Security’s Role in Enterprise Risk Management

Jeff Spivey, CRISC, CPP, PSP, ISACA International Board of Directors
jspivey@srmsig.com
Global debt hits all-time high of $152 trillion as IMF warns of world-wide economic stagnation
Enterprise Risk Management (ERM) is defined as comprehensive risk management that allows corporations to identify, prioritize, and effectively manage their critical risks. An ERM approach integrates risk solutions into all aspects of the business practices and decision-making processes. With an ERM solution, companies have a uniform approach aligned with their strategies and objectives. ERM is a process that is continuously evaluated to ensure that companies effectively identify and manage risks of all types.

- Comprehensive
- Identify, prioritize, effectively manage critical risks
- Integrated risk solutions
- ALL aspects of the business practices and decision-making
- Align Strategies with Objectives
- Continuously evaluated
Risk and Opportunity

Security’s ONLY Role is to ENABLE the Organization
Criteria:
Request For Comment: Enterprise Risk Management Analysis For Credit Ratings Of Nonfinancial Companies

Primary Credit Analyst:
Steven J. Dreyer, New York (1) 212-498-7187, steven_dreyer@standardandpoors.com

Secondary Credit Analyst:
David Ingram, New York (1) 212-498-7104; david Ingram@standardandpoors.com
Is ERM here to stay?

The use of ERM has nearly doubled in just one year.
Traditional Risk Management

- Risk Identification
- Loss Control
- Claims Analysis
- Insurance and Risk-Transfer Methods
Progressive Risk Management

Traditional +

- Alternative Risk Financing
- Business Continuity
- Total Cost of Risk
- Education and Communication
Strategic Risk Management

Traditional +

Progressive +

- Enterprise-wide Risk Management
- Indexing of Risk
- Use of Technology
<table>
<thead>
<tr>
<th>Category</th>
<th>Risk Factor</th>
<th>Strategic</th>
<th>Traditional</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hazard Risk</td>
<td>Property</td>
<td>3%</td>
<td></td>
</tr>
<tr>
<td></td>
<td>General Liability</td>
<td>4%</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Auto</td>
<td>2%</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Terrorism</td>
<td>23%</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Workers Compensation</td>
<td>13%</td>
<td></td>
</tr>
<tr>
<td>Operational Risk</td>
<td>Regulatory/Compliance Risk</td>
<td>15%</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Technology/E-Risk</td>
<td>19%</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Absenteeism/Total Absence Management</td>
<td>14%</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Environmental Risk</td>
<td>18%</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Employment Practices Liability</td>
<td>4%</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Business Continuity/Crisis Management Risks</td>
<td>32%</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Intellectual Property</td>
<td>24%</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Products Liability</td>
<td>8%</td>
<td></td>
</tr>
<tr>
<td>Strategic Risk</td>
<td>Human Capital</td>
<td>19%</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Political Risk</td>
<td>33%</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Brand/Reputation</td>
<td>30%</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enterprise Risk</td>
<td>43%</td>
<td></td>
</tr>
<tr>
<td>Financial Risk</td>
<td>Credit Risk</td>
<td>12%</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FX/Commodity Risk</td>
<td>14%</td>
<td></td>
</tr>
</tbody>
</table>
Brand and regulatory compliance are rated top exposures by both the C-suite and risk managers; views diverge for human capital and technology risks.

### Exposure Risks Ranked

<table>
<thead>
<tr>
<th>Risk Category</th>
<th>C-Suite</th>
<th>Risk Managers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brand Reputation</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Human Capital</td>
<td>2</td>
<td>8</td>
</tr>
<tr>
<td>Regulatory Compliance</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Business Continuity</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>Technology/E-Risk</td>
<td>5</td>
<td>7</td>
</tr>
<tr>
<td>Property</td>
<td>8</td>
<td>4</td>
</tr>
<tr>
<td>Workers Compensation</td>
<td>9</td>
<td>5</td>
</tr>
</tbody>
</table>

- **Ranked Above 5 (Not Top 5)**
Business Impact of Security Incidents

- Financial losses: 37.5%
- Intellectual property theft: 31.8%
- Brand/reputation compromised: 31.2%
- Fraud: 15.8%
- Legal exposure/lawsuit: 12.2%
- Loss of shareholder value: 11.3%
- Extortion: 7.1%

Mature risk management drives financial results

(E&Y, 2012)

Compound annual growth rates 2004-11* by risk maturity level

- Top 20%
- Middle 60%
- Bottom 20%

Revenue:
- Top 20%: 16.8%
- Middle 60%: 8.3%
- Bottom 20%: 10.6%

EBITDA:
- Top 20%: 20.3%
- Middle 60%: 9.5%
- Bottom 20%: 7.4%

EBITDA/EV:
- Top 20%: 4.1%
- Middle 60%: 2.5%
- Bottom 20%: 2.1%
“C-Suite Slipping on Information Security”

