Journal of Information Technology Education: Discussion Cases

10/14/2016

MANISH AGRAWAL, SHIVENDU SHIVENDU

CYBER INSURANCE AT USF[1]

I really think we should have some form of cybersecurity insurance.

Alex Campoe, Director for Information Security at the University of South Florida, had just come out from a meeting with the CIO of the University, and this thought summed up the CIO's opinion. While Alex had heard of the term cyber insurance, this was the first time he had actually been compelled to think seriously about it. Until now, he had not considered the possibility that he might actually negotiate the terms of such a policy. There had not been any significant cyber incident at USF, and by all accounts, the IT team at USF did a fine job. Besides, he had always assumed that as a state institution, he had the backing of the State of Florida in case a severe cyber-incident were to affect USF. So, the possibility that the leadership at USF might seriously consider paying for a cyber insurance policy had not occurred to him until his CIO actually brought it up that morning.

To be clear, Alex's CIO had not pushed him into deciding in favor of going ahead with a cyber insurance policy. He had only been asked to consider the utility of such a policy for the institution. Alex was confident that he enjoyed his CIO's trust, so that his recommendations would be taken very seriously. And though this was a new domain for him, Alex wanted to make sure he had considered all relevant issues before making his recommendation. First, there was the issue of what exactly was a cyber insurance policy. What did it cover? What did it leave out? What obligations did it place on him as the Director of Information Security at USF? Second, was the issue of the costs of such a policy. Even if cyber insurance was useful, would it still be worth the costs? There were many buildings on campus running hardware that was purchased over 30 years ago, which had not been supported by their manufacturers for over 10 years. Upgrades to such obsolete equipment were being put off year after year due to lack of funds. In this environment, would USF still consider it a good decision to invest in such a policy if it made no claims for many years? Given that this kind of insurance policy was still new to the market, were there some examples of organizations that had bought this kind of insurance, and if so, what was their experience?

While cyber insurance seemed unlikely to be budgeted in the short run at USF, Alex could clearly see that businesses were taking it seriously. Such business innovations were not common, and Alex was eager to be the subject matter expert in this emergent domain, when presented the opportunity. Yes, he was going to learn enough about cyber insurance to be able to make an informed recommendation to his CIO next week.

Insurance

The Oxford dictionary defines insurance as the arrangement by which a company or government agency provides a guarantee of compensation for specified loss, damage, illness, or death in return for payment of a premium. Insurance is a mechanism by which organizations reduce the financial impacts of adverse events by transferring risks to those best able to absorb them.

Why would an organization need insurance? In their day to day operations, all organizations face the possibility of unpleasant surprises. These are called risks. Competitors entering markets, increases in raw material prices, and changing customer tastes are all examples of such risks. Managers spend a lot of time anticipating and responding to these risks. However, some risks are very large, and can have financial impacts that can be catastrophic or even fatal to the organization. For example, hurricanes are a fact of life in the state of Florida, and a hurricane passing over the university campus could cause extensive damage to many classrooms, thereby disrupting student learning at the university. If the university does not have the funds to repair the damaged classrooms soon after the hurricane passes, then student learning could be impacted for a long time while the university mobilizes the funds to repair the classrooms.

In anticipation of this problem, most organizations purchase insurance. In return for steady payments, when the specified risk occurs, the insurer guarantees to pay according to the terms of the contract. These payments usually meet most of the costs of responding to the risk. The primary benefit to the insured party is to replace uncertainty with certainty. The specific case of insurance for damage to classrooms at USF is interesting in that the State of Florida offers insurance coverage to the university (see Exhibit 4). This is an example of self-insurance.

Origins[2]

Insurance is a very old concept in human society. The earliest arrangements resembling insurance were called bottomry contracts. They were used by the merchants of Babylon as early as 4000–3000 BC. In a bottomry contract, lenders gave money to merchants with the agreement that the loan did not have to be repaid if the shipment was lost at sea. The cost of this provision was included in the interest charged on the loan. These insurance-like arrangements facilitated the growth of marine trade by eliminating catastrophic risk to merchants.

In England, the Great Fire of London in 1666 led to the development of fire insurance. Eventually these operations led to the development of modern property and liability insurance. Lloyd's of London, the world's international insurance market, was a key player in the early development of insurance in Europe. Edward Lloyd (1648–1713), ran a coffeehouse frequented by merchants, bankers, and insurance underwriters. Sensing user requirements, Lloyd supplied his customers with shipping information gathered from the docks and other sources, information that is still published as Lloyd's List (http://www.lloydslist.com). Slowly, Lloyd's coffee house gained the reputation as being the place where merchants were most likely to find underwriters for marine insurance. In 1769, Lloyd's reorganized as a group of underwriters accepting marine risks. The word underwriter probably refers to the practice of each risk taker writing his name under the total amount of risk he was willing to accept at a specified premium. Today Lloyd's is a major reinsurer as well as primary insurer, with member underwriters competing with each other to offer insurance.

In the United States, Benjamin Franklin set up the first insurance company in 1752 as the Philadelphia Contributionship. These early efforts at providing insurance on a large scale highlighted the challenges of

[2] This section is drawn from the article on the historical development of insurance in the Encyclopedia Britannica.

operating insurance as a business. Many early property insurance companies failed as a result of speculative investments. Some others failed when the insurance companies were faced with extensive claims following the Great Chicago Fire in 1871 and the San Francisco earthquake and fire of 1906. These failures highlighted the need for regulation in the industry as well as the need for robust statistical models to price insurance.

Life insurance grew steadily in the United States throughout the 20th century. The annual growth rate of life insurance in force over the period 1910–90 was approximately 8.4 percent. Approximately 3,800 property-liability and 2,270 life insurance companies were operating in the United States in 1989, employing nearly two million workers. At that time, U.S. insurers wrote about 37 percent of all insurance premiums collected worldwide.

Japan was another country with a well-established insurance industry. The industry grew rapidly as the country industrialized following World War II. Toward the end of the 20th century, Japan ranked number one in the world in life insurance in force. About 25 percent of all insurance premiums collected in the world were in Japan, making it the second largest insurance market, exceeded only by the United States.

In 1990 the 10 leading insurance markets in the world in terms of the percentage of total premiums collected were: the United States (35.6 percent), Japan (20.5 percent), the United Kingdom (7.5 percent), Germany (6.8 percent), France (5.5 percent), the Soviet Union (2.6 percent), Canada (2.3 percent), Italy (2.2 percent), South Korea (2.0 percent), and Oceania (1.8 percent).

Several trends were underway in the insurance industry. There was a move towards the development of worldwide insurance programs to cover the operations of multinational corporations. Reinsurance was becoming popular, as was the increasing use of self-insurance programs administered directly (as in the case of property insurance for state-owned buildings in the State of Florida) or by wholly owned insurance subsidiaries (captive companies).

Common Types of Insurance[3]

The different types of insurance can broadly be classified in the following categories.

Property Insurance

Property insurance covers accidental destruction of property. The two common types of property insurance are homeowner's and commercial property insurance. The standard contract typically specifies the agreement, the covered property, stipulations, and any exclusions.

The agreement specifies the different sources of damage covered. Typically, these include fire, theft, lightning, and other common sources of damage. Policies generally also cover the costs of relocation if that becomes necessary as a result of a covered risk. The agreement also specifies the extent of compensation provided when the policy is invoked. A common agreement is to cover the cost of restoring the damaged property to its pre-damage state.

Business property insurance policies are similar to home property insurance policies, but can include coverage for indirect losses. The most commonly covered indirect loss is loss of income. A retail store damaged from fire can be shut down for a month, leading to lost income for the month. The business income

[3] This section is based on the Encyclopedia Britannica article on Insurance.

insurance component of the store's property insurance policy compensates the store owner for the income lost during this period.

The covered property specifies the structure covered by the policy. Typically, this includes the main structure as well as any structures such as garages and fences on the property, and within limits, damages to personal property within the covered structures.

The stipulations or conditions specify the obligations of the insured. The most common conditions include requirements for payment of premium, commitment to truthful representation, staying away from fraudulent claims, and documentation for loss claims.

Exclusions specify the conditions under which the policy will not cover damages. Common exclusions include losses from freezing when the structure is unoccupied, loss from neglect, and gradual damage from mold or water leakage. Losses from floods and earth movement are also a common exclusion by default.

Liability Insurance

Another large segment of the insurance market covers obligations arising out of negligence. Liability insurance covers claims against individuals or businesses that, in the eyes of the law, did not act reasonably or with due care. There are numerous incidents where court judgments in these cases have run into the millions of dollars. There are 4 major types of liability insurance--auto insurance, business liability insurance, professional negligence, and personal liability. Professional negligence often applies to physicians, and personal liability often applies to people in sporting activities.

Important features of all liability insurance include a requirement that the insurer defend the insured in court where needed and to pay court settlements. For this reason, liability insurance is sometimes also called defense insurance. However, most liability insurance policies have limits on the maximum amounts payable by the policy in a settlement.

Another interesting feature of liability insurance policies is that the definition of insured is quite broad. For example, auto insurance policies cover not just the owner, but also anyone who drives the car with the owner's permission.

Workers' compensation insurance is another important class of liability insurance. It compensates workers for losses incurred from work-related injuries. Unlike most other forms of liability insurance, negligence is generally not a requirement for eligibility. Though workers' compensation was originally limited to workers in hazardous professions, it is now generally also extended to workers in clerical positions.

There are some other popular forms of liability insurance. Theft insurance covers all acts of stealing, including burglary, robbery, and other theft. Credit insurance pays creditors in case of default by borrowers.

Transportation Insurance

Transportation insurance in the form of ocean marine insurance was one of the earliest forms of insurance. Transportation insurance covers merchandise from the moment it leaves the warehouse of the seller till the time the goods arrive at the warehouse of the buyer. Commonly, these insurance policies also cover damages to the ships used to transport the goods.

Suretyship

Surety insurance contracts protect businesses against the possible dishonesty of their employees. An important exclusion in all theft insurance policies is that they do not cover against losses from persons in a position of trust. Surety bonds are therefore useful for contractors working on personal or commercial property and their clients. The surety bond reimburses clients from any losses arising from failures or dishonesty of the contractor's workers.

Life and Health Insurance

Life insurance policies compensate beneficiaries of the insured upon the death of the insured person. In the developed world, life insurance has become an important form of personal savings. Life insurance is also gaining popularity in developing countries.

Health care expenses are the focus of an important class of insurance policies--private health care insurance. In most countries, residents have access to health care facilities provided by the government as well as physicians and health care facilities operating commercially. Private health care insurance policies are intended to cover the costs of hospitalization, surgeries, and other major medical expenses. However, many private health care insurance policies also cover routine health care expenses such as doctor visits.

