Where is the true value in Security and how do you make it deliver Privacy?

February 2014

Experience the commitment®

…….any effort to protect private infrastructure and assets—whether physical or virtual—“**is more a matter of business models and regulation … than of technology.**”

Ross Anderson,
Professor of Security Engineering
University of Cambridge,

CGI

Experience the commitment®

It’s all about risk management

- Clients are keen to understand the risk to their organization:
  - Strategic Risk
  - Financial Risk
  - Reputational Risk
  - IP Risk
  - Identity breach Risk
  - Regulatory Risk (SOX, Privacy Regs etc.)
  - Corporate Liability
  - Availability Risk
  - Hostile geo-political Risk

I need to understand the possible risk to my business (impact on profit, brand reputation)and how to manage it

There are four major categories of dealing with risk:

- Avoidance (eliminate, withdraw from or not become involved)
- Reduction (optimize – mitigate)
- Sharing (transfer – outsource or insure)
- Retention (accept and budget)

Challenges in managing the risk

- **Changing threats:** increasingly dynamic and advanced threats
- **Limited IT resources:** these may not be IT security staff – strong IT security personnel have become costly to hire and retain
- **Demonstrating value:** Pressure to demonstrate risk reduction, compliance and adherence to best practices
- **Increasing complexity:** Threat and risk complexity leading to increased technology and process complexity
- **Increased expenditure:** training and capital expenditure increases while value over time quickly decreases
- **Operating costs:** need to reduce operating costs while improving services
- **Need to be ahead of the threat** – proactive versus reactive

Because we put cyber on the front of it, is it new?

Cyber Crime Anatomy

How to measure risk management success

- Cyber security model needs to be risk based
  - No silver bullet or infinite funding model
- Risk = Threat x Vulnerability x Impact (Not new)
- Can't change the threat
- Can change the vulnerability (lots of definitions and therefore options)
  - *A weakness in design, implementation, operation or internal control* (ISACA)
- Can reduce the impact
  - *greatest reduction in data breach costs by having a strong security posture, incident response plan and CISO appointment (Ponemon)*
- Determine KPI's

