Quantifying Technology Risk in Dollars and Cents

Richard Van Horn
Founder, Technology@Risk Working Group

1 My Background

2 Benefits of Quantifying Technology Risk

3 Determining Inherent Value

My Background: From Control To Risk

- As an IT Auditor:
  - Provided Independent Testing and Opinions on the Effectiveness of IT Controls
- In Information Security:
  - Provided Critical & Enabling Security Services
- In IT Risk:
  - Qualitative & Quantitative Assessments of Risk Related to IT Services

CISA® Certified Information Systems Auditor®
An ISACA® Certification

CRISC™ Certified in Risk and Information Systems Control™
An ISACA® Certification

The views expressed are my own and do not reflect those of my current or prior employers.

FEDERAL RESERVE BANK OF BOSTON™

Goldman Sachs

DTCC Securing Today. Shaping Tomorrow.®

JPMorganChase

Glossary of Terms

Audit

- An inspection of an organization's controls, typically by an independent body. Results are typically shared with a committee that has oversight responsibilities for the organization.

Compliance

- Processes and procedures to ensure legal, regulatory and corporate mandates are met. This is typically performed by a department of subject matter experts.

Information Security – Cyber Security

- The ongoing administration, operational processes and technical controls that protect the firm's IT assets and related business services.

Technology Risk

- Tools and analysis to assess the potential business impact of technology related issues and ongoing governance to determine the firm's appetite for those events.

Benefits of Quantifying Technology Risk

- Managing Technology Involves Multiple Drivers:
  - Functionality, Cost Benefit, Staff Skill Sets.
- IT Risk is an Additional Component:
  - For Analysis, Planning.
- Quantifying IT Risk Provides Many Benefits:
  - Proactive Risk Management rather than Reactive.
  - Prioritization of Projects Based on Cost & Risk Benefit.
  - Valuation of Security Tools Based on their Cost & Risk Benefit.

Data Breaches - We Know Them So Well

If you have a credit report, there's a good chance that you're one of the 143 million American consumers whose sensitive personal information was exposed in a data breach at Equifax, one of the nation's three major credit reporting agencies.

Here are the facts, according to Equifax. The breach lasted from mid-May through July. The hackers accessed people's names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers. They also stole credit card numbers for about 209,000 people and dispute documents with personal identifying information for about 182,000 people. And they grabbed personal information of people in the UK and Canada too.

The IT Risk Trifecta – July 8th, 2015

THE WALL STREET JOURNAL.
WSJ

CNN Money Business Markets Tech Media Personal Finance Small Biz Luxury stock tickers

Wall Street Journal hit with tech woes

NYSE

MARKETS

Glitch Freezes NYSE Trading for Hours

Technical issues had forced exchange to halt trading

Technical glitch disrupts United flights nationwide

Ben Mutzabaugh, Bart Jansen, Trevor Hughes, USA TODAY 10:24 p.m. EDT July 8, 2015

