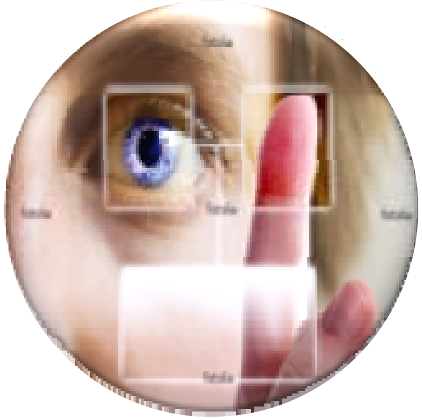
Cyber Security and Leadership Solutions

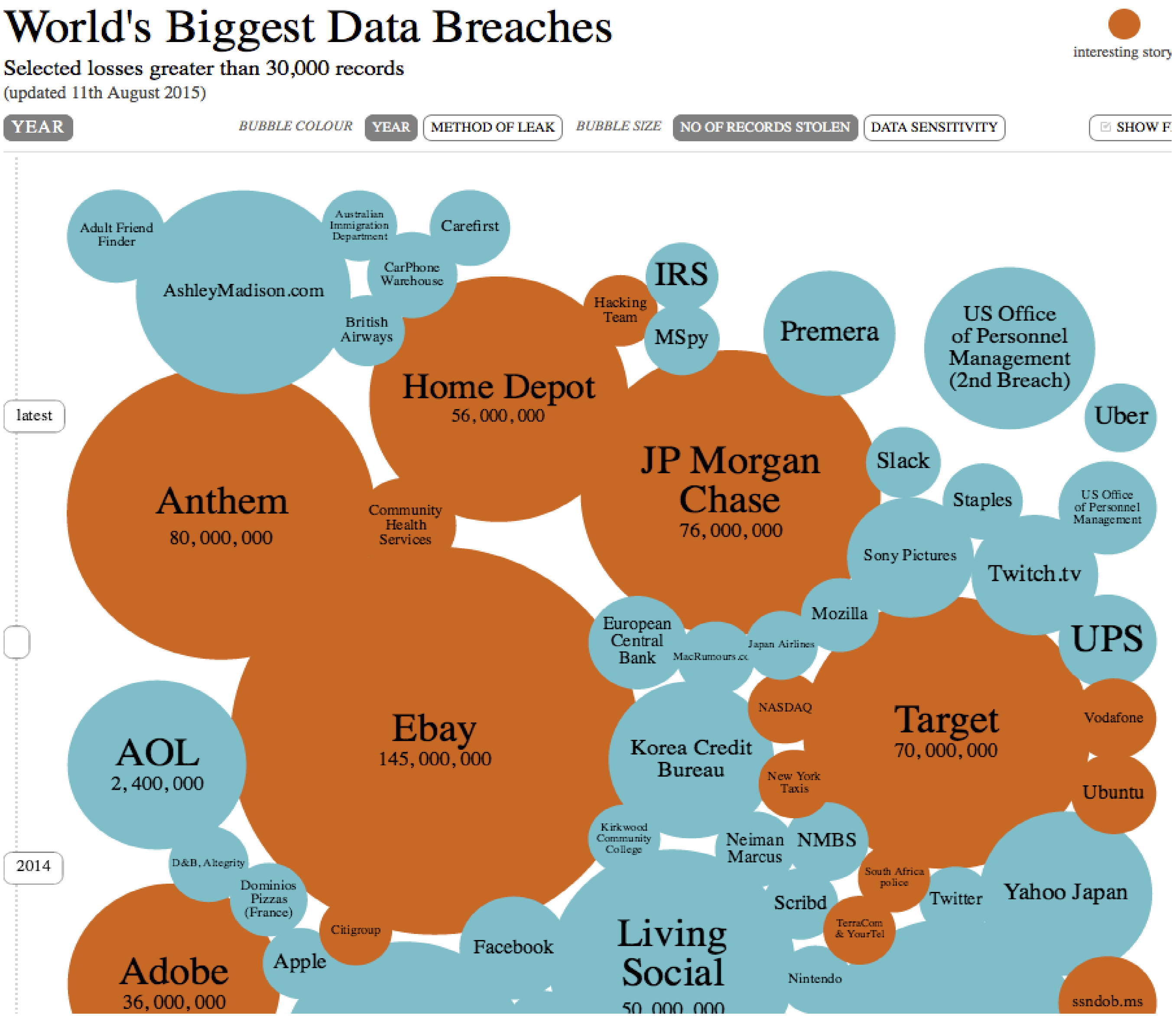
James Risler
Manager – Security Content Development
MBA, CISSP #456200, CCIE# 15412
jarisler@cisco.com

Outline



- The "Why"
- Trends
- Threat Landscape
- Examples of Cyber Attacks
- Business Challenge
- People Problem
- Recommendations
- Conclusion & Q&A

The “Why”



World's Biggest Data Breaches

Selected losses greater than 30,000 records

(updated 11th August 2015)

