RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace

SESSION ID: CCT-W09

Protecting the Energy Industrial Infrastructures from Advancing Threats

Wayne L. Loveless III

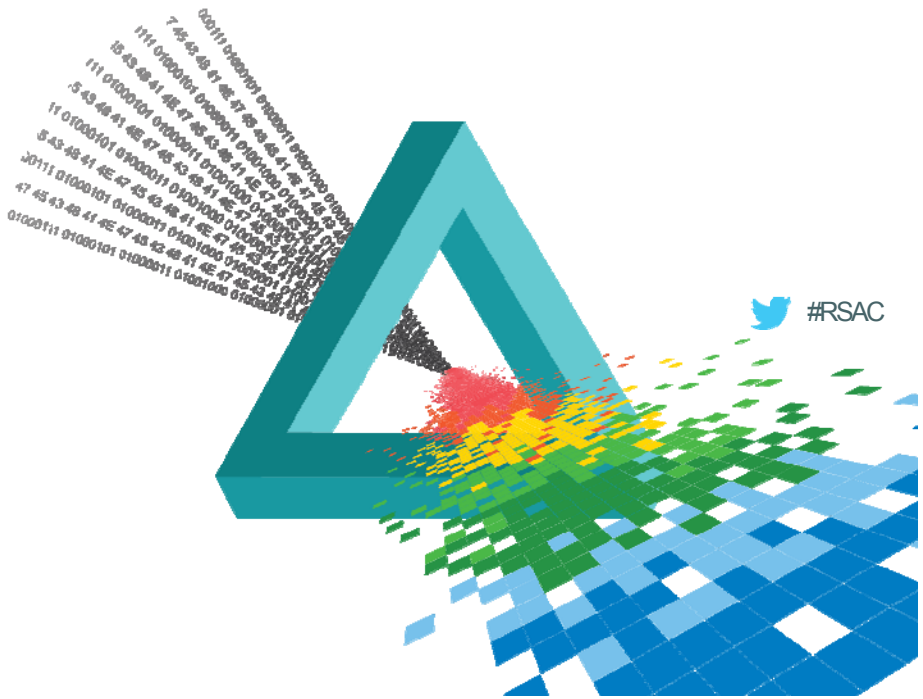
Senior Associate
Booz Allen Hamilton
@Loveless1976

#RSAC

RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace

Framing the problem



What is the most important resource in the Middle East?

Hint, its not oil…..

Booz | Allen | Hamilton

Hydrocarbons may be king, but water and electricity play a far bigger role in the Middle East

#RSAC

Water Production and Distribution

- Clean, potable water is the most vital resource to any stable society
- Water in the Middle East is in very short supply
- Industrial and agricultural production are both highly dependent on dependable water supplies

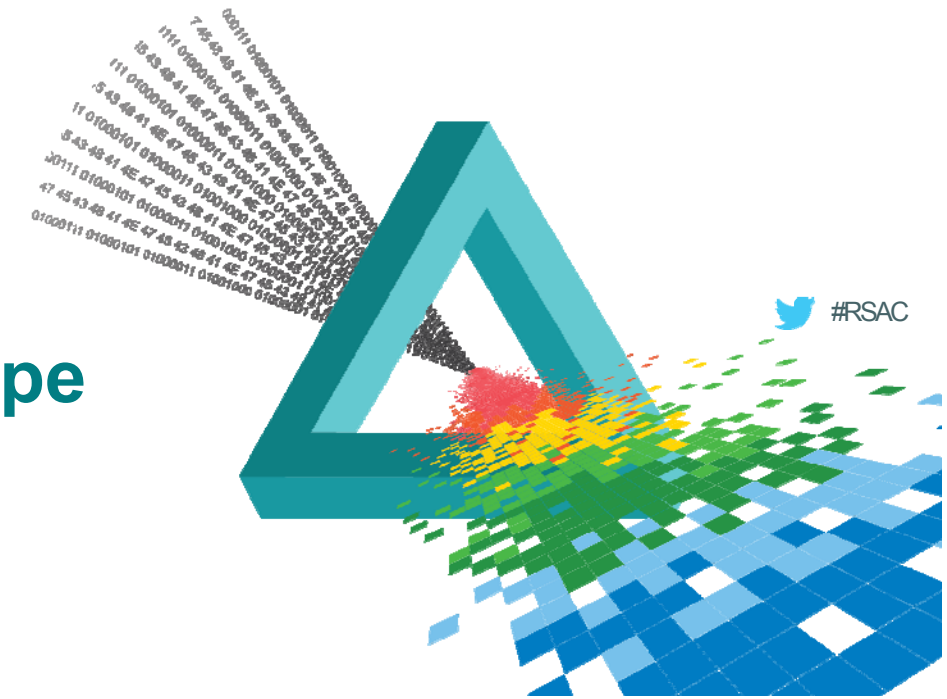
Electric Production and Distribution

- Hydrocarbon production and refinement require vast amounts of reliable electric power
- Climate control and air conditioning make the region more hospitable and enable the tourism and retail industries
- Key to water desalination

