Technology Risk Management: Determining Inherent Value

January 9th, 2018

Richard J. Van Horn

rvanhorn@technologyatrisk.info

https://www.linkedin.com/in/rvanhorn

http://www.technologyatrisk.info

Table of Contents

Editors & Reviewers

Executive Summary

It has become clear that modern industry's reliance on information technology comes with many benefits: automation, accelerated time to market, scale and efficiencies to name a few. However, it is also clear that relying on information technology so extensively has risks. Hacker attacks, data breaches, service outages and other issues continue to occur across industries and in increasing numbers. That growth is in spite of the expanding regulatory and industry requirements that firms are expected to comply with to secure their technology environments. Legislatures and regulators continue to add obligations that firms must comply with to ensure client data is protected and services are readily available. However, in spite of these obligations, costly outages and data breaches continue to occur. In some cases, those events can be catastrophic to the company. (See Appendix A)

These expensive outages and data breaches portend the need for better ways to manage technology. One way, proposed in this white paper, is to govern technology based on the 'risk' that technology presents to the firm. Fundamentally, the higher the 'risk' a technology asset or related service presents to the firm, the more controls and oversight may be required. In theory, those additional controls and oversight should decrease the likelihood of an event or at a minimum, decrease its impact. This 'risk' based view of technology - where controls and oversight are driven by the potential economic cost of an outage or other technology issue - can be a complement to other facets of technology management, including return on investment, strategic direction, business requirements and regulatory obligations. Given the history of losses due to technology outages and breaches - which happen in spite of regulatory obligations - managing technology based on 'risk' or possible economic impact seems to be a logical next step.

It should be clear the primary driver of a 'risk' based approach to managing technology is the inherent economic value of the firm's IT assets and services. Of course this value goes far beyond the direct cost of the assets. Value is inherited from the business services those IT assets supports. After all the regulatory requirements, industry requirements and best practices have been used to 'secure' technology assets - which should be considered a baseline of security and controls - the organization should focus on its most valuable technology assets. Those assets are considered valuable based on the business services those assets support. The corollary being the 'risk' to the firm is the cost if those services are unavailable or there is a data loss or other issue. This

increased focus on the firm's most valuable technology assets should decrease the likelihood of outages or other events or at least minimize their economic impact.

Scope, Scale and Inherent Value

As explained in an earlier white paper, proper management of technology related risks has to include all services that touch technology assets (the scope of technology risk management) and be able to show business impact in economic terms (to indicate the possible scale of impact).

An extension of the discussion around impact and scale is how to determine the economic impact of a possible event. This white paper proposes the economic value of any IT related event is directly related to the economic value of the business services the IT asset or service supports. The greater the economic impact of an outage or other technology event, the higher the 'risk' of that IT asset. That economic value is not based on the price paid for the IT asset, but the value of the business services they support: the more valuable a business service, the controls and oversight may be necessary. Higher 'risk' technology assets or services may warrant more focus and possibly more controls than lower 'risk' assets. Given there is only so much time and money to protect a firm's technology environment, prioritizing focus and controls on the firm's most valuable assets is logical. Business value is the only way to assess the dollar impact of a server having an outage or other issues. It is also the best way to show scale of an outage or data beach; showing impact in economic terms inherently includes scale.

The economic value of IT assets or services is determined by the economic value of the business services they support. With that inherent value in mind, additional controls beyond the baseline of best practice or regulatory controls can be implemented to protect those valuable assets: higher value technology assets and services may warrant more stringent controls than lower value IT assets.

While this point may seem entirely intuitive, it does not always seem to be the case. Let's use a simple example: updating vulnerable software. Software 'patching' is a well established process widely performed at most organizations. Typically, a patch is typically prioritized as high, medium, low or critical. That rating indicates the priority of that patch for deployment when compared to other patches: this is done as an industry best practice using agreed upon scoring mechanisms and data sharing tools. However,

once a patch is prioritized for deployment, there is no standard methodology to prioritize that patch across the dozens or hundreds of assets that need to be updated within an organization. Prioritization may be performed if the IT assets are Internet facing, or known to support high value business services. But this is typically not uniform and only focused on extremely sensitive or high value targets. One way to prioritize that deployment would be the economic value of the servers to the organization: high value servers would be patched first. Other services would be patched in order based on decreasing value to the firm.

For example, given 2 servers, one used by the Payroll Department and the other used by the Treasury Department, the Treasury Department server is significantly higher value to the firm. That is due to both the higher value of the dollars Treasury processes when compared to Payroll, and the criticality of the function to the firm. An outage of Treasury has broader implications and impact than an outage of Payroll. As a result, all processes and activities that support the Treasury server have a higher value than the same services that support the Payroll server.