Anthem
Home Depot
JP Morgan
Adobe
Target
Univ. of MD
Neiman Marcus
TJ Maxx
Sony
Zappos
LinkedIn
Citigroup
Florida Courts

http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

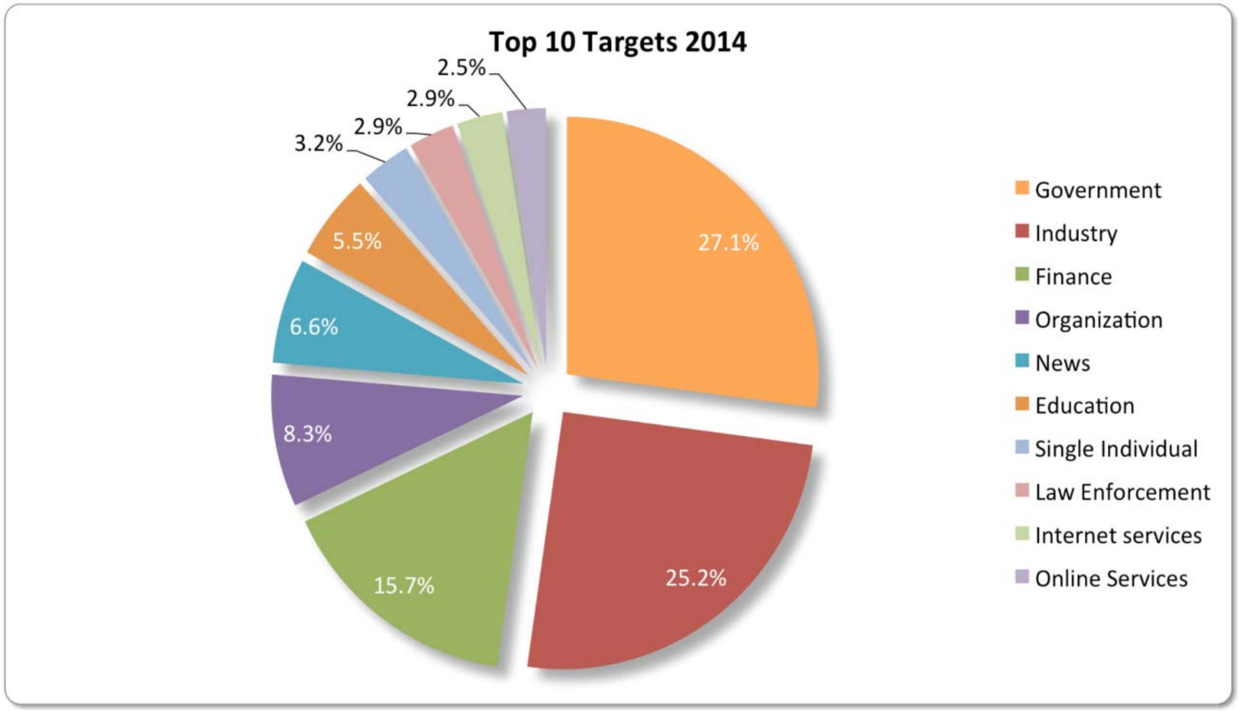
There are two types of companies: those who **have been hacked**, and those who **don’t yet know** they have been hacked.

John Chambers
Chief Executive Officer of Cisco

Trends and tendencies

Attacks per vertical segment

- Over 15% of attacks are targeted at financial institutions
- Attacks include :
  - DDoS
  - Spyware
  - Ransomware
  - Mobile devices
  - SPAM
  - Web Exploits



