

2007

**SENATE
INFORMATION
TECHNOLOGY**

MINUTES



Senate Information Technology Committee

Co-Chairman	Sen. Janet Cowell
Co-Chairman	Sen. Katie G. Dorsett
Vice Chairman	Sen. Malcolm Graham

Members	Sen. Tom Apodaca
	Sen. Doug Berger
	Sen. Philip E. Berger
	Sen. Andrew C. Brock
	Sen. Tony Foriest
	Sen. Steve Goss
	Sen. Fletcher L. Hartsell, Jr.
	Sen. John H. Kerr III
	Sen. Robert Pittenger
	Sen. Joe Sam Queen

ATTENDANCE

Committee: Information Technology (Senate)

NAME	Meeting: April 18, '07	Meeting: May 2, '07	Meeting: June 20, '07
Sen. Janet Cowell, Co-Chair	X	X	X
Sen. Katie Dorsett, Co-Chair		X	X
Sen. Malcolm Graham, Vice Chair	X		X
Sen. Tom Apodaca	X		X
Sen. Doug Berger	X	X	
Sen. Phil Berger			
Sen. Andrew Brock	X	X	X
Sen. Tony Foriest		X	X
Sen. Steve Goss	X	X	X
Sen. Fletcher Hartsell			
Sen. John Kerr	X		X
Sen. Robert Pittenger	X	X	X
Sen. Joe Sam Queen	X		X
Karlynn O'Shaughnessy, Fiscal Staff	X	X	X
Brenda Carter, Research Staff	X	X	X
Peter Capriglione, ISD Staff	X	X	X
Phyllis Cameron, Committee Asst.			
Cindy Garrison, Committee Asst.	X	X	X

Principal Clerk
Reading Clerk

SENATE
NOTICE OF COMMITTEE MEETING
AND
BILL SPONSOR NOTICE

The Senate Committee on **Information Technology** will meet at the following time:

DAY	DATE	TIME	ROOM
Wednesday	April 18, 2007	12:00 p.m.	1124 LB

The following will be considered:

BILL NO.	SHORT TITLE	SPONSOR
S876	Agency/State CIO Dispute Resolution	Cowell/ Dorsett
S878	ITS/Employee Background Investigations	Cowell/ Dorsett
S879	ITS Project Management.	Cowell/ Dorsett

Senator Janet Cowell, Co-Chair
Senator Katie Dorsett, Co-Chair
Senator Malcolm Graham, Vice-Chair

SENATE INFORMATION TECHNOLOGY COMMITTEE
Wednesday, April 18, 2007

AGENDA

Welcome and Opening Remarks

Introduction of Pages

Bills

SB 876	Agency/State CIO Dispute Resolution	Cowell / Dorsett
SB 878	ITS/Employee Background Investigations	Cowell / Dorsett
SB 879	ITS Project Management	Cowell / Dorsett

Presentations

Other Business

Adjournment

SENATE VISITOR REGIST
Information & Tech

Date _____

4-18-07

VISITORS: PLEASE SIGN BELOW AND RETURN TO COMMITTEE ASSISTANT -

FORM OR AGENCY -

JAMES L. FORTE	OSA
PAUL SAKSA	OSA
George Bakolia	Governor's office
NANCY LOWE	DOS
Eric Hamilton	NC Tech. Assoc.
Sarah Preston	ACLU-NC
Gary Kearney	NC Dept Juvenile Justice
Angie Harris	Williams Muller
Fred Aikens	The Aikens Group LLC
Ron McCorquodale	SAS
Danny Lindsey	ITS
Emily Atkinson	Postnet
Judy McConnell	IOG
Donna	S.A.
TANIEC PRUN	RLC
Carri Cree	BPMHL
Webb	SS

Senate Standing Committee
on
Information Technology
Wednesday, April 18, 2007 at 12:00 p. m.
Room 1124 - Legislative Building

MINUTES

The Senate Standing Committee on Information Technology met at 12:00 p.m. on April 18, 2007, in Room 1124 of the Legislative Building. Ten members of the Committee were present. Senator Janet Cowell, Co-Chair, presided.

Senator Cowell welcomed members and guests, and asked members to introduce themselves. She announced names of the Senate Pages in attendance: Cliff Howell of Murphy, sponsored by Senator John Snow and Lauren Hovis of Pffafftown, sponsored by Senator Peter Brunstetter. Also present were General Assembly staff members Karlin O'Shaughnessy, of Fiscal Research and Peter Capriglione, of the Information Systems Division.

Senator Cowell recognized Co-Chair, Senator Katie Dorsett to preside in her place as a Cowell-sponsored bill was under consideration. Senator Dorsett introduced SB 876, Agency/State CIO Dispute Resolution and called State Chief Information Officer (CIO) George Bakolia to speak to the bill. After discussion, Senator Tom Apodaca moved adoption of the bill and the motion carried.

Senator Dorsett asked Mr. Bakolia to speak to the second bill on the agenda, SB 878, ITS/Employee Background Investigations. After Mr. Bakolia's presentation, Senator Dorsett recognized Senator Cowell, who said the State Employees Association of North Carolina (SEANC) supported the bill. There was discussion about the CIO office retaining information gathered in the form of background checks. Mr. Bakolia said his office could certainly clear their files of this in the interest of security as the Department of Justice retained the information, making it attainable in the event it was ever needed. Ms. Nancy Lowe of the Department of Justice offered to check on the availability of the information to the CIO ongoing. Senator Malcolm Graham moved to pass the bill. The motion carried.

Senator Dorsett introduced discussion of SB 879: ITS Project Management and Mr. Bakolia, once again, spoke to the bill. Senator Dorsett said she would entertain a motion on the bill and Senator Pittenger moved to pass the bill. The motion carried.

The meeting was adjourned at 12:21 p.m.



Senator Janet Cowell, Co-Chair



Cindy Garrison, Committee Clerk

Senator Katie Dorsett, Co-Chair

**GENERAL ASSEMBLY OF NORTH CAROLINA
SESSION 2007**

S

1

SENATE BILL 876*

Short Title: Agency/State CIO Dispute Resolution. (Public)

Sponsors: Senators Cowell; Berger of Franklin and Dorsett.

Referred to: Information Technology.

March 19, 2007

A BILL TO BE ENTITLED

AN ACT INCREASING THE AMOUNT OF TIME AN AGENCY HAS TO REQUEST A REVIEW OF A DECISION BY THE STATE CHIEF INFORMATION OFFICER TO DENY OR SUSPEND APPROVAL OF AN INFORMATION TECHNOLOGY PROJECT OR DENY A REQUEST FOR A DEVIATION.

The General Assembly of North Carolina enacts:

SECTION 1. G.S. 147-33.72D(a) reads as rewritten:

"(a) Agency Request for Review. – In any instance where the State CIO has denied or suspended the approval of an information technology project, or has denied an agency's request for deviation pursuant to G.S. 147-33.84, the agency may request a committee review of the State CIO's decision. The agency shall submit a written request for review to the State Controller within ~~10~~15 working days following the agency's receipt of the State CIO's written grounds for denial or suspension. The agency's request for review shall specify the grounds for its disagreement with the State CIO's determination. The agency shall include with its request for review a copy of the State CIO's written grounds for denial or suspension."

SECTION 2. This act is effective when it becomes law.

GENERAL ASSEMBLY OF NORTH CAROLINA

SESSION 2007

S

1

SENATE BILL 878*

Short Title: ITS/Employee Background Investigations.

(Public)

Sponsors: Senators Cowell; Berger of Franklin, Dorsett, and Rand.

Referred to: Information Technology.

March 19, 2007

A BILL TO BE ENTITLED

AN ACT MAKING EMPLOYEES AND PROSPECTIVE EMPLOYEES OF THE OFFICE OF INFORMATION TECHNOLOGY SERVICES SUBJECT TO BACKGROUND INVESTIGATIONS; EXEMPTING FROM THE PUBLIC RECORDS LAWS THE CRIMINAL HISTORIES OF AGENCY SECURITY LIAISONS AND PERSONNEL IN THE OFFICE OF STATE AUDITOR, AND MAKING CONFORMING CHANGES.

The General Assembly of North Carolina enacts:

SECTION 1. G.S. 147-33.77 is amended by adding a new subsection to read:

"(g) The State Chief Information Officer may require background investigations of any employee or prospective employee, including a criminal history record check, which may include a search of the State and National Repositories of Criminal Histories based on the person's fingerprints. A criminal history record check shall be conducted by the State Bureau of Investigation upon receiving fingerprints and other information provided by the employee or prospective employee. If the employee or prospective employee has been a resident of the State for less than five years, the background report shall include a review of criminal information from both the State and National Repositories of Criminal Histories. The criminal background report shall be provided to the State Chief Information Officer and is not a public record under Chapter 132 of the General Statutes."

SECTION 2. G.S. 147-33.113(a)(4) reads as rewritten:

"(4) Designating an agency liaison in the information technology area to coordinate with the State Chief Information Officer. The liaison shall be subject to a criminal background report from the State Repository of Criminal Histories, which shall be provided by the State Bureau of Investigation upon its receiving fingerprints from the liaison. If the liaison has been a resident of this State for less than five years, the background report shall include a review of criminal information from both the State and National Repositories of Criminal Histories. The criminal background report shall be provided to the State Chief Information Officer and the head of the agency. In addition, all personnel in the Office of State Auditor who are responsible for information technology security reviews pursuant to G.S. 147-64.6(c)(18) shall be subject to a criminal background report from the State Repository of Criminal Histories, which shall be provided by the State Bureau of Investigation upon receiving fingerprints from the personnel designated by the State Auditor. For

designated personnel who have been residents of this State for less than five years, the background report shall include a review of criminal information from both the State and National Repositories of Criminal Histories. The criminal background reports shall be provided to the State Auditor. Criminal histories provided pursuant to this subdivision are not public records under Chapter 132 of the General Statutes."

SECTION 3. Article 4 of Chapter 114 of the General Statutes is amended by adding a new section to read:

"§ 114-19.20. Criminal record checks for the Office of Information Technology Services.

(a) The Department of Justice may provide to the Office of Information Technology Services from the State and National Repositories of Criminal Histories the criminal history of any current or prospective employee, volunteer, or contractor of the Office of Information Technology Services. The Office of Information Technology Services shall provide to the Department of Justice, along with the request, the fingerprints of the current or prospective employee, volunteer, or contractor, a form signed by the current or prospective employee, volunteer, or contractor consenting to the criminal record check and use of fingerprints and other identifying information required by the State and National Repositories, and any additional information required by the Department of Justice. The fingerprints of the current or prospective employee, volunteer, or contractor shall be forwarded to the State Bureau of Investigation for a search of the State's criminal history record file, and the State Bureau of Investigation shall forward a set of fingerprints to the Federal Bureau of Investigation for a national criminal history record check. The Office of Information Technology Services shall keep all information obtained pursuant to this section confidential.

(b) The Department of Justice may charge a fee to offset the cost incurred by it to conduct a criminal record check under this section. The fee shall not exceed the actual cost of locating, editing, researching, and retrieving the information."

SECTION 4. This act is effective when it becomes law.

GENERAL ASSEMBLY OF NORTH CAROLINA
SESSION 2007

S

1

SENATE BILL 879*

Short Title: ITS Project Management.

(Public)

Sponsors: Senators Cowell; Berger of Franklin and Dorsett.

Referred to: Information Technology.

March 19, 2007

A BILL TO BE ENTITLED

AN ACT PROVIDING FOR ADDITIONAL PROJECT MANAGERS ON
INFORMATION TECHNOLOGY PROJECTS AND INCREASING THE
THRESHOLD FOR THE MANDATORY DESIGNATION OF PROJECT
MANAGER ASSISTANTS BY THE STATE CHIEF INFORMATION OFFICER.

The General Assembly of North Carolina enacts:

SECTION 1. G.S. 147-33.72E reads as rewritten:

"§ 147-33.72E. Project management standards.

(a) Agency Responsibilities. – Each agency shall provide for ~~a project manager~~ one or more project managers who meets-meet the applicable quality assurance standards for each information technology project that is subject to approval under G.S. 143-33.72C(a). ~~The-Each~~ project manager shall be subject to the review and approval of the State Chief Information Officer.

~~The-Each~~ agency project manager shall provide periodic reports to the project management assistant assigned to the project by the State CIO under subsection (b) of this section. The reports shall include information regarding project costs, issues related to hardware, software, or training, projected and actual completion dates, and any other information related to the implementation of the information technology project.

(b) State Chief Information Officer Responsibilities. – The State Chief Information Officer shall designate a project management assistant from the Office of Information Technology Services for ~~projects that receive-any project that receives~~ approval under ~~G.S. 147-33.72C(a).~~ G.S. 147-33.72C(a) if the project costs or is expected to cost more than one million dollars (\$1,000,000), whether the project is undertaken in single or multiple phases or components. The State Chief Information Officer may designate a project management assistant for any other information technology project.

The project management assistant shall advise the agency with the initial planning of a project, the content and design of any request for proposals, contract development, procurement, and architectural and other technical reviews. The project management assistant shall also monitor agency progress in the development and implementation of the project and shall provide status reports to the State Chief Information Officer, including recommendations regarding continued approval of the project."

SECTION 2. This act is effective when it becomes law.

Principal Clerk _____
Reading Clerk _____

Corrected:

SENATE
NOTICE OF COMMITTEE MEETING
AND
BILL SPONSOR NOTICE

The Senate Committee on **Information Technology** will meet at the following time:

DAY	DATE	TIME	ROOM
Wednesday	May 2, 2007	12:00 Noon	1124 LB

The following will be considered:

BILL NO.	SHORT TITLE	SPONSOR
SB 112	E-NC Connectivity Incentives Funds.	Senator Malone
SB 1552	BEACON/Data Integration Funds.	Senator Cowell

Senator Janet Cowell, Co-Chair
Senator Katie G. Dorsett, Co-Chair

**SENATE INFORMATION TECHNOLOGY
COMMITTEE**

**Wednesday, May 2, 2007, 12:00 Noon
1124 Legislative Building**

AGENDA

Welcome and Opening Remarks

Introduction of Pages

Bills

SB 112	E-NC Connectivity Incentives Funds.	Senator Malone
SB 1552	BEACON/Data Integration Funds.	Senator Cowell

Presentations

Jane Patterson, Executive Director, E-NC,
NC Rural Economic Development Center
Robert Powell, North Carolina Controller

Other Business

Adjournment

VISITOR REGISTRATION SHEET

Name of Committee INFORMATION TECHNOLOGY MAY 3, 2007

VISITORS: PLEASE SIGN IN BELOW AND RETURN TO COMMITTEE CLERK

NAME

FIRM OR AGENCY AND ADDRESS

Lee Mandell	NCLM
Harold Webb	NCCOM
Joanna Wright	e-NC Authority
John Chured	Warren Co. EDC
ERNIE FLEMING	WARREN Co. COMM.
Penny McArthur Young	Franklin County Comm.
Bob Winter	Franklin County Comm.
Tom Morrow	Nenoe
Bill Randall	NCCCS
Linda Nelms	nees
Paula Joshi	SAS

VISITOR REGISTRATION SHEET

Name of Committee INFORMATION TECHNOLOGY MAY 2, 2007

VISITORS: PLEASE SIGN IN BELOW AND RETURN TO COMMITTEE CLERK

NAME

FIRM OR AGENCY AND ADDRESS

Greg Henderson	SAS
Tim Vickers	SAS
Al Coffey	Warren Co. Board of Educ.
Bill Davis	Warren County Commissioner
Ed Fody	Allen Tabor
George Bakolia	ETS
Robert Powell	OSC
Ed Turlington	SPMHL
Joan Myers	NCTA
Randy Fraser	TWC
Sam Hansen	EXPSS

VISITOR REGISTRATION SHEET

Name of Committee INFORMATION TECHNOLOGY MAY 2, 2007

VISITORS: PLEASE SIGN IN BELOW AND RETURN TO COMMITTEE CLERK

NAME

FIRM OR AGENCY AND ADDRESS

~~Loren Maynard~~

CMS

Ray V. Spain

Warren County Schools

Sarah Price

BGA

Mia Bailey

Electric Cities of NC, Inc.

Amy McConkey

Smith Anderson

Don McConkey

SAS

Ken Melton

N.C. D.O.R.

Senate Standing Committee
on
Information Technology
May 2, 2007 at 12:00 p. m.
Room 1124 - Legislative Building

MINUTES

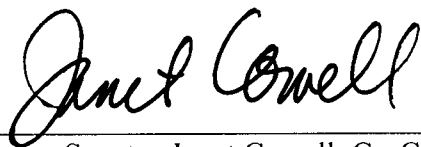
The Senate Standing Committee on Information Technology met at 12:00 PM on May 2, 2007, in Room 1124 of the Legislative Building. Seven members of the committee were present. Senator Janet Cowell, Co-Chair, presided.

Senator Cowell called the meeting to order at 12:03, welcomed members and guests and introduced Senate Pages in attendance: Vincent Brown of Durham sponsored by Senator Vernon Malone and Darien Ball of Whitakers, sponsored by Senator A. B. Swindell.

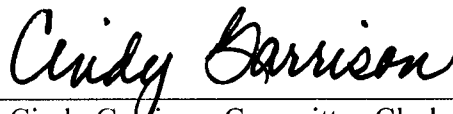
Senator Cowell introduced Senate Bill 112: E-Connectivity calling on primary sponsor, Senator Vernon Malone, to present speakers. Senator Malone introduced Ms. Jane Patterson, Executive Director, E-NC, North Carolina Rural Economic Development Center (REDC). Ms. Patterson explained the objectives of the bill and impact on rural development (See Attachment I). There was a period of questions and answers. Senator Doug Berger moved a favorable report of the bill. The motion carried.

Senator Cowell introduced Senate Bill 1552: BEACON/Data Integration Funds and as she was primary sponsor of the bill, relinquished the gavel to Co-Chair, Senator Katie Dorsett. Senator Dorsett called upon Senator Cowell to discuss the bill and introduced North Carolina State Controller Robert Powell who spoke to the particulars of the bill and took questions afterward. Senator Cowell explained a technical change in the bill requiring amendment. Senator Dorsett moved the adoption of the amendment and the motion carried. She entertained a motion for a favorable report of the bill as amended. Senator Tony Foriest made the motion, which carried.

