WHATABURGER®

ACP MEMBER MEETING WEBINAR

Cyber Resiliency and Supply Chain Business Continuity

BY: Rudy Saenz & Kristopher Loveless

09/12/2019

AGENDA

Agenda

- Introduction
- Top ten industry risks (DRI)
- Cyber Resilience
  - Trends
  - Scenario
  - Best Practices
  - New Laws
- Retail Business Continuity
  - Supply Chain
  - SCM Business Continuity
  - Case Study

TOP TEN INDUSTRY RISKS (DRI)

1 Major **IT Disruption** (deliberate)

2 Severe **Data Breach**

3 Extreme **Natural Disaster**

4 Major **IT Disruption** (accidental)

5 **State** Sponsored **Cyber** Attack

6 **Cyber Terrorism** on Operational Technology (OT)

7 Critical National **Infrastructure** (CNI)(CNI) **Failure**

8 Serious **Supply Chain** Disruption

9 **Man-made Major** Disasters

10 Global **Financial** Crash

CYBER RESILIENCE

Cyber-resilience means measuring the ability of an enterprise to limit the impact of security incidents.

Highly Cyber-Resilient Companies Are Able to:

- Quickly identify the full extent of the breach
- Quickly recover business operations due to devalued breach material
- Quickly restore customer confidence and ensure them of future security posture

Many companies suffer a breach event to move them from vulnerable to resilient, usually at a high cost.

EQUIFAX *Over 147 Million records lost, including personally identifiable information and credit card data*

Actions taken to improve resiliency:

- Refocus on Security – with the board of directors leading the initiative for the entire company
- Hired new Chief Information Security Officer and new Security staff
- Invested $200 million on data security infrastructure
- Overhauled all security processes, including patching, vulnerability management, and certificate management
- Improved data protection, by use of segmentation and better detection/response systems
- Implemented formal security training focusing on prevention and response activities

CYBER RESILIENCE- BEST PRACTICES

	Prepare/Identify - Identify, assess, and manage the risks
	Protect - Protect information and systems
	Detect - Detect anomalies/cybersecurity incidents
	Respond - Respond with proven capabilities
	Recover - Recover via incident management plan

CYBER RESILIENCE

Resilient? Movie**Pass**.

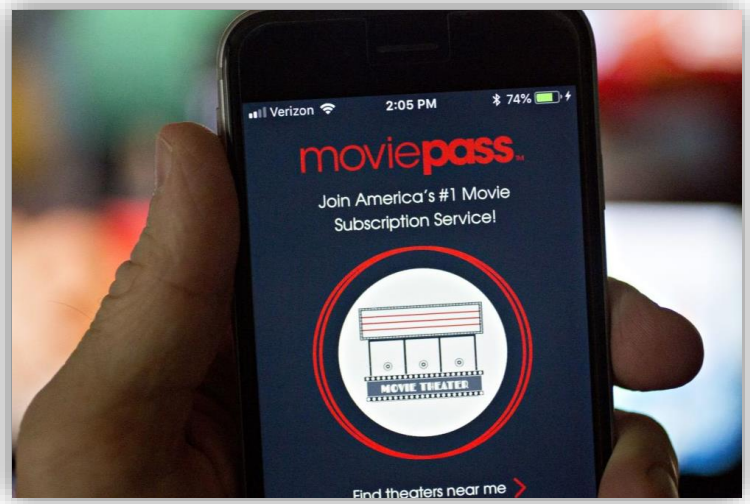
Wednesday 8/21/19, MoviePass confirmed a security lapse.

- Security misconfiguration of a live database – open access
- Database contained clear text information, including credit cards and MoviePass card numbers

Result: Up to 161 million customers records exposed

<u>*Actions immediately needed*</u>:

- Shut down access to the database
- Devalue the data – encrypt the data and remove extraneous elements
- Identify records exposed -> Notify consumers and government agencies



CYBER RESILIENCE – CHANGE TO TEXAS DATA BREACH LAWS

HB 4390 is a Bill which amends the state's data breach notification law and creates an advisory council tasked with studying and developing recommendations regarding data privacy legislation.

Old- Texas' law required businesses to disclose "as quickly as possible" any breach to individuals whose sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

New- The Bill introduces a timing requirement, mandating that individual notice be provided within 60 days of determining that the breach occurred.

