RSAConference2018
San Francisco | April 16 – 20 | Moscone Center

SESSION ID: CXO-W12

VALUE AT RISK: DECISION MAKING IN CYBERSECURITY INVESTMENTS

Sateesh Bolloju

Principal Architect,
Product Security, Inflyt Experience
Thales Avionics Inc.
@s_bolloju

Views and opinions expressed in this session are mine and not those of Thales, RSA or any other entity.

Digital is *The Economy*

What's at risk?

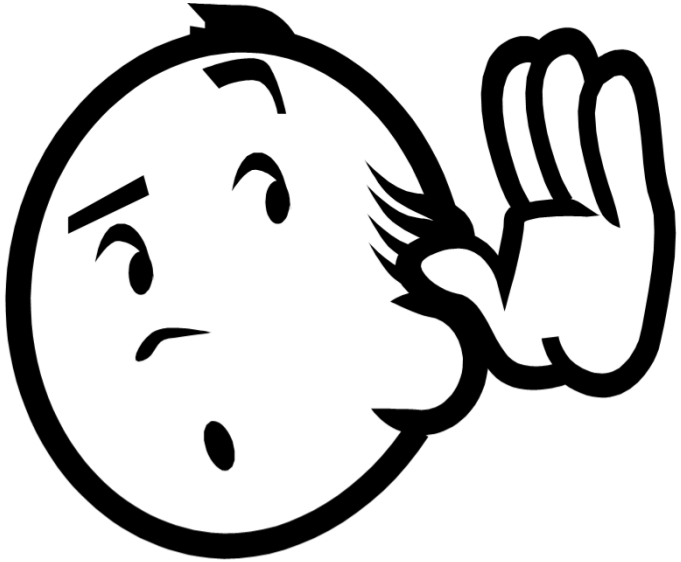
Financial Risk

Business Disruption

Regulatory & Compliance

Customer Trust

You heard this?



Polling question?

- Session ID: CXO-W12
- You are challenged to justify security investments
  - Agree
  - Neutral
  - Disagree

Poll Results


Decision making
+11,00.00
Cyber Security Investments

Challenge today

Cyber Security Investments

What's the answer?

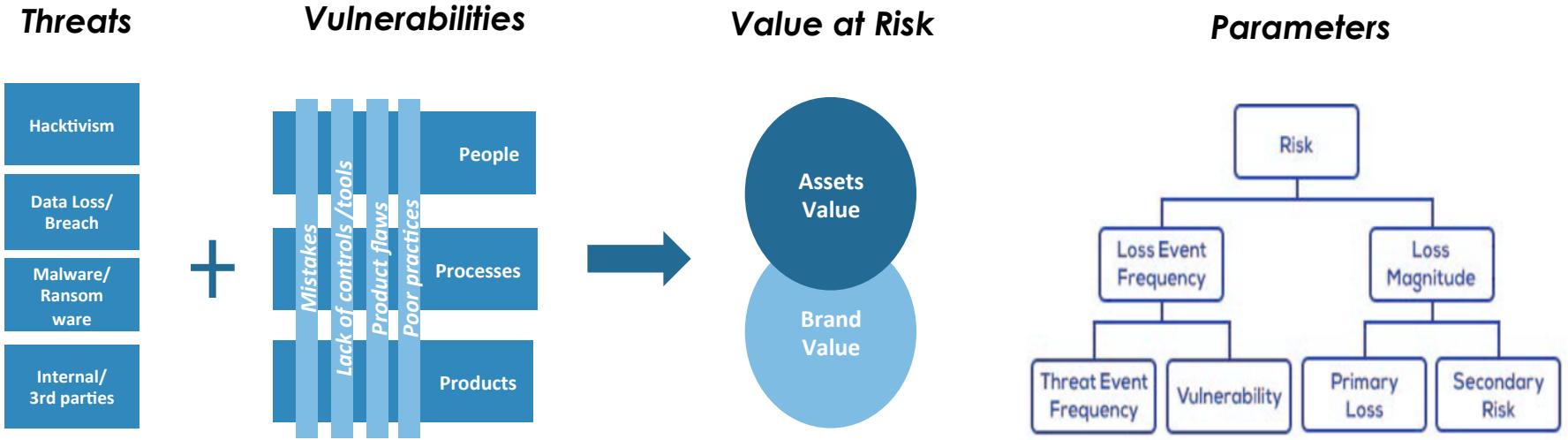
Value at Risk (VaR):

A measure to quantify

the potential loss

over a specific time frame

Framework & Methodology



Lose no more than $$$$$ amount over a period of time with 95% confidence with a successful attack

Quantify Risks

Value at Risk =

Expected Loss * Probability * Frequency

Standardize VaR model based on identified parameters, environment, specific to the company and cyber maturity

Value at Risk in Action

Scenario

Lack of privileged access controls for an infrastructure leads to data loss

Expected loss = $116.3 million

- $110 million (Say 500,000 customers' data breached , $221/record**)
- $1 million (Incident response, recovery, liability/legal fees)
- $5 million (Brand value, 1% percent of annual revenue)
- $300,000 (Productivity loss to manual and inefficient PAM processes)

Probability = 10% (3% after investment)