- Source : IDC ™

Example of Financial Cyber attacks

Heartland
PAYMENT SYSTEMS™
The Highest Standards | The Most Trusted Transactions

JPMorganChase

OP-Pohjola

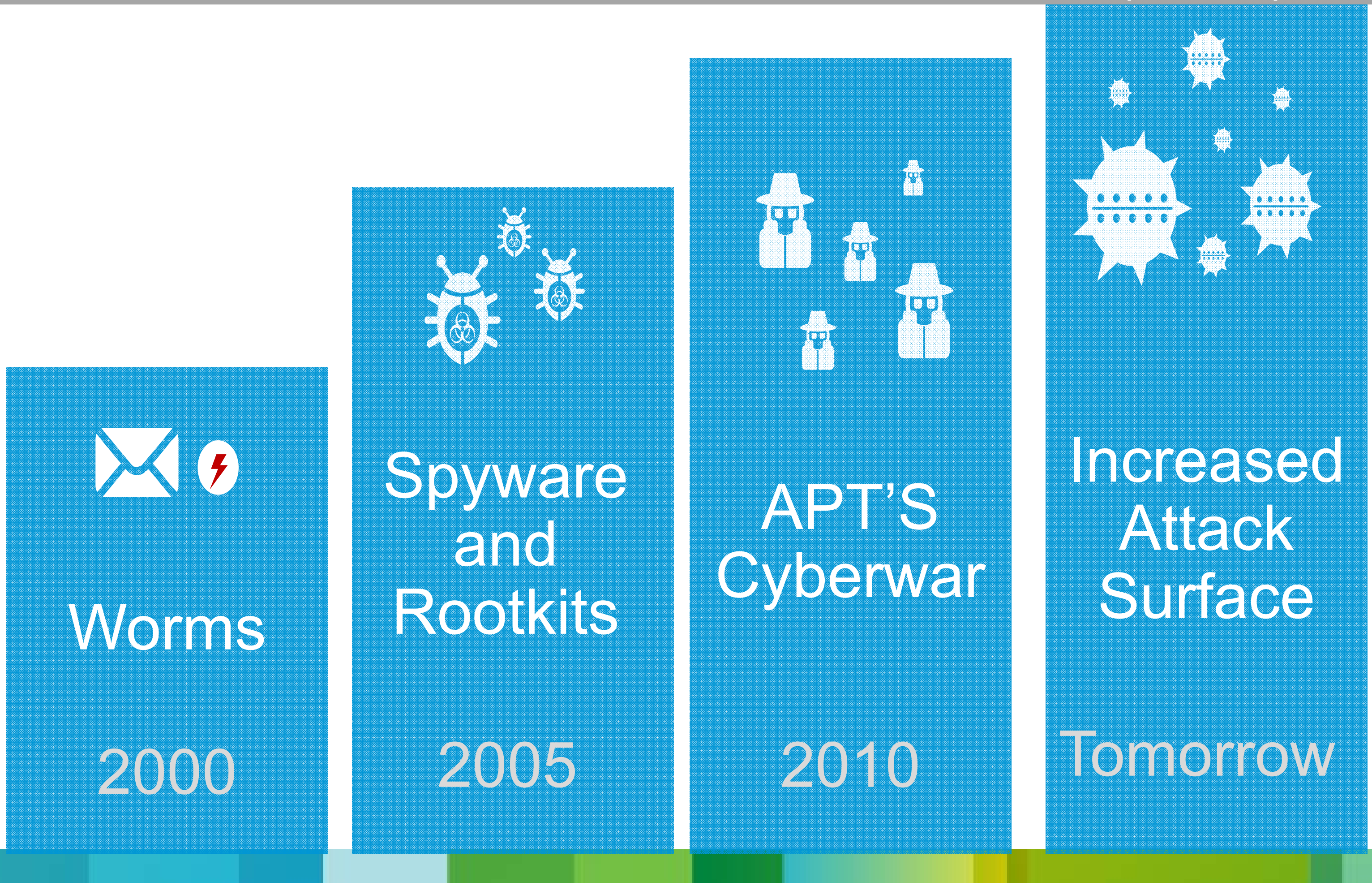
Danske Bank

- 2008 – 100 Million Credit and debit card numbers stolen by spyware from Heartland Payment Systems
- 2014 – 76 Million household accounts and 7 million SMB accounts compromised at JP Morgan Chase
- 2015 - DDoS attack launched on OP-Pohjola and Danske Bank
- ... And more :

