

**Statement of  
Stephanie Reich, Manager, State Government Relations  
Symantec Corporation**

**March 7, 2008**

**Before the Connecticut Joint Committee on Energy & Technology  
H.B. 5816**

Good Morning Chairman Fonfara, Chairman Fontana and members of the Joint Committee on Energy and Technology, thank you for the opportunity to testify. My name is Stephanie Reich and I manage state government relations for Symantec's Northern and Great Lakes Region. I am pleased to be here today to support H.B. 5816 An Act Concerning Internet Security and share with you Symantec's comments regarding the importance of this Bill. H.B. 5816 specifically addresses state agency information security management. It requires the development of policies, procedures and standards for assessing security risks, determining the appropriate security measures, and performing security audits of government electronic information. It also requires annual reviews of information security plans as well as provides strong compliance enforcement powers.

Symantec is the world leader in providing solutions to help individuals, governments and other enterprises assure the security, availability, and integrity of their information. As well as secure and manage their IT infrastructure. We are the fourth largest software company in the world. Headquartered in Cupertino, California, Symantec has operations in more than 40 countries. Here in the U.S., we have facilities in several states, including Florida, California, Virginia, Oregon, Minnesota, Texas, Colorado and Washington and an office here in Connecticut.

As you aware, State government has a duty to residents to ensure that the information entrusted to public agencies is safe, secure, and protected from unauthorized access, unauthorized use, or destruction. However, the pace of government operations has never been faster, and unscheduled downtime can often be an unpleasant fact of life. While some research firms have determined that the majority of downtime is planned, it is the unplanned downtime that causes the most significant, if not catastrophic, interruptions in operations. Hurricane Katrina and other recent natural disasters have underscored the need for effective continuity of operations (COOP) planning.

We often think about disaster prevention and recovery in terms of issues like delivering medicine and meeting health care needs in the event of a disaster, removing debris from roadways, providing shelter to displaced residents, or swiftly evacuating residents. However, as legislators you should also be thinking about how robust and secure Connecticut's IT infrastructure is. (Attached please find Eight Questions a Legislator Should Ask Their CIO)

But what does it mean to have a better disaster recovery plan for information?

Often it may mean more operations centers, more secure operations centers, more disaster-proof operations centers from tornadoes, hurricanes, ice storms, earthquakes, floods, etc. It also means more staff and more equipment, all of which is established for back-up systems in case of failure and to save data or to re-route the flow of information from one center to another.

Every government agency, function and capability is reliant on IT systems. The ability of government organizations to accomplish their missions and objectives in spite of unforeseen events hinges on safeguarding government-held information and ensuring the effective operation of their IT assets and systems at all times.

Think about the volume of sensitive data Connecticut maintains, the number of tax records Connecticut stores electronically, health records, DMV records, marriage, birth and other vital records, payroll for your state employees....the list goes on.

The questions for you as legislators are, “does your state have an effective plan to ensure continuity of government operations? Are the plans being regularly tested, and are they being regularly updated? In the event of a disruption of the state’s IT systems, how will the state get the systems up and running to ensure basic government needs are met?”

Additionally, are your Connecticut’s networks adequately protected against hacking, malicious software attacks, or some other breach in the state’s networks? And are the state’s networks adequately protected against natural disasters like floods, hurricanes or earthquakes?

The risks associated with widespread data loss or state IT systems shutting down is so high, legislators like you need to assume a leadership role in ensuring that key data will not be lost and IT systems will keep running, even in the event of a severe and prolonged disruption. Recent studies have indicated that more than 25% of the breaches to date have been from government agencies, many of which were at the state level.

The physical threats to government operations are as vast as we can imagine – hurricanes, tornadoes, floods, earthquakes, terrorist attacks. These threats can have a devastating impact on government IT systems.

But what about cyber attacks? What is Connecticut doing in terms of prevention, remediation, and recovery from intrusions, attacks and data loss on your IT systems?

Every six months, Symantec puts out our Internet Security Threat Report (ISTR) (Attached), which provides a comprehensive analysis of the emerging threats and trends on the Internet. The report data is obtained from 50,000 sensors worldwide monitoring network activity in 180 countries, More than 120 million client, server, and gateway antivirus systems, 250 million e-mail accounts and 2 million decoy honeypot e-mail accounts.

The most recent ISTR found that while past attacks were designed to destroy data, today’s attacks are increasingly designed to silently steal data for profit. For example, as we’ve seen in previous reports, malicious code for profit is on the rise. We saw malicious code threats that could reveal confidential information rise from 74 percent of the top 50 malicious code samples last period to 80 percent this period.

