Threats and Opportunities

Tom Blauvelt

Principal Security Architect, Public Sector

Symantec

@TomBlue01

Enterprise Threat Landscape

Attackers Moving Faster

5 of 6 large companies attacked

317M new malware created

1M new threats daily

60% of attacks targeted SMEs

Digital extortion on the rise

113% increase in ransomware

45X more devices held hostage

Malware gets smarter

28% of malware was Virtual Machine Aware

Zero-Day Threats

24 all-time high

Top 5 unpatched for **295 days**

Many Sectors Under Attack

Healthcare **+ 37%**

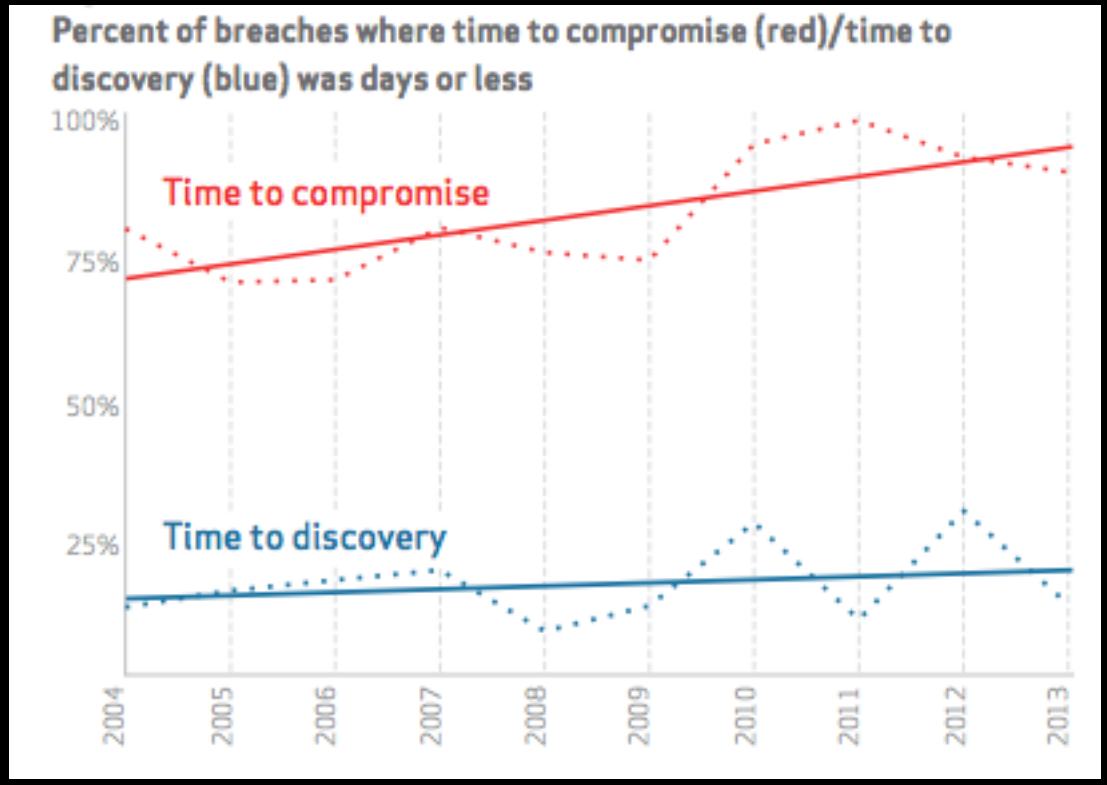
Retail **+11%**

Education **+10%**

Government **+8%**

Financial **+6%**

Effectiveness of Attacker Outpacing the Defender

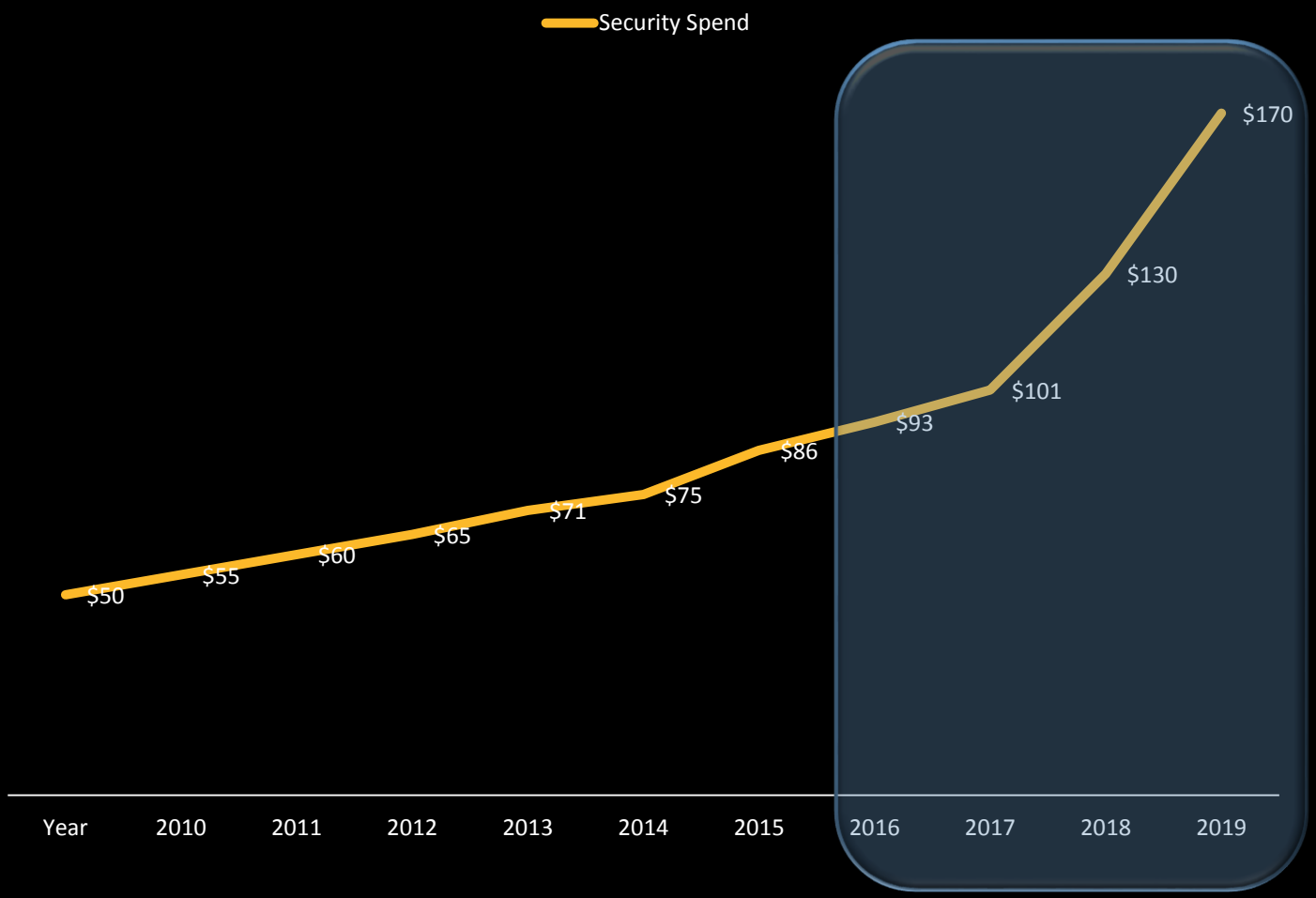


From Verizon's 2014 DBIR; http://www.verizonenterprise.com/DBIR/

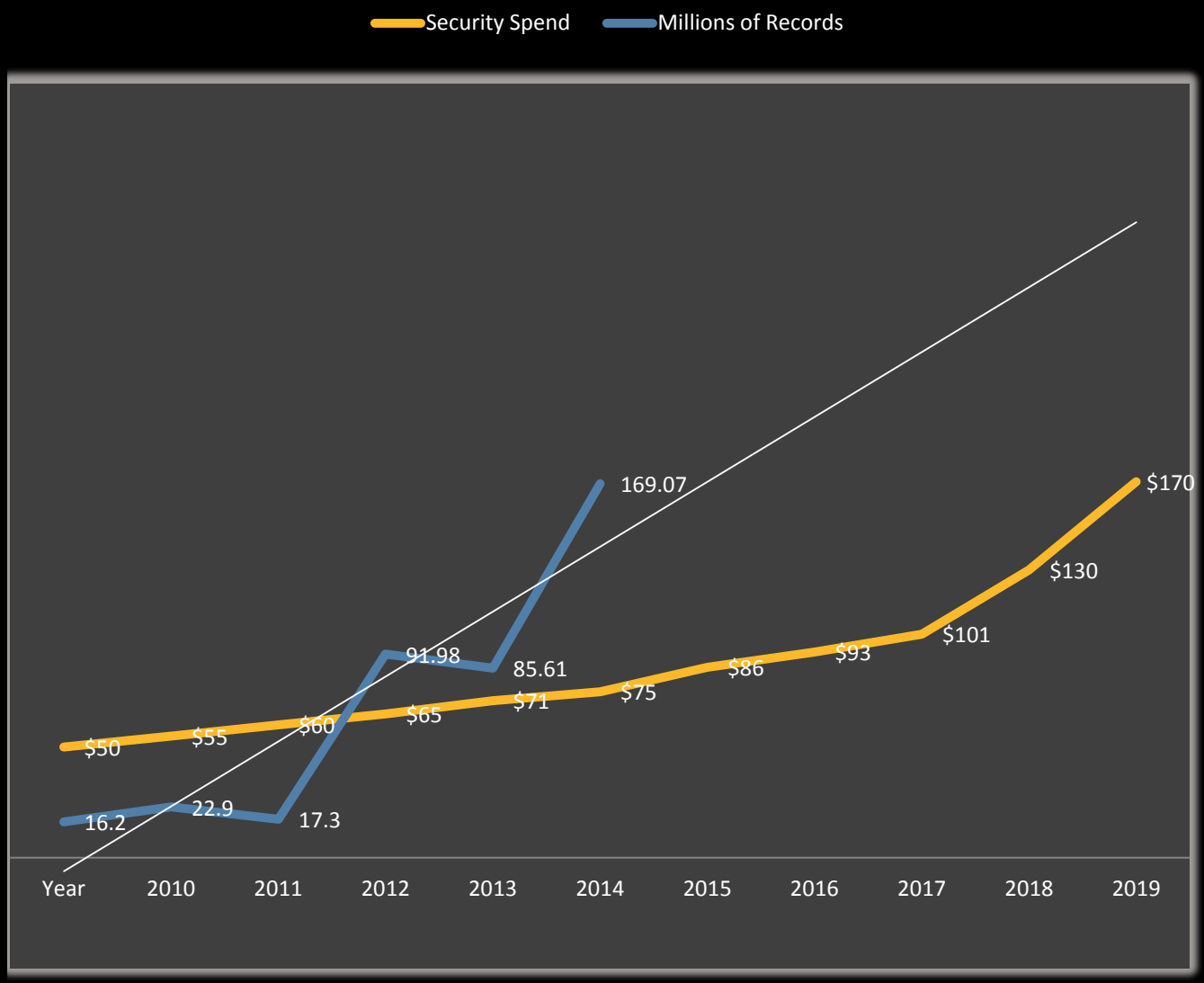
Why Are We Loosing So Often?

- Attackers are better and faster than many Defenders
  - Faster to exploit than we typically defend
  - Quick to adjust tactics, techniques and procedures
  - They are masters of blending in and staying entrenched
- Defenders are bogged down
  - Slow to detect, average ~8 months till breach is detected
  - Investigations – lack of skills, tools and telemetry, manual process
  - Response – can be ineffective; manual process; slow to change environment
  - Lack of meaningful Intelligence and related workflows – difficult to share, more difficult to use, even more difficult to automate

