Office of Superintendent of Schools
Board Meeting of June 18, 2014

June 4, 2014

Financial Services
Richard H. Hinds, Chief Financial Officer

SUBJECT: **REQUEST AUTHORIZATION TO PURCHASE CYBER LIABILITY INSURANCE COVERAGE**

COMMITTEE: **INNOVATION, EFFICIENCY, AND GOVERNMENTAL RELATIONS**

LINK TO STRATEGIC FRAMEWORK: **FINANCIAL EFFICIENCY/STABILITY**

At the Board Meeting of December 15, 2010, the Board awarded its Property and Casualty Insurance Broker Services contract to Arthur J. Gallagher Risk Management Services, Inc. (Gallagher), pursuant to Request For Qualifications (RFQ) #004-LL10, Request For Qualifications for Property and Casualty Insurance Broker Services, effective January 1, 2011. As such, the following recommended insurance placement is subject to the brokerage contract's provisions.

As was highly publicized this past holiday season, retailer Target suffered a data breach to their computer system resulting in theft of consumers' financial information, including credit card-card numbers, personal identification numbers, and e-mail addresses of 110 million customers. Soon thereafter, department store Neiman Marcus suffered a similar breach which affected as many as 350,000 thousand consumer records. According to USA Today, Target is expected to lose 5-10% of its client base as a result of this significant data breach.

Data breaches are not limited to retail businesses. In fact, several colleges as well as a local hospital have reported significant data breaches.

According to the Department of Justice, credit-card data theft surged 50 percent between 2005 and 2010 and is likely to increase. President Barack Obama has stated that "Cyber threats pose one of the gravest national security dangers that the United States faces." President Obama also instructed the National Institute of Standards and Technology (NIST) to develop national voluntary industry standards and best practices to prevent cyber attacks. The NIST published the "Framework for Improving Critical Infrastructure Cyber Security."

E-70

The Framework was created through a strategic collaboration between the government and the private sector. It was noted that the Framework should be used to complement an organization's risk management and cyber security program.

Any entity which hosts a website; conducts e-transactions; or stores personally identifiable information is at risk of a data breach. Based on the ever evolving exposure associated with living in the digital age, it is incumbent upon a proactive risk management program to perform its due diligence regarding this exposure. The Department of Information Technology (ITS) has already implemented many of the guidelines that are described in the Framework which are considered best practices to insulate the District from cyber risks. However, even with cyber security measures in place there are always risks associated with human error, theft, a lost laptop, phone or USB device which holds student or employee information. The compromise of such devices could expose the district to a significant data breach.

It is for these reasons that staff from various departments, including the Office of Risk and Benefits Management, ITS, The Department of Finance, and School Operations met to discuss the issue and it was determined that the district should explore the possibility of purchasing a cyber liability policy. Typical cyber liability policies provide the following coverages:

- Multimedia Liability - Allegations your internet site or printed media cause defamation, libel slander or harm to reputation of others.
- Security or Privacy Liability - Failing to prevent or hinder unauthorized access of your computer system and the confidential material thereon such as the loss of employee and student information and the transmissions of malicious codes to others.
- Privacy and Regulatory Defense and Penalties
- Privacy Breach Response Costs - Customer Support and credit monitoring
- Network Asset Protection – Restoring, updating or replacing digital assets to a level beyond that which existed prior to a loss.
- Cyber Extortion - Covers expense and money losses in the event of cyber extortion
- Cyber Terrorism - Expenses and losses as a result of cyber terrorism
- Crisis Management – Provide expertise on a pre and post loss basis on behalf of the insured including public relations

Following a review of the risk the District has from potential cyber exposures, staff requested that Gallagher obtain quotes with various limits and self-insured retention levels. Quotes were received from ACE, Beazley, Brit-Lloyd's and AIG. Staff narrowed down the quotes to ACE and Britt based on coverage options and premiums.

Quote Comparison

	ACE	BRIT Lloyd's
$3M Limit Premium (Per Claim/Annual Aggregate)	$71,688	$76,450
$5M Limit Premium (Per Claim/Annual Aggregate)	$108,772	$93,925
$10M Limit Premium (Per Claim/Annual Aggregate)	$154,136	$139,500
Coverages		
Media Liability	Not Included	Policy Limit
Security and Privacy Liability	Policy Limit	Policy Limit
Regulatory Action Sublimit	$1,000,000 – $3M opt $2,000,000 – $5M opt $2,500,000 – $10M opt	Policy Limit
PCI Fines and Costs Sublimit	$1,000,000	$1,000,000
Crisis Management & PR Sublimit ACE-Data Breach Fund Beazley-Privacy Breach Response Brit-Security Breach Response AIG-Event Mngt./Electronic Data *Notification, Credit Monitoring, ID Theft Services, Forensics, Legal & PR Expenses*	**$3M opt.** $1,000,000 Agg Tier 1: $500,000 Tier 2: $1,000,000 **$5M opt.** $2,500,000 Agg. Tier 1: $1,000,000 Tier 2: $2,500,000 **$10M opt.** $3,000,000 Agg. Tier 1: $1,000,000 Tier 2: $3,000,000	Policy Limit
Cyber Extortion	Policy Limit	Policy Limit
Retentions		
Each Claim (or Breach)	$250,000 - $3M opt $500,000 - $5M opt ($250k Data Breach) $500,000 - $10M opt	$250,000

The original team which met to discuss the exposures, convened to review received quotations for Cyber Liability Insurance. Following a detailed analysis of these quotes, staff is recommending purchase of Cyber Liability Coverage with Brit-Lloyd's (A.M. Best A, XV) through Arthur J. Gallagher Risk Management Services, Inc., consisting of a coverage limits of $10 million per claim/annual aggregate subject to a $250,000 self-insured retention with an annual premium of $141,313.50 inclusive of 1.3% Florida Hurricane Assessment Fee, for a one-year period effective July 1, 2014 thru June 30, 2015. It is recommended that funds from the District's self insured general/automobile/professional liability account be used for payment of this insurance premium.

One of the main reasons for this recommendation is that the Brit quotation was not only more comprehensive; but key elements including Crisis Management, Notification, Credit Monitoring, ID Theft Services, Forensics and Legal and Public Relations expenses were not subject to a sub-limit of coverage. Also, many entities are experiencing recommendations from external auditors to purchase cyber liability insurance, when it is determined that the entity has significant cyber exposures.

Most recently, a District employee was arrested with two others on charges of stealing about 400 student identities from several high schools and filing more than 200 fraudulent tax returns. More so than ever, staff believes that the District is susceptible to future cyber losses and it is in the best interest of the District to protect itself with a specific insurance program to cover this exposure.

RECOMMENDED: That The School Board of Miami-Dade County, Florida, authorize the purchase of cyber liability coverage with Brit-Lloyd's (A.M. Best A, XV) Arthur J. Gallagher Risk Management Services, Inc. with coverage limits of $10 million per claim/annual aggregate subject to a $250,000 self-insured retention with an annual premium of $141,313.50 inclusive of a 1.3% Florida Hurricane Assessment Fee for a one-year period effective July 1, 2014 thru June 30, 2015.

RHH:sc