CFO Magazine

- **Security’s responsibility** to tell the story - NOT management’s to have to ask
- Continuously inform the C-Suite and ERM owners of **Security Risk, Impact and Likelihood** - in the same context as all other risk are reported - to allow apples to apples
- Speak the language of the C-Suite → $$
- Answer the “SO WHAT” question
• “...if each part of a system is made to operate as efficiently as possible, the system as a whole will not operate as effectively as possible. The performance of a system depends more on how its parts interact than on how they act independently of each other”

• Russell Ackoff,
COBIT 5 Enabling Processes

Processes for Governance of Enterprise IT

Evaluate, Direct and Monitor
- EDM01 Ensure Governance Framework Setting and Maintenance
- EDM02 Ensure Benefits Delivery
- EDM03 Ensure Risk Optimisation
- EDM04 Ensure Resource Optimisation
- EDM05 Ensure Stakeholder Transparency

Align, Plan and Organise
- APO01 Manage the IT Management Framework
- APO02 Manage Strategy
- APO03 Manage Enterprise Architecture
- APO04 Manage Innovation
- APO05 Manage Portfolio
- APO06 Manage Budget and Costs
- APO07 Manage Human Resources
- APO08 Manage Relationships
- APO09 Manage Service Agreements
- APO10 Manage Suppliers
- APO11 Manage Quality
- APO12 Manage Risk
- APO13 Manage Security

Build, Acquire and Implement
- BAI01 Manage Programmes and Projects
- BAI02 Manage Requirements Definition
- BAI03 Manage Solutions Identification and Build
- BAI04 Manage Availability and Capacity
- BAI05 Manage Organisational Change Enablement
- BAI06 Manage Changes
- BAI07 Manage Changes Acceptance and Transitioning
- BAI08 Manage Knowledge
- BAI09 Manage Assets
- BAI10 Manage Configuration

Deliver, Service and Support
- DSS01 Manage Operations
- DSS02 Manage Service Requests and Incidents
- DSS03 Manage Problems
- DSS04 Manage Continuity
- DSS05 Manage Security Services
- DSS06 Manage Business Process Controls

Processes for Management of Enterprise IT

Monitor, Evaluate and Assess
- MEA01 Monitor, Evaluate and Assess Performance and Conformance
- MEA02 Monitor, Evaluate and Assess the System of Internal Control
- MEA03 Monitor, Evaluate and Assess Compliance with External Requirements
Risk Scenario Components

- **Event**: Disclosure, Interruption, Modification, Theft, Destruction, Ineffective design, Ineffective execution, Rules and regulations, Inappropriate use.

- **Asset/Resource**: People and organisation, Process, Infrastructure (facilities), IT infrastructure, Information, Applications.

- **Threat Type**: Malicious, Accidental/error, Failure, Natural, External requirement.

- **Actor**: Internal (staff, contractor), External (competitor, outsider, business partner, regulator, market).

- **Time**: Duration, Timing of occurrence (critical, non-critical), Timing to detect.
Threat intelligence is a key process to add to Risk Management

• Security teams must be able to rapidly and effectively translate large volumes of threat information into intelligence to help detect threats and protect the business.

• Organizational specific threat intelligence is a key process that needs to be managed

• Operationalized threat intelligence will benefit a broad set of internal consumers

• Threat intelligence platform to harness the power of threat intelligence and translate threat intelligence into action.

• Proactively protect the business from advanced threats,
Chief Information Security Officer

• Reporting Structure?
CLUELESS IN THE Boardroom

Our exclusive research shows that boards of directors still don’t understand IT. It’s your job to fix that!
Myth #1: We know what cloud computing is.

51% of respondents to a 2012 CITRIX survey believed that stormy weather can interfere with cloud computing.
Cloud Controls Matrix Tool

- Controls derived from guidance
- Mapped to familiar frameworks: ISO 27001, COBIT, PCI, HIPAA, FISMA, FedRAMP, Countries
Emerging technologies will change everything – how we work, how we live, how we communicate

• Mega Trends* are global, sustained and macro economic forces of development that impact business, economy, society, cultures and personal lives thereby defining our future world and its increasing pace of change

Of the Top 10 Mega Trends* to 2020, 8 have significant emerging technology components

*Frost & Sullivan Top 10
Emerging Trends → Emerging Risks

• Urbanisation
• Smart is the New Green
• Social Trends
• Economic Trends
• Connectivity & Convergence
• Innovating to Zero (Gates: Mega Vision of a zero concept world with zero emissions, zero accidents, zero fatalities, zero defects, and zero breaches of security)
• New Business Models
• Health, Wellness and Wellbeing
• Homecentering
• Tech Vision 2020
Emerging technologies will be the dominant driver of disruptive change for the foreseeable future, bringing significant opportunities and threats.