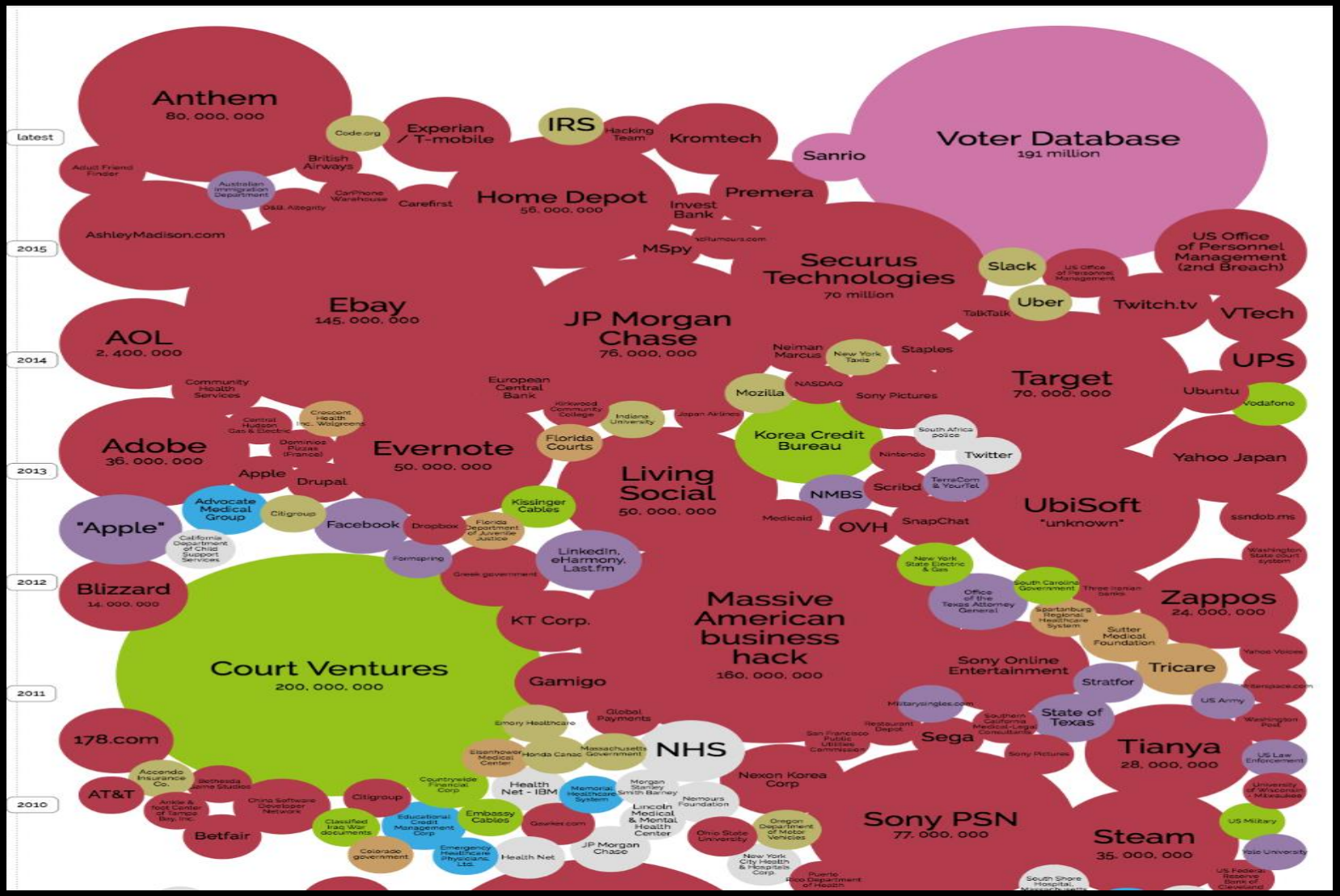
Security Spend – Past and Projected



Breached Record Loss Climbing Despite Massive Spending Increases

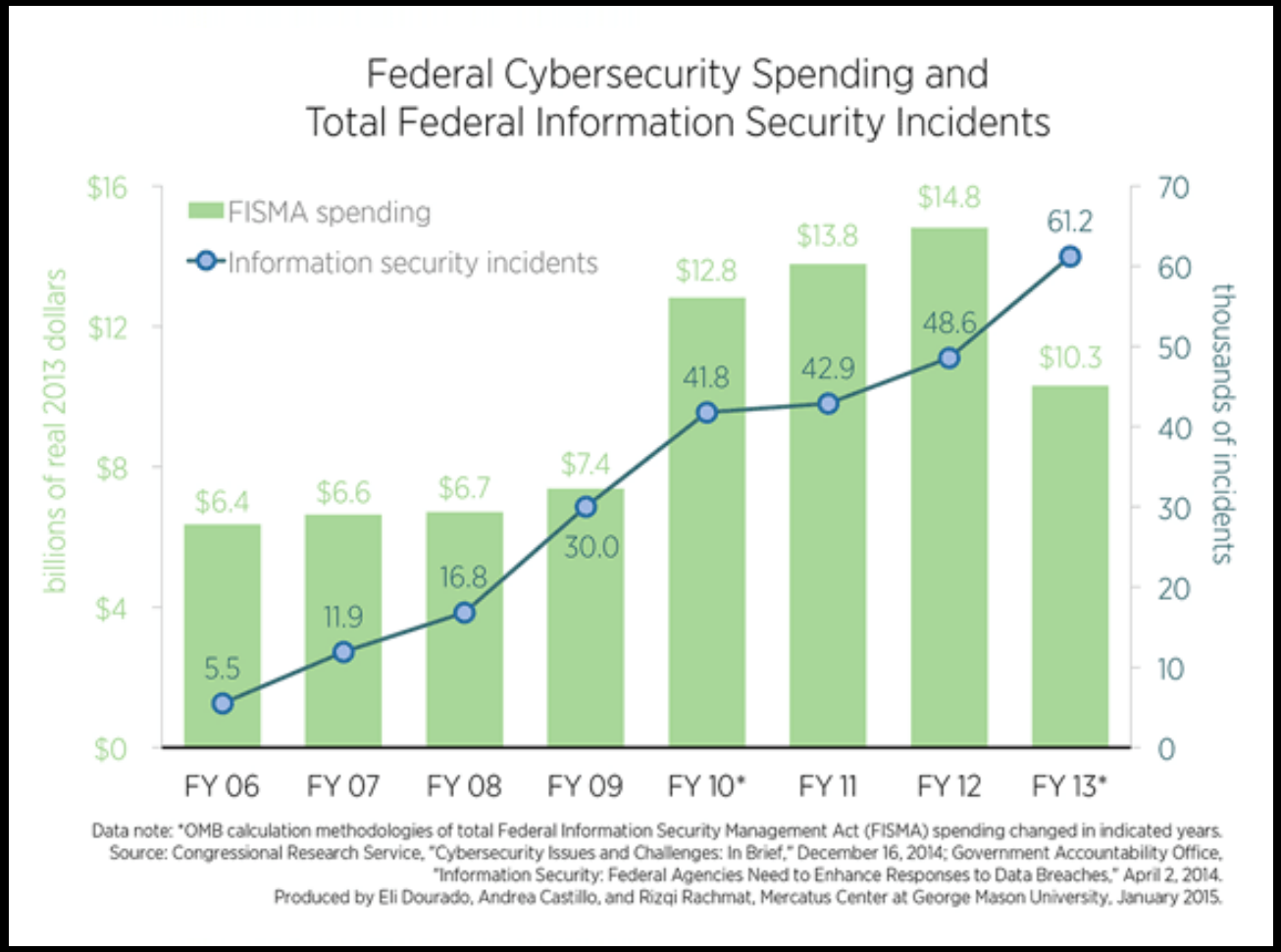


Breaches Keep Coming



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

Increased Federal Spending Has Not Stopped A Growing Rate of Loss



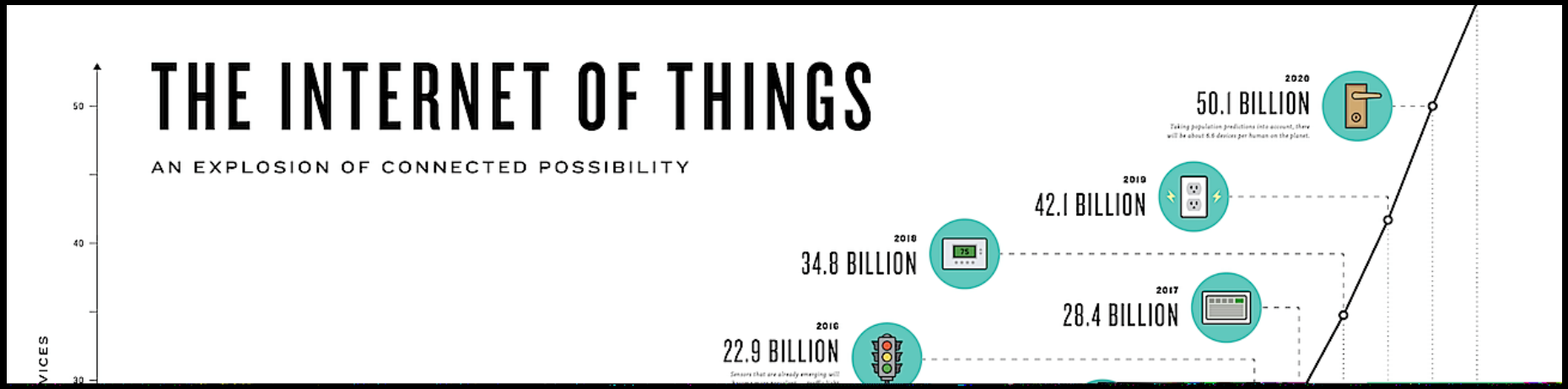
Impacts

Source: http://news.microsoft.com/stories/cybercrime/index.HTML

CYBERCRIME WILL COST BUSINESSES OVER $2 TRILLION BY 2019

Source: Juniper Research

Exponential Growth in IoT Means Increased Attack Surface



> *All of the potential weaknesses that could afflict IoT systems, such as authentication and traffic encryption, are already well known to the security industry...*

To find out for ourselves how IoT devices fare when it comes to security, we analyzed 50 smart home devices that are available today.