Global Threat – Global SOC

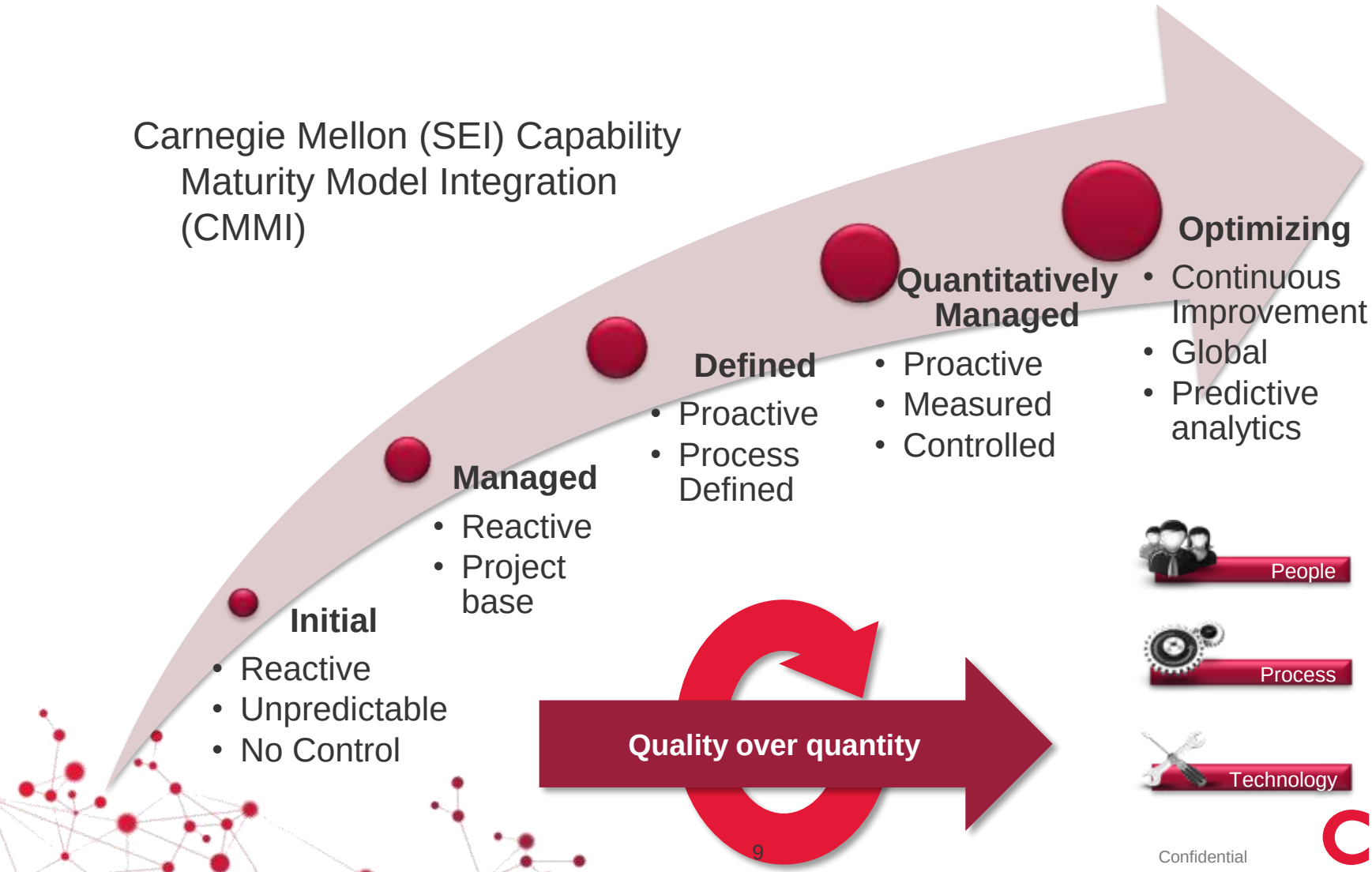
GMSS Portal


CGI Global Managed Security Services
Logo Client
(150px X 70px)
Global Dashboard
Service Reports
Client Documents
Service Portfolio
Contact Us
Help
Service Dashboards
HIDS
NIDS
Log
Inc. & RFI
MSS ▸ John Hancock ▸ Global Dashboard
Global Managed Security Services
We detected
402
Threats on your network last day
We detected
19
High severity NIDS events last day
We detected
2
High severity HIDS events last day
There are
1
Incidents or RFIs opened
Top 10 countries by activity detected
John Hancock
Global
Day
Week
Month
RSS
IT Security News
Google Releases Google Chrome 31.0.1650.63
09/12/13 11:56 AM
US-CERT
Original release date: December 09, 2013
Google has released Google Chrome 31.0.1650.63 for Windows, Mac, Linux and Chrome Frame to address multiple vulnerabilities. These vulnerabilities could allow a remote attacker to hijack a web session, spoof the address bar or cause a denial of service condition.
US-CERT encourages users and administrators to review the Google Chrome Release blog entry and follow best practice security policies to determine which updates should be applied.
This product is provided subject to this Notification and this Privacy & Use policy.
Microsoft Releases Advance Notification

Security Maturity: based on CMMI

Implement Continuous Process Improvement

Carnegie Mellon (SEI) Capability Maturity Model Integration (CMMI)



At the business level

Enable business

- Develop security services for innovative business models and new technologies

Build a trust relationship

- Report regularly on evidences & trends
- Define security service catalog for projects

Manage risks proactively

- Carry out risk assessment and manage vulnerabilities
- Implement pro-actively security measures

Comply with given standards

- Enforce laws & regulations
- Define & comply with corporate rules

React to audit findings

- Fix red issues raised by auditors efficiently
- React to major incidents

CGI

Privacy / Security Expertise

PIPEDA | FIPPA | HIPAA | PIPA

Alignment to Legislative Requirements

Privacy Management Framework

Privacy Law

Personal Info Management

27001 | SOX | GLB | PCI DSS

Performance against Security Control Objectives

Reporting Engine

Regulatory Standards

SIEM Engine

Compliance dashboard

Global Threats | Asset Vulnerability | Client Response | Log Monitoring, Alerting and Notification

Normalization & Correlation Engine

Optional Service Components

SIEM Engine

Security Information Mgmt

Log Browsing | High Availability | Custom Adapters | Activity Reports | Long Term Archival

Log Aggregation

Optional Service Components

Base Service

Security Event Log Mgmt

Firewall | IDS | AV | URL | Etc.

