

# **Cybersecurity Overview**

## **IT Council, Public Session**

---

**Leslie Williams**

**Chief Information Security Officer**

***August 17, 2012***

# Agenda

---

- Authority
- Current Environment
- Top Threats
- Top Vulnerabilities
- Questions

# Authority

---

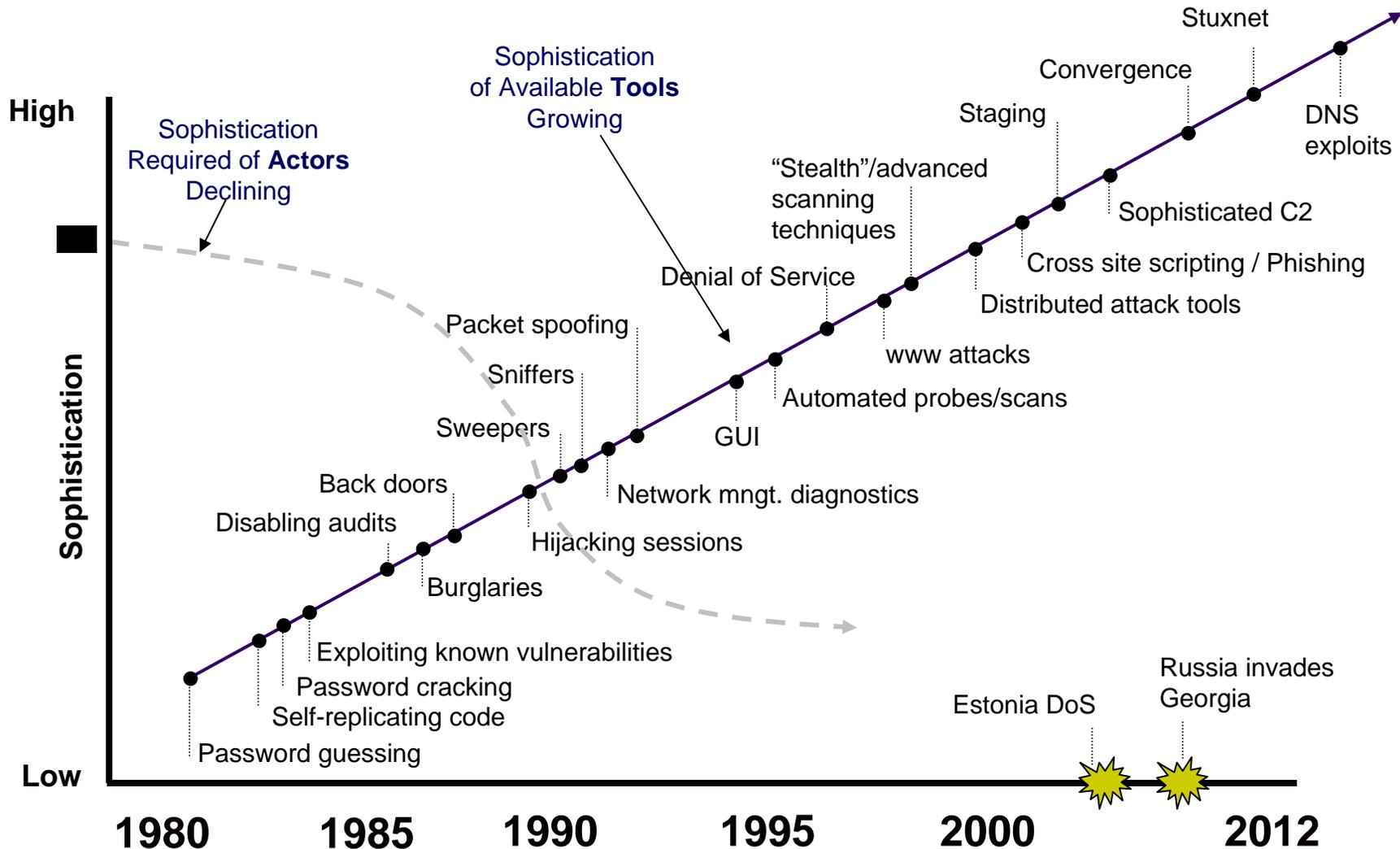
- HB1593 passed for Executive Branch agencies
- Amended to the Duties of the Commissioner/CIO:
  - *Developing and implementing a strategy to address cybersecurity risks to the state's data, information assets, and technology resources*
- Cybersecurity Strategic Plan being created:
  - Improved Awareness
  - Enhanced Standards and Controls
  - Proactive Risk Management
  - Robust Incident Response

