RSAConference2020
Asia Pacific & Japan

A Virtual Learning Experience | 15–17 July

HUMAN ELEMENT

SESSION ID: **SAO-W05**

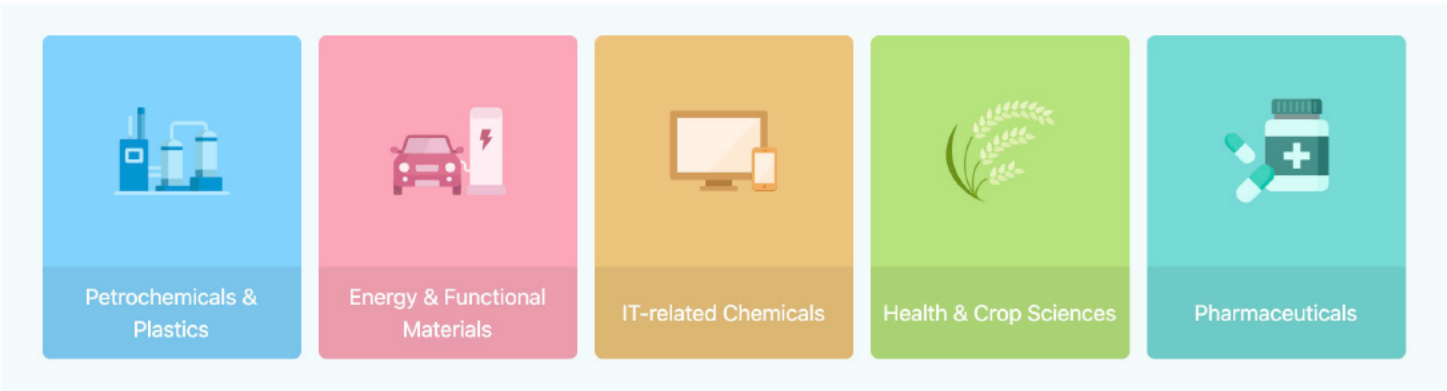
Building Cyber Security as a shared service

Erwin Eimers

General Manager, IT - Regional Headquarters in the Americas
Sumitomo Chemical America, Inc.
https://www.linkedin.com/in/erwineimers/

