Preventing Cyber Crime & Business Identity Theft

Aaron Hanson
Senior Manager, Regional Product Marketing, SMB & .cloud
Symantec Mission

We protect the world’s people and information.
Threats stop business
We stop threats
Powered by Security Intelligence

- Attack Quarantine System
- Endpoints
- Gateways
- Honeypots
- Global Sensor Network
- 3rd Party Affiliates
- Global Data Collection

Global Intelligence Network

- Big Data Analytics
- Analysts
- Hosted Intelligence
- DeepSight
- Intelligence Feeds
- Warehouse

Probes in 200 countries & territories
Visibility into 30% of global email traffic
Over 2 million decoy accounts
Today’s Threat Landscape

5.5 billion
attacks blocked by Symantec in 2011 (3 billion in 2010)

4,989 new vulnerabilities
1.1 million identity exposed per breach
4,595 Web attacks per day blocked
403,000,000 unique malware variants vs. 286,000,000 in 2010

A Whole Industry Exists To Help Malware Authors Evade Detection
Bare Minimum Security No Longer an Option for SMBs

- Small businesses are increasingly being targeted
  - Targeted attacks against SMBs **doubled** between 2011 and 2012.*
  - Direct correlation between a **rise in attacks against small companies** and a drop in attacks against larger ones.

*Source: Symantec Intelligence Report, June 2012
SMBs Are **Weakest Link** in Supply Chain

- **Hackers use SMBs** as stepping stone into larger companies
  - 28 percent to 41 percent of data breaches caused by a third-party\(^1\)

- **Top 500 global businesses average 60 alliances each with smaller companies**\(^2\)

- **Becoming the gateway to a major client’s or partner’s data can destroy an SMB**
  - Contracts now demanding partners have top-level security

---

1. Source: Ponemon 2011 Global Cost of a Data Breach
2. Source: [House Small Business Committee](https://www.congress.gov/committee/ahrgb/112th-congress/house-small-business-committee)
No Cybersecurity Plans...No Worries

Nearly 3/4 of SMBs

- Indicate a safe Internet is important to success
- Say strong cybersecurity is good for their brand

However – over 6 out of 10 SMBs

- Say they are not concerned about cyber threats
- Don’t even have an informal internet security policy

AND the majority of SMBs surveyed (59%)

- Do not have a contingency plan to respond to a breach

Small Businesses Need:
Simple, Affordable, Automatic Protection
That is Easy to Manage
Symantec Cloud Solutions Make Protection Simple

- Set up in minutes with Web-based management from anywhere
- No hardware, software, or specialized training needed
- One login to manage both backup and security in one easy-to-use console

Start your free 30-day trial:
http://go.symantec.com/trycloud
Symantec Web-Based Console Makes Management Easy

- Centralized view of computers configured for backup
- Manage computers, users, and policies for both backup and security
- Centralized view of computers protected against viruses and malware
- Get the critical information you need at a glance

http://go.symantec.com/trycloud
Simple, Fast, Effective Cloud-Managed Security

End of page.
Automated, Continuous, Secure Online Backup & Recovery

Main or Branch Office

Symantec Data Centers

Remote and Mobile Users

Backup Exec.cloud Admin Anywhere
Deploy | Manage | Monitor
Automated, Continuous, Secure Online Backup & Recovery

Backup Exec.cloud

Protected

Get the critical information you need at a glance

Continuous backup is active  Pause

- Total Data Protected: 4.6 GB (3265 files)
- Last Recovery Point Created: -
- Next Recovery Point Scheduled: Tuesday, November 20, 2012 @ 12:00:00 PM

Quickly and easily configure backups or restore data
Steps you can take

• **Know** what you need to protect
  – Where is your information being stored and used

• **Encrypt** confidential information

• **Use a Reliable** Security Solution
  – You need more than just Anti-virus
Steps you can take

• Map out a disaster preparedness plan today
  – Don’t wait until it’s too late

• Protect Information Completely
  – Combine backup with robust security

• Stay up to date
  – Security is only as good as the frequency with which it is updated
Steps you can take

• Educate employees
  – About latest threats
  – Spammer/Social media techniques
  – Develop Internet security guidelines
  – Enforce strong passwords: 8+ characters with letters, numbers, symbols
Resources to Help You Get Started

• Internet Security Threat Report

• In-depth view of cyber threat landscape

• Understand how it affects you

• Learn to defend your business and employees

www.symantec.com/threatreport

INTERNET SECURITY THREAT REPORT

Best Practice Guidelines For Businesses

Employ Defense-In-Depth Strategies:

- Establish multiple, overlapping, and mutually supportive defensive systems to guard against single-point failures, even in any specific technology or protection method. This should include the deployment of security gateway devices, as well as gateway detection, intrusion protection systems, and Web security gateway solutions throughout the enterprise.

- Monitor For Network Threat,
  Vulnerabilities And Brand Abuse.

- Monitor for network intrusions, propagation attempts and other threats against your corporate network. Automated systems can flag these types of events. Response plans for potential attacks can be designed to prevent or contain the attack.

- Antivirus On Endpoints Is Not Enough:

- On endpoints, signature-based antivirus alone is not enough to protect against today’s threats. Deploy comprehensive endpoint security solutions that include additional layers of protection, including:
  - Real-time anti-virus protection that stops targeted attacks, protects against new vulnerabilities and prevents malware from spreading.
  - Network protection for protection against DDoS and Web-based attacks.
  - Web content filtering to prevent access to known malicious websites and phishing attacks.

- Use network-based intrusion prevention to provide proactive protection against unknown threats.

- Use Web-based reputation solutions that provide a real-time reputation rating of any URL or site. Protect your organization from malware and phishing attacks.

- Use behavioral analysis capabilities that look at the behavior of applications and malware and prevent attacks.

- Application control settings that can prevent applications and browser plugins from downloading or launching untrusted content.

- Develop and maintain policies that prevent and limit the types of undesirable content.

- Secure Your Websites Against MITM Attacks And Malware Infection:

- Avoid compromising your trusted relationship with your customers by:
  - Implementing SSLv3.
  - Scanning your website daily for viruses.
  - Surveilling the security for all website content.
  - Regularly renewing your website for security vulnerabilities.
  - Using SSL certificates with extended validation to display the green browser address bar to web users.
  - Displaying certified trust marks in highly visible locations on your website to assure trust and show consumers your commitment to their security.

- Make sure to get your digital certificate from an established, reputable source and ensure your website is secured by the latest security practices. Protect your organization by implementing strong security practices to secure and protect your private data.

- Use secure HTTP signing and bandwidth allocation in your applications.

- Use secure HTTP, including HTTPS, to ensure your data is encrypted when it traverses the Internet.

- Use encryption to protect sensitive data:

  - Implement and enforce a security policy whereby sensitive data is encrypted. Access to sensitive data must be restricted. This should include a Data Loss Prevention (DLP) solution, which is a system to classify sensitive data and protect it.

  - Use DLP technology to protect data if it is transferred or shared.

Use encryption to protect sensitive data, but also be sure to mitigate the damage of potential data leaks from within an organization.
Resources to Help You Get Started

**Connect** and join the conversation

www.symantec.com/connect
Looking Ahead in 2013 – **Top 5 Security Predictions**

1. Cyber conflict becomes the norm

2. Ransomware is the new scareware

3. Madware adds to the insanity

4. Monetization of social networks introduces new dangers

5. As users shift to cloud, so will attacks

Thank you!

Aaron Hanson
Aaron_Hanson@symantec.com

Start your free 30-day trial:  http://go.symantec.com/trycloud