In the race to the future, organizations that manage risk for the right emerging technologies will better survive and prosper.

— those that don’t, will NOT

So What?
Generic Approaches to Organization Security

- Silos of Independence: Little or no communication or coordination
- Councils of Collaboration: Periodic, ad hoc and incident-focused
- Unified Organization: Formal, structured and aligned
Security Roles

- Information security
- Disaster/business continuity
- Risk assessments
- Security technology

- Incident response
- Protection of people, property & tangible assets from loss, destruction, theft, alteration or unauthorized access
- Investigations

- Digital asset security

- Inspection procedures

- Independent controls & assessments
- Internal/external regulatory compliance
- Risk management

Enterprise Risk Management
Changes Ahead for Security Professionals

- Cybercrime failures will result in major liability judgments.
- The public & private sector will formally share infrastructure protection roles.
- CSOs will assume responsibility for all operational risks.
- Security will be subsumed into ERM and Finance/CROs will predominate.
- Certification & licensing will be required for security professionals.

The public & private sector will formally share infrastructure protection roles.
Traditional Security

Personnel Security
- Policy & Procedures
  - Pre-Employment Background Verification
  - Employee/Manager Security Awareness Training & Education
  - Business Travel Advisories & Emergency Response
  - Key Executive Protection & Expatriate Support
  - Workplace Violence Prevention, Training & Support

Physical Security
- Policy & Procedures
  - Risk Assessment & Physical Security Standards
  - Protective Services & Guard Operations
  - Alarm Monitoring (Fire, Security & Critical Systems)
  - Security Technology Design, Engineering, Integration & Service
  - Vendor and Contractor Controls

Loss Prevention Investigation
- Policy & Procedures
  - Business Practices
  - Team & Internal Administrative Inquiries
  - M&A & Due Diligence Inquiries
  - Fraud, Waste & Abuse Prevention, Detection, & Investigation
  - Security Incident Report Database & Investigation Case Management

Information Security
- Policy & Procedures
  - IP Asset Evaluation
  - IP Classification Management
  - Employee & Trade or Process Partner Disclosure Agreements
  - IP Protection Standards & Methods
  - Competitive Intelligence & Counter Intelligence

Computer Security
- Policy & Procedures
  - Information Systems & Network Access Management
  - Encryption & Key Management for Voice, Data & Video Information systems
  - Firewall Monitoring & Virus Protection
  - Telecommunications Security for PBX, Cellular & Voice Mail
  - Internet/Intranet, E-mail & Mobile computing

Business Continuity
- Policy & Procedures
  - Business Impact Analysis of Key Processes and Sites
  - Crisis Management Plan Development & Team Coordination
  - Business Continuity Plan Development & Maintenance
  - Disaster Recovery Plans for Data Center & Distributed Systems
  - Site Emergency Response Team Management
Extended Enterprise Risks

Joint Ventures

Parts

Services

Transportation

"Organization (Risk) Community"

Contract Manufacturing

Contract Design

Customers

Untrustworthy Cyber

Cyber

Parts

Services

Transportation

"Organization (Risk) Community"

Contract Manufacturing

Contract Design

Customers
Complex Protection Systems

- Too many pieces
- Few qualified personnel
- Lack of standards
- Lack of integrated safeguards
A Security Professional for All Seasons

- Business acumen
  - Diplomatic
  - Capable Project/Program Manager
  - Passion for learning
  - Adaptable
  - Adept at framing risk issues for management
  - Professional training
    - Certifications
  - Grounded in multiple protection disciplines

[ISACA Indonesia Chapter logo]
# Top Three Cybersecurity Game Changers

<table>
<thead>
<tr>
<th>Game Changer</th>
<th>Attributes</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Always-on Connectivity</strong></td>
<td>• Critical data and information are clustered in clouds.</td>
<td>Increases window of opportunity for attack</td>
</tr>
<tr>
<td></td>
<td>• Wi-Fi hotspots are growing.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Work systems are easily accessed at home or on the go.</td>
<td></td>
</tr>
<tr>
<td><strong>IT-centric Business and Society</strong></td>
<td>• Online systems are the new critical infrastructures.</td>
<td>Increases number of business processes that can be targeted</td>
</tr>
<tr>
<td></td>
<td>• Society’s reliance on “always-on” creates wider windows of attack time.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• There is no paper fallback in emergencies.</td>
<td></td>
</tr>
<tr>
<td><strong>New Class System by Technology Skills</strong></td>
<td>• Mobile device features remain a mystery to many.</td>
<td>Increases role of human error in enabling cybercrime</td>
</tr>
<tr>
<td></td>
<td>• Fewer digital natives have deep IT skills.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• New apps and operating systems favor convenience over user control.</td>
<td></td>
</tr>
</tbody>
</table>

