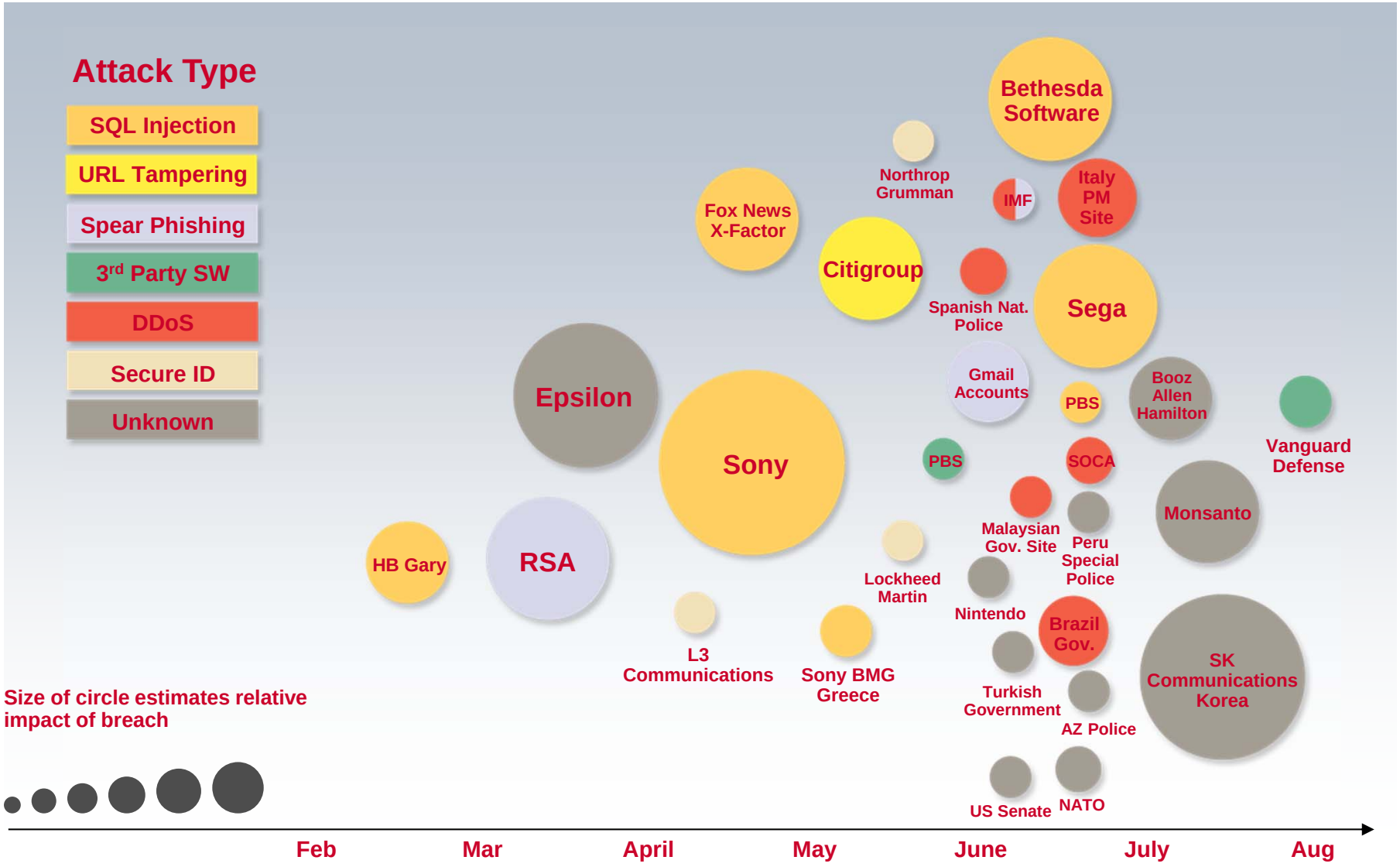
# Security Metrics & The Boardroom

*How does security articulate business value*

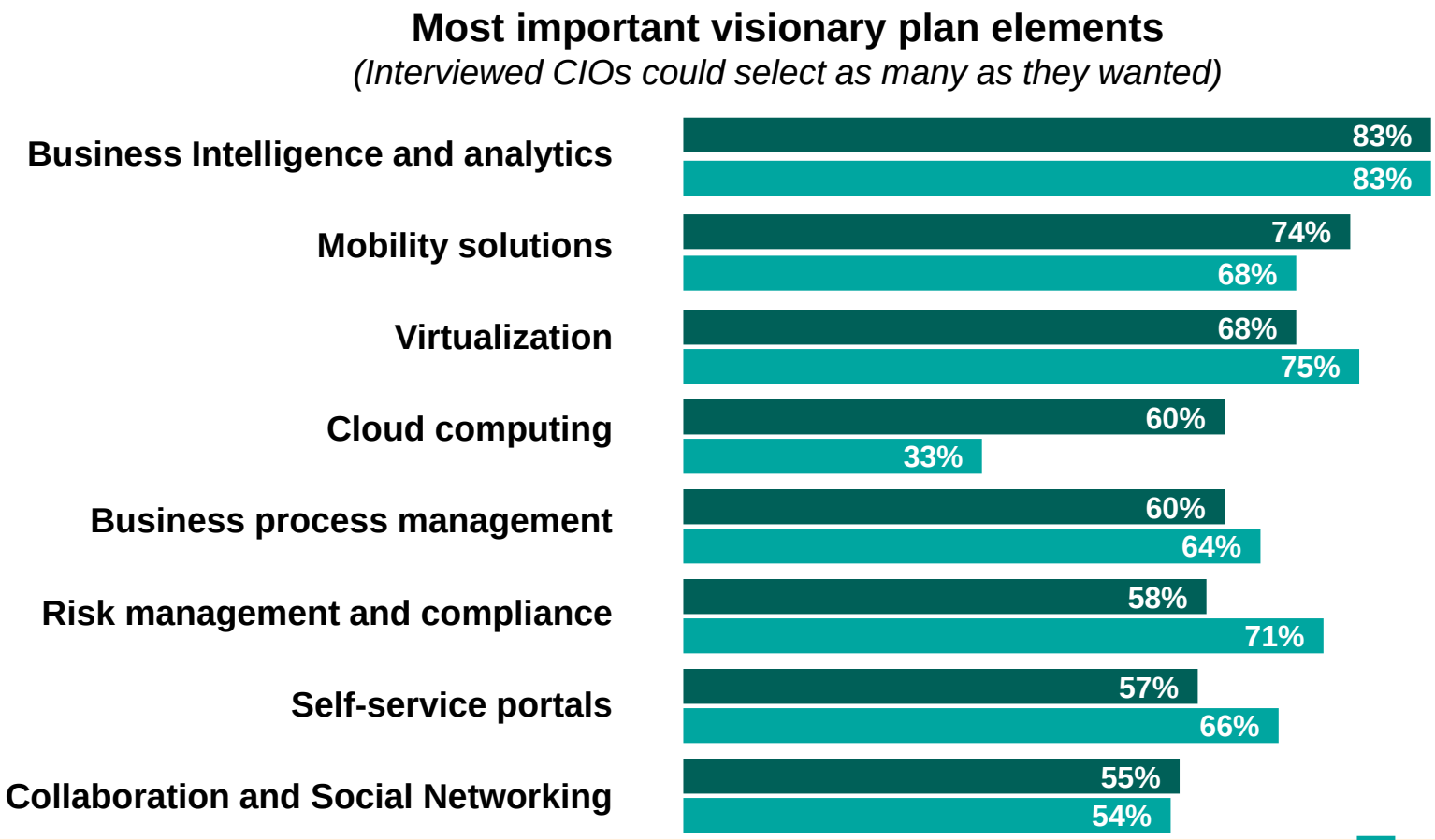