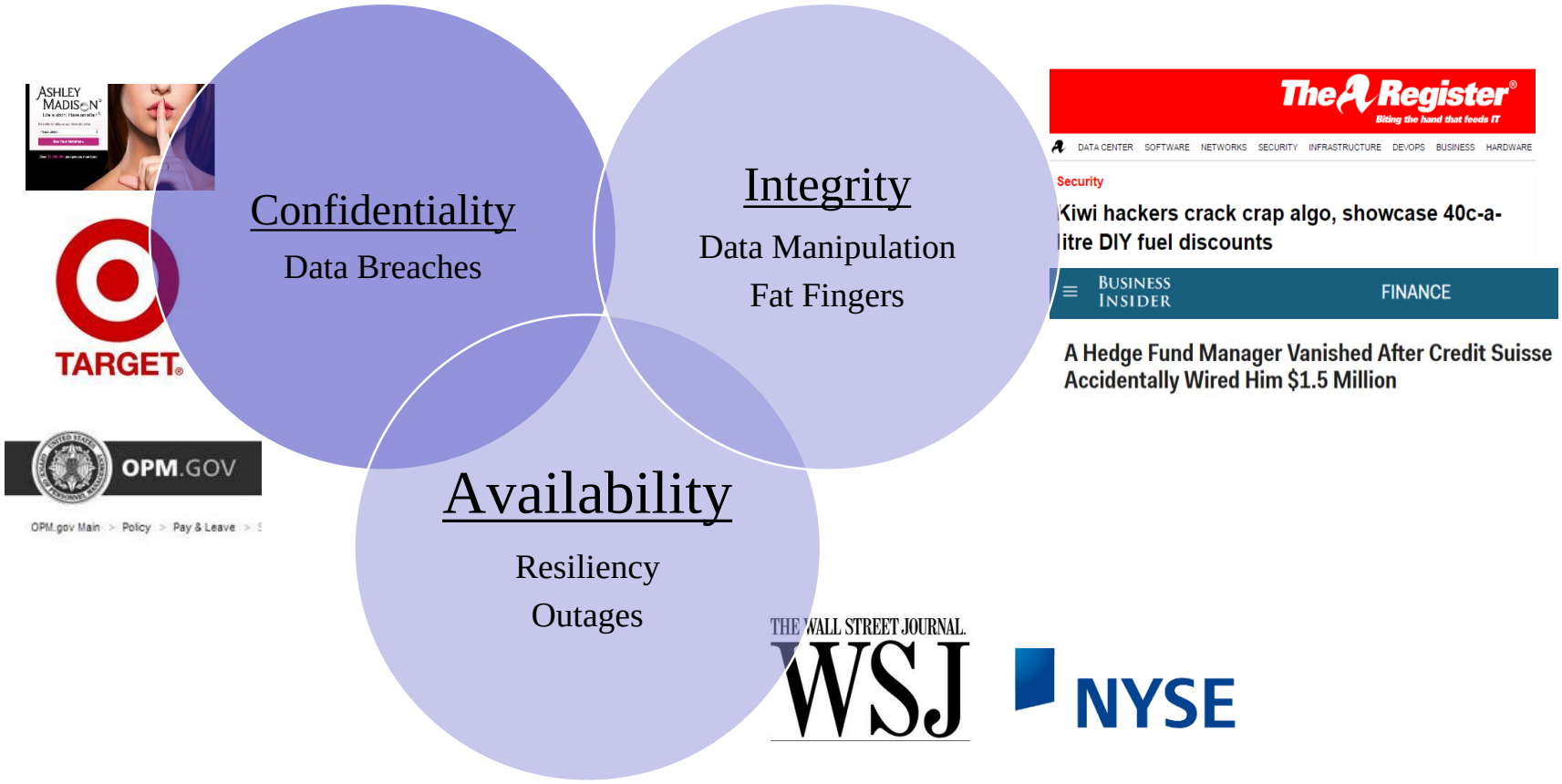
The Catastrophic Example - Knight Capital

Not a Hack or a Data Breach

- Internal Governance Oversight:
  - Core Business Malfunction.
  - Out of Business in a Week.
- Fundamentally an SDLC Issue:
  - Poor Testing.
  - Poor Change Control.

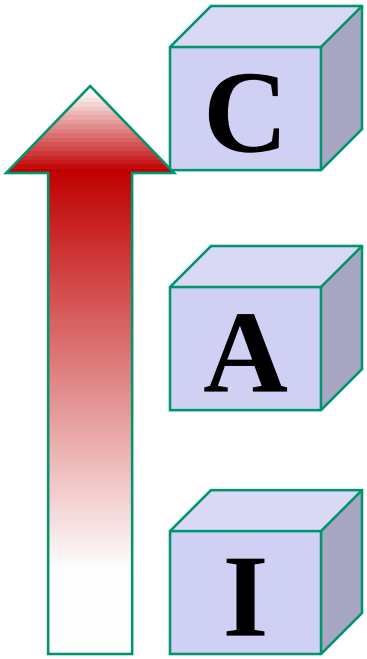
The **Knight Capital Group** was an American global financial services firm engaging in market making, electronic execution, and institutional sales and trading. With its high-frequency trading algorithms Knight was the largest trader in U.S. equities, with a market share of 17.3% on NYSE and 16.9% on NASDAQ. The company agreed to be acquired in December 2012 after an August 2012 trading error lost $460 million. The merger was completed in July 2013, forming KCG Holdings.