IoT vendors need to do a better job on security before their devices become ubiquitous in every home, leaving millions of people at risk of cyberattacks.

We found that none of the devices enforced strong passwords, used mutual authentication, or protected accounts against brute-force attacks.

Almost two out of ten of the mobile apps used to control the tested IoT devices did not use Secure Sockets Layer (SSL) to encrypt communications to the cloud. The tested IoT technology also contained many common vulnerabilities.

"We believe that data is the phenomenon of our time. It is the world's new natural resource. It is the new basis of competitive advantage, and it is transforming every profession and industry. If all of this is true – even inevitable – then cyber crime, by definition, is the greatest threat to every profession, every industry, every company in the world." --Ginni Rometty, IBM CEO

It’s 2016. Do you know where your data is at?

- 64% of organizations don’t have a complete picture of where their sensitive data is located
- Thus, they are unable to determine if such data is compromised or breached

Why Attackers Succeed

- Many reasons; certainly Advanced Attacks require advanced defenses, however…
- Many breaches and security incidents could have been prevented with basic cyber hygiene

Center For Strategic & International Studies findings

- 80 to 90 percent of successful breaches of corporate networks required only the most basic techniques.
- …Found four risk reduction measures block most attacks. Agencies and companies implementing these measures saw risk fall by 85 percent and, in some cases, to zero.
  - Whitelisting
  - Rapid Patching of the OS
  - Rapid Patching of programs
  - Reduce Administrator privileges