For more information, download ISACA’s *Transforming Cybersecurity Using COBIT 5* at [www.isaca.org/cybersecurity-cobit](http://www.isaca.org/cybersecurity-cobit).
ISACA
International Board of Directors

Jeff Spivey, CRISC, CPP, PSP
President
Security Risk Management, Inc.
jspivey@srmsig.com
+1 704-521-8401
Security Risk Management Framework
Why focus on defining a risk management framework?

The Security team has created and implemented a structured methodology that lets us quantify risk, establish risk appetite/tolerance, identify and prioritize controls, and establish a system of record to meet a multitude of legal and compliance obligations for our companies systems and information assets.
<table>
<thead>
<tr>
<th>CobiT's processes</th>
<th>Processes</th>
<th>Framework component affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Strategic plan definition</td>
<td>Planning and organization</td>
<td>Vision and principles</td>
</tr>
<tr>
<td>2. IT architecture design</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Definition of technological guidelines</td>
<td></td>
<td>Vision &amp; principles; security practices and technologies</td>
</tr>
<tr>
<td>4. Definition of IT operations and accountability schemes</td>
<td></td>
<td>Security operations</td>
</tr>
<tr>
<td>5. IT investment management</td>
<td></td>
<td>Business case</td>
</tr>
<tr>
<td>6. Internal communication of management guidelines</td>
<td></td>
<td>Change management and BU guidelines</td>
</tr>
<tr>
<td>7. Organization design/Human resource management</td>
<td></td>
<td>Organization and governance</td>
</tr>
<tr>
<td>8. Assurance of external IT requirements compliance</td>
<td></td>
<td>Linkages to other enterprise activities</td>
</tr>
<tr>
<td>9. Risk management</td>
<td></td>
<td>Various risk related components. Sections 2A to 2D</td>
</tr>
<tr>
<td>10 Project management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11: Data management/Quality management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>12 IT solution design</td>
<td>Acquisition and implementation</td>
<td></td>
</tr>
<tr>
<td>13 Application s/w development1</td>
<td></td>
<td>Security operations</td>
</tr>
<tr>
<td>14 Acquisition and maintenance of IT infrastructure</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15 Development and maintenance of IT processes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16 IT system installation and accreditation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>17 Change management</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1 Includes acquisition, personalization and maintenance
Linking CobiT's process to our IS&C risk management framework (2/2):

<table>
<thead>
<tr>
<th>CobiT's process</th>
<th>Framework component affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>18 Service level definition and management</td>
<td>Security operations</td>
</tr>
<tr>
<td>19 Third parties service management</td>
<td>Security operations</td>
</tr>
<tr>
<td>20 Performance and capacity management</td>
<td>Security operations</td>
</tr>
<tr>
<td>21 Assurance of continuity in IT processes</td>
<td>Security operations</td>
</tr>
<tr>
<td>22 System security management</td>
<td>Security operations</td>
</tr>
<tr>
<td>23 Cost accounting and allocation</td>
<td>Security operations</td>
</tr>
<tr>
<td>24 End-user training and education</td>
<td>Security operations</td>
</tr>
<tr>
<td>25 End-user support and advice</td>
<td>Security operations</td>
</tr>
<tr>
<td>26 Management of IT assets/equipment</td>
<td>Security operations</td>
</tr>
<tr>
<td>27 Problem management</td>
<td>Security operations</td>
</tr>
<tr>
<td>28 IT operations monitoring/supervision</td>
<td>Security operations; Compliance, metrics and reporting</td>
</tr>
<tr>
<td>29 Compliance with physical and environmental requirements</td>
<td>Compliance, metrics and reporting</td>
</tr>
<tr>
<td>30 Operations management</td>
<td>Security operations</td>
</tr>
<tr>
<td>31 IT process monitoring</td>
<td>Security operations</td>
</tr>
<tr>
<td>32 Evaluation of controlling processes</td>
<td>Compliance, metrics and reporting</td>
</tr>
<tr>
<td>33 Independent quality assurance</td>
<td>Compliance, metrics and reporting</td>
</tr>
<tr>
<td>34 Independent operation auditing</td>
<td>Compliance, metrics and reporting</td>
</tr>
</tbody>
</table>
Vision and Charter for Risk Management Framework