First Step – Determining Inherent Value



IT Events Categorized by Type

Impact by CIA: Payroll as an Example

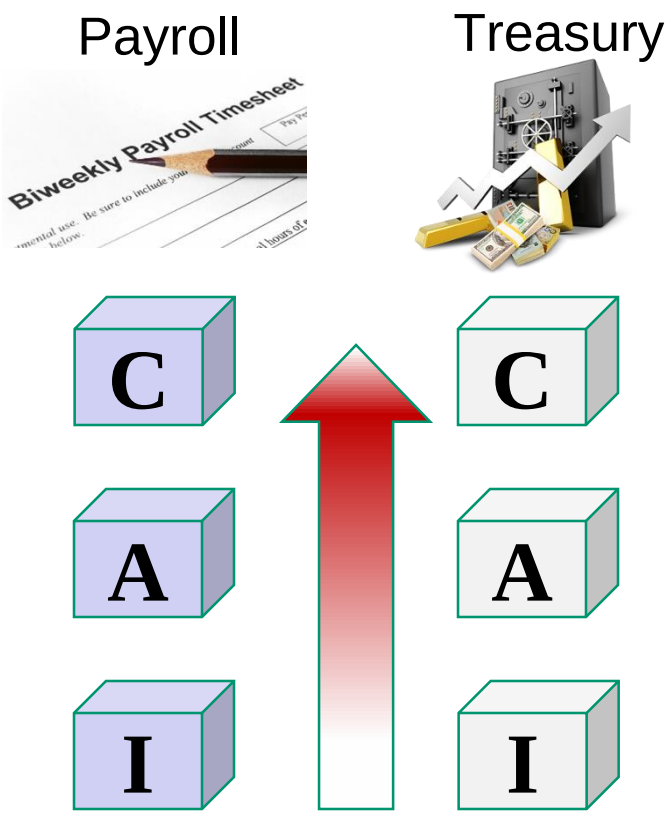


Depending on the volume of records and the data included, this could have significant regulatory impact and direct costs.

Employees that live paycheck to paycheck would be greatly impacted. Though impact would vary based on timeframe.

Paying someone the wrong amount is an issue, but ACH rules allow for recall and re-issuing payments is manageable.

Impact by CIA: A Comparison



Disclosure of commercial partnerships or payments is not regulated. Much lower impact that PII.

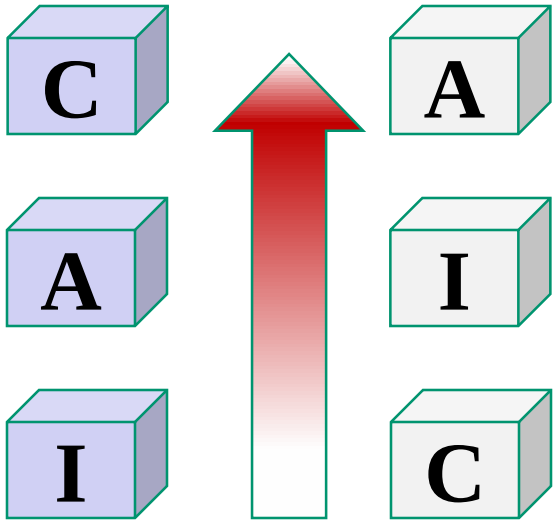
A delay in payments could be catastrophic to the firm in terms of bond covenants, bank loans, etc.

Depending on the amount, a significant a risk especially since EFT's are not easily reversed.