This is very important because it changes the view of technology services. Generally speaking, technology is managed as a layer, where similar assets are treated uniformly in the same way. Going back to the vulnerability example, when vulnerabilities are identified, the vulnerability itself is prioritized for deployment across that horizontal layer. Historically, there has been no way to prioritize that specific deployment vertically based on the business services an asset supports. All servers were treated relatively the same and the patch would be applied at generally the same time. This additional view says the patch should be deployed based on the economic value of the servers to be patched. Or, the economic impact if they are not patched and that vulnerability is exploited. This view prioritizes IT assets based on the business service they support and the value of those business services.

Determining the economic value of an IT asset based on the value of the business services it supports is the focus on this white paper.

Inherent Value Versus Inherent Risk

When discussing technology risk management with colleagues in other risk disciplines, there have been debates around the definition of inherent risk and its applicability to

managing technology. Inherent risk within financial risk models typically includes the probability of an event over a time horizon with specific economic impact. That definition is difficult to apply to information technology and technology risk. That is why this paper has put 'risk' in quotes when discussing technology events. For the purposes of this discussion, the definition of technology risk is slightly different than financial risk. For one, determining the probability of an event is a significant challenge due to a lack of data and the inability to correlate that available data to an organization's control environment. While an event might be public, the data necessary to determine the probability of that exact event happening to another firm is not typically available. In addition, determining a time horizon for an event is equally challenging, also due to a lack of correlatable data. Finally, determining the probability of an event does not accommodate one time 'black swan' type events that, even if they happen just once, may be the beginning of the end for the impacted firm. The one time black swan event at the Knight Capital Group is a prime example. (Appendix A).

Given the challenges with determining the time horizon and probability of technology related events, this white paper will not define 'technology risk' with the same attributes of financial risk: probability and time horizon. Rather, 'technology risk' will focus exclusively on the inherent economic value of IT asset and services.

Future white papers will comment on probability and time horizon.

'CIA' as Scenarios

In the field of Information Security, it is generally known that there are three types of scenarios that can impact technology assets and services.

- Loss of Confidentiality - data breaches and other losses are examples of lost confidentiality.
- Loss of Integrity - this can be a loss of data integrity or service integrity. The Knight Capital Group is an example of a service integrity issue.
- Loss of Availability - many examples exist when a business service is just not working.

This concept of CIA is well known and adequately identifies scenarios for technology related issues: data can be lost or corrupted, services can be corrupted or unavailable.

It should be noted that CIA addresses the three scenarios that can result from a technology event, it does NOT address the many diverse vectors that can cause an issue. Vector analysis and related impact will be discussed in a future white paper.

This white paper proposes that separating impact by CIA is the first step to determining the possible economic impact of an event.

For example, going back to the Payroll / Treasury comparison, the impact of a data breach or service outage are drastically different for those 2 services. A loss of confidentiality of Payroll data is a well understood event. Unfortunately data breaches of personally identifiable data occur quite frequently. The Ponemon Institute is a primary source of the economic cost of those breaches, which can be up to $125 per record. Now, compare that potential economic impact to a data breach of Treasury data. Treasury data consists of business information: name, address, wire transfer routing information. While sensitive and should not be disclosed, there is no regulatory requirement to protect that data. As a result, the direct cost of a data breach of Treasury data is minimal.

Now compare the two services from a reliability perspective. If Payroll has a service outage and employees are not paid on time, there is impact to the employees - they may be late to pay bills and generally be dissatisfied with the fact they were not paid on time. However, it is expected they will be eventually be paid and will continue to go to work. Generally speaking , there is little to no economic impact to the firm if it does not pay its employees on time. Now contrast that to an outage of Treasury services. Depending on the day of the month or time of year, a service outage of Treasury presents a significant risk to an organization. Depending on a few factors, it may be an existential risk that impacts the long term viability of the organization.

These examples highlight how the economic impact of a technology event, is dependent on the type of event. The type of event, whether a data breach (C), integrity issue (I) or service outage (A) can significantly change the economic impact of that event to an organization. Viewing business services in light of CIA is an important first step to assessing inherent value of the underlying technology assets that support those business services.

Types of Financial Loss

The next component to determining the economic impact of technology events is the type of financial loss that can be incurred. Below is a list of loss types with a brief explanation:

- Regulatory Fines
    - Regulators can impose one time fines for data breaches, service outages, etc. These costs are typically related to the number of records lost or the length of the outage.

