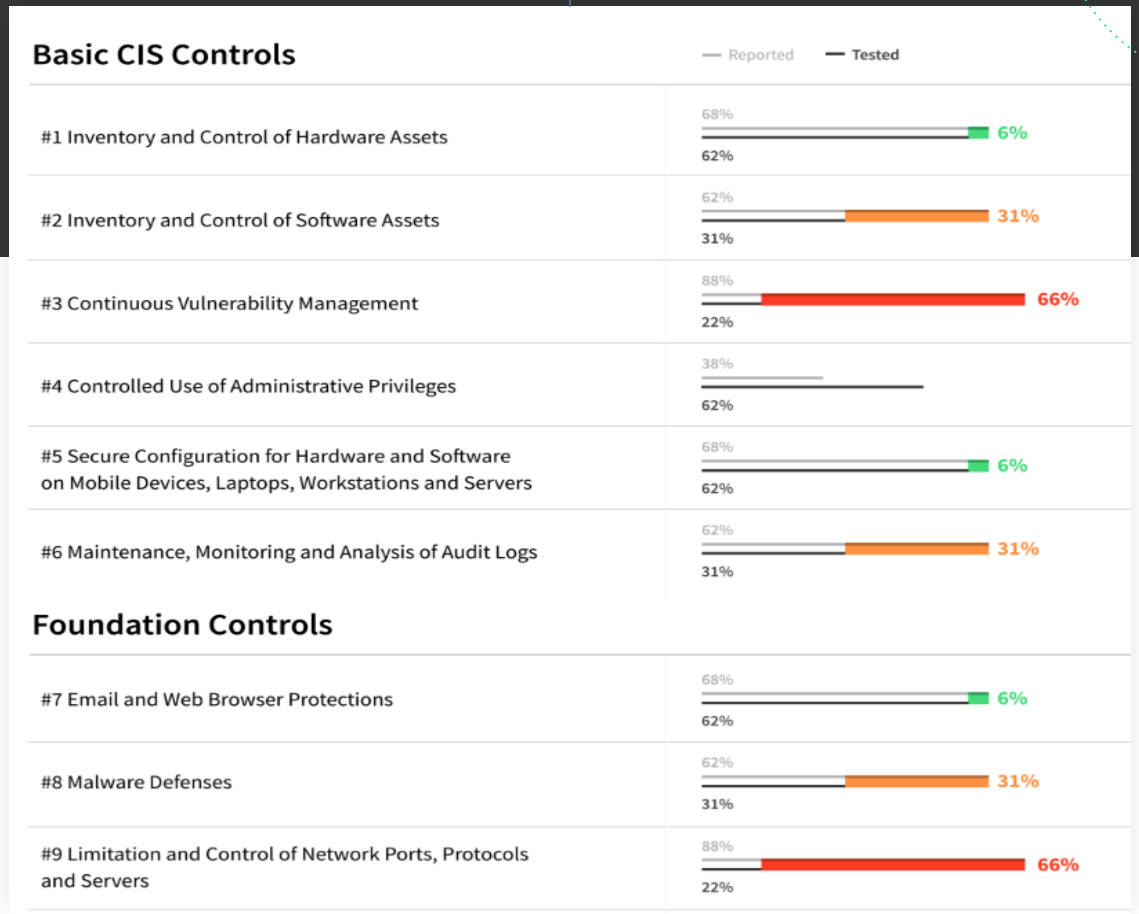
Risk Assessment

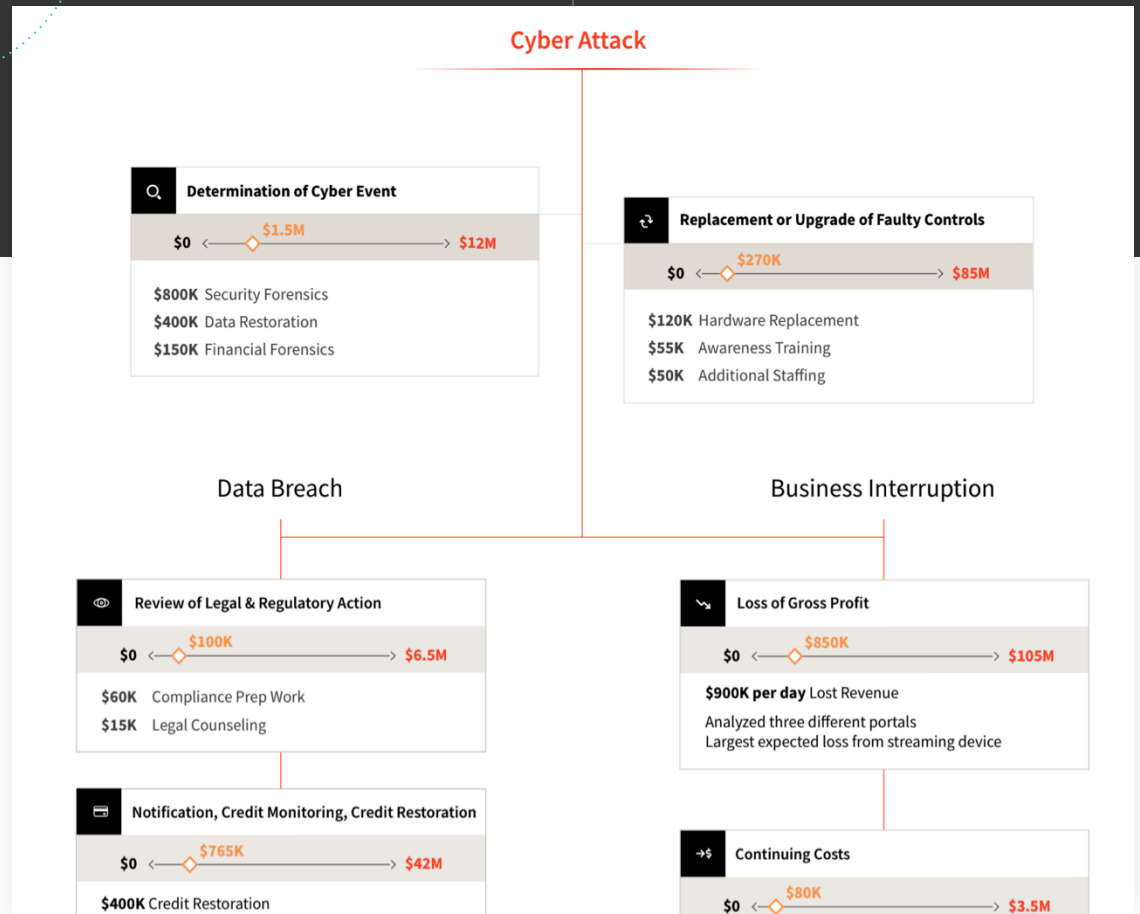
CIS Controls Help Facilitate CFO / CEO Discussion

Upgrade The Story by Financials

Financial Quantification

Bridges to CFO/CEO/CRO/Legal





The Benefits of **Quantification**

Internal:

→ Enhances CISO and CFO / CEO dialogue and understanding

→ Financial measurement of balance sheet impact

→ Financial accuracy and substantiation of cyber budget requirements and application

→ Assimilation of cyber risk into enterprise risk management (ERM)

→ Acceptance of CISO role as a strategic function

External:

→ Enables CEO to present tangible assessment of cyber risk to stakeholders

→ Enhances financing prospects

→ Strengthening of company's position with External constituents (e.g. regulators, etc.)

→ M&A and other growth strategy advantages

→ Enables superior risk solutions (insurance; capital markets; security tech channel sales)

At the Center is CISO, CFO & CEO **Synchronicity**

How is it **done?**

Cyber Risk Analysis

→ Breakdown of main risk drivers: Data Theft; Malicious Attack; DDoS; Human Error

→ Insurance grade level model for every risk driver; modeling frequency & severity of loss events.

→ Final loss distribution obtained using internal Monte Carlo simulation framework

→ **3 main data inputs:**
(i) historical breach database;
(ii) panel of SMEs to account for missing historical security data
(iii) security & loss assessment data