  European Central Bank extortion attempt

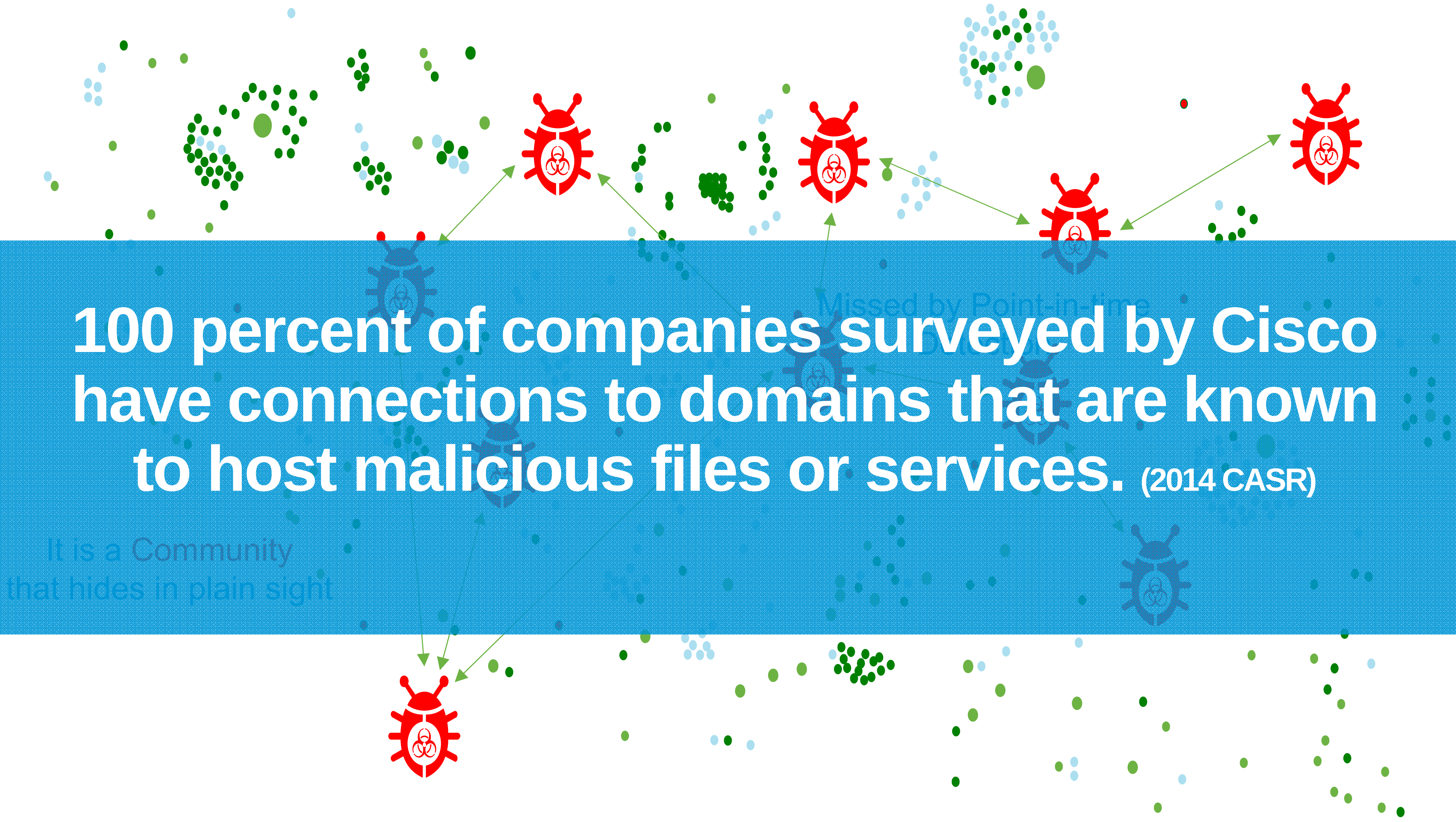
  Multi-bank attack by Eurograbber

Threat Landscape is Evolving…



Enterprise Response	Antivirus (Host-Based)	IDS/IPS (Network Perimeter)	Reputation (Global) and Sandboxing	Intelligence and Analytics (Cloud)
	Worms	Spyware and Rootkits	APT'S Cyberwar	Increased Attack Surface
	2000	2005	2010	Tomorrow

Today’s Advanced Malware is Not Just a Single Entity



100 percent of companies surveyed by Cisco have connections to domains that are known to host malicious files or services. (2014 CASR)