Reinsurance

Reinsurance is the practice of distributing risks among multiple insurers to reduce loss exposures to a single insurer when faced with a catastrophe. A common form of reinsurance is excess-of-loss reinsurance where the client insurance company covers losses up to a specified amount, and the reinsurers cover any losses in excess of the specified amount. Another form of reinsurance is pro-rate reinsurance where a group of insurers divide premiums and losses among themselves.

A benefit of reinsurance is that an insurer that operates in a market can expand its risk taking ability in a responsible manner by distributing risks to other insurers.

Insurance Concerns

Insurance has been the subject of much theoretical work in economics. George Akerlof (1970) and other economists argued early on about the possibility that private insurance markets could fail as a result of asymmetric information. Since 2000, economists have paid considerable attention to empirically verify the expectations generated from these theoretical arguments. Chiaporri and Salanie (2002) have provided a good summary of this line of work.

While the evidence thus far has been mixed, one experiment cited by Chiaporri and Salanie (2002) was the Rand Health Insurance Experiment (HIE) conducted between November 1974 and February 1977. Participating families were randomly assigned to one of 14 different insurance plans in six different sites across the US, with different coinsurance rates and different upper limits on annual out-of-pocket expenses. The use of medical services was found to respond to changes in the amount paid by the insured. The largest decrease in the use of outpatient services occurred between a free plan and a plan involving a 25% copayment rate; larger rates did not significantly affect expenditures. The HIE and other experiments have suggested that asymmetric information before and during the period of coverage affects and is affected by the availability of insurance. Consumers have prior information about their exposure to risk and select insurance contracts accordingly, or purchasers of greater coverage take less care after being covered by insurance. The former problem is called adverse selection, and the latter problem is called moral hazard.

Adverse Selection

Adverse selection is a problem that occurs when buyers and sellers have different information (asymmetric information). Traders participate in trades that are most beneficial to them, and those with superior private information can benefit at the cost of the others.

American Airlines' AAirpass is a great example of what happens when a business errs in its estimates of value. American Airlines introduced the AAirpass in 1981 at $250,000, and offered unlimited first-class travel on the airline for the life of the customer. Bob Crandall, American's CEO at the time said, "We thought originally it would be something that firms would buy for top employees." However, the purchasers of the AAirpass were such frequent fliers that some of them would have paid $125,000 in one month for their flights. American's CEO continued, "It soon became apparent that the public was smarter than we were." American Airlines tried raising the price, reaching $1 million for the AAirpass. However, the only people who bought it were those whose needs significantly exceeded the price of the pass. American Airlines eventually gave in and stopped offering the deal (Oyer, 2013).

Adverse selection is a common problem in insurance since people use their private information about their own insurance needs before deciding to buy the contract.

Moral Hazard

Moral hazard refers to the phenomenon where an insured person takes on more risks than they would otherwise take, since they know that someone else bears the burden of those risks. Moral hazard refers to the change in behaviors of a person after the insurance contract has been established. For example, some holders of the AAirpass admitted to flying just because they liked being on planes, and it cost them nothing to do so (Bensinger, 2012). In private health insurance markets, co-payments and deductibles are used to reduce the risk of moral hazard by imposing out-of-pocket expenses on consumers, reducing the likelihood of claims for frivolous and unnecessary medical expenses.

Insurance Practice

While adverse selection and moral hazard are two well understood problems associated with insurance, empirical tests for the effects of adverse selection and moral hazard have yielded no clear results, suggesting that insurers are doing a very good job at anticipating these effects, and designing insurance contracts accordingly. This comes from two core functions performed by insurers to ensure competitive and viable coverage of risks--underwriting and rate making. Underwriting refers to the selection of risks to insure, and rate making refers to pricing accepted risks.

Rate Making

Rate making is the determination of the price per unit of risk exposure. The rate typically reflects three major elements of the insurance contract: the expected loss per unit of exposure, the administrative expenses associated with operating the business, and the profit margins. Expenses and profits typically account for about one-third of the premium in property insurance contracts. The remaining two-thirds of the premiums cover expected losses over the term of the policy.

Rates are typically expressed in terms of exposure. For example, if the rate for a policy is determined to be $1 per $100 of exposed property, insurance coverage for $1,000 of exposed property will cost $10.

Rate making involves four basic issues: (1) allocating risk expenses fairly so that insurance rates reflect the differences in risks involved; (2) pricing contracts so that they are adequate to meet expenses under most situations imaginable, but without unreasonably large profits; (3) revising rates frequently enough to

reflect coverage costs; and (4) designing contracts that account for adverse selection and moral hazard effects so that the insured have incentives to minimize losses.

Examples can be cited for each of these issues in contemporary insurance practice. In allocating risk expenses, an element is identifying the variables that have the greatest impact on risks. For example, in life insurance policies, a very important factor that determines the risks associated with writing an insurance contract is age. Accordingly, insurance rates are different for people in different age groups. Reasonable pricing involves allowing home insurers in coastal states to accumulate reserves over multiple years of low hurricane activity in order to develop the ability to remain solvent in the event of a catastrophic hurricane such as in the 2004 hurricane season. The Florida Office of Insurance Regulation monitors companies offering insurance to Florida residents to ensure their solvency, including in the event of a 1 in 100-year storm (McCarty, 2009). Since the likelihood of such extreme events is almost impossible to predict, it can be very difficult to accurately assess the risks involved.

The third issue is about revising rates as needed. Auto insurance companies change rates when the claim frequency or cost of injuries change (Geico, 2016). Finally, an example arrangement to prevent abuse of asymmetric information is the use of market discipline to prevent abuse of FDIC insurance by banking institutions. Stockholders in banks are exposed to losses when banks fail, and therefore have the incentive to closely monitor the management and financial activities of these banks (FDIC, 2016). This monitoring prevents banks from weak lending standards, which usually arises out of competitive pressures, thereby protecting the Federal Deposit Insurance Corporation as well as the insured depositors who use banks as savings vehicles through checking and savings deposits. Another mechanism to prevent moral hazard is called merit rating, where insurers reward the insured for good behavior. For example, auto drivers get discounts for accident-free driving. Property owners get discounts for installing safety features. In health insurance, discounts are offered when a particular group of employees increases participation in health programs, or avoids frivolous claims.

Underwriting

Underwriting is the selection of risks to insure. The main objective of underwriting is to ensure that the risks accepted by the insurer are compatible with the assumptions made while rating the risks. For example, if an auto insurer rates its insurance rates for relatively safe drivers, the underwriting process needs to ensure that each insured driver has an acceptably safe driving history. Improper underwriting is a very common cause for the failure of insurance companies. For example, in 2000-2001, several worker's compensation insurance companies went out of business as a result of weak underwriting in response to competitive pressures (Brennan, Clark, & Vine, 2013). Surprisingly, there was no major insurance failure during the financial crisis of 2008. AIG, a large insurer was in the news at the time, but the problems at AIG did not emerge from its insurance operations.

An interesting feature of underwriting is that insurance industry profits often rise and fall in fairly regular patterns. This phenomenon is called the underwriting cycle. At the beginning of the cycle, profits are high, and some insurers lower prices to expand their businesses. The profits also attract new entrants, increasing competitive pricing pressures. At the margin, this leads to insurance pricing that does not cover the risks, leading to underwriting losses. Insurers then raise rates, and only accept the safest risks, sometimes even abandoning unprofitable markets. Eventually this restores profits, and the underwriting cycle repeats itself. Customers experience this cycle when they find insurance rates falling in certain years, and insurance not even being available for new policy holders in other years.

Cyber Insurance

As the economy was becoming more digital, individuals and companies were storing increasing amounts of sensitive and fine-grained information online. Bad actors found it very attractive to steal this information to access bank accounts, intellectual property, and other personal information. When the technology systems were online, they could be accessed from anywhere in the world, giving bad actors the ability to stay out of the reach of law enforcement agencies representing the hurt victims. Among the common cyber risks were:

- Identity theft, where personal information including social security numbers, credit card numbers, birth dates, and PIN numbers were stolen. These were then used to forge credit cards, transfer funds from bank accounts, etc.
- Business interruption from a hacker damaging database records.
- Costs associated with replacing stolen credit cards.
- Theft of valuable digital assets, including customer lists and intellectual property.
- Introduction of malware and viruses into an organization's network.

Recent high-profile incidents affecting hundreds of millions of people and some of the nation's most respected businesses have created an opportunity for insurance companies to offer liability insurance coverage in the event of cyber-attacks. Typical coverage provided by such cyber liability policies included the following (NAIC, 2016):

- The costs associated with a privacy breach, such as consumer notification, customer support, and costs of providing credit monitoring services to affected consumers.
- The costs associated with a forensics investigation of the incident, to identify the threat agents, the vulnerabilities exploited, and the threat actions used.
- The costs associated with restoring the IT systems to normal use.
- The costs associated with court judgements for allowing the loss of confidential information, or failing to prevent unauthorized access to computer systems.
- Expenses related to cyber extortion or cyber terrorism.

Exhibit 5 has a sample cyber insurance policy for reference. The sample policy highlights the coverages available in a typical cyber insurance policy, as well as the most common exclusions.

Purchasing

While the opportunity was tempting, rate making for insurance coverage for the unique cyber risks faced by an organization was difficult due to a lack of actuarial data. As of the time of writing this case (Oct. 2015), insurers compensated for the lack of actuarial data by using qualitative assessments of an applicant. Such qualitative assessments included evaluating management procedures and the firm's risk culture. As a result, cyber insurance policies were more customized than standard liability insurance policies, and also more expensive. Rate making at the time of the case included factors such as the industry, size and scope of the business, number of customers, types of data collected and stored, the business' disaster response plan, the business' risk management of its networks and intellectual property, employees' access to data systems, end-point protection (antivirus and anti-malware software), update policies, and firewalls.

It is evident from this list of factors that rate-making for cyber insurance is more complex than other forms of commercial liability insurance available at this time (2015). The relative severity of these variables and their impacts on risk pricing are not fully estimated at this time.

USF

Founded in 1956, the University of South Florida System was a young and agile system that included three institutions, each separately accredited by the Commission on Colleges of the Southern Association of Colleges and Schools: USF, USF St. Petersburg, and USF Sarasota-Manatee. USF was the first independent state university conceived, planned, and built in the 20th century. At the time of the case serving more than 48,000 students, the USF System had an annual budget of nearly $1.6 billion and was ranked 43rd in the nation for research expenditures among all universities, public or private. The organizational chart of the institution is in Exhibit 1.