Firewall | IDS | AV | URL | Etc.

Performance

Fault

Security Component Mgmt

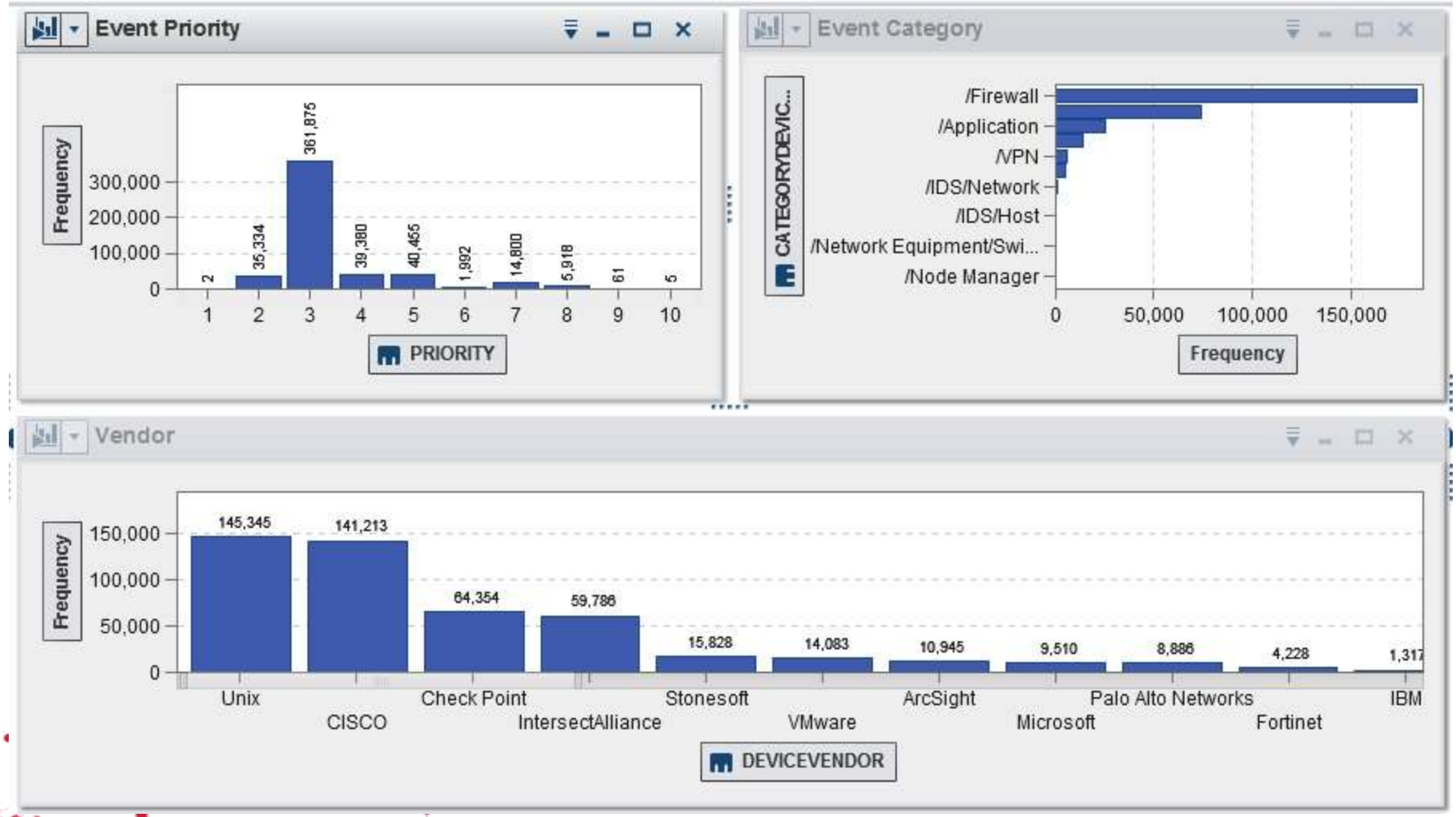
CGI

SAS Analytics – Visual Analyzer

Modelling and analyzing current security posture

Predicting future security requirements

Business Intelligence and Showing Value



Thank You

CGI