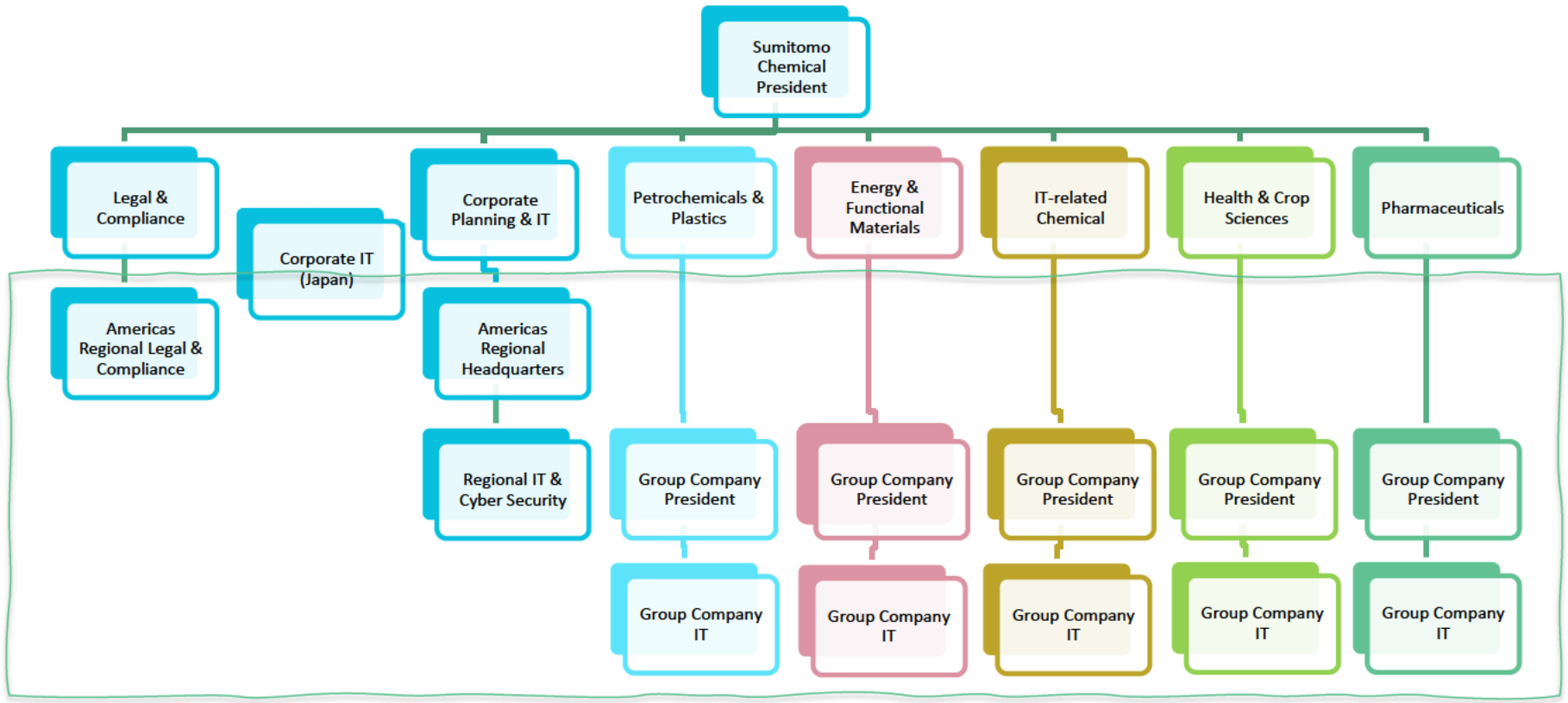
Introduction

- Sumitomo Chemical regionally structured like a group of separate companies
  - Globally some sector autonomy, regionally some group company autonomy
- Long history of local group company independence and freedom to act
- Group companies vary greatly in size and business model and have varying IT needs
- Sumitomo Chemical board decided that Digital Innovation is a “material issue” across all sectors to create value in the future
- Targeting more common platforms globally and locally as part of Digital Innovation



Sumitomo Chemical sectors

Sumitomo Chemical Americas structure



Introduction

- Situational Overview:
  - Increasing cyber security threats acknowledged by top management
  - Global standards needed to be established or improved and enforced to ensure CIA (Confidentiality-Integrity-Availability)
  - Insufficient communication and understanding of issues and needs between all levels
  - Acknowledgement of these issues by the group companies worldwide is critical
  - Autonomy of group companies important due to vastly different business model/product/customer
    - For example just in the USA we have group companies that:
      - Manufacturing and sales of chemical and organic crop protection and enhancement products
      - Biosciences – soil/public/forest health
      - Develop and manufacture thermoplastic automotive products (car interior, doors and trims)
      - Production of epitaxial wafers, resorcinol (tires, wood adhesives, dyes) and super engineered plastics (in-flight aerospace, medical)
      - Develop and market pyrethrum-based pest control products (from bed bug to scorpion control)

Introduction

Facts

Limited IT resources/skills at group company level

Some shared services exist in Americas region

Some common systems exist in Americas region

Existing shared services all infrastructure based:
- Connectivity
- Server hosting + IaaS
- Web hosting
- Remote infrastructure support

Questions

Do common systems/shared services make sense?

Why are existing services not always effective?

How do we get buy-in from all group companies?

How do we improve/enhance the communication and understanding?

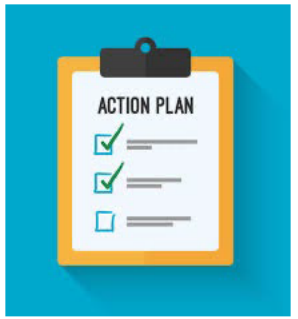
RSAConference2020 APJ
A Virtual Learning Experience

Cyber Security as a service

The journey

Action Plan

- Lessons learned of existing shared services
- Analyze gaps and confirm needs
- Develop security improvement plan that is:
  - Prioritized
  - Effective
  - Realistic
- Get buy-in, acceptance and support from Sumitomo Chemical globally and locally from the group companies