USF, the main doctoral research institution in Tampa was home to USF Health, which included the Colleges of Medicine, Nursing, Public Health, and Pharmacy; and to the College of Marine Science that was physically located in St. Petersburg. The university is one of only four public universities in Florida classified by the Carnegie Foundation for the Advancement of Teaching in the top tier of research universities, a distinction attained by only 2.3 percent of all universities. At the time of the case, it offered more than 180 degree programs at the undergraduate, graduate, specialty, and doctoral levels, including the doctor of medicine degree. Its near term goal was to position itself for membership in the Association of American Universities (AAU), the group of leading national universities, which currently has 62 members.

The University of South Florida's mission was to deliver competitive undergraduate, graduate, and professional programs, to generate knowledge, foster intellectual development, and ensure student success in a global environment.

Its vision was to achieve its mission through competitive execution on 4 points:

- Student access, learning, and success through a vibrant, interdisciplinary, and learner-centered research environment incorporating a global curriculum.
- Research and scientific discovery to strengthen the economy, promote civic culture and the arts, and design and build sustainable communities through the generation, dissemination, and translation of new knowledge across all academic and health-related disciplines.
- Partnerships to build significant locally- and globally-integrated university-community collaborations through sound scholarly and artistic activities, and technological innovation.
- A sustainable economic base to support USF's continued academic advancement.

USF Facts

USF served 48,793 students as of Fall 2015, of whom 36,108 were undergraduate, 9,889 graduate, 697 medical students, and 2,099 were non-degree seeking students. Included in that number were 4,054 international students. In 2014 – 2015, USF awarded 9,468 undergraduate and 3,156 master's degrees. Arts and Sciences was the largest college with 15,357 students; followed by business and engineering with 5,470 and 5,584 students respectively. Global studies and marine sciences were the smallest colleges with about 95 students in each.

At the time of the case, USF was tightly focused on improving its graduation rates from the current 66% 6-year graduation rate for the freshman class that started in 2008, and 67% 4-year graduation rate for the transfer class that started in 2010. Among other resources that supported this effort were almost $60 mil-

lion in scholarships, and over $150 million in grants and waivers. These were made possible by a $418 million endowment, and $2.5 million in licensing revenues.

USF's academic mission was supported by both physical and intellectual resources. USF has 295 buildings on an overall campus area of 1,657 acres comprising 11,667,026 sq. ft. of built up space. Its students were served by 2,479 faculty, 2,427 administrative staff, 6,358 support and other personnel, and over 5,000 student assistants including graduate assistants. USF faculty and researchers secured $497 million in research funding in 2014 - 2015, of which $226 million was federal funding.

USF's library system was comprised of 5 facilities, and had 2,588,609 books, 91,680 journals, and 930 electronic databases, spending $8,669,103 in 2014 - 2015 to build and maintain its collections.

USF Points of Pride

In its short history, USF has made significant progress towards its mission. Its points of pride at the time of the case (2015) included:

- 46 national scholarship and fellowship student awardees for 2012-13 academic year.
- 72 distinguished university professors, and 36 endowed professorships.
- Online MS MIS program ranked #27 in the nation in the 2015 USNWR Online Education Program rankings.
- USF School of Accountancy was ranked 1st in the nation in accounting information systems research, as well as top 30 in other areas of research (audit #21 and tax #29), according to the 2012 rankings released by Brigham Young University (BYU).
- USF's part-time MBA is the top program among Florida's 12 state universities, and No. 16 among public universities in the nation (Bloomberg BusinessWeek, 2013).
- The Princeton Review and Entrepreneur Magazine once again ranked USF's interdisciplinary graduate entrepreneurship program among the top 25 programs in the nation (#13), the only Florida program that was included (2015).
- USF was a top producer of Fulbright U.S. Scholarship recipients, boasted the highest research and patent productivity among all Florida public universities, and was one of only 15 universities in the nations selected as a Tillman Partnership University of the Pat Tillman Foundation.
- USF was ranked 43rd in the nation for research expenditures, among all U.S. universities, public or private, by the National Science Foundation (2013).
- USF was ranked 27th in total research expenditures among public universities by the National Science Foundation (2013).
- The Chronicle of Higher Education ranked USF as the fifth fastest growing Research University in the U.S. from 2000-2010.
- USF ranked 15th world-wide for granted U.S. patents among all universities according to the Intellectual Property Owners Association (2013), and has ranked in the Top 15 worldwide among all universities for U.S. patents granted for the past four years (2010-2013).
- USF ranked in the Top 10 nationally for patents and in the Top 15 for startup companies and number of licenses and options, when compared to other U.S. universities in the most recent survey by the Association of University Technology Managers (2013).

- USF had a record breaking year in Technology Transfer in 2014, with 91 license/options, 11 new startup companies, 190 patent disclosures, and 113 new patents.
- USF's Tampa Bay Technology Incubator at the time of the case was home to 62 resident and affiliate companies and growing.

USF was the founder and home of the National Academy of Inventors (NAI), a non-profit member organization with over 3,000 individual inventor members and fellows spanning more than 200 U.S. universities, and governmental and non-profit research institutions. The USF Chapter of the NAI had over 300 USF faculty, staff, students, and alumni members, who collectively held more than 1,740 U.S. patents.

USF IT and IT Security Infrastructure at USF

Information Technology at USF was led by the Vice President of IT, who also served as the CIO of the University. In 2014-2015, the total IT budget at USF was over $30 million, which included expenses on salary, maintenance contracts, and the purchase of equipment and services. Services provided by USF IT included wired and wireless networks across the campus; computer labs across the campus; cybersecurity across the IT infrastructure; development of technology policies, procedures, standards and guidelines; compliance with laws such as the Gramm-Leach-Bliley act; email to all members of the campus community; IT help desk services; user account management; application support; and research computing support. As more and more information moves online, USF IT's work responsibilities have steadily increased over the years. Exhibit 2 presents the organizational chart of USF IT.

In response to the increase in cyber threats, USF has built an IT security infrastructure composed of technology, policy, and human components. In general, in keeping with the open academic model of university work, end user machines were usually supported by individual units, although over the years, many services such as email and application support have been centralized or virtualized. Cybersecurity was one of the areas where the need for centralization and specialization was acute because of the increased risks of security-related incidents on campus as well as the accompanying compliance requirements, and security audits. Centralization also helped with the coordination of security efforts among departments to address security threats quickly and efficiently. The cybersecurity responsibilities at USF have been partitioned into the following roles:

Information Security Manager

The Information Security Manager (ISM) was responsible for organizing campus-wide efforts in the area of security, such as development of USF data security policies, negotiation and evaluation of site licenses for security-related software, training, and dissemination of security-related information and incidents, which could affect the availability and integrity of computing resources on campus. When needed, the Information Security Manager had the authority and responsibility to isolate any compromised computing resource until the issue had been resolved. At the time of the case, Alex was in this role at USF.

Incident Response Team

The Incident Response Team (IRT) was responsible for quickly identifying threats to the campus data infrastructure, and taking steps to mitigate the threat. The IRT at USF was composed of the Information Security Manager, members of the campus backbone network administration personnel, and security staff. When threats were identified, IRT members notified local Information Security Officers and Administrators of any incident involving their resources.

Information Security Workgroup

The Information Security Workgroup (ISW) reviewed the policies and best practices initiated by the Information Security Manager prior to implementation and enforcement. The ISW was involved in campus-

wide contract negotiations related to security, such as vulnerability scanners, file integrity tools, and anti-virus software. Members of the Information Security Workgroup (ISW) included the Data Security Administrator, volunteer representatives from computing departments throughout the campus, and representatives from University Police, General Counsel, and Inspector General's Office. The ISW offered guidance to the Information Security Manager when new areas of concern developed and needed attention.

Information Security Administrator

The Information Security Administrator (ISA) was the technical person(s) in each department responsible for the security maintenance of computing resources within their organization. This included applying patches, installing and configuring virus detection software, and performing periodic vulnerability assessments on clients and servers within his or her area of responsibility. The ISA was usually the face of USF IT and cybersecurity to end users on campus.

Example: The State of Montana

While doing his research on cyber insurance, Alex became aware of the experience of the State of Montana with its cyber insurance policy. Following a well-publicized data breach in 2010, the state government purchased cyber insurance in 2011. A summary of the coverage is provided in Exhibit 3.

On May 15, 2014, the state became aware that it was the victim of a data breach. An investigation indicated that the server was first breached on May 22, 2013. The compromised data included client, employee, and contractors' names, addresses, dates of birth, social security numbers, clinical and medical data, and dates of service. There was also payroll information about employees of Montana's department of public health and human services on the server. It was estimated to be the fifth-largest HIPAA breach ever, and the largest-ever HIPAA breach caused by computer hacking (McCann, 2014).

An interesting feature of this breach for the cyber insurance community was that state officials acknowledged the assistance of its cyber insurance provider in responding to the breach. Lynne Pizzini, deputy CIO and CISO of the State of Montana participated in an hour-long webcast describing her experience with cyber insurance following the breach (MS-ISAC, 2015).

In the presentation, she described how insurance company representatives helped the state draft a notification to be sent out in a timely manner to the 1.3 million suspected victims.[4] The cyber insurance provider also assisted with media response, independent forensic investigation, and general incident response. State officials were overwhelmingly appreciative of the assistance offered by the cyber insurance provider for their work following the discovery of the breach. A list of the cyber insurance services provided during the 2014 DPHHS incident included:

- Forensic investigation
- Public relations consultation
- Legal consultation
- Website content recommendations--FAQs
- Recommendations on all communications (internal and external)
- Mail notifications
- Credit monitoring (one year)
- Call center for 60 days

[4] For a critical view of this response, please see http://www.healthcareitnews.com/news/montana-health-data-breach-textbook-example-what-not-do

Towards the end of the presentation, in the question and answer session, the insurance company executives volunteered some information on cyber insurance premiums. Essentially larger and more hazardous operations had greater premium rates. Smaller organizations typically had premium rates in the range of $7,000 - $15,000 for each $1 million in coverage. Larger organizations, with annual revenues in hundreds of millions of dollars or greater typically had rates in the range of $20,000 - $40,000 per $1 million in coverage. Revenues and record counts were two important factors in determining cyber insurance premiums. Record counts were important because an important component of many commercial cyber insurance liability policies was credit monitoring services for affected customers. And these costs were greater for organizations with a larger number of records.

The Decision

As the Director for Information Security at USF IT, Alex Campoe was one of the members of the USF IT senior leadership team. He was confident that USF IT would abide by his recommendations, so he felt the burden of making the right recommendations. A cyber breach could happen any time, and if USF were to invest in obtaining cyber liability insurance coverage, it was better to be quick than to be late. He had talked to many of his colleagues at USF IT, and even to some of his peers at other institutions. But since cyber insurance was so new, all his peers were in situations such as his--in the evaluation stage, and were unable to offer much advice.

