Global Internet Security Threat Report, Volume XV

Mark Bregman

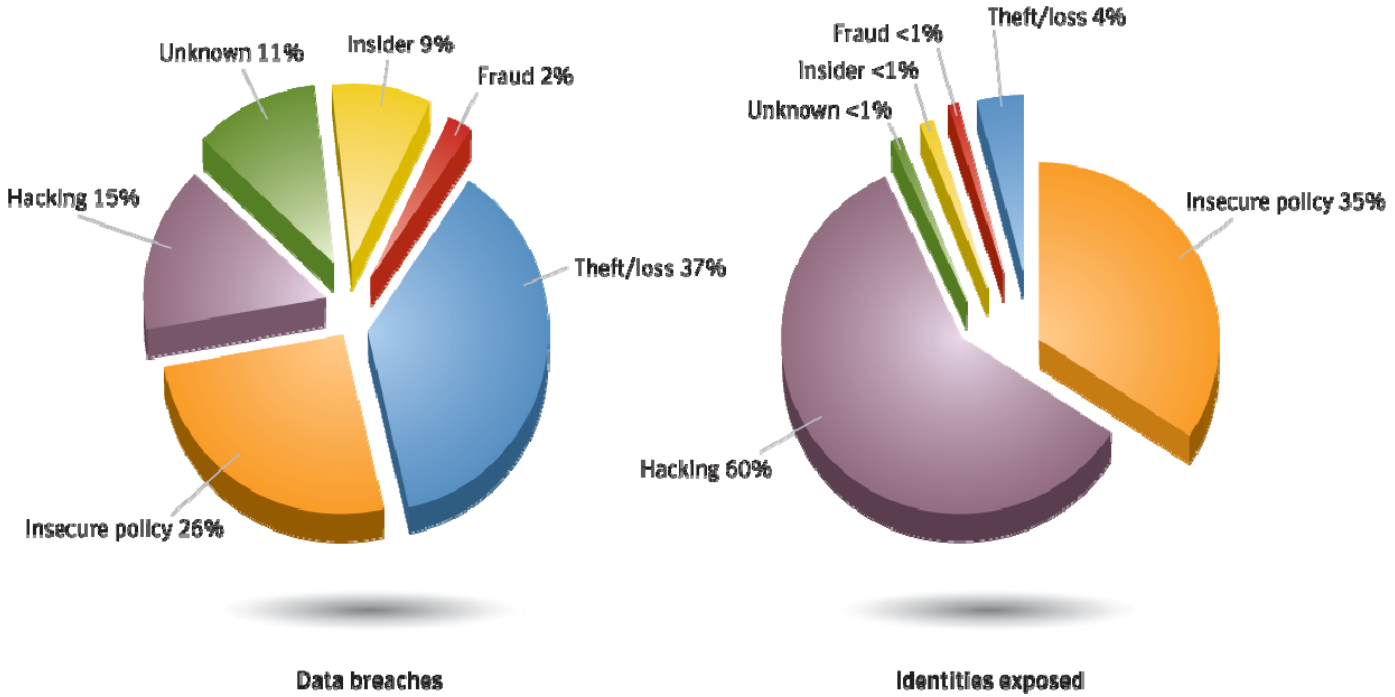
Executive Vice President and Chief Technology Officer

ISTR Volume XV: Key Findings Summary

- Cybercrime's financial and geographic growth shows no slowdown during the global economic crisis.
- Targeted attacks focus on enterprises.
- Attack kits make information theft easier for novices.
- Underground economy unaffected by the global economy.