Common Underlying Cyber Attack Methods

Social Engineering

Phishing, Spam
Malvertising

Technical Exploit

Patching, new
vulnerabilities

Zero-day Attack

Unknown code
exploits

Top Cyber Risks for Users

Untrustworthy sources

Clickfraud and Adware

Outdated browsers

10%

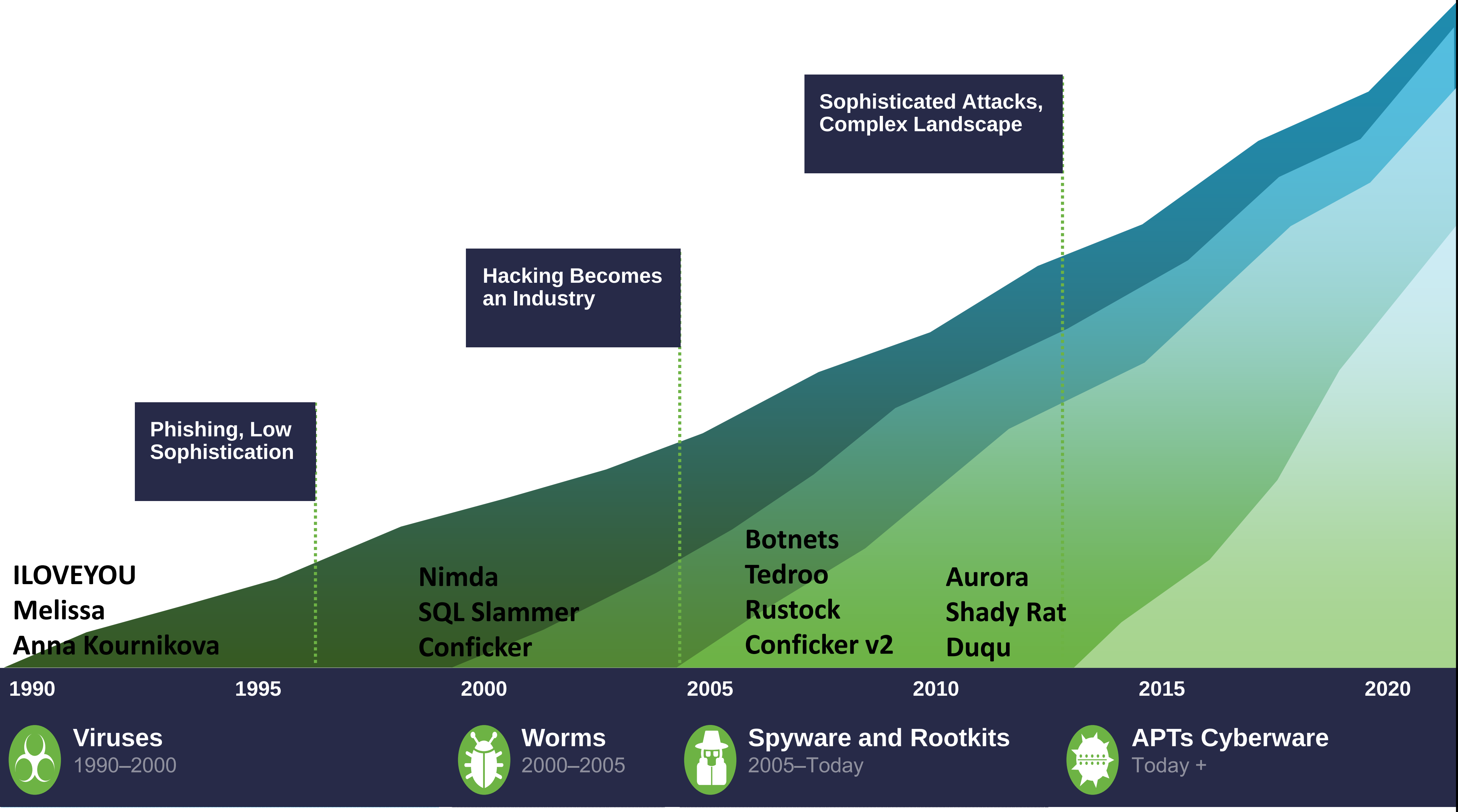
IE requests running latest version

64%

Chrome requests running latest version

2015 Cisco Annual Security Report

The History of Hacking and Examples



Phishing, Low Sophistication

Hacking Becomes an Industry

Sophisticated Attacks, Complex Landscape

ILOVEYOU
Melissa
Anna Kournikova

Nimda
SQL Slammer
Conficker

Botnets
Tedroo
Rustock
Conficker v2

Aurora
Shady Rat
Duqu

Viruses
1990–2000

Worms
2000–2005

Spyware and Rootkits
2005–Today

APTs Cyberware
Today +

How Industrial Hackers Monetize the Opportunity

Social Security
$1

Medical Record
>$50

Credit Card Data
$0.25−$60

DDoS as a Service
~$7/hour

Bank Account Info
>$1000
depending on account type and balance

Global Cybercrime Market: $450B-$1T

Mobile Malware
$150

Spam
$50/500K emails

Exploits
$100k-$300K

Malware Development
$2500
(commercial malware)

Facebook Account
$1 for an account with 15 friends

Welcome to the Hackers' Economy

Source: CNBC

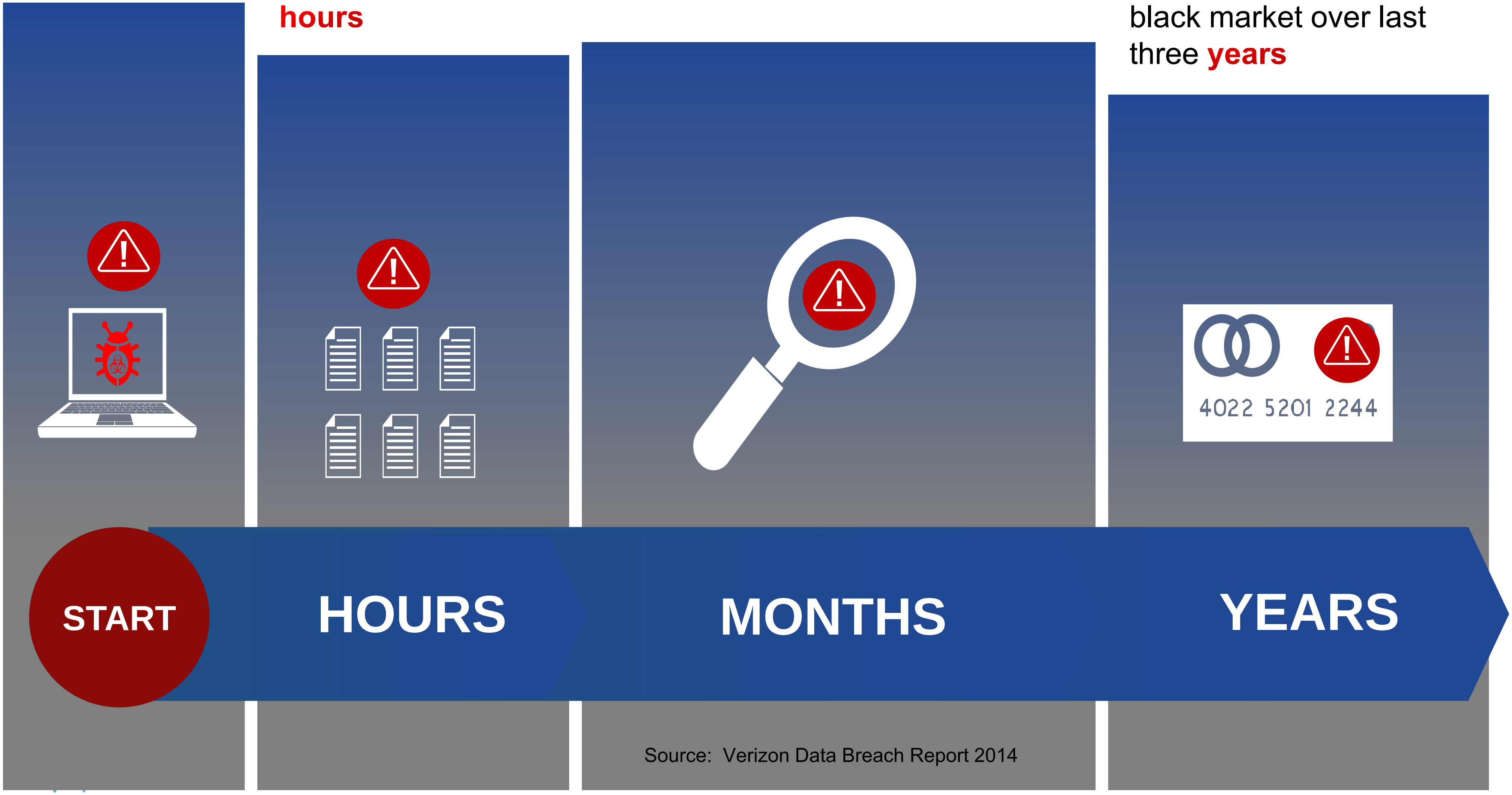
Impact of a Breach

Breach occurs

60% data in breaches is stolen in **hours**

54% of breaches remain undiscovered for **months**

Information of up to **750 million** individuals on the black market over last three **years**