However, even at this early stage, some outlines of the decision making process were taking shape in his mind. There were certain assessments he needed to make, including:

- **Identify and Characterize USF's Cyber Assets:** He needed to create an inventory of the cyber-reachable assets in the organization. On a napkin, he wrote down personal information, intellectual property, and healthcare information as broad categories of information that would require protection. On the same napkin, he also began listing some critical technology systems such as the learning management system that would need special attention. Along with identifying these assets, he would need to characterize them to prioritize them by criticality and sensitivity.

- **Determining USF's Threat Model:** Once he had identified and characterized the assets, following the standard template, he needed to develop the threat model facing his highest priority assets. This included identifying the major agents (internal, external and partners), and the most likely actions these agents might take to compromise these assets.

- **Determining the Risk Model:** For each important threat identified, Alex would need to estimate the associated risks. These risk estimates would give him dollar values of the risks he faced.

- **Determining Insurable Risks:** Alex knew that some of these risks, such as reputational risks, were not recoverable from insurance. So, he needed to shortlist his identified risks to the insurable risks.

Alex felt that with this information, he might be able to talk to some insurance companies, and negotiate prices and insurance coverage. But he realized he did not have enough information at this point to estimate these prices.

As he went through this exercise, he thought there might be a side benefit to this exercise. He might be able to do some spring cleaning of the IT infrastructure at USF. Over the years, numerous servers had been fired up across campus, and often they were kept running unmaintained. So the risk of USF being caught in a situation like Montana's DPHHS, where a single stray server could cause so much embarrassment, were real. He thought he could develop a plan to minimize the likelihood of such stray services

continuing to operate on campus. There did not seem to be any point in incurring insurable liabilities for services that had outlived their utility. But that could be a project for another day.

Alex felt good about his work so far. He had given himself a mini-tutorial on the cyber insurance market, and had developed a work plan to prepare himself to enter the marketplace as a buyer of insurance. The only remaining work was to develop the estimates he had shortlisted. USF was a large university with increasingly popular management information systems and cybersecurity programs. Surely, he could get the help of some students from these programs to do the assessments for him.

References

Akerlof, G. A. (1970). The market for "lemons": Quality uncertainty and the market mechanism. *Quarterly Journal of Economics, 84*(3), 488-500.

Bensinger, K. (2012). The frequent fliers who flew too much. *Los Angeles Times.* Retrieved from http://articles.latimes.com/2012/may/05/business/la-fi-0506-golden-ticket-20120506

Brennan, M., Clark, R. A., & Vine, M. J. (2013). *What may cause insurance companies to fail--and how this influences our criteria.* Retrieved from http://docplayer.net/75575-What-may-cause-insurance-companies-to-fail-and-how-this-influences-our-criteria.html

Chiaporri, P. A., & Salanie, B. (2002). Testing contract theory: A survey of some recent work. *Research Papers in Economics (REPEC).* Retrieved from https://ideas.repec.org/p/ces/ceswps/_738.html

Cybersecurity. (2016). Retrieved from http://www.naic.org/cipr_topics/topic_cyber_risk.htm

Florida rate increase information. (2016). Retrieved from https://www.geico.com/information/states/fl/florida-rate-increase-information/

Green, M. R. (2014). *Insurance.* Retrieved from http://www.britannica.com/topic/insurance

McCann, E. (2014, June). Hackers steal health data of 1.3M. *Healthcare IT News.* Retrieved from http://www.healthcareitnews.com/news/hackers-steal-health-data-13m

McCarty, K. M. (2009) *Insurance company solvency regulation.* Retrieved from http://www.floir.com/siteDocuments/CabinetPresentation01132009.pdf

MS-ISAC (Multi-State Information Sharing and Analysis Center). (2015). *July hot topics webcast - cyber risk insurance-20150715 1844-1.* Retrieved from https://cis-alliance.webex.com/cis-alliance/lsr.php?RCID=293db3a4ad5e50a3c3cff88fcafc653d

Options for addressing moral hazard. (2016). Retrieved from https://www.fdic.gov/deposit/deposits/international/guidance/guidance/moralhazard.pdf

Oyer, P. (2013). Cherry-pick profitable customers by understanding adverse selection. *Harvard Business Review.* Retrieved from: https://hbr.org/2013/12/cherry-pick-profitable-customers-by-understanding-adverse-selection

Acknowledgements

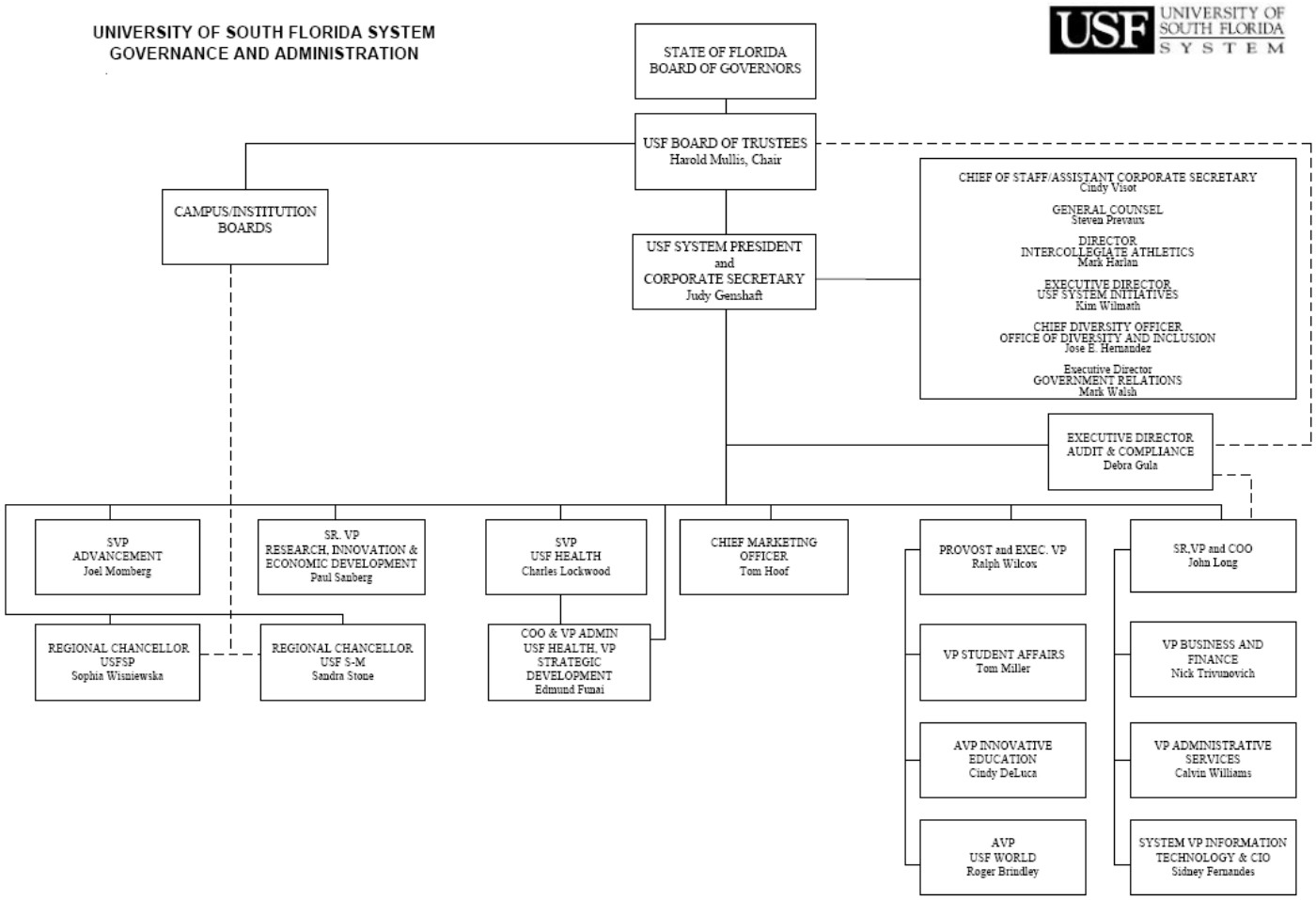
This case study is based upon work supported by the National Science Foundation under Grant No. 1043919.

Biographies

Manish Agrawal is an Associate Professor in the Information Systems and Decision Sciences department of the College of Business Administration at the University of South Florida in Tampa, Florida. His current research interests include social media monitoring during extreme events, information assurance, and software quality. Dr. Agrawal teaches classes on Web Applications Development, Information Security, and Computer Networks at both the graduate and undergraduate levels.