Threats to confidential information can be present in almost any type of malicious code, including Trojan horses, worms, and viruses. Many worms and Trojans contain keystroke-logging and back door functionality in addition to their other components.

Phishing attacks are becoming more sophisticated. Consumers are now seeing phishing emails coming from trusted email addresses and ISP accounts. Attackers are spoofing charitable sites (i.e. American Red Cross), and taking advantage of consumers when they are most vulnerable and trusting. You may be aware of the recent national Cyber Initiative that was just announced in January 2008. Due to recent malicious threats to U.S. federal government systems, this federal

initiative has been developed to protect federal government networks from future intrusions and cyber attack.

State government networks are just as much at risk.

While there is no silver bullet solution, there are many things legislators can do. What is most important is that any state disaster preparedness and recovery plan include activities aimed at ensuring the state's IT systems stay up and running to ensure basic government needs are met. This requires a coordinated effort and cooperation among all levels of government and the private sector.

There are three general areas with regards to Connecticut's IT systems to think about: prevention, remediation, and recovery.

**1. Prevention:**

Protect against and prevent data loss and downtime. Assess the threats, and implement security policies to guard against these threats.

Ensure data and systems are protected yet remain accessible wherever, whenever, and to whomever operational needs dictate.

**2. Remediation:**

Fix the problem. Identify systems to patch, isolate the points of attack, the application failures, and the data loss.

**3. Recovery:**

Restore data and recover application services.

Unplanned-for incidents can require a continuum of restorative operations. Some events may require a complete restoration of the IT infrastructure, while other incidents may require the restoration of only pieces of the infrastructure.

Many of these responsibilities lie with Connecticut's CIO, but it is up to legislators to ensure Connecticut is implementing effective strategies and dedicating adequate resources to prevent, remediate, and recover from security risks and downtime of applications and data.

Look to the states of Oregon, Virginia, Texas and Colorado, which just passed some of the most comprehensive information security laws in the nation.

For example, Colorado state lawmakers, led by Senator Ron May, approved information security legislation for the state of Colorado. Modeled after the Federal Information Security Management Act (FISMA), the bill does the following:

- a. establishes a state Chief Information Security Officer (responsible for reporting directly to the Governor);
- b. requires all agencies to come up with a comprehensive security plan, which will include ongoing security assessments, a process for ensuring security, regular training, reporting and responding to incidents, and plans to ensure the continuity of information resources;
- c. if agencies fail to comply with the development of a plan or the plan does not get approved by the state CISO, the CISO has the authority to discontinue or suspend the operations of the agency's information resources;

- d. requires annual reporting by the agencies, and quarterly reporting by the CISO to the Governor and legislature;
- e. gives the CISO review powers of agency security budgets; and
- f. authorizes the CISO to enter into contracts with private entities to assist with resolving security incidents.

Finally, to assist state agencies in the development of their security plans, we recommend the following provisions (several of which are included already in H.B. 5816) be included in any information security plan:

- (1) Periodic assessments of the risk and magnitude of the harm that could result from a security incident;
- (2) A process for providing adequate information security for the communication and information resources of the agency;
- (3) Periodic security awareness training to inform the employees and users of the agency's communication and information resources about information security risks and the responsibility of employees and users to comply with agency policies, standards, and procedures designed to reduce those risks;
- (4) Periodic vulnerability assessment testing and evaluation of the effectiveness of information security for the agency, to be performed not less than annually;
- (5) A process for detecting, reporting, and responding to security incidents consistent with information security standards, policies, and guidelines issued by the chief information security officer; and
- (6) Plans and procedures to ensure the continuity of operations for information resources that support the operations and assets of the agency in the event of a security incident

State legislators can play a leading role in ensuring that your state disaster preparedness and recovery plans include activities aimed at ensuring the continuity of Connecticut's IT systems in order to ensure basic government needs are met.

With me is Lou Zeidman, Regional Manager of Solutions with SYMANTEC Corporation. In this role Lou supports the sales, marketing and strategic relationships with customers and partner organizations. Lou's Compliance work focuses on enabling organizations to effectively and efficiently manage IT risk through a consistent and repeatable process of definition, distribution, assessment, enforcement and remediation of organization policy and IT controls. Additionally, Lou develops and provides executive level management strategies for Government operations that focus on the placement, integration and interoperability of complex business applications, as well as compliance for records management.

Symantec looks forward to working with you as Connecticut moves forward on this important piece of legislation.