CHEMISTRY THAT MATTERS™

SABIC UK PETROCHEMICALS & TEKGEM

IDENTIFYING & MANAGING ONGOING CYBER SECURITY THREATS

NEPIC Industry Insights Session: Cyber Security for Industrial Automation & Control Systems
Wilton Centre: Thursday 22nd March 2018

IACS CASE STUDY

Tony Porritt

Manager, Applications & Infrastructure

SABIC UK Petrochemicals

Ian Gemski

Managing Director

Tekgem (UK) Limited

IACS: MANAGING CHANGE

The chemical processing industries have become increasing reliant on, and pushed towards technology innovation.

- Increased productivity through control, automation & optimisation
- However, move to open networking standards & OS pose risks & challenges
- Accidental – Unintentional, Human Error
- Malicious – Targeted, Destructive

Ultimately, if our industry is to sustain success we must find ways to implement and integrate the new IACS Operational Guidelines for Cyber Security.

SABIC'S IACS STORY

Global IACS Cyber Security Framework released in 2012

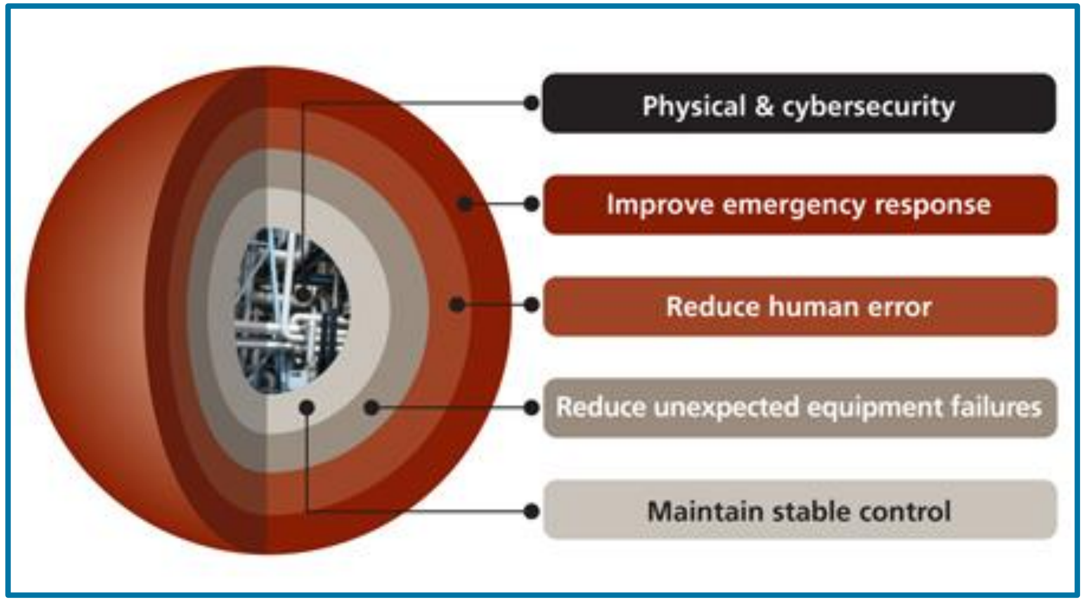
SABIC Manufacturing Systems Maturity Models

- Set of 8 Standards that all SABIC Affiliates must meet minimum requirements
- Contains Best Practices, Example Architectures, Implementation Guides & Assessments
- Provide a "Defence in Depth" Approach
- Measures level of risk to ensure safe and secure operation of facilities
- Have proved invaluable dealing with major Cyber Security incidents…

DEFENSE IN DEPTH

RISK ASSESSMENT

- ANTIVIRUS
- BACKUP & RESTORE
- ELECTRONIC IDENTITY
- FIREWALL
- REMOTE ACCESS
- REMOVEABLE MEDIA
- SECURITY UPDATES
- SYSTEM ADMINISTRATION
- CHANGE CONTROL