The meeting was adjourned at 12:43.



Senator Janet Cowell, Co-Chair



Cindy Garrison, Committee Clerk

Senator Katie Dorsett, Co-Chair



Legislative Priorities

2007 Session

“Broadband enhances economic activity, helping to promote job creation both in terms of the total number of jobs and the number of establishments in communities with broadband.”

- Gillett & Sirbu,
Measuring
Broadband's
Economic Impact,
MIT and Carnegie
Mellon University,
2005

The e-NC Authority is a state authority, created by the North Carolina General Assembly under S.L. 2003-423.

A Reminder: What is The e-NC Authority?

Increasing statewide access to broadband connectivity, and paving the way for all the corresponding economic, health and educational benefits, is both the legislative mandate and tireless mission of the e-NC Authority's dedicated commissioners and staff. The work of the e-NC Authority, along with citizens and businesses of our state, has enabled North Carolina to move from a national ranking of 47 to 11 in citizens' ability to purchase broadband connectivity.

Critical disparity in high-speed Internet access and the resources it delivers remains however, with 26 rural counties significantly lagging in access to that connectivity. Since January 2001, the e-NC Authority (formerly the Rural Internet Access Authority) has led those communities toward a more competitive position where affordable broadband access can create and sustain high-value jobs and improve the quality of life. The e-NC Authority provides leadership and vision at the grassroots-level in an effort to champion and enable technology-based economic development. Creative, locally-defined and implemented projects are the sources of sustainable changes that are improving the way of life in our rural and urban distressed communities. With initial support of \$30 million from MCNC, the e-NC Authority has been successful in **leveraging over \$200 million in additional funds.**

Upcoming Goals, 2007-2008 Funding Needed:

A total expansion budget of \$10 million will be required to support initiatives identified by the e-NC Authority as being core to the success of its mission of increasing broadband connectivity and enabling technology-based economic development throughout the state.

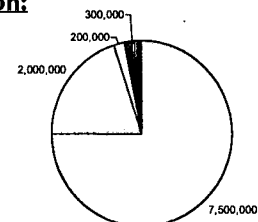
Requested Total for Expansion Initiatives - \$10 million:

NONRECURRING Funds: \$2 million

- \$2 million Business & Technology Telecenters (BTTs) Support Grants Program

RECURRING Funds: \$8 million

- \$7.5 million Connectivity Incentives Fund
- \$300,000 Operations and Research
- \$200,000 Competitive Innovation Grants Program



□ Connectivity Incentives □ BTT Support Grants
□ Competitive Innovation Grants ■ Operations & Research

What Are These Programs and How Are They Critical?

Business & Technology Telecenter (BTT) Support Grants Program funds (\$2 million nonrecurring) are requested to provide scale-up support to the four newest BTTs that were provided start-up funding by the N.C. General Assembly in 2004. As a reminder, seven BTTs have been spearheaded thus far by the e-NC Authority. They serve as small business resource centers in otherwise economically-distressed areas, and provide business start-up counseling, low-cost office space, technological resources, and public access to the Internet. The BTTs that would benefit from this funding are:

- New Ventures Business Development, **Wadesboro, Anson County** (2005)
- The Roanoke Center, **Rich Square, Northampton County** (2005)
- Rockingham County Business & Technology Center, **Wentworth, Rockingham County** (2005)
- Foothills Connect Business & Technology Center, **Rutherfordton, Rutherford County** (2005)

From the BTT support grant funds, it is anticipated that approximately \$400,000 will be made available through a RFP process to each of the BTTs started in 2005, for an initial total of \$1.6 million. An

- continued -

Commissioners of The e-NC Authority

Opette N. Jordan, Chair
Carolina Gateway Partnership

George Belkoff
N.C. Office of Information
Technology Services

John Davido
Western Carolina University

Jim Bate
N.C. Justice Center

Herb Greenshaw
ARRT Research Institute

Jim Fahn
N.C. Department of
Transportation

Greg Fowler
Carolina Cyber Systems

Billy Ray Hall
N.C. State University
Department of Agriculture

John R. Hession
HHS/ARL

Lewis C. Hoggard
Beaufort County

Joseph Harrell
Millsboro Market

Leo Mandall
N.C. League of Municipalities

Bo McNiff
Mental Programs

Rebecca Prosser
N.C. Association of Counties
Communications

Jane Smith Patterson
Hesse & Associates

For additional information:
The e-NC Authority
www.e-nc.org
1.866.627.8728

additional \$400,000, which creates the \$2 million total requested, would be for the establishment of a new BTT to be located in the southeastern portion of the state. Funding would also allow for continuation of the BTT "technopreneur" program, which employs a local, BTT-based mentor and counselor for the support of entrepreneurs and small businesses. In addition to those BTTs that were founded in 2005, three BTTs began operations in 2001: Blue Ridge Business Development Center in **Sparta, Alleghany County**, Tri-County Community College Telecenter in **Murphy, Cherokee County**, and Northeast Technology & Business Center in **Williamston, Martin County**.

Between 2001 and 2006, the seven existing BTTs have **created 1,190 jobs**. With initial funding from the e-NC Authority, the seven BTTs have been able to collectively **leverage an additional \$9,966,760**.

Connectivity incentives funds (\$7.5 million recurring) will bring all 100 counties up to a statewide average of at least 70 percent access to broadband connectivity. The funds granted will be **matched** 100 percent by bidding service providers in order to install the broadband infrastructure. Recurring funds would allow the e-NC Authority to then obtain 80 percent access for all counties, followed by 90 percent access - and finally - complete connectivity access for all North Carolina businesses and citizens. Access to high-speed Internet is vital to economic development. Large and small businesses cannot operate and be competitive in areas of the state that do not have access. Listed below are the twenty-six counties that have connectivity levels below the critical 70 percent threshold, five of which have less than 50 percent connectivity (**BOLD/UNDERLINED**):

Alexander, Burke, Caldwell, Caswell, Chatham, Cherokee, Columbus, Duplin, Franklin, **Gates**, Graham, **Greene**, **Jones**, Macon, **Madison**, Martin, McDowell, Montgomery, Pamlico, Pender, Person, Rutherford, Stokes, Tyrrell, Vance, **Warren**

Operations and Research funds (\$300,000 recurring) are needed to support the work of the e-NC Authority, which operates statewide and regularly responds to connectivity research and data needs from county leadership, state legislators, citizens and service providers. These funds are particularly important for research operations and the collection of information about the telecommunications infrastructure in the state, which is maintained on the e-NC Authority's public GIS mapping program. During the 2005-2007 biennium, the e-NC Authority was granted \$500,000 in recurring annual operating support from the N.C. General Assembly. This prior allocation, plus the additional funding request, will support approximately 70 percent of the e-NC Authority's annual costs for operations, research and programs. This requested additional funding is necessary for the e-NC Authority to carry out the core duties as mandated in S.L. 2003-425, and new responsibilities related to monitoring PEG Channel grants as mandated in S.L. 2006-151.

Competitive Innovation Grants Program funds (\$200,000 recurring) will be distributed and monitored by the e-NC Authority in support of model programs and value-added business initiatives that enhance the technology capacity and economies of rural and urban distressed regions of the state. These funds would be made available to programs facilitated in cooperation with the seven existing Business & Technology Telecenters in the state, as well as the e-NC Authority's e-communities program. Other potential uses for this competitive seed fund could include digital literacy and e-commerce programs for small business entrepreneurs, pilot urban distressed programs and e-government projects.



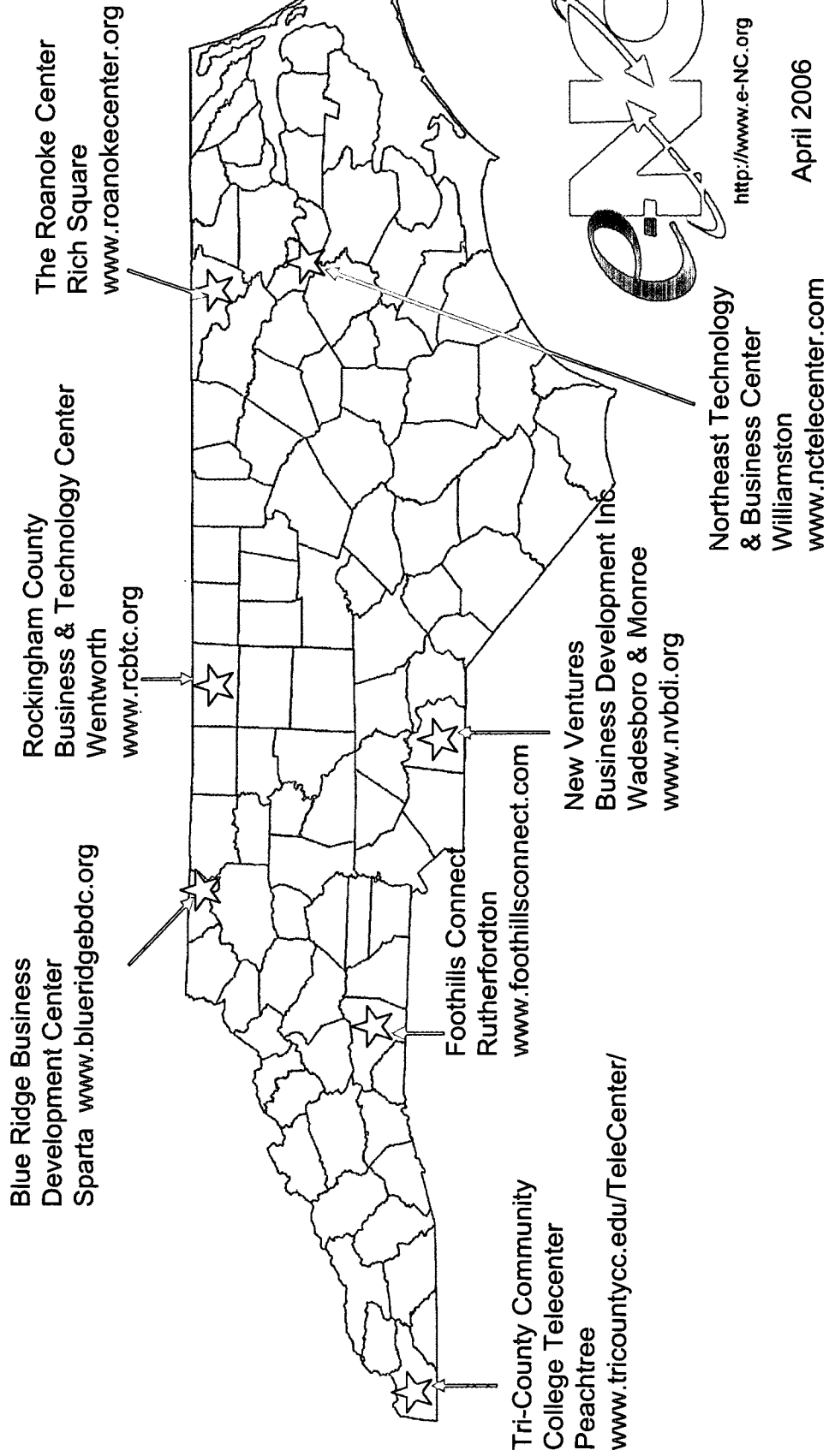
3/27/07

2005 High-Speed Internet Availability			
DSL and Cable Modem Composite			
County	Composite Hholds	Cable Modem % Households	DSL% Households
Jones	40.96%	34.99%	40.96%
Greene	44.26%	0.00%	44.25%
Warren	44.42%	37.58%	33.21%
Gates	48.51%	0.00%	48.50%
Madison	48.83%	26.74%	39.92%
Pamlico	50.14%	0.00%	50.13%
Duplin	51.47%	46.82%	51.47%
Tyrrell	52.68%	37.39%	52.66%
Caswell	53.12%	45.23%	50.25%
Person	53.80%	27.39%	53.79%
Graham	56.00%	0.00%	56.00%
Columbus	56.71%	18.34%	56.71%
Cherokee	57.62%	43.69%	57.62%
Burke	59.37%	32.49%	59.37%
Franklin	60.23%	55.90%	49.52%
Vance	62.37%	59.87%	62.37%
McDowell	62.87%	62.59%	50.46%
Macon	63.63%	63.63%	62.46%
Caldwell	65.35%	63.26%	65.35%
Stokes	66.13%	51.55%	66.13%
Martin	66.33%	45.99%	59.50%
Montgomery	66.42%	12.07%	66.41%
Alexander	66.59%	31.72%	66.56%
Chatham	67.21%	57.05%	67.21%
Rutherford	68.72%	61.52%	67.96%
Pender	69.22%	53.11%	63.23%
Clay	71.01%	0.00%	71.00%
Mitchell	71.36%	59.36%	59.58%
Buncombe	72.49%	63.09%	72.49%
Avery	72.62%	0.00%	72.62%
Scotland	73.37%	60.35%	73.37%
Swain	73.39%	57.10%	55.81%
Granville	73.66%	71.75%	56.91%
Onslow	74.09%	58.37%	74.09%
Robeson	74.11%	74.11%	50.51%
Nash	74.17%	61.21%	74.17%
Lenoir	74.34%	56.94%	74.34%
Edgecombe	75.05%	56.97%	75.05%
Northampton	75.39%	71.24%	36.97%
Currituck	75.40%	75.40%	52.92%
Johnston	75.60%	75.60%	74.05%
Washington	76.24%	68.89%	68.35%
Rockingham	76.74%	76.74%	58.57%
Jackson	76.93%	56.69%	70.47%

County	Composite Hholds	Cable Modem % Households	DSL% Households
Wilkes	77.12%	38.88%	77.12%
Halifax	77.18%	61.98%	77.18%
Rowan	77.61%	63.57%	74.37%
Anson	78.10%	56.05%	78.10%
Lincoln	78.13%	40.58%	78.13%
Pasquotank	78.16%	78.16%	73.93%
Alamance	78.42%	71.81%	78.42%
Alleghany	79.19%	8.58%	79.19%
Camden	79.31%	79.31%	41.62%
Sampson	79.32%	49.27%	76.72%
Perquimans	79.71%	68.64%	63.25%
Henderson	79.72%	74.97%	72.42%
Ashe	79.75%	0.00%	79.74%
Haywood	80.11%	61.12%	80.11%
Bertie	80.43%	61.50%	52.82%
New Hanover	80.48%	73.29%	76.32%
Bladen	81.02%	60.39%	75.80%
Union	81.02%	80.48%	48.10%
Davidson	81.20%	66.12%	81.20%
Gaston	81.25%	79.47%	78.63%
Hertford	81.27%	77.67%	68.43%
Harnett	82.16%	34.52%	82.16%
Moore	82.22%	71.02%	78.72%
Mecklenburg	82.23%	78.35%	75.80%
Wayne	82.60%	69.75%	71.17%
Beaufort	82.83%	54.20%	82.59%
Watauga	83.25%	67.39%	81.31%
Catawba	83.82%	59.62%	83.60%
Hoke	84.03%	53.30%	80.43%
Polk	84.88%	25.59%	84.88%
Iredell	85.24%	70.20%	85.24%
Craven	85.34%	82.19%	78.14%
Surry	85.71%	70.51%	85.71%
Randolph	87.12%	68.17%	84.44%
Wilson	87.51%	78.34%	75.63%
Lee	87.54%	53.88%	87.54%
Richmond	87.55%	87.55%	56.45%
Chowan	87.76%	83.38%	52.00%
Forsyth	88.06%	76.00%	83.56%
Pitt	88.77%	72.50%	85.82%
Cumberland	90.80%	80.31%	85.63%
Guilford	91.11%	86.48%	81.71%
Hyde	91.21%	84.60%	56.29%
Orange	91.67%	82.36%	87.24%
Cleveland	91.74%	82.09%	69.66%
Wake	91.74%	91.19%	67.70%
Durham	92.54%	87.06%	87.77%
Carteret	93.71%	80.84%	78.93%
Yancey	94.18%	47.07%	47.12%

County	Composite Hholds	Cable Modem % Households	DSL% Households
Dare	94.21%	81.10%	94.20%
Brunswick	95.44%	84.80%	95.44%
Yadkin	95.61%	78.75%	95.60%
Davie	95.66%	79.64%	95.66%
Stanly	95.94%	84.49%	95.93%
Transylvania	96.73%	0.00%	96.73%
Cabarrus	97.66%	93.60%	97.66%

e-NC Business & Technology Telecenters



The e-NC Authority Business & Technology Telecenters

PERFORMANCE METRICS

2001-2003:

	Jobs Created	Tenants	Public Access Visits	Tech/Bus. Service Clients	\$ Leveraged by the e-NC Authority \$
Total Original Telecenters:	199	23	50,977	1,080	\$5,710,574

2004:

	Jobs Created	Tenants	Public Access Visits	Tech/Bus. Service Clients	\$ Leveraged by the e-NC Authority \$
Total Original Telecenters:	289	33	46,038	16,673	\$2,974,747

2005:

	Jobs Created	Tenants	Public Access Visits	Tech/Bus. Service Clients	\$ Leveraged By the e-NC Authority \$
Total 7 Telecenters:	403	19	4,103	785	\$700,965

2006:

	Jobs Created	Tenants	Public Access Visits	Tech/Bus. Service Clients	\$ Leveraged by the e-NC Authority \$
Total 7 Telecenters:	299	22	32,048	1,995	\$580,474

TOTALS 2001-2006

	Jobs Created	Tenants	Public Access Visits	Tech/Bus. Service Clients	\$ Leveraged by the e-NC Authority \$ *
TOTAL:	1,190	97	132,770	20,533	\$9,966,760

* This figure does not include the independent business revenue generated by each Telecenter.

