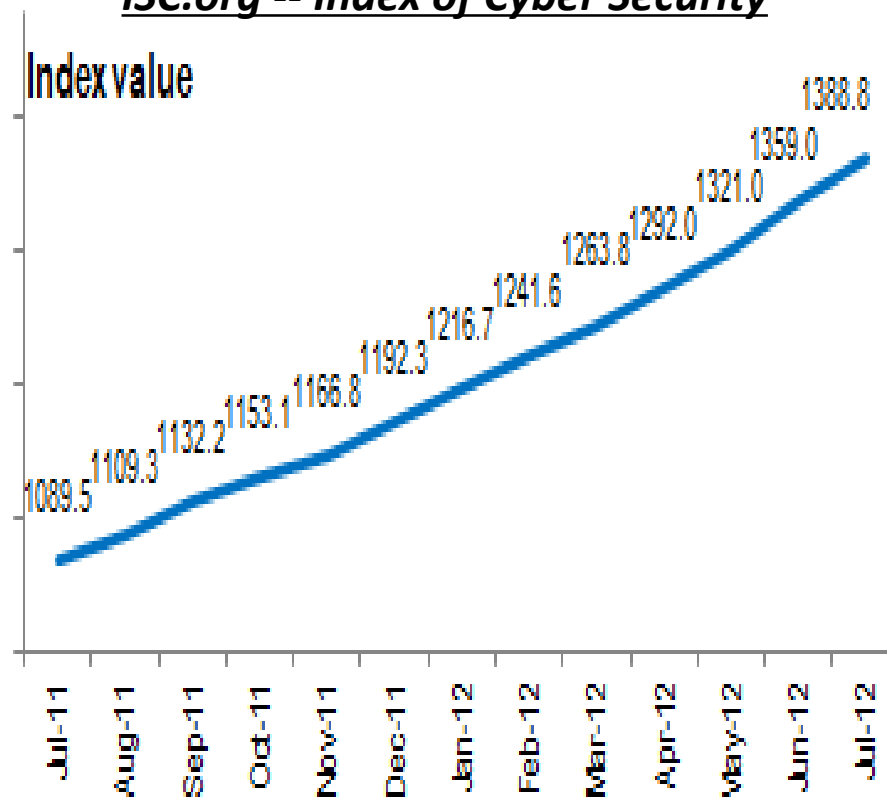# The State of Security

- **Adversaries have significant technical means funded by cyber-crime profits and nation-state taxation**
- **Defending with a low-cost defense**
- **Current tools quickly becoming obsolete by rapidly changing technology**
  - **Cloud computing**
  - **Virtualization**
- **Third party transparency is a major issue**
- **Compliance burden is dramatically increasing and is, generally, not accretive to improving the security posture**

The Statistics of Security

- **Highly agile adversaries exploit vulnerabilities in less than 24 hours**

- **Signature-based defenses stop about 80% of attacks**

  - **Compliance continues to dominate the security agenda growing 12% YOY**

  - **Cyber-crime risk grew overall 27.5% YOY**

  - **Third Party Risk grew 44% YOY**

  - **Insider Risk grew 33% YOY**

  - **Staff retention drop 6%**

  - **Recruiting subject matter expertise (0% unemployment rate among security professionals)**

  - **Flat Budgets**

  - **Impacted by IT transformation to new technology and cloud and lack of security tools.**

ISC.org -- Index of Cyber Security

Index value

1089.5 1109.3 1132.2 1153.1 1166.8 1192.3 1216.7 1241.6 1263.8 1292.0 1321.0 1359.0 1388.8

Jul-11 Aug-11 Sep-11 Oct-11 Nov-11 Dec-11 Jan-12 Feb-12 Mar-12 Apr-12 May-12 Jun-12 Jul-12

Change Course

Security is the absence of unmitigatable surprise

When you get to a fork in the road take it. -- *Yogi Berra*

Resilient Defense
Detect, Deflect, Deter, Defend

- **Recognize Anomalies**
- **Assume you will fail and pick more tolerable failure modes**
- **Pair robust application and network security with rapid and effective incident response.**
- **Couple interplay between inbound penetration and outbound exfilitration create increased visibility and thus detection opportunities**
- **Create strong visible deterrents**
- **Integrate defense and intelligence**

Implementation

- **Aggregate**
  - **Holistic security can only be achieved when it is integrated**
  - **Converged Security is a must**
- **Automate**
  - **Reduce compliance burdens**
  - **Zeroing mean time to repair, not infinitizing mean time between failures**
  - **Reduce false positives to a manageable roar**
- **Arbitrage It**
- **Accelerate It – processes, reaction time, change, diversity**

'Killing the most dangerous animal on your front porch does nothing to change the number of dangerous animals in your front yard'
-- Dan Geer

"The future ain't what it used to be"
-- Yogi Berra