RSAConference2015

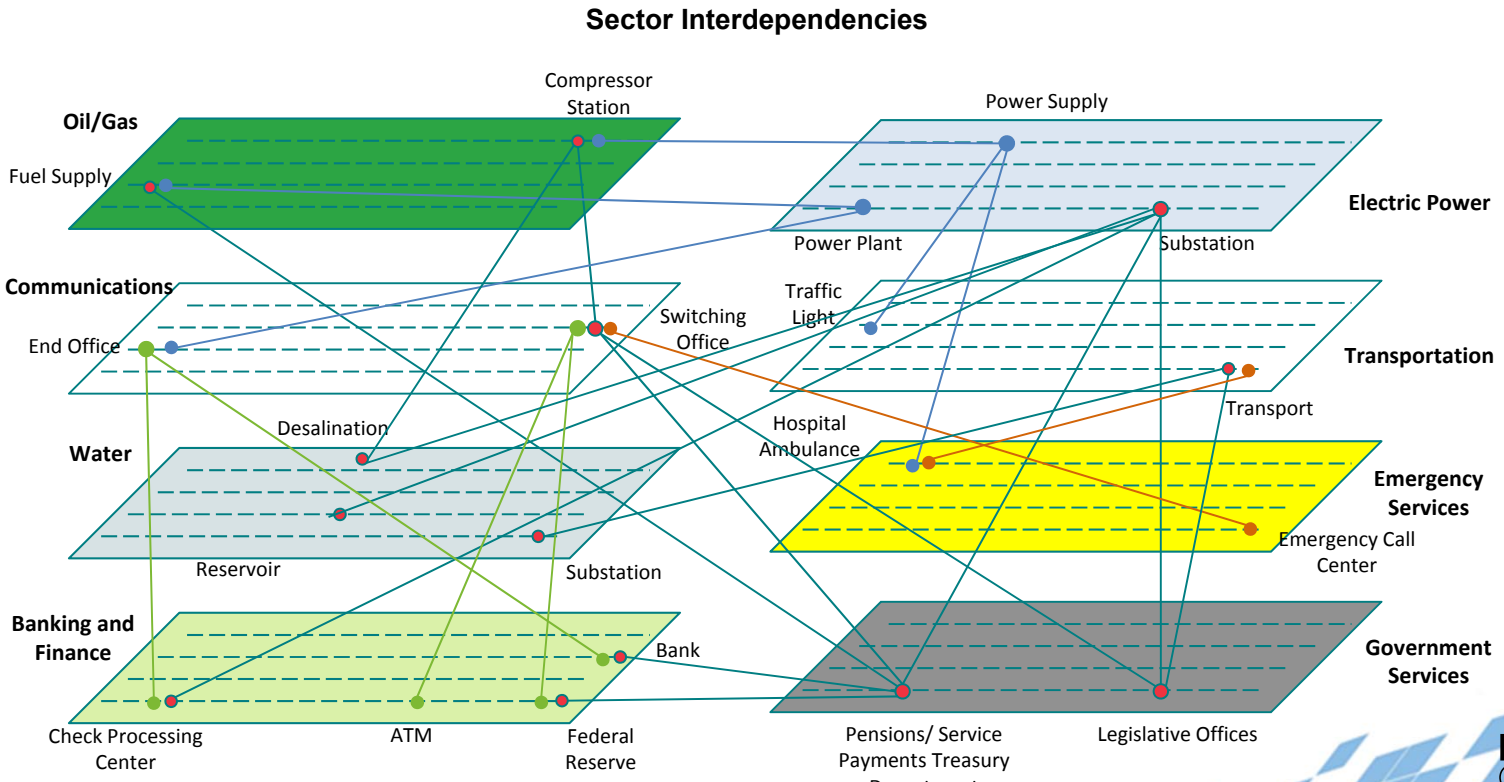
Abu Dhabi | 4–5 November | Emirates Palace

Evolving Threat Landscape



The impact of a major attack on any critical sector in the region would be devastating