Source: Verizon Data Breach Report 2014

Examples of Cyber Attacks

“Kimusky” Operation: A North Korean APT

- 4 Key South Korean Targets

  Phishing against Hyundai Merchant Marine

- Infecting Systems

  Trojan Dropper – DLL library against Windows 7

- Install Spying Modules

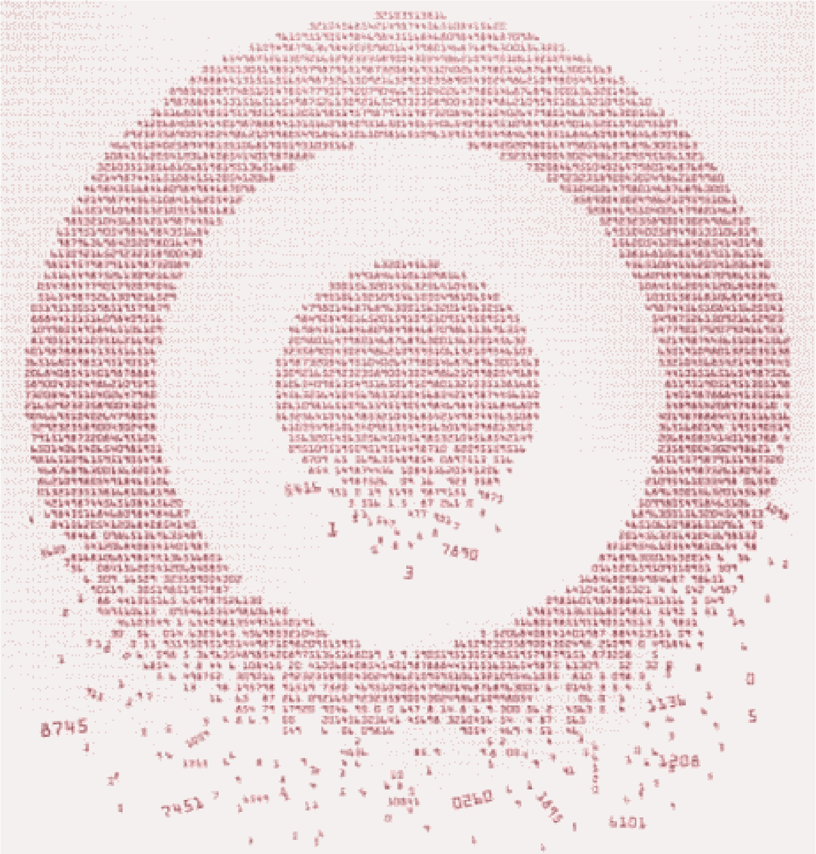
  Key Stroke Logger, Directory Listing, Remote Control & Execution, Remote Control Access

- Disable Firewall
- Communication

  Command and control Bot done through a Bulgarian web-based free email server

- Regular Reporting and RC4 Encryption and Exporting of Data

Phases of Retail Cyber Attack



Phases of Attack on Target Stores

TARGET

1. Phish HVAC Vendor
   Steal credentials – Target hosted web server

2. Scan Network – Determine HVAC vendor access shared web server

1. Upload PHP Script to Web Server – Vulnerability in Application

1. Control of Webserver – Scan for relevant targets for propagation (MSSQLSvc/Billing)

1. Attack Microsoft AD Domain – Steal access tokens on Webserver (Pass-the-hash)

Phases of Attack – cont.

6. Create new Admin Account in MS AD Domain

7. Propagate to relevant computers (“Angry IP Scanner”) by pass security solutions (Tunneling with PsExec’s)

7. Attack SQL Server – Steal 70 Million PII records (no credit cards because PCI compliant)
   - Osql.exe
   - Isql.exe
   - Bcp.exe

Phases of Attack – cont.

