



# Kaspersky Industrial Cybersecurity Conference

Risk Management &  
Executive  
Communication

# Success Factors

- Know **yourself**
- Know your **business**
- Know your **executives**
- Know the risks that matter to them, **not you**
- Know how to prioritize for **business**, not security
- Know the **language**
- Know how to **close**

# Security Doesn't Matter

- Executives, Boards, C-levels **do not care** about security
  - They do, but they do not
  - It is confusing, expensive, and restrictive
- Airgaps, isolation and **similar myths** prevail
- It has **never happened** to me, so why worry?
- This is the way we have **always** done it
- Insanely high operations and equipment **costs win**
- How can security compete? It can not. But **risk can.**

# Look in the Mirror

- Management **never listens** to their own staff
- Lose the **ego**; you are insignificant in their world
- Degrees, certs, S4/BH/DC presentations **do not matter**
- Technical skills **do not matter**
- Be prepared to **accept** WAY more risk than you want
- Be prepared to repeat yourself with **different words**
- “**Soft skills**” are worth more than anything

# Know Your Business

- Business **age** matters
- **Governance**
  - Investor owned
  - Private
  - Municipal
  - Multinational
- Product **diversity**
  - Vertical integration
  - Multiple industries or supply chains

# Put on Your Executive Hat

- You are **good at business** or you wouldn't be a C-level
- You know some things well, but **not deep** everywhere
- Very **unwilling to lose** anything
- Do not **care** if people do not like you or your decisions
- Do not like looking stupid or weak in front of **peers**
- Everyone sees you as a **target**
- Small circle of **trust**; anyone else is an outsider
- You can get fired for just about **any reason**

# Executives Speak RISK

- Risk = **probability** (likelihood) x **impact** (consequence)
- Risk options: **accept**, mitigate or transfer
- No risk, no reward
- The executive's job is to make as much **money** as possible by taking as much risk as possible
  - ...with the least amount of loss to the company or self
- Security is one of **many** risks in the “all hazards” view

# Risk Types

- Confidence (business/**brand** integrity)
  - Market
  - Shareholder
  - Customer
- Competitor **advantage**
- **Credit** rating; access to capital
- **Regulation**
  - Safety, environmental, security, etc
  - Rate (cost recovery)

# More Risk Types

- Loss
  - Revenue
  - Production downtime (outage); **think in terms of \$/minute**
  - Human error, equipment failure
  - Costs for loss control measures
  - Administrative costs
- Liability & insurance (also a form of loss)
  - Increase in premium
  - Lack of coverage or exclusions
  - Insufficient coverage
  - Claim management expenses

# Even More Risk Types

- Product and process
  - Tariffs
  - Proprietary information
  - Supply chain
- Workforce disruption
  - Labor disputes
  - Automation
- Market
  - Supply, demand and cost
  - Purchasing trends

# Do Your Homework

- How does your problem **fit** into their risk framework?
- Do not bring problems without **solutions**
- Have you thoroughly analyzed the **business** issue?
- What is the **root cause** of the problem?
- What are the **gaps**?
  - People, process and technology are easy categories
- Executives love **precedent**
  - What solutions have worked for **similar companies** in similar situations? Do you have **proof**?

# FUD Does Not Work

- Remember, security is a **cost center** not a profit center
- Security has a **stigma**; confusing, expensive, restrictive
- They already think they are spending **too much** on security and it only seems to **increase** every day
- Scaring them into action can **backfire** on you
- Why are we **spending** on security if it will not work?
- If the problem is bad enough, the **governments** will help
- Stay away from **stories** about hackers, terrorists, nation states, organized crime and other existential threats

# Say This Instead of That

- Executives do not speak IT or OT. They speak **business**.
- Do not say security. Instead, **rebrand** it as...
  - Risk **reduction**
  - Reliability/continuity **improvement**
  - Loss **prevention**
  - Operational **efficiency**
  - **Reduced** downtime or recovery **enhancement**
  - Process **improvement** or **reduction** of human error
  - Insurance coverage **improvement** or premium reduction
  - Anything from the aforementioned list of risks
- Speak in terms of **gaps/strengths** and **maturity/growth**

# Prioritization

- Tactical – **More difficult** to sell
  - Near term, less than a year
  - Typically a stand alone project; steeper ramp
- Strategic – **Less difficult** to sell
  - Longer term, 1-5 years
  - Typically can be woven into existing project; less effort
- Priority is based on:
  - Degree of impact
  - Probability of occurrence in a specified timeframe
  - Cost model for payment/recovery

# Make It Easy to Understand

- Give the problem a simple, positive “business name” not a “security name” – **branding matters** more than you think
- Stoplight charts; red, yellow, green
- Up arrow, down arrow (**trending**)
- Keep it **simple**:
  - Problem/**solution** statement
  - Risk – why does this **need** to happen?
  - Maturity – how **easy** will this be?
  - Cost – how much will it cost and is there cost **recovery**?
  - Priority (tactical or strategic) – **when** should we do this?
- Keep it to a **single page**

# Close The Deal

- You are there to **educate** them on the risks and provide a range of solution options
- Do not criticize/blame any person or business unit directly
  - **Enable** problem area to grow/fix
- Require a **decision**, give an expected timeframe
  - No decision means that the risk is **accepted by default**
  - Risk will change if decision is delayed
- Recommend the best path, but be prepared with **options**
  - Accept, mitigate or transfer
  - They will probably want to shift the priority
- Never lose your temper; **balance** your intensity

# Example...

- Problem: Lack of operational monitoring of ICS assets
- Solution: “*Visible Operations*” – new tools & network designed for monitoring provides additional operational data & visibility
  - Increases system operational data & analysis capability
  - Faster issue detection & root cause analysis
  - Increases uptime; lowers maintenance costs
- Cost: low per network segment; high cost recovery potential
- Capability: high; mature corporate skillset
- Risk: low; close to current system/network model, but with minimal new hardware, software and training
- Priority: strategic; added with capital improvements

# Summary

- Executives do not care about security but they do care about **making and losing money**
- Do your homework, be prepared, **speak their language**
- Never bring a problem without **solutions**
- Make your message **easy** for them to understand
- You are there to help them make a decision; that decision will probably come with more **risk** than wanted
- Your role **is not** to secure the company, **it is** to enable the business to make (and keep) more money

 @PATRICKCMILLER

 LINKEDIN.COM/IN/MILLERPATRICKC

 P.MILLER@ARCHERINT.COM

 WWW.ARCHERINT.COM

 WWW.PATRICKCMILLER.COM

 +1.503.272.1414