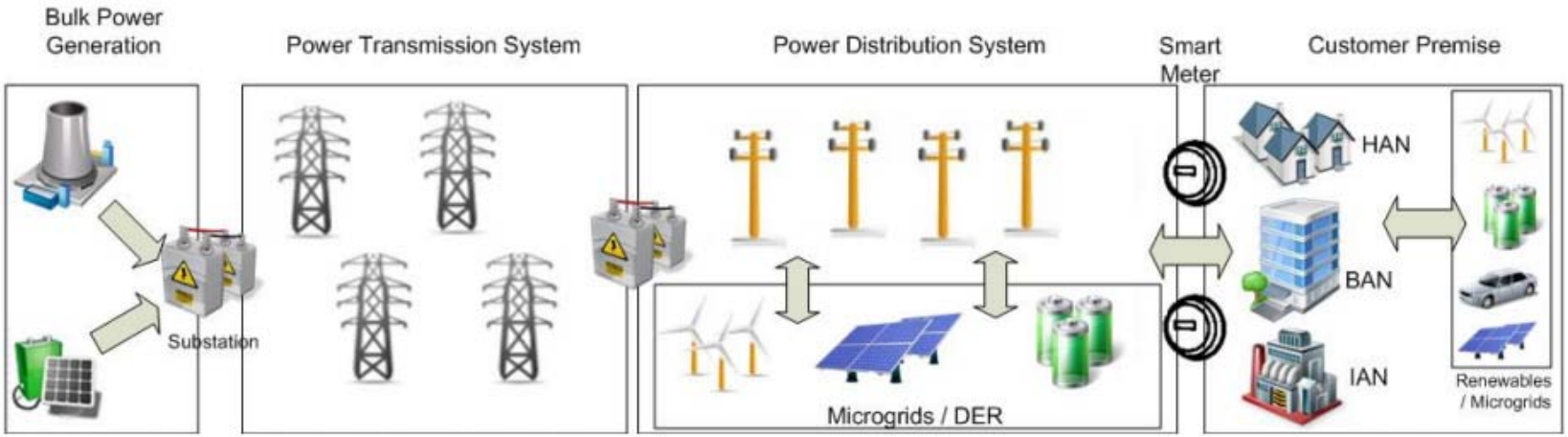
#RSAC



Booz | Allen | Hamilton

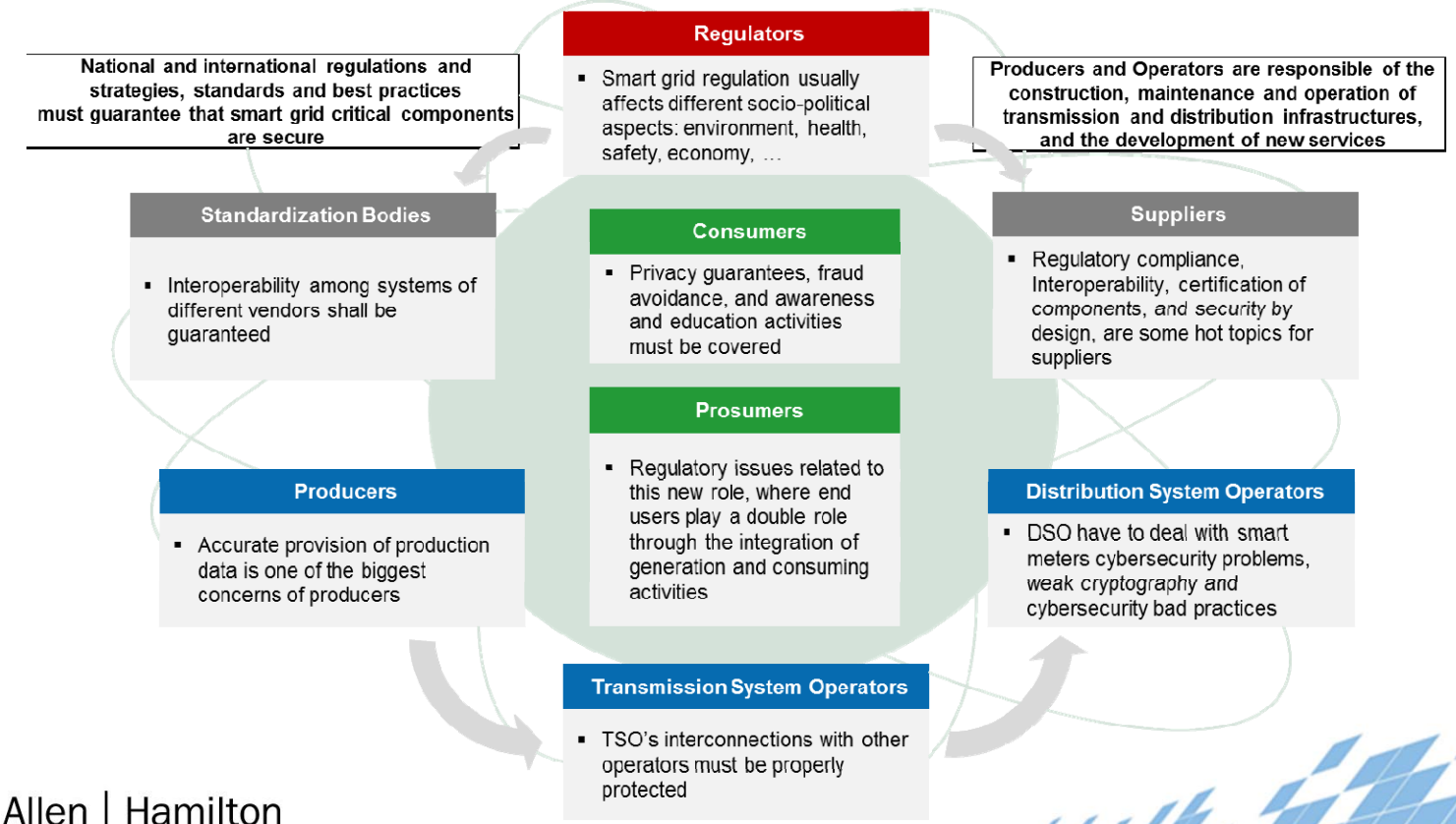
RSA Conference 2015 Abu Dhabi

Smart Grids and Distribution bring new security challenges and obstacles that must be addressed…



- Privacy Implications
- Point to point cyber security
- Security by design
- Unforeseen and new risks
- Resiliency
- Technical weaknesses
- Awareness
- Data protection
- Lack of knowledge
- Lagging regulatory environment
- Standardization issues
- Not prioritizing cyber security

And are creating even more complex, integrated environments, shifting the cyber security view



The emerging threats to the vital water sector are clearly focused on SCADA systems