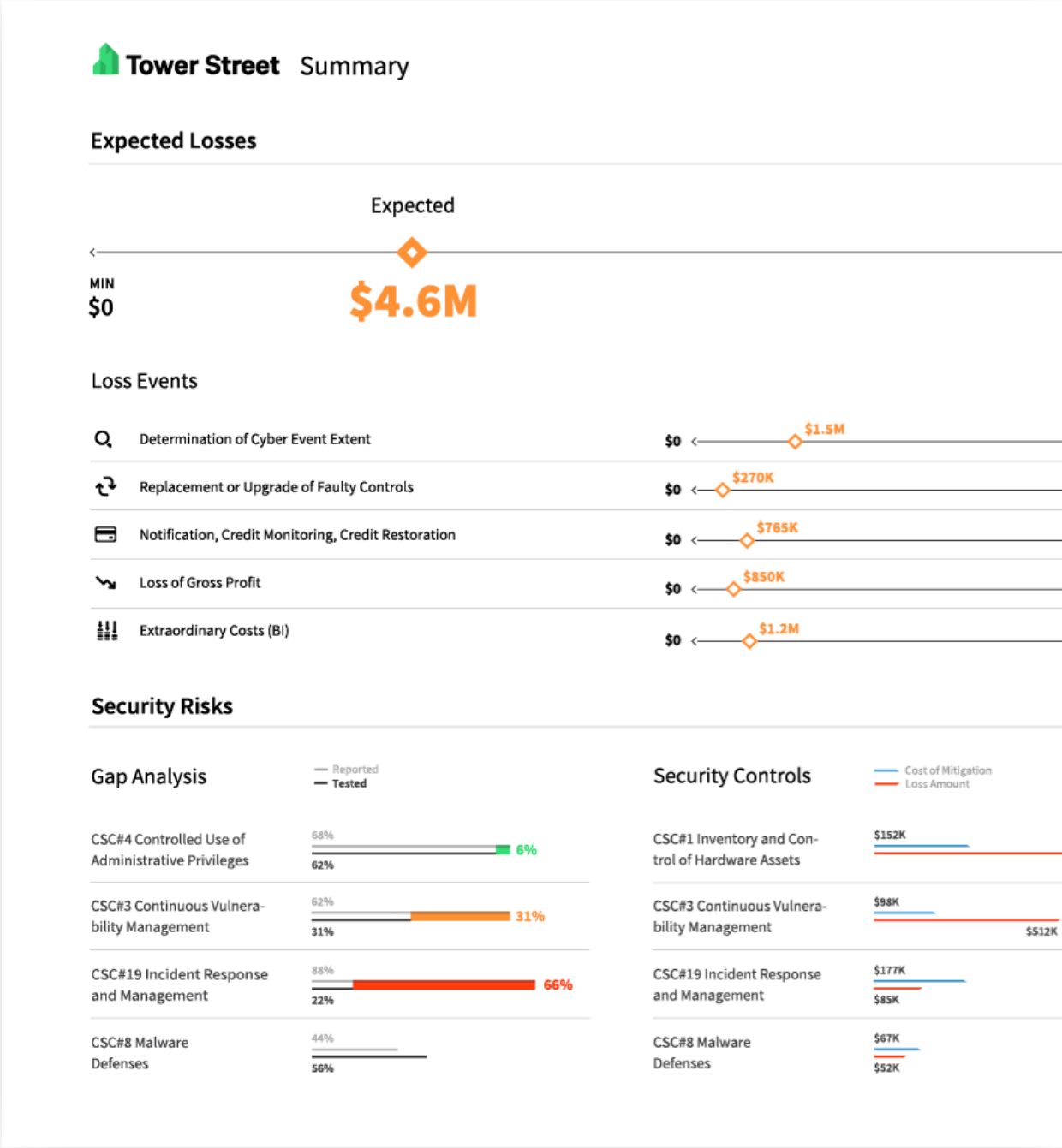
Cyber Risk Assessment

3 MAIN COMPONENTS:

→ Controls based inside-out security assessment; critical assets identification & mapping to critical business outcomes

→ Real-life security controls evaluation & testing to produce gap analysis

→ Customized mitigation recommendation to obtain



How is it **done?**

Cyber Risk Analysis

→ Breakdown of main risk drivers: Da
DDoS; Human Error

→ Insurance grade level model for eve
frequency & severity of loss events.

→ Final loss distribution obtained usin
Monte Carlo simulation framework

→ **3 main data inputs:**
(i) historical breach database;
(ii) panel of SMEs to account for mis
(iii) security & loss assessment data

