

THE SECURITY STANDARDTM



Securing the Enterprise from a Dangerous Cyberworld

September 19-20, 2011 • Marriott Brooklyn Bridge, New York City

Protecting the Enterprise Technology Supply Chain

Vijay Viswanathan Director & CISO HD Supply





Securing the Enterprise from a Dangerous Cyberworld

STUXNET

- Stuxnet is a computer worm or virus that was developed for the purposes of manipulating and sabotaging industrial controls inside factories, power plants and electric utilities that use Siemens SIMATIC WinCC (Windows) and PCS 7 control systems
- Stuxnet is the first virus to be active in the physical world
- Stuxnet contains a mysterious numerical infection marker
- It took over 10 man-years to create Stuxnet
- Stuxnet has a built-in kill date
- No existing programs or standards could have prevented Stuxnet

ATTACK VECTOR – USB STICK, CARELESS HUMAN BEHAVIOR



Technology Supply Chain?

- FIREWALL We have the best control "IN HERE" What happens "OUT THERE" is beyond the CISO control.
- OUTSOURCING Deliver more with less, Improve operational efficiency and tighten that IT Budget
- CLOUD/SaaS A porous perimeter, a virtual firewall and anything is "On Demand"

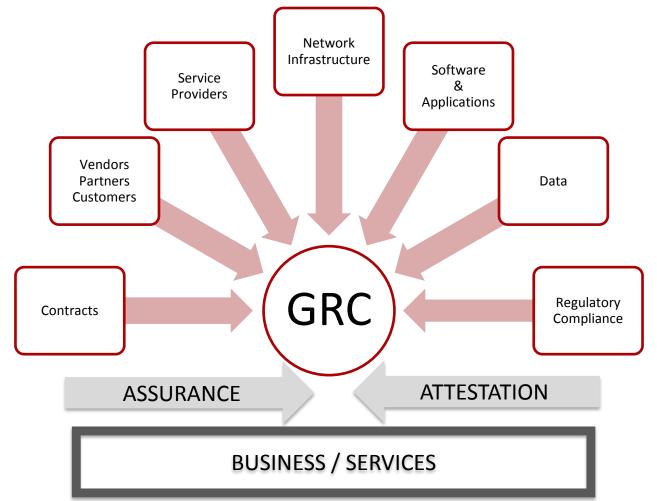






Securing the Enterprise from a Dangerous Cyberworld

Supply Chain Protection Framework





THE SECURITY STANDARD^{**}

Securing the Enterprise from a Dangerous Cyberworld

Framework Implementation – Example Data Loss Prevention

End Point	Network	Servers	Database & Applications	Storage	Legal & Contracts
 Encryption AV & Malware HIDS Patching Logging Peripheral device control IDAM 	 DMZ Virtual Perimeter NextGen Firewall DPI NAC NIDS IDAM 	 Server Build OS Hardening Patching & Pen test Physical Access IDAM 	 Sensitive Data Protection Monitoring Interfaces IDAM SSL Cross site scripting Session controls 	 Data at Rest Data in motion Back up DR Export Control 	 Ownership Beach Insurance IP Liabilities Outsourcing

GRC - Dashboard

ASSURANCE & ATTESTATION





Securing the Enterprise from a Dangerous Cyberworld

Review

- Understand your Business first
- Develop a Business IT/IS process map
- Catalog Risk on High Value Components
- Develop & Identify Availability plans
- Ensure contracts have the right verbiage
- Keep up with Compliance requirements
- Breach is inevitable, but know where it can happen to diffuse the opportunity for occurrence & protect your Technology Supply chain







Securing the Enterprise from a Dangerous Cyberworld

Thank You!

Vijay Viswanathan Director & CISO HD Supply





Securing the Enterprise from a Dangerous Cyberworld