"Sensitive Personal Information" defined as:

(A) an individual's first name or first initial and last name in combination with any one or more of the following items, if the name and the items are not encrypted:

(i) social security number;

(ii) driver's license number or government-issued identification number; or

(iii) account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account; or

(B) information that identifies an individual and relates to:

(i) the physical or mental health or condition of the individual;

(ii) the provision of health care to the individual; or

(iii) payment for the provision of health care to the individual.

CYBER RESILIENCE – CHANGE TO TEXAS DATA BREACH LAWS

The Bill also adds a requirement to notify the Texas Attorney General if notifying at least 250 Texas residents.

Notice to the Attorney General must be provided by the same deadline (within 60 days of determining the breach occurred) and include:

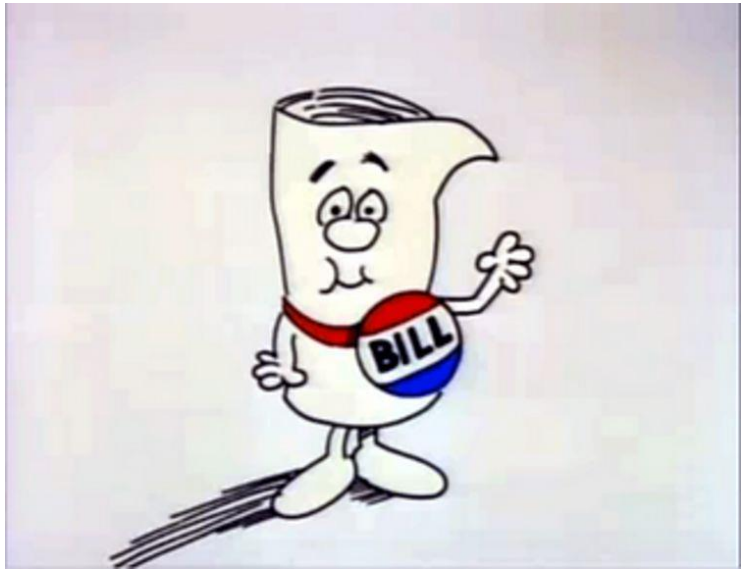
(1) a detailed description of the nature of the breach or the use of sensitive personal information acquired as a result of the breach,

(2) the number of Texas residents affected,

(3) measures taken regarding the breach,

(4) any measures intended to be taken after Attorney General notification, and

(5) information regarding whether law enforcement is engaged in investigating the breach.



Bill also creates the Texas Privacy Protection Advisory Council to study data privacy laws in Texas, other states and in relevant foreign jurisdictions.

The council is charged with reporting its findings and recommendations regarding data privacy and protection by September 1, 2020

