STOP.THINK.CONNECT.™

National Cybersecurity Awareness Campaign

Small Business Presentation

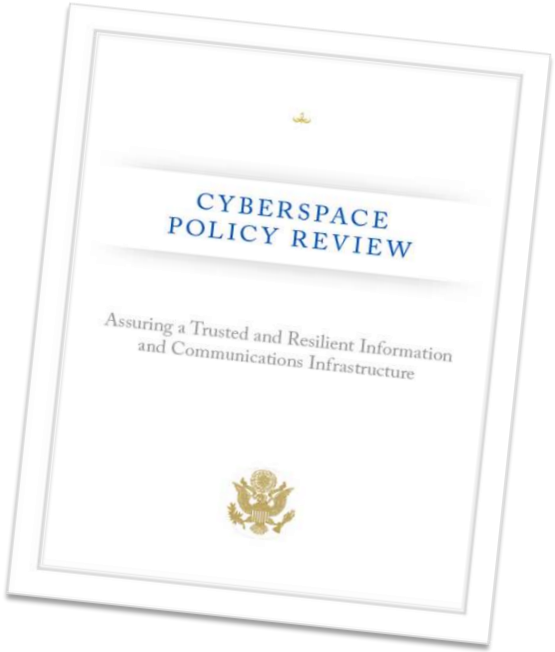
Homeland Security

STOP | THINK | CONNECT™

About Stop.Think.Connect.

- In 2009, President Obama issued the *Cyberspace Policy Review*, which tasked the Department of Homeland Security with creating an ongoing cybersecurity awareness campaign–Stop.Think.Connect.– to help Americans understand the risks that come with being online.

- Stop.Think.Connect. challenges the American public to be more vigilant about practicing safe online habits and persuades Americans to view Internet safety as a **shared responsibility** in the home, in the workplace, and in our communities.



National Cyber Security Awareness Month

Shared Responsibility

Today, we are more interconnected than ever before. Most businesses today wouldn't exist without the Internet

- Not only do businesses rely on technology to perform daily functions, but the Internet provides easy ways for businesses to stay connected, informed, and involved
- With these increased conveniences comes increased risk
- Many of the crimes that occur in real life are now done - or at least facilitated - through the Internet. Human trafficking, credit card fraud and identity theft, embezzlement, and more – all can be and are being done online
- No country, industry, community, or individual is immune to cyber risks, and no one government agency, company, or individual can solve the riddle of cybersecurity
- We all have to work together to secure cyberspace

STOP.THINK.CONNECT.™

Did You Know?

40% of all cyber attacks target business with fewer than 500 employees?

- 52% of businesses have a cybersecurity plan[1]
- 40% of businesses do not have an incident response plan should a loss of data occur[1]
- 77% revealed they do not have a formal, written Internet security policy for employees[1]
- 74 % of small businesses reported attacks from 2009 to 2010 with an average cost of about $190,000 per attack[2]
- Cyber crime has surpassed illegal drug trafficking as a criminal moneymaker[2]

Homeland Security

1. 2011 National Small Business Study by the National Cyber Security Alliance and Symantec
2. Symantec

STOP | THINK | CONNECT™

The Reality of Cyber Attacks

- **All businesses**, regardless of size, are at risk. Small businesses may feel like they are not targets for cyber attacks either due to their size or the perception that they don't have anything worth stealing
- Only a small percentage of cyber attacks are considered targeted attacks, meaning the attacker group is going after a particular company or group of companies in order to steal specific data
- The majority of cybercriminals are indiscriminate; they target vulnerable computer systems regardless of whether the systems are part of a Fortune 500 company, a small business, or belong to a home user

"It's easy for small businesses to become lax in regards to their Internet security, thinking they're too small for hackers to bother with. However, according to the Minnesota Cyber Crime Task Force, these are the businesses which are squarely in the crosshairs of cyber criminals."