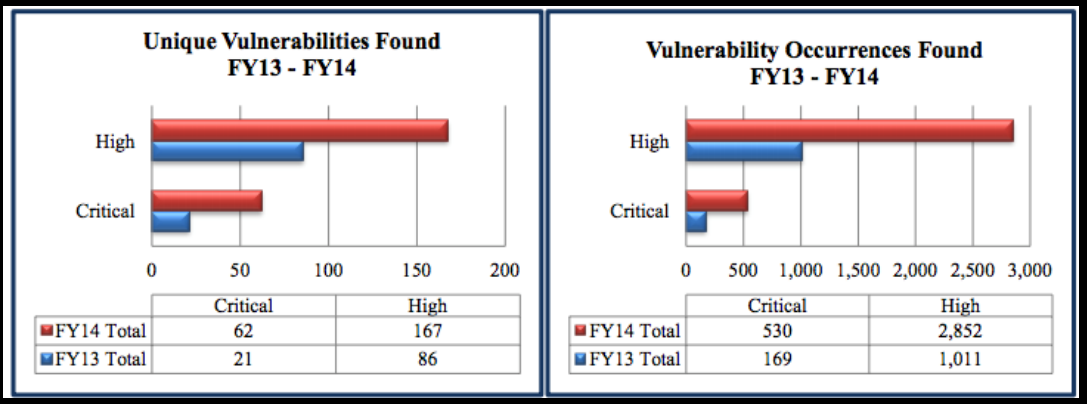
Center for Strategic & International Studies; Raising the Bar for Cybersecurity

DHS NCATS - Cyber Hygiene Scans

68 Participating stakeholders

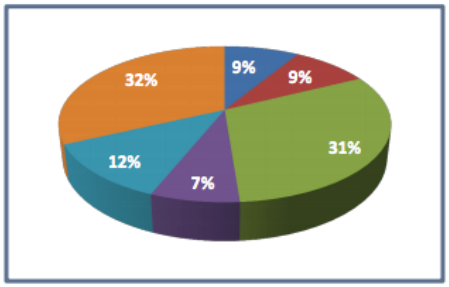
384 Cyber Hygiene scans conducted in FY14

16.9 Million Scanned IP addresses



Top Three Findings & Main Method of Identification

1. Patch Management (88 percent found with automated testing)
2. Sensitive Business Data Disclosure (100 percent found with manual testing)
3. Cross-site Scripting (63 percent found with manual testing)



- Access Control (9%)
- Awareness and Training (9%)
- Configuration Management (31%)
- Identification and Authentication (7%)
- System and Communications Protection Testing (12%)
- System and Information Integrity (32%)

Achilles Heel + Password = 258,000 Google Hits

THE NO. 1 CAUSE OF BREACHES AND COMPROMISED RECORDS IN LARGE ORGANIZATIONS?

STOLEN CREDENTIALS

Top 500 Passwords

Beyond The Basics – Threat Intelligence

- Currently slow turn around between receipt & processing of threat intelligence and adjustment of the control environment
- Manual work for analyst to investigate
  - Given an IoC, what is vulnerable and where?
  - What are current / future impacts to the environment? Compromised or infected hosts? Data at risk? Pivots points?
  - Related telemetry and forensic data – where is this data captured, how can I retrieve it quickly and in a single location that supports my analysis workflow?
  - Remediation - What gets priority?
  - What controls are already in place to mitigate threat?
- Manual response
  - Update network, email, endpoint control points
- Sharing Threat intelligence
  - Variety of tools and data formats
  - Lack of meaningful shared Course of Action
  - Community data – is it accurate? Duplicated? Complete? From reliable source?

Beyond the Basics - Detection

- Prevention is ideal but Detection is an absolute must
- Missed detection = compromise, breach, etc.
- Detection capabilities must detect quickly to thwart attack as early in the kill chain as possible
- Detection services are often stand-alone
  - No awareness of environment or control state or actions
  - No coordinated telemetry to leverage in gaining context of wider view of attack both internally or globally
- Attackers adjust to detection capabilities
  - Virtual aware malware - Virtual combustion chambers no longer adequate
- Once threat is detected, response actions are often not orchestrated / automated
  - Lack of coordinated C2 across heterogeneous environments
  - Update all control points automatically and reference other telemetry to further harden environment

Beyond the Basics – People, Services and Process

- Governance & Risk Management
- High Value Services
- Process maturity
- Security Talent

Thank you!

Tom Blauvelt
Principal Security Architect
Symantec

@TomBlue01