Strategic Cyber Security

The Best protection is good defensive measures

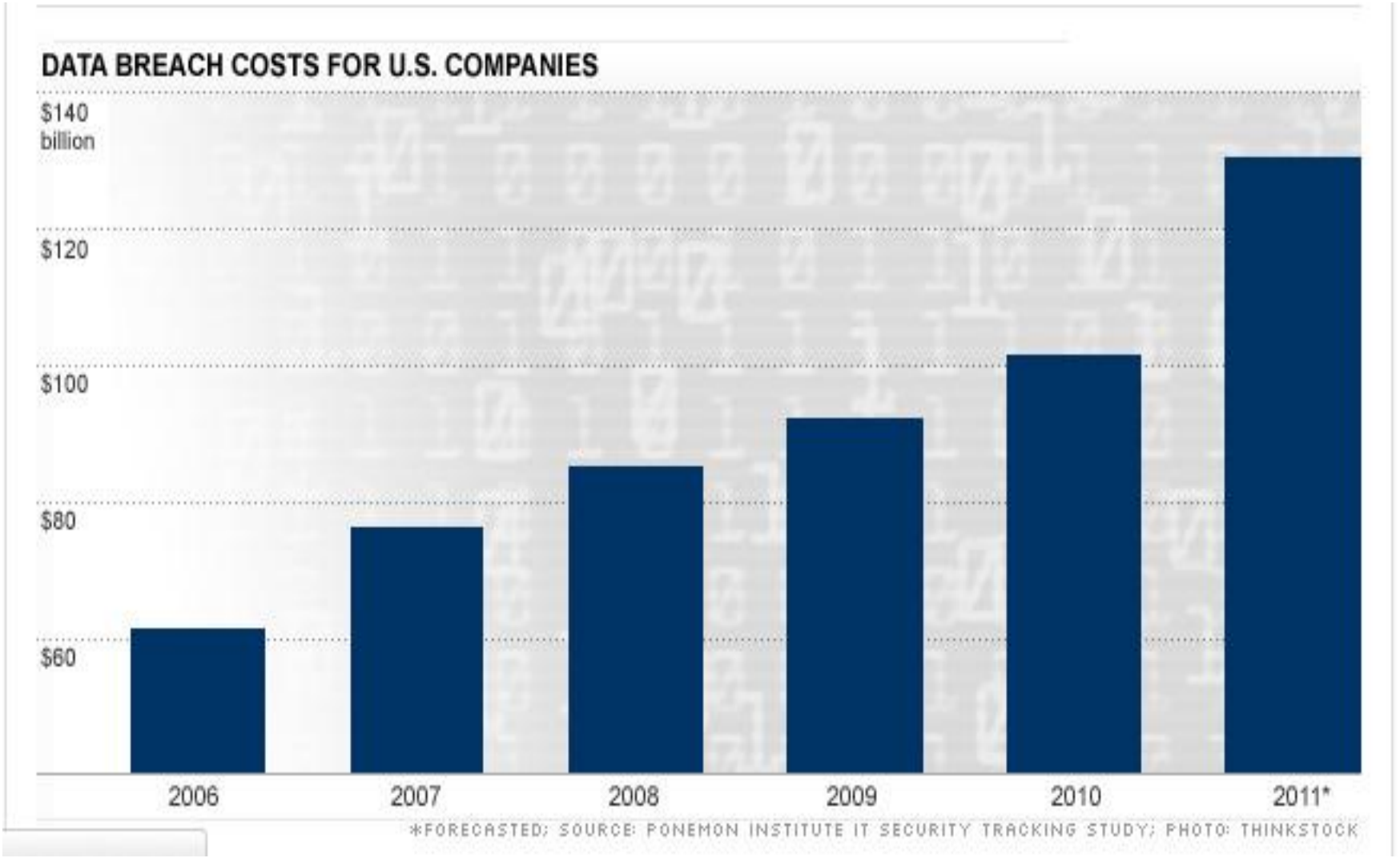
Bernard Tatera P.E.
Principal Automation Engineer, System Automation & SCADA
PG&E

March, 27, 2014

Cybercrime costs the United states economy about $100 billion each year, according to a study by the Center for Strategic Studies and software maker McAfee

San Francisco Chronicle –

Sunday February 2, 2014


DATA BREACH COSTS FOR U.S. COMPANIES
$140 billion
$120
$100
$80
$60
2006
2007
2008
2009
2010
2011*
*FORECASTED; SOURCE: PONEMON INSTITUTE IT SECURITY TRACKING STUDY; PHOTO: THINKSTOCK

Defensive Measures

Top 10 list for Cyber Security

1. Segregate Networks (Guest, Corporate and Control)
2. Remove or disable unnecessary software, services and Guest accounts
3. Limit or control who can install software
4. Classify Data and Encrypt sensitive data
5. Use complex passwords and different passwords for various accounts
6. Install Ad Blocking software –DRIVE BY MALWARE
7. Connect using VPN or https whenever possible – FIRESHEEP
8. Train employees not to click on suspicious links or open suspicious files
9. Establish and use standard and secure configurations of OS
10. Update operating systems and application software regularly

Segregate Networks (Guest, Corporate and Control)

