In the Dark

Critical Industries Confront Cyberattacks

McAfee's Second Annual Report on Critical Infrastructure written by CSIS

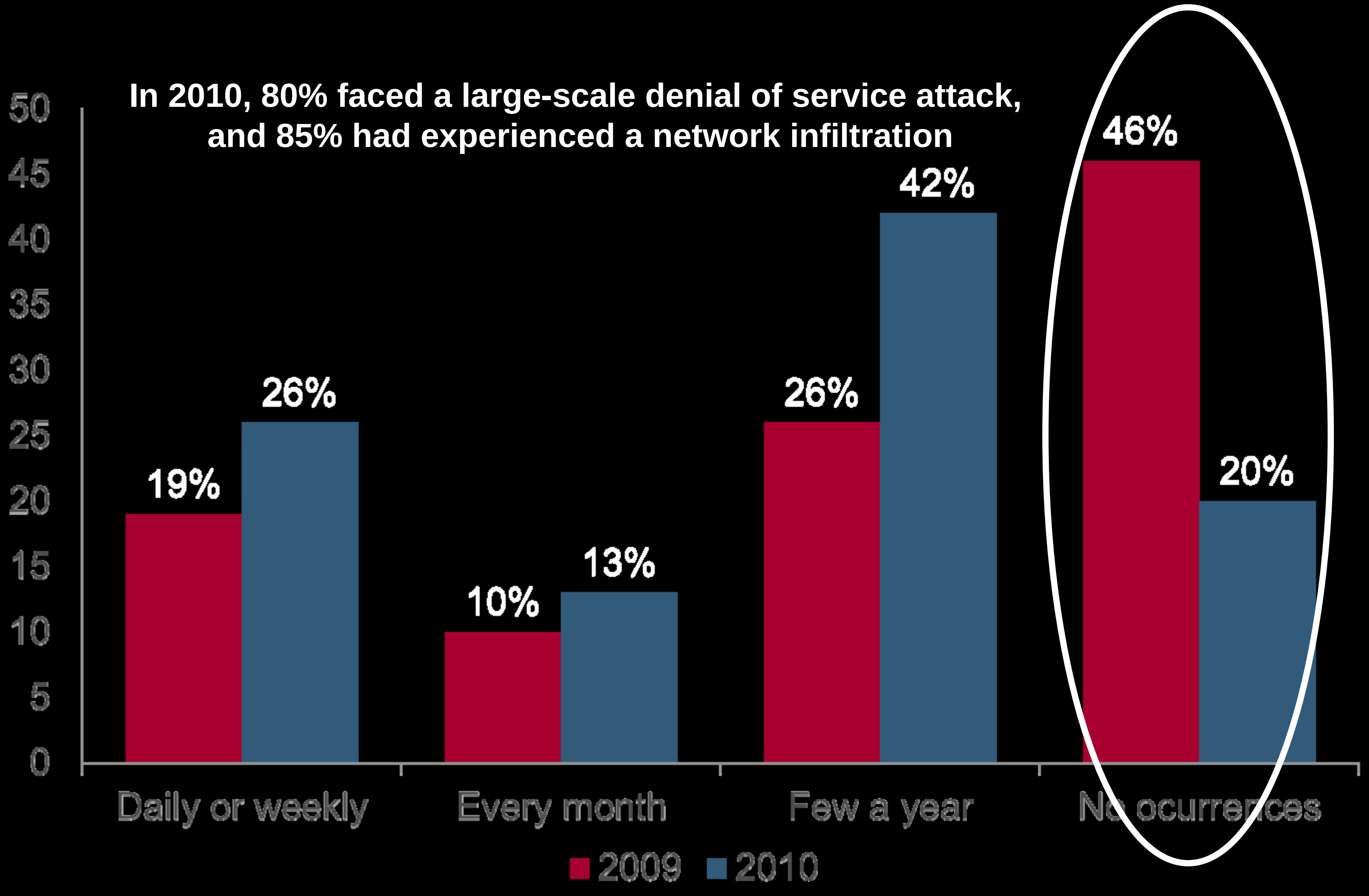
Stewart Baker, Steptoe & Johnson and CSIS
Phyllis Schneck, McAfee