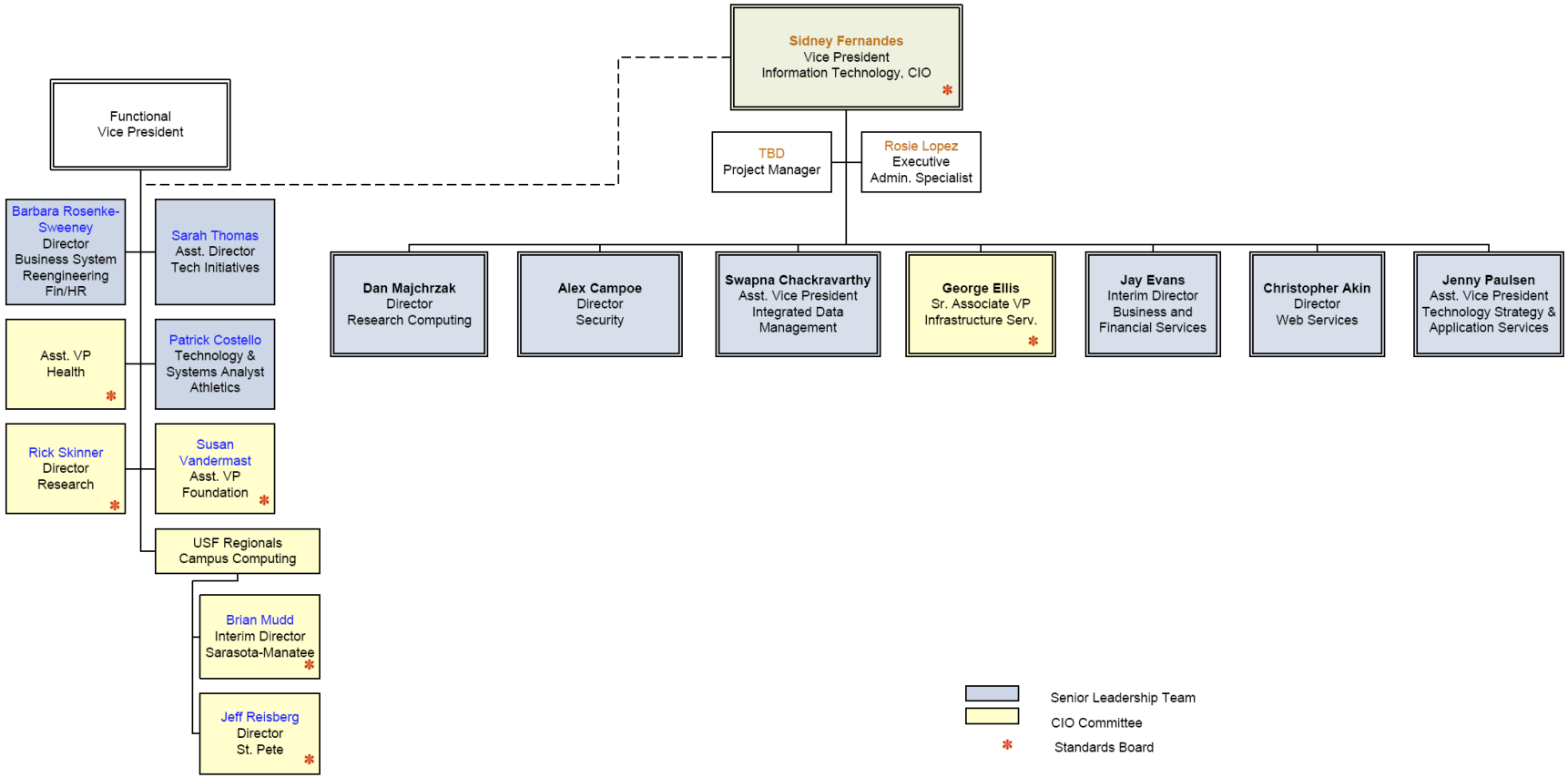
Shivendu Shivendu is an Assistant Professor in the Information Systems & Decision Sciences department at the University of South Florida.. He has created and taught undergraduate, MBA/MS, and doctoral courses in areas related to economics of information systems, management of information systems, IT strategy, IT consulting, and electronic commerce. Shivendu's research focuses on analytical modeling of business models based on technology platforms. His research studies economics of digitization of information, intellectual property rights protection in digital mediums, pricing of digital goods, digital product strategies including versioning and bundling, sourcing of IT services, security and privacy in Big Data, digital goods supply chain, information goods pricing under dual medium access, pricing of cloud computing services, multilayer platforms, and technology policy.

Exhibit 1: USF Organization Chart



Source: http://system.usf.edu/system-overview/pdfs/System-Governance-and-Admin-no-BOG.pdf (Sept. 2015)

Exhibit 2: USF IT Organization Chart[5]



[5] http://www.usf.edu/it/documents/org-chart.pdf (Revised: 3/3/15)

Exhibit 3: State of Montana Cyber/Data Insurance Policy Summary[6,7]

A summary of data/information security insurance coverage, exclusions, and policy information is provided below. Coverage may vary by agency. This summary does not alter or amend coverage provided in statute or under the state property/casualty insurance program. If your agency experiences a data/information security incident involving the unauthorized disclosure of private, non-public information, please follow the instructions on our website at http://rmtd.mt.gov/claims/agenciesreportclaims.aspx and submit the claim to the Risk Management & Tort Defense Division. For additional information, please contact us at (406)444-2421.

SUMMARY

1. **Insurer**: Beazley Insurance Company and Barbican Insurance Company
2. **Broker**: Alliant Insurance Services, Inc.
3. **Term**: 7/1 to 6/30 each fiscal year.
4. **Coverage Territory**: This policy applies to insured events worldwide.
5. **Coverage Summary**: This policy provides coverage for the following:

Data/Information Security Liability

a. Damages and claims expenses associated with theft, loss, and unauthorized disclosure of private, non-public information.

b. Damages and claims expenses associated with alteration, corruption, and deletion of private, non-public information caused by malicious code and/or service denial failure.

c. Damages and claims expenses associated with unauthorized sharing and unauthorized selling of private, non-public information.

d. Failure to administer an identity theft protection program.

Privacy Notification Costs

a. Cost of hiring computer security experts to determine the existence and cause of a breach of private, non-public information.

b. Cost to comply with breach notification laws.

c. Cost of notifying parties affected by the breach.

d. Cost of credit monitoring for one year for those affected by the breach of privacy laws.

Regulatory Defense and Penalties

a. Claims expenses and penalties arising from regulatory proceedings involving the unauthorized disclosure of private, non-public information.

b. Claims expenses and penalties arising from violations of privacy laws.

---

[6] http://rmtd.mt.gov/insurance/cyberdatasecurityinsurance

[7] Note: Losses that fall outside of commercial insurance limits are the responsibility of each agency/university.

Website Media

a. Damages and expenses associated with defamation, libel, slander, caused by the disclosure of private, non-public information.

b. Damages and expenses associated with public disclosure of private information.

c. Damages and expenses associated with plagiarism, piracy, misappropriation of ideas involving private, non-public information.

d. Damages and expenses associated with infringement of copyright of private, non-public information.

6. **Exclusions**: A summary of exclusions is hereby provided.

    1. Bodily Injury or Property Damage
    2. Any employer-employee relations policies and practices
    3. Contractual liability or obligation
    4. Unlawful collection or acquisition of personally identifiable non-public information
    5. Anti-trust violations
    6. Unfair trade practices
    7. Incidents occurring prior to retroactive date of coverage
    8. Securities Act violations
    9. Fair Labor Act violations
    10. Discrimination
    11. Patent infringement
    12. Money/securities/funds transfer
    13. Broadcasting, publications, and advertising
    14. War and terrorism
    15. Pollution
    16. Nuclear events
    17. Radioactive contamination

7. **Co-Insurance**: There is no deductible. However, each agency or university is responsible for 20% of reasonable and necessary expenses incurred by the Risk Management & Tort Defense Division to investigate, evaluate, and resolve data/information security claims. The division will bill agencies for their fair share of co-insurance payments up to a maximum of $20,000.

8. **Limits**: $2,000,000 per occurrence Information Security & Privacy Liability

    a. $2,000,000 per occurrence Privacy Notification Costs

    b. $4,000,000 per occurrence Regulatory Fines and Penalties

    c. $2,000,000 per occurrence Website Content & Media

    d. $2,000,000 annual aggregate All coverage combined

Exhibit 4: USF Property Coverage

USF receives property coverage from the State of Florida, as part of the state's self-insurance program (please see figure below for the opening statement of the coverage). The details of the coverage are available from USF at:

http://www.usf.edu/administrative-services/environmental-health-safety/documents/riskmanagement-propertycoverage.pdf

DEPARTMENT OF FINANCIAL SERVICES
Division of Risk Management

State Risk Management Trust Fund

Certificate of Property Coverage

Various provisions in this certificate restrict coverage. Read the entire certificate carefully to determine rights, duties and what is and is not covered.

Coverage for defending and paying claims under this certificate is provided under the authority of Chapter 284, Florida Statutes, wherein the state is authorized to administer a self-insurance program. Provision of this certificate does not constitute the issuance of insurance other than on a self-insurance basis, and payment of any covered claim obligations is contingent upon availability of legislative funding.

Source: http://www.usf.edu/administrative-services/environmental-health-safety/documents/riskmanagement-propertycoverage.pdf

Exhibit 5: Sample Cyber Insurance Policy

AIG

Variable for Paper Company
A capital stock company (the "**Insurer**")

Policy Number: Replacement of Policy Number:

CyberEdge PCSM

NOTICES:

DECLARATIONS

Policyholder:		**Policy Period:**	**From:**	
			To:	
Policyholder Address:		**Insurer Address:**		
Premium:	$ XX,XXX,XXX	**Policy Aggregate:**		$ XXX,XXX,XXX

COVERAGE SUMMARY

Coverage Type	Minimum Attachment	Event DIC Limit	Minimum Underlying Limits	Event Limit	Coverage Type Aggregate Limit
Cyber Event Response	$ XX,XXX,XXX	Not Applicable	Not Applicable	$ XXX,XXX,XXX	$ XXX,XXX,XXX

OTHER TERMS AND INFORMATION

Claims Notice:	**Mail:**	[Variable]
	e-mail:	cyberedgefnol@aig.com

Specimen Draft 4-25-2014

AIG

CyberEdge PC℠

In consideration of the payment of the premium, the **Insurer** and the **Insureds** agree as follows:

1. INSURING AGREEMENTS

For any **Triggering Event** that takes place during the **Policy Period**, this policy will provide the following coverage:

Cyber Event Response	This policy will pay **Event Response Costs** incurred in response to a **Security Failure** that an **Insured** knows caused, or **Suspects** is likely to have caused, a **Triggering Event**.
Cyber Follow Form Excess	For each **Coverage Type**, this policy will provide coverage excess of the **Underlying Limits** for **Loss** caused by a **Security Failure**. Such coverage shall be provided in accordance with the same terms, conditions and limitations of the applicable **Followed Policy**, as of the inception date of this policy, as modified by and subject to the terms, conditions and limitations of this policy.
Cyber Difference in Conditions ("DIC")	For each **Coverage Type**, other than *Cyber Event Response*, this policy will drop down and pay **Loss** caused by a **Security Failure** that would have been covered within an **Underlying Policy**, as of the inception date of this policy, had one or more of the following not applied: A. a **Cyber Coverage Restriction**; and/or B. a **Negligent Act Requirement**.

In all events, coverage under this policy will apply only if: (i) the **Security Failure** is first discovered on or after the inception date of the **Policy Period** and prior to the expiration of the latest **Successive AIG Policy**; and (ii) the **Triggering Event** and the **Security Failure** are reported to the **Insurer** as required by this policy. Coverage under this policy will not apply to any **Loss**, **Security Failure** or other event that was known by any **Insured** prior to the inception of this policy.

2. DEFINITIONS

The terms **Claims Notice**, **Coverage Type Aggregate Limits**, **Insurer**, **Insurer Address**, **Event DIC Limit**, **Event Limit**, **Minimum Attachment**, **Minimum Underlying Limits**, **Policy Aggregate**, **Policyholder**, **Policyholder Address** and **Premium** are used in this policy with the meanings and values ascribed to them in the Declarations.
The other terms in "**Bold**" typeface are used in this policy with the meanings ascribed to them below.