# Current Environment

---

- **Attacks**: High value, low risk repeated attacks; less skill and cost
- **Methods**: Constantly changing to evade detection
- **Motives**: Financial, political, protests, prestige, revenge
- **Attackers**: Hacktivists, organized crime, those with grudges
- **Targets**: Personal and organization data, credentials
- **Victims**: Broad diversity - government, business, public
- **Loss**: Identity, credit card information, intellectual property

# Growth of Cyber Threats



Source: Department of Homeland Security



Homeland Security

# Top Threats

---

THREATS: Anything which has the potential to do harm

Top threats continue to be **Malware** and **Hacking** to:

- disrupt computer operations
- capture sensitive information
- gain access to computer systems
- **Malware** (malicious software) is a general term that refers to a variety hostile, intrusive, or annoying software. It includes viruses, worms, spyware, adware, and is commonly served through phishing emails and untrustworthy websites.
- **Hacking** - subverting computer security for malicious purposes. Long-term targeted hacking attacks are called Advanced Persistent Threats
- **Insiders** also a concern: Employees/contractors; accidental/intentional

# Top Vulnerabilities

---

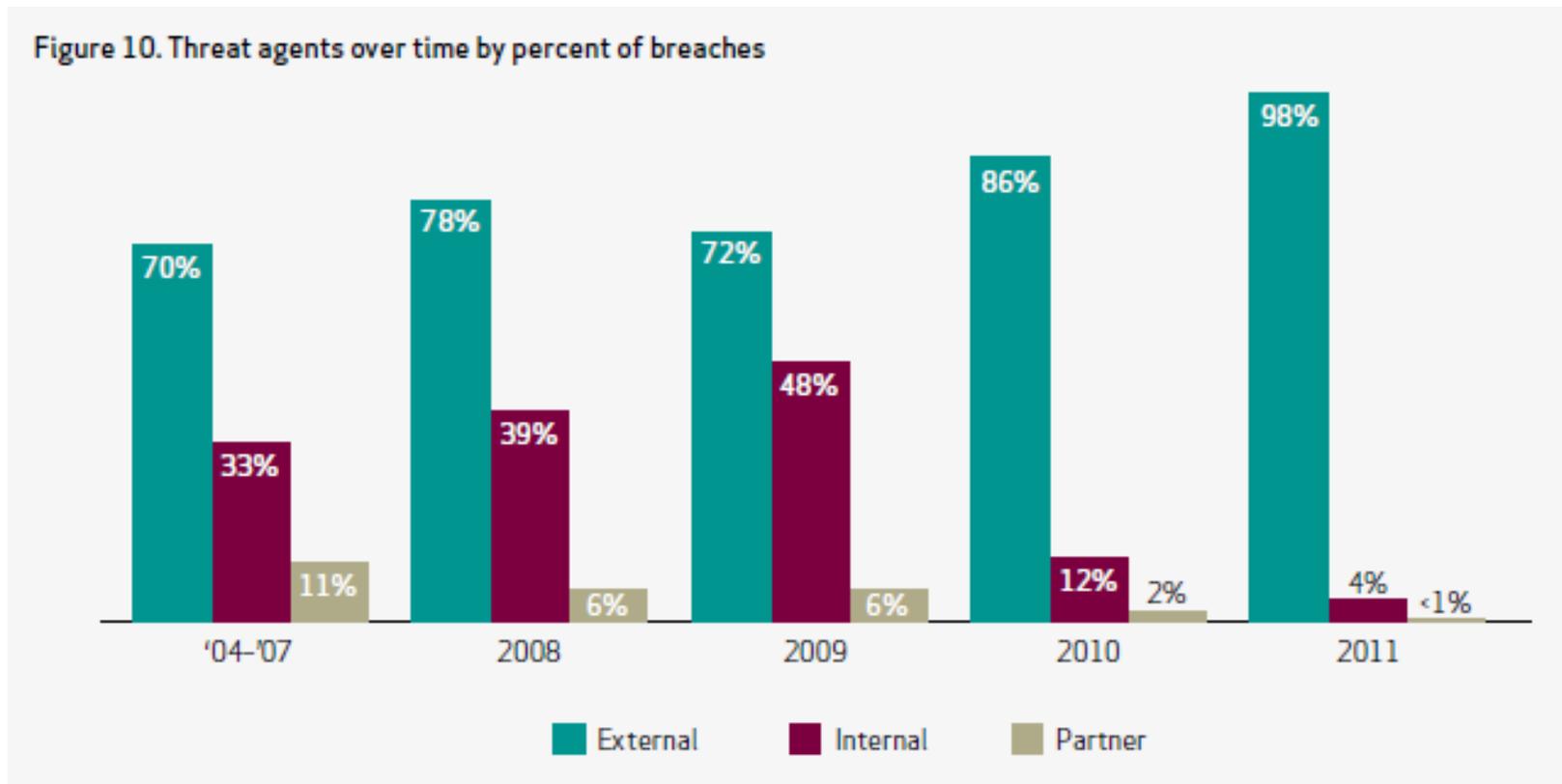
**VULNERABILITIES:** A weakness which can be exploited to cause harm