Note:

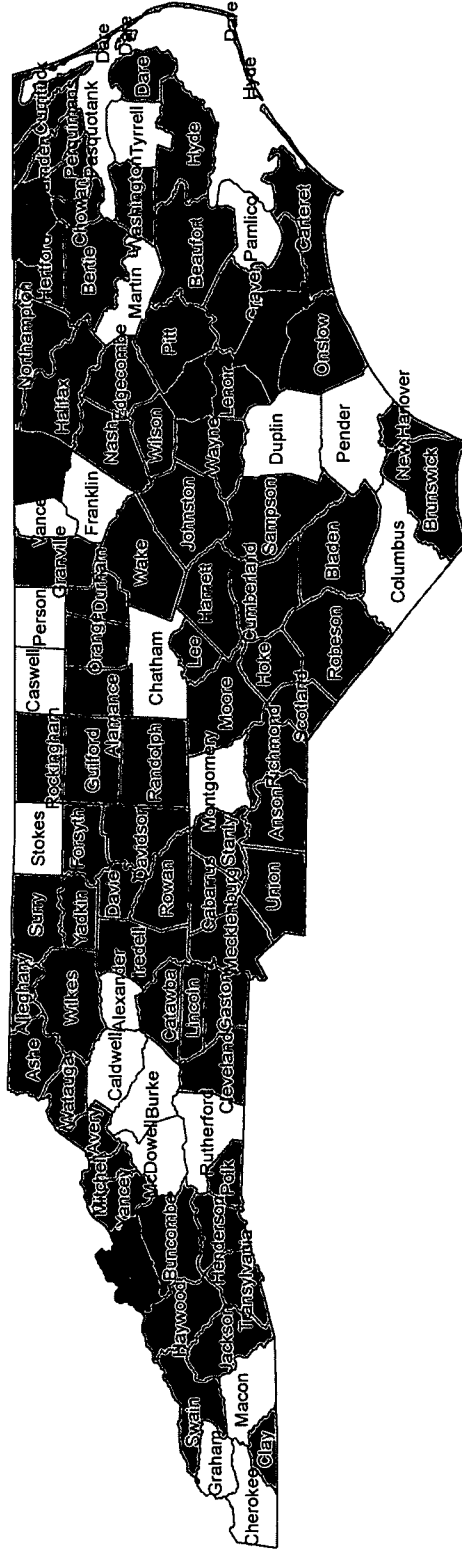
Total funding invested in Telecenters, directly from the e-NC Authority: \$6,033,592

Cost per job created: \$5,070



NC Households High Speed Internet Availability

2005 DSL and Cable Modem Composite
State Average - 82%



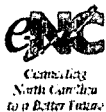
2005_HSIA COMPOSITE

- < 50%
- 50% - 69%
- 70% - 100%

Based on data supplied by Service Providers



12/13/06



CREATING SUCCESS

"E-NC's Charlie Pittman understood exactly the problem I was facing. He didn't have any quick fixes but he said he would do all that he could to address my concerns and hopefully bring some solutions to this problem... I appreciate e-NC so much. I cannot thank them enough for taking an interest in my situation."

— Donna Evans

Stokes County resident

The e-NC Authority

Service Inquiries Contact Information

Toll Free: 866.627.8725

Phone: 919.250.4314

Fax: 919.250.4325

E-mail: info@e-nc.org

Web: www.e-nc.org

4021 Cary Drive
Raleigh, NC 27610

e-NC Service Inquiries Program

Connecting citizens to providers to Internet solutions

Donna Evans is a 38 year-old mother of three. She lives in the Sandy Ridge exchange in Stokes County, but her complaints are not unique to that area. Residents across the state, particularly in rural areas, share frustrations over their lack of access to affordable Internet services.

Most of the communities surrounding Evans' home have access to local dial-up Internet service through providers such as Earthlink and Net Zero, and many have access to high-speed service through Sprint. Until recently, Evans could use her modem to dial a local number and access the Internet. Now, there are small pockets in the area where toll free local dial-up service is unavailable and Evans' home happens to be in one of those pockets. In order to connect to the Internet, people in those areas must add an extended calling feature to their local telephone service or dial a long distance number every time they log on.

"I have a cousin who lives within a fourth of a mile and he is in the same boat as me," said Evans. "But I know several other people that live three or four miles from me who have great Internet service through Sprint DSL. My family is in a small area that is not able to get this service. It is not any more rural than all the areas around me, but it feels like we have to take a backseat to everyone else. And because we are rural and not everyone uses Internet in

this area, it is difficult to convince the service providers to give us a local number."

Evans was so disappointed when she lost her local dial-up number, she began surfing the Internet in search of a place to vent her frustrations. She came across the Web site for the e-NC Authority, called their toll free number, and was connected to Charlie Pittman, who handles service inquiries for the organization.

"Charlie was not aware that our Internet provider was going to drop us," said Evans. "He was glad I contacted him. He said he would work to get another provider to our area. I was encouraged by our conversation and felt that Charlie understood exactly the problem I was facing. He didn't have any quick fixes but he said he would do all that he could to address my concerns and hopefully bring some solutions to this problem."

Evans hopes high-speed Internet service will ultimately become available to her home address. In the meantime, she has enrolled in an expanded area service plan through her phone company, allowing her to access a local ISP when connecting to the Internet.

Having someone listen to her concerns and commit to helping her discover new options meant a lot to Evans. "I appreciate e-NC so much," she said. "They are the only ones that seem to understand my frustrations. I cannot thank

them enough for taking an interest in my situation."

In 2000, the NC General Assembly charged the e-NC Authority with ensuring all citizens, businesses and communities are aware of, know how to use, and have access to Internet services at affordable prices. Since that time, e-NC's concentrated efforts have had a measurable impact on North Carolina, which has expanded infrastructure, applications and training. By working with both public and private service providers, e-NC has helped ensure that more than 80 percent of citizens and businesses have access to high-speed Internet.

A unique collaboration between public and private sectors, e-NC brings together nonprofits; national, state and local governments; telecommunications companies; small Internet service providers; software and equipment companies; foundations; universities and think-tanks in an effort to improve North Carolina's connectivity.

An important step in providing access is understanding local needs. E-NC continually maps the state's high-speed Internet access and, thereby, the gaps in that access, in unparalleled detail. The organization also communicates with citizens to see where service gaps have developed, passes information on local need to service providers, and advocates for increased coverage.

In 2001, e-NC verified that North Carolinians had 100

"The young people here learned about the Internet in school and are hungry for it. The Post Office and NC Ferry terminal here also want broadband... I cannot say enough about how much I appreciate the work of e-NC to bring broadband to Cedar Island."

*- Steve Johnson
Carteret County resident*

percent access to dial-up Internet services via a local call - meaning no long distance charge is associated with connecting to the Internet. Since that time, e-NC has maintained a database on its Web site where citizens can enter their home phone numbers and identify local Internet service providers in their calling areas. Using this database, e-NC realized this year that some areas are losing their local ISPs, causing small pockets of the state to lack local dial-up service.

E-NC believes this trend is due partly to providers switching to broadband access, and also to recent changes in telecommunications regulations by the Federal Communications Commission. Telecommunications companies are no longer required to share broadband lines with local ISPs, forcing some out of business and creating pockets in the state where local dial-up service is no longer available.

The e-NC Authority has received service inquiry calls since its inception. Sometimes callers want providers to upgrade their service from dial-up access to high-speed. Sometimes, like in Evans' case, ISPs have cut service or gone out of business, leaving shortages in areas that previously had Internet access.

E-NC's Charlie Pittman listens to callers' stories and concerns, then explains their options. Once he has collected information from the caller, he contacts local service providers, who typically dispatch an engineer to explore service options in the area. If they decide they cannot provide or expand ser-

vice, Pittman communicates the reason to the citizens who call in. He discusses with callers the pros and cons of satellite service and lets them know if their area offers wireless service - he tries to give them choices.

"People are frustrated," said Pittman. "They read that 82 percent of the state has access and want to know why they don't. Many times, they have already tried to call their local ISP. But they get service reps who are ill equipped to handle requests. They usually read from a script and don't do a good job of explaining when areas will have service, because they don't know. They aren't familiar with the areas and they don't understand local needs, particularly as communities build up."

The e-NC Authority receives calls from the general public and legislators alike, sometimes as many as 10-15 per week. "The more e-NC is in the news, the more calls come in," said Pittman. "Anytime a story comes out on what e-NC does, or what percent of the state is connected, the number of calls goes up. Even when news is quiet, the calls are constant."

Usually, if e-NC receives enough calls from one area, a strong enough business case can be established to convince service providers to speed up plans to provide service. Such was the case for Steve Johnson and his wife, who run a bed and breakfast on Cedar Island, along North Carolina's east coast. The island is isolated by a saltwater marsh, and while residents have access to dial-up services, they would like high-speed capabilities on the island.

"The population of the island is about 350 and most of the workers are fishermen or work

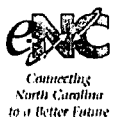
for the NC Ferry System," said Johnson. "The young people here learned about the Internet in school and are hungry for it. These are smart kids, many go on to college even though their folks do not make much money. Families are very close here so the kids get a lot of attention when it comes to education. They want the World Wide Web - they want the same access as their classmates in the city. My B&B takes online reservations, which is a slow process with dial-up. The Post Office and NC Ferry terminal here also want broadband."

Johnson contacted his local senator, who asked e-NC to look into the request. Pittman called the cable company serving that area and was told they were looking to upgrade but did not know when because of infrastructure engineering challenges in the area.

To add voices to the effort, Johnson began circulating a petition for expanded service, which more than 100 of Cedar Island's 350 residents signed in a matter of days. Johnson sent the petition to e-NC, who presented it to Sprint. Representatives of the telecommunications provider said the petition demonstrated enough of a business case to provide broadband service to the area. A short time later, Johnson signed up as a Sprint DSL customer.

"I cannot say enough about how much I appreciate the work of e-NC to help bring broadband to Cedar Island," said Johnson. "E-NC is a true advocate for rural areas and, as in this case, it's a job they do quite well."

Creating Success chronicles the achievements of the e-NC Authority's grantees and programs.



CREATING SUCCESS

**"They're the
best game
[in Oriental]
when it
comes to
broadband."**

**- Julie Rahm,
Community
Customer**

Quick Facts

Pamlico County

13,071 people

337 square miles

County seat:
Bayboro

Eastern NC
3 hrs to Raleigh
2.5 hrs to
Wilmington

In 2004:
0 Jobs Announced
0 Investment
Announced
0 Job Losses

Economic facts from NC
Department of Commerce

PineLink

Pamlico County, North Carolina

It is Friday, which means Justus Straubmuller has just wrapped up another grueling 60-hour workweek. And he doesn't get paid a dime.

President of PineLink, a non-profit 501(c)3 corporation that provides high-speed Internet service to Pamlico County, Straubmuller is a very busy man. There is a three-week backlog on installations and eager customers won't wait for better weather. So out he goes into chilling coastal winds every morning.

Like many of PineLink's volunteers, Straubmuller puts in long hours in order to connect his neighbors to the Internet. He wants the possibilities the Internet offers for the businesses and citizens of Pamlico County.

PineLink rose out of the efforts of e-Pamlico, part of a statewide grassroots effort led by e-NC to bring high-speed Internet services to all areas of North Carolina.

"We studied Pamlico for a year. We met with Sprint and TimeWarner to see when they would bring service to more than just the businesses off the main roads," said Jerry Prescott an e-Pamlico and now a PineLink volunteer. "They said they had no plans to install high-speed broadband off the main road. So we decided to create a nonprofit to do what the for-profit companies wouldn't."

Local students, especially Alex Goodwin, researched Internet options. Retired engineers, including Dr. Robert Couranz who joined PineLink just before the first site was installed, have worked to improve its design and reliability.

"A 900 MHz, wireless system was chosen because our population is spread out over a large area. We also needed something that could penetrate past the pine trees," said Couranz.

PineLink's Treasurer Bud Aldridge pointed out "you can't put fiber in the ground affordably for our application, but you can do wireless."

In May 2003, PineLink started serving Oriental, NC. The nonprofit rented space for its first transmitter on a cell phone tower. PineLink also started to build two towers of their own, one in Vandemere and the other in Dawson's Creek for two more transmitters. The nonprofit had thirty community customers.

Today, PineLink has more than 150 community customers and a backlog of more than 100 more waiting for service. The nonprofit operates a 24-hour call-in line as well.

"I know at least three people on the wait list. Everyone wants it," said PineLink cus-

tomers Julie Rahm, a partner with EagleForce Associates in McLean, VA, who works part-time from her home in Oriental. "It is hard to imagine they do so much for so little."



Volunteers for PINE include (from left to right) Bud Aldridge, Justus Straubmuller (president), Jerry Prescott and Robert Couranz

Currently, PineLink charges from \$24.95 per month for basic residential service (256 Kb/s) to \$64.95 per month for the premium business package (1 Mb/s). The fees cover the basic cost of service and ensure service expansion.

Quick Facts

PineLink

150 community customers

100 installations on backlog

10+ new service requests per week

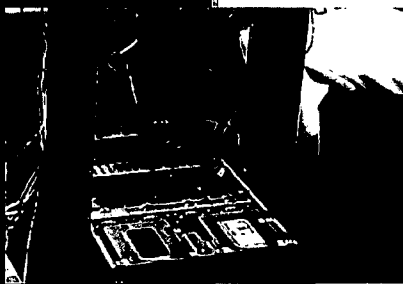
1 24-hour help desk

135+ volunteer hours per week

www.pinelink.org

Figures since Fall 2003

Alex Goodwin, PineLink board member and now a college sophomore at NCSU, helps to install PineLink's primary server at the Mel Tower.



"I am so thrilled and grateful that they're in town," said Rahm, a software developer. "They're the best game here when it comes to broadband."

All PineLink Internet service speeds are symmetrical upstream and downstream as well.

The ability to download information as fast as she can upload it is particularly critical to Frieda Hudson, publisher of the Pamlico News. Hudson and her staff download large advertising files for the paper in seconds — an activity that used to take 10 minutes per file when she had dial-up service.

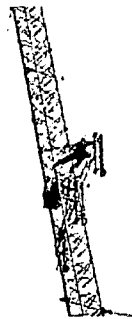
"Before, it would take me four hours to get the paper to the printer between sending and resending the different pages individually — I learned the hard way not to send files bigger than 1 Mb/s," said Hudson. "Now it takes me two to three minutes. And I can send the whole paper at once."

Hudson compares PineLink to the rural electric and tele-

phone membership cooperatives that brought critical services to rural areas when for-profit companies wouldn't.

"In the mid-1950s, there were parts of Pamlico county that didn't have electricity — and wouldn't because we weren't a money maker," said Hudson. "A group formed and called themselves Tideland Electric Membership Cooperative and they extended service throughout the area."

"PineLink has done the same thing," continued Hudson. "They've formed a nonprofit and brought services to us that otherwise we wouldn't see for another ten years."



Hundreds of feet in the air, subcontractors install PineLink equipment on the Mel Tower.

Ten years ago, B&B Yacht Designs of Vandemere was one of the first companies in their industry to have an online presence. Today, they conduct 90 percent of their business on the computer.

The company sells stock and custom plans for boat builders. On its Web site, B&B points visitors to an independent online forum created by their customers and to the online journal of Joe Nelson, a B&B customer who asked the company if he could take visitors through the step-by-step process of building a B&B boat.

exposure that boat companies would kill to have," said Carla Byrnes, wife of chief naval designer Graham Byrnes. "Early on, people knew boats by their designers' names. Since the 1980s, companies have used teams of nameless designers. But the Internet has put Graham's name out there again. People know his boats by his name."

While dial-up worked for B&B for several years, the service had its difficulties and was relatively slow. With only one business line, it was impossible to be online and on the phone with a customer at the same time.

"For a small business, installing another phone line is a big expense," said Byrnes. "With PineLink I can be talking to my customer while we're both looking at the same Web page."

PineLink's fast service is affordable because of volunteer drive and dedication, grant and loan money from e-NC and Pamlico County, and the organization's 501(c)3 status. The e-NC Authority contributed \$263,000 to the project. In February 2005, Pamlico County provided PineLink with a \$42,500 low-interest loan so that the nonprofit could purchase additional modems and clear the backlog of customers.

"The installs will go quicker this summer with longer days and better weather," says Straubmuller as he assesses the work ahead. "We'll have another 200 people online by then."



Installing PineLink equipment on the Oriental water tower.

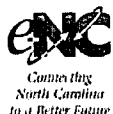
"The Internet has given us

Creating Success chronicles the achievements of the e-NC Authority's grantees and programs.

"They've brought services to us that otherwise we wouldn't see for another ten years."

- Frieda Hudson, Community Customer

All photos this page courtesy of the Pamlico News.



CREATING SUCCESS

Sprint & e-NC Deploy DSL in 32 Counties

Targeted Counties

Eastern NC

Beaufort
Bertie
Bladen
Camden
Columbus
Currituck
Dare
Duplin
Edgecombe
Halifax
Hertford
Hyde
Jones
Lenoir
Martin
Northampton
Onslow
Pamlico
Pasquotank
Perquimans
Pitt
Tyrell
Washington
Wilson

Central NC

Caswell
Chatham
Montgomery
Moore
Stokes
Warren

Western NC

Alleghany
Ashe

Project brings access to rural areas, with focus on eastern NC

In 2002, the e-NC Authority launched its Connectivity Incentive Grants program, intended to encourage groups to provide affordable, high-speed Internet access and to develop new and expanded services for users in rural areas of the state.

As part of this program, a special effort was made to install digital subscriber line (DSL) service for counties in eastern North Carolina. After a competitive grant/bid process, the e-NC Authority partnered with Sprint, a major telecommunications provider in the state, in August 2002.

Sprint was awarded \$600,000 to bring service to previously unserved areas. Monies went toward the deployment of DSL, high-speed Internet service to 35 exchanges in 24 counties. In March 2003, the Authority awarded Sprint \$200,000 more to provide DSL to an additional 17 wire centers in 16 counties.

With this project, a total of 32 counties received up-graded service, including 24 in the east, six in central

North Carolina, and two in the western part of the state.

Those counties were Alleghany, Ashe, Beaufort, Bertie, Bladen, Camden, Caswell, Chatham, Columbus, Currituck, Dare, Duplin, Edgecombe, Halifax, Hertford, Hyde, Jones, Lenoir, Martin, Montgomery, Moore, Northampton, Onslow, Pamlico, Pasquotank, Perquimans, Pitt, Stokes, Tyrell, Warren, Washington, and Wilson.