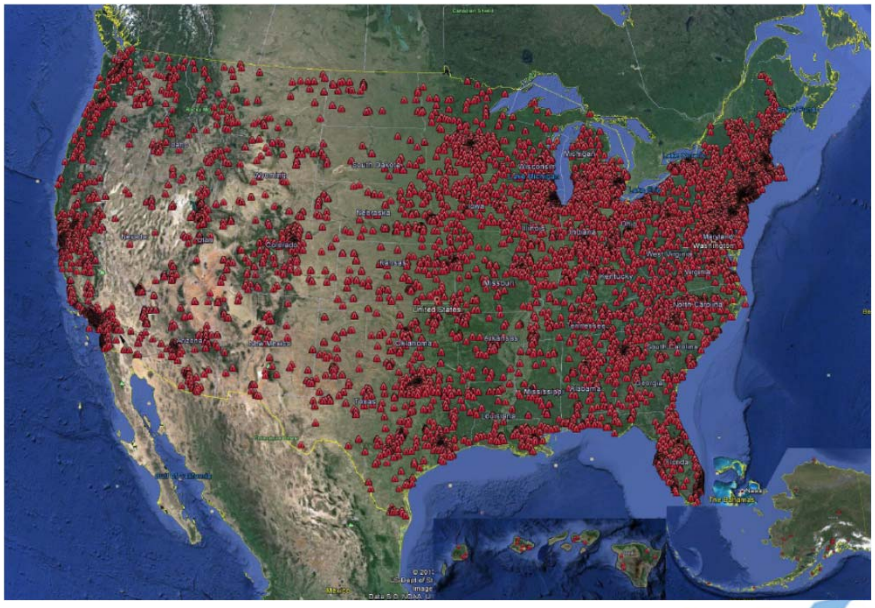
#RSAC

Water utility "honeypot" SCADA systems assessed:

- Who/what is attacking devices and why
- If the attack performed on these systems was targeted and for what purpose it was targeted

- Within 28 days, 39 attacks from 14 different countries occurred
  - 12 attacks were unique and classified as "targeted"
  - 13 attacks were "automated"

SHODAN
Computer Search Engine



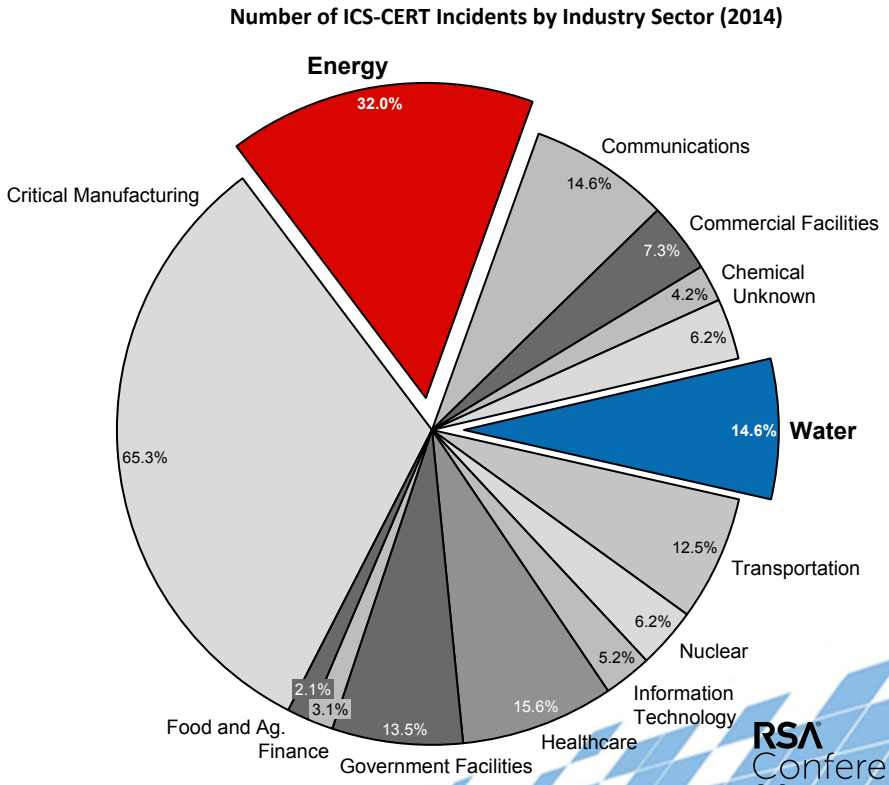
U.S. Map of Internet Connected ICS/SCADA Systems

Booz | Allen | Hamilton

The Energy and Water sectors have been a major cyber target

#RSAC

Examples of Recent IACS Cyber Attacks	
German Steel Plant (2014)	Control components and entire production machines impacted preventing the shut down of a blast furnace, resulting in significant damage *Source: SecurityWeek*
Operation Cleaver (2014)	Focused surveillance and infiltration campaign against numerous infrastructure targets in multiple countries, including Qatar and the UAE *Source: Cylance*
Energetic Bear (2014)	Persistent, widespread campaign against 1,000+ global energy companies over multiple years *Source: Powertechnology.com*
Shamoon (2012)	30,000+ workstations disrupted in August 2012 *Source: DarkReading.com*
RasGas Attack(2012)	In 2012, RasGas was hit with a virus that shutdown its website and email servers *Source: BBC News*