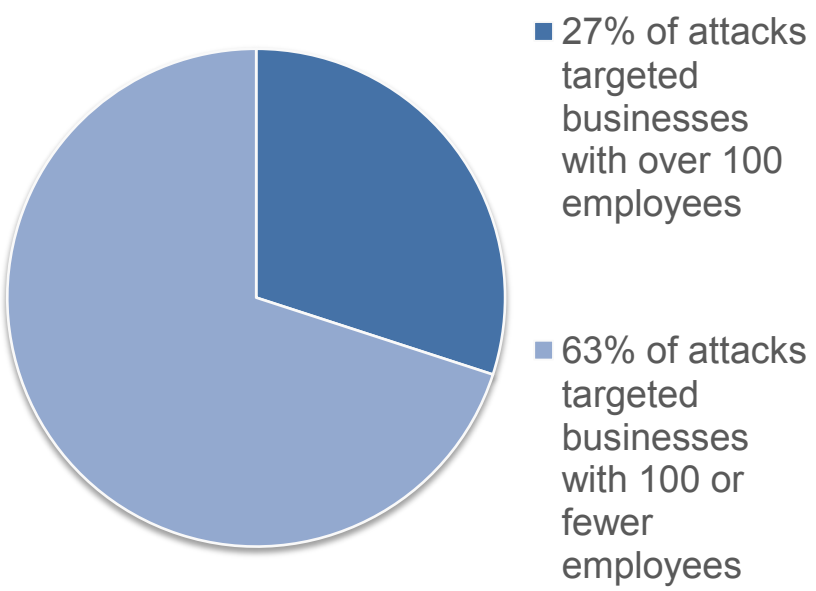
-Dana Badgerow, President and CEO of the Better Business Bureau

Small Business Breaches

Small companies, which are making the leap to computerized systems and digital records, have now become targets for hackers

- With limited budgets and few or no technical experts on staff, small businesses generally have weak security
- In 2010, the U.S. Secret Service and Verizon Communications Inc.'s forensic analysis unit, which investigates attacks, responded to a combined 761 data breaches, up from 141 in 2009. Of those, 482, or 63%, were at companies with 100 employees or fewer
- Visa estimates about 95% of the credit-card data breaches it discovers are on its smallest business customers

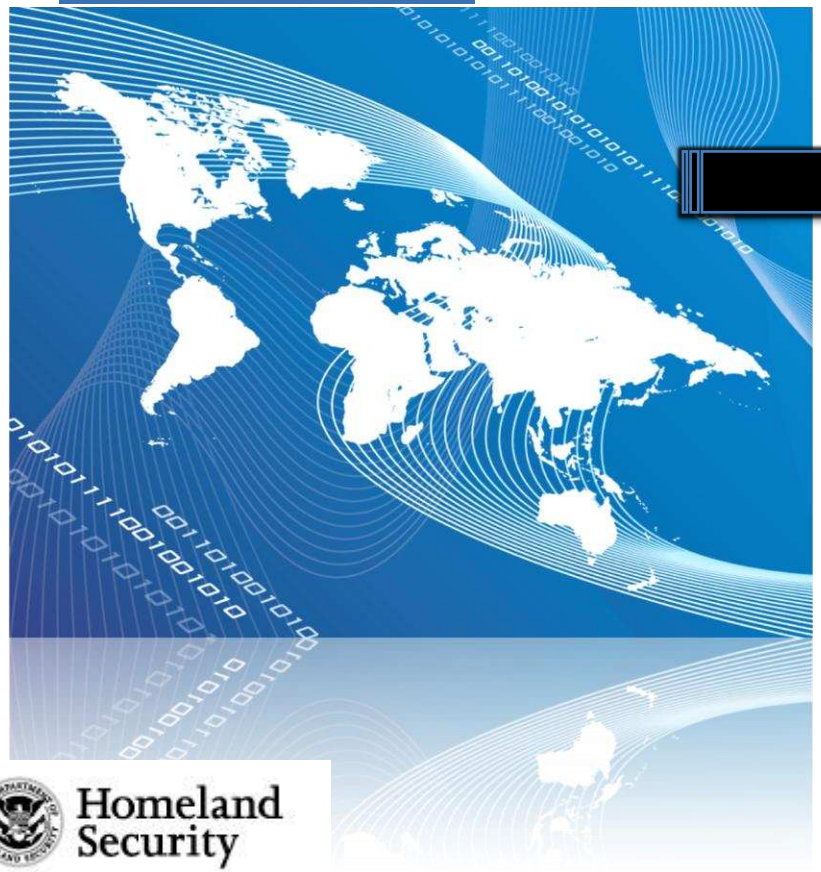
2010 Breaches Reported to Verizon, Inc. and the U.S. Secret Service



Big Business Breaches

Google claims attacks came from abroad.