Lessons learned

- Issues with existing shared services:
  - Inflexible (hard to create one-size fits-all)
  - Not cost-effective for smaller group companies
    - Cost were not subsidized by HQ, so charges were relatively high
  - Infra outsourcing model not very popular by group companies (giving up control)
  - Doesn't address most security issues (phishing, CEO fraud, DoS)

Gap analysis

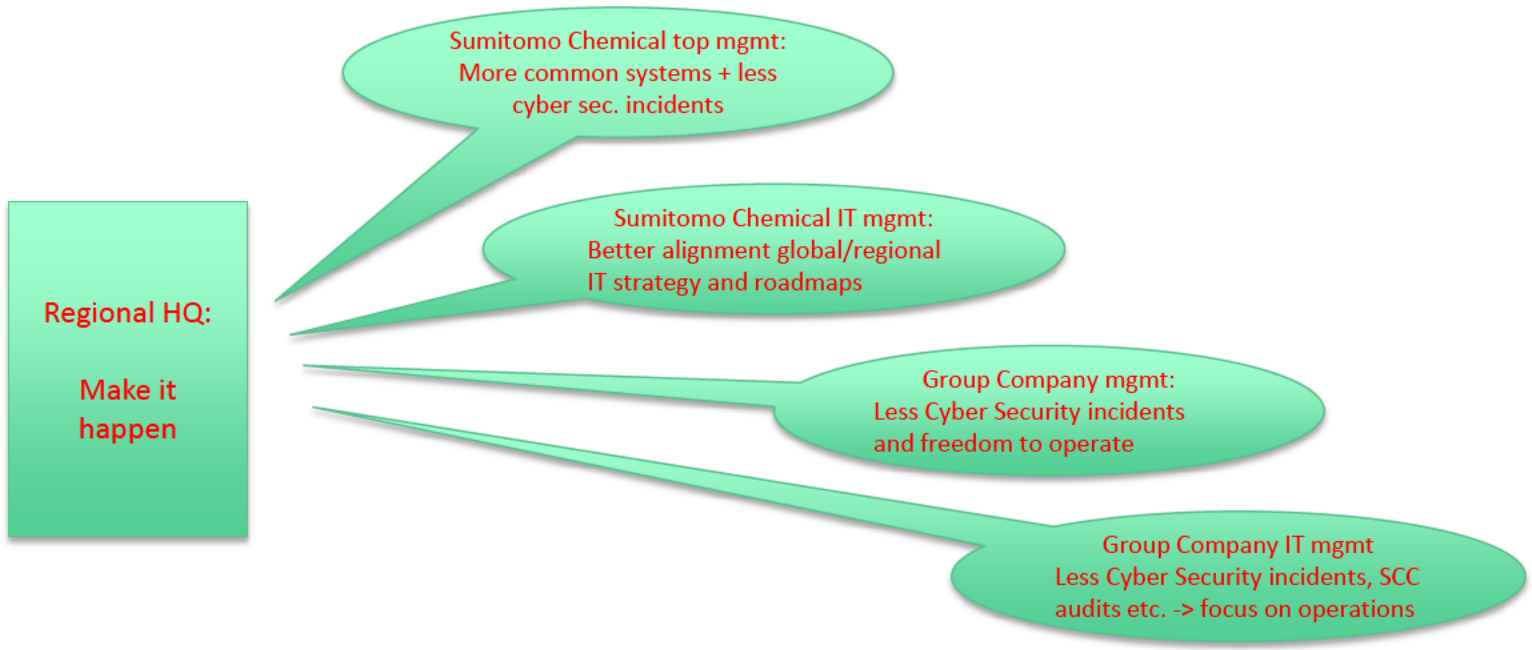
- Most issues Confidentiality/Integrity related, not Availability
- Social engineering (phishing, whaling, CEO fraud) big issue that needs to be addressed
  - Incidents created a need for group companies they couldn't resolve individually
- Cyber Sec Processes, Tools, Skills at group company level need improvement