Booz | Allen | Hamilton

RSA Conference 2015 Abu Dhabi

Recent events have shown how susceptible these resources are to disruption

#RSAC

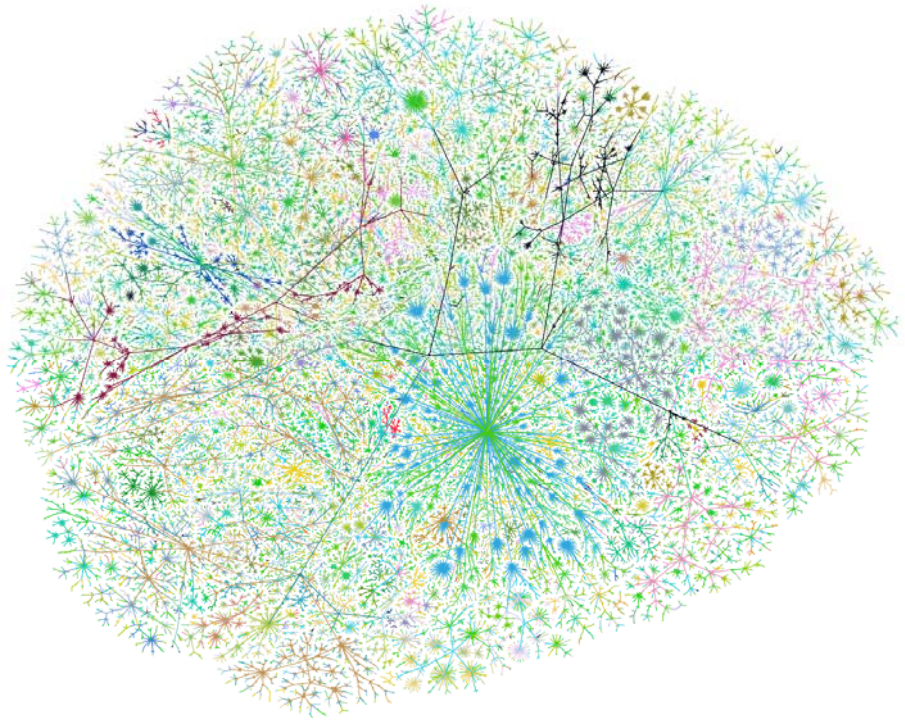
- March 2015 – Large scale blackouts in Turkey (possible cyber attack) where the distribution systems were impacted
- June 2014 – Yemen physical attack left the entire nation without power
- September 2011 – US water utility was attacked via SCADA supplier vulnerability, destroying a pumping station

Booz | Allen | Hamilton

RSA Conference 2015 Abu Dhabi

IoT and the convergence of traditional IT and ICS is expanding the attack surface

#RSAC

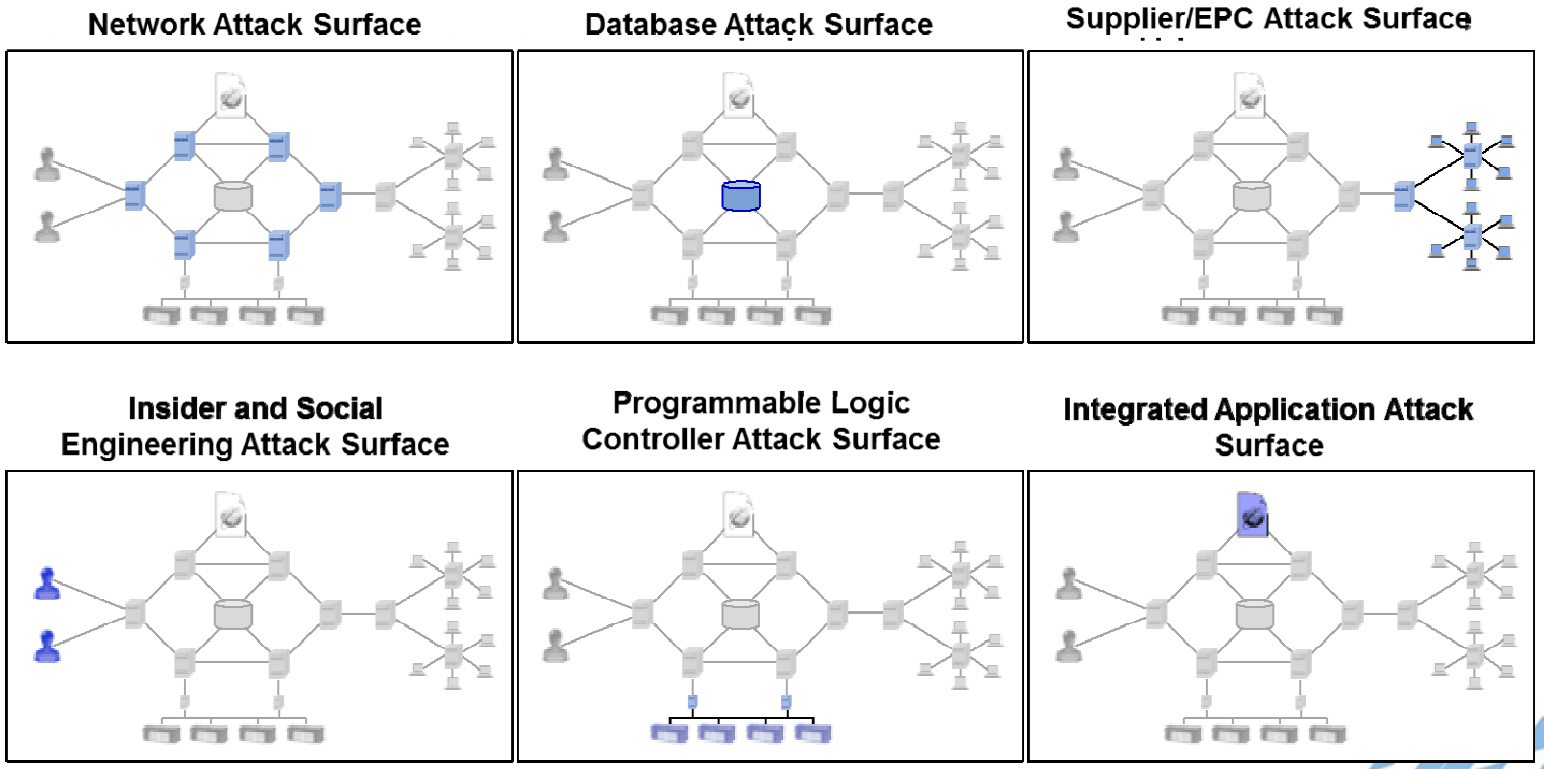


- Smart devices, smart metering, web enabled SCADA…web enabled toaster ovens, cars, wearables…
- IoT is pushing the boundary of traditional cyber security from beyond the firewall and expanding the attack surface

