Acquiring Risk:
Information Security Due Diligence

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

Professional Techniques – T24

ISACA®

Trust in, and value from, information systems

San Francisco Chapter

SF ISACA FALL CONFERENCE NOVEMBER 9-11, 2015 HOTEL NIKKO-SAN FRANCISCO

"AN AMERICA ONLINE FILM": MERGERS AND ACQUISITIONS

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

WARNER BROS. PICTURES
An AOL Time Warner Company

CAVEAT EMPTOR:
HOW WE GOT INTO THIS BUSINESS

Story Time

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

WAS $970M THE RIGHT PRICE?

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

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

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

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