In May 2005, Sprint passed a major milestone when the company connected its **10,000th customer** in the state to DSL service as a result of its project with e-NC. By June 2005 all exchanges east of I-95 had DSL service installed.

Without incentives from e-NC, it is unlikely Sprint would have had a business case to take on the project because all of the targeted 32 counties are rural and sparsely populated.

According to Sprint's State Executive of the Carolinas Steve Parrott, however, "in rural areas, if you have the

*"In rural areas,
if you have the right
training and integra-
tion advice, and if
you put in
service, people will
take
you up on it."*

- Steve Parrott, Sprint's state
executive of the Carolinas

right training and integration advice, and if you put in the service, people will take you up on it."

With e-NC's help, citizens across the state of North Carolina received faster, more affordable Internet service sooner than they would have otherwise.

Creating Success chronicles the achievements of the e-NC Authority's grantees and programs.

Principal Clerk _____
Reading Clerk _____

SENATE
NOTICE OF COMMITTEE MEETING
AND
BILL SPONSOR NOTICE

The Senate Committee on **Information Technology** will meet at the following time:

DAY	DATE	TIME	ROOM
Wednesday	June 20, 2007	12:00 Noon	1124 LB

The following will be considered:

BILL NO.	SHORT TITLE	SPONSOR
HB 584	ITS/Employee Background Investigations.	Representative Tolson

Senator Janet Cowell, Co-Chair
Senator Katie G. Dorsett, Co-Chair

SENATE INFORMATION TECHNOLOGY COMMITTEE

**Wednesday, June 20, 2007, 12:00 Noon
1124 Legislative Building**

AGENDA

Welcome and Opening Remarks

Introduction of Pages

Bills

HB 584 ITS/Employee Background
 Investigations

Rep. Tolson

Presentations

Owen Sweeney, Manager of State Government Relations,
Symantec Corporation

Other Business

Adjournment

VISITOR REGISTRATION SHEET

SENATE INFORMATION TECHNOLOGY COMMITTEE June 20, 2007

Name of Committee

Date _____

VISITORS: PLEASE SIGN IN BELOW AND RETURN TO COMMITTEE CLERK

NAME

FIRM OR AGENCY AND ADDRESS

T Greg Doucette

NCGA (Sen Forest)

Ed Turlington

BPattC

Danny Furlberg

YFS

Dennis Patterson

OSC

**Senate Standing Committee
on
Information Technology
June, 20, 2007, 12:00 Noon
Room 1124 Legislative Building**

MINUTES

The Senate Standing Committee on Information Technology met at 12:00 p.m. on June 20, 2007, in Room 1124 of the Legislative Building. Senators Apodaca, Brock, Cowell, Dorsett, Foriest, Goss, Graham, Kerr, Pittenger and Queen were in attendance. Mr. Peter Capriglione of the Information Systems Division, Ms. Karlynn O'Shaughnessy of Fiscal Research Staff and Ms. Brenda Carter of the Research Division, were also present.

Co-Chair Senator Janet Cowell, presided, calling the meeting to order at noon. She welcomed members and guests, acknowledging Senate Pages who function as support staff at the meeting. Senator Cowell introduced discussion on House Bill 584: ITS/Employee Background Investigations. Representative Joe Tolson stood to explain the bill, which he said would authorize the state's Chief Information Officer to do background investigations on employees and others who work with the State CIO office. Secondly, the bill proposed a reconfigured Advisory Information Technology Committee to be set up more traditionally, with appointments by the Governor, President Pro Tempore and Speaker of the House. Senator Tom Apodaca moved adoption of a proposed committee substitute and the bill passed.

Senator Cowell introduced Mr. Guy Rowland, Mr. Walt Adams and Mr. Owen Sweeney of the Symantec Corporation, to present to the committee (please see the attached materials from Symantec). A discussion followed with questions and answers.

Co-Chair, Senator Cowell thanked members and guests for their attendance and adjourned the meeting at 12:45 p.m.

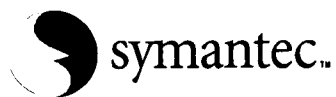


Senator Janet Cowell, Co-Chair



Cindy Garrison, Committee Clerk

Senator Katie Dorsett, Co-Chair



Symantec Internet Security Threat Report

Trends for July–December 06

Volume XI, Published March 2007

Executive Summary

Over the past two reporting periods, Symantec has observed a fundamental shift in Internet security activity. The current threat environment is characterized by an increase in data theft and data leakage, and the creation of malicious code that targets specific organizations for information that can be used for financial gain.

Instead of exploiting high-severity vulnerabilities in direct attacks, attackers are now discovering and exploiting medium-severity vulnerabilities in third-party applications, such as Web applications and Web browsers. Those vulnerabilities are often used in "gateway" attacks, in which an initial exploitation takes place not to breach data immediately, but to establish a foothold from which subsequent, more malicious attacks can be launched.

Symantec has observed high levels of malicious activity across the Internet, with increases in phishing, spam, bot networks, Trojans, and zero-day threats. However, whereas in the past these threats were often used separately, attackers are now refining their methods and consolidating their assets to create global networks that support coordinated criminal activity.

This has resulted in an increasing interoperability between diverse threats and methods. For example, targeted malicious code may take advantage of Web-enabled technologies and third-party applications to install a back door, which then downloads and installs bot software. These bots can, in turn, be used to distribute spam, host phishing sites, or launch attacks in such a way as to create a single coordinated network of malicious activity. Once entrenched, these networks can be used in concert as global networks of malicious activity that support their own continued growth.

Dean Turner
Executive Editor
Symantec Security Response

David McKinney
Analyst
Symantec Security Response

Ollie Whitehouse
Security Architect—Advanced
Threat Research
Symantec Security Response

David Cowings
Sr. Business Intelligence
Manager
Symantec Business Intelligence

Stephen Entwistle
Senior Editor
Symantec Security Response

Ronald Bowes
Analyst
Symantec Security Response

Zulfikar Ramzan
Analyst—Advanced Threat
Research
Symantec Security Response

Shravan Shashikant
Pr. Business Intelligence
Manager
Symantec Business Intelligence

Marci Denesluk
Editor
Symantec Security Response

Nicholas Sullivan
Analyst
Symantec Security Response

Contributors

Igor Mouchnick
Sr. Software Engineer
Symantec Instant Messaging
Security

Marc Fossi
Analyst
Symantec Security Response

Peter Coogan
Analyst
Symantec Security Response

David Cole
Director Product Management
Symantec Security Response

Joseph Blackbird
Analyst
Symantec Security Response

Candid Wueest
Analyst
Symantec Security Response

Peter Szor
Security Architect
Symantec Security Response

This volume of the *Internet Security Threat Report* will offer an overview of threat activity that took place between July 1 and December 31, 2006. This brief summary and the discussion that follows will offer a synopsis of the data and trends that are presented in the main report. Symantec will continue to monitor and assess threat activity in order to best prepare consumers and enterprises for the complex Internet security issues to come.

Internet Security Threat Report Overview

The Symantec *Internet Security Threat Report* provides a six-month update of Internet threat activity. It includes analysis of network-based attacks, a review of known vulnerabilities, and highlights of malicious code. It also assesses numerous issues related to online fraud, including phishing, spam, and security risks such as adware, spyware, and misleading applications. This summary of the *Internet Security Threat Report* will alert readers to current trends and impending threats. In addition, it will offer recommendations for protection against and mitigation of these concerns. This volume covers the six-month period from July 1 to December 31, 2006.

Symantec has established some of the most comprehensive sources of Internet threat data in the world. The Symantec™ Global Intelligence Network, which includes Symantec DeepSight™ Threat Management System and Symantec™ Managed Security Services, tracks attack activity across the entire Internet. It consists of over 40,000 sensors monitoring network activity in over 180 countries. As well, Symantec gathers malicious code data along with spyware and adware reports from over 120 million client, server, and gateway systems that have deployed Symantec's antivirus products.

Symantec operates one of the most popular forums for the disclosure and discussion of vulnerabilities on the Internet, the BugTraq™ mailing list, which has approximately 50,000 direct subscribers who contribute, receive, and discuss vulnerability research on a daily basis.¹ Symantec also maintains one of the world's most comprehensive vulnerability databases, currently consisting of over 20,000 vulnerabilities (spanning more than a decade) affecting more than 45,000 technologies from over 7,000 vendors. Symantec also tracks and assesses certain criminal activities using online fraud monitoring tools.

Finally, the Symantec Probe Network, a system of over two million decoy accounts, attracts email messages from 20 different countries around the world, allowing Symantec to gauge global spam and phishing activity. These resources give Symantec analysts unparalleled sources of data with which to identify emerging trends in attacks and malicious code activity. Symantec also gathers phishing information through the Symantec Phish Report Network, an extensive antifraud community of enterprises and consumers. Members of the network contribute and receive fraudulent Web site addresses for alerting and filtering across a broad range of solutions.

The Symantec *Internet Security Threat Report* is grounded principally on the expert analysis of data provided by all of these sources. Based on Symantec's expertise and experience, this analysis yields a highly informed commentary on current Internet threat activity. By publishing the analysis of Internet security activity in the *Symantec Internet Security Threat Report*, Symantec hopes to provide enterprises and consumers with the information they need to help effectively secure their systems now and in the future.

¹ The BugTraq mailing list is hosted by SecurityFocus (<http://www.securityfocus.com>). Archives are available at <http://www.securityfocus.com/archive/1>

Executive Summary Highlights

The following section will offer a brief summary of the security trends that Symantec observed during this period based on data provided by the sources listed above. This summary includes all of the metrics that are included in the main report. Following this overview, the Executive Summary will discuss selected metrics in greater depth.

Attack Trends Highlights

- The government sector accounted for 25 percent of all identity theft-related data breaches, more than any other sector.
- The theft or loss of a computer or other data-storage medium made up 54 percent of all identity theft-related data breaches during this period.
- The United States was the top country of attack origin, accounting for 33 percent of worldwide attack activity.
- Symantec recorded an average of 5,213 denial of service (DoS) attacks per day, down from 6,110 in the first half of the year.
- The United States was the target of most DoS attacks, accounting for 52 percent of the worldwide total.
- The government sector was the sector most frequently targeted by DoS attacks, accounting for 30 percent of all detected attacks.
- Microsoft Internet Explorer was targeted by 77 percent of all attacks specifically targeting Web browsers.
- Home users were the most highly targeted sector, accounting for 93 percent of all targeted attacks.
- Symantec observed an average of 63,912 active bot-infected computers per day, an 11 percent increase from the previous period.
- China had 26 percent of the world's bot-infected computers, more than any other country.
- The United States had the highest number of bot command-and-control computers, accounting for 40 percent of the worldwide total.
- Beijing was the city with the most bot-infected computers in the world, accounting for just over five percent of the worldwide total.
- The United States accounted for 31 percent of all malicious activity during this period, more than any other country.
- Israel was the highest ranked country for malicious activity per Internet user, followed by Taiwan and Poland.
- Fifty-one percent of all underground economy servers known to Symantec were located in the United States, the highest total of any country.
- Eighty-six percent of the credit and debit cards advertised for sale on underground economy servers known to Symantec were issued by banks in the United States.

Vulnerability Trends Highlights

- Symantec documented 2,526 vulnerabilities in the second half of 2006, 12 percent higher than the first half of 2006, and a higher volume than in any other previous six-month period.²
- Symantec classified four percent of all vulnerabilities disclosed during this period as high severity, 69 percent were medium severity, and 27 percent were low severity.
- Sixty-six percent of vulnerabilities disclosed during this period affected Web applications.
- Seventy-nine percent of all vulnerabilities documented in this reporting period were considered to be easily exploitable.
- Seventy-seven percent of all easily exploitable vulnerabilities affected Web applications, and seven percent affected servers.
- Ninety-four percent of all easily exploitable vulnerabilities disclosed in the second half of 2006 were remotely exploitable.
- In the second half of 2006, all the operating system vendors that were studied had longer average patch development times than in the first half of the year.
- Sun Solaris had an average patch development time of 122 days in the second half of 2006, the highest of any operating system.
- Sixty-eight percent of the vulnerabilities documented during this period were not confirmed by the affected vendor.
- The window of exposure for vulnerabilities affecting enterprise vendors was 47 days.
- Symantec documented 54 vulnerabilities in Microsoft Internet Explorer, 40 in the Mozilla browsers, and four each in Apple Safari and Opera.
- Mozilla had a window of exposure of two days, the shortest of any Web browser during this period.
- Twenty-five percent of exploit code was released less than one day after vulnerability publication. Thirty-one percent was released in one to six days after vulnerability publication.
- Symantec documented 12 zero-day vulnerabilities during this period, a significant increase from the one documented in the first half of 2006.
- Symantec documented 168 vulnerabilities in Oracle database implementations, more than any other database.

Malicious Code Trends Highlights

- Of the top ten new malicious code families detected in the last six months of 2006, five were Trojans, four were worms, and one was a virus.
- The most widely reported new malicious code family this period was that of the Stration worm.³

² The Symantec *Internet Security Threat Report* has been tracking vulnerabilities in six-month periods since January 2002.

³ http://www.symantec.com/security_response/writeup.jsp?docid=2006-092111-0525-99

Symantec Internet Security Threat Report

- Symantec honeypot computers captured a total of 136 previously unseen malicious code threats between July 1 and December 31, 2006.
- During this period, 8,258 new Win32 variants were reported to Symantec, an increase of 22 percent over the first half of 2006.
- Worms made up 52 percent of the volume of malicious code threats, down from 75 percent in the previous period.
- The volume of Trojans in the top 50 malicious code samples reported to Symantec increased from 23 percent to 45 percent.
- Trojans accounted for 60 percent of the top 50 malicious code samples when measured by potential infections.
- Polymorphic threats accounted for three percent of the volume of top 50 malicious code reports this period, up from one percent in the two previous periods.
- Bots made up only 14 percent of the volume of the top 50 malicious code reports.
- Threats to confidential information made up 66 percent of the top 50 malicious code reported to Symantec.
- Keystroke logging threats made up 79 percent of confidential information threats by volume of reports, up from 57 percent in the first half of the year and 66 percent in the second half of 2005.
- Seventy-eight percent of malicious code that propagated did so over SMTP, making it the most commonly used propagation mechanism.
- Malicious code using peer-to-peer to propagate rose from 23 percent of all propagating malicious code in the first six months of 2006 to 29 percent in the last half of the year.
- The majority of malicious code reports during this period originated in the United States.
- During the second half of 2006, 23 percent of the 1,318 documented malicious code instances exploited vulnerabilities.
- MSN Messenger was affected by 35 percent of new instant messaging threats in the second half of the year.

Phishing, Spam, and Security Risks Highlights

- The Symantec Probe Network detected a total of 166,248 unique phishing messages, a six percent increase over the first six months of 2006. This equates to an average of 904 unique phishing messages per day for the second half of 2006.
- Symantec blocked over 1.5 billion phishing messages, an increase of 19 percent over the first half of 2006.
- Throughout 2006, Symantec detected an average of 27 percent fewer unique phishing messages on weekends than the weekday average of 961.

Symantec Internet Security Threat Report

- On weekends, the number of blocked phishing attempts was seven percent lower than the weekday average of 7,958,323 attempts per day.
- Organizations in the financial services sector accounted for 84 percent of the unique brands that were phished during this period.
- Forty-six percent of all known phishing Web sites were located in the United States, a much higher proportion than in any other country.
- Between July 1 and December 31, 2006, spam made up 59 percent of all monitored email traffic. This is an increase over the first six months of 2006 when 54 percent of email was classified as spam.
- Sixty-five percent of all spam detected during this period was written in English.
- In the last six months of 2006, 0.68 percent of all spam email contained malicious code. This means that one out of every 147 spam messages blocked by Symantec Brightmail AntiSpam contained malicious code.
- Spam related to financial services made up 30 percent of all spam during this period, the most of any category.
- During the last six months of 2006, 44 percent of all spam detected worldwide originated in the United States.
- The United States hosted the largest proportion of spam zombies, with 10 percent of the worldwide total.
- The most commonly reported security risk was an adware program named ZangoSearch.
- All of the top ten security risks reported in the last six months of 2006 employ at least one anti-removal technique compared to only five of the top ten security risks in the last reporting period.
- All of the top ten security risks reported during this period employ self-updating.
- Potentially unwanted applications accounted for 41 percent of reports in the top ten new security risks in the second half of 2006.
- Misleading application detections increased by 40 percent in the second half of 2006.

Executive Summary Discussion

This section will discuss selected metrics from the *Internet Security Threat Report* in greater depth, providing analysis and discussion of the trends indicated by the data. The following metrics will be discussed:

- Malicious activity by country
- Data breaches that could lead to identity theft
- Underground economy servers
- Zero-day vulnerabilities
- Threats to confidential information
- Malicious code types
- Phishing
- Spam
- Bot-infected computers

Malicious activity by country

For the first time, in this volume of the *Internet Security Threat Report*, Symantec is evaluating the countries in which malicious activity takes place or originates. To determine this, Symantec has compiled geographical data on numerous malicious activities, namely: bot-infected computers, bot command-and-control servers, phishing Web sites, malicious code reports, spam relay hosts, and Internet attacks.

Between July 1 and December 31, 2006, the United States was the top country for malicious activity, accounting for 31 percent of the worldwide total (table 1). For each of the malicious activities taken into account for this measurement, the United States ranked number one by a large margin with the exception of bot-infected computers. It ranked second for that criterion, 12 percentage points lower than China.