- Lost Revenue
    - Obviously a service outage can have direct impact on revenue, both during the time of the outage and possibly long term as clients may chose to take their business elsewhere.

- Contractual Losses and Liabilities
    - Contracts may include liability clauses that are invoked in the event of lost business due to data breaches, service outages or other issues.

- Immediate Clean Up Costs
    - Depending on the event, the cost of clean can be insignificant or substantial.

- Long Term Organizational Costs
    - In some cases, regulators may require firms to establish additional audit and oversight requirements, which would be a long term, ongoing, additional cost to the firm.

Excluded from this list are the impact on a public company's stock price. Stock market fluctuations were excluded as they have been generally shown to be temporary and more related to long term revenue prospects than the cost of the breach or other event. In addition, stock fluctuations typically do not directly impact an organization's long term viability. They reflect the organization's long term viability but are not typically a direct contributor to that viability, unless the stock price is extremely low. A technology issue

can directly impact an organization's long term viability. This paper is focused on direct financial impact and so stock fluctuations are excluded from this analysis.

Determining Inherent Value

Given a business service, this white paper proposes 2 sets of criteria to determine the inherent value of IT assets that support that business service:

- The type of event that can occur:
  - A data breach (C)
  - Data or software integrity issue (I)
  - Service outage (A)

- The type of loss that could be incurred:
  - Lost revenue
  - Regulatory fines
  - Contractual obligations
  - Immediate Clean Up Costs
  - Additional governance and oversight obligations

These criteria can be mapped to an organization's business services to determine the value of those services, which can then be applied to the underlying IT assets that support them. For simplicity, the chart below highlights a few of these services.

The cost of additional governance and oversight obligations is not listed in the chart, as that is expected to be the same independent of the type of technology event that might occur. All other events have costs related to the specific event:

#	Client Services	Confidentiality	Integrity	Availability
1	E-Commerce Service	○ Lost revenue ○ Regulatory fines ○ Contractual	○ Lost revenue ○ Regulatory fines ○ Contractual	○ Lost revenue ○ Regulatory fines ○ Contractual

		Obligations ○ Cost of Clean Up	Obligations ○ Cost of Clean Up	Obligations ○ Cost of Clean Up
2	Logistics System			
3				
#	**Employee Services**	**Confidentiality**	**Integrity**	**Availability**
1	Payroll			
2	Human Resources			
3				
#	**Corporate Services**	**Confidentiality**	**Integrity**	**Availability**
1	Treasury			
2				
3				
#	**Shared IT Services***	**Confidentiality**	**Integrity**	**Availability**
1	Networking			
2	Active Directory			
3				

* It should be noted that shared services aggregate the value of the business services they support. If a network router supports 5 different client services, than the economic value of that router to the firm is the aggregate of these 5 services.

This basic structure provides a framework for determining the inherent value of technology assets based on the business services they support. However, there is still a significant amount of work to do. Determining the inherent value of technology assets and services based on the business services they support - even an indicative value - requires in depth analysis of factors unique to that business service. For example, there are multiple data types where a breach would have different economic impacts, including Materially Non Public Information (MNPI), Personally Identifiable Information (PII), medical information related to the Health Information Portability and Accountability Act (HIPAA), intellectual property, etc. Each needs more research to model the cost of

a data breach. This is an initial proposed approach to begin that analysis. More detailed models will be proposed to assess the value of specific business services within this framework.

On a 'positive' note, the number of technology events that have occurred over the past 10 years provide an initial set of data points to help complete this model, including the outages of various airline services, payment services, etc. These events can be used to populate the data and provide a model for others to rely on. Unfortunately, future events will be added as appropriate. Addendums to this white paper will use various scenarios to model the inherent value of technology assets based on the business services they support.

Conclusion

Over the past 25 years, information technology has become the lifeblood of almost every organization in the developed world. Information technology and services - managed directly by an organization or indirectly via a service provider - are indispensable when providing services to clients, partners and employees. However, the benefits of Information Technology can be overshadowed by issues - including breaches of data, service outages and other events.

To minimize those issues or their impact, regulators and industry bodies have issued control requirements for organizations to follow. Those obligations have become a baseline to protect data and ensure services are reliable. However, data breaches and outages continue to occur in spite of those regulatory obligations. With that in mind, those controls should be considered a baseline. Depending on several factors, additional controls may be necessary to minimize technology issues or their impact.