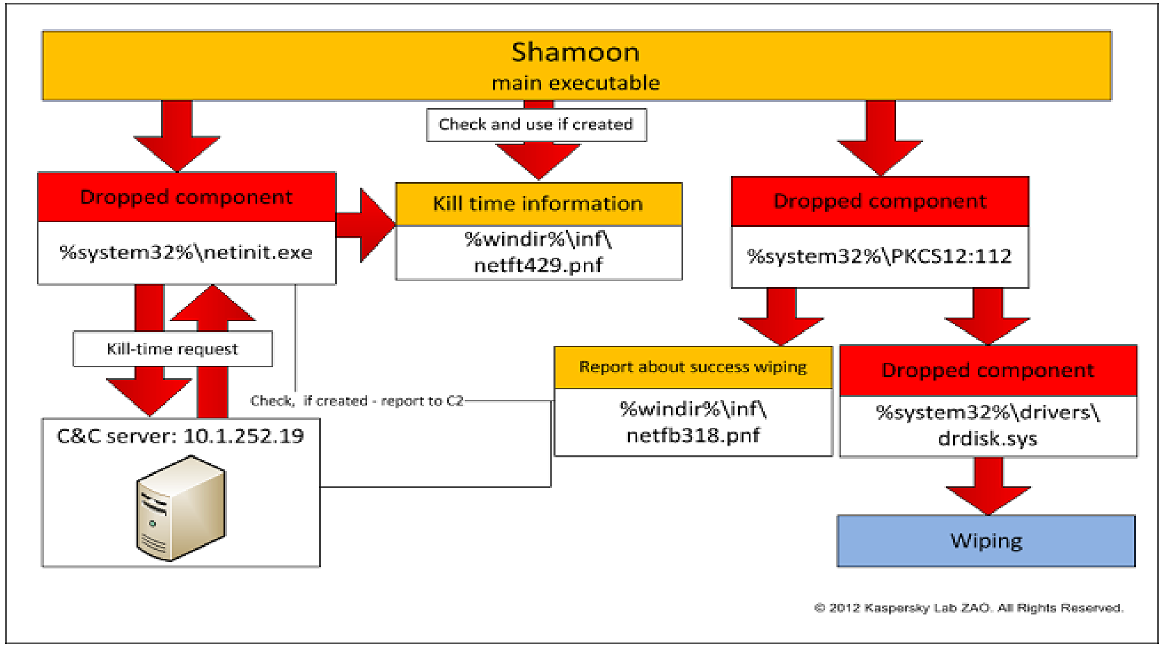


Tekgem
Systems and Technology

EXAMPLE: MALICIOUS ATTACK – PULL THE PLUG

Saudi Aramco falls victim to the biggest ever hack in history with a targeted attack which took over 35,000 systems down. Shamoon.

Reliable intel warns of imminent targeted cyber attack. C-Level instruction received to disconnect ALL control systems from the corporate network immediately.



© 2012 Kaspersky Lab ZAO. All Rights Reserved.

> *“Never underestimate how dependant you are on your information technology and systems. It’s become like oxygen. You think you can live without it but you can’t.”*
> ***Khalid A. Al-Falih – CEO Saudi Aramco***

CYBER SECURITY MATURITY MINIMIZES DISRUPTION

- Incident Response plans in place (with backup paper copies)
- Network diagrams in place summarising data flows between key business and manufacturing systems
- Impact assessments in place with summary of business impact upon loss of network
- Network disconnection procedures in place – with pictures
- Ensure the situation is monitored closely and people are on standby
- Ensure full offline backups are offline and protected

Option 1 - Disconnect DCS Networks

- No data from the plant means no data / into out of SAP
- Product flows between plants secure connections between plants means production issues
- Customer orders cannot be fulfilled, contractual agreements in place – penalties waiting
- Logistics and Shipping affected
- Business systems still vulnerable – SAP, Labs, MES, etc

Option 2 - Disconnect UK from Rest of World

- No Internet access
- No internal or external electronic communications
- Plants can continue to run and not affect production
- Customer orders continue to be fulfilled
- No logistics or shipping affected
- Business systems also isolated from rest of world so not vulnerable.