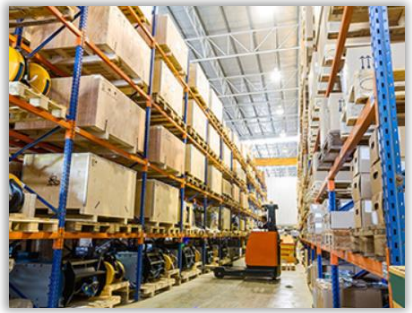
Questions

Supply Chain Business Continuity

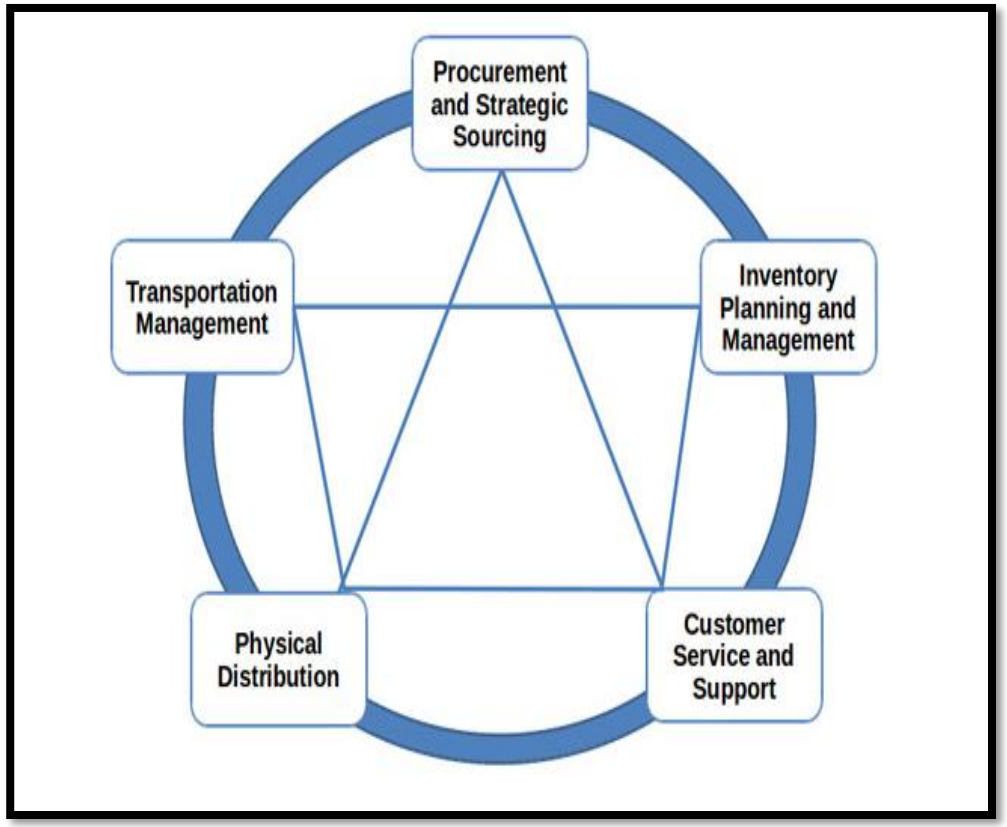
DEFINING SUPPLIERS

- Manufacturers and Vendors - companies that research, develop and produce the finished product or service ready for use. Manufacturers and vendors are the source of the supply chain.
- Wholesalers and Distributors - companies that buy in bulk from several manufacturers or vendors
- Affiliate Merchants - merchant is a supplier that wishes to drive traffic to their website or sales of their product through banner ads and links placed throughout a network of affiliates.

- Franchisors - an individual, which allows them to develop their own business using the trademark.
- Importers and Exporter- suppliers will purchase products from manufacturers in one country and either export them to a distributor in a different country.
- Independent Crafts People - normally manufacturers of products they have designed or produced on smaller unique scales of economy.
- Drop Shippers - suppliers of products from single or multiple companies that will deliver direct to the buyer once they have made the purchase from your business.



INTERRELATIONSHIP OF SUPPLY CHAIN PROCESSES



Procurement and Strategic Sourcing – an institutional purchasing process that continuously improves and re-evaluates the purchasing activities of a company.

Transportation Management – a subset of supply chain management concerning transportation operations and may be part of an enterprise resource planning system.

Physical Distribution – the movement of materials from the producer to the consumer.

Customer Service and Support – a range of services to assist customers in making cost effective and correct use of a product.

Inventory Planning and Management – the process that any organization adopts to determine the optimal quantity as well as timing, with the sole aim of aligning such plans with the organization's capacity to produce and make sales.

BUSINESS CONTINUITY AS IT APPLIES TO SUPPLY CHAIN MANAGEMENT

Here are some other scenarios to consider when assessing supply chain resilience:

- Sole source – goods and/or services that only one supplier can provide.
- Single source – goods and/or services in which one supplier provides but alternate suppliers can be utilized.
- Just in time (JIT) – an inventory strategy companies use to increase efficiency and decrease waste by receiving goods only as they are needed in the production process, thereby reducing inventory costs.
- Lead times – the time between when goods and/or services are ordered and when they are delivered.
- Safety stocks – extra stock that is maintained to mitigate risk of the shortfall in raw material and/or packaging.
- Enterprise resource planning (ERP) – the integrated management of core business processes, often in real-time, and mediated by software and technology.

NOKIA VS. ERICSSON -- MARCH 17, 2000

Not having a Supply Chain Business Continuity plan can cripple a company. A fire at a Phillips microchip plant in Albuquerque, New Mexico on March 17, 2000. The plant supplied micro chips for Ericsson and Nokia, at the time they both made up 44% of the market. The fire contaminated almost the plant's entire stock.

Nokia

Acted quickly and moved production to other plants and looked for alternate suppliers. In addition, they adjusted the make of their phones so they could work with other types of chips from other suppliers from Japan and America.