Overall Rank	Country	Overall Proportion	Malicious Code Rank	Spam Host Rank	Command and Control Server Rank	Phishing Host Rank	Bot Rank	Attack Rank
1	United States	31%	1	1	1	1	2	1
2	China	10%	3	2	4	8	1	2
3	Germany	7%	7	3	3	2	4	3
4	France	4%	9	4	14	4	3	4
5	United Kingdom	4%	4	13	9	3	6	6
6	South Korea	4%	12	9	2	9	11	9
7	Canada	3%	5	23	5	7	10	5
8	Spain	3%	13	5	15	16	5	7
9	Taiwan	3%	8	11	6	6	7	11
10	Italy	3%	2	8	10	14	12	10

Table 1. Malicious activity by country
Source: Symantec Corporation

The high degree of malicious activity originating in the United States is likely driven by the expansive Internet infrastructure there. The United States accounts for 19 percent of the world's Internet users.⁴ Furthermore, the number of broadband Internet users in that country grew by 14 percent between December 2005 and July 2006.⁵ Despite the relatively well developed security infrastructure in the United States, the high number of Internet-connected computers there presents more targets for attackers to compromise for malicious use. Symantec predicts that the United States will remain the highest ranked country for malicious activity until another country exceeds it in numbers of Internet users and broadband connectivity.

China was the second highest country for malicious activity during this six-month reporting period, accounting for 10 percent of all worldwide malicious activity. Germany was third, with seven percent. The prominence of both of these countries can likely be attributed to the high number of Internet users there, as well as the rapid growth in the country's Internet infrastructure.

Having determined the top countries by malicious activity, Symantec evaluated the top 25 of these countries according to the number of Internet users located there. This measure is intended to remove the bias of high numbers of Internet users from the "Malicious activity by country" measurement. The percentage assigned to each country in this discussion equates to the proportion of malicious activity that could be attributed to a single (average) Internet user in that country.

Israel was the most highly ranked country for malicious activity per Internet user. If one person from each of the top 25 countries were to represent their country's Internet-connected population, the average Internet user in Israel would carry out nine percent of the group's malicious activity. Taiwan had the second most malicious activity per Internet user, accounting for eight percent of the sample group's activity. Poland ranked third, accounting for six percent.

Data breaches that could lead to identity theft

Identity theft is an increasingly prevalent security issue. Organizations that store and manage personal identification information must take care to ensure the confidentiality and integrity of such data. Any compromise that results in the leakage of personal identity information could result in a loss of public confidence, legal liability, and/or costly litigation.

In the second half of 2006, the government sector accounted for the majority of data breaches that could lead to identity theft, making up 25 percent of the total (figure 1). Government organizations store a lot of personal information that could be used for the purposes of identity theft. Furthermore, they often consist of numerous semi-independent departments. As a consequence, sensitive personal identification information may be stored in separate locations and be available to numerous people. This increases the opportunity for attackers to gain unauthorized access to this data. Governments may also be more likely to report such breaches than private organizations, which may fear negative market reaction.

⁴ <http://www.internetworldstats.com>

⁵ http://www.oecd.org/document/9/0,2340,en_2649_34225_37529673_1_1_1_1,00.html

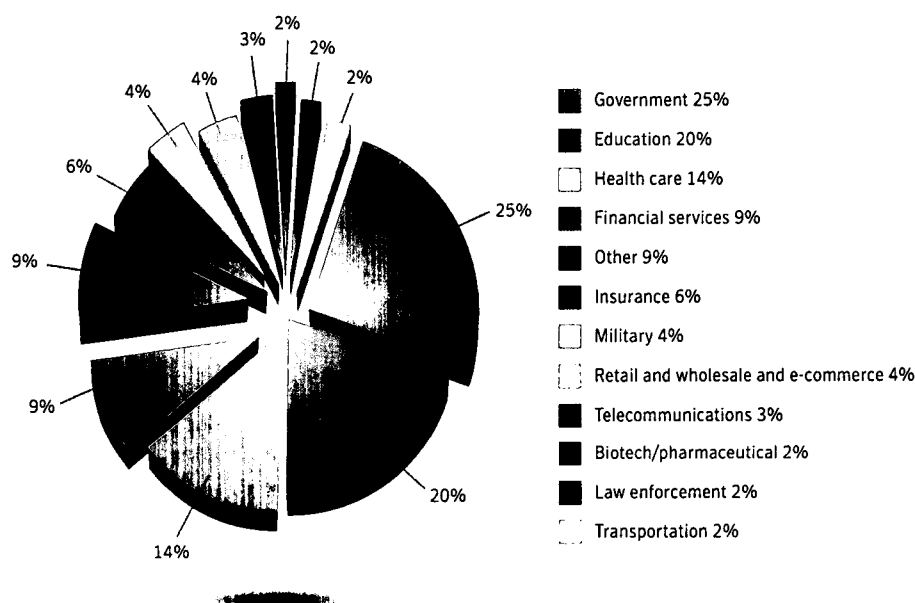


Figure 1. Data breaches that could lead to identity theft by sector
Source: Based on data provided by Privacy Rights Clearinghouse and Attrition.org

During this period, 54 percent of all data breaches that could lead to identity theft were caused by the theft or loss of a computer or data-storage medium (such as a USB memory key or back-up media). Twenty-eight percent of such breaches were caused by insecure policy, which includes a failure to develop, implement, and/or comply with adequate security policy. For example, this could mean posting personal identification information on a publicly available Web site or sending it through unencrypted email.

Most breaches of this type are avoidable. In the case of theft or loss, the compromise of data could be averted by encrypting all sensitive data. This would ensure that even if the data were lost or stolen, it would not be accessible to unauthorized third parties. This step should be part of a broader security policy that organizations should develop, implement, and enforce in order to ensure that all sensitive data is protected from unauthorized access.

Underground economy servers

Underground economy servers are used by criminals and criminal organizations to sell stolen information, typically for subsequent use in identity theft. This data can include government-issued identity numbers, credit cards, bank cards and personal identification numbers (PINs), user accounts, and email address lists.

During the second half of 2006, 51 percent of all underground economy servers known to Symantec were located in the United States, the highest total of any country (figure 2). The prominence of the United States is no surprise, as the expansive Internet infrastructure and continual broadband growth there create numerous opportunities for criminals to carry out malicious activities. Sweden ranked second, accounting for 15 percent of the worldwide total, and Canada ranked third, accounting for seven percent.

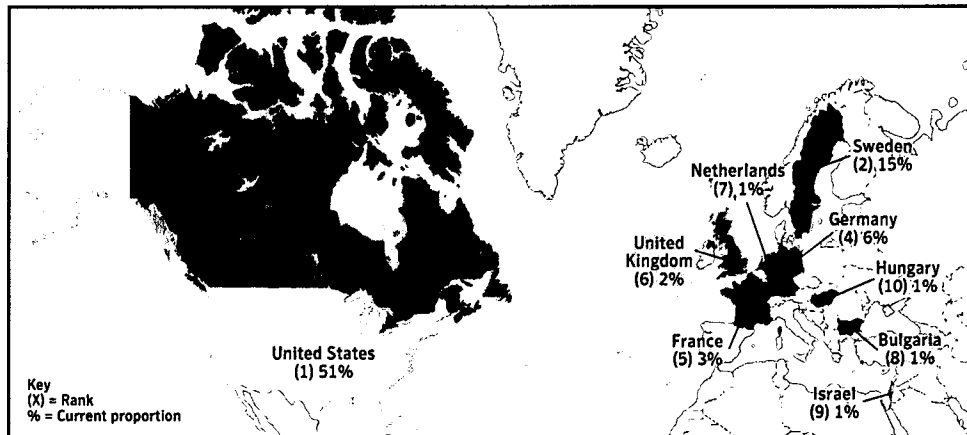


Figure 2. Location of underground economy servers
Source: Symantec Corporation

By far the most credit and debit cards advertised for sale on underground economy servers were issued by banks in the United States. The prominence of the United States is not entirely unexpected, as the vast majority of the data breaches that could lead to identity theft reported during this period took place there.

In order to reduce the likelihood of facilitating identity theft, it is important that organizations take the necessary steps to protect data stored on their computers or transmitted over networks. This should include the development and implementation of a policy requiring that all sensitive data is encrypted. This would ensure that, even if the data were lost or stolen, it would not be accessible. This step should be part of a broader security policy that organizations should develop and implement in order to ensure that any sensitive data is protected from unauthorized access.

Zero-day vulnerabilities

A zero-day vulnerability is one for which there is sufficient public evidence to indicate that the vulnerability has been exploited in the wild prior to being publicly known. It may not have been known to the vendor prior to exploitation, and the vendor had not released a patch at the time of the exploit activity.

Zero-day vulnerabilities represent a serious threat in many cases because there is no patch available for them and because they will likely be able to evade purely signature-based detection. They may be used in targeted attacks and in the propagation of malicious code. As Symantec predicted in Volume IX of the *Internet Security Threat Report*, a black market for zero-day vulnerabilities has emerged that has the potential to put them into the hands of criminals and other interested parties.⁶

In the second half of 2006, Symantec documented 12 zero-day vulnerabilities. This is a significant increase over the first half of 2006 and the second half of 2005 when only one zero-day vulnerability was documented for each reporting period.

The second half of 2006 saw a large number of high-profile zero-day vulnerabilities. This activity peaked in September of 2006, when four zero-day vulnerabilities were made known. The majority of these were client-side vulnerabilities that affected Office applications, Internet Explorer, and ActiveX controls. Many of these may have been discovered through the use of fuzzing technologies.

⁶ Symantec *Internet Security Threat Report*, Volume IX (March 2006):
http://eval.veritas.com/mktginfo/enterprise/white_papers/ent-whitepaper_symantec_internet_security_threat_report_ix.pdf : p. 21

Zero-day threats appear to be occurring more frequently than in the past. While it is believed that zero-day vulnerabilities have previously posed a threat, the recent rise in incidents may be partially accounted for by increasing capabilities to detect these attacks in the wild. Such capabilities include improved vulnerability-handling procedures within organizations, improved cooperation between enterprises and vendors, and better technologies for the detection and analysis of exploits and malicious code.

In order to protect against zero-day vulnerabilities, Symantec recommends that administrators deploy intrusion detection/intrusion prevention systems (IDS/IPS) and regularly updated antivirus software. Security vendors may be able to provide rapid response to recently discovered zero-day vulnerabilities in the wild by developing and implementing new or updated IDS/IPS and antivirus signatures before the affected vendor has released a patch. Generic signatures may also block zero-day threats, as may behavior-blocking solutions and heuristic technologies.

Threats to confidential information

Some malicious code programs are designed specifically to expose confidential information that is stored on an infected computer. Threats to confidential information are a particular concern because of their potential use in criminal activities. Compromises of this nature can result in significant financial loss, particularly if credit card information or banking details are exposed.

Exposure of confidential information within the enterprise can lead to significant data leakage. If it involves customer-related data—such as credit card information—it can severely undermine customer confidence as well as violate local laws. Sensitive corporate information, including financial details, business plans, and proprietary technologies, could also be leaked from compromised computers.

In the last six months of 2006, threats to confidential information made up 66 percent of the volume of the top 50 malicious code reported to Symantec (figure 3). This is an increase over the 48 percent reported in the first half of the year and the 55 percent reported during the second half of 2005.

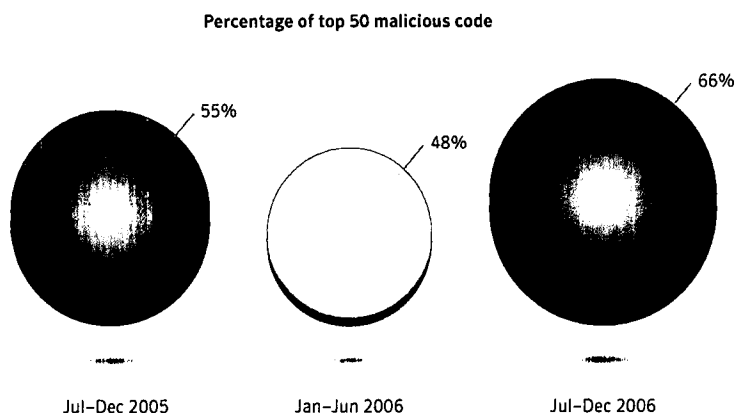


Figure 3. Threats to confidential information
Source: Symantec Corporation

In the second half of the 2006, threats that allow remote access, such as back doors, made up 84 percent of the volume of confidential information threats. Keystroke logging threats made up 79 percent of confidential information threats by volume of reports, and threats that could be used to export user data accounted for 62 percent of confidential information threats during this reporting period.

Malicious code types

During the current reporting period, worms made up 52 percent of the volume of malicious code threats, down from 75 percent in the previous period.⁷ However, the number of unique samples of worms in the top 50 malicious code reports remained fairly constant over the last six months of 2006. During this period, 36 worms were reported to Symantec, compared to 38 in the previous period.

The volume of Trojans in the top 50 malicious code samples reported to Symantec increased significantly in the last six months of 2006. During this period, they constituted 45 percent of the volume of the top 50 malicious code samples, a significant increase over the 23 percent last period and the 38 percent reported in the second half of 2005.

As is discussed in the “Future Watch” section of this report, attackers are moving towards staged downloaders, also referred to as modular malicious code. These are small, specialized Trojans that download and install other malicious programs such as a back door or worm. During the current period, 75 percent of the volume of the top 50 malicious code reports contained a modular component such as this.

For the first time, in this edition of the *Internet Security Threat Report*, Symantec is assessing malicious code according to the number of unique samples reported to Symantec and the number of potential infections. This is an important distinction. In some cases, a threat that may create a large number of reports may not cause a large number of potential infections and *vice versa*.

For instance, worms made up 52 percent of malicious code reports in the second half of 2006, but caused only 37 percent of potential infections (figure 4). The main reason for this is that mass-mailing worms generate a significant number of email messages to which they attach their malicious code. Each message that is detected will generate a malicious code report. Because of the high volume of email that one worm can generate, a single infection can result in many reports. However, once a malicious code sample is detected, antivirus signatures are quickly developed that can protect against subsequent infections by that sample. Furthermore, gateway policies and technologies can block the executable attachments that also come with a mass mailer. So, only a small percentage of the high volume of email messages will result in additional infections.

⁷ It is important to note that a malicious code sample can be classified in more than one threat type category. For example, bots such as variants of the Mytob family are classified as both a worm and a back door. As a result, cumulative percentages of threat types in the top 50 malicious code reports may exceed 100.

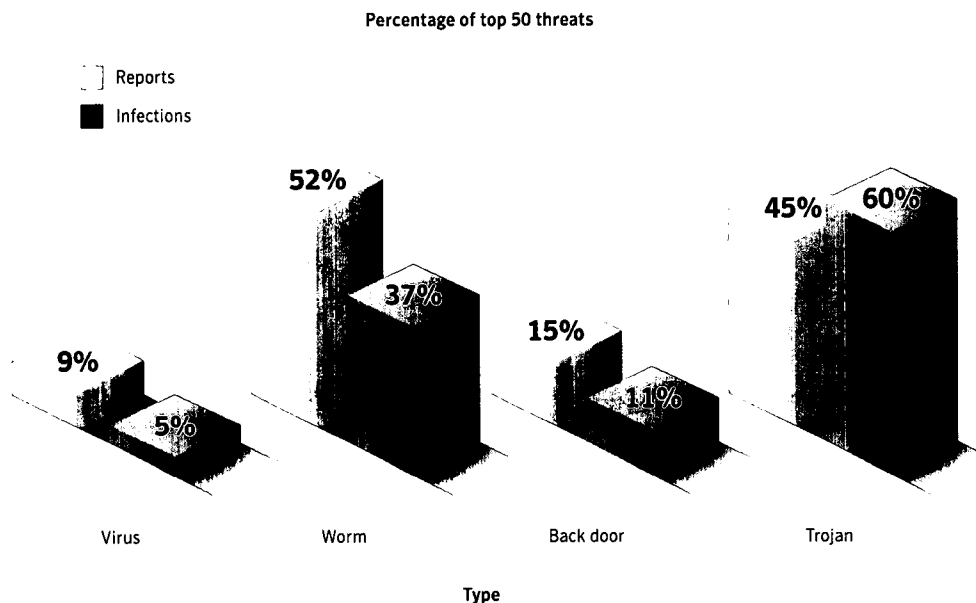


Figure 4. Malicious code types, by reports and by potential infections, July–December 2006
Source: Symantec Corporation

Trojans, on the other hand, only constituted 45 percent of the volume of the top 50 malicious code reports during the last six months of 2006. However, they accounted for 60 percent of potential infections by the top 50 malicious code samples during the same period. Since Trojans do not contain any propagation mechanisms, they do not proliferate as widely as mass-mailing worms, resulting in fewer reports. Because they are frequently installed by exploiting Web browser and zero-day vulnerabilities, a Trojan report is more likely to be the result of an infection. Consequently, the ratio of potential infections to reports is likely to be higher for Trojans than for worms.

Phishing

Over the last six months of 2006, the Symantec Probe Network detected a total of 166,248 unique phishing messages, an average of 904 per day. This total is a six percent increase over the first six months of 2006 when 157,477 unique phishing messages were detected.

In the second half of 2006, Symantec blocked over 1.5 billion phishing messages, an increase of 19 percent over the first half of 2006, and a six percent increase over the second half of 2005. This means that Symantec blocked an average of 8.48 million phishing emails per day over the last six months of 2006.

In the second half of 2006, 46 percent of all known phishing Web sites were located in the United States, a much higher proportion than in any other country. This is likely because a large number of Web-hosting providers—particularly free Web hosts—are located in the United States. Furthermore, the United States has the highest number of Internet users in the world, and it is home to a large number of Internet-connected organizations, both large and small.

Most of the unique brands phished in the last six months of 2006 were in the financial services sector. Organizations in that sector accounted for 84 percent of the brands that were used in phishing attacks this period. This is not surprising, as most phishing attacks are motivated by profit. A successful phishing attack on a financial entity is likely to yield information that an attacker could subsequently use for financial gain.

Spam

Between July 1 and December 31, 2006, spam made up 59 percent of all email traffic monitored by Symantec. This is an increase over the first six months of 2006 when Symantec classified 54 percent of email as spam.

The most common type of spam detected in the latter half of 2006 was related to financial services, which made up 30 percent of all spam on the Internet during this period. Spam related to health services and products made up 23 percent of all spam, while spam related to commercial products was the third most common type of spam, accounting for 21 percent of the total.