Computer System	means any computer hardware, software, or any components thereof, that are linked together through a network of two or more devices accessible through the Internet, internal network or connected with data storage or other peripheral devices (including wireless and mobile devices), and provided that such hardware, software, components, devices and internal networks are under ownership, operation or control of, or are leased by, an **Entity Insured**.
Coverage Type	means the coverage afforded under each discrete set of terms, conditions and limitations within each tower of coverage named as a "Coverage Type" in the *Underlying Policy Summary Appendix*. "**Coverage Type**" also means the discrete set of coverage terms, conditions and limitations in this policy for *Cyber Event Response*.
Cyber Coverage Restriction	means a limitation of coverage in an **Underlying Policy** expressly concerning, in whole or in part, the security of a **Computer System** (including **Electronic Data** stored within that **Computer System**).
Electronic Data	means any software or electronic data stored electronically on, or that forms part of, a **Computer System**, but excluding **Personal Information**.
Entity Insured	means, for each **Coverage Type**, the **Policyholder** and any **Insured** that is not a natural person.

AIG

2. DEFINITIONS (Continued)

Event Response Costs means the reasonable and necessary expenses and costs incurred by an **Entity Insured**, and consented to in writing by the **Insurer**, in:

A. investigating (including forensically) the cause of the **Security Failure** and how it caused the **Triggering Event**;

B. a targeted public relations response to the **Triggering Event**, including, without limitation, the costs of crisis management services directed to mitigating the financial harm to such **Entity Insured** from the **Security Failure**; and

C. assessing whether **Electronic Data** can or cannot be restored, recollected or recreated, and, if reasonably feasible, in restoring, recollecting or recreating such **Electronic Data**.

"**Event Response Costs**" shall not mean, and this policy shall not cover: (i) compensation, fees, benefits, overhead or internal charges of any **Insured**; or (ii) any costs or expenses relating to advertising, promotion or publicity, other than those necessitated as a direct result of a **Security Failure**.

Followed Policy means, for each **Coverage Type** and subject to the *Maintenance of Underlying Insurance and Changes* Clause, the policy identified in the *Underlying Policy Summary Appendix* to this policy with an "*" at the beginning of its row.

Insured means: (A) the **Policyholder** and (B) for each **Coverage Type**, is used in this policy with the same meaning as that term has in the **Followed Policy** applicable to that **Coverage Type**.

Limit of Insurance means, for each **Coverage Type**, the amount set forth in the *Underlying Policy Summary Appendix* to this policy for each **Underlying Policy**.

Loss

A. for *Cyber Event Response*, means **Event Response Costs**; and

B. for each other **Coverage Type** (other than *Cyber Event Response*), means any:

(i) covered bodily injury, covered property damage or other covered loss, costs or expenses as established in the **Followed Policy** applicable to that **Coverage Type**; and

(ii) bodily injury, property damage or other loss, costs or expenses that would have been covered within an **Underlying Policy** applicable to that **Coverage Type** if a **Cyber Coverage Restriction** and/or a **Negligent Act Requirement** not applied.

"**Loss**" shall not mean, and this policy shall not cover, costs or expenses arising out of, based upon or attributable to: (1) updating, upgrading, enhancing, improving, restoring or replacing any **Computer System** to a level beyond that which existed prior to the **Security Failure** or **Triggering Event**; (2) unfavorable business conditions; (3) the removal of software program errors or vulnerabilities; or (4) any **Insured** satisfying its obligations under this policy, including, without limitation, proving loss as required under Clause 6. *Obligations of the Insureds*.

Negligent Act Requirement means a requirement in an **Underlying Policy** that the event, action or conduct triggering coverage under such **Underlying Policy** result from a negligent act, error or omission.

Personal Information means any information: (A) from which an individual may be uniquely and reliably identified or contacted; (B) that would be considered nonpublic personal information, protected personal information, protected health information or electronic protected health information; or (C) used for authenticating individuals for normal business transactions.

Policy Period means the period set forth as such in this policy's Declarations. The **Policy Period** incepts and expires as of 12:01 A.M. at the **Policyholder Address**. In the event of cancellation, the **Policy Period** shall be deemed amended to reflect that it expires upon the effective time of cancellation.

AIG

2. DEFINITIONS (Continued)

Related Event	means, for each **Coverage Type**, the **Triggering Event** and any subsequent event, action or conduct that: (A) is the same as, related to, or a continuation of, the **Triggering Event**; or (B) arises from the same, a related, or a continuous, **Security Failure** that caused, or that an **Insured Suspected** caused, a **Triggering Event** or any **Related Security Failure**. All **Related Events** shall be deemed to have occurred at the time that the first **Triggering Event** occurred.
Related Security Failure	means: (A) the **Security Failure** that caused, or that an **Insured Suspected** caused, a **Triggering Event**; and (B) any other **Security Failure** that enabled, facilitated or is a result of the **Security Failure** that caused, or that an **Insured Suspected** caused, a **Triggering Event**.
Security Failure	means a failure or violation of the security of a **Computer System** that: (A) results in, facilitates or fails to mitigate any: (i) unauthorized access or use; (ii) denial of service attack; or (iii) receipt, transmission or behavior of a malicious code; or (B) results from the theft of a password or access code from an **Entity Insured's** premises, the **Computer System**, or an officer, director or employee of an **Entity Insured** by non-electronic means. "**Security Failure**" shall not include any of the foregoing that results, directly or indirectly, from any: (1) natural or man-made earth movement, flood, earthquake, seaquake, shock, explosion, tremor, seismic event, lightning, fire, smoke, wind, water, landslide, submarine landslide, avalanche, subsidence, sinkhole collapse, mud flow, rock fall, volcanic activity, including eruption and lava flow, tidal wave, hail, or act of God; or (2) satellite or other infrastructure failure.
Successive AIG Policy	means, for each **Coverage Type**, each CyberEdge PC policy successively issued by the **Insurer** or its affiliate to the **Policyholder** that provides the same or comparable coverage for that **Coverage Type**.
Suspects(ed)	means reasonably believes(ed) based on specific, verifiable information.
Triggering Event	means, for each **Coverage Type**, the event, action or conduct that first triggers coverage under any **Underlying Policy** or would have triggered such coverage had a **Cyber Coverage Restriction** or a **Negligent Act Requirement** not applied. A "**Triggering Event**" shall not mean a notice of circumstance; however, any event, action or conduct that first triggers coverage under an **Underlying Policy** due to a notice of circumstance will be deemed a **Triggering Event** under this policy at the time of such notice of circumstance to the **Underlying Insurer**. "**Triggering Event**" shall not mean the **Security Failure** itself.
Underlying Insurer	means, for each **Coverage Type**, the insurer(s) of each insurance policy identified in the *Underlying Policy Summary Appendix* to this policy.
Underlying Limits	means, for each **Coverage Type**, the greater amount of either the applicable **Minimum Underlying Limits** or the actual underlying limits in place at the time of the **Triggering Event**. In the event coverage is afforded under an **Underlying Policy** and one or more renewal or replacement of that policy for any **Related Events**, then all such policy's limits shall be treated as **Underlying Limits**.
Underlying Period	means, for each **Coverage Type**, the period of time set forth in the *Underlying Policy Summary Appendix* to this policy.
Underlying Policy	means, for each **Coverage Type**, the policy(ies) identified in the *Underlying Policy Summary Appendix* to this policy.

Specimen Draft 4-25-2014 3

AIG

3. EXCLUSIONS

This policy shall not cover the defense of any matter, or any loss, injury, damage, costs, expenses or other amounts:

Acts of War	arising out of, based upon or attributable to any strike, lockout, disturbance or similar labor action, war, invasion, military action (whether war is declared or not), political disturbance, civil commotion, riot, martial law civil war, mutiny, popular or military uprising, insurrection, rebellion, revolution, military or usurped power, or any action taken to hinder or defend against any of these events; whether or not any other cause or event contributed concurrently or in any sequence to any resulting loss, injury, damage, costs, expenses or other amounts;
Advertising/ Personal Injury	arising out of, based upon or attributable to: (A) false advertising or misrepresentation in advertising; (B) false arrest, detention or imprisonment; (C) libel, slander or defamation of character; (D) wrongful entry or eviction; or (E) malicious prosecution;
Conduct	A. arising out of, based upon or attributable to any dishonest, fraudulent, criminal or malicious act, error or omission, or any intentional or knowing violation of the law, committed alone or in collusion with others by, directed by, approved by, acquiesced to by, known by or that should have been known by any past or present director, officer, trustee, general or managing partner or principal (or the equivalent positions) of an **Entity Insured**; B. arising out of, based upon or attributable to any profit or advantage to which any **Insured** is not legally entitled; or C. paid or incurred by, chargeable to, or otherwise due and owing from, any natural person who intentionally, knowingly or recklessly caused, aided or abetted a **Security Failure** or any **Related Security Failure**, whether or not for personal gain, and whether or not with the intent of causing any harm or a **Triggering Event**;
Government Action	arising out of, based upon or attributable to any seizure, confiscation, nationalization, breach of security, use, misuse or destruction of a **Computer System** or **Electronic Data** by or on behalf of any governmental, military, enforcement or other public body or authority; whether or not any other cause or event contributed concurrently or in any sequence to any resulting loss, injury, damage, costs, expenses or other amounts;
Intellectual Property	arising out of, based upon or attributable to any actual or alleged trade secret, patent, copyright, trademark, trade dress or other intellectual property;
Prior Notice	arising out of, based upon or attributable to any event, action, conduct, circumstance, claim, occurrence or loss caused by a **Security Failure**, if, prior to the inception of this policy, that **Security Failure**, event, action, conduct, circumstance, claim, occurrence or loss had been reported, or deemed reported, under any insurance or had been reported to the legal or risk management functions of any **Entity Insured**; or
Privacy, Personal Information and Confidential Information	arising out of, based upon or attributable to any invasion of privacy; or any: A. theft, disappearance, destruction or other loss, disclosure, publication, collection, use or storage of; B. failure to protect, or exercise any duty of care with respect to; or C. failure to comply with any law (statutory or common), rule or regulation, or any policy concerning; **Personal Information**, confidential information or any other information or data.

The exclusions and other limitations in any **Underlying Policy** for each applicable **Coverage Type** also apply, except that, for the *Cyber DIC Coverage*, such exclusions and limitations shall not apply to the extent they fall within the definition of **Cyber Coverage Restriction** or **Negligent Act Requirement**.

AIG

4. ATTACHMENT

Cyber Event Response Coverage

The **Insurer** shall be liable only for those covered amounts under this policy in excess of the **Minimum Attachment** applicable to *Cyber Event Response Coverage*. A single **Minimum Attachment** shall apply to all covered **Event Response Costs** in response to any **Security Failure** or incurred in connection with any **Related Event**.