1. Threats Growing Faster Than Security Measures

Stuxnet Ushered in a New Era

- For years, industry experts were reluctant to acknowledge the risk, fearing new security regulation
- Stuxnet is a weapon, it shows that hostile governments can easily target SCADA systems on which a nation’s power, gas, oil, water and sewage infrastructure depends .
- 57% launched special security audits or other measures in response to the widespread publicity concerning the Stuxnet
- Almost 40% of respondents found Stuxnet in their environment
- Most critical infrastructure was not designed with cybersecurity in mind

Threats & Vulnerabilities Accelerating



In 2010, 80% faced a large-scale denial of service attack, and 85% had experienced a network infiltration

Responding to Threats
Resources and preparedness

- 37% of respondents said their sector was either "not at all prepared" or "not very prepared" to deal with large-scale DDOS attacks in the future.
- 35% of companies are not prepared for stealthy infiltration to their networks by organised crime organisations or a nation state
- 1 in 4 companies are not prepared for a malware attack designed for sabotage
- Low confidence in preparedness of government services. Only 36% of respondents are confident their government services could continue in the face of a major cyber attack.

2. The “Smart” Grid

Smart Grid

- Power companies are increasing the danger by implementing “smart grid” technology
- This technology controls the delivery of power to individuals or appliances
- Without better security, this increased control can give criminals or “hacktivists” the ability to modify billing information and perhaps even control which customers or appliances get electricity.
- But security is not a priority for smart grid designers

32% of companies **have not adopted** adopted special security measures for smart grid controls

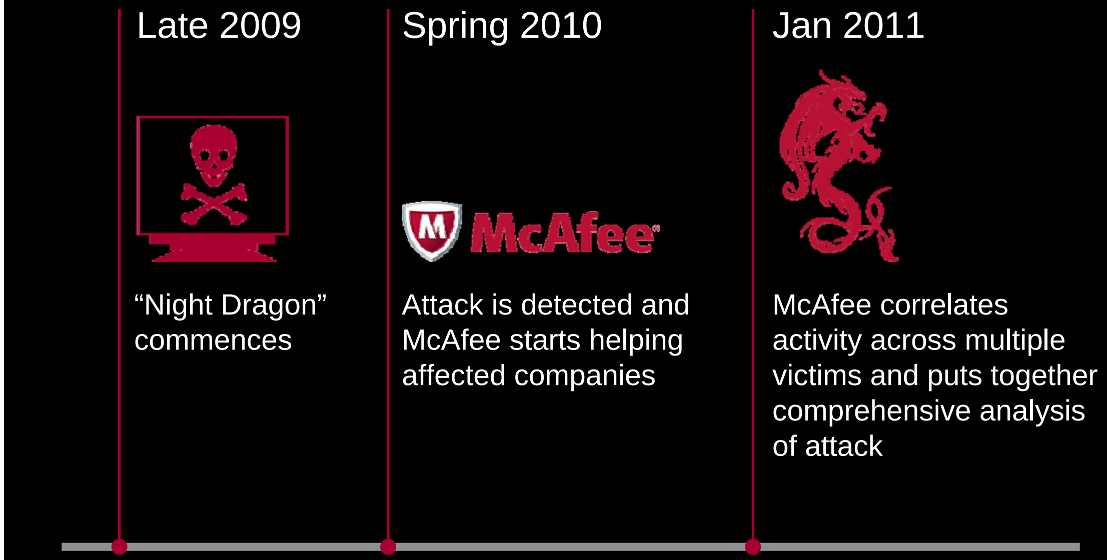
Smart Grid -- Not so Smart

- Four out of five executives intended to implement some form of “smart grid”, such as time-sensitive rates, service cutoffs, and service reductions.
- 56 percent of the executives whose companies are planning new smart grid systems also plan to connect to the consumer over the Internet.
- Most realized that the new systems will add challenging security vulnerabilities, but only two-thirds plan to adopt special security measures for the systems

At least one executive we interviewed decried “the dumbness of ‘let's put every household's power supply on the Internet -- and call it 'smart'!"