The rise in financially-related spam was due mainly to a noticeable increase in stock market "pump and dump" spam. Pump and dump is the name given to schemes in which criminals profit by creating an artificial interest in a stock they own. They buy a penny stock when the price is low. They then artificially pump up demand for the stock by sending out spam that appears to be from a respected stock advisor, but that actually contains false predictions of high performance for the stock. Recipients of the message, trusting the spam content, buy the stock, creating demand for it and thereby raising the price. When the prices are high, the perpetrators of the scheme sell their stock for a profit.⁸

This type of spam has been proven to allow the spammers to generate revenue directly and almost immediately.⁹ This alone is likely to make it more appealing than other types of spam.

A spam zombie is a computer infected with a bot or some other malicious code that allows email messages to be relayed through it. Between July 1 and December 31, 2006, ten percent of all spam zombies were located in the United States, making it the highest country in this category. During this period, the United States was one of the top reporting countries for bots such as Spybot and Mytob, which are commonly used to send spam.

China and Germany were the second and third highest countries for spam zombies, hosting nine and eight percent of the worldwide total, respectively. The small variance between the top countries hosting spam zombies is quite different from the distribution of bots during this period. This indicates that not all spam zombies are necessarily bots and that not all bots are used to send spam.

Bot-infected computers

Bots are programs that are covertly installed on a user's machine in order to allow an unauthorized user to control the computer remotely through a communication channel such as IRC. These channels allow the remote attacker to control a large number of compromised computers over a single, reliable channel in a bot network, which can then be used to launch coordinated attacks.

⁸ <http://www.sec.gov/answers/pumpdump.htm>
⁹ http://papers.ssrn.com/sol3/papers.cfm?abstract_id=920553

Bots allow for a wide range of functionality and most can be updated to assume new functionality by downloading new code and features. Bots can be used by external attackers to perform DoS attacks against an organization's Web site. Furthermore, bots within an organization's network can be used to attack other organizations' Web sites, which can have serious business and legal consequences. Bots can be used by attackers to harvest confidential information from compromised computers, which can lead to identity theft. Bots can also be used to distribute spam and phishing attacks, as well as spyware, adware, and misleading applications.

Between July 1 and December 31, 2006, Symantec observed an average of 63,912 active bot-infected computers per day. This is an 11 percent increase over the previous six-month period. Furthermore, Symantec observed 6,049,594 distinct bot-infected computers during the current reporting period, a 29 percent increase from the previous period. This increase is largely driven by a peak in bot activity in September when a number of vulnerabilities were disclosed that were actively exploited by bots.

Command-and-control servers are computers that bot network owners use to relay commands to bot-infected computers on their networks. In the last six months of 2006, Symantec identified 4,746 bot command-and-control servers, a 25 percent decrease from the first six months of 2006.

A drop in the number of command-and-control servers combined with a rise in the number of bot-infected computers indicates that, on average, bot networks are increasing in size. Bot networks are thus becoming more consolidated. Consolidated bot networks will likely mean that organizations will have to deal with a well entrenched, experienced, and dedicated group of bot network owners instead of a population of hobby hackers.

It could also signal a fundamental change in the way bots communicate with one another. Symantec has seen bots that are structured on a peer-to-peer model, in which the machines connect together rather than connecting to a central command-and-control server. Symantec has also observed that command-and-control servers are beginning to adopt encryption so that they are less visible.

China had the highest number of bot-infected computers during the second half of 2006, accounting for 26 percent of the worldwide total (figure 5). This is an increase of six percentage points over the previous six months. This increase was driven by a rise in the number of bots in the country rather than a decrease in other countries. This coincides with and illustrates a trend that Symantec first discussed in 2005, in which bot activity in China appeared to be increasing.¹⁰ During the second half of 2006, the United States had the second highest number of bot-infected computers, accounting for 14 percent of the worldwide total.

¹⁰ Symantec *Internet Security Threat Report*, Volume VII (March 2005): http://eval.veritas.com/mktginfo/enterprise/white_papers/ent-whitepaper_symantec_internet_security_threat_report_vii.pdf : p. 26

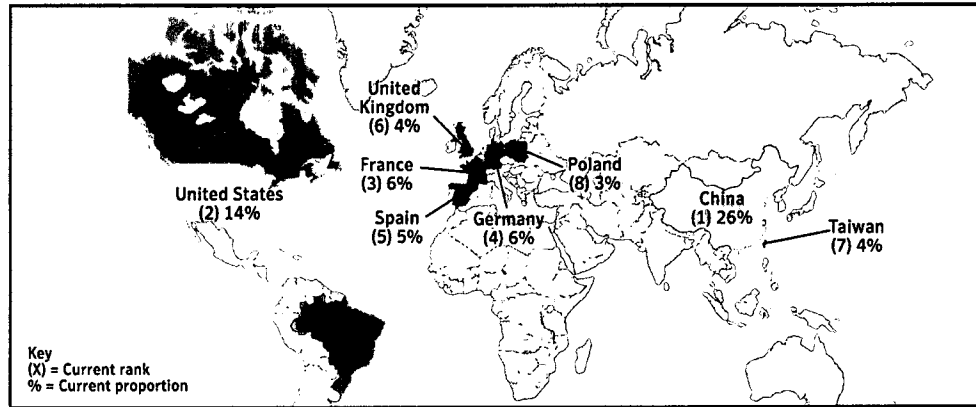


Figure 5. Bot-infected computers by country
Source: Symantec Corporation

The United States was the site of 40 percent of all known command-and-control servers, making it the highest ranked country in this category. The high proportion of command-and-control servers likely indicates that servers in the United States control not only bot networks within the country but offshore as well.

Organizations should monitor all network-connected computers for signs of bot infection, ensuring that any infections are detected and isolated as soon as possible. They should also ensure that all antivirus definitions are updated regularly. As compromised computers can be a threat to other systems, Symantec also recommends that the enterprises notify their ISPs of any potentially malicious activity. Creating and enforcing policies that identify and limit applications that can access the network may also be helpful in limiting the spread of bot infections.

To prevent bot infections, Symantec recommends that ISPs perform both ingress and egress filtering to block known bot traffic.¹¹ ISPs should also filter out potentially malicious email attachments to reduce exposure to enterprises and end users.

End users should employ defense-in-depth strategies, including the deployment of antivirus software and a firewall.¹² They should update antivirus definitions regularly and ensure that all desktop, laptop, and server computers are updated with all necessary security patches from their operating system vendor. Symantec also advises that users never view, open, or execute any email attachments unless the attachment is expected and comes from a known and trusted source, and unless the purpose of the attachment is known.

¹¹ Ingress traffic refers to traffic that is coming into a network from the Internet or another network. Egress traffic refers to traffic that is leaving a network, bound for the Internet or another network.

¹² Defense in-depth emphasizes multiple, overlapping, and mutually supportive defensive systems to guard against single-point failures in any specific technology or protection methodology. Defense in-depth should include the deployment of antivirus, firewalls, and intrusion detection systems, among other security measures.

Future Watch

This section of the *Internet Security Threat Report* will discuss emerging trends and issues that Symantec believes will become prominent over the next six to twenty-four months. These forecasts are based on emerging research that Symantec has collected during the current reporting period and are speculative in nature. In discussing potential future trends, Symantec hopes to provide organizations and end users with an opportunity to prepare themselves for rapidly evolving and complex security issues. This section will discuss potential security issues associated with the following:

- Windows Vista™
- Windows Vista and third-party software
- New phishing targets and methods
- Spam and phishing targeting mobile devices
- Virtualization

Threats posed to Windows Vista becoming evident

Microsoft's latest operating system, Windows Vista, was released publicly in January 2007. The release of an operating system that is expected to be widely adopted will likely have a significant effect on the security landscape. The previous *Internet Security Threat Report* discussed some of the general security concerns that may be associated with Windows Vista.¹³ Over the past six months, Symantec has continued to research potential issues associated with the new Microsoft operating system, which this section will discuss. These issues fall into three categories: vulnerabilities, malicious code, and attacks against the Teredo protocol.

In December 2006, Symantec reported a vulnerability in previous versions of Windows that also affects the version of Windows Vista that was released to consumers in January.¹⁴ This indicates that Microsoft's Security Development Lifecycle,¹⁵ while thorough, does not necessarily identify all potential vulnerabilities. This may be because some vulnerabilities can be extremely subtle.

That said, it appears that Microsoft's implementation of mitigating technologies such as address space layout randomization (ASLR), GS,¹⁶ and data execution prevention (DEP) could reduce the successful exploitation of any vulnerabilities that are discovered. Nevertheless, Symantec expects that new threats for Windows Vista will utilize older exploitation techniques that have been previously successful—such as those developed to successfully exploit Windows XP SP2—in order to bypass improvements in Windows Vista. For example, attackers may revert to attacks that utilize email, P2P, and other social engineering techniques.

Existing malicious code may also pose a problem for Windows Vista. According to research conducted by Symantec, some malicious code that did not originally target Windows Vista may affect the new operating system. This could be problematic because some enterprises may act on the belief that their installations of Windows Vista are immune from older malicious code samples. As a result, they may not deploy appropriate security solutions on new Windows Vista hosts, potentially leaving them vulnerable to infection by older malicious code samples. For instance, Symantec has already noted that some malicious code samples can infect Windows Vista.¹⁷

¹³ Symantec *Internet Security Threat Report*, Volume X (September 2006):

http://www.symantec.com/specprog/threatreport/ent-whitepaper_symantec_internet_security_threat_report_x_09_2006.en-us.pdf : p. 28

¹⁴ http://www.symantec.com/enterprise/security_response/weblog/2006/12/vista_vulnerable.html

¹⁵ The Secure Development Lifecycle is a development paradigm that incorporates security at every stage from the initial architecture to programming and in the quality assurance/testing phases. Threat modeling is a security auditing methodology that involves formally identifying and mapping out all possible attack vectors for an application. See the following for more information: <http://www.microsoft.com/presspass/features/2005/nov05/11-21SecurityDevelopmentLifecycle.mspx>

¹⁶ GS is a compiler technology. The name is derived from the compiler parameter that is used to enable this functionality. The use of GS will enable stack cookies to be placed around vulnerable functions in order to mitigate stack-based overflows.

¹⁷ For example, please see: http://www.symantec.com/enterprise/security_response/weblog/2006/12/hit_or_miss_vista_and_current.html

The third potential Windows Vista security issue identified by Symantec for this discussion is Teredo. Teredo is a protocol developed by Microsoft to enable the transition between versions of Internet protocol (IP), one of the protocols underlying all Internet-based communications. Teredo is enabled by default in Windows Vista. Computers using Windows Vista can easily be identified through Teredo.

Attacks sent over Teredo will often bypass organizations' network security controls since the protocol is tunneled through network address translation (NAT) over an IPv4 UDP connection. Many security products don't support Teredo and thus would not inspect it. This could make Windows Vista susceptible to attacks through Teredo.¹⁸

Symantec recommends that enterprises planning a migration to Windows Vista do so first in small, non-critical environments, and that thorough security audits be conducted to reduce possible exposure to attack. In addition, enterprises should ensure that any third-party security solutions they currently use will run on Windows Vista and are deployed in accordance with any existing security policies. Organizations contemplating using IPv6 within Windows Vista rather than Teredo should plan the IPv6 transition carefully, including native access and updated security controls.

Windows Vista release makes third-party software security paramount

With the advent of Windows Vista and the continued use of the Security Development Lifecycle, it is likely that Microsoft-authored code will become more difficult to exploit. As a result, attackers may turn their focus to common third-party applications that are authored by companies that have not employed the Security Development Lifecycle. These third-party applications may not use accepted best software-development practices, such as secure design, secure coding practices, code reviews, or secure developer tools such as Microsoft's Visual Studio.¹⁹ As a result, they may be less secure than Microsoft applications or the Windows Vista platform on which they are deployed.

These third-party applications could include third-party security software (such as antivirus), Web browsers, instant message clients, email clients, and office suites. They may include applications that have a significant user base, either globally or regionally. Symantec has already observed the emergence of a number of zero-day vulnerabilities being exploited in targeted attacks against office suites that are deployed in particular regions.²⁰

Due to the security improvements in Windows Vista, third-party drivers may be targeted as a means of gaining kernel-level access on compromised hosts. This is because these applications may not have been developed using the Security Development Lifecycle or other secure development practices. As a result, they may be susceptible to compromise. This could allow attackers to bypass the security improvements in Windows Vista, which are designed to prevent complete compromises, by running applications with non-administrative user privileges.

Only by implementing secure development practices can developers ensure the optimal security of their applications. Failure to employ all available secure coding measures will likely increase the probability of the discovery and successful exploitation of vulnerabilities.

¹⁸ For a more in-depth discussion on the security consequences of Teredo, please visit: http://www.symantec.com/avcenter/reference/Teredo_Security.pdf

¹⁹ Microsoft Visual Studio is important as it introduces a number of security features that can be enabled for unmanaged code. These features include enabling key security features for the application when executed under Windows Vista.

²⁰ A zero-day attack is one that attacks a vulnerability for which there is no available patch. It also generally means an attack against a vulnerability that is not yet publicly known or known of by the vendor of the affected technology. For example, Justsystem's Ichitaro zero-day was used to transmit a Trojan: http://www.symantec.com/enterprise/security_response/weblog/2006/08/justsystems_ichitaro_0day_used.html

New phishing economies

As phishing becomes entrenched as a mainstream attack activity, antiphishing techniques are improving and phishers are being forced to focus on new targets and adopt new methods. Symantec believes that, in the near future, phishers will expand the scope of their targets to include new industry sectors. For example, they will likely start to target a number of the secondary economies introduced through so-called massively multiplayer online games (MMOGs).²¹ MMOGs have become big business and are already attracting large groups of organized criminals who are using digital attacks for financial gain. In December 2006, forty-four suspects were arrested for stealing \$90,000 USD worth of digital assets from a single game.²²

Symantec also expects that phishers will develop new techniques to evade antiphishing solutions. Symantec has already started to see techniques to counter the effectiveness of block lists. For instance, phishers can use multiple unique URLs to direct users to a single Web site. Each URL is discarded after one use, so that even if they are placed on a block list, the lists still will not be able to block other URLs that direct potential victims to the same Web site. In some cases, Symantec has observed thousands of distinct URLs directing users to a single Web site.²³ Finally, attackers may already be using ready-made phishing kits. A phishing kit is a set of tools that an attacker can use to easily construct phishing email messages and Web sites based on a template.

Symantec has also observed that phishers are starting to adopt a technique known as intelligence lead phishing. This is a practice in which the phisher compromises a database or social networking site to obtain user information. This information is then used in a targeted phishing attempt against the user in question. The high degree of personalization made possible by the illicitly gained information can increase the effectiveness of the phishing attempt significantly. As widespread phishing attempts are increasingly choked off by antiphishing technologies, Symantec expects to see more phishing attacks that use these intelligence techniques.

In addition to the evolved phishing techniques outlined above, Symantec expects to see more generic phishing attacks; that is, attacks that are not restricted to spoofing a particular brand. For instance, instead of being required to know which bank the targeted user currently uses, a generic phishing attack could instead prompt the victim to "switch to Bank XYZ." These more generic phishing attempts can be restricted to a particular country if the phished institution is nationally based, thereby increasing the phisher's chance of success.

These recently evolved techniques illustrate the need for enterprises and end users to deploy effective antiphishing and antifraud solutions. Enterprises should be aware of and implement effective antiphishing technologies and practices. Enterprises that engage their clients over the Internet should continue to stay abreast of new phishing methods and techniques.²⁴ They should also monitor abuses of their brand in order to react appropriately and minimize potential damage to the company's reputation.

End users should follow best security practices, including the use of regularly updated antivirus software, antispyware software, firewalls, toolbar blockers, and other software detection methods. Symantec also advises end users to never disclose any confidential personal or financial information unless and until they can confirm that any request for such information is legitimate.

²¹ A massively multiplayer online game is an Internet-based computer game on which hundreds to thousands of players are capable of participating simultaneously.

²² Please see "Virtual Item Theft Ring Busted" <http://playnoevil.com/serendipity/index.php?archives/1051-Virtual-Item-Theft-Ring-Busted.html>

²³ http://www.symantec.com/enterprise/security_response/weblog/2006/12/phishing_2006_the_year_in_revi.html

²⁴ See the Symantec Phish Report Network, an extensive antifraud community where members contribute and receive fraudulent Web site addresses for alerting and blocking attacks across a broad range of solutions. It is available at: <http://www.phishreport.net>

Enterprises that use the Internet for any transaction-based activity should ensure that they have implemented phishing detection and response processes and procedures. In addition to providing a structured, standardized response to a phishing incident, this will also ensure that information is passed on to the appropriate resources, thereby protecting against subsequent use of the same attack.

Enterprises should ensure that their users are educated about phishing techniques and are informed of the latest phishing scams. For further information, the Internet Fraud Complaint Center (IFCC) has released a set of guidelines on how to avoid Internet-related scams.²⁵

SMiShing—Spam and phishing go mobile

In July 2006, Symantec reported that SMS and MMS had emerged as new vectors for spam and phishing activity.²⁶ Subsequently, the term SMiShing was coined by the industry to describe this class of threat.

There is a logical evolution from email to SMS and MMS as transport mechanisms for spam and phishing attacks. This is due in part to the fact that the technological and procedural defenses for devices deploying these services may not be as well developed or as widely deployed as those for other platforms. Additionally, users of mobile devices typically perceive messages received by SMS and MMS as being more personal than those received by email on a desktop computer. Furthermore, threats against these surfaces have been rare thus far. As a result, users are more likely to trust those messages and to act on them.

Targeting SMS and MMS may also offer attackers a significant benefit over targeting a specific mobile operating system. SMS and MMS are sufficiently well established and are deployed widely enough that they are available on almost all handsets on all networks. Most legacy and proprietary operating system handsets will support both of these technologies. As a result, they have a much larger target user base than smartphones.