Develop plan

- Clear need for improved security at group company level
  - Need for enforced security standards easy to explain due to incidents
- Plan must solve problem/needs for Sumitomo Chemical as well as group companies
  - Creating structured approach between HQ IT -> RHQ IT -> group company IT
  - Ties global IT roadmap, regional priorities and group company issues together
  - Cost effective for HQ and group companies
- Plan must have buy-in from group companies

Get buy-in

- How do we get buy-in from Sumitomo Chemical?
  - Tying in the regional solution with global IT roadmap
  - Create 3 tier (HQ, Regional HQ, group company) collaborative responsibility
  - Communicate, Communicate, Communicate



Get buy-in

- How do we get buy-in from group companies?
  - Understand and agree on their needs and issues
  - Understand their culture
  - Provide solutions they cannot accomplish individually
  - Implement in a way they feel in control
    - Transparency on solution planning and future roadmap
    - 3 tier approach (collaborative responsibility between all levels)
    - Security standards, training and help in implementation rather than operationally involved
  - Communicate, Communicate, Communicate

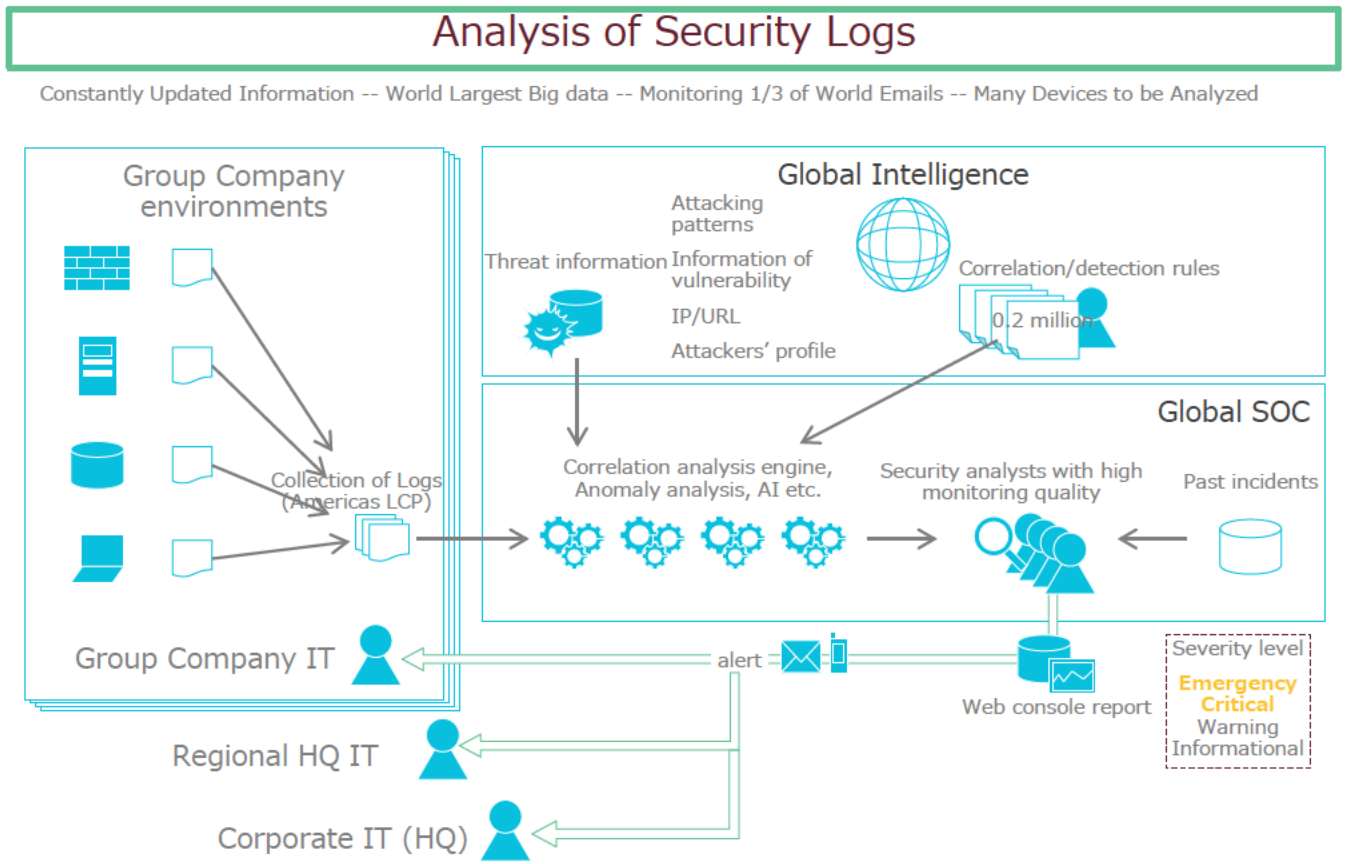
What we did

Common systems	Regional HQ services for group companies
Global Microsoft365 multi-tenant	Microsoft365 migration support Microsoft365 emergency support
Global Managed Security (SIEM) Solution (portal for HQ, RHQ and group company)	Managed regional SD-WAN (VeloCloud as a managed service) Incident reporting
Annual Security Awareness training	Regional training + phishing campaigns
Global web/internet-facing security baseline	
Global endpoint detection + remediation tool	Regional IRP + tabletop exercise Regional pen testing service Regional remediation + forensics support

How we implemented the services

- Common systems (Microsoft365 and Symantec MSS) implemented jointly between vendor, HQ, regional HQ and group company IT
- HQ covered implementation costs and group companies leverage Sumitomo's global pricing. Internal billing done by regional HQ
- Regional HQ provides cyber incident reporting assistance (also working with HQ on automation)
- HQ provides regular Microsoft365 support, regional HQ emergency support (AM business hours)
- HQ and regional HQ are defining baseline for website / internet facing systems
- Regional HQ provides security awareness training contents for region