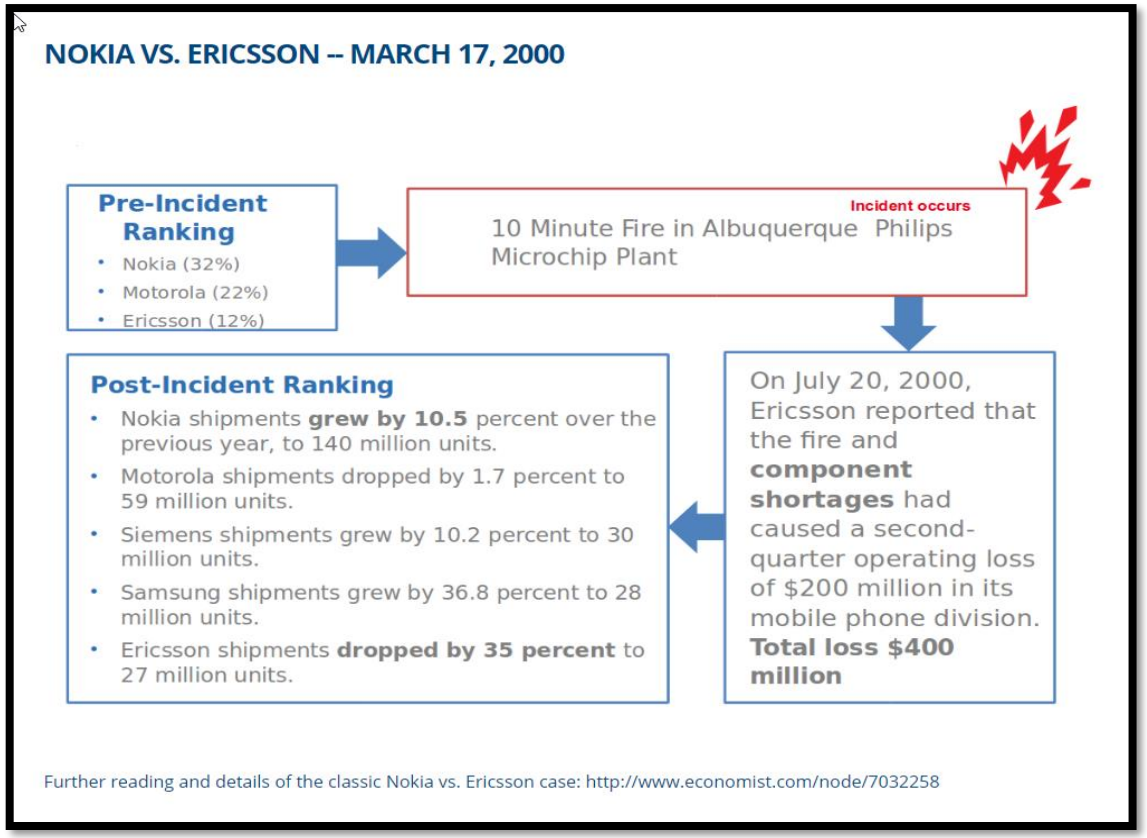
Ericsson

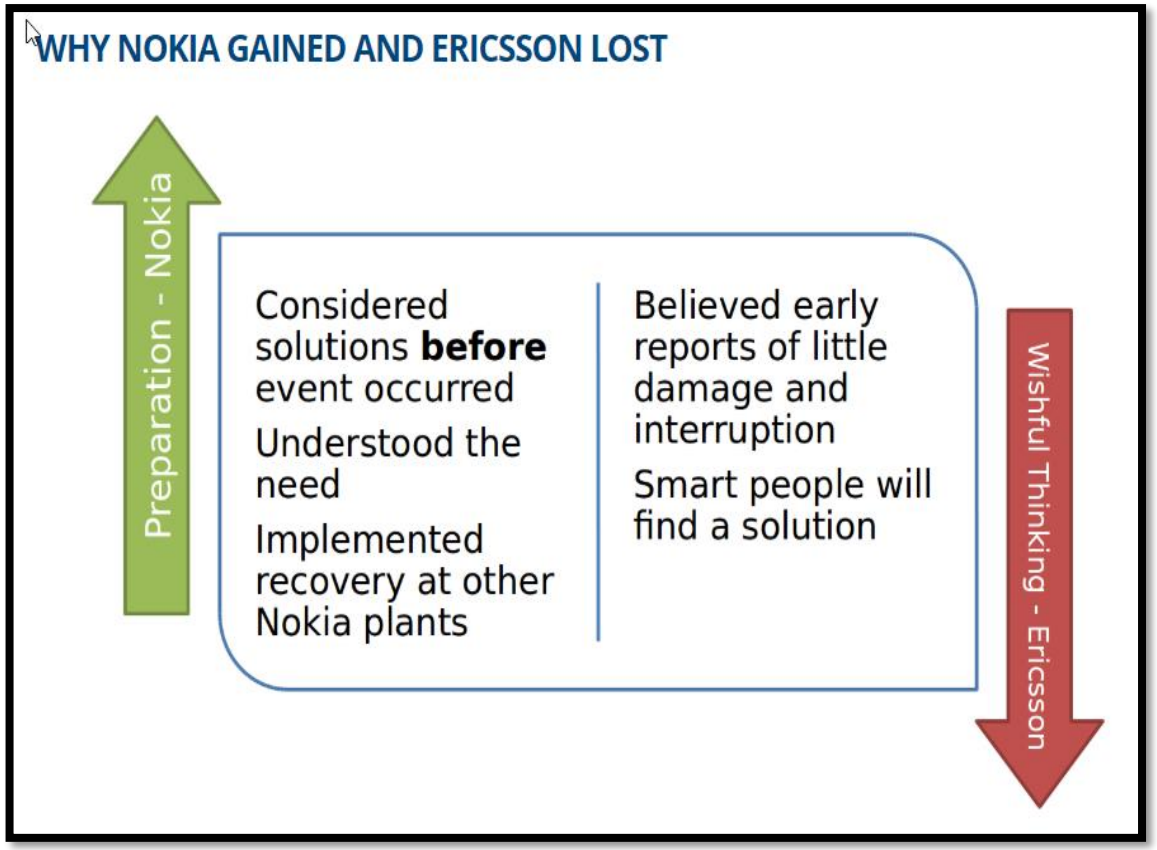
Accepted the assurance from suppliers that the fire would not cause a big problem. The suppliers communicated to Ericsson to wait it out. When the Ericsson realized they had made a mistake it was to late and had lost significant time against their competitor. Nokia had already secured all the available suppliers. In addition, few years earlier the company decided to move a from a sole source supplier to simplify their supply chain.

Motorola

Motorola learned by watching this incident and took a proactive approach by implementing Business Continuity Management.

NOKIA VS. ERICSSON -- MARCH 17, 2000





NOKIA VS. ERICSSON – RESULTS

Ericsson lost months of production and this allowed Nokia to take control of the market.

- Mobile phones would be spun off into a joint venture with Sony in October 2001 (Sony Ericsson Mobile Communications)
- Rounds of restructuring, refinancing and job-cutting; during 2001
- Staff numbers fell
    - 2001 - 107,000 to 85,000
    - 2002 – 85,000 to 65,000
    - 2003 - 65,000 to 54,000

Motorola learned by watching this incident and took a proactive approach:

- Incorporating supply chain processes and considerations into their business continuity strategy
- Requiring suppliers to share their plans and notify Motorola in the event of an activation
    - Business impact
    - Risk assessment
    - Crisis management
    - Information technology
    - Disaster recovery
    - Business continuity

VENDOR BUSINESS CONTINUITY

1. Personnel loss and planning