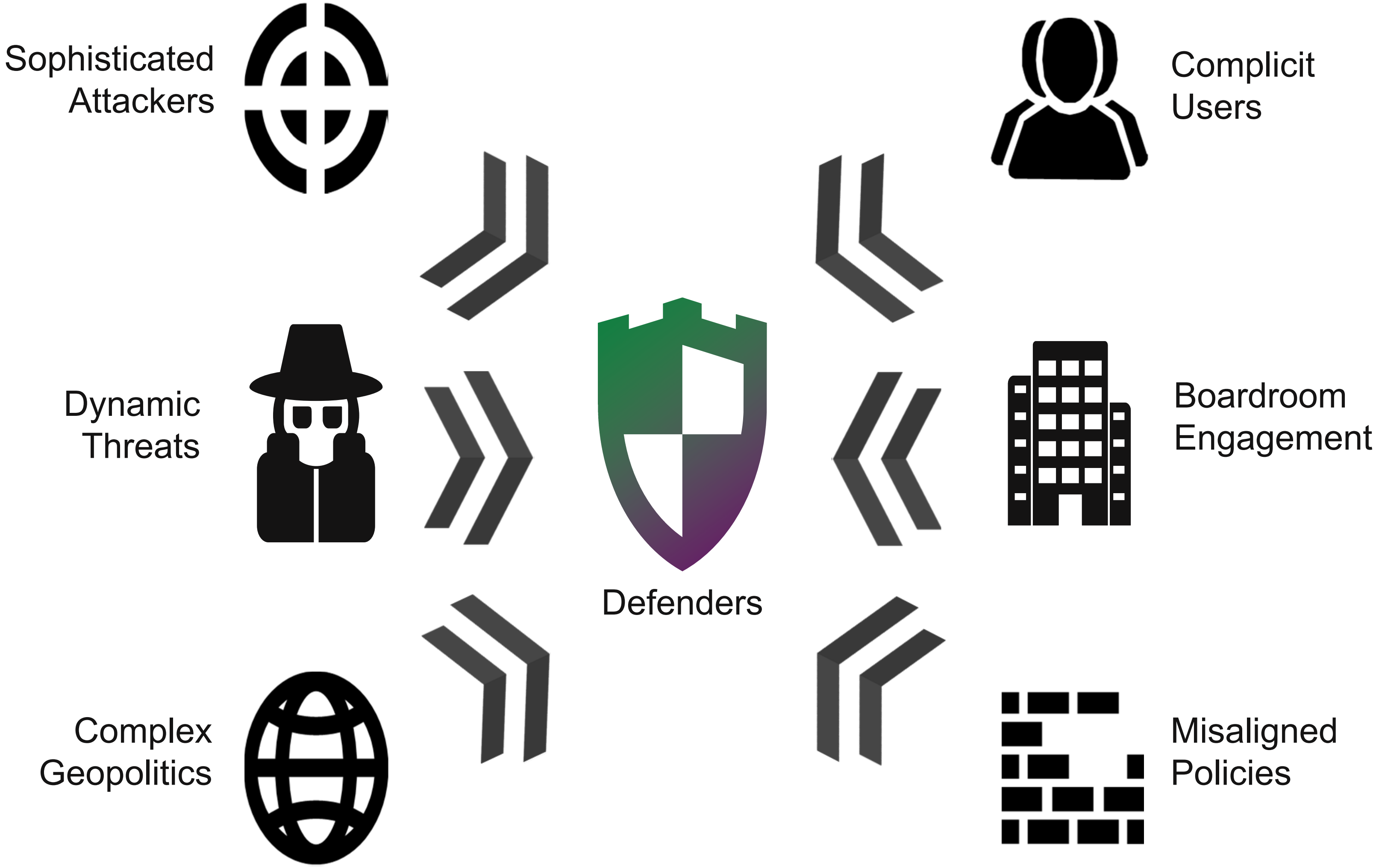
9. Download POS Malware and install on POS (“Kaptoxa” Malware)

10. Send stolen Credit Card info to network share (FTP transfer)

10. Upload Credit Card information to FTP site

If you knew you were going to be compromised, would you do security differently?

The Challenges Come from Every Direction



Business Transformation Challenges

Industrialization of Hackers

- Zeus, Phishing, Mules
- Targeted Attacks for Profit
- Advanced Persistent Threats (APT)
- Cyber and Economic Espionage

Evolving Borders

- Traditional Signature Enforcement less Effective Influx of Mobile Devices, BYOD
- Dual Profiles—Personal and Corporate
- Access Policy Inconsistent, Difficult to Maintain

Compliance

- Rapid Growth of Regulatory Requirements: PCI, HIPAA, NERC CIP, FISMA, SOX, ISO
- Legal Liabilities Drive Internal Requirements
- Little to No Guidance On How to Meet New Standards

THE WALL STREET JOURNAL.

Cyber Security is a Boardroom Discussion

Security Breaches are Costly

Security is the #1 Issue for Your Customers

Protect Now the Value You Intend to Create Tomorrow

Discussion in Board Room & Executive Level

Summary Cisco 2015 Annual Security Report Key Findings

- Lack of Security Leadership in Small companies (only 22 percent respondents see security has high priority)
- Gap between CISO and SecOp Manager in terms of confidence
- Less than 50% of respondents use following tools:
  - Identity Administrator or user provisioning
  - Patching and configuration
  - Penetration testing or Endpoint Forensics
  - Vulnerability scanning
- Only 40% of companies do Correlated event/log analysis

Solution

- New approaches to Security through alignment with People, Process and Technology