- Regional HQ provides SD-WAN (VeloCloud) connectivity for region
- Regional HQ provides phishing campaigns (Mimecast) for region
- (future) Regional Incident Response Plan for group companies (incl. tabletop exercise and pen testing)
- All services by HQ or regional HQ are paid by Sumitomo except licenses and 3rd party costs

MSS implementation



Regional IRP and pen testing

- Regional HQ IT and regional Legal and Compliance are working on IRP. Will be implemented this year at regional HQ with tabletop exercise.
- In next 3 years it will be implemented at all group companies
- Each tabletop exercise will improve IRP for all group companies
- Pen testing will be a regional service by regional HQ (3rd party)

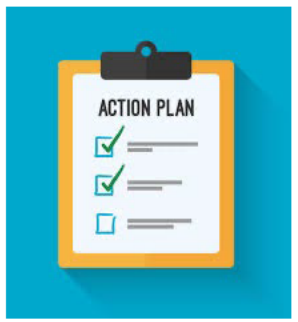
RSAConference2020 APJ
A Virtual Learning Experience

Cyber Security as a service

Summary

Summary

- Learn lessons from existing shared services and past experience
- Analyze gaps and Understand Needs
- Develop security improvement plan that meets needs and is:
  - Prioritized
  - Effective
  - Realistic
- Get buy-in from Sumitomo Chemical globally and locally
  - Address a need - tie global and local needs together
  - Understand and deliver to expectations
  - Communicate, Communicate, Communicate



Summary

- Had a real need for Improvement of Security
- “Outsourced” centralized operational IT support not a fit in our culture
- Some Common systems and standards needed and accepted
- Security standards and implementation Assistance/Competence very much accepted
- Training and testing (results shared on group company level) creates value and accountability
- Multi-tier collaboration and support benefits everyone
- Frequent and consistent communication

RSAConference2020 APJ

A Virtual Learning Experience

Cyber Security as a service

Tips

"Apply" Slide

- Is my shared service addressing the real issues?
  - Do I really understand what is needed from a shared service?
  - Is a shared service the right model?
- Are we trying to do too much as a service?
  - Are we focusing on the right things?
  - Can we deliver?
- Would I sign off on this service as a group company head?
  - Would I buy this service externally as a group company?
  - Is it priced fairly?
- How do I know if my service is successful?
  - Agree with the customer (group company) how we will make success measurable
  - Clear Feedback Loop (regular dialogue)

RSAConference2020 APJ

A Virtual Learning Experience

RSAConference2020 APJ

A Virtual Learning Experience