One of those factors should be the inherent value of the technology assets. That value should not be based on the assets direct cost, but based on the business services they support. Properly valuing technology assets based on the business services they support would allow additional focus and governance based on the value of the assets. Additional controls would complement the baselines of controls requirement by regulators and be commensurate with the potential negative impact of technology issues. This white paper proposes a high level framework to assess that inherent value. Additional addendums will further detail specific ways to determine economic inherent value. In the eyes of many, this new view of technology assets allows for complementary controls to minimize the economic impact of technology issues beyond reacting to events they occur

Appendix A: A Compelling Example

The purpose of this white paper was to highlight the scope of Technology Risk Management - what should fall under its purview - and that dollars and cents is the best scale to show the possible economic impact of technology events.

Unfortunately, there is an example - a poster child company - that shows the value of managing all technology processes that might impact high value services (scope) and that 'high' cannot convey true impact (scale).

Knight Capital Group

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[1].

In a widely known event - called a glitch[2] by the press, which again is the simplistic adjective used to describe these types of technology issues - one of the firm's proprietary trading algorithms executed a series of orders over a matter of minutes rather than days, resulting in a loss of $460 million dollars and driving the firm into a merger that ended it's independence.

While the details have been discussed in many other publications[3] [4], the results of the event have made Knight Capital Group the poster child of technology risk management: a single technology related event - in this case an existential event for the firm - literally bankrupted the company in 30 minutes.

Wikipedia has the best summary of the technical details that led to the trading losses:

2012 stock trading disruption

> On August 1, 2012, Knight Capital deployed untested software to a production environment which contained an obsolete function. The incident happened due to a technician forgetting to copy the new Retail Liquidity Program (RLP) code to

[1] https://en.wikipedia.org/wiki/Knight_Capital_Group
[2] http://dealbook.nytimes.com/2012/08/02/knight-capital-says-trading-mishap-cost-it-440-million/?_r=0
[3] http://money.cnn.com/2012/08/09/technology/knight-expensive-computer-bug/
[4] https://www.bloomberg.com/news/articles/2012-08-02/knight-shows-how-to-lose-440-million-in-30-minutes

> one of the eight SMARS computer servers, which was Knight's automated routing system for equity orders. RLP code repurposed a flag that was formerly used to activate the old function known as 'Power Peg'. Power Peg was designed to move stock prices higher and lower in order to verify the behavior of trading algorithms in a controlled environment. Therefore, orders sent with the repurposed flag to the eighth server triggered the defective Power Peg code still present on that server. When released into production, Knight's trading activities caused a major disruption in the prices of 148 companies listed at the New York Stock Exchange, thus, for example, shares of Wizzard Software Corporation went from $3.50 to $14.76. For the 212 incoming parent orders that were processed by the defective Power Peg code, Knight Capital sent millions of child orders, resulting in 4 million executions in 154 stocks for more than 397 million shares in approximately 45 minutes.

This event is significant from a Technology Risk Management perspective for two reasons. For one, this was NOT an attack by a nation state or 'hackers' that normally makes headlines - other wise known as a Cyber attack and typically managed by the Cyber Security department. Rather, this was the result of a breakdown in well known, relatively mundane technology processes: quality assurance testing and change control. Those processes are well known components of the Software Development Life Cycle. Again, SDLC is not typically part of a Cyber Security program. However, in this example, given the potential impact on high risk services, it would be part of a Technology Risk Management program.

The second reason is that the cost of this event has been quantified in dollars and cents: $440 to $460 million dollars depending on the source. As discussed earlier, qualitative measures of risk cannot convey this magnitude of loss: 'high does not begin to indicate the size of this economic impact. To repeat, this is not a hypothetical 'what if' scenario but an actual technology related breakdown that lead to significant dollar losses, the firm losing its independence and merging with another company only days later.

Appendix B: Sources of Loss Data

This is a very short list of outages or other technology related events that can be used as data points to determine the economic impact of similar future events. This list does not include data breaches, as the Ponemen Institute focuses on that type of event. It is also not meant to be comprehensive:

CIA plot led to huge blast in Siberian gas pipeline

1982 (Published in 2004): A CIA operation to sabotage Soviet industry by duping Moscow into stealing booby-trapped software was spectacularly successful when it triggered a huge explosion in a Siberian gas pipeline, it emerged yesterday. Mr Reed writes that the software "was programmed to reset pump speeds and valve settings to produce pressures far beyond those acceptable to pipeline joints and welds".

Australian Wastewater Attack

October 2001: An Australian man was today sent to prison for two years after he was found guilty of hacking into the Maroochy Shire, Queensland computerised waste management system and caused millions of litres of raw sewage to spill out into local parks, rivers and even the grounds of a Hyatt Regency hotel.

