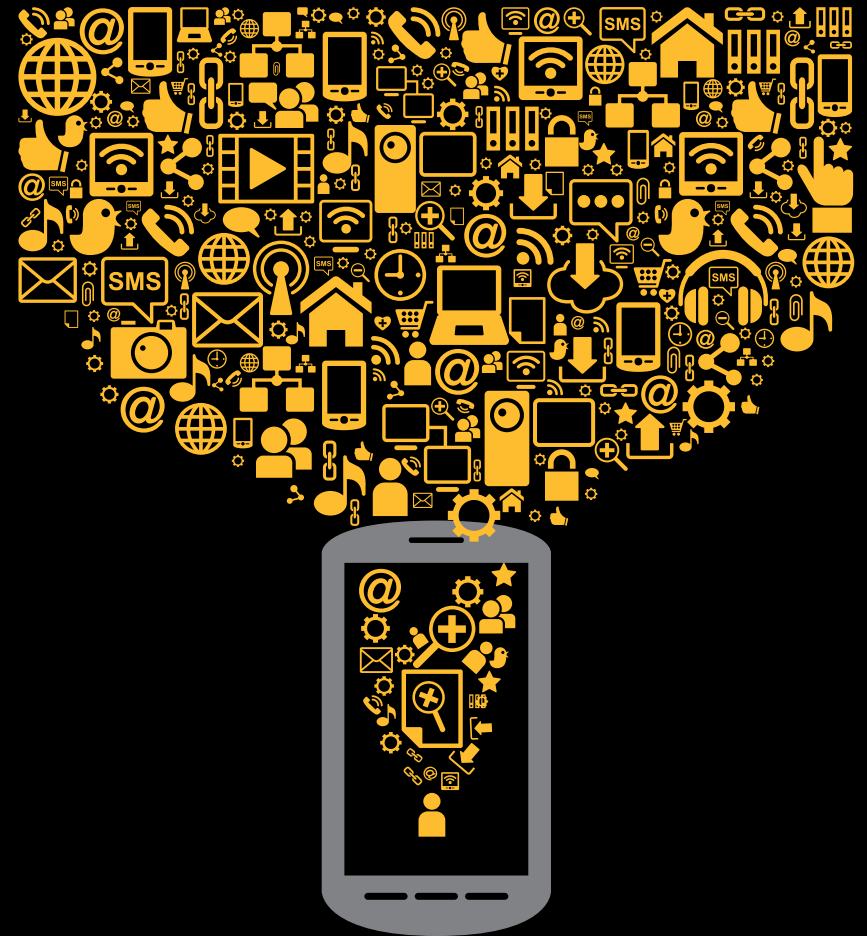




The Security Challenge

Shantanu Ghosh

Vice President, Data Center Security &
Managing Director, India Product Operations



Which of These Have Been Used in a Cyber Attack?



Trash Can

A



Smart TV

B



Baby Monitor

C

Security Threat Landscape

A Fundamental Shift...



Hacking

Cyber Crime

Cyber Espionage

Cyber Warfare

Surge in Targeted Attacks and APTs

Targeted Attacks Up

42%

According to the
Symantec ISTR

Identities Exposed
In Past Year

93M

More than the Entire
Population of
Germany

Websites with
Unpatched
Vulnerabilities

53%

24% are Critical
Vulnerabilities

Critical infrastructure under threat

2000: Gazprom, the largest extractor of natural gas was successfully attacked using a Trojan to gain access to the control for the gas pipelines.

2003: A marine terminal in Venezuela was targeted by a sabotage attack through access to the SCADA network of the oil tanker loading machinery and overwriting the programmable logic controllers (PLCs) with an empty program module.

2010: Disruption of the Iranian nuclear program believed to be a uranium enrichment facility by the Stuxnet worm.

2013: Part of the Austrian and German power grid nearly broke down after a control command was accidentally misdirected.

Hidden Lynx

Duqu

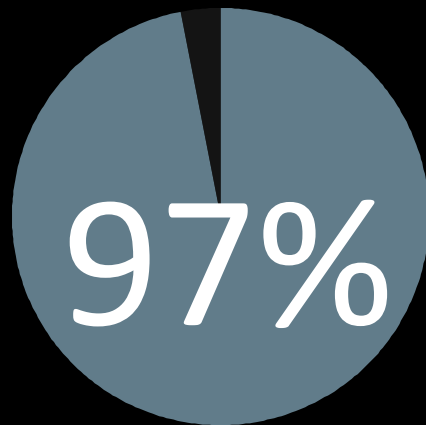
Stuxnet

Zero Access

Elderwood
Project

Flame

Data Center: The Real Target



stolen data is from
servers

“ More often endpoints / user devices simply provide an initial “foothold” into the organization, from which the intruder stages the rest of their attack.”

What Makes Cyber Criminals So Successful?