**Rick Miller**
**IBM, Director Managed Security Services**

Session ID: SECT-203
Session Classification: General Interest

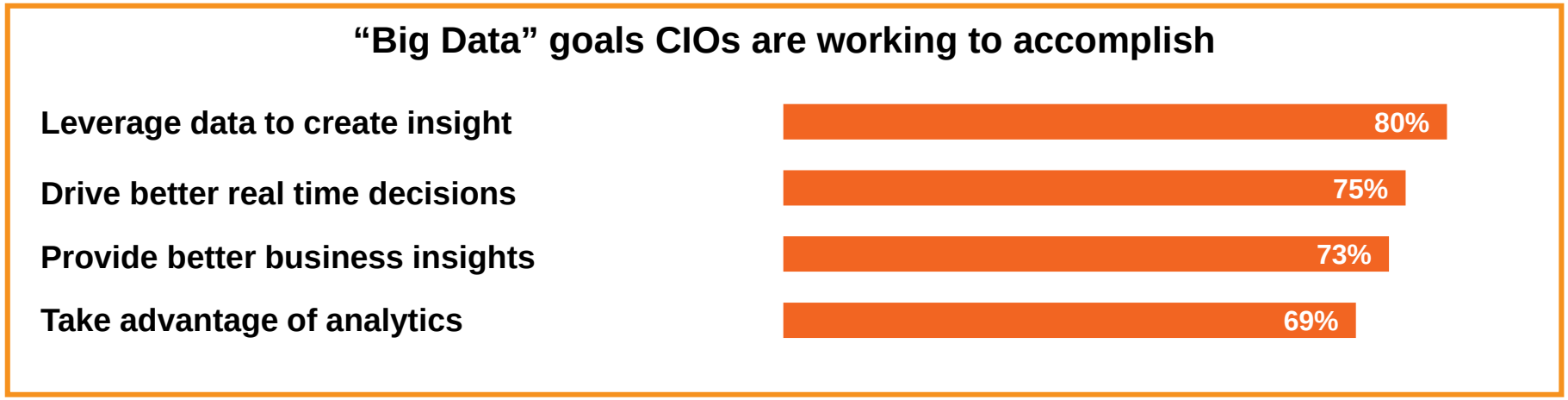
# 2011 – The Year of the Security Breach