Ohio Nuclear Power Plant

September 2003: The Slammer worm penetrated a private computer network at Ohio's Davis-Besse nuclear power plant in January and disabled a safety monitoring system for nearly five hours, despite a belief by plant personnel that the network was protected by a firewall.

Poland Train Station Attack

January, 2008: A Polish teenager allegedly turned the tram system in the city of Lodz into his own personal train set, triggering chaos and derailing four vehicles in the process. Twelve people were injured in one of the incidents.

SAN FRANCISCO ADMIN CHARGED WITH HIJACKING CITY'S NETWORK

July, 2007: A California judge on Tuesday continued the $5 million bail for a San Francisco city worker accused of hijacking the city's computer system, and ordered the network administrator to enter a plea on Thursday. Terry Childs, 43, is accused of locking out the city from its FiberWAN network containing city e-mails, payroll, police records, information on jail inmates – it was virtually an all access pass to City Hall. He was arrested Sunday after refusing to hand over passwords to the Wide Area Network system he is accused of taking control of illegally.

Sony Playstation Attack

April, 2011: The 2011 PlayStation Network outage was the result of an "external intrusion" on Sony's PlayStation Network and Qriocity services, in which personal details from approximately 77 million accounts were compromised and prevented users of PlayStation 3 and PlayStation Portable consoles from accessing the service. On May 4 Sony confirmed that personally identifiable information from each of the 77 million accounts had been exposed. The outage lasted 23 days.

Sony Pictures Attack

November 24, 2014: A hacker group which identified itself by the name "Guardians of Peace" (GOP) leaked a release of confidential data from the film studio Sony Pictures. The data included personal information about Sony Pictures employees and their families, e-mails between employees, information about executive salaries at the company, copies of then-unreleased Sony films, and other information. The perpetrators then employed a variant of the Shamoon wiper malware to erase Sony's computer infrastructure.

German Steel Plant

December 2014: Details of the incident emerged in the annual report of the German Federal Office for Information Security (BSI). It said attackers used booby-trapped emails to steal logins that gave them access to the mill's control systems. This led to parts of the plant failing and meant a blast furnace could not be shut down as normal.

The IT Risk Trifecta - July 8, 2015:

United Airlines: Flights were grounded for almost two hours early Wednesday due to a computer hardware problem, creating travel headaches for tens of thousands of passengers that stretched into the afternoon.

Wall Street Journal: The homepage for the digital site of the Wall Street Journal experienced technical difficulties on Wednesday. The technical glitch came at almost the same that the New York Stock Exchange halted trading due to its own "technical issue," which was a major story for the news outlet. At approximately 11:45 a.m. on Wednesday the homepage for WSJ.com presented an error page that read "oops, 504! Something did not respond fast enough, that's all we know..." Soon after the homepage returned, but with a temporary homepage design. At the top of the temporary page it read, "WSJ.com is having technical difficulties. The full site will return shortly."

NYSE: A faulty software upgrade to part of the machine at the center of trading at the New York Stock Exchange was the culprit behind a nearly four-hour outage Wednesday, exchange officials said Thursday.

Bank of New York

September 15, 2015: At the height of the market volatility on Aug. 24, executives at Bank of New York Mellon Corp. got the news they wanted to hear: A glitch affecting the system that keeps more than a thousand mutual funds running was likely to be fixed soon. BNY Mellon relayed the news to some clients.

Delta Airlines

January 2017: Delta Air Lines domestic planes were taking to the skies again early Monday but a nationwide ground stop due to a "systems outage" caused departure delays and at least 150 cancellations overnight, the airline said.

RushCard

February, 2017: RushCard, the debit card company founded by hip-hop mogul Russell Simmons, is being fined and forced to pay millions in restitution to customers that were affected by a 2015 outage that cut users off from their money.

Yahoo!!!

February 2017: Everyone knows corporate data breaches can be expensive, but does anyone really know exactly how expensive? Recent estimates for the average cost have landed all over the map, ranging from $4 million to $7 million. But when it comes to the top end of the scale, those appraisals turn out to be laughably small.

British Airways Outage

June, 2017: A power outage at British Airways that disrupted tens of thousands of people's travel plans last weekend plunging hubs Heathrow and Gatwick into chaos, was reportedly caused by a staff blunder.

About the Author

Richard Van Horn

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 now JP Morgan Chase. He was certified as a Certified Information Systems Auditor (CISA) and is currently as a Certified Risk and Information Systems Control (CRISC) from the Information Systems Audit and Control Association (ISACA). Richard resides in New Jersey and has three children.