

Acquiring Risk: Information Security Due Diligence

Andrew McDonnell, VP–Security Solutions,
AsTech Consulting, Inc.

Professional Techniques – T24



Trust in, and value from, information systems

San Francisco Chapter

The CyberSizelT logo is set against a background illustration of the San Francisco skyline, including the Golden Gate Bridge and various skyscrapers. The word "CyberSizelT" is written in a large, stylized font where the letters are interconnected. The "C" and "S" are significantly larger than the other letters. The text is colored in a gradient from dark red to light red, with a white outline.

“AN AMERICA ONLINE FILM”: MERGERS AND ACQUISITIONS



Trust in, and value from, information systems

San Francisco Chapter

The background of the slide features a stylized illustration of the San Francisco skyline, including the Golden Gate Bridge and various skyscrapers, rendered in shades of yellow, orange, and black. Overlaid on this illustration is the text "CyberSizeIT" in a large, bold, red font with a white outline. The "C" is significantly larger than the other letters.

CyberSizeIT

How Does This Work?

1. Identification of interest
2. Assessment of worth
 - a. Obligations
 - b. Liabilities
 - c. Litigation
 - d. Infringement
 - e. Contracts
 - f. ...

How Does This Work?

1. I like you
2. Are you good for me?

How Does This Work? Sometimes Badly



CAVEAT EMPTOR: HOW WE GOT INTO THIS BUSINESS



Trust in, and value from, information systems

San Francisco Chapter

A stylized graphic of the San Francisco skyline, including the Golden Gate Bridge and various skyscrapers, rendered in a dark silhouette against a light background.

CyberSizelT

Story Time

1. Customer Identifies Target
2. Standard Due Diligence
3. Purchase
4. Security Review
5. Regret

WAS \$970M THE RIGHT PRICE?



Trust in, and value from, information systems

San Francisco Chapter

The background of the bottom section is a stylized illustration of the San Francisco skyline, featuring the Golden Gate Bridge and various skyscrapers. The text "CyberSizeIT" is overlaid on this illustration in a large, bold, red font with a white outline. The "C" and "I" are significantly larger than the other letters.

CyberSizeIT

Heard of this one?

2007 – Justin.tv launched

2011 – Gaming spun off as Twitch.tv

2013 – 43M monthly viewers, profitable

2014 – Acquired by Amazon for \$970M

2015 – User credentials, payment info(?) hacked

HEADLINE INSURANCE: APPROACHES TO MEASURE RISK



Trust in, and value from, information systems

San Francisco Chapter

The CyberSizeIT logo is set against a background illustration of the San Francisco skyline, including the Golden Gate Bridge and various skyscrapers. The text "CyberSizeIT" is rendered in a large, bold, red font with a white outline. The "C" is significantly larger than the other letters, and the "y" is lowercase. The "I" and "T" are also large and bold.

CyberSizeIT

Return On Security Investment

- Software Assessment
 - Quickly evaluate security liabilities
 - Quantifiable liability impact
- Infrastructure Assessment
 - Data exposure
 - Risk assessment maturity
- Salable Context For Traditional Assessments

EVERYONE IS IN THE SOFTWARE BUSINESS



Trust in, and value from, information systems

San Francisco Chapter

The background of the bottom section is a stylized illustration of the San Francisco skyline, featuring the Golden Gate Bridge and various skyscrapers in silhouette against a warm, yellowish-orange sky. The text "CyberSizeIT" is overlaid on this background in a large, bold, red font with a white outline. The "C" is significantly larger than the other letters, and the "y" is lowercase. The "S" is also large, and the "I" is a simple vertical bar. The "T" is also large and has a horizontal bar.

Quantifying Software Liabilities

- Find vulnerabilities and flaws
- Evaluate code complexity
- Determine costs
- Contextualize within risk tolerance

Identify Security Flaws

- Static analysis
- Code review

Web Applications

- Dynamic analysis
- Penetration testing

Establish Code Complexity

- Development maturity
- Application model
- User roles
- Transaction depth
- Interface type(s)
- Sensitive data handling
- Dependent architecture

Estimate Costs

- Difficulty to fix
 - Flaw types
 - Code complexity
- Developer familiarity
- Volume of flaws
- Market delays

Adjust Risk Thresholds

- Cost-benefit curves
- Target identification
- Price adjustment

Contextual Static Analysis

- Automated assessment
- Results validation
- Code disposition
- Risk ranking
- Liability projection

SETEC ASTRONOMY: WHAT DATA LOSS WILL COST



Trust in, and value from, information systems

San Francisco Chapter

A silhouette of the San Francisco skyline is shown against a light, hazy background. The Golden Gate Bridge is the most prominent feature on the left, with its towers and suspension cables. Other buildings and bridges are visible in the background.

CyberSizeIT

IT Infrastructure Liability

- Establish data flows
- Map infrastructure zones
- “Data balance sheet”
- Apply to value model

Data Flows

- Data classification
- Least privilege
- Retention necessity
- Unintentional accumulation

Zone Defense

- Asset classification
- Role segmentation
 - Ingress
 - Egress
 - Reuse
 - Recovery
- Encryption / storage protection

Profit and Loss

- Parameterize data value
- Relate to breach cost
- Assess breach likelihood
- Contextualize breach in assets and liabilities

Example

- SaaS platform
- 500k subscribers
- Average subscription \$60/year
- Breach cost averages \$150/record
- Lax data protection => 2.5 lost years
- Assign weight and apply to liabilities

Return of the Return On Security Investment

- Software Assessment
- Infrastructure Assessment
- Salable Context For Traditional Assessments

- Value For Buyers *and* Sellers

Thank You

Andrew McDonnell

andrew@astechconsulting.com

510.270.5551

astechconsulting.com