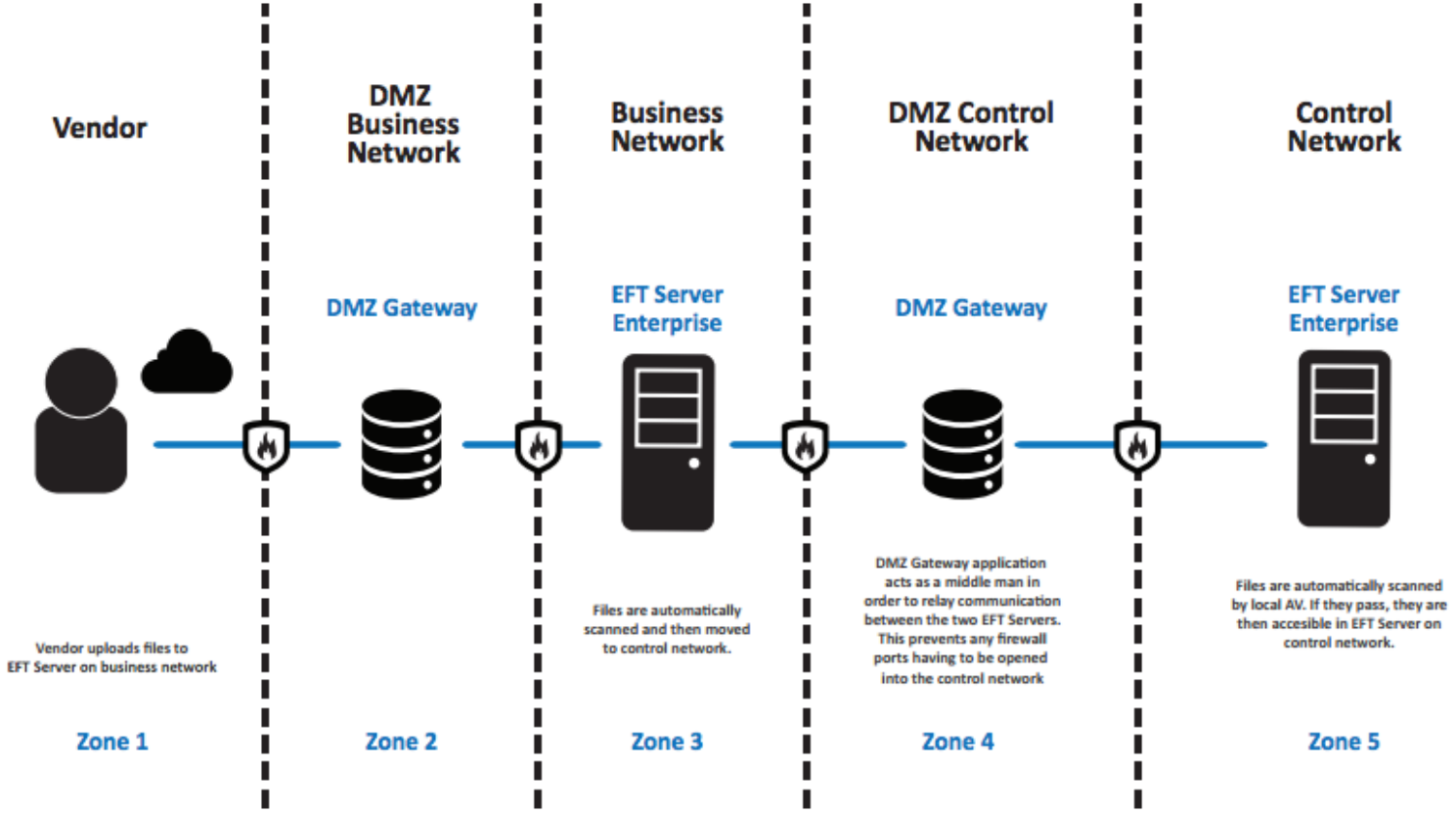
By properly segregating the network, you are essentially minimizing the level of access to sensitive information for those applications, servers, and people who don't need it, while enabling access for those that do.

Meanwhile you're making it much more difficult for a cyber-attacker to locate and gain access to your organization's most sensitive information.

Network Segmentation Example

globalscape™
securely connected

EFT SERVER ENTERPRISE HELPS TO REDUCE THESE RISKS CONSIDERABLY THROUGH MULTI-ZONE ARCHITECTURE



Our security architecture involves a total of five zones:

WIFI Hotspots & Network Security

The bottom line:

Wi-Fi hotspots pose greater risk because data capture is so easy there, but sidejacking is a network-independent attack against HTTP that can be performed in a wide variety of wired and wireless networks.

If you don't know how a network is secured or whether a website is vulnerable, just assume that you need to protect yourself.

Security for Control Systems

NIST 800-82 Guide to Industrial Control System Security

ISA-99 Industrial Automation and Control Systems Security Standard

DHS – Mitigations for Vulnerabilities found in Control (CS) Networks

DOE Control Systems Security Publications Library

Additional Resources for ICS Security

- National Cyber Security Division's Control Systems Security Program (CSSP) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)
- ISA99, Industrial Automation and Control Systems Security
- National Security Agency, A Framework for Assessing and Improving the Security Posture of Industrial Control Systems
- National Vulnerability Database (NVD)
- Department of Energy Control Systems Security Publications Library
- Idaho National Laboratory Critical Infrastructure Protection Program
- Sandia National Laboratories Center for Control System Security

Thank You

Bernard Tatera
bst1@pge.com