Impact by CIA: A Comparison

Payroll

Treasury

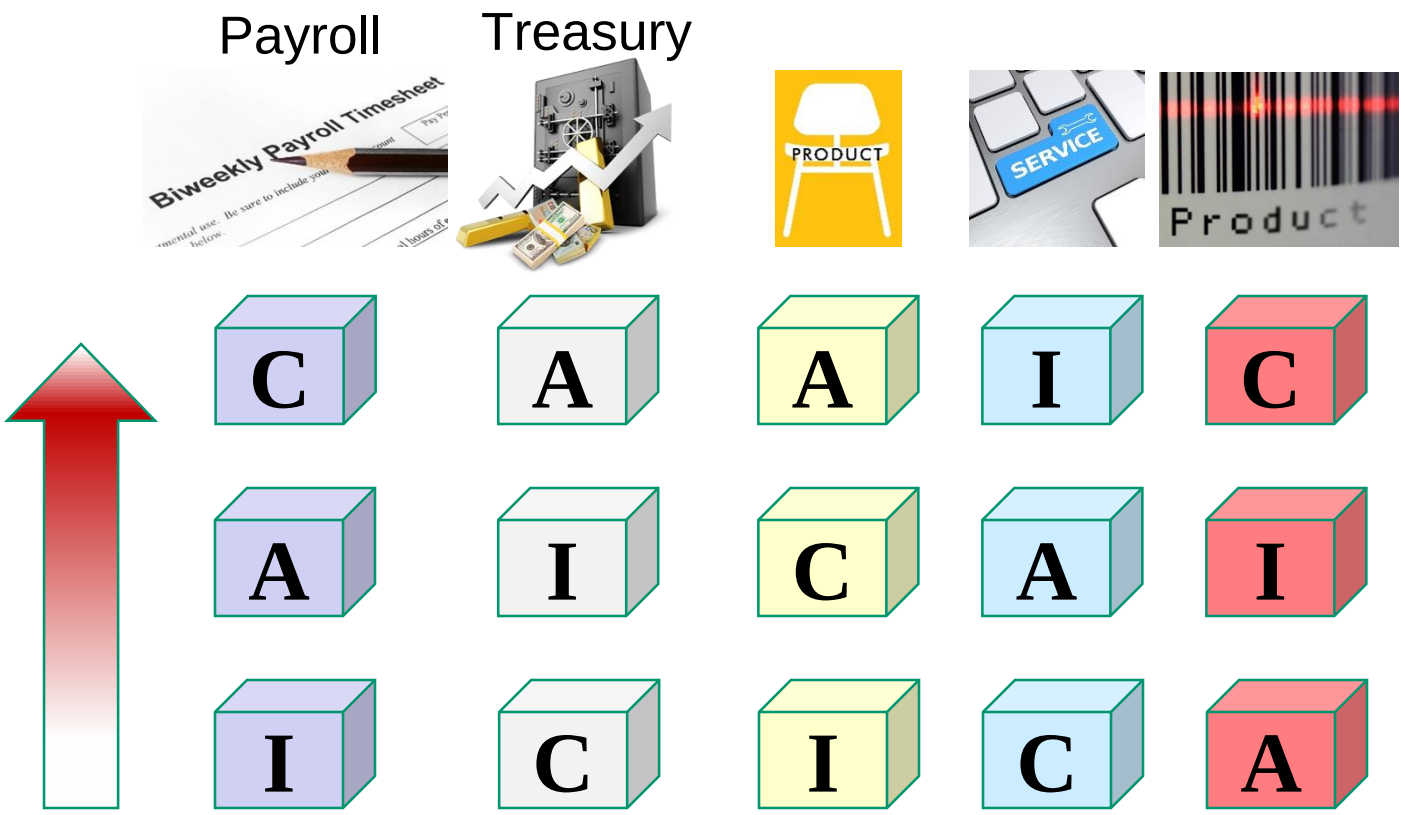


A delay in payments could be catastrophic to the firm in terms of bond covenants, bank loans, etc.