There has been a rise in the amount of SMS-based premium-rate spam over the past few years since the introduction of subscriber-billed SMS.²⁷ This is a payment model in which the subscriber is billed a considerably higher cost for receiving a message than for sending one. This mechanism is typically used lawfully by the suppliers of ring tones, wallpapers, and other mobile content such as games. It is a convenient way of making micro-payments without having to introduce another payment tool such as a debit or credit card. However, some criminals have utilized the technology to obtain money, which has resulted in a number of national telecommunications regulators stamping out the practice.²⁸

Symantec speculates that SMS- and MMS-based phishing and spam will continue to increase. Cellular operators will likely be forced to invest in filtering technologies to combat this growing problem. This issue will be compounded by the fact that there are a number of different Internet-based SMS gateways that could allow users to supply their own originating number or name, which could be spoofed and used to send spam. As the costs of SMS services goes down, the likelihood that these gateways will be used for spam activities will increase.

²⁵ <http://www.fbi.gov/majcases/fraud/internetschemes.htm>

²⁶ SMS (short messaging service) is a service that is used for sending short text messages to mobile phones and other mobile text devices such as pagers. MMS (multimedia messaging service) is a service that allows mobile devices to send phone messages as well as multimedia files, such as images, audio, and video.

²⁷ <http://www.grumbletext.co.uk>

²⁸ <http://news.bbc.co.uk/1/hi/technology/4708167.stm>

Software virtualization brings new security threats

Software virtualization is a technology that allows one computer (the host) to run one or more distinct virtual computers (the guests). These virtual computers each run independently of the others and have their own virtual hardware, allowing the user to run multiple different operating systems on the same physical hardware.

Software virtualization has become a very powerful tool, bringing with it numerous benefits. However, many users assume that virtual machines provide a foolproof security barrier, leading to a false sense of security. While it is true that virtual machines can insulate against some current attacks, there are others against which they offer no protection. Further, they could potentially make new classes of attack possible. Symantec believes that the potential security implications of software virtualization have not yet been fully investigated and understood.

Guest virtual machines may not run the same security software as the host. For instance, they may not include antivirus software, personal firewalls, or host-based intrusion prevention products. As a result of these omissions, the virtual machines may be more exposed to threats than if they were run on independent hardware. Furthermore, virtual machines will do little to protect the data on the host. Consequently, virtualization technology may not diminish or protect against the threat of application-oriented threats such as phishing and data theft.

Symantec also believes that threats that are specific to virtualization technologies could emerge. With many different virtual machines being used, Symantec believes that these virtualization-specific threats could fall into two distinct classes of threat.

The first type of threat targets the use of real hardware in virtualized machines. Hardware drivers that provide software emulation of hardware acceleration outside of the virtual machine in the host operating system could be targeted from inside the guest operating system. An example of a vulnerability that illustrated this principle was the NVIDIA Binary Graphics Driver for Linux Buffer Overflow Vulnerability.²⁹ Symantec speculates that this type of vulnerability could be exploited from within the guest operating system to break into the host system. For enterprises that rely on separation through the use of software virtualization technology, the impact of this type of threat could be considerable.

The second type of threat that Symantec believes could emerge is related to the impact that software-virtualized computers may have on random number generators that are used inside guest operating systems on virtual machines. This speculation is based on some initial work done by Symantec Advanced Threat Research in a paper on GS and ASLR in Windows Vista. This research showed that the method used to generate the random locations employed in some security technologies would, under certain circumstances, differ wildly in a software-virtualized instance of the operating system. If this proves to be true, it could have considerable implications for a number of different technologies that rely on good randomness, such as unique identifiers, as well as the seeds used in encryption.

In the short to medium term, enterprises need to fully understand any potential impact that the use of software virtualization may have on the security of their environment and plan accordingly. They should control and monitor host operating systems very strictly, as the expected activity would likely be limited to the starting and stopping of virtual machines. Symantec feels that these threats constitute an important area of research and will continue to investigate and monitor these issues.

²⁹ <http://www.securityfocus.com/bid/20559>

About Symantec

Symantec is a global leader in infrastructure software, enabling businesses and consumers to have confidence in a connected world.

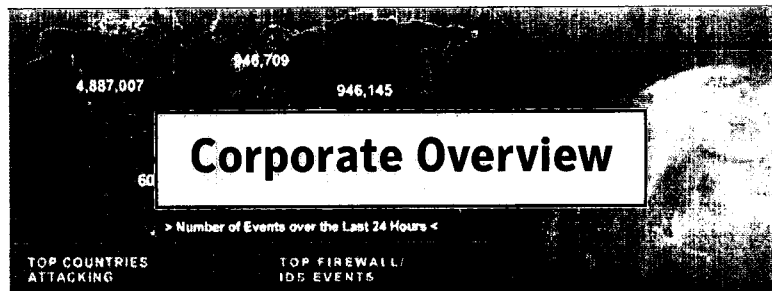
The company helps customers protect their infrastructure, information, and interactions by delivering software and services that address risks to security, availability, compliance, and performance. Headquartered in Cupertino, Calif., Symantec has operations in 40 countries.

More information is available at www.symantec.com.

For specific country offices and contact numbers, please visit our Web site. For product information in the U.S., call toll-free 1 (800) 745 6054.

Symantec Corporation
World Headquarters
20330 Stevens Creek Blvd.
Cupertino, CA 95014 USA
+1 (408) 517 8000
1 (800) 721 3934
www.symantec.com

Copyright © 2007 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo, Brightmail, and DeepSight are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Apple and Mac OS are registered trademarks of Apple Computer, Inc. Safari is a trademark of Apple Computer, Inc. Microsoft, Win32, Windows, and Windows Vista are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Sun and JavaScript are trademarks or registered trademarks of Sun Microsystems, Inc., in the U.S. or other countries. Other names may be trademarks of their respective owners. Printed in the U.S.A.
03/07 12114892



SYMANTEC CORPORATION | FOUNDED: April 1982 | **IPO:** June 23, 1989 | **HEADQUARTERS:** Cupertino, California, USA

PROFILE

Enterprises and consumers need to keep their infrastructures up and running 24x7. They need to be able to access information anytime and anywhere. That means that their critical systems must be up and running all the time.

Therefore, it is important that they protect the physical systems, the operating environments, and the applications - across all tiers of their infrastructure. They must protect a broad range of information types - from email to business documents to digital photos to audio and video files.

And, they must ensure that the interactions - the connections, the collaborative environments, and the movement of data while in use - are protected.

Symantec is focused on helping customers protect their infrastructures, their information, and their interactions. Headquartered in Cupertino, Calif., Symantec has operations in 40 countries.

SENIOR MANAGEMENT TEAM

- John W. Thompson, chairman and chief executive officer
- James Beer, executive vice president, chief financial officer
- Mark Bregman, executive vice president, chief technology officer
- Jeremy Burton, group president, enterprise security and data management
- Janice Chaffin, executive vice president, chief marketing officer
- Art Courville, executive vice president, corporate legal affairs and secretary
- Kris Hagerman, group president, data center management
- Greg Hughes, executive vice president, worldwide services and support
- Tom Kendra, group president, worldwide sales and services
- Rebecca Ranninger, executive vice president, chief human resources officer
- Enrique Salem, group president, consumer business unit
- James Socas, senior vice president, corporate development
- David Thompson, executive vice president, chief information officer

GEOGRAPHIC LEADERS

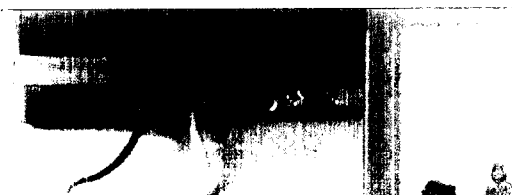
- John Brigden, senior vice president, Europe, Middle East, and Africa geography
- Steve Messick, senior vice president, The Americas geography
- Bill Robbins, senior vice president, Asia Pacific and Japan geography

BOARD OF DIRECTORS

- John W. Thompson, chairman and CEO, Symantec Corporation
- Michael Brown, former chairman and CEO, Quantum Corporation
- William (Bill) Coleman, founder, chairman, and CEO, Cassatt Corporation
- David Mahoney, former co-CEO of McKesson HBOC, Inc. and CEO of iMcKesson LLC
- Robert S. Miller, chairman and CEO, Delphi Corp.
- George Reyes, chief financial officer, Google
- David Roux, co-founder and managing director, Silver Lake Partners
- Daniel H. Schulman, chief executive officer, Virgin Mobile USA
- Paul Unruh, former chief financial officer and vice chairman, Bechtel Group, Inc.

HISTORICAL HIGHLIGHTS

<i>February 2006</i>	Relicore Inc. Acquisition
	IMlogic, Inc. Acquisition
<i>January 2006</i>	Bindview Acquisition
<i>October 2005</i>	Sygate Acquisition
	Whole Security, Inc. Acquisition
<i>July 2005</i>	VERITAS Software Merger
<i>May 2005</i>	XtreamLok Acquisition
<i>April 2005</i>	DataCenter Technologies, Inc. Acquisition
<i>December 2004</i>	Platform Logic Acquisition
<i>October 2004</i>	@stake Acquisition
	LIRIC Associates Acquisition
<i>September 2004</i>	KVault Software Limited Acquisition
<i>July 2004</i>	TurnTide Acquisition
	Invio Software, Inc. Acquisition
<i>June 2004</i>	Brightmail Acquisition
<i>February 2004</i>	ON Technology Acquisition
<i>January 2004</i>	Ejasent, Inc. Acquisition
<i>December 2003</i>	PowerQuest Acquisition
<i>October 2003</i>	SafeWeb, Inc. Acquisition
<i>June 2003</i>	Precise Software Solutions Ltd. Acquisition
<i>January 2003</i>	Jareva Technologies Acquisition
<i>August 2002</i>	Riptech, Inc. Acquisition
	Recourse Technologies Acquisition
	SecurityFocus Acquisition



July 2002	Mountain Wave Acquisition
October 2001	Lindner & Pelc Acquisition
July 2001	Foster-Melliar Acquisition
December 2000	AXENT Technologies Acquisition
November 2000	Network Storage Management Group of Seagate Acquisition
February 2000	L-3 Network Security Acquisition

GLOBAL PRESENCE

Symantec has facilities in 40 countries, with research and development facilities located in:

- AUSTRALIA
- BELGIUM
- CANADA
- CHINA
- GERMANY
- INDIA
- IRELAND
- ISRAEL
- JAPAN
- NEW ZEALAND
- UNITED KINGDOM
- UNITED STATES
 - California
 - Colorado
 - Florida
 - Maryland
 - Massachusetts
 - Minnesota
 - Oregon
 - Pennsylvania
 - Texas
 - Utah
 - Virginia

- Symantec has a number of Security Operations Centers and Security Response Labs around the world, providing 24x7 information security expertise.
- Symantec also has more than 25 Support Centers globally, helping individuals and enterprises with their security and availability needs.
- Symantec's primary manufacturing facility is located in Dublin, Ireland.
- Symantec has 260 issued U.S. patents in technologies addressing security, systems management, and storage needs for consumers, small businesses, and enterprises.

NOTABLE RECOGNITIONS

- Symantec ranked 672 on the 2006 *FORTUNE* 1,000 list, April 2006
- *FORTUNE Magazine* named Symantec a Blue Ribbon Company, a designation reserved for those select few corporations that achieve recognition on four or more of *FORTUNE*'s exclusive, trademarked lists, April 2005
 - Symantec ranked 65 on *FORTUNE*'s Fastest Growing Companies list, Sept 2005
 - Symantec ranked 792 on the 2005 *FORTUNE* 1,000 list, April 2005
 - Symantec debuted on *FORTUNE*'s 2005 America's Most Admired Companies list at number two in the Computer Software category, March 2005
 - Symantec ranked 43 on *FORTUNE*'s 2005 list of 100 Best Companies to Work For in America, January 2005

- Symantec ranked 32 on *BusinessWeek*'s 2005 Top 50 Performing Companies, April 2005

INDUSTRY LEADERSHIP

- Recognized by IDC as the world's leading hardware-independent provider of storage software, and the leader in backup and archiving and file system segments of the storage software market, December 2005
- Recognized by IDC as the world's leading vendor for secure content management for the fifth straight year, November 2005
- Listed in the Leaders Wave in the following Forrester Waves:
 - Enterprise antispyware, January 2006
 - Application mapping for configuration management database, January 2006
 - Message archiving software products, December 2005
- Listed in the Leaders Quadrant in the following Gartner Magic Quadrants:
 - Personal Firewall, June 2006
 - Email Archiving, May 2006
 - Managed Security Services, December 2005
 - Combined SRM and SAN Management Software, November 2005
 - Enterprise Backup/Restore, August 2005
 - Email Security Boundary, June 2005
 - J2EE Application Server Management, April 2005
- Recognized as global market share leader in the following categories:
 - Antivirus software, Gartner, June 2006
 - Core storage management software, Gartner, June 2006
 - Distributed systems backup/recovery software, Gartner, June 2006
 - Overall systems backup/recovery software, Gartner, June 2006
 - Messaging security software, IDC, November 2005
 - Clustering and availability software, IDC, July 2005

CUSTOMERS

- Symantec does business with 99 percent of the companies listed on the 2005 *FORTUNE* 1,000 list.

CONSUMER PRODUCTS

Symantec is leading the consumer industry with "Security 2.0," the company's vision for delivering end-to-end security for consumers and rebuilding confidence online. With Security 2.0, Symantec is focused on securing increasingly sensitive online consumer interactions, such as financial transactions and instant messaging, as well as increasingly malicious threats and crimeware. Symantec will deliver on this vision over the next several years via a combination of consumer client-side technologies, online infrastructure and key partnerships. Recently announced products like Norton Confidential, which will include new transaction security, and Norton 360, a new all-in-one subscription service, are first steps.

Symantec's Norton brand of consumer security solutions delivers Internet security and problem-solving capabilities to individual



users, home offices, and small businesses. The Norton brand of products is a market leader in desktop protection, with integrated products that work seamlessly to protect customers' computers from virus outbreaks and malicious attacks.

Internet Security Solutions help defend home and home office users against viruses, worms, and other security risks. These solutions include spyware, spam, and personal firewall protection for PCs, Macintosh® computers, and mobile devices.

System Performance Solutions help users prevent and resolve computer problems.

Backup and Recovery Solutions provide consumers with tools to undo computer malfunctions and safeguard their important data.

Remote PC Solutions allow users to manage remote computers securely.

ENTERPRISE AVAILABILITY

Symantec offers products for backup and recovery of data and systems, optimizing storage resource utilization, simplifying administration of heterogeneous environments, and providing continuous availability of mission-critical applications and data.

Application Performance Management products optimize the performance and availability of enterprise applications.

Data Management Solutions are designed to protect, backup, archive, and restore data across a broad range of computing environments - from large corporate data centers to remote groups and desktop and laptop computers. The products integrate to provide solutions to manage data throughout its lifecycle - from creation to disposal, onsite and offsite, across all levels of storage hierarchy - including disk, tape, and optical storage media.

Infrastructure Management Solutions allow customers to manage virtually any function at any point in the lifecycle of their computing systems and devices. Solutions include network auto-discovery and IT asset management, operating system provisioning and application deployment, ongoing security updates and configuration management, rapid system recovery, de-provisioning, and help desk remote control.

Data Center Management Solutions help organizations gain control, improve service levels, and drive down costs within complex data center environments. These technologies deliver storage automation, virtualization, replication, high-availability clustering, server provisioning, and server management software across heterogeneous storage and server platforms.

ENTERPRISE SECURITY

Symantec provides enterprise security solutions for all network tiers: the gateway, the server, and the client level, including PCs, laptops, and handhelds.

Antivirus Solutions offer critical protection at the gateway, server, and client tiers against known and unknown threats.

Antispam Solutions filter spam and other undesired messages at the gateway and are critical to an overall email security solution.

Integrated Client Security Solutions are designed to ensure enterprise client systems are safe by providing comprehensive, proactive protection against blended threats, spyware, unauthorized network access, and other attacks.

Integrated Gateway Security Solutions are easy to manage, multifunction security appliances designed to provide fully integrated, layered security at the network gateway.

Intrusion Protection Solutions monitor systems for patterns of misuse and abuse and can warn organizations before systems or information is compromised.

Managed Security Services provide a comprehensive array of outsourced security management, monitoring, and response services to help organizations solve security problems cost effectively. Managed Security Services allow organizations to leverage the knowledge of Symantec's Internet security experts to protect the value of their networked assets and infrastructure.

Policy Compliance Management Solutions help customers define, manage, and enforce policies from a central location as well as probe for network vulnerabilities and suggest remedies to proactively reduce business risk.

Security Management Solutions provide a comprehensive solution for the consolidation of security events, the containment of security threats, and the centralization of security policy enforcement. These products are built on an open, interoperable framework that enables Symantec products to work together with third party solutions to provide secure, manageable, and scalable enterprise security.

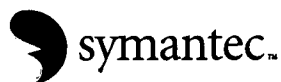
Threat and Early Warning Systems provide customized and comprehensive alerts of impending cyber attacks worldwide - with countermeasures to prevent attacks before they occur - enabling companies to mitigate risk, manage threats, and help ensure business continuity.

SERVICES

Symantec provides a full range of services to assist our customers in assessing, architecting, implementing, supporting, and maintaining their security, storage, and infrastructure software solutions. Our global services organization also provides customers with maintenance and technical support, consulting, and education services.

WORLDWIDE HEADQUARTERS

20330 Stevens Creek Blvd.
Cupertino, CA 95014
+1 408 517 8000
+1 408 517 8186 fax
www.symantec.com





RECOMMENDATIONS FOR STATE POLICYMAKERS TO SECURE THEIR STATE IT INFRASTRUCTURE AND PROMOTE CYBER AWARENESS

State governments looking to ensure the security of their networks should consider these basic best practice principles that are outlined in The National Strategy to Secure Cyberspace:

Take a comprehensive, risk-based approach.

Examine the state's IT inventory, analyze present and future risks, and develop mitigation plans.

Focus on prevention.

Develop processes and implement technologies that assist in stopping threats before they occur.

Use automated tools.

Relieve the burden of multiple manual processes, and provide effective tools for security reporting.