2. Relocation plans
3. Remote access availability
4. Facility loss contingencies
5. Breach/disruption notification procedures
6. Testing frequency of their plans
7. How often their plan is updated
8. Are there changes to the plan after an event
9. Sub-service vendor communication plans if critical functions are outsourced
10. SLAs and contractual obligations for outsourced systems
11. Business continuity plans should include Business Impact Analysis (BIA) on your vendors

RISK IN SUPPLY CHAIN

Build a risk assessment chart and work towards analyzing the risk down to the supplier level from three positions:

What are the risks to the product itself?

What are the risks to the production site?

What are the risks to the production line?

REFERENCES

1. *"Sony Ericsson Mobile Communications established today - Ericsson". News.cision.com. 1 October 2001. Retrieved 11 November 2016.*
2. *Svenolof Karlsson; Anders Lugn. "The first cutbacks". Ericsson History. Retrieved 11 November 2016.*
3. *Svenolof Karlsson; Anders Lugn. "Second round of cuts". Ericsson History. Retrieved 11 November 2016.*
4. *Svenolof Karlsson; Anders Lugn. "A new chairman of the board". Ericsson History. Retrieved 11 November 2016*
5. DRI International. Business Continuity for Supply Chain Management. *11 March 2019*
6. https://www.huntonprivacyblog.com/2019/06/26/texas-amends-data-breach-law-now-requires-regulator-notification/
7. https://variety.com/2019/digital/news/moviepass-security-breach-customer-records-1203309976/
8. Wade P. Richmond “Achieving Cyber-Resilience” DRII. 23 December 2018

THANK YOU

WHATABURGER®