Information
Sharing

Technology
Adoption

Well
Funded

Specialization of Skill In The Attack Chain

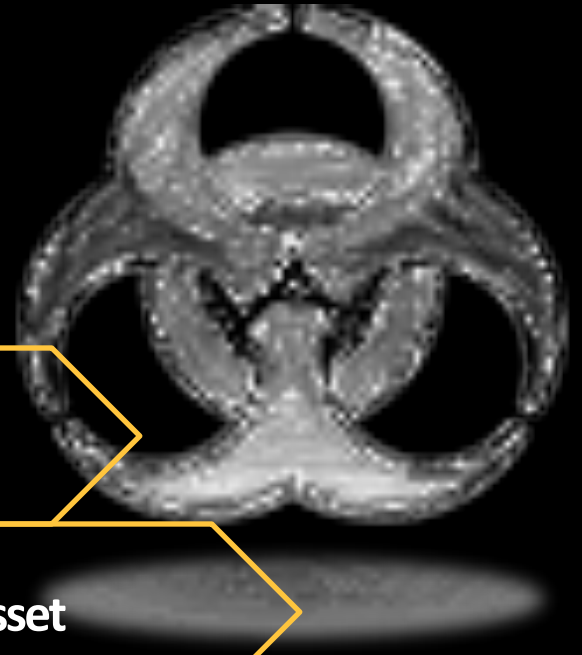
Reconnaissance: Know your Targets

Incursion: Gain Access

Discovery: Create a Map to the Asset

Capture: Take Control of the Asset

Exfiltration: Steal or Destroy Asset



Digitalization

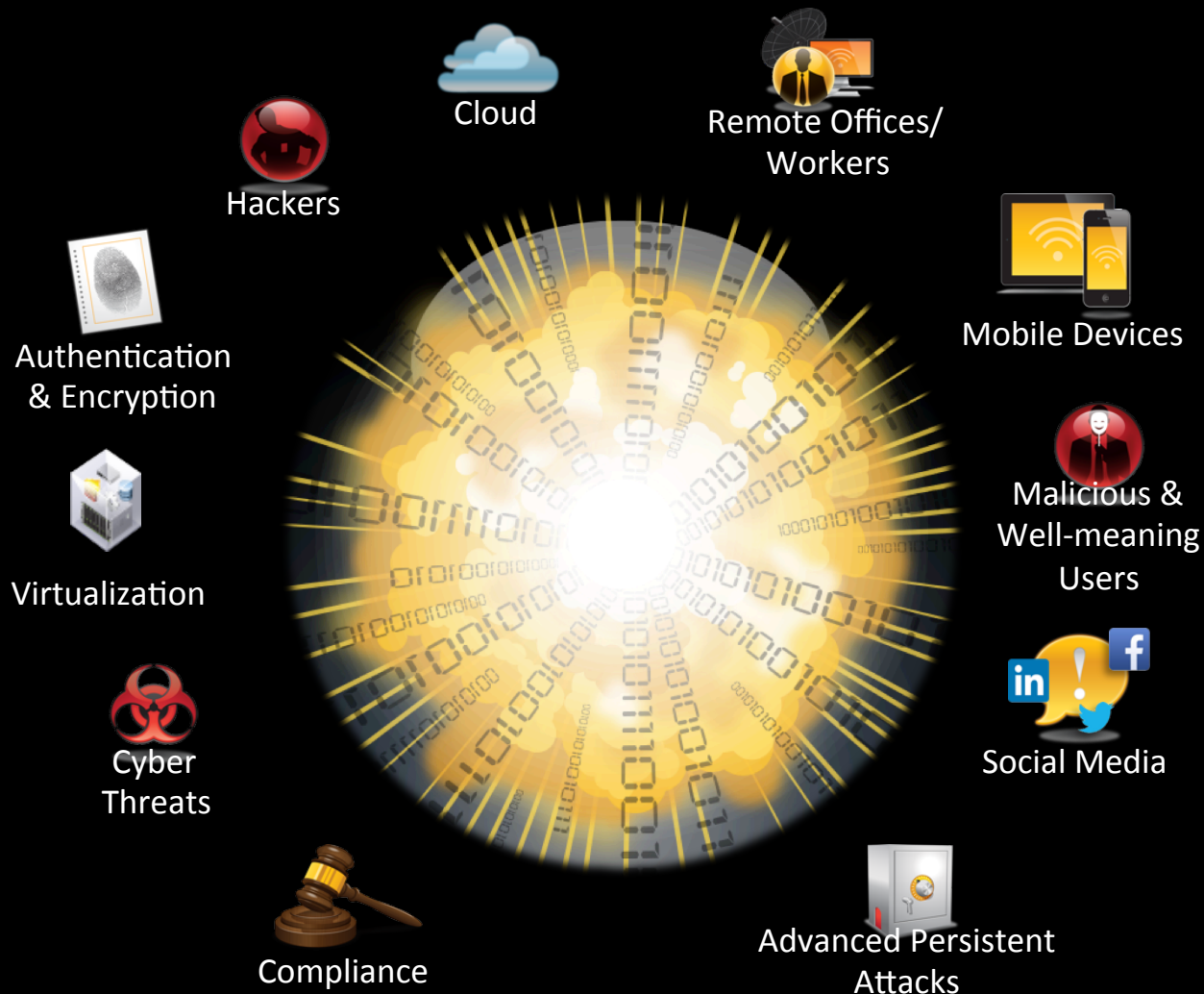






2020

Expanding boundaries create risk everywhere



Internet of Things



Everything is Connected



Sophisticated
Attacks

Limited Skills
and Expertise

Complex
Heterogeneous
Infrastructure

Increased
Cost of
Incidents

Information
Explosion

Cyber Security Challenge



Need for unified security to protect information from the most advanced threats

Risk-based approach to identify and protect the most important assets

Keep the bad guys out

Minimize the impact of a cybersecurity event

Respond and recover quickly



What Can We Do As A Community To Win Against Cyber Criminals?

Public/Private
Collaboration

Security
Intelligence

Education
Programs



Thank you!

Shantanu_Ghosh@Symantec.com

Copyright © 2012 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.