Vision statement

Emerge as cyber security leader in this industry

Details

- Deliver robust, efficient, proactive, adaptive and cost effective security solutions for all stakeholders (i.e., employees, customers)
- Lead and guide industry thinking in cyber security and risk management

Become a stronger business partner

Details

- Align to business strategy, needs and goals
- Shape business strategy/environment
- Balance technical/ business/financial needs
- Create constructive relationships and effective communications between business, security & partners

Mature our security capabilities

Details

- Build capability and capacity; Grow a critical mass of security technical/ management professionals
- Cascade security strategy into the company - Engender an environment and culture of “security first”
- Measure performance

SOURCE: Team analysis
## Guiding principles “The Backbone of our Strategy”

<table>
<thead>
<tr>
<th>Principle</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Least privilege</td>
<td>Users and system processes should be given the least authority and minimum access to resources required to accomplish a given task</td>
</tr>
<tr>
<td>Accountability</td>
<td>All significant system and process events should be traceable to the initiator</td>
</tr>
<tr>
<td>Minimum dependence on secrecy</td>
<td>Controls should still be effective even if an opponent knows of their existence and mode of operation</td>
</tr>
<tr>
<td>Control automation</td>
<td>Wherever possible, automatic controls should be used rather than controls that depend on human vigilance and behavior</td>
</tr>
<tr>
<td>Resiliency</td>
<td>Systems should be designed and managed so that in the event of breakdown or compromise only least possible damage and inconvenience are caused</td>
</tr>
<tr>
<td>Defense in depth</td>
<td>Controls should be layered such that if one layer of control fails, there is another different type of control at the next layer that will prevent a security breach</td>
</tr>
<tr>
<td>Approved exception</td>
<td>Policy exceptions should always have management approval</td>
</tr>
<tr>
<td>Secure emergency override</td>
<td>Controls must be bypassed only in predetermined and secure ways. Systems are most vulnerable when normal controls are removed for emergency maintenance or other similar reasons. There should always be procedures and controls to minimize the level of risk in these circumstances</td>
</tr>
<tr>
<td>Auditability</td>
<td>It must be possible for an independent expert to verify that the system conforms to the security policy. A necessary but not totally sufficient condition for this is that the system must be able to record security-related events in a tamper-resistant audit log</td>
</tr>
<tr>
<td>Practicality</td>
<td>Security levels need to be commensurate with the level of risk</td>
</tr>
<tr>
<td>Privacy</td>
<td>Employees should have no expectations of privacy related to internet and email usage</td>
</tr>
</tbody>
</table>

SOURCE: ISO 17799 and 27001 serve as a baseline
Framework for understanding and analyzing risk exposures

Risk identification
- Proactive threat profiling
- Real time threat detection
- Risks highlighted by metrics/dashboards
- Long term trends and implications for risk profile

Risk assessment
- Risk classification and likelihood
- Risk impact assessment

Risk levelling and prioritization
- Draft prioritization of risk
- Confirm and refresh priorities with senior management

Cross functional management involvement in risk exposure analysis

1 Conversation would likely include investment - risk tradeoffs
Framework for understanding and analyzing risk exposures (example)
Security will continue to play a role in both emerging and existing standards and regulations.

<table>
<thead>
<tr>
<th>Standards</th>
<th>Enterprise</th>
<th>Customer care</th>
<th>Transmission and distribution</th>
<th>Generation</th>
<th>Corporate</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Existing</strong></td>
<td>NERC, CIP, ISO 17799, ISO 27001¹</td>
<td>California SB 1386, SB 355, AB 1950²</td>
<td>WISE³</td>
<td>WISE</td>
<td>Sarbanes-Oxley</td>
</tr>
<tr>
<td><strong>Emerging</strong></td>
<td></td>
<td></td>
<td>NIST⁴ Smart grids</td>
<td>NERC CIP⁴, NIST</td>
<td>–</td>
</tr>
</tbody>
</table>

1. NERC is North American Electric Reliability Council; CIP is Critical Infrastructure Protection; ISO is International Organization for Standardization. 27001 is basically part 2 of 17799.
2. SB 1356 is California Security Breach Information act; SB 355 is California Anti-Phishing Act of 2005; AB 1950 is California Assembly Bill 1950 that requires organizations owning personal information to implement security measures.
3. WISE is Water Infrastructure Security Enhancement. It has several processes for physical security that may have IT Security implications.
4. PCI is Payment Card Industry Data Security Standard.
5. NIST is National Instutes of Standards and Technology.

