NAREIT's Law, Accounting & Finance Conference

JW Marriott Desert Ridge Resort & Spa
Phoenix, AZ

Cyber Security

March 31-April 2, 2015

Agenda

1

State of the Union for Cyber Security

- New Vectors of Threats
- Dynamic World of Change
- Real Estate Cyber Security Risks
- Common Cyber Security Mistakes