Booz | Allen | Hamilton

Adversaries have expanded attack opportunities by exploiting IT/OT integrated attack surfaces

#RSAC

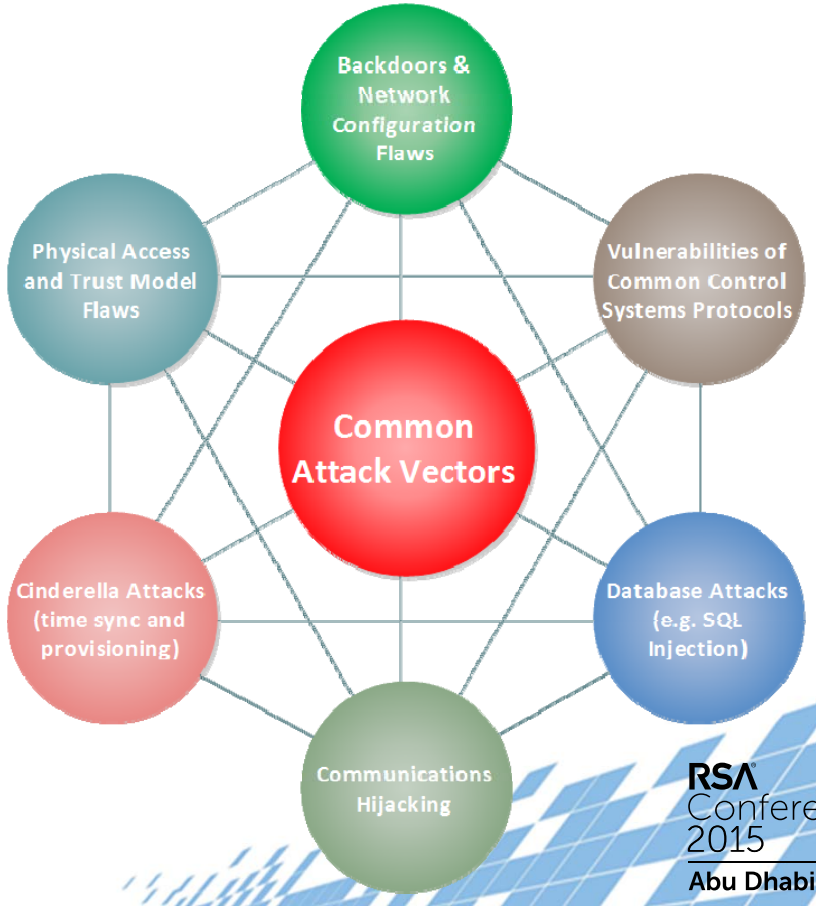


Booz | Allen | Hamilton

Control systems are vulnerable to a variety of unique but also shared attack vectors with IT

#RSAC

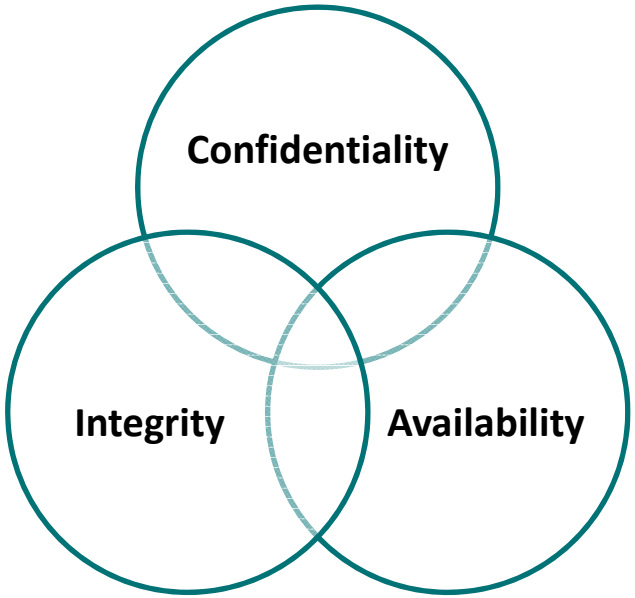
- Database attacks, communications hijacking, and, network configuration flaws are among some attack vectors that impact both IT and OT systems
- Protocols of control systems and trust models provide for some unique and more difficult security issues in controls systems



Prioritization of confidentiality over availability has put control systems at greater risk over time

#RSAC

- Traditional IT Security is focused primarily on confidentiality of data
- SCADA and Industrial Systems are all about availability first
- Another primary security property not in the CIA model is Timeliness
- Most ICS security solutions focused on Denial of Service

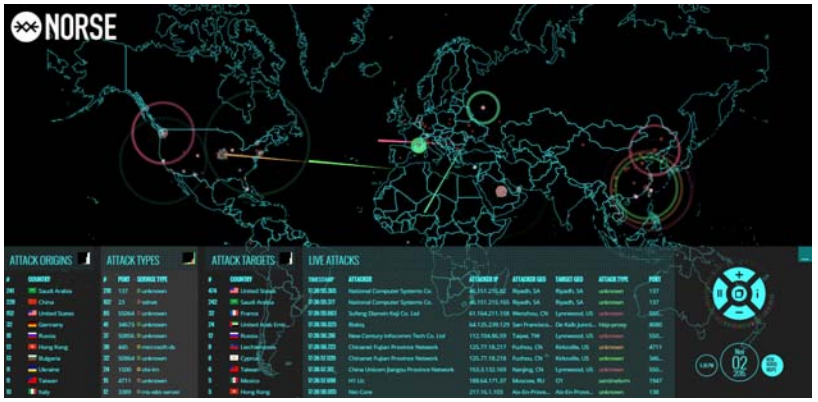


CIA Cyber Security Triad

The Who of Industrial Controls Systems (ICS) attacks is just as important as How

#RSAC

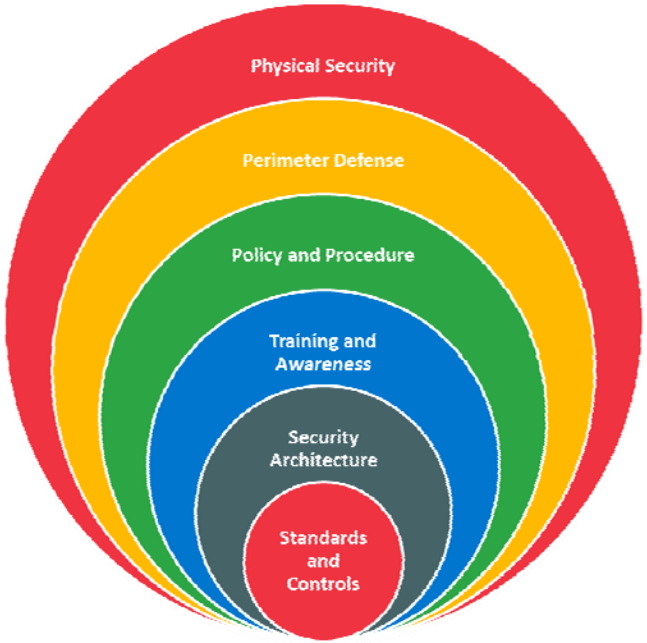
- Beyond just DOS/DDOS and industrial espionage
- Advanced threat actors gathering data, finding weaknesses to exploit, and waiting
- Prepositioning cyber “weapons”
- Entering a new age of Cyber



Source: Norse, http://map.norsecorp.com/

Defense in Depth is important, but it is impossible to prevent ALL attacks…..

#RSAC



- Decreasing effort (Malware as a service, botnets, etc.)
- Greater level of success
- Number of adversaries ever increasing
- Sophistication of adversaries is growing
- Understanding advanced threats is becoming more difficult

Arthur C. Clarke – "Any sufficiently advanced technology is indistinguishable from magic"

Defense in Depth thinking has created an imbalance between prevention versus mitigation

#RSAC

Prevention

- Must prevent all attacks all the time
- Requires significant and ongoing investment in tools, training, and people
- Must account for every change, ongoing updates

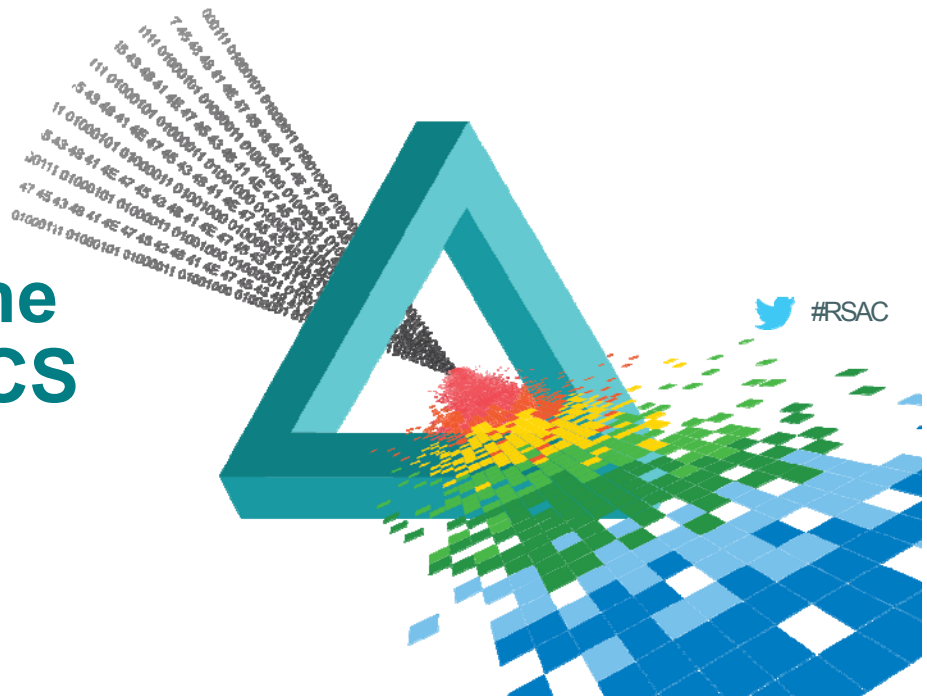
Mitigation

- Focus is on limiting impact of vulnerabilities
- Targeted and methodical focus on design and architecture
- Creates a culture where risk and security become part of the culture

RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace

How are we addressing the convergence of IoT and ICS in Cyber?