SOURCE: McKinsey Research
Counter measure portfolio framework

Steps

**Generation**
- Create and compile options – damage potential vs. investment
- Create portfolio view

**Selection**
- Make risk exposure vs. investment level at the portfolio level
  - Approve actions
  - Accept residual risks
- Formulate and coordinate risk-mitigating actions

**Realization**
- Track realization of recommended actions and escalation when necessary
  - For example, temporarily lock down an IT service to address threat
- Manage exposure

**Portfolio Inputs**

- Risk exposure and prioritization
- Standards, legislation and regulation
- Security practices and technologies

1 Includes remediation tracking

SOURCE: Team analysis
Vulnerability Dashboard in Development

"Countermeasure portfolio framework"
Security metrics will plugged into both the enterprise risk and the IT report cards.

**Enterprise risk score card**

**IT score cards**

### Security metrics

1. Roadmap metrics (i.e., how we are doing on from-to journey)
2. Risks uncovered and mitigated; Residual risk
3. Compliance and Audits (e.g., items pending from SOX compliance)
4. Operating metrics (e.g., metrics highlighting service readiness)
5. Change management and talent development (i.e., key talent gaps)
6. Financial

**SOURCE:** Team analysis
SOURCE: Client interviews and team analysis
IT Security investments will be driven by a comprehensive investment case incorporating security and business factors.

- Risk exposure and prioritization
- Standards, legislation and regulation
- Security practices and technologies
  - Countermeasures portfolio
  - Management burden
  - Operations burden

- Business drivers
  - Case for IT security investments
  - IT security budget
    - Link investments to risk tolerance

SOURCE: Team analysis
Business case for security investments will require technical as well as business expertise.

While the ROI formulas are straightforward:

<table>
<thead>
<tr>
<th>Impact of risk × probability of risk</th>
<th>Number of incidents prevented by investment</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Number of incidents expected without investment</td>
</tr>
<tr>
<td>Risk mitigation ROI =</td>
<td>(Risk exposure × % risk mitigated) – cost of security investment</td>
</tr>
<tr>
<td></td>
<td>Cost of security investment</td>
</tr>
</tbody>
</table>

...they are not very easy to use:

- Estimating values for the factors of the ROI formula is not straightforward.
- There is no standard method for estimating risk exposure and mitigation effectiveness of investments in security.

Security business cases draw heavily upon individual capabilities and domain expertise.

Leveraging expert knowledge (e.g., by using the Delphi method) has produced reliable results.

SOURCE: McKinsey research
We will continue to evaluate IS&C’s structure and ensure that it is in sync with IS&C risk management framework.

A comprehensive study of the security organization would evaluate the following:
- Size (i.e., Do we have enough FTEs)
- Structure (i.e., Is the structure in line with security strategy?)
- Security expertise (i.e., both technical and management)
- Coverage (i.e., gaps in services/functions)
- Interfaces (i.e., with IT and non IT functions)

SOURCE: Team analysis
Governance model has three major components and needs to be tailor made for the organization.
## Current snapshot of high level security governance

<table>
<thead>
<tr>
<th>Board</th>
<th>Vision and principles</th>
<th>Understand risk exposure and prioritization</th>
<th>Standards, legislation and regulation</th>
<th>Security practices and technologies</th>
<th>Counter measure portfolio</th>
<th>Compliance, metrics and reporting</th>
<th>Business case (i.e., investments and ROI)</th>
<th>Organization &amp; governance</th>
<th>Change management and BU integration</th>
<th>Security operations</th>
<th>Linkages to other enterprise activities</th>
<th>Linkages to Partners &amp; suppliers</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Inform</td>
<td>Inform</td>
<td>Approve</td>
<td>Create</td>
<td>N/A</td>
<td>Create</td>
<td>Inform</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>2A</td>
<td>–</td>
<td>Inform</td>
<td>Inform</td>
<td>Approve</td>
<td>Create</td>
<td>Inform</td>
<td>–</td>
<td>Inform</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2B</td>
<td>–</td>
<td>Inform</td>
<td>Inform</td>
<td>Approve</td>
<td>Create</td>
<td>Create</td>
<td>–</td>
<td>–</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2C</td>
<td>–</td>
<td>Inform</td>
<td>Approve</td>
<td>Approve</td>
<td>Create</td>
<td>Create</td>
<td>–</td>
<td>–</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2D</td>
<td>–</td>
<td>Review</td>
<td>Approve</td>
<td>Review</td>
<td>Create</td>
<td>Create</td>
<td>–</td>
<td>–</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2E</td>
<td>Inform</td>
<td>Review</td>
<td>Review</td>
<td>Approve</td>
<td>Create</td>
<td>Inform</td>
<td>–</td>
<td>–</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>–</td>
<td>Inform</td>
<td>Approve</td>
<td>Create</td>
<td>N/A</td>
<td>Create</td>
<td>Approve</td>
<td>Inform</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>–</td>
<td>Review</td>
<td>Approve</td>
<td>Create</td>
<td>Inform</td>
<td>Inform</td>
<td>N/A</td>
<td>Inform</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>–</td>
<td>Approve</td>
<td>Review</td>
<td>Create</td>
<td>Inform</td>
<td>Inform</td>
<td>Inform</td>
<td>–</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>–</td>
<td>Inform</td>
<td>Inform</td>
<td>Approve</td>
<td>Create</td>
<td>Create</td>
<td>–</td>
<td>–</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>–</td>
<td>–</td>
<td>Approve</td>
<td>Create</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>–</td>
<td>–</td>
<td>Approve</td>
<td>Create</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**SOURCE:** Client interviews
Maintain a robust talent management strategy to grow security capabilities!