More than $200 billion is expected in global smart-grid investment expected between 2008 to 2015 by, with almost US$53 billion just in the U.S.
– Source: Pike Research Group 2010

“Night Dragon” Energy Cyberattacks Validate Findings



Late 2009

“Night Dragon” commences

Spring 2010

Attack is detected and McAfee starts helping affected companies

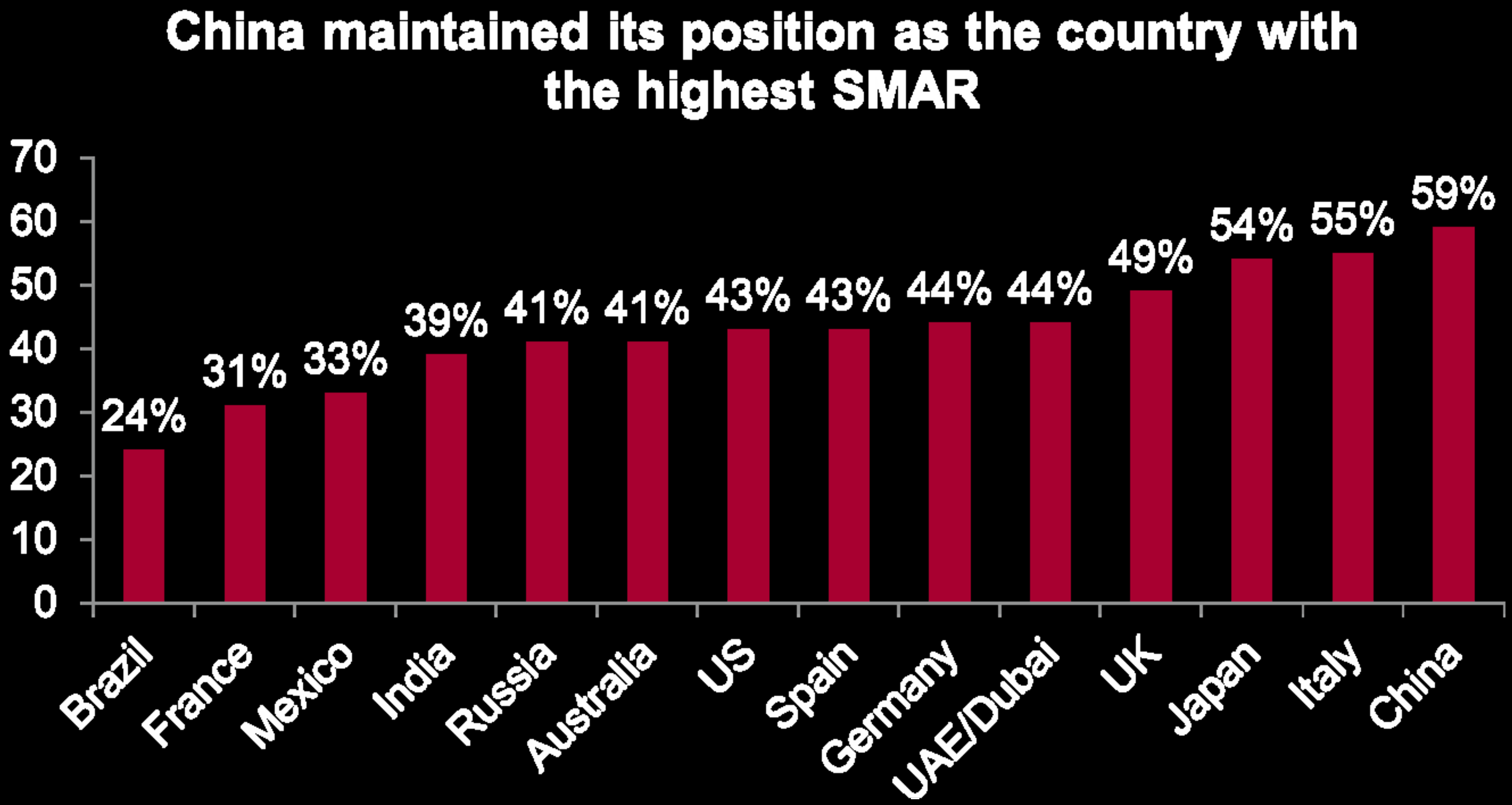
Jan 2011

McAfee correlates activity across multiple victims and puts together comprehensive analysis of attack

- Named by McAfee in January 2011 and investigated since early 2010
- Long-term, targeted attack against global oil, energy and petrochemical companies
  - Gigabytes of documents related to oil/gas field bidding projects, oil discoveries and industrial control (SCADA) data compromised
- C&C servers and source attack traffic coming from IP addresses all over the world