- Mobile devices: Smart phones, thumb drives
- Social media: Source of viruses, trojans, worms, & malicious attacks
- Aging infrastructure: Security vulnerabilities no longer 'patched'
- SCADA control systems: Impact to critical infrastructure
- Cloud computing: Exposes data outside the protected network
- Web Applications: Subject to unauthorized access and attack

**RISK =** Likelihood that threat will exploit a vulnerability and cause harm

# Top Threat Agents - WHO

---

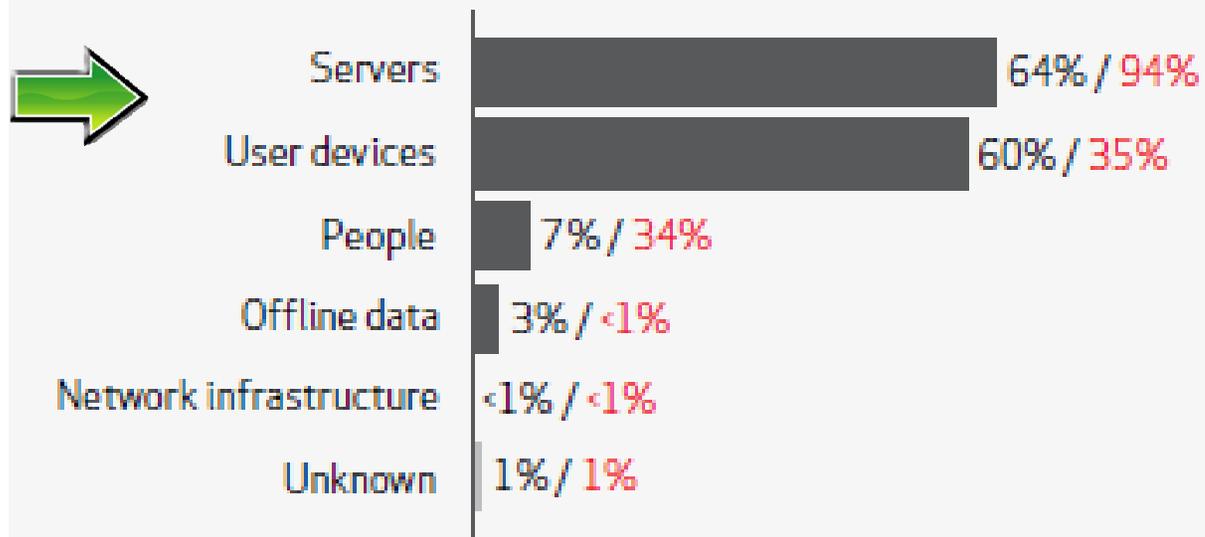


Source: Verizon 2012 Data Breach Investigations Report

# Top Targets - WHAT

---

Figure 26. Categories of compromised assets by percent of breaches and percent of records



Source: Verizon 2012 Data Breach Investigations Report

# Data Breach Summary - HOW

---

## HOW DO BREACHES OCCUR?

81% utilized some form of hacking (+31%)

69% incorporated malware (+20%)

10% involved physical attacks (-19%)

7% employed social tactics (-4%)

5% resulted from privilege misuse (-12%)



## WHAT COMMONALITIES EXIST?

79% of victims were targets of opportunity (-4%)

96% of attacks were not highly difficult (+4%)

94% of all data compromised involved servers (+18%)

85% of breaches took weeks or more to discover (+6%)

92% of incidents were discovered by a third party (+6%)

97% of breaches were avoidable through simple or intermediate controls (+1%)

96% of victims subject to PCI DSS had not achieved compliance (+7%)

Source: Verizon 2012 Data Breach Investigations Report

# Summary

---

- Guiding Principles:
  - **Follow best practices**
  - **Use standard products and controls**
  - **Share information - dissemination and reporting**
  - **Promote good user computing practices**
  - **Cultivate partnerships - EM, LE, IT, Business**
  - **Prepare for incident response**
  - **Integrate security into operations**

# Questions

---