January 2010, Google announced that it had been the victim of a cyber attack…



Google™

Google Breach

- Proprietary code was stolen, and Gmail accounts of human rights activists were broken into, possibly to spy on them
- One of the first companies to ever publicly announce a data breach as soon as it happened and then go to the government for help

STOP.THINK.CONNECT.™

. . . June 2010, hackers used an exploit in AT&T's website to steal 114,000 user emails and the names associated with them…

AT&T Breach

- Obtained data through a script in the Apple website.
  - Almost all "A-Listers," including movie stars, generals, and head political figures.
- Could lead to far more precise phishing attacks.
  - More precise phishing increases the criminal's chances of success.
  - Could cause malware to be installed on their computers, giving away secret/sensitive information.

STOP.THINK.CONNECT.™

…April 2011, PlayStation Network and Sony Online Entertainment were breached, causing the loss of millions of users' data.

Sony Breach

- 77 Million credit card numbers stolen, along with names and addresses
- PlayStation Network was shutdown for a month, and was re-hacked 2 days after it was brought back
  - Hackers used an exploit that allowed them to change a user's password if they knew the e-mail address and date of birth
- A group called LulzSec claimed credit and would go on to hack into Senate.gov and DDoS CIA.gov

5 Tips for Your Business

- **Assess risk and identify weaknesses** – Is your sensitive information linked to the Internet?
- **Create a contingency plan** – Enact security practices and policies to protect the sensitive information of your organization and its employees, patrons, and stakeholders; hold employees accountable to the policy.
- **Educate employees** – Make sure that employees are routinely educated on new and emerging threats and the best ways to identify and report suspected incidents; require that employees use strong passwords and regularly change them.
- **Back up critical information –** Establish a schedule to perform critical data backups to ensure that critical data is not lost in the event of a cyber attack or natural disaster. Store all backup in remote locations away from the office, such as on an external hard drive, and encrypt any sensitive data about the company or customers .
- **Secure your Internet connection** – Use and regularly update antivirus and antispyware software on all computers; use a firewall, encrypt information, and hide your Wi-Fi network.

Do Your Part

Consumers are taking notice of how businesses secure their data and are more willing to trust and reward businesses for good security practices. Nearly 85% of consumers in a recent survey said they would increase their shopping at a store known for good cyber security practices, while only 20% said they would continue shopping at a store that had a recent data breach. [1]

- As a business owner, you can earn customers' respect as a trusted business partner by promoting the security practices that you have implemented to protect their data.
- The losses resulting from cyber crimes, which can severely damage a businesses' reputation, often outweigh the costs associated with the implementation of a simple security program.
- By implementing a security program that involves both technical controls and cultural adjustments, you, small businesses can take a big step in fighting cyber crime.

1. Javelin Strategy & Research

Call to Action

Cybersecurity is a shared responsibility that all Americans must adopt in their communities in order to keep the nation secure in the 21st Century. Become an advocate in your community to help us educate and empower the American public to take steps to protect themselves and their families online.

How to get involved:

- Become a *Friend* of the Campaign by visiting **www.dhs.gov/stopthinkconnect.**
- Make cybersecurity a priority. Discuss safe online practices with your fellow employees.
- Inform your community about the Stop.Think.Connect. Campaign and the resources available.
- Blog or post about the issue of cybersecurity and the Stop.Think.Connect. Campaign.
- Host a cybersecurity activity in your office.
- Download and distribute Stop.Think.Connect. materials, such as the brochure, bookmark, and poster, to your employees and communities.

STOP.THINK.CONNECT.™

Securing cyberspace

starts with **YOU**