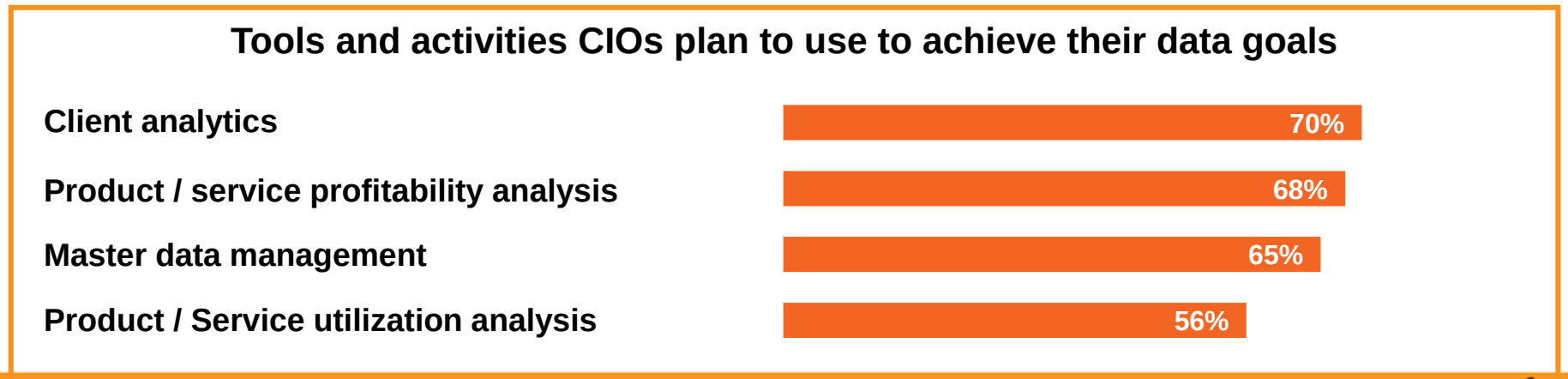


# CIO visionary plans are evolving: business intelligence and analytics remain at the top.



# Big Data, what to do with it, and how to use it are top-of-mind issues for Transform mandate CIOs



# Security challenges are impacting innovation

## External threats

Sharp rise in external attacks from non-traditional sources

- Cyber attacks
- Organized crime
- Corporate espionage
- State-sponsored attacks
- Social engineering

## Internal threats

Ongoing risk of careless and malicious insider behavior

- Administrative mistakes
- Careless inside behavior
- Internal breaches
- Disgruntled employee actions
- Mix of private / corporate data

## Compliance

Growing need to address an increasing number of mandates

- National regulations
- Industry standards
- Local mandates

**Impacting innovation**

**Data Explosion**

**Business Analytics**

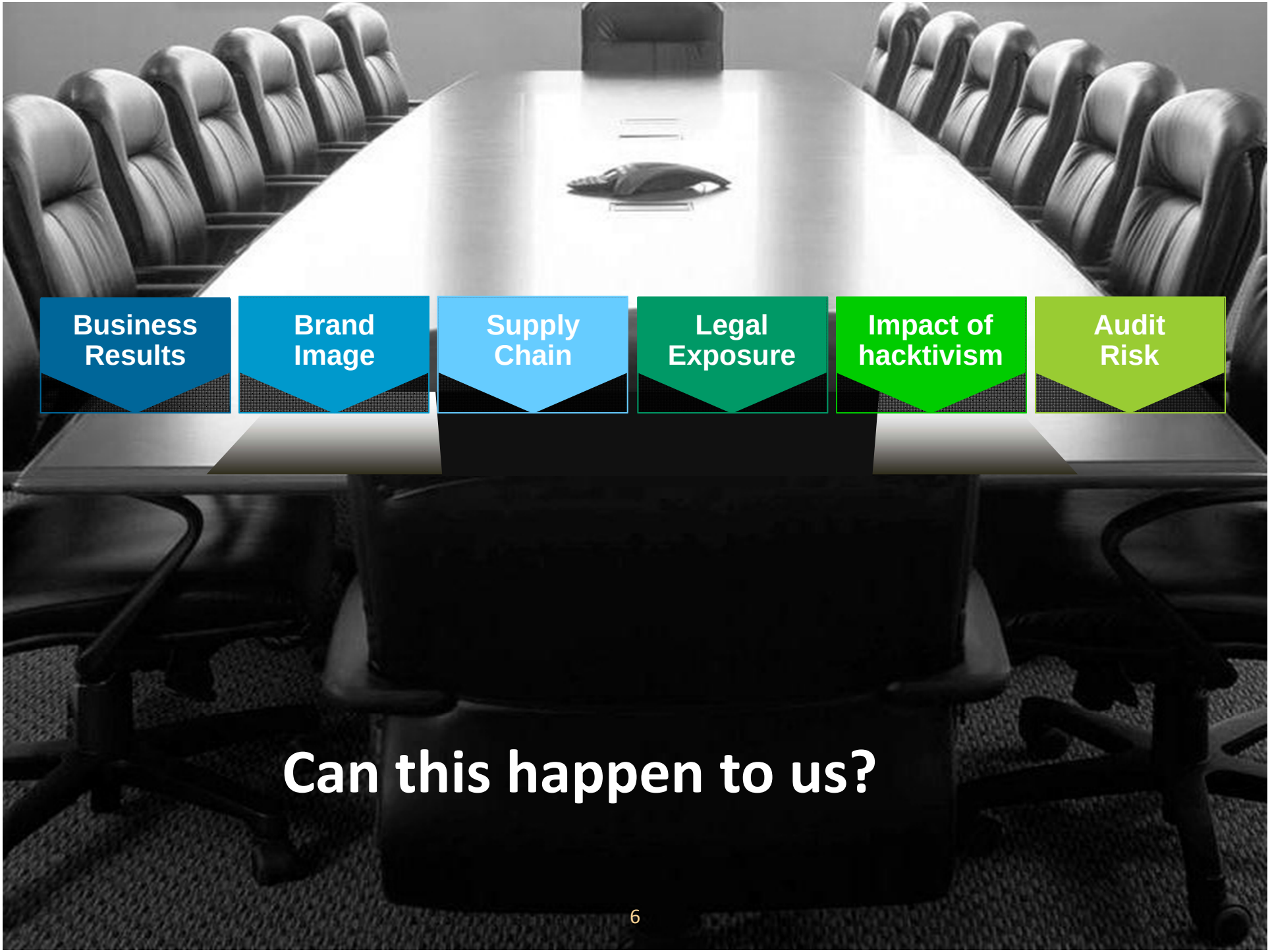
**Consumerization of IT**

**Mobile Computing**

**Social Business**

**Everything is Everywhere**

**Cloud Computing**




# Can this happen to us?

# Companies Will Have To Embrace Cyber Security Issues

Smart Supply Chains

Smart Countries

Smart Retail

Smart Water Management

Smart Weather

Smart Energy Grids

INSTRUMENTED

INTERCONNECTED

INTELLIGENT

Smart Oil Field Technologies

Smart Regions

Smart Healthcare

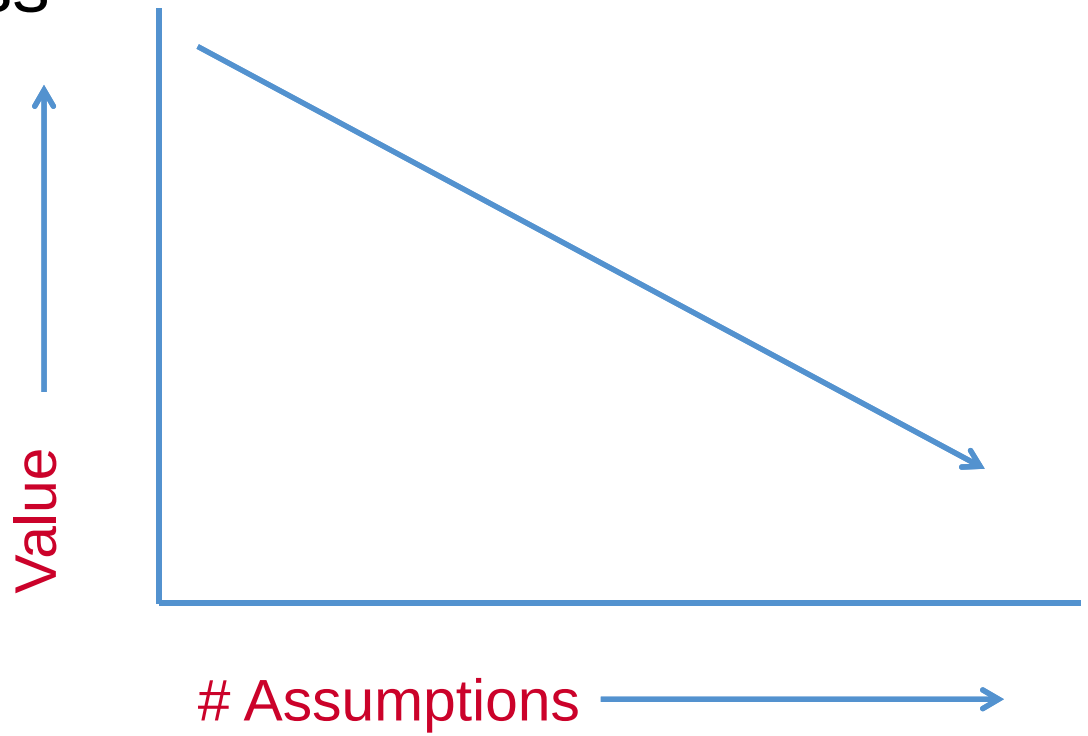
Smart Traffic Systems

Smart Cities

Smart Food Systems

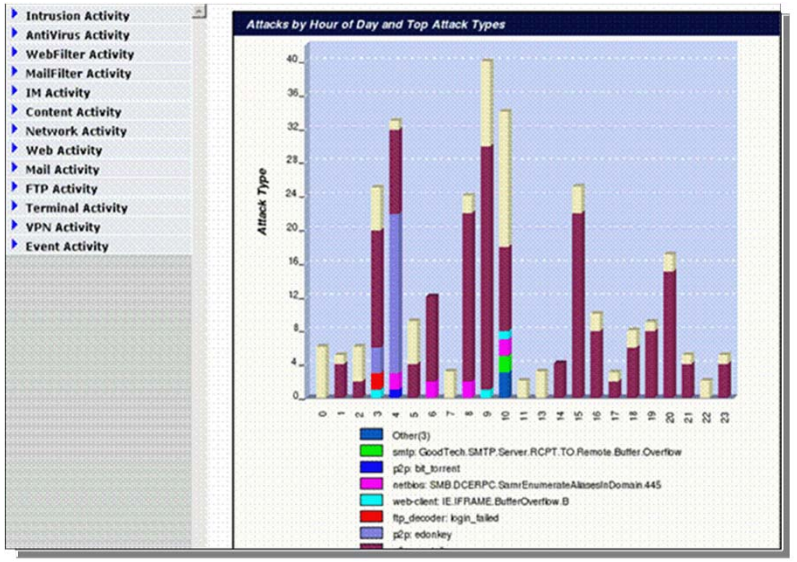
# Security Metrics - Why it is Really Hard

- Annualized Expected Loss
- Risk
- ROI
- TCO



# Cyber Security Metrics – the early days

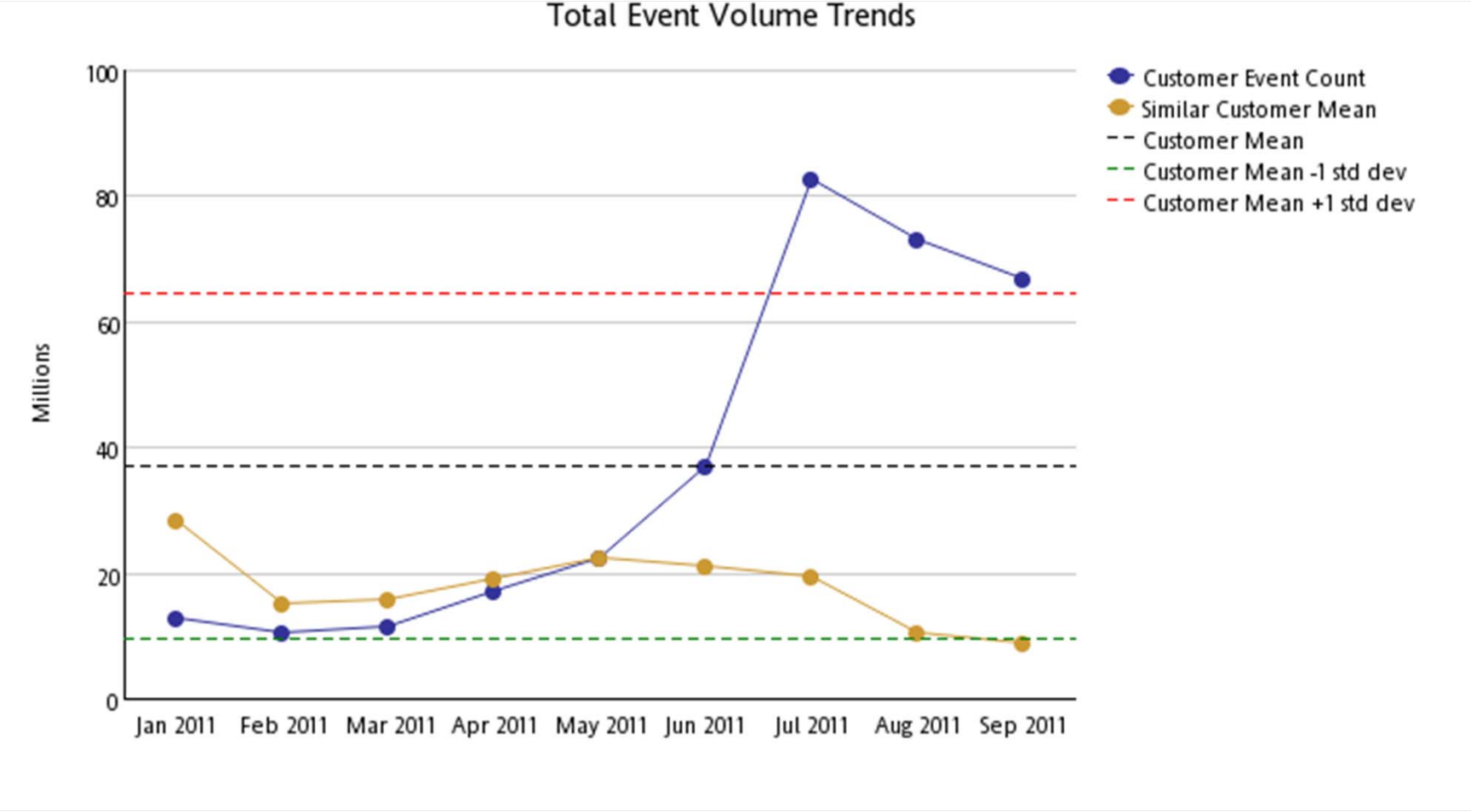
- # Attacks
- # Vulnerabilities
- # Virus Outbreaks
- Legitimate Email Traffic Analysis
- Password Strength
- Platform Compliance Scores
- Patch Latency



# Things that Execs Care About

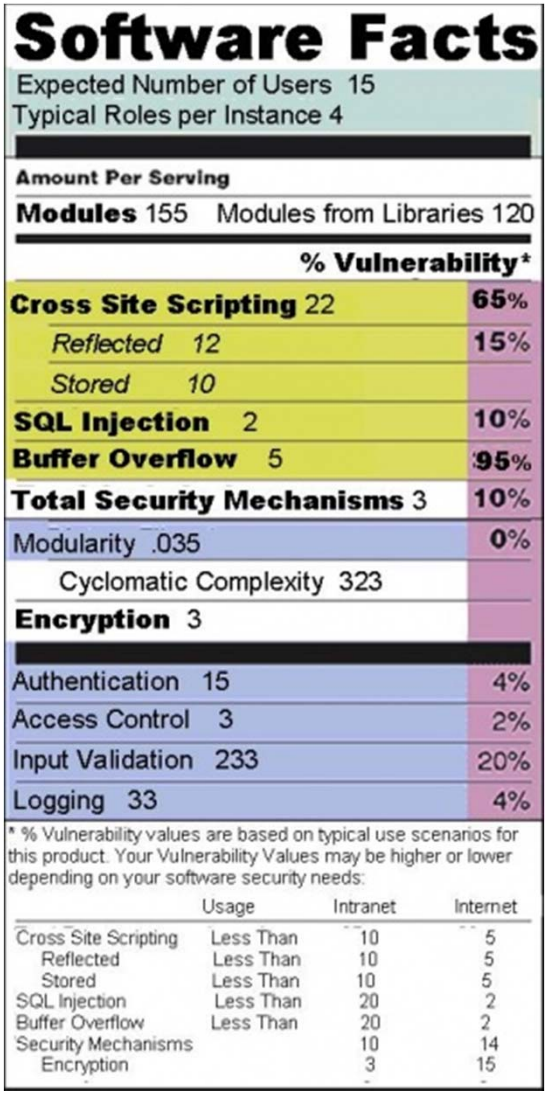
- Don’t talk to them about Security Metrics
- Do talk to them about business
- Do security metrics improve operations or financials,or customer satisfaction?
- Are we doing what is reasonable and expected?
- Are there things that make us unique?
- How can we do a nice job, how much spending is enough?


# An Improvement: Event Counts…but with comparative context.



# Security Metrics

- What makes a good metric?
  - Specific
  - Measurable
  - Attainable
  - Repeatable
  - Time dependent
- Larger Goals of Security Metrics
  - Are we more secure today than we were before?
  - How do we compare to others in this regard?
  - Are we secure enough?



**Software Facts**

Expected Number of Users 15
Typical Roles per Instance 4

**Amount Per Serving**

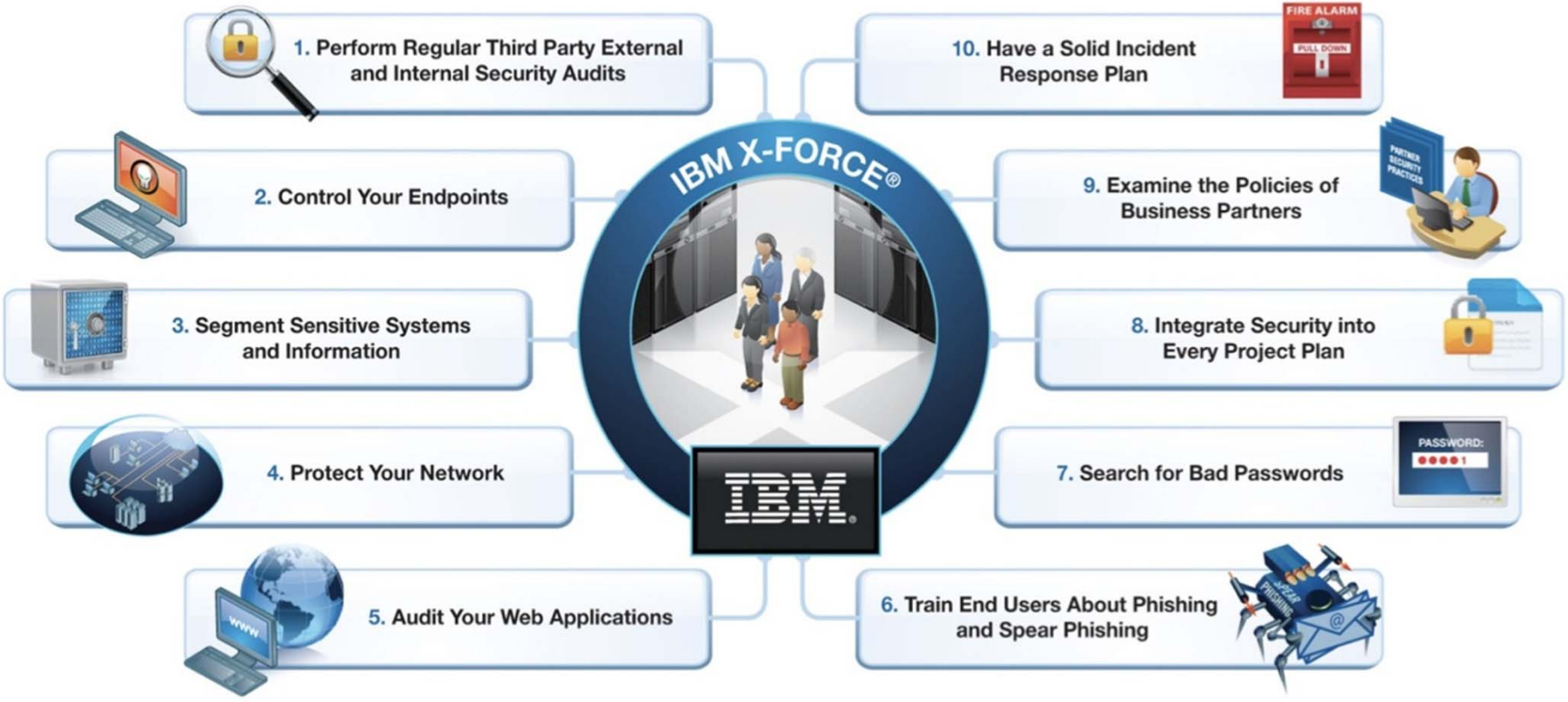
**Modules** 155 Modules from Libraries 120

| | **% Vulnerability*** |
|---|---|
| **Cross Site Scripting** 22 | **65%** |
| *Reflected* 12 | **15%** |
| *Stored* 10 | |
| **SQL Injection** 2 | **10%** |
| **Buffer Overflow** 5 | **95%** |
| **Total Security Mechanisms** 3 | **10%** |
| Modularity .035 | **0%** |
| Cyclomatic Complexity 323 | |
| **Encryption** 3 | |
| Authentication 15 | 4% |
| Access Control 3 | 2% |
| Input Validation 233 | 20% |
| Logging 33 | 4% |

* % Vulnerability values are based on typical use scenarios for this product. Your Vulnerability Values may be higher or lower depending on your software security needs:

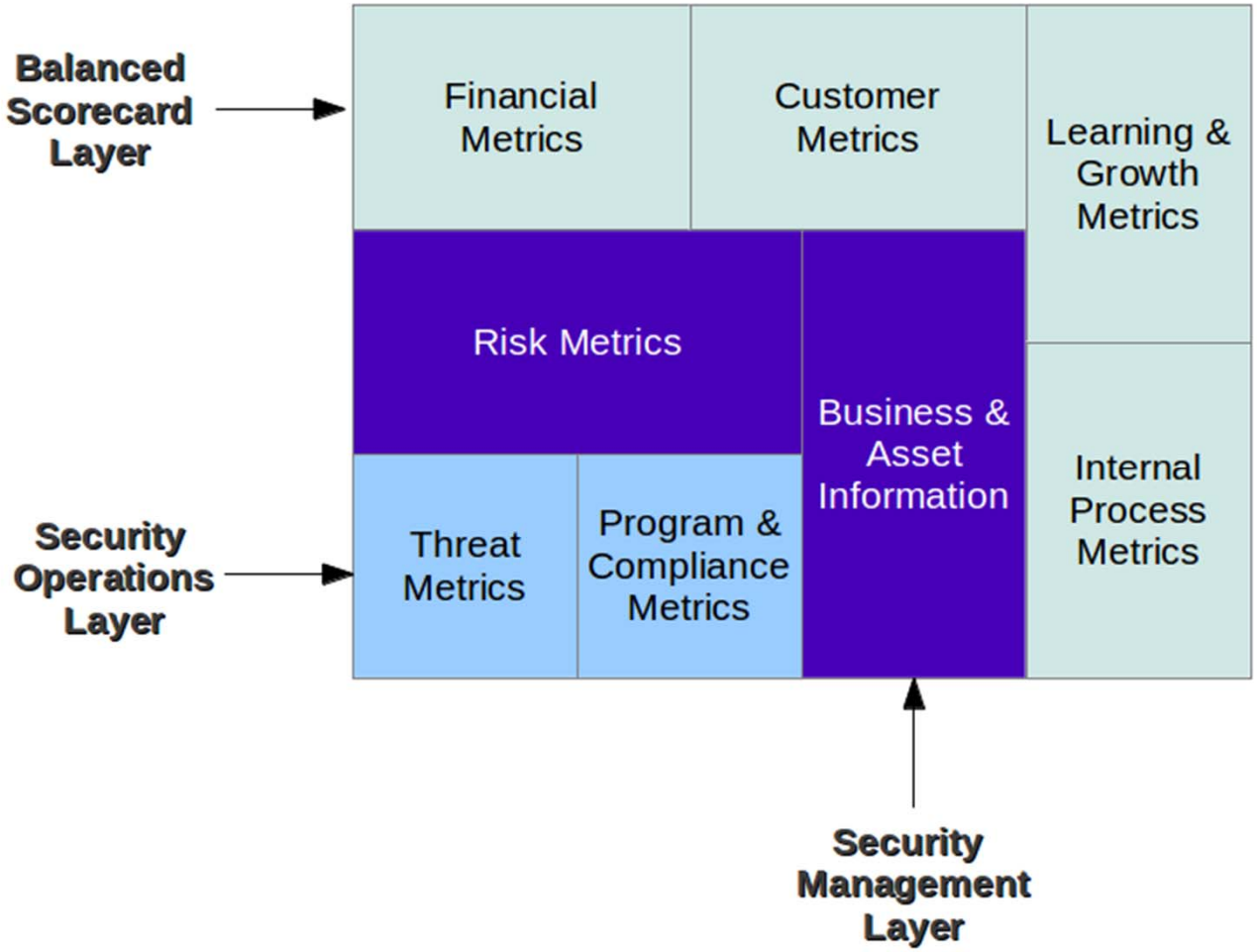
| | Usage | Intranet | Internet |
|---|---|---|---|
| Cross Site Scripting | Less Than | 10 | 5 |
| Reflected | Less Than | 10 | 5 |
| Stored | Less Than | 10 | 5 |
| SQL Injection | Less Than | 20 | 2 |
| Buffer Overflow | Less Than | 20 | 2 |
| Security Mechanisms | | 10 | 14 |
| Encryption | | 3 | 15 |

# Security is not just a technical problem, but also a business challenge




Source: IBM X-Force® Research and Development

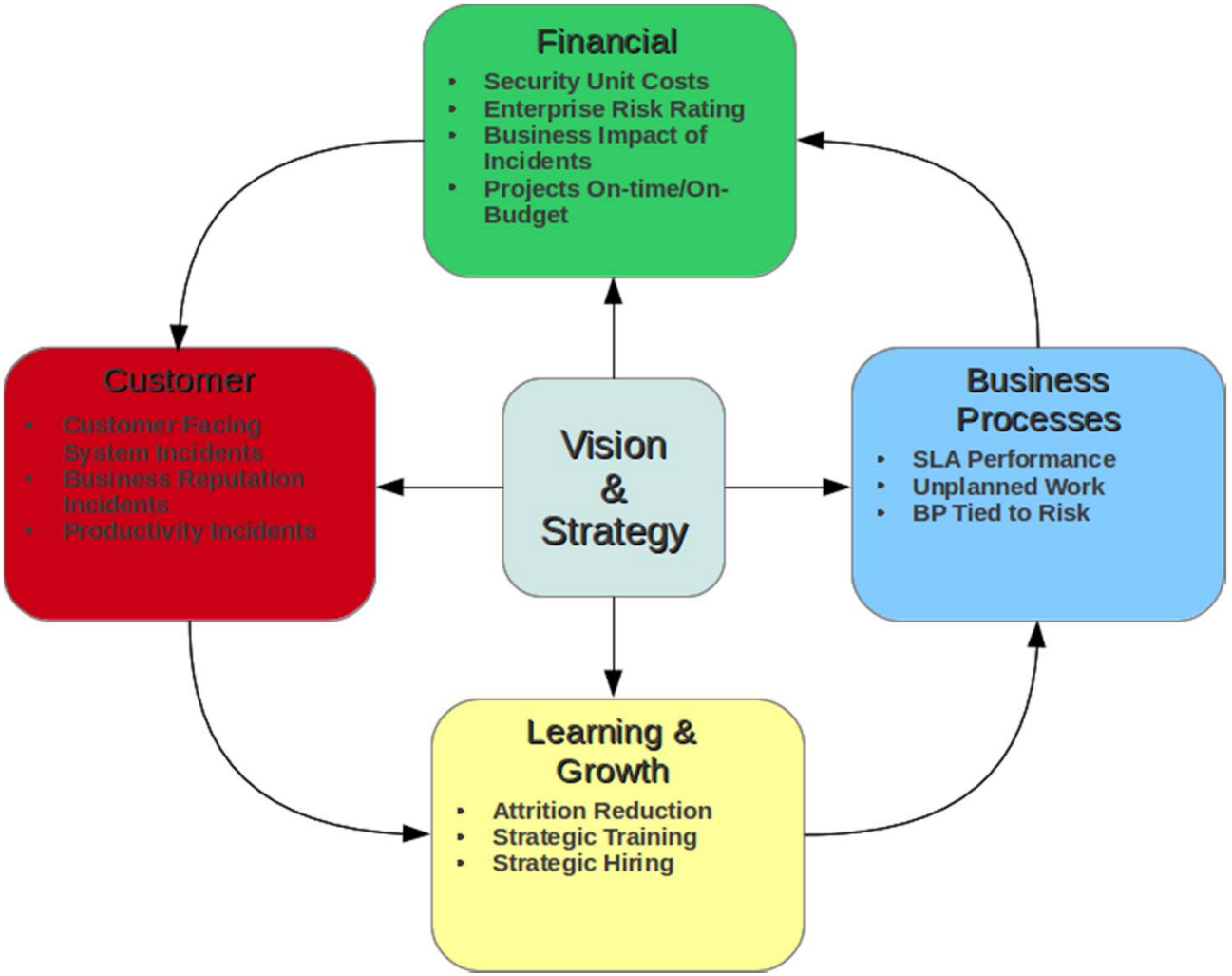
# The Building Blocks of a Boardroom Ready Metrics Program



# Example Metrics for Security Metrics Building Blocks

- Threat Metrics
  - % of Blocked Attacks Targeting Vulnerable Systems
  - Attacks Targeting High Severity Vulnerabilities
- Program & Compliance Metrics
  - % of Security Controls with Current Policy
  - % of Business Units Covered by Security Controls
- Risk Metrics
  - Organization Risk Rating
  - % of Systems Susceptible to Compromise
- Business & Asset Information
  - CMDB Information
  - Asset Value Information

# Balanced Scorecard to Communicate Security Metrics in Business Terms



# End to End Security Metrics Example: Patch Management

- Threat Metric + Program/Compliance Metric = Number of Systems susceptible to compromise over period of time(Risk Metric):
- Threat Metric: # of observed attacks targeting high severity vulnerabilities.
- Program/Compliance Metric: Mean time to patch high severity vulnerabilities
- Risk Metric + Business/Asset Information = Balanced Scorecard Metric:
- **Customer:**
- Customer Facing Systems <= 5% Vulnerable Systems
- **Business Process:**
- Business Units with <= 5% Vulnerable Systems
- 90% of Business Units Integrated into Enterprise Patch Management Initiative
- **Financial:**
- Reduce Security Program Spend by 10% Through Implementation of Enterprise Patch Management
- **Learning & Growth:**
- % of Target Employees Completed Enterprise Patch Management System Training

# Actions


1. Start with what you have.
2. Turn what you have into something in line with business objectives.
3. Think … SO What?
4. Be well rounded in what you report

5. Acknowledge the emerging business threat