If there was a ticking time bomb planted then both options still vulnerable

Tekgem
Systems and Technology

EXAMPLE: ACCIDENTAL INCIDENT – DISASTER RECOVERY

- One half of Manufacturing DMZ suffers catastrophic failure affecting 80 servers and 200 database systems
- Virtual machine based systems located on highly available cluster become unavailable with data corruption
- Occurs out of normal business hours
- Two Plants in the middle of turnaround requiring key systems back online in order to start back up
- E.g. Permit for Work, Shipping System, Lab Analysis, Plant Historian, Controlled Engineering Documents, Startup/Shutdown Procedures

Timeline of Events

1. Incident raised with vendor re: system instability
2. Vendor determines unsupported HW
3. Vendor supplies replacement HW
4. Vendor provides incorrect procedure for HW replacement
5. Causes major HW failure and data corruption
6. Major Disaster Recovery operation implemented
7. Issues with backups caused further delay
8. All systems restored within SLA

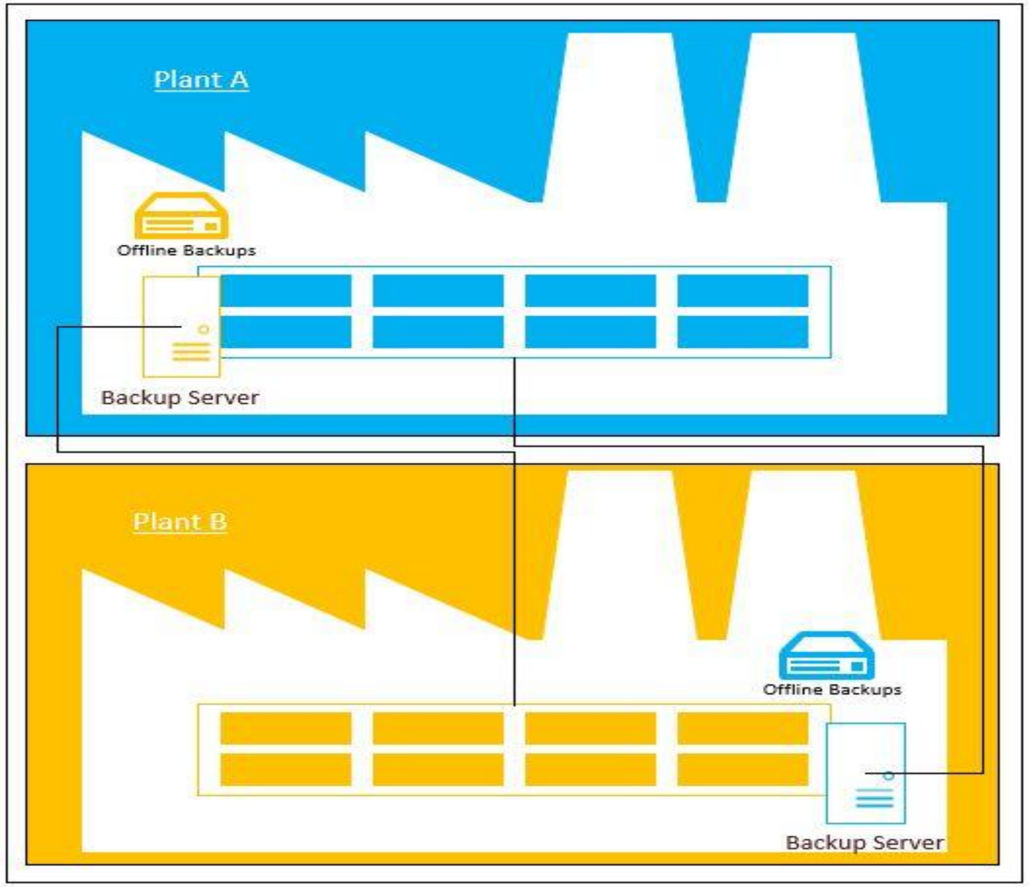
Disasters do and will occur. Do NOT think it won't happen to me!

Tekgem
Systems and Technology

DO YOU HAVE BACKUPS? ARE YOU SURE? REALLY SURE?