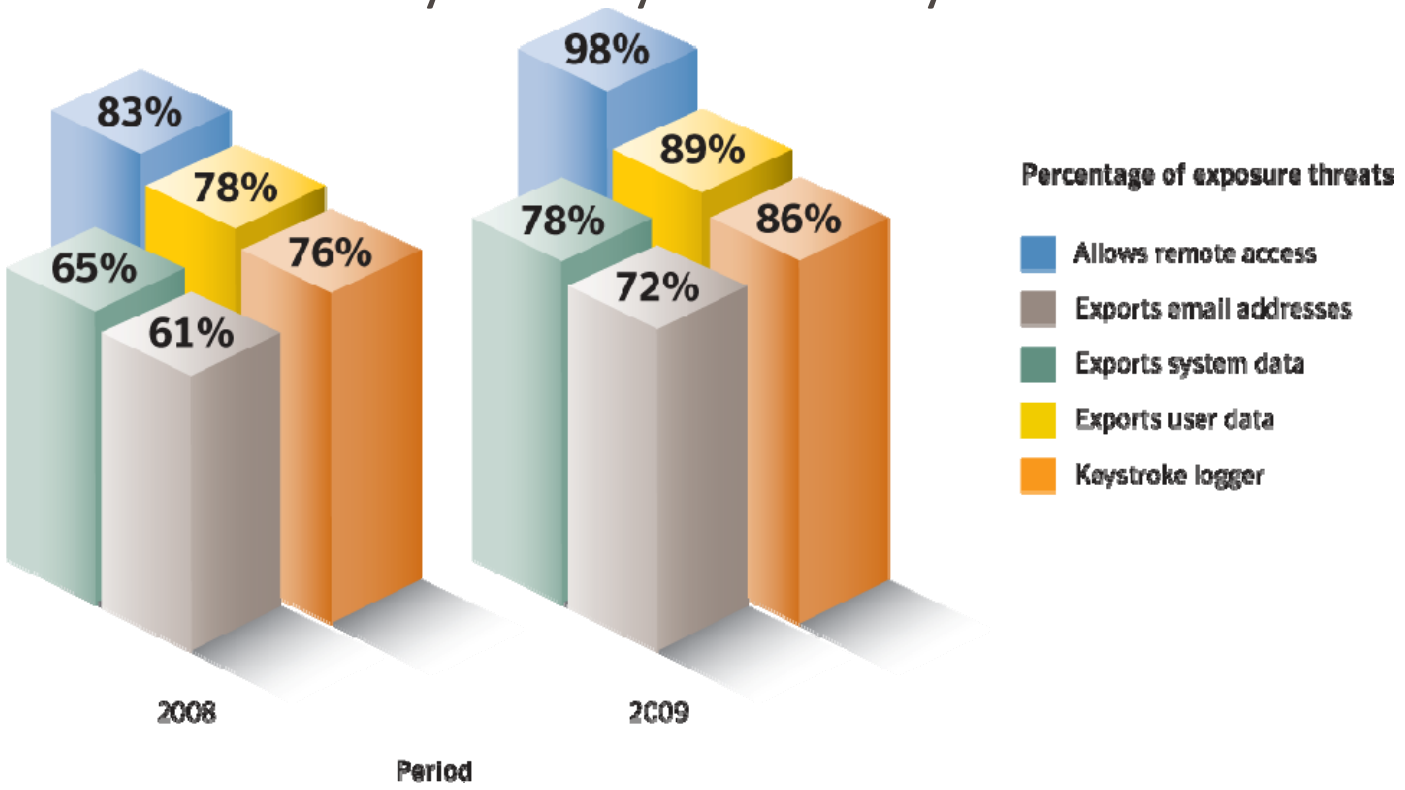
Targeted attacks focus on enterprises

- Frequently carried out by Advanced Persistent Threats (APTs).
- These threats remain undetected to penetrate deeply into the network.



Attack kits make information theft easier for novices

- Kits allow unskilled attackers to enter the market with sophisticated tools.
- Increase in kit activity notably marked by Zeus.