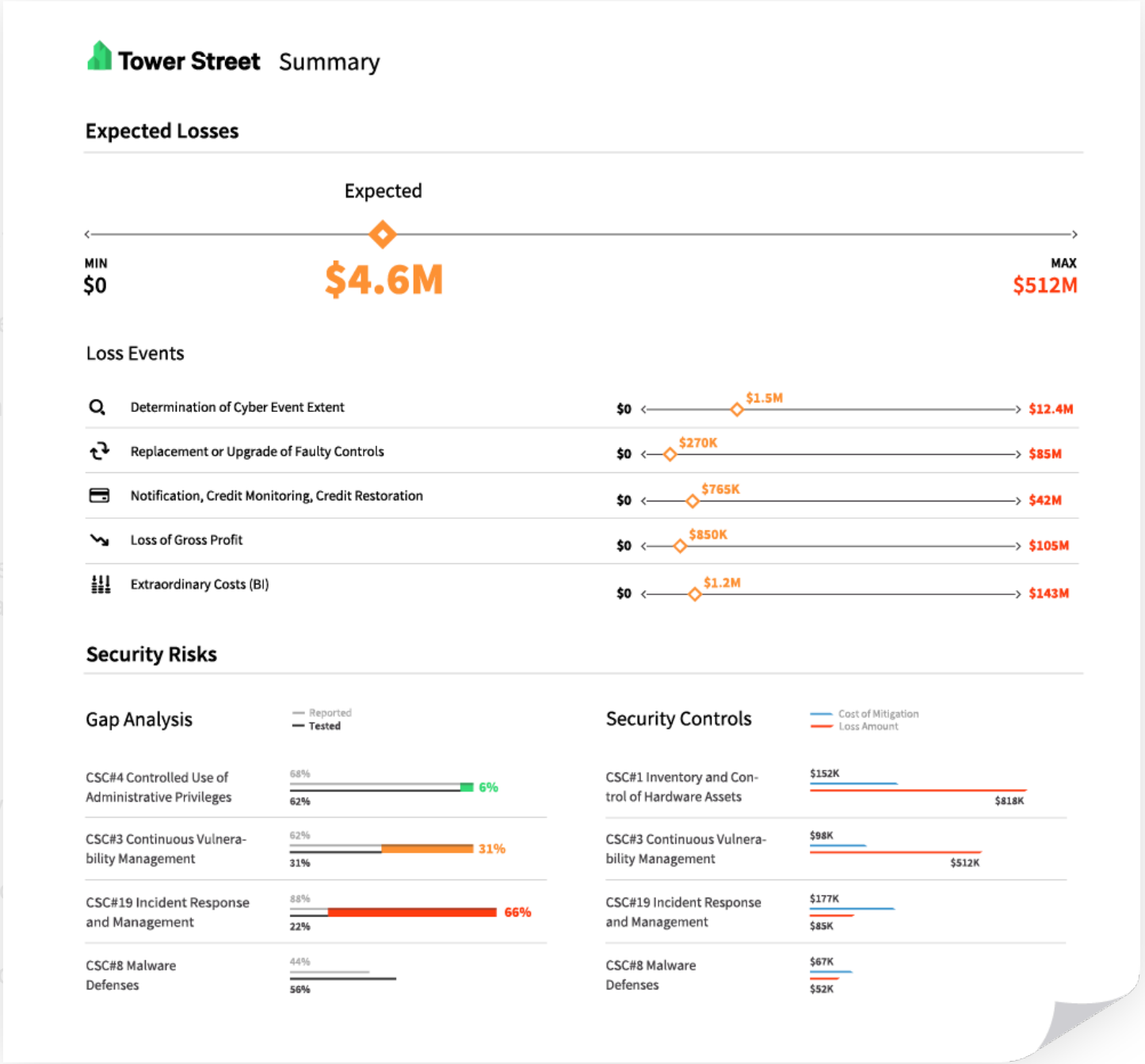
Cyber Risk Assessment

3 MAIN COMPONENTS:

→ Controls based inside-out security
identification & mapping to critical

→ Real-life security controls evaluati
to produce gap analysis

→ Customized mitigation recommen
maximum risk reduction.



What's **next?**

- **Meet** Tower Street & ASMGi in San Francisco at RSA March 4-8
- **Join** Tower Street, ASMGi and their cybersecurity network for drinks at RSA on March 7 (RSVP at towerstreet.co/rsadrinks)
- **Download** → Tower Street whitepapers on Loss Graph
  https://www.towerstreet.co/campaigns/ts-asmgi-loss-graph-wp/
  → Why Corporates are Targets in a Global Cyber Arms Race
  https://www.towerstreet.co/campaigns/standing-in-the-crossfire/
- **Follow** Tower Street (@towerstreetHQ) and ASMGi (@ASMGi_CLE) to get the latest updates
- **Contact** Tower Street (Jeffrey Sirr, jeffrey.sirr@towerstreet.co) & ASMGi (Steve Roesing, sroesing@asmgi.com) with any questions or inquiries

About Tower Street

Tower Street is a full stack cyber risk solution bridging the gap between the CISO/ CIO technical view of security risk, and the board's financial view. Quantifying cyber risk exposure in financial terms helps key decision-makers to uplevel their dialogue and drive risk management decisions around security budgets and protect their most important financial metrics.

Our multi-tiered security framework allows to select a level of assessment that matches client's current needs - from a **light half-day security assessment** to **a continuous assessment and monitoring.**

Tower Street is able to provide the most trusted risk insights by leveraging deep industry and company specific financial and security models, built on top of **the richest breach dataset in the world.**

QUESTIONS?

Next in our Cyber Webinar Series

Future-Ready Threat Detection & Response

Presented by ASMGi and Rapid7, on Thursday March 7, 1PM ET

What we will cover:

- How Security Analytics and SIEM have evolved, along with key buying criteria
- How Security Analytics and SIEM have evolved, along with key buying criteria
- Managed Detection and Response: Are vendors meeting their bold claims?
- Processes: What are surprising time sucks, and what's ripe for automation?
- Future Investments: Is it Security Automation & Orchestration, or something else?

Visit www.asmgi.com Resources page to sign up

ASMGi

Thank You

800 Superior Ave E, Ste 1050
Cleveland, OH 44114

Phone: 216.255.3040
Fax: 216.274.9647

Email: info@asmgi.com

www.asmgi.com