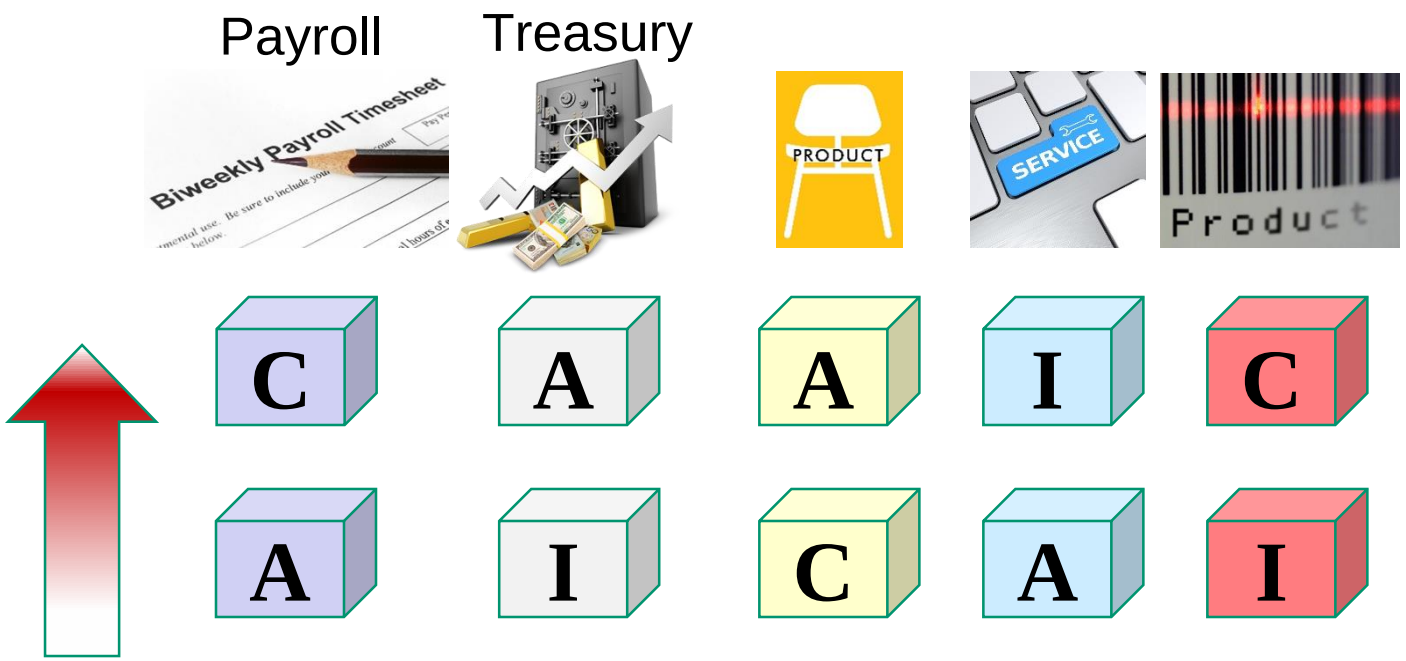
Depending on the amount, a significant risk especially since EFT's are not easily reversed.

Disclosure of commercial partnerships or payments is not regulated. Much lower impact that PII.

Impact by CIA: All Products & Services

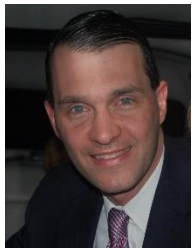


Totals of All Products & Services



Totals by Business Function	$$	$$$$	$$$	$	$$

Questions & Follow-Ups



Richard Van Horn, CRISC

Richard has been in the world of IT Governance, Risk & Control over 20 years, and is currently a Vice President at JP Morgan Chase. His career has evolved along with the field, from working as an IT Auditor at the Federal Reserve Bank of Boston, to implementing enterprise security solutions at Fidelity Investments, to managing IT Risk at Goldman Sachs, the CIT Group, DTCC and JP Morgan Chase. He is certified as a Certified Information Systems Auditor (CISA - Expired) and Certified Risk and Information Systems Control (CRISC) from the Information Systems Audit and Control Association (ISACA).

Richard Van Horn

C: 201-738-6104

Email: rvanhorn@technologyatrisk.info