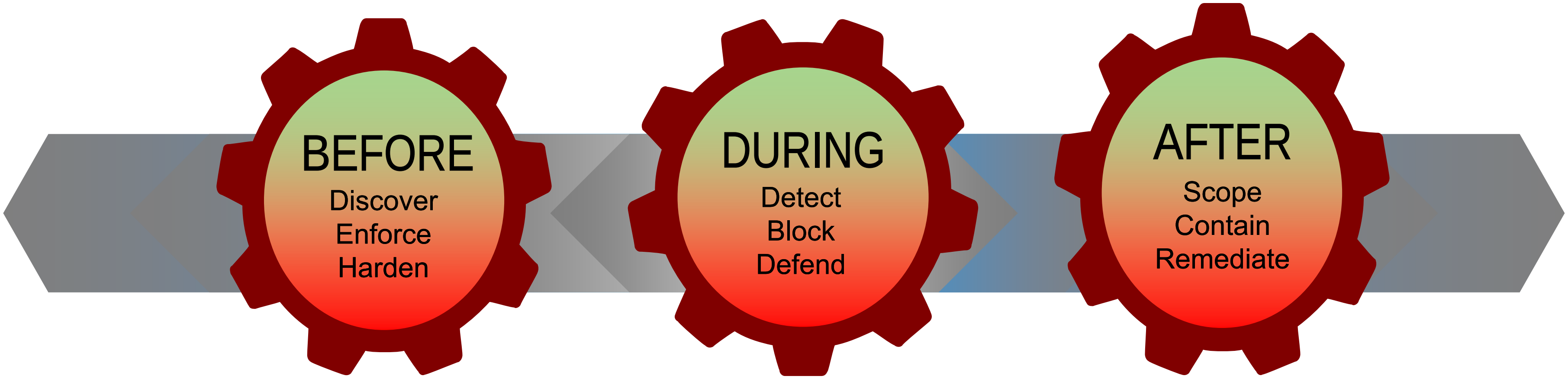
The People Problem

- “Caught in the middle are the users. But now, it appears they not only are the targets, but also the **complicit enablers of attacks**.”
- “Users’ **careless behavior** when using the Internet, combined with **targeted campaigns by adversaries**, places many industry verticals at higher risk of web malware exposure”
- People are part corporate system

Solution

- Training Programs
- Leadership from Executives on down

New Focus - Attack Continuum



BEFORE
Discover
Enforce
Harden

DURING
Detect
Block
Defend

AFTER
Scope
Contain
Remediate

Monitoring

Identification

Impact Mitigation

Visibility and Context
Mission Critical Business Systems and Solutions

Policies, Process
and People

Response Policy
and

Communication
Strategy

Recommendations

- Develop a Cybersecurity Management Framework
- 3 Distinct Layers with seven discret focus area
  1. Strategy – Define, document, and publish
  2. Operational – develop operational standards, process, and proceedures
  3. Tactical – implement security controls and monitoring with defined metrics
- Critical – Executive Sponsorship
- **Plane for … Before During and After the Attack**

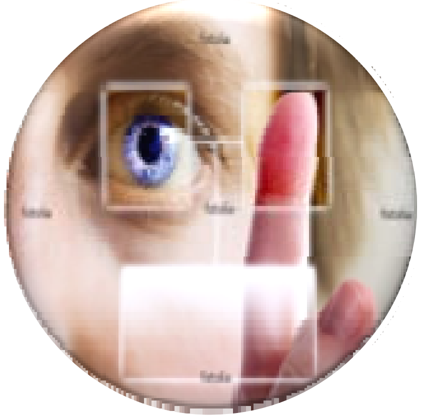
  What is the critical components of the business?

  Have you done a risk assessment?

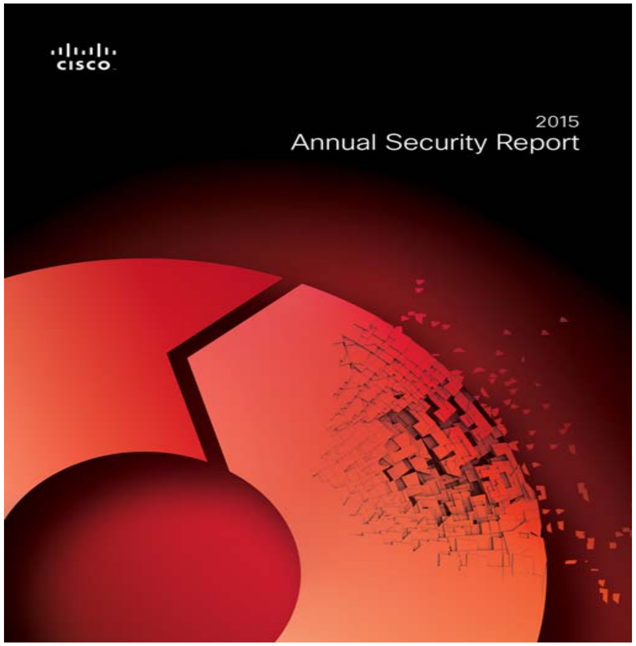
  Use existing business cases (Target, Home Depot, etc)

  How will the board respond to a Cyber attack?

Conclusion



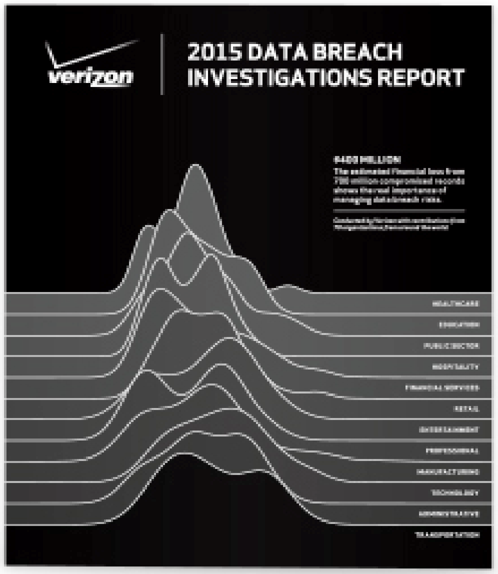
- Threat Landscape Rapidly Changing
- Business Leaders must drive security
- Business Challenge - Tools, Process, and People
- Cybersecurity Framework is critical



Cisco 2015 Annual Security Report

Now available:

cisco.com/go/asr2015



Verizon 2015 Data Breach Investigation Report

http://www.verizonenterprise.com/DBIR/

Questions/Discussion?

Thank You

Reference

http://www.cisco.com/c/dam/en/us/products/collateral/security/cybersecurity-management-programs.pdf

http://www.datacenterdynamics.com/security/ciscos-2015-security-report-its-a-people-problem/94536.fullarticle