CenturyLink and Cyber Security

Chris Wallace
Lead Intelligence Analyst
2014: The Year of the Data Breach

783 US. data breaches tracked in 2014, with a 261% increase in size over 2013!

70 M credit cards compromised due to vendor leak. $200 Million+

56 M credit cards leaked after security turnover & software issues. $200 Million

Digital business assets exploited, damaging the brand, and taking down parts of the network for months. $15 Million+

### Five Primary Sources of Threats

**INSIDE AND OUTSIDE THE NETWORK**

<table>
<thead>
<tr>
<th>STATE SPONSORED</th>
<th>CYBER CRIMINALS</th>
<th>TERRORISTS</th>
<th>HACKTIVISTS</th>
<th>INSIDER THREATS</th>
</tr>
</thead>
<tbody>
<tr>
<td>GOVERNMENT FUNDED ESPIONAGE</td>
<td>WELL FUNDED CRIMINALS</td>
<td>ZEALOTS W/ STRONG VIEWS</td>
<td>PROTESTERS WITH AN AXE TO GRIND</td>
<td>EMPLOYEES</td>
</tr>
<tr>
<td>Target governments and private industry to further political change</td>
<td>Seek companies with customers and money to lose</td>
<td>Seek revenge, damage, change</td>
<td>Promote political ends by targeting specific companies</td>
<td>Malicious or not, represent up to 40% of data breaches</td>
</tr>
</tbody>
</table>

**Where is the danger? Top threats in 2014:**

1. Malicious Code
2. Web-based attacks
3. Web application attacks
4. Botnets
5. DDoS
6. Spam
7. Phishing
8. Exploit Kits
9. Data Breaches
10. Physical damage / threat / loss
11. Insider threats
12. Information Leakage
13. Identity Theft / Fraud
14. Cyber espionage
15. Ransomware

Source: “enisa Threat Landscape 2014"
Cyber Kill Chain

Pre-Compromise Phase:

- **Reconnaissance**
  - Find a Target.
  - Develop a plan of attack based on opportunities.

- **Weaponization**
  - Creation of the payload, this could be the creation of malware or any other tool, process, or action needed in the attack.

Compromise:

- **Delivery**
  - Use of Social Engineering to induce target to access malware, exploit, or other weapon

- **Exploitation**
  - Exploit vulnerabilities on the target system to acquire access

Post Compromise:

- **Installation**
  - Installation of Payload

- **Command & Control**
  - Establish persistence and remote control of system

- **Action on Objectives**
  - Complete objectives

---

CenturyLink Business
EXAMPLE
Criminal Activity: How The Underground Economy Works

THE UNDERGROUND ECONOMY CHAIN
Source: Michael Yip, The University of Southampton, Oct 2012
An Expansive View of Cyber Threats

- “Hackers”/Traditional Information Security
- Supply Chain/Vendors/Partners
- International Operations
- International Travel
- Insider Threat
- Physical Infrastructure
CenturyLink Works with Many Government and Private Entities for National Security and Customer Protection

<table>
<thead>
<tr>
<th>Defense</th>
<th>Homeland Security</th>
<th>Justice</th>
<th>Private Sector</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Department of Defense" /></td>
<td><img src="image" alt="Department of Homeland Security" /></td>
<td><img src="image" alt="Department of Justice" /></td>
<td><img src="image" alt="Microsoft" /></td>
</tr>
<tr>
<td><img src="image" alt="National Institute of Standards and Technology" /></td>
<td><img src="image" alt="National Cyber Security Coordination Center" /></td>
<td><img src="image" alt="Department of Homeland Security" /></td>
<td><img src="image" alt="National Cyber Security Coordination Center" /></td>
</tr>
<tr>
<td><img src="image" alt="Federal Communications Commission" /></td>
<td><img src="image" alt="Cyber Unified Coordination Group" /></td>
<td><img src="image" alt="Defense Information Systems Agency" /></td>
<td><img src="image" alt="Global Infrastructure Alliance for Internet Safety" /></td>
</tr>
<tr>
<td><img src="image" alt="FCC" /></td>
<td><img src="image" alt="NCCIC" /></td>
<td><img src="image" alt="DSAC" /></td>
<td><img src="image" alt="Network Service Provider (NSP) Security (NSP-SEC)" /></td>
</tr>
<tr>
<td><img src="image" alt="Centers for Disease Control and Prevention" /></td>
<td><img src="image" alt="Active contributor/participant" /></td>
<td><img src="image" alt="SANS" /></td>
<td><img src="image" alt="Network Information Sharing Exchange (NSIE)" /></td>
</tr>
<tr>
<td><img src="image" alt="Centers for Disease Control and Prevention" /></td>
<td><img src="image" alt="24/7 presence within DHS" /></td>
<td><img src="image" alt="State Department" /></td>
<td><img src="image" alt="Defense Industrial Base Information Sharing Exchange (DSIE)" /></td>
</tr>
<tr>
<td><img src="image" alt="Centers for Disease Control and Prevention" /></td>
<td><img src="image" alt="Permanent seat on NCCIC floor" /></td>
<td><img src="image" alt="State Department" /></td>
<td><img src="image" alt="OPS-Trust" /></td>
</tr>
<tr>
<td><img src="image" alt="Centers for Disease Control and Prevention" /></td>
<td><img src="image" alt="Member of Cyber Unified Coordination Group" /></td>
<td><img src="image" alt="State Department" /></td>
<td></td>
</tr>
</tbody>
</table>
NIST Framework

• Voluntary Framework to develop a comprehensive cybersecurity program
• Based on existing standards, guidelines, and practices - for reducing cyber risks to critical infrastructure.
• US-based collaboration between government and industry, becoming a best practice.

Download the framework overview: