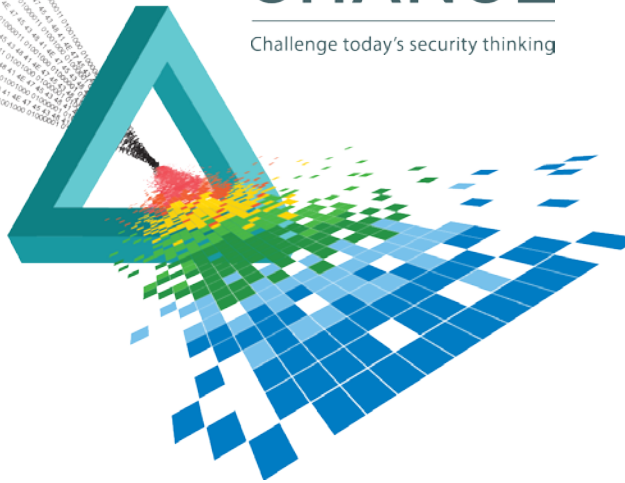
RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace

CHANGE

Challenge today's security thinking

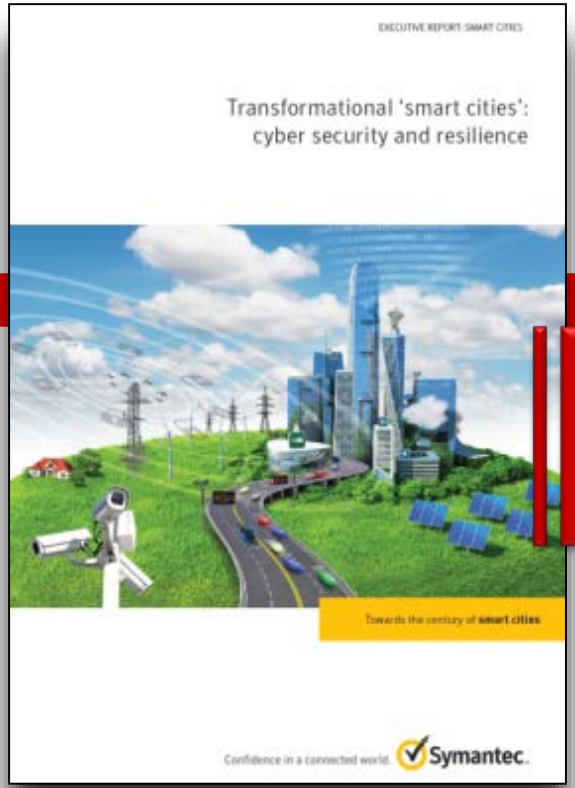


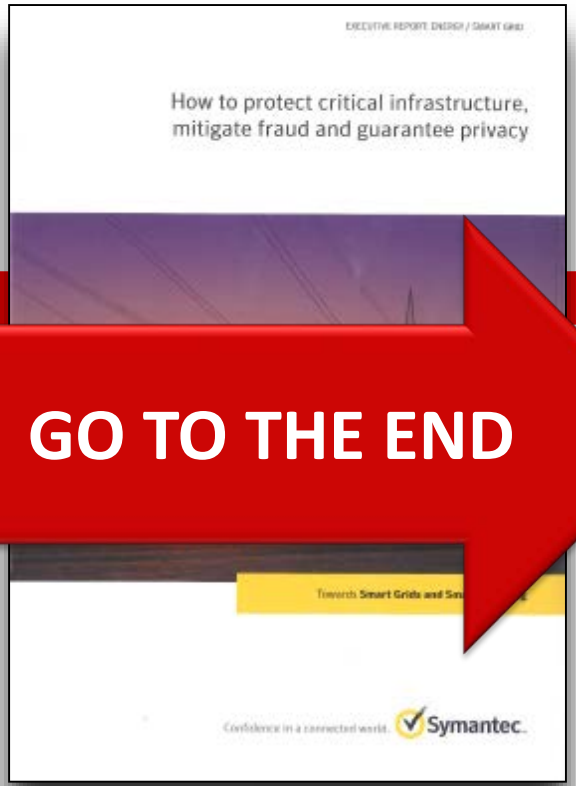
SESSION ID: PST-W07

Security Posture for Critical Information Infrastructure Protection (CIIP)

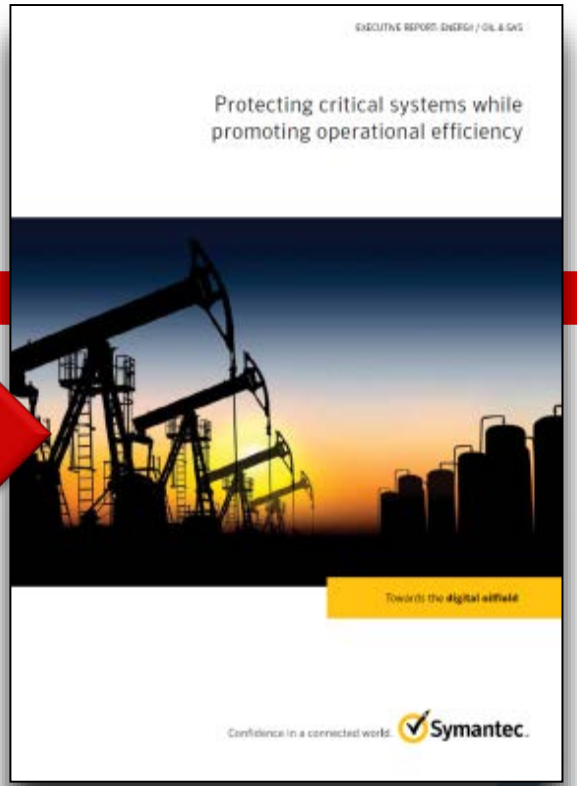
Giampiero Nanni

Government Affairs EMEA
Symantec
@Giampieronanni


Transformational 'smart cities':
cyber security and resilience
Towards the century of smart cities
Confidence in a connected world.
Symantec.


How to protect critical infrastructure,
mitigate fraud and guarantee privacy
Confidence in a connected world.
Symantec.

GO TO THE END


Protecting critical systems while
promoting operational efficiency
Towards the digital oilfield
Confidence in a connected world.
Symantec.

Imagine… you have to tell the Board of Directors, that your organization has been compromised by an attack…

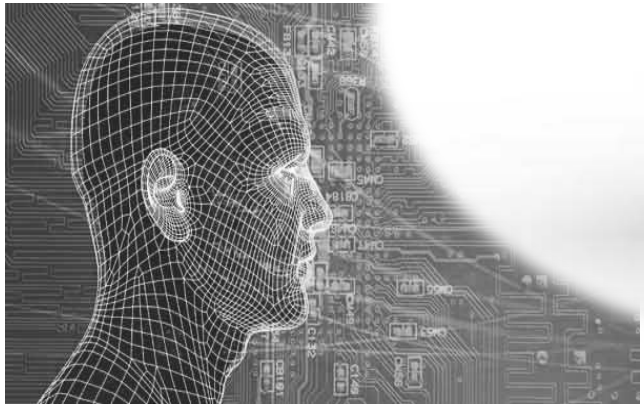
*It took the attackers only **six minutes** to circumvent the perimeter defenses. From there, they achieved domain administrator privileges in **less than 12 hours**.In less than a week they **fully compromised** all 30 of our global domains.*

*They harvested **all our credentials**, giving them the ability to log in to the network **masquerading as any of us**. There was **no place** on our global network they could not go and only a handful of computers they did not have **easy access to**.*

*The attackers were in a position to electronically **transfer millions of dollars** out of our bank accounts through our accounts payable system.*

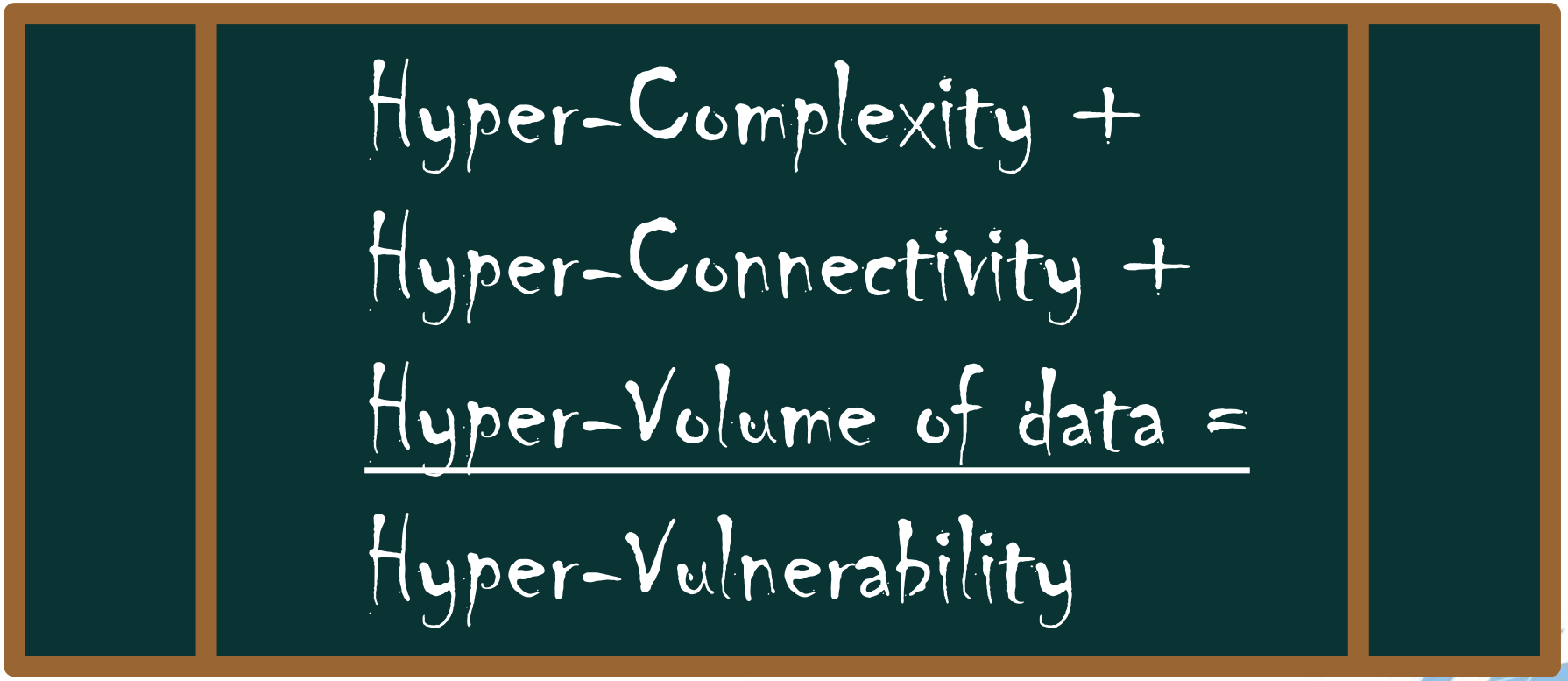
Operational Tech. vs. Information Tech.

OT: The application of technologi
changes in plant operations a
highly customized by industr
of products and services
an enterprise.



uting technology and
retrieve, transmit and
ns are relatively consistent
pport corporate functions through
human interface.

Critical Information Infrastructure: It all adds-up (1)



Critical Information Infrastructure: It all adds-up (2)

Chatham House: Cybersecurity at civil nuclear facilities – C. Bylon et al

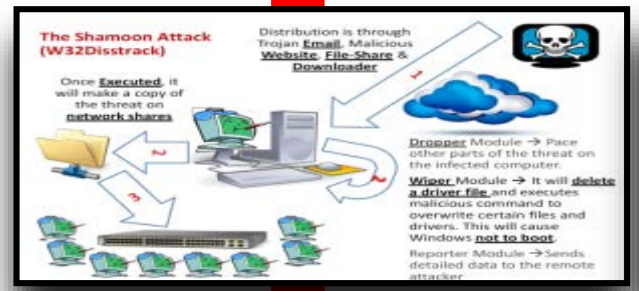
RSAConference2015

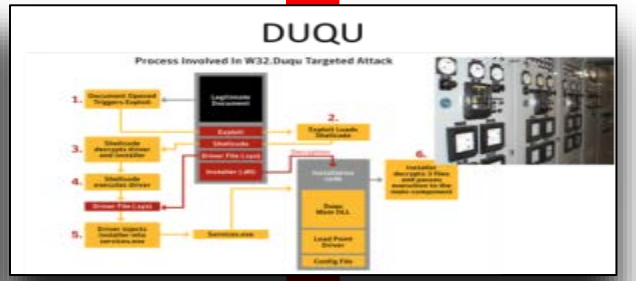
Abu Dhabi | 4–5 November | Emirates Palace

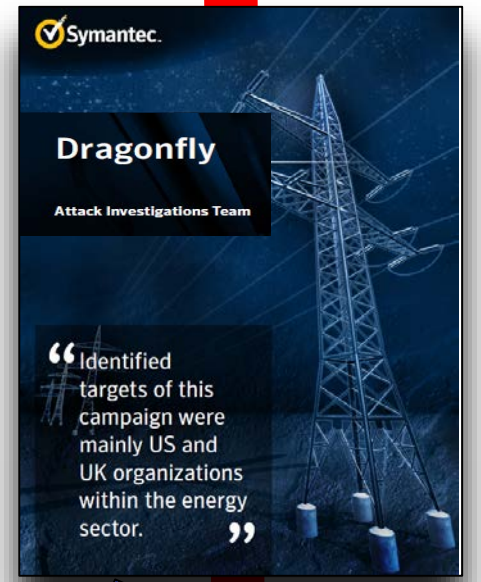
1. Cyber-attacks to Critical Information Infrastructure DO happen

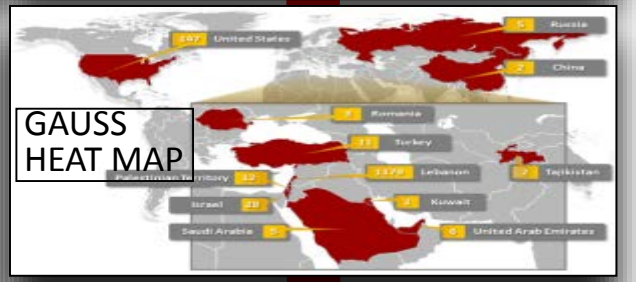
#RSAC

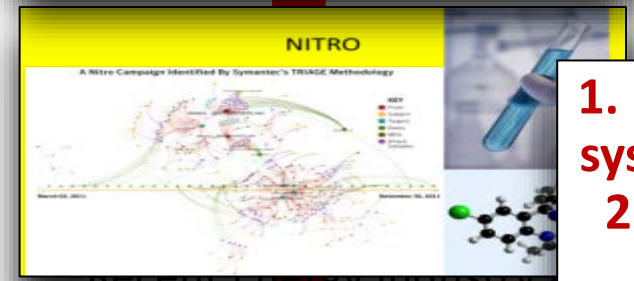
High-profile CII Attacks

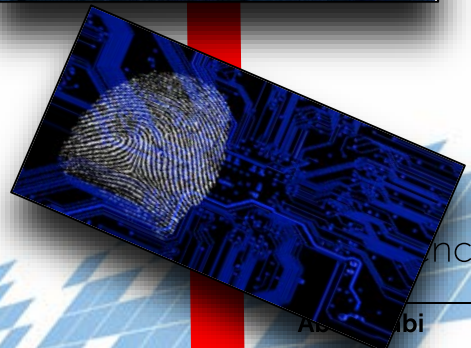












1. Even isolated industrial control systems (ICS) are vulnerable AND
2. Cyber-attacks can inflict vast physical damage

Recent Energy Industry

Other high-profile incidents

Country DDOS Estonia

Drugs traffickers using hacked port - Belgium

Water treatment plant disabled - USA

Steel mill hacked, severely damaged - Germany

Explosion hits hacked gas pipeline - Turkey

A noteworthy example: Dragonfly

Energy Companies Under Sabotage Threat

- Ongoing cyberespionage campaign
- Targeting the **energy sector** in USA/Europe
- Hallmarks of **state sponsored** operation
- Priorities appear to be:
  - Persistent access to targets
  - Information stealing
  - Sabotage
- Sophisticated attack techniques and vectors
  - Spam emails with disguised malware as PDF attachment.
  - Watering hole attack
  - Compromising third party software/downloads

A local-focused threat: Trojan.Laziok

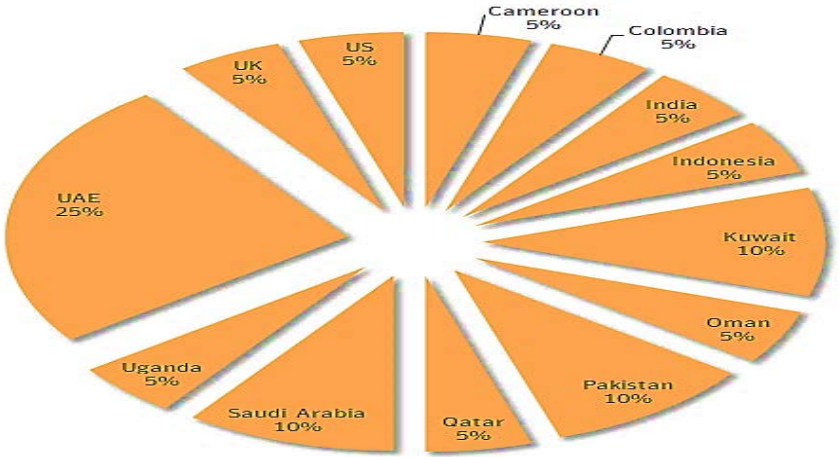
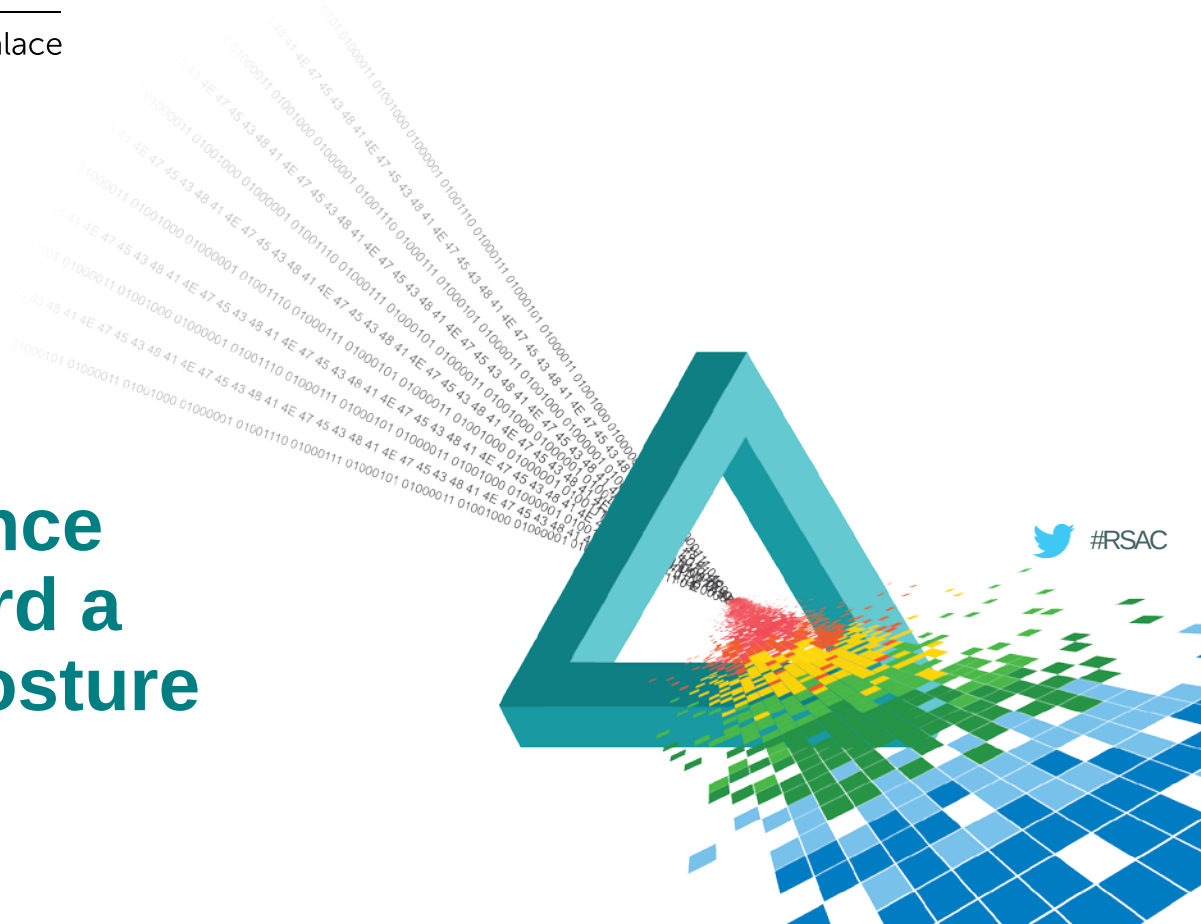


Figure 1. Regions affected by Trojan.Laziok

Symantec.

2. Cyber-Intelligence as first step toward a sound security posture



Global Intelligence Network

"Cyber-attackers are leap-frogging defences in ways organisations lack insight to anticipate"

Worldwide Coverage | Global Scope and Scale | *24x7 Event Logging*

Enterprise Threat Landscape

Attackers Moving Faster

5 of 6 large companies attacked

317M new malware created

1M new threats daily

60% of attacks targeted SMEs

Digital extortion on the rise

113% increase in ransomware

45X more devices held hostage

Zero-Day Threats

24 all-time high

Top 5 unpatched for **295 days**

Malware gets smarter

28% of malware was Virtual Machine Aware

Symantec.

RSA Conference 2015 Abu Dhabi

3. Actors, motivations, objectives

Actors, motivations, objectives (not exhaustive)

<table>
<tr><th>Attackers</th><th>Underlying Motivations</th><th>Industrial Espionage</th><th>Intelligence (Data Exfiltration)</th><th>Financial</th><th>Sabotage (ICT)</th><th>Sabotage (Physical infrastructure)</th></tr>
<tr><td>Solitary hackers</td><td>Personal credit with hacker community</td><td></td><td>Expose sensitive or embarrassing information</td><td rowspan="2">Money theft from oper-ators</td><td colspan="2">Newsworthy action</td></tr>
<tr><td>Criminals (organised crime or individual)</td><td>Financial gain</td><td colspan="2">Commerce of sensitive information</td><td>Ransom</td><td></td></tr>
<tr><td>State Military</td><td>Undeclared conflicts Various stages</td><td rowspan="2">Support national industry</td><td>Military Espionage</td><td></td><td rowspan="2">Neutralise enemy's ICT - Inflict damage to enemy State</td><td rowspan="3">Inflict physical damage to enemy State or organisation</td></tr>
<tr><td>State-sponsored groups</td><td>Paid support of State activity</td><td>Espionage in various domains</td><td></td></tr>
<tr><td>Terrorism</td><td>Political, Religious</td><td></td><td>Acquire info for attacks</td><td rowspan="2">Group Funding</td></tr>
<tr><td>Hactivists</td><td>Political campaigns on specific themes</td><td colspan="2">Expose sensitive or embarrassing information</td><td>Damage to State ICT & reputation</td></tr>
</table>

4. Policy and regulatory aspects

Network and Information Security (NIS) Directive

- EU Governments need to build national cyber-security capabilities
  - Create/Equip national CERTs (Computer Emergency Readiness Team)
  - National Cybersecurity Strategies
  - Responsible Authorities
  - Exchange information
- Operators of Critical infrastructure
  - Need to develop a risk management approach
  - Are subject to audit and supervision by national authorities
  - Need to report security incidents
  - Need to share information
- Current Status
  - Discussion at Parliament and Council – Active usually 18 months after adoption

NIST framework to improve CII security

"The national and economic security of the United States depends on the reliable functioning of critical infrastructure. A voluntary framework for reducing cyber risks to critical infrastructure. Cybersecurity threats exploit the increased complexity and connectivity of critical infrastructure systems, placing the Nation's security, economy, and public safety and health at risk".

Based on the EO and outcome-based, the Framework provides guidelines on:

- Standards, methodologies, procedures, and processes
- Align policy, business, and technological approaches
- Governance of cybersecurity risk
- Incorporate international voluntary consensus standards and industry best practices to the fullest extent possible
- Provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach
- Information security measures and controls
- Identify, assess, and manage cyber risk for CI

NIST

Symantec.

Cybersecurity Roles

Government:

- Develop, implement, enforce cybersecurity policies and strategies with industry and civil society input
- Encourage adoption of industry-led consensus standards and best practices
- Promote market-driven technology innovation
- Raise awareness and education
- Serve as regulator for critical sectors of economy

Industry:

- Innovate, build and maintain security of technologies and services
- Coordinate on incident response and vulnerability management
- Participate in public-private partnerships
- Raise awareness and education

PPP Fundamentals for Success (W-W-W)

- Cybersecurity is a “shared responsibility” across society
- Aligns industry and government priorities, goals, objectives
- Embraces core aspect of inclusiveness
- Provides the structure, processes, and environment for trusted collaboration and repeatable consultation
- Flexible and adaptable to address the changing risk landscape

- Clear objectives, limits and deliverables – Manageable size
- Identify “critical infrastructure at greatest risk” - where a cybersecurity incident could have catastrophic effects on public health or safety, economic security, or national security

What should each side aim to get?

- Not for profit and not for free riding
- Industry usually aims to get
  - Useful information on threats
  - Recognition as a good corporate citizen
  - Deeper understanding of the organisations participating
  - A community of trust
- Government usually aims to get
  - Better threat awareness
  - A better collective defense capability
  - Raise the bar
  - Participate in a community of trust

PPP considerations

PPPs are not easy but….

- Industry sees value and comes in good faith
- Necessary in the current threat environment
- Public perception critical after recent facts
- Clarity will drive trust, participation and result
- Manageable size matters
- Keep it open and transparent but be selective
- Don’t re-invent the wheel
- Begin with small but focused steps

Norms

UN's Group of Governmental Experts (GGE) agreed in June on a set of norms.

- Three key commitments:
  - Nations should not attack each other's critical infrastructure
  - Nations should not target each other's cyber emergency responders
  - Nations should help investigate cyber attacks launched from their own territory
- Limiting norms:
  - States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs;
  - States should not conduct or knowingly support ICT activity that intentionally damages critical infrastructure;
  - States should take steps to ensure supply chain security, and should seek to prevent the proliferation of malicious ICT and the use of harmful hidden functions;
  - States should not conduct or knowingly support activity to harm the information systems of another state's emergency response teams (CERT/CSIRTS) and should not use their own teams for malicious international activity;
  - States should respect the UN resolutions that are linked to human rights on the internet and to the right to privacy in the digital age.

Information sharing

- Easier said that done
- Private sector recognizes the mutual benefit but is impeded...
  - By public perception
  - Lack of reciprocity
  - Lack of legal clarity
  - Lack of structures
  - Question of trust
- Models of effective partnership
- Effective PPP require clearly defined limited, specific operational goals

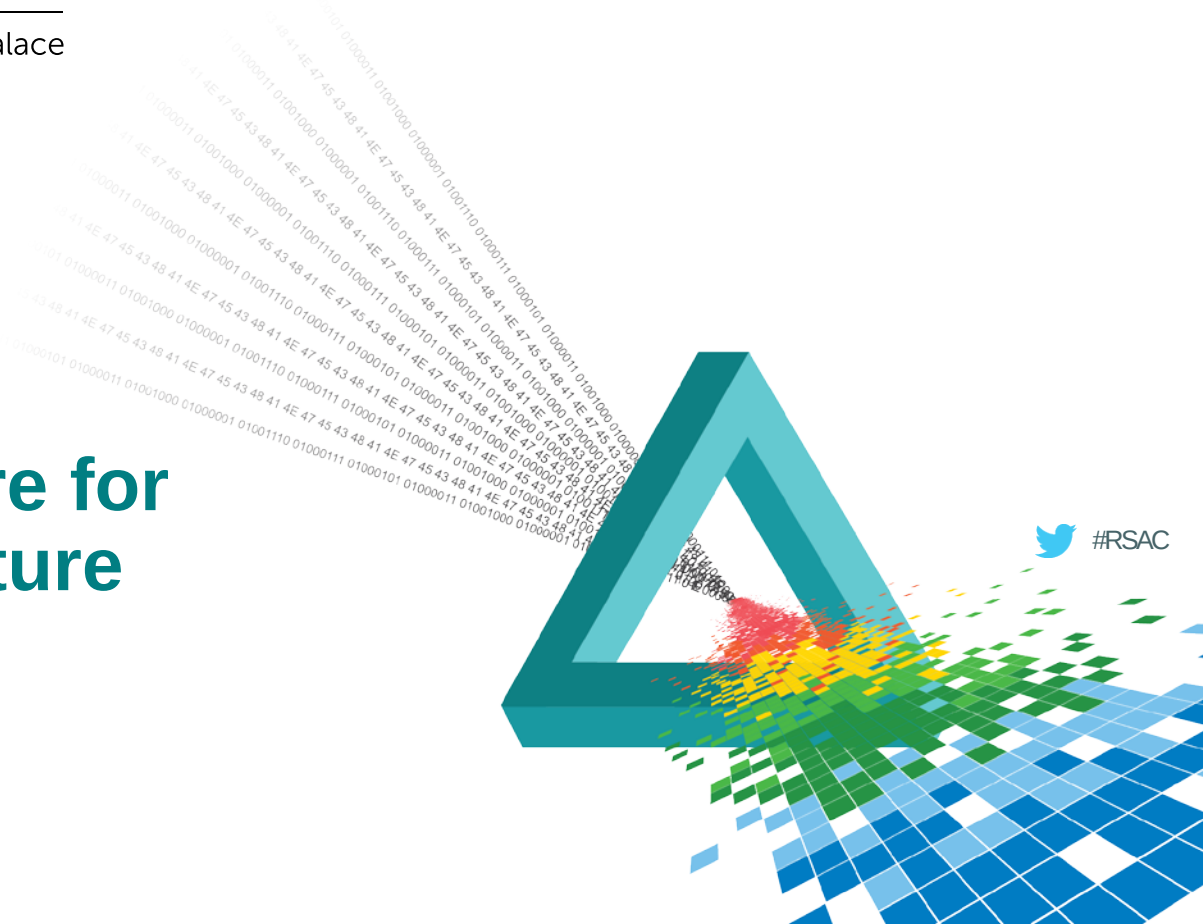
How does Symantec work with governments?

- Other than providing them with capabilities…..
- PPP = Public-Private Partnership
- Historically Symantec has:
  - Participated in PPP and info-sharing groups for cyber threats and policy
  - Provided strategic insight to policy makers (e.g., testimony, white papers)
  - Cooperated in education and awareness raising programs
  - Led capacity building initiatives in Countires
  - Participated on expert committees and working groups
  - Participated in cyber exercises
  - Participated in jointly funded R&D

RSAConference2015

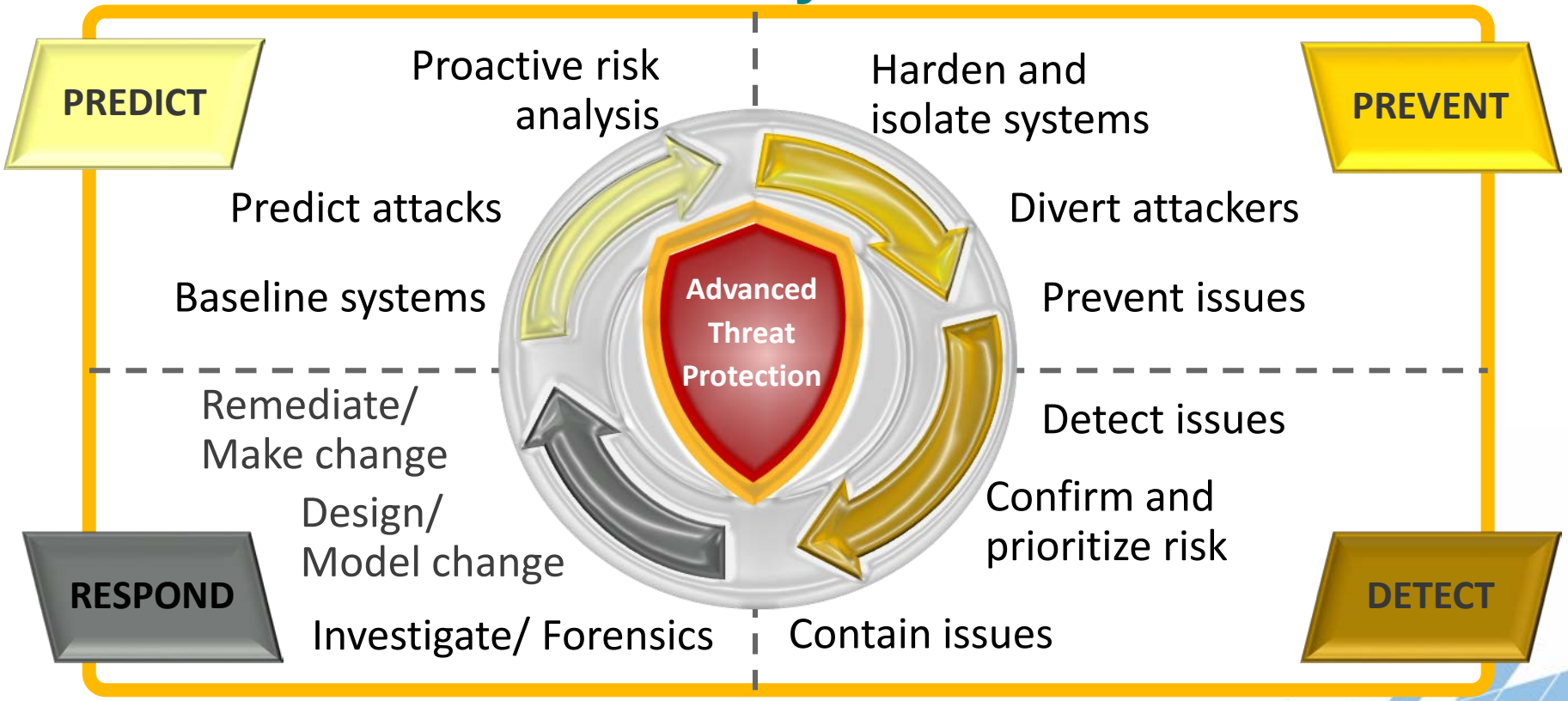
Abu Dhabi | 4–5 November | Emirates Palace

5. Security posture for critical infrastructure ecosystems



#RSAC

Full Threat Protection life cycle



Source: Gartner

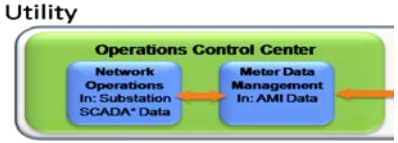
Symantec.

Approach to Industrial Systems – 'Four Pillars'

#RSAC

Not just the device: data flows device to system, network, data center/NOC & Cloud

Operations Security (Network + Endpoint)



- Provide a strong view of events happening in the network and the anomalies
- Control network = compliance + threat perspective
- Anti-malware valuable, but system hardening, code signing are other important technologies which can help strengthen the network

Manage Data Explosion (Data)

Information Infrastructure

- Storage management
- Data protection
- Archiving
- Legal discovery
- Data Loss Prevention

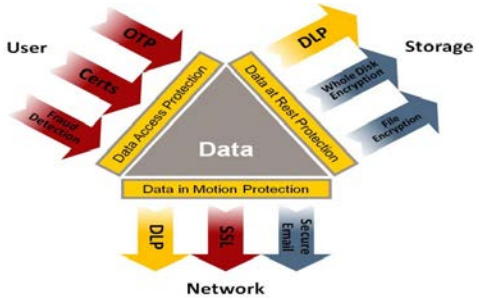
Information Governance

- Compliance
- Control access
- Regulatory & auditing
- Customer Privacy
- Reporting

Manage Devices (Endpoints)

- Manage Windows sub-station automation systems
- Securely update device firmware e.g. AMI collectors
- Securely invoke SSL services through trusted mechanisms resident on device

Embed Security with Data (Channel)



- Encrypt information
- Authenticate devices
- Manage keys
- Manage certificates at scale
- Managed / hosted PKI & device level certificates
- Controlling and securing systems

Symantec.

Recommendations for a secure critical infrastructure (1)

…in order to deliver service continuity and 24x7 availability of the critical infrastructure.

Establish the governance framework

- Fulfil Governance, Risk and Compliance (GRC)
- Deliver Service Continuity
- Identify and protect vital information proactively
- Balancing traditional versus cloud delivery
- Authenticate users (Strong authentication)
- Manage security services
- Developing an information management strategy

Recommendations for a secure critical infrastructure (2)

Fulfilling Governance, Risk and Compliance (GRC)

- Policies and processes, standards and regulations, enabled by ad hoc IT tools
- Ensure that IT departments monitor their environment against the evolving regulation scenarios
- Stay compliant and mitigate risks.

Delivering service continuity

- Adopt solutions and methodologies for security, backup, data loss prevention, archiving and disaster recovery
- Ensure 24x7 availability of the critical infrastructure and resilience in case of an incident through solid backup and recovery software or appliances, policies, processes and tools
- Able to protect and manage heterogeneous environments
- Legacy systems and newer deployments, Open Source, managed mobile devices, virtualised systems, etc.

Recommendations for a secure critical infrastructure (3)

Identify and protect vital information proactively

- Adopt an information-centric approach: embed security within data
- Encryption and white/black-listing
- Strong authentication policies and tools.

Managing security services

- Consider outsourcing security services to providers who can leverage extensive, global expertise in the field of cyber security
- Choose a partner with worldwide visibility of threats and attacks trends, able to address the complete range of security challenges described in this report.
- ICT leadership to focus on the functional duties of running the city
- Rely on national Computer Emergency Response Teams (CERT)

Cyber-security: NOT just a technological problem

- Critical Infrastructure → Country's national security, economic wellbeing and public safety as well as Geopolitical considerations

…and therefore

Cyber-security (and CIIP) are a:

- Political problem.
- Business problem.
- Individual's problem.
- That technology will help solving.

Apply Slide

- Next week you should:
  - Identify the leadership team that should engage in enhancing the security posture of your organisation
- In the next three months:
  - Assess your intelligence capabilities and identify an appropriate source
  - Assess readiness (skills, tools, general porsture people, processes, compliance) and adapt accordingly, including training staff and building posture
- Within six months
  - Put in place a CERT
  - Keep assessing readiness against evolving threats

Thank you!

Giampiero Nanni

Government Affairs EMEA – Symantec

giampiero_nanni@symantec.com

+44 7808248100

@Giampieronanni