It starts by increasing visibility, inside and outside – its all about the data

#RSAC

Threat Intelligence

Data and Analytics

Advanced, Integrated Security Operations Center

Booz | Allen | Hamilton

Harnessing the 3C's – Collaboration, Coordination, Commitment

- **Collaboration** – encouraging information sharing within sectors and across industry verticals
- **Coordination** – All of us is stronger than one of us. Coordination among producers, distribution, regulators, government agencies and industry experts
- **Commitment** – Dedicated, motivated, and knowledgeable resources, along with senior leadership support are key

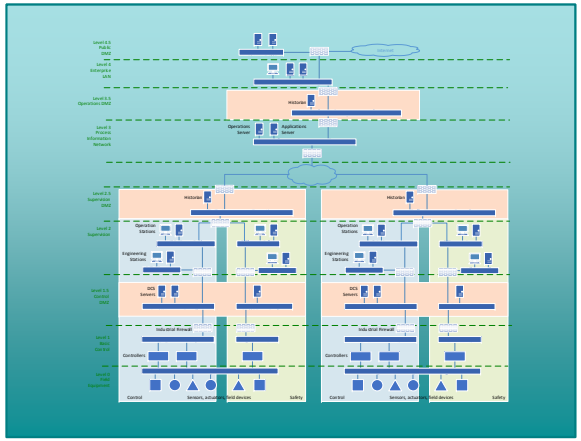
Injecting security into the design, development, deployment and operations of controls systems

#RSAC

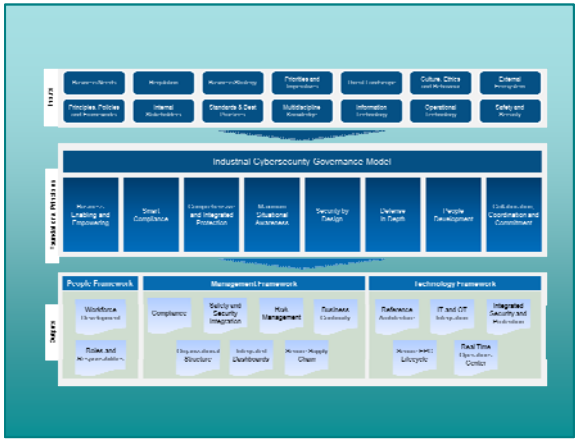
Employ the Industrial Cybersecurity Principles

Assess

Design



Enhance



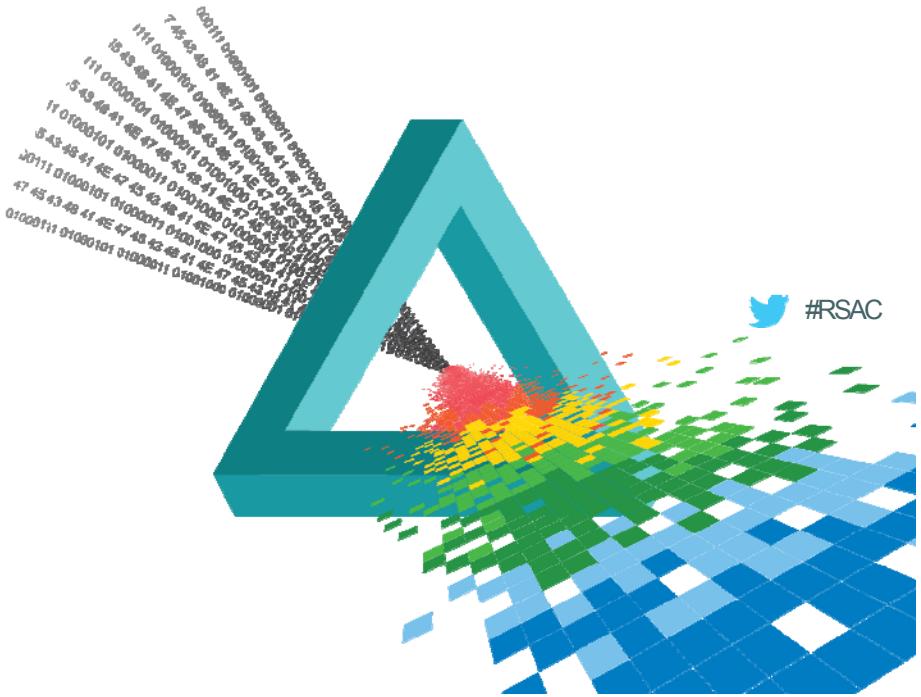
Booz | Allen | Hamilton

RSA Conference 2015 Abu Dhabi

RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace

Applying what we have learned today



If we were to embark on a mission to protect your critical infrastructure, where would start?

#RSAC

Key questions to address

- There is so much to take in, where do we even start?
- What can I do now?
- What do I need to do going forward?

Apply new thinking now….

- Shift your cyber thinking away from the “how much” to the “how” and “who.” It’s not how much you spend on compliance and technology, but rather the knowledge and experience needed to shift to a proactive rather than reactive defense
- Make Cyber a priority. Just like HSE, Cyber should have a core emphasis as part of your organization’s operations
- Move beyond thinking about just Malware and prevention

And during the coming weeks….

- Seek out industry expertise to provide an external view and assessment of your organization's current exposure and risk
- Get a handle on your environment – not just in the plant, but the distribution systems, remote sites, and supplier connections
- Build a network of like minded individuals and organizations, and start sharing information through formal channels (e.g. http://www.ics-isac.org/)

And then build on that new thinking….

- Implement a cyber security transformation program that moves beyond standards and that establishes a culture of security
- Gain visibility by considering an integrated Security Operations Center (SOC) and subscribing to a focused threat intelligence service from industry or government

Conclusion

- Change and evolution are coming to the world of industrial security, putting more of our critical infrastructure at risk
- The time is now to get in front of this growing problem