**Taxonomy of talent management**

<table>
<thead>
<tr>
<th>Elements</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
</tr>
<tr>
<td>II</td>
</tr>
<tr>
<td>III</td>
</tr>
<tr>
<td>IV</td>
</tr>
<tr>
<td>V</td>
</tr>
<tr>
<td>VI</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Core topics</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
</tr>
<tr>
<td>II</td>
</tr>
<tr>
<td>III</td>
</tr>
<tr>
<td>IV</td>
</tr>
<tr>
<td>V</td>
</tr>
<tr>
<td>VI</td>
</tr>
</tbody>
</table>

- Recruiting Strategy
  - Branding architecture and selection of key attributes
  - Attraction and selection processes for new hires
- Performance Management
  - Target setting and consequence management
  - Mid-year and target review
- Performance & Potential Review (PPR)
  - Potential discussion with focus on development
  - Individual development plan including follow-up
- Development
  - Leadership-level-oriented training programs
  - Overall training systematic with focus on on-the-job-training
- Succession/Changes in Position
  - Succession planning for critical jobs
  - Job rotation as key development tools
  - Mentoring
- Leadership System
  - Top management groups
  - Competency model/management
  - Formal requirements (skills, competencies for leadership level)
Designing a functional committee of senior partners to drive change:

- CIO lead 10+, cross functional senior leaders including legal
- Committee has final decision rights on IT security policy

**Committee inputs**
- Security best practices (e.g., size of email inboxes)
- Technology forecasts (e.g., 3rd party expert analysis)
- Security events (e.g., breaches)
- Security management framework

**Firm technology committee (decision body)**

**Committee output**
- IT security policies and decisions that can be enforced by technology

**Key success factors**

**Decision body**
- Vest decision making rights in cross functional executive governance body (e.g., FTC)
  - Allow/compel group to exercise rights
- Orchestrate initial FTC meetings to establish authority and bounds
- Ensure committee output takes meaningful steps forward

**IT**
- Establish clear guidelines on what is in scope for decision body
  - For example, strategic decisions are in scope but budgets are not
- Limit organizational debate on pros and cons of security measures
  - Decisions come from the governance body with explanation but limited feedback opportunity
- Be patient
  - Security changes take place over a long time and involve steps
- Be opportunistic
  - For example using an attack to rollout a new security solutions or policy

*SOURCE: McKinsey research and Team analysis*
The Influence Model: Change levers and lever categories

**Lever categories**
- Leadership actions
- Opinion shapers
- Interactions

**Talent management**
- Hiring
- Replacing
- Retaining

**Learning**
- On-the-job development
- Training
- Action learning

**Lever categories**
- Story development (includes all the key elements, e.g., values, strategy, case for change)
- Story delivery (across relevant levels, i.e., organizational, employee, functional)

**Mindset & behavior shifts**

- **Role-modeling**
  "I see superiors, peers and subordinates behaving in the new way"

- **Fostering under-standing and conviction**
  "I know what is expected of me – I agree with it, and it is meaningful"

- **Developing talent and skills**
  "I have the skills and competencies to behave in the new way"

- **Reinforcing with formal mechanisms**
  "The structures, processes and systems reinforce the change in behavior I am being asked to make"

**Lever categories**
- Organization structure
- Targets and metrics
- Management processes
- Business processes
- "Rewards, recognition and consequences"
- Information systems

SOURCE: McKinsey
Cyber security operational excellence is achieved by ensuring coverage of key elements (1/3)

6.1. Security policy management
6.2. Security services
6.3. Core processes
6.4. Technology, equipment, vendor management

SOURCE: Team analysis
Cyber security operational excellence is achieved by ensuring coverage of 4 key elements (2/3):