- Backups are as important as production systems
- Online backups stored in separate geographical location from production systems
- Offline backups stored in addition to online backups
- Guard against single point of failure (malware, ransomware, hardware, software etc)
- Ensure backups are successful, Have visibility
- Have an offline copy
- Keep it simple

‘Total protection is impossible. Some attacks will get through. What you need to do [at that point] is cauterise the damage.’
Ciaran Martin – Head of UK Government National Cyber Security Centre



EXAMPLE: WANNACRY VS MELTDOWN

WannaCry & NotPetYa

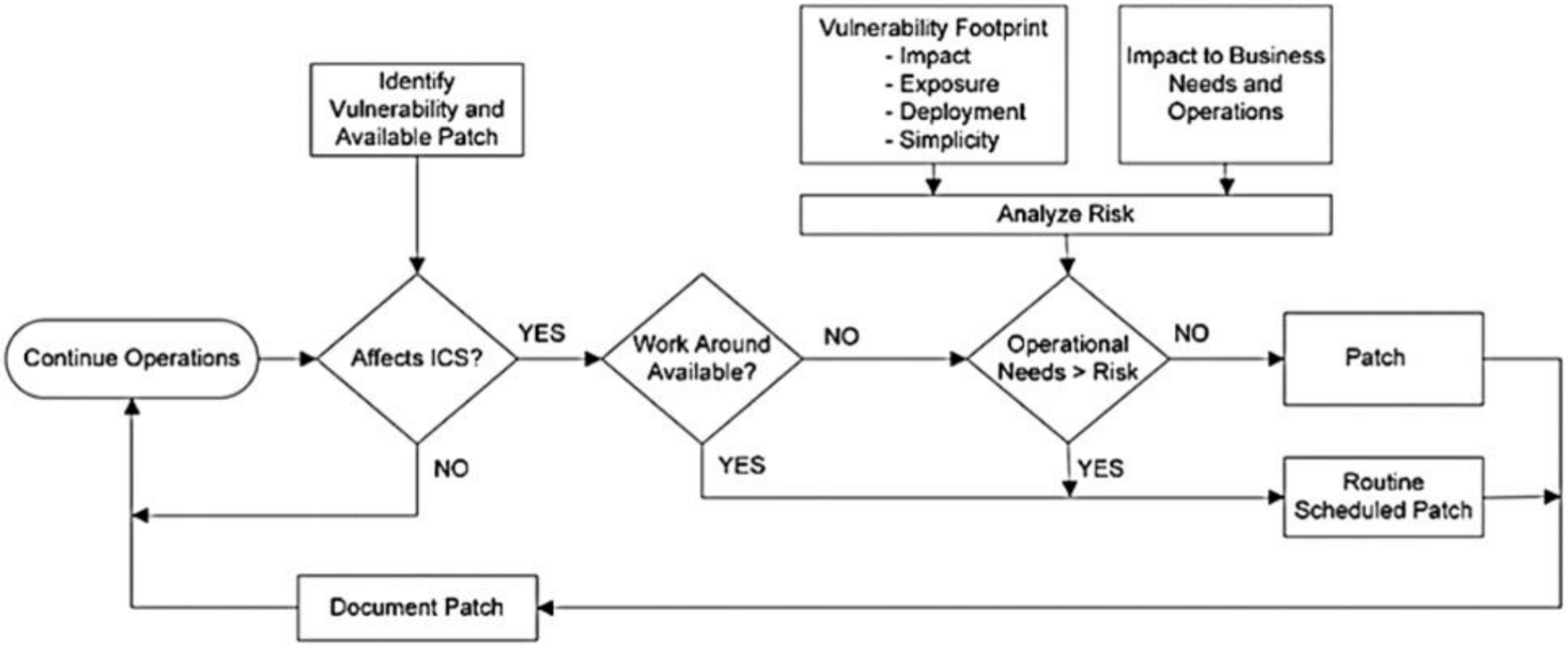
- High media coverage
- Fast moving / spreading fast
- Exploit causing large scale disruption
- Causing fear / panic
- Analyse & Evaluate all available information
- Emergency Meeting – Patch Everything Immediately

Meltdown & Spectre

- High media coverage
- No known exploits / no immediate threat
- Patches causing large scale disruption
- Patches causing fear / panic
- Analyse & Evaluate all available information
- Emergency Meeting – Stop Patching Immediately

Do not use a "One Size fit's all Approach", treat each threat independently.

PATCH DECISION TREE



Tekgem Systems and Technology

ACCIDENTAL OR MALICIOUS

- It doesn’t really matter... Both can have the same impact
- Plan for disaster, simulate disaster, test your disaster recovery
- Strategy is important, create policies, standard procedures, top-down
- Build a diverse team with skills and experience in business, process control and technology, good people are key
- The game is changing fast, remain agile and use all available resources
- Keep it simple

THANK YOU