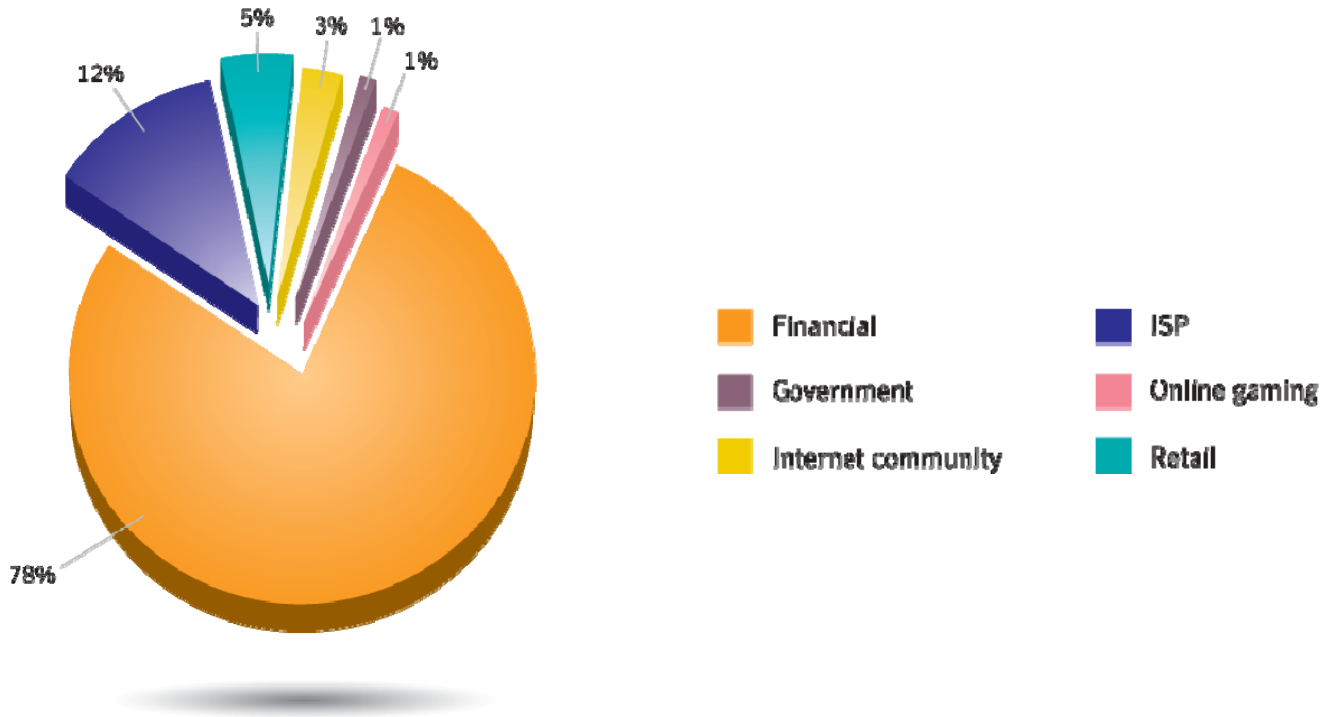
Underground Economy unaffected by global economy

- Credit card info and bank accounts still top advertised items on underground economy.
- Credit card dumps saw a marked increase in advertisements.

Overall Rank 2009	Overall Rank 2008	Item	Percentage 2009	Percentage 2008	Range of Prices
1	1	Credit card information	19%	32%	$0.85–$30
2	2	Bank account credentials	19%	19%	$15–$850
3	3	Email accounts	7%	5%	$1–$20
4	4	Email addresses	7%	5%	$1.70/MB–$15/MB
5	9	Shell scripts	6%	3%	$2–$5
6	6	Full identities	5%	4%	$0.70–$20
7	13	Credit card dumps	5%	2%	$4–$150
8	7	Mailers	4%	3%	$4–$10
9	8	Cash-out services	4%	3%	$0–$600 plus 50%–60%
10	12	Website administration credentials	4%	3%	$2–$30

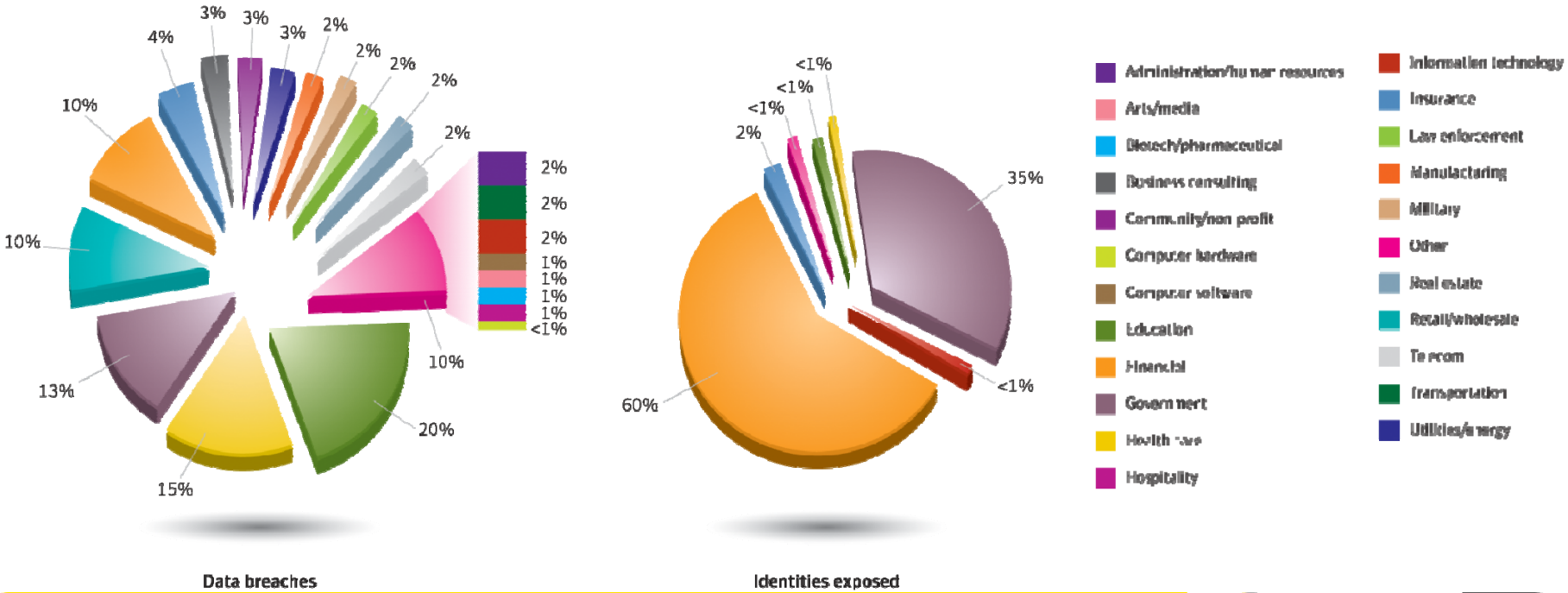
Threat Landscape
Underground Economy unaffected by global economy