Cyber Follow Form Excess Coverage

For each underlying **Coverage Type**, the **Insurer** shall be liable only for those covered amounts under this policy in excess of the **Underlying Limits** applicable to that **Coverage Type**. The **Insurer's** obligations shall attach only after the **Underlying Limits** applicable to such **Coverage Type** have been exhausted through payments of covered amounts. The risk of uncollectability of any part of the **Underlying Limits** is retained by the **Policyholder** and the **Insureds**, and is not insured under this policy or assumed by the **Insurer**.

Cyber DIC Coverage

For each underlying **Coverage Type**:

A. the **Insurer** shall only be liable for covered amounts under this policy in excess of the **Minimum Attachment** applicable to that **Coverage Type**; and
B. only one such single **Minimum Attachment** shall apply to all covered **Loss** for that **Coverage Type** in response to a **Security Failure** or incurred in connection with any **Related Event**.

5. LIMITS OF LIABILITY

Policy Aggregate

The **Policy Aggregate** is the most the **Insurer** will pay, in the aggregate, under this policy for all **Coverage Types** and Insuring Agreements combined, regardless of the number of **Insureds**, **Triggering Events** or **Security Failures**.

Each Coverage Type

For each **Coverage Type**:

A. the **Coverage Type Aggregate Limit** is the most the **Insurer** will pay under this policy, in the aggregate, for that **Coverage Type**;
B. the **Event Limit** is the most the **Insurer** will pay under this policy for that **Coverage Type** from any **Triggering Event** and any **Related Events**; and
C. the **Event DIC Limit** is the most the **Insurer** will pay under the *Cyber DIC Coverage* under this policy for all coverage of that **Coverage Type** from any **Triggering Event** and any **Related Events**.

Applicable to All Limits

The **Insurer** shall not pay any amounts over the applicable limits of liability stated above, and the **Insurer's** duty to pay, indemnify, reimburse or otherwise cover **Loss** under the relevant **Coverage Type** ceases upon exhaustion of any such limit of liability.

Each **Event DIC Limit** shall be part of, and not in addition to, the applicable **Event Limit**; each **Event DIC Limit** and each **Event Limit** shall be part of, and not in addition to, each applicable **Coverage Type Aggregate Limit**; and all such limits shall be part of, and not in addition to, the **Policy Aggregate**. Nothing stated herein or otherwise shall in any way serve to increase any other limit under this policy, including, but not limited to, the **Coverage Type Aggregate Limit** or the **Policy Aggregate**.

Notwithstanding anything to the contrary in any **Followed Policy**, expenses incurred to defend or investigate any **Triggering Event**, **Security Failure**, suit, proceeding or other matter under this policy shall be part of, and not in addition to, and will serve to erode any applicable **Event Limit**, **Event DIC Limit**, **Coverage Type Aggregate Limit** and the **Policy Aggregate**.

No limit of liability under this policy shall be reinstated, regardless of any provision in any **Underlying Policy**.

Specimen Draft 4-25-2014 5

AIG

6. OBLIGATIONS OF THE INSUREDS

Notice and Reporting

As a condition precedent to coverage under this policy, the **Insurer** must be notified by any **Insured** of any **Triggering Event** as soon as practicable after a an **Insured** first knows or **Suspects** that a **Security Failure** caused, or is likely to have caused, such **Triggering Event**, but in all events no later than the expiration of the latest **Successive AIG Policy**. Such notice must be in writing (including by e-mail) and must:

A. include the Policy Number set forth in the Declarations; and
B. identify the **Coverage Type(s)** the **Insureds** believe may be implicated and fully describe what is known about, and the circumstances surrounding, the **Security Failure** and **Triggering Event**, including the relevant times, places and actual or suspected causes of such **Security Failure** and **Triggering Event**.

If written notice of a **Triggering Event** and **Security Failure** has been given to the **Insurer** in accordance with this Clause 6. then each and every **Related Event** shall be considered to have been reported at the time the first such notice was given.

Any notice to the **Insurer** relating to coverage for a **Triggering Event** must be to the **Insurer** by mail or e-mail to the **Claims Notice** addresses provided in the Declarations. Any other notice to the **Insurer** must be by mail to the **Insurer's Address**.

Cooperation

For each **Coverage Type**, each **Insured** shall, at a minimum, have the same obligation to cooperate with the **Insurer** under this policy as they have to the insurer of the **Followed Policy**. Also, the **Insureds** shall provide the **Insurer** with such information, assistance and cooperation as the **Insurer** may reasonably request and the **Insureds** shall not do anything that prejudices the **Insurer's** rights under this policy. Such rights include the right to enforce any legal rights an **Insured** or the **Insurer** may have, including executing any documents that the **Insurer** deems necessary to secure such rights.

Cyber Event Response Proof of Loss

As a condition precedent to any obligation to pay under the *Cyber Event Response Coverage* of this policy, the **Insurer** must be provided with a written, detailed proof of loss, signed and affirmed by an **Entity Insured**, and delivered to the **Insurer**, no later than ninety (90) days (unless such period has been extended by the **Insurer** in writing) after it appears reasonably likely that this policy may be required to make an **Event Response Cost** payment.

The proof of loss must include, among other pertinent information: (A) a detailed calculation of known, and an estimate of any additional, **Event Response Costs**; and (B) all documents and materials that reasonably relate to or form any part of the proof of such **Event Response Costs**. Each **Insured** shall, upon the **Insurer's** request, submit to an examination under oath.

AIG

7. DEFENSE AND SETTLEMENT

No Duty to Defend

The **Insurer** does not assume any duty to defend regardless of whether an **Underlying Insurer** has the right and duty to defend any suit, claim or other matter pursuant to the terms and conditions of such insurer's policy. The **Insurer** shall not be required to assume the defense of any suit, claim or matter under this policy.

Right to Tender Defense

Notwithstanding the foregoing, if *Cyber DIC Coverage* is the only valid and collectible coverage that responds to a **Triggering Event**, the **Insureds** shall have the right to tender to the **Insurer** the defense of any suit or formal legal proceeding, including any administrative proceeding, mediation or arbitration, but not any investigation or inquiry, arising out of such **Triggering Event**. This right only can be exercised in writing by the **Policyholder** on behalf of all **Insureds**, and such assumption will become effective at point in time when written confirmation of such assumption has been sent by the **Insurer** to the **Policyholder**.

This right to tender defense to the **Insurer** will terminate if:

(i) not exercised by the **Policyholder** within sixty (60) days after the first **Insured** becomes aware of such suit or proceeding; or

(ii) any **Insured** takes any action that prejudices, or fails to take any required action to avoid prejudicing, the rights of the **Insureds** or the **Insurer** at any time prior to the **Insurer** accepting the tender of defense.

Once any applicable **Event DIC Limit**, **Event Limit**, **Coverage Type Aggregate Limit** or the **Policy Aggregate** becomes exhausted by payment of covered amounts, the **Insurer** shall withdraw from the defense of the suit or proceeding and shall have no further obligation to provide such defense. An **Insurer's** withdrawal from the defense of such suit or proceeding shall become effective upon its tendering control of the defense to the **Insured**. The **Insurer** will not be required to pay any attorneys' fees, costs or expenses incurred after that tender or excess of any such applicable limits.

Participation

The **Insurer** shall have the same rights, privileges and protections afforded to the insurers of each **Underlying Policy**.

In the event that defense is not tendered or the **Insurer** has not assumed the defense pursuant to this Clause 7., the **Insurer** also shall have the right, but not the duty or obligation to effectively associate with the **Insureds** and/or to participate in the investigation, defense and settlement of any matter that appears to be reasonably likely to involve this policy. If the **Insurer** exercises this right, it will do so at its own expense.

Applicability

This Clause 7. is not applicable to **Event Response Costs**. Nonetheless, the **Insurer** does not, with respect to *Cyber Event Reponse Coverage*, assume any duty to defend.

AIG

8. GENERAL TERMS AND CONDITIONS

Action Against Insurer

No action shall lie against the **Insurer** unless, as a condition precedent thereto, there shall have been full compliance with all of the terms and conditions of this policy, or until the amount of the **Insured's** obligation to pay shall have been finally determined either by judgment against such **Insured** after actual trial and any appeal or by written agreement of the **Insured**, the claimant and the **Insurer**.

Any **Insured** or the legal representative thereof who has secured such final judgment or written agreement shall thereafter be entitled to recover under this policy solely to the extent of the insurance afforded by this policy. No person or organization shall have any right under this policy to join the **Insurer** as a party to any action against any **Insured** or **Entity Insured** to determine the **Insured's** liability, nor shall the **Insurer** be impleaded by any natural person **Insured**, his or her spouse or legally recognized domestic partner, any **Entity Insured** or any legal representative of the foregoing.

Alternative Dispute Resolution

For each **Coverage Type**, this policy shall follow form to any alternative dispute resolution provision set forth in the applicable **Followed Policy** for that **Coverage Type** and the **Insurer** will have the same rights and privileges as afforded to the **Underlying Insurers**. In the event any dispute involves more than one **Coverage Type**, the **Policyholder**, on behalf of all **Insureds**, will select one of the potentially applicable alternative dispute resolution provisions to be used to resolve such dispute.

Assignment

This policy and any and all rights hereunder are not assignable without the prior written consent of the **Insurer**.

Authority

The **Policyholder** shall act on behalf of each and every **Insured** with respect to tendering any defense pursuant to Clause 7. *Defense and Settlement*, the giving and receiving of notice of cancellation or non-renewal, the payment of any premiums and the receiving of any return premiums that may become due under this policy, the receipt and acceptance of any endorsements issued to form a part of this policy.

Cancellation

A. *By the Policyholder:* This policy may be canceled by the **Policyholder** at any time only by mailing written prior notice to the **Insurer** at the **Insurer Address** or by surrender of this policy to the **Insurer** or its authorized agent.

B. *By the Insurer:* This policy may be canceled by the **Insurer's** delivering to the **Policyholder** by registered, certified, other first class mail or other reasonable delivery method, at the **Policyholder Address**, written notice stating when, not less than sixty (60) days thereafter (ten (10) days in the event of cancellation for non-payment of premium), the cancellation shall be effective. Proof of mailing or delivery of such notice as aforesaid shall be sufficient proof of notice and this policy shall be deemed canceled as to all **Insureds** at the date and hour specified in such notice.

C. *Return of Premium:* The **Insurer** shall have the right to the premium amount for the portion of the **Policy Period** during which the policy was in effect. If the **Policyholder** shall cancel this policy, the **Insurer** shall retain the *pro rata* proportion of the premium hereon.

Conformance To Law

Coverage under this policy shall not be provided to the extent prohibited by any applicable law.