Frequency = 1 in 3 years (0.2 after)

Value at Risk = $ 11.63 million

Benefit = VaR (B) – VaR (A)

** Cost per record for US, refer to 2016 Cost of Data Breach Study by Ponemon/IBM research

Value at Risk Case Study Scenarios

Scenario 1	Scenario 2	Scenario 3
Product design documents stolen by rogue employee (IP loss)	Exploited known CVE (Apache, Android or Open SSL) disrupted business services	Lack of privileged access controls for an infrastructure leads to data loss
Expected loss = $21.6 million ▪ $20,000,000 (10% of revenue loss) ▪ $350k, Incident response, recovery, & communications ▪ $ 250k, Productivity loss ▪ $ 1 million, Loss due to secondary risk ▪ No additional brand value loss	**Expected loss = $13.5 million** ▪ No data loss ▪ $500k, Incident response and discovery analysis due to lack of automated AIM tools ▪ $2 million due to fines for not providing services ▪ $1 million due to productivity loss ▪ $ 10 million (10% of potential contract loss)	**Expected loss = $116.3 million** ▪ $110 million (Say 500,000 customers data breached , $221/record**) ▪ $1 million, Incident response, recovery, liability ▪ $5 million, Brand value loss (1% percent of annual revenue) ▪ $300,000, Productivity loss to manual and inefficient PAM processes)
Probability = 5%	Probability = 10%	Probability = 10%
Frequency = 1 event in 3 years	Time frame = 2 events in 3 years	Time frame = 1 event in 3 years
Value at Risk = $1.08 million	**Value at Risk = $ 2.70 million**	**Value at Risk = $ 11.33 million**

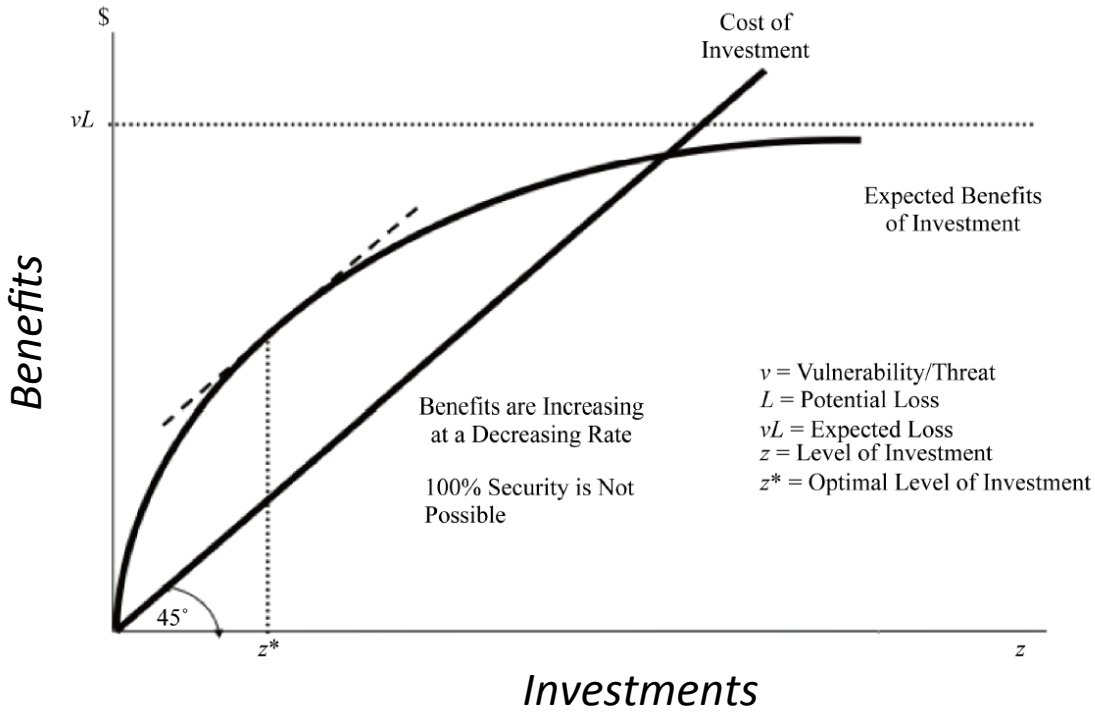
** Cost per record for US, refer to 2016 Cost of Data Breach Study by Ponemon/IBM research

How much should be invested in Cybersecurity?

Optimal Cyber Investments?

Benefits > Cost of Investment

Invest no more than 1/3 of Value at Risk



** Adapted from Gordon-Loeb Model*

TO SUMMARIZE…

Summary

- Understand product security threats
- Quantify cyber risks
- Determine VaR
- Decide ‘What, Where and How much’ to invest

Lessons Learned

- Keep it simple
- Make it realistic and apply to your situation
- Educate your stakeholders
- Don’t fall in love with products or technologies
- Always ask what’s the “Value at Risk”

How to apply?

Understand VaR model

Determine applicability

Identify scenarios and adopt

Socialize and obtain buy-in

Implement VaR

Questions?

sateesh.bolloju@us.thalesgroup.com

www.linkedin.com/in/sateeshbolloju

@s_bolloju

Thank you!