- Spam and phishing attacks targeting financial services unaffected.
- 78% of phishing URLs observed target financial brands.



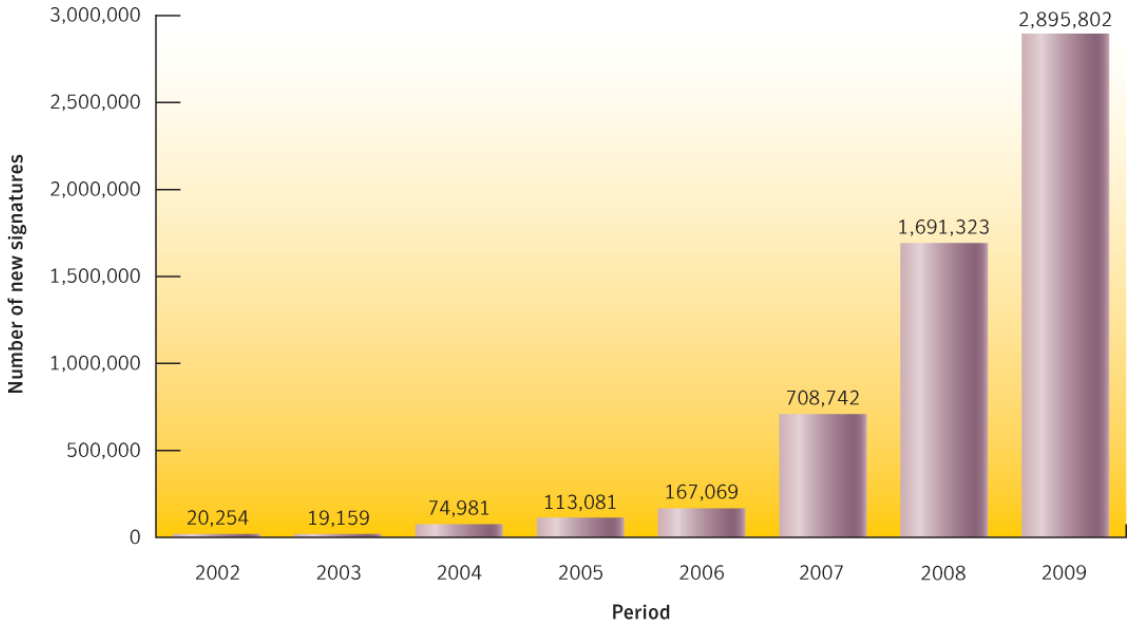
Threat Activity Trends
Data Breaches by Sector

- Information on data breaches that could lead to identity theft. Data collected is not Symantec data.
- The Education sector accounted for the majority of data breaches with 20%, followed by Healthcare (15%) and Government (13%) but Financial resulted in the most identities exposed (60%).



Malicious Code Trends
New Malicious Code Signatures

- In 2009, Symantec identified more than 240 million distinct new malicious programs, a 100% increase over 2008.
- Of the threat instances that Symantec's reputation-based techniques protected users from in 2009, approximately 57% corresponded to singletons.



Thank you!

Copyright © 2010 Symantec Corporation. All rights reserved. Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.