Headings

The descriptions in the headings and any subheadings of this policy are solely for convenience, and form no part of the terms and conditions of coverage.

AIG

8. GENERAL TERMS AND CONDITIONS (Continued)

Maintenance of Underlying Insurance and Changes

The **Insureds** agree that during the **Policy Period**:

A. each **Underlying Policy** will be kept in full force and effect;

B. the terms, definitions, conditions, exclusions and limitations of the **Underlying Policy** will not materially change;

C. the **Limit of Insurance** of each **Underlying Policy** will not decrease, except for any reduction or exhaustion of aggregate limits by payment of covered amounts thereunder; and

D. any renewals or replacements of an **Underlying Policy** will provide equivalent coverage to and afford limits of insurance equal to or greater than the policy being renewed or replaced.

If any **Insured** fails to comply with these requirements, the **Insurer** will be liable only to the same extent that the **Insurer** would have been, had the **Insured** fully complied with these requirements.

If during the **Policy Period** of this policy, the terms, definitions, conditions, exclusions or limitations of any **Underlying Policy** are modified or changed in any manner from those in effect at the inception of this policy, the **Policyholder** and the **Insureds** shall, as a condition precedent to their rights under this policy, give to the **Insurer** as soon as practicable written notice of the full particulars thereof. This policy shall become subject to any such changes upon the effective date of the changes in the **Underlying Policy**, but only upon the condition that the **Insurer** agrees in writing to follow such changes, and the **Insured** agrees to any additional premium or amendment of the provisions of this policy required by the **Insurer** relating to such changes. Any change in coverage is conditioned upon the **Insured's** payment when due of any additional premium required by the **Insurer** relating to such changes.

Other Insurance

The insurance provided by this policy shall apply only as excess over any other valid and collectible insurance, unless such other insurance is specifically written as excess insurance over either the **Policy Aggregate** or a **Coverage Type Aggregate Limit** of this policy. Nothwithstanding the foregoing, *Cyber Event Response Coverage* is written as primary insurance, except when any **Underlying Policy** has cyber event response coverage, in which case *Cyber Event Response Coverage* in this policy shall be excess to such other cyber event response coverage.

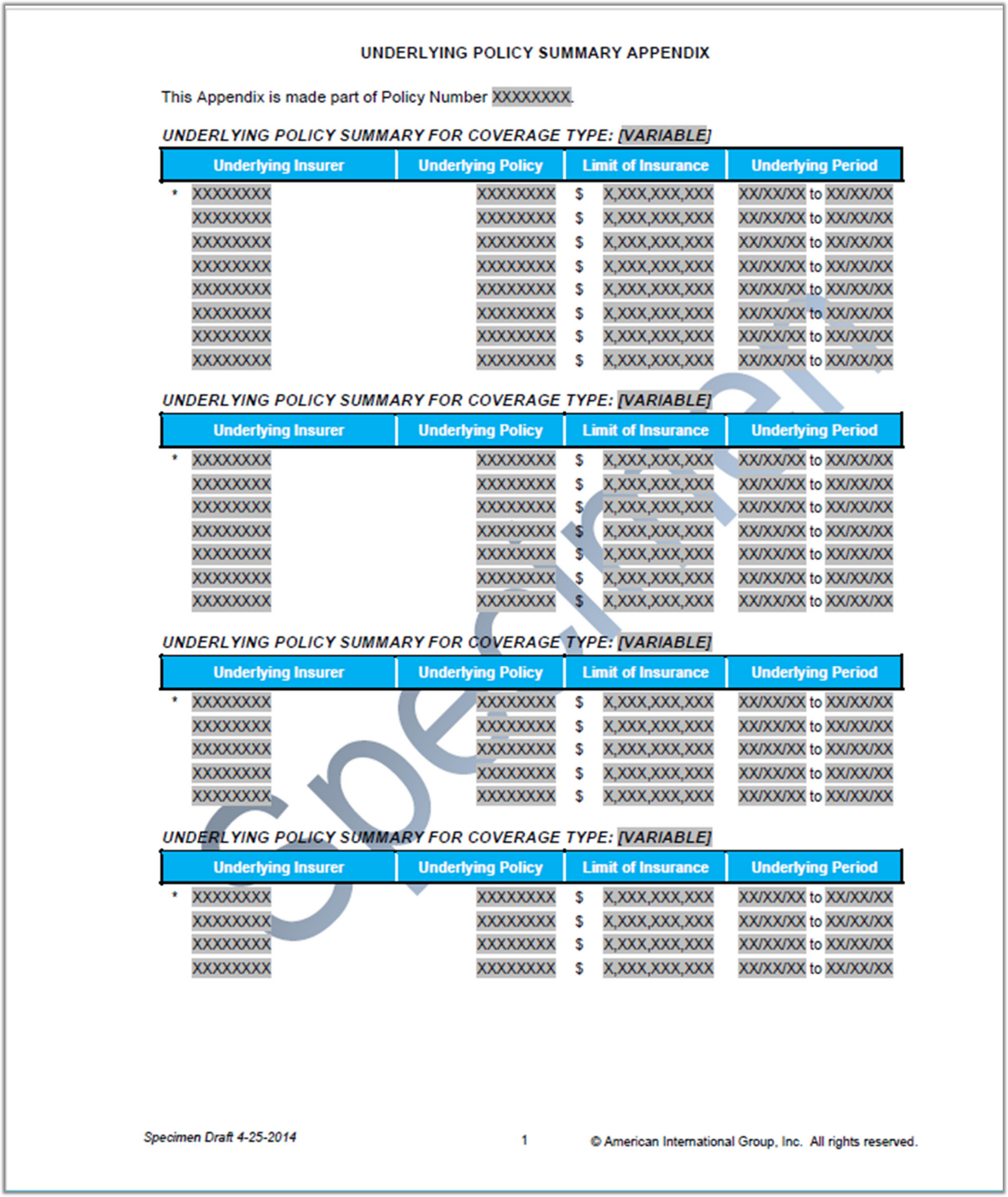
Subrogation

To the extent of any payment under this policy, the **Insurer** shall be subrogated to all of the **Insureds'** rights of recovery. Each **Insured** must do all that is possible to preserve any such rights of recovery and do whatever is necessary, including signing documents to help the **Insurer** obtain that recovery.

IN WITNESS WHEREOF, the **Insurer** has caused this policy to be signed below by its President, Secretary and its duly authorized representative.

PRESIDENT	SECRETARY	AUTHORIZED REPRESENTATIVE
COUNTERSIGNATURE (WHERE REQUIRED BY LAW)	DATE	COUNTERSIGNATURE LOCATION

Specimen Draft 4-25-2014 9



UNDERLYING POLICY SUMMARY APPENDIX

This Appendix is made part of Policy Number XXXXXXXX.

UNDERLYING POLICY SUMMARY FOR COVERAGE TYPE: [VARIABLE]

Underlying Insurer	Underlying Policy	Limit of Insurance	Underlying Period
* XXXXXXXX	XXXXXXXX	$ X,XXX,XXX,XXX	XX/XX/XX to XX/XX/XX
XXXXXXXX	XXXXXXXX	$ X,XXX,XXX,XXX	XX/XX/XX to XX/XX/XX
XXXXXXXX	XXXXXXXX	$ X,XXX,XXX,XXX	XX/XX/XX to XX/XX/XX
XXXXXXXX	XXXXXXXX	$ X,XXX,XXX,XXX	XX/XX/XX to XX/XX/XX
XXXXXXXX	XXXXXXXX	$ X,XXX,XXX,XXX	XX/XX/XX to XX/XX/XX
XXXXXXXX	XXXXXXXX	$ X,XXX,XXX,XXX	XX/XX/XX to XX/XX/XX
XXXXXXXX	XXXXXXXX	$ X,XXX,XXX,XXX	XX/XX/XX to XX/XX/XX
XXXXXXXX	XXXXXXXX	$ X,XXX,XXX,XXX	XX/XX/XX to XX/XX/XX

UNDERLYING POLICY SUMMARY FOR COVERAGE TYPE: [VARIABLE]

Underlying Insurer	Underlying Policy	Limit of Insurance	Underlying Period
* XXXXXXXX	XXXXXXXX	$ X,XXX,XXX,XXX	XX/XX/XX to XX/XX/XX
XXXXXXXX	XXXXXXXX	$ X,XXX,XXX,XXX	XX/XX/XX to XX/XX/XX
XXXXXXXX	XXXXXXXX	$ X,XXX,XXX,XXX	XX/XX/XX to XX/XX/XX
XXXXXXXX	XXXXXXXX	$ X,XXX,XXX,XXX	XX/XX/XX to XX/XX/XX
XXXXXXXX	XXXXXXXX	$ X,XXX,XXX,XXX	XX/XX/XX to XX/XX/XX
XXXXXXXX	XXXXXXXX	$ X,XXX,XXX,XXX	XX/XX/XX to XX/XX/XX
XXXXXXXX	XXXXXXXX	$ X,XXX,XXX,XXX	XX/XX/XX to XX/XX/XX

UNDERLYING POLICY SUMMARY FOR COVERAGE TYPE: [VARIABLE]

Underlying Insurer	Underlying Policy	Limit of Insurance	Underlying Period
* XXXXXXXX	XXXXXXXX	$ X,XXX,XXX,XXX	XX/XX/XX to XX/XX/XX
XXXXXXXX	XXXXXXXX	$ X,XXX,XXX,XXX	XX/XX/XX to XX/XX/XX
XXXXXXXX	XXXXXXXX	$ X,XXX,XXX,XXX	XX/XX/XX to XX/XX/XX
XXXXXXXX	XXXXXXXX	$ X,XXX,XXX,XXX	XX/XX/XX to XX/XX/XX
XXXXXXXX	XXXXXXXX	$ X,XXX,XXX,XXX	XX/XX/XX to XX/XX/XX

UNDERLYING POLICY SUMMARY FOR COVERAGE TYPE: [VARIABLE]

Underlying Insurer	Underlying Policy	Limit of Insurance	Underlying Period
* XXXXXXXX	XXXXXXXX	$ X,XXX,XXX,XXX	XX/XX/XX to XX/XX/XX
XXXXXXXX	XXXXXXXX	$ X,XXX,XXX,XXX	XX/XX/XX to XX/XX/XX
XXXXXXXX	XXXXXXXX	$ X,XXX,XXX,XXX	XX/XX/XX to XX/XX/XX
XXXXXXXX	XXXXXXXX	$ X,XXX,XXX,XXX	XX/XX/XX to XX/XX/XX

Specimen Draft 4-25-2014 1

Source: http://www.aig.com/business/insurance/cyber-insurance