**6.1. Security policy management**
- Create detailed service catalogue to satisfy business needs and strategy
  - Customize services where needed (e.g., Business unit specific changes)
- Manage service lifecycle
  - Definition
  - Budgeting
  - Test
  - Deployment
  - Operations
- Define and enforce decision rights (e.g., Which services are opt in and which ones are compulsory)
- Operations
- Training
- Monitoring
- Audit

**6.2. Security services**
- Access rights and control
- Identification and authentication
- Encryption
- Incident detection and management
- Audit
- Recovery
- Administration
- Standards compliance

**6.3. Core processes**

**6.4. Technology, equipment, vendor management**

SOURCE: Team analysis
Appendix
Cyber security operational excellence is achieved by ensuring coverage of 4 key elements (3/3)

Sub components
- Setting and implementation
- Life cycle management

Sub components
- Define and implement processes for
  - Policy development and review
  - Service development and review
  - Monitoring of common operations
  - Audit and assessment
  - Define linkages to other PG&E processes

SOURCE: Team analysis
IT security services should map to it architecture layers

<table>
<thead>
<tr>
<th>Security services</th>
<th>Access</th>
<th>Authentication</th>
<th>Encryption</th>
<th>Detection</th>
<th>Audit</th>
<th>Recovery</th>
<th>Administration</th>
<th>Standards compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT architecture layers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application/ databases</td>
<td>▪ Service 1</td>
<td>▪ Service 2</td>
<td>▪ ...</td>
<td>▪ Service 1</td>
<td>▪ Service 2</td>
<td>▪ ...</td>
<td>▪ Service 1</td>
<td>▪ Service 2</td>
</tr>
<tr>
<td>▪ Applications ▪ Databases</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Centralized infrastructure</td>
<td>▪ Service 1</td>
<td>▪ Service 2</td>
<td>▪ ...</td>
<td>▪ Service 1</td>
<td>▪ Service 2</td>
<td>▪ ...</td>
<td>▪ Service 1</td>
<td>▪ Service 2</td>
</tr>
<tr>
<td>▪ Servers ▪ Mainframes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>▪ Routers ▪ Switches ▪ Cables</td>
<td>▪ Service 1</td>
<td>▪ Service 2</td>
<td>▪ ...</td>
<td>▪ Service 1</td>
<td>▪ Service 2</td>
<td>▪ ...</td>
<td>▪ Service 1</td>
</tr>
<tr>
<td>▪ Computing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>End-user computing</td>
<td>▪ Computers ▪ Notebooks ▪ Fax/phones</td>
<td>▪ Service 1</td>
<td>▪ Service 2</td>
<td>▪ ...</td>
<td>▪ Service 1</td>
<td>▪ Service 2</td>
<td>▪ ...</td>
<td>▪ Service 1</td>
</tr>
</tbody>
</table>

SOURCE: Team analysis
We need to clearly define roles, responsibilities and interfaces in areas of overlapping accountability

**SOURCE:** Team analysis

**ILLUSTRATIVE**

- Activity completely outside the scope of IT security
  - For example, non IT part of enterprise audit

- Security gets the activity started but relies on partner organization to execute
  - For example, inform physical security team of risk to data center gathered by horizon scan

- Security orchestrates activity and manages entire lifecycle
  - Guides entries process
  - Manages and ensures quality of end product
  - For example, ensure that we have the right security insurance

- Activity completely owned and managed by the group
  - For example, security audit
Partner classification is the first step in determining how and when to apply framework

Inside firewall?

Yes
Access levels?

Yes
Same as employees
Extend framework to partner

No
Limited
Apply variant/subset of IT security framework

Involvement level?

Yes
High
Apply variant/subset of IT security framework

No
Arms length
Analyze partner framework during selection/due-diligence

1 Includes those with frequent contacts or where non-public information may need to be exchanged. Often you will have confidentiality agreement with such parties

SOURCE: Team analysis
Example of risk assessment and leveling

Example framework considers 3 factors in prioritizing risks
- Probability of occurrence
- Impact on business objective
- Investment needed to fix

Other factors that may be relevant include
- Frequency of occurrence
- Reactive vs. Preventive fixes
- Organizational capability
- Different time horizons (e.g., 6 months vs. 5 years)
Security transformation shall progress in 3 distinct phases

Evaluate

Where do we stand?
- Get buy-into framework
- Create baseline
- Develop high level plan

Today

6 months

Initialize

Build strong capabilities on strong foundations
- Complete baseline
- Finalize plan
- Get approval and budget
- Staff and start execution

Execute

Move forward and evolve
- Mature baselines and plan
- Execute at full pace and refine

24 months

12 months