3. Growing Divergence in How Countries Respond

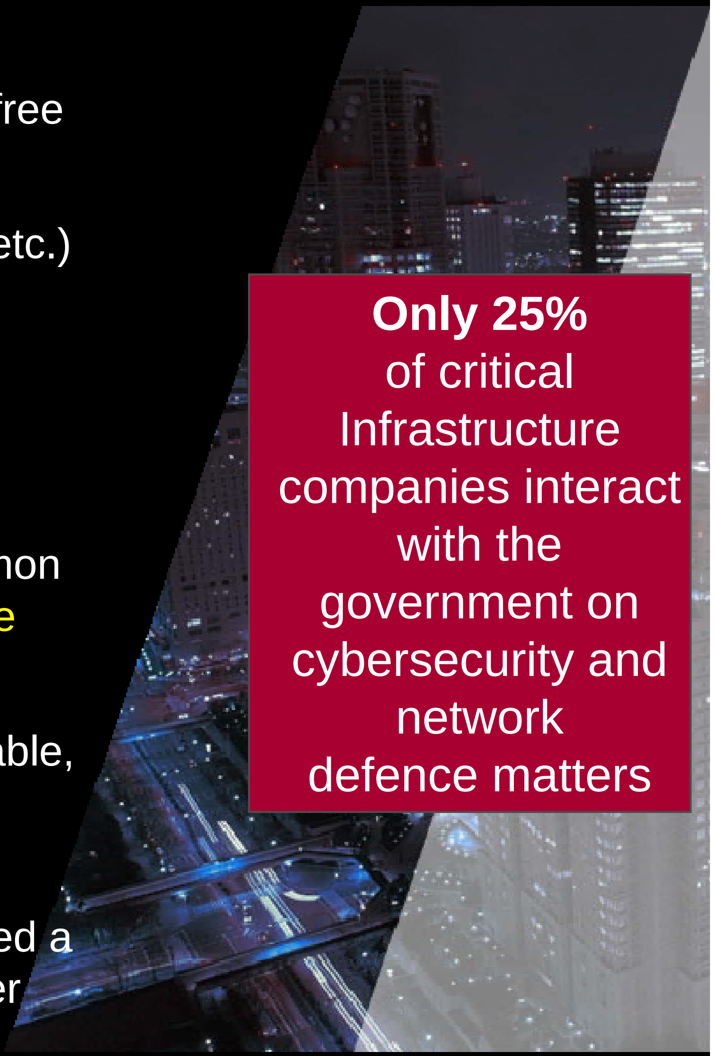
Security Measure Adoption Rates (SMAR)



July 18, 2011

What is Government's Role?

- Reasons for divergence among countries in terms of security is also related to the role the Government plays
- The private sector bears responsibility of keeping systems free of cyber attacks
- Most critical infrastructure (water supplies, electrical grids, etc.) are today privately owned in developed countries
- The current lack of communication between government and the private sector will make it difficult to be proactive against a cyber attack
- The government is generally responsible to provide a common defence but country's with high public-private interaction are better prepared for cyberattacks, notably Japan and China
- 54% of respondents report that authorities are "mostly capable, capable or completely capable" of preventing or deterring attacks.
- Countries such as Brazil, Mexico and India have experienced a loss of confidence in their Government's capabilities to deter attacks



Only 25% of critical Infrastructure companies interact with the government on cybersecurity and network defence matters

Summary

Cyber attacks on critical infrastructure are becoming more widely publicized such as Aurora and Operation Night Dragon protection

•Stuxnet ushered in the next phase of cyberattacks, SCADA systems being targeted

•40% of CIP executives found Stuxnet in their environment

•57% launched special security audits in response

SMART Grids are not so smart

•32% of companies have not adopted special security measures for smart grids

Threat and vulnerabilities accelerating

- 80% have experienced large scale DDOS, and 85% have experienced a network infiltration

- 37% have experienced an increase

Extortion is widespread

-1 in 4 infrastructure entities are victims of extortion, especially in Mexico and India

Preparedness to attacks on critical infrastructure

•37% are not prepared for a cyber attack attack

•35% not prepared for a network infiltration

•Least prepared are Brazil, France and Mexico

•Energy sector is the most vulnerable