These basic principles provide states with a broad menu of options. Each state should evaluate its own unique situation and develop a plan that best addresses its individual needs and goals. Some of the options available include:

Vulnerability Assessments

State governments should conduct a thorough vulnerability assessment of their networks. Risks should be understood and acknowledged and then states should consider a balanced approach to implementing security measures that address those risks.

Legislation to Secure State Information and IT Infrastructure

State legislatures should consider legislation that sets information security requirements for state agencies. Risk-based security policies based on industry best practices should be aligned with state government objectives. To develop requirements, states can model their legislation on the Federal Information Security Management Act (FISMA), and the privacy provisions contained in the Gramm-Leach-Bliley Act and the Health Insurance Portability and Accountability Act.

Education

This is perhaps the single most potent weapon available to states. Educating at all levels of state government through a well-organized security-training program will arm state legislators, executive branch officials, and state employees with the knowledge to responsibly protect the state's networks.

State Awareness Campaigns

State legislatures can help build awareness of cybersecurity both within the government and among the state's residents by passing a resolution calling for a greater focus on information security. States can also take an active part in the

national cyber security awareness campaign with DHS and the National Cyber Security Alliance (www.staysafeonline.info).

Consolidation of IT purchasing

Consolidating IT purchasing statewide provides several benefits to states. In addition to ensuring uniformity of systems, it also allows states to leverage their purchasing power and benefit from economies of scale.

Information Sharing

States should consider establishing information sharing and analysis centers to better coordinate the efforts of officials at all levels of government and the private sector in monitoring, analyzing, and responding to information security threats and attacks.

Executive Orders

Some of the options available to states can be accomplished through executive orders of the governor. Through the budgetary process and executive order, governors can stress the importance of planning and budgeting for cybersecurity, as well as promoting organizational changes that allow for more efficient, consistent, economical, and secure IT practices within and across states.

Symantec looks forward to working with you on important information security issues facing your state. Please feel free to contact our State Government Relations Team:

Stephanie Reich
Manager, Northeast/Great Lakes
Phone: (202) 742-6584
E-mail:
Stephanie_Reich@Symantec.com

Owen Sweeney, Jr.
Manager, Southeast/Midwest
Phone: (202) 742-6583
E-mail:
Owen_Sweeney@Symantec.com

Leslie Bar-Ness
Manager, West
Phone: (408) 517-5273
E-mail:
Leslie_Bar-Ness@Symantec.com



EIGHT QUESTIONS A LEGISLATOR SHOULD ASK THE CHIEF INFORMATION OFFICER¹

Question 1: How are we doing so far?	Incidents. Over the past year: <ul style="list-style-type: none">• Was confidential data compromised?• Was data lost or corrupted?• Was equipment stolen or misused?• Was email or Internet service interrupted?• Did virus or spam attacks cause shutdowns?
	Causes. Were problems caused by: <ul style="list-style-type: none">• Inadequate technical safeguards?• Insufficient staff training?• Unauthorized access to or use of systems by insiders?• Intrusion by outsiders?
	Impact. Did security problems result in: <ul style="list-style-type: none">• Loss of efficiency, productivity, or other costs?• Failure to meet state objectives?• Damage to reputation?• Harm to citizens or government employees?
Question 2: Do we have a security plan?	Security plan status. <ul style="list-style-type: none">• When was our security plan last updated?• When was our security plan most recently reviewed by outside experts?• What steps does the plan require us to do?• What are the major risks we are still exposed to?
Question 3: Do we have adequate security and privacy policies in place?	Agency security rules. <ul style="list-style-type: none">• Do we have a clear policy about data privacy?• Have rules been effectively communicated to employees and other officials?
	Legal review. <ul style="list-style-type: none">• Has the policy been reviewed by legal counsel to ensure alignment with local, state, and federal laws and regulations – including FISMA, HIPAA and GLB?

¹ Adapted from the Consortium for School Networking document "Eight Questions A Superintendent Should Ask the Chief Technology Officer."

	<p>External controls.</p> <ul style="list-style-type: none"> • Are we confident that the data and communication systems of our outside service providers (payroll, email, data warehouse) are secure? • How have we verified those assurances?
<p>Question 4: Are our network security procedures and tools up to date?</p>	<p>Hardware.</p> <ul style="list-style-type: none"> • Can our network equipment support current security standards? • Are all desktop computers individually protected from internal viruses?
	<p>Software.</p> <ul style="list-style-type: none"> • Do all our computers receive security patches or virus definition updates automatically? • If not, how long does it take to fully install patches/updates from the time they are released?
	<p>Monitoring.</p> <ul style="list-style-type: none"> • Do we have the capacity to centrally monitor the status of all our equipment to know which machines are not secure, and to remotely perform other troubleshooting? • Are our systems set up to enforce all our network security, system access, and data privacy policies?
<p>Question 5: Is our network perimeter secured against intrusion?</p>	<p>Design.</p> <ul style="list-style-type: none"> • Is our network designed to prevent unwanted intrusion? • Do we have external and internal firewalls?
	<p>Laptop problems.</p> <ul style="list-style-type: none"> • Are we able to deal with viruses and other problems brought in through home-used laptops and other mobile devices?
	<p>Wireless security.</p> <ul style="list-style-type: none"> • Have we secured wireless networks against intruders?
	<p>Passwords.</p> <ul style="list-style-type: none"> • Do we enforce regular updates of secure passwords by all users?
<p>Question 6: Is our network physically secure?</p>	<p>Environmental hazards.</p> <ul style="list-style-type: none"> • Is all network equipment located in facilities protected against flooding, burst pipes, freezing, overheating, or fire?

	<p>Physical security.</p> <ul style="list-style-type: none"> • Do we regularly check to ensure that only authorized people can physically access key equipment? • Is all network equipment located in locked rooms dedicated solely for that purpose (no secondary custodial or secretarial use)? • Is all end user equipment cabled down and labeled?
<p>Question 7: Have we made our users part of the solution?</p>	<p>Awareness.</p> <ul style="list-style-type: none"> • How well do all users understand their own self-interest in keeping our IT systems operational, and know what they need to do to maintain system security? • How do we encourage user involvement in setting, enforcing, and reviewing security policies?
	<p>Training. Is there a sufficient program of user training, and does that training include security issues?</p>
	<p>Communication. Is there a regular flow of communication with and feedback from all users? What happens to user complaints and suggestions?</p>
<p>Question 8: Are we prepared to survive a security crisis?</p>	<p>Backups. Is all our data regularly backed up to both a secure internal and a secure external location?</p>
	<p>Redundant systems. Do we have redundant network connections (with at least minimal capacity among our buildings and from our network to our key external vendors) so that we can continue operations if our communication networks are compromised?</p>
	<p>Communication plan. If a crisis were to occur, are we prepared to stay in touch with employees, legislative and executive officials, municipal leaders, the media, and other stakeholders about the extent of the problem and our progress in dealing with it?</p>
	<p>Preparedness.</p> <ul style="list-style-type: none"> • Are crisis response staff identified and trained? • Have we done a "dry run" test of our crisis management plan recently? • Have we improved our crisis management plan as a result of that test?



PROTECTING INVISIBLE BORDERS: A DIGITAL CHALLENGE FOR STATES IN THE 21ST CENTURY

OVERVIEW OF THREATS FACING STATE GOVERNMENTS

Ensuring the security of government-held information and protecting government information technology infrastructure are critical issues for state governments. This infrastructure includes those systems so vital to the U.S. that the incapacity or destruction of them would have a debilitating impact on security. States are responsible for protecting this critical infrastructure to ensure reliable access to important services, to ensure agencies can communicate with their first responders, and to maintain the privacy of citizens' personal information. In our digitally-connected world, legislators and executive branch officials play an indispensable role in creating and implementing consistent information security policies that enable efficient and secure agency operations.

IT networks are increasingly vulnerable to attack. The cyber threats we are seeing today are more sophisticated, more aggressive and are able to spread more rapidly than ever before. Equally important, the time from the discovery of a new vulnerability in a network to the release of an exploit targeting that vulnerability is rapidly shrinking.

Further, the types of threats facing networks are increasingly diverse and complex. Keeping abreast of the threat environment can be a full-time job. Symantec produces a six-month update about Internet threat activity titled the *Internet Security Threat Report*. It includes an analysis of network-based attacks, a review of known vulnerabilities, and highlights of malicious code. With over 40,000 sensors monitoring network activity in over 180 countries, as well as information compiled from over 120 million client, server and gateway systems that have deployed our antivirus products, and 25 million e-mail messages we filter for our customers every day, Symantec has established one of the most comprehensive sources of threat data in the world. Some highlights of the most recent report include:

- The shift from attacks for notoriety towards targeted attacks for financial gain continued during the first half of 2006;
- Between January 1 and June 30, 2006, the home user sector was the most highly targeted sector, accounting for 86% of all targeted attacks;
- The Symantec Probe Network detected 157,477 unique phishing messages, an increase of 81% since the last report;
- Symantec identified an average daily total of 57,717 active "bot" network computers—programs that are covertly installed on a targeted system that allow unauthorized users to remotely control the compromised computer;

- Symantec documented 2,249 vulnerabilities during the first half of 2006 – the highest total Symantec has ever recorded. Systems in the United States are the primary source of attacks; however, the percentage of attacks originating in other countries is increasing;
- The majority of documented vulnerabilities – 78% – affected Web browsers.

Finally, should a serious attack hit a government IT system, there would be significant costs incurred. Estimated costs of cyber attacks amongst a randomly picked sample in 2005 alone were \$130,104,542 (Source: CSI/FBI Computer Crime Survey, 2005). However, these costs do not include the related costs of responding to the attacks, restoring systems to their pre-attach state, and recovering lost data, all of which are extraordinarily expensive. There would also be costs associated with lost productivity of the government workforce when there is a disruption in service. System recovery costs would increase exponentially with the scope of the incident and any delays in effective response.

STEPS THE FEDERAL GOVERNMENT IS TAKING TO SECURE ITS INFORMATION AND IT INFRASTRUCTURE AND HOW THEY RELATE TO STATES:

As some state legislators and executive branch officials are already aware, the federal government has detailed information security policies and standards in place that some state networks must adhere to. In December 2002, the E-Government Act was signed into law by President Bush. Title III of this act is the Federal Information Security Management Act, or FISMA. The primary purpose of FISMA is to provide a comprehensive framework for ensuring the effectiveness of information security controls in federal agencies. However, the law also stipulates that state agencies which use federal systems, or which manage portions of federal programs where information systems must be shared, are subject to FISMA security requirements. For example, state tax agencies that share federal tax data are subject to FISMA. Other federal security requirements pertaining to personal consumer information are contained in the Gramm-Leach-Bliley Act and the Health Insurance Portability and Accountability Act.

Key requirements contained in FISMA that apply to certain state agencies include:

Agency-wide security program – FISMA requires that each agency develop and implement information security policies, procedures, and control techniques in accordance with risk and the magnitude of potential harm.

System configuration management – FISMA requires that each agency establish and maintain standard system security settings as well as a patch management process.

Inventory of systems – The head of each federal agency must develop and maintain an annually updated inventory of major information systems operated by or under the control of the agency. The identification of information systems in this inventory must include the interfaces between each

system and all other systems and networks, including those not operated by or under the control of the agency.

Continuity of operations – In compliance with FISMA, each system security plan must include the provision for continuity of operations for information systems that support the operations and assets of the agency.

Testing and evaluation of security controls – FISMA requires that testing and evaluation be performed annually.

Incident response capability – FISMA requires that each agency have the technical and procedural means to detect, respond to, and report security incidents, as well as to share information on common vulnerabilities.

Use of NIST standards and guidelines – The National Institute of Standards and Technology has developed compulsory and binding standards that will be used to “categorize all information and information systems collected or maintained by or on behalf of each agency.”

CONCLUSION

Networks are only as strong as the weakest link. In an ever increasingly inter-connected world, one state's lack of security can quickly become the problem of an entire nation. However, many options are available to state governments to address the need for security.

The Federal government's FISMA requirements, as well as the privacy requirements contained in Gramm-Leach-Bliley privacy law and the Health Insurance Portability and Accountability Act, are good models for states to adopt. Additionally, the states of Oregon and Colorado recently passed two of the most comprehensive information security laws in the nation, which are modeled after FISMA.

Security is more than just installing a piece of software; it is a process as well as a state of mind. Symantec promotes public-private partnerships with state governments to help ensure a safe and secure computing environment that ultimately better protects users and our critical infrastructure.

We look forward to working with you on important information security issues facing your state. Please feel free to contact Symantec's State Government Relations Team:

Stephanie Reich
Manager, Northeast/Great Lakes
Phone: (202) 742-6584
E-mail:
Stephanie_Reich@Symantec.com

Owen Sweeney, Jr.
Manager, Southeast/Midwest
Phone: (703) 283-0347
E-mail:
Owen_Sweeney@Symantec.com

Leslie Bar-Ness
Manager, West
Phone: (408) 517-5273
E-mail:
Leslie_Bar-Ness@Symantec.com



2007 STATE PUBLIC POLICY PRIORITIES

Data Security

Symantec strongly supports passage of effective and meaningful data security law that requires public and private entities to secure the integrity of consumers' sensitive personal information. Rather than focusing on the aftermath of a data breach, a state's data security law should minimize the likelihood of a breach by:

- Requiring companies to take reasonable security measures to ensure the integrity of sensitive personal information.
- Including incentives for companies to protect data, such as an exemption for entities that adopt reasonable data security measures or best practices, like encryption.
- Encouraging heightened enforcement -- through increased appropriations -- against entities that fail to use reasonable security measures to protect consumers' data.

Cyber Crime: Spyware & Phishing

Symantec urges States to enact laws that provide strong criminal penalties for entities that distribute crimeware to consumers' computers. States should:

- Enact specifically tailored anti-spyware legislation with strong criminal penalties to help deter cyber crime. Such legislation should focus specifically on eliminating bad behavior, not defining "bad" technologies, since technologies can be used for multiple uses.
- Enact laws to criminalize "phishing", which are e-mail fraud scams conducted for purposes of information or ID theft.

Data Retention/E-Discovery of Public Electronic Records

Since databases containing personal information are becoming prime targets for cybercrime, Symantec believes that any data retention bill considered should: specifically address not just what data is retained by state government authorities, but how it is secured.

Increased awareness of the importance of the retention and production of public electronic records for FOIA and civil litigation purposes requires State authorities to more proactively deal with how these records are managed. Recent amendments to the Federal Rules of Civil Procedure and concomitant State Supreme Court Guidelines and NCCUSL draft rules suggest that State Authorities consider the following:

- Apply practicable record retention policies to electronic public records, including email records, so that these records are preserved consistent with legal requirements and the interests of the public, balanced by the need for efficiency and streamlined cost of government operations.
- In order to achieve consistency of retention policy enforcement, implement systems to automate the process for classification and retention of records, as well as their disposition.
- Implement comprehensive and automated systems to suspend the disposition of public records pursuant to a retention policy, where there is an additional duty to preserve, for example based on a specific FOIA request or due to pending civil litigation.

eHealthcare Reform: Security and Privacy

Symantec supports initiatives to drive improved quality, efficiency and cost-savings in the U.S. healthcare system through the adoption of technology-based systems to integrate, manage and protect health records. Specifically:

- Symantec urges States to establish a policy for security and privacy of electronic health records. Such a policy should adopt reasonable security and privacy standards in keeping with the Standards Harmonization Process and HIPAA requirements.
- As States continue addressing the challenges incumbent in developing policies for an interoperable, reliable, and secure system for widely adopting the use of e-health records, HIPAA's Security and Privacy Standard be used as a guiding principle as you discuss and develop statewide policies. The HIPAA Security and Privacy Standard defines administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of electronic protected health information. However, if the state feels that specific security and privacy measures are missing from HIPAA, Symantec healthcare experts would be happy to work with the state to help formulate these additional measures.
- Symantec believes that for statewide e-health privacy and security policies to be most effective, they should be applied equally to both private sector health institutions and public sector institutions.

Securing State Systems

Symantec supports efforts to enhance law that requires baseline levels of cyber security at State agencies. Specifically, the State should:

- Enhance oversight of State agency IT security;
- Press for modernization of State agency IT security without prescribing technology mandates.
- Symantec has been working with several states on developing more comprehensive information security management policies.

On-Line Safety and Security

Symantec is committed to empowering parents and educators with the tools they need to create a safe and trusted online experience for children. We believe that comprehensive online safety legislation should include three different aspects:

- 1) Cyber Safety Best Practices: These practices incorporate many social behavior tips to protect children from online dangers. Some examples include:
 - i. Keep safe your personal information—all of it! Never give your real name, address, phone number, the name of your school, or a picture of yourself to anyone online.
 - ii. Keep away from Internet strangers—no matter what they tell you, because you have no way of knowing who they really are. Don't talk with them online, and I never meet them face-to-face.
 - iii. Keep open lines of communication with a parent or teacher. If you are worried about something you have seen or been sent online, tell them right away.
 - 2) Cyber Security Best Practices: In addition to teaching a child about how to turn on a computer, type in a URL and use a mouse, we should be teaching children how to be computer savvy and secure. Tips like "Use antivirus, a firewall, and antispyware and keep them current" are very important so that children understand there are technology solutions to help keep them and their information protected.
 - 3) Cyber Ethics: We teach children from an early age that stealing something from someone's desk or breaking into someone's home is wrong and against the law. But we forget to teach them these same ethics apply in the cyber world. For example, hacking into someone's computer and taking information or something from is just as wrong as breaking into someone else's home. Cyber bullying is just as wrong as bullying someone at the playground. You set rules, boundaries, and codes of acceptable behavior in the real world; do the same for the virtual world. By instilling these values, we are preventing children from becoming cyber criminals.
- We would suggest you also coordinate with some other non-profit organizations, like the National Cyber Security Alliance and IKeepSafe who have significant expertise in this area and would be happy to act as a co-convenor in these discussions. In fact, NCSA has already held several education roundtable discussions on this very issue and have plans to work with several states on online safety, security and ethics programs this year. The NCSA is also in the process of developing a school assembly toolkit for K-5 children and are planning to retool their kit that was already created for middle/high school students. This kit can be found at www.staysafeonline.org.