

Security Lessons Learned From Our FSI Customers

Bill Horne

Project Manager, HP Labs



FSI is a business like any other

- ... except they are a high profile target
- Most security problems are not specific to FSI
- The Large Enterprise Problem
 - Hundreds of thousands of user machines
 - Tens of thousands of servers
 - Thousands of network devices
 - Petabytes of storage
 - 20 TB/day transaction data
 - “an order of magnitude more network log data”
 - Complex, labor-intensive processes
 - Not static, constantly changing
 - Multi-national organizations dealing with local regulations
 - Even basic questions such as, “What is on my network?” are exceedingly difficult to answer in practice.

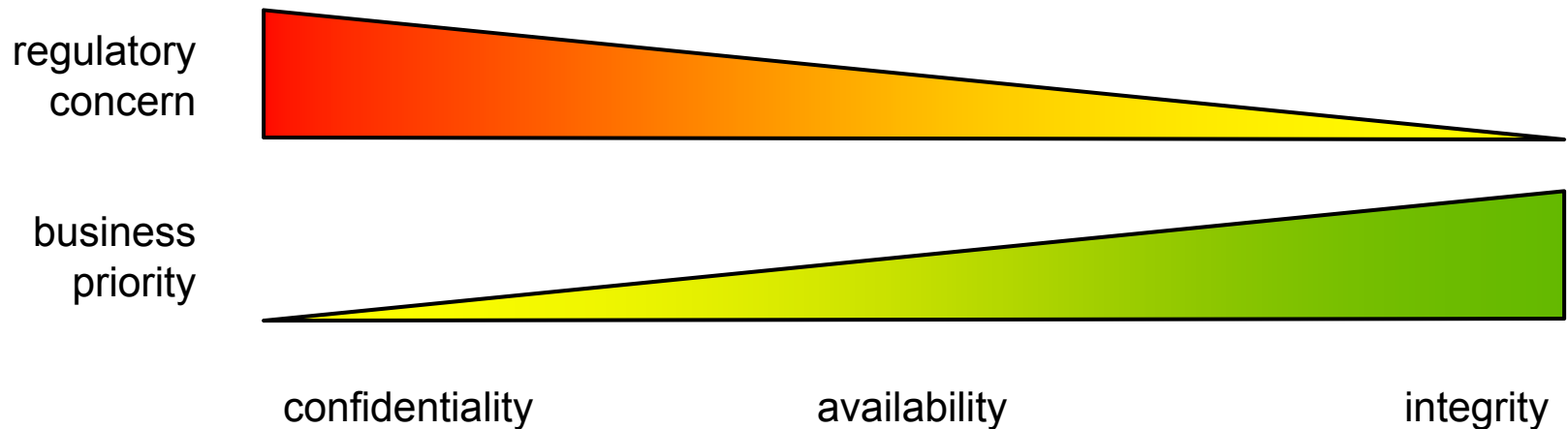
Major initiatives at our FSI customers

- Extended enterprise
 - How do you validate the security of your partners, suppliers, customers?
- Identity and entitlement management (SSO, role management, provisioning/deprovisioning)
 - Extremely difficult to deploy and maintain
- Data protection
 - Portable media
 - Laptop encryption
- Risk Management
- Rationalizing alphabet soup of standards & regulations
 - CoBIT, COSO, ISO2700x, ISO17799, SOX, Basel II, GLBA, PCI, ...

Business Drivers

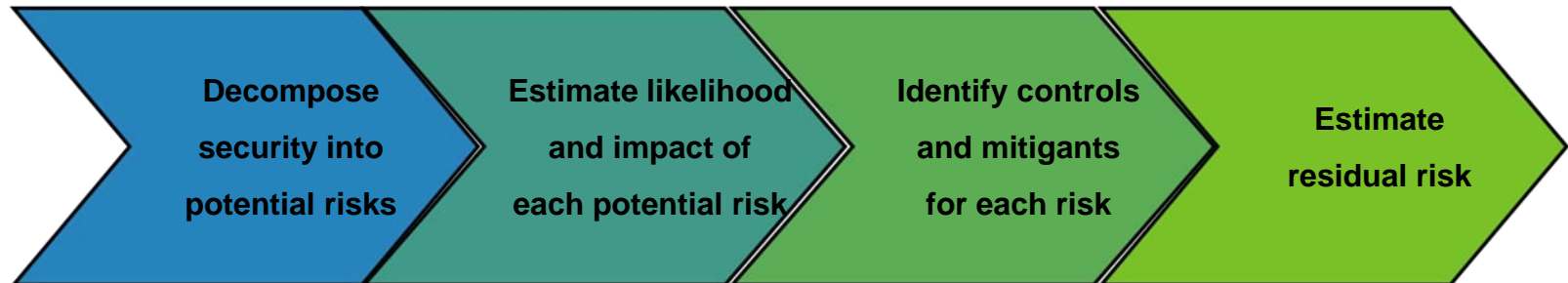
- FSI is fundamentally an information business
 - They don't manufacture anything
 - They aren't primarily a services business
 - Their business *is* information
- Growth is primarily inorganic
 - Desperately seeking ways to innovate

The problem with regulatory driven security



- There is a tension between what the regulators want and what the business is trying to achieve
- Strong trend to move from being regulatory driven, to being risk driven
- CRA grand challenge of “*development of quantitative information-systems risk management that is at least as good as quantitative financial risk management within the next decade*” is more relevant than ever.

IT Security Risk Management Best Practices



risk = likelihood x impact

\$\$\$

\$\$\$ < risk reduction?

- Different methodologies advocate different approaches: by threat, vulnerability, asset, etc.
- How do you know you have the right decomposition?

- Estimates are more qualitative than quantitative
- Typically bucketed into low, medium, high.

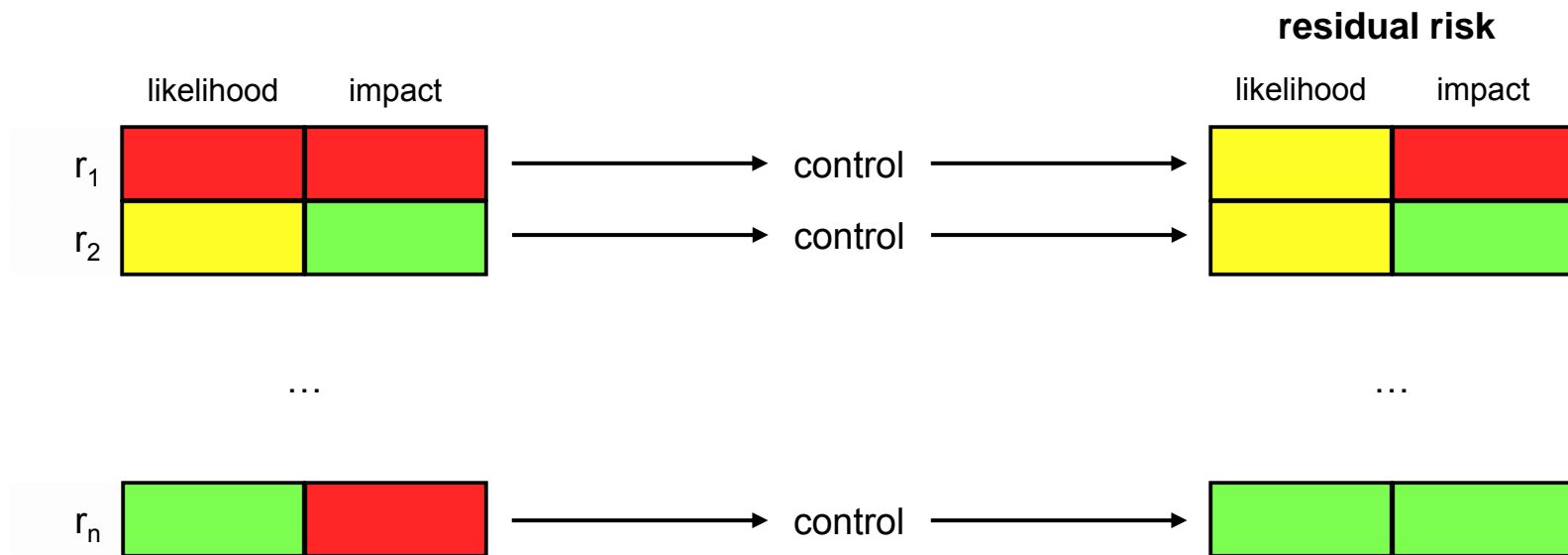
- Many-to-many relationship between controls/ mitigants and potential risks

- Residual risk is typically done on a “line item” basis.
- Poor ability to account for composite controls
- Difficult to optimize over entire security portfolio

Based on
Octave, FAIR, NIST, FRAAP

Best Practices

Typical Heat Map Approach



| Impact | Likelihood | | | | |
|---------|------------|----------|------------|----------|--------|
| | immediate | imminent | occasional | sporadic | rare |
| level 4 | critical | high | high | medium | medium |
| level 3 | high | high | medium | medium | low |
| level 2 | high | medium | medium | low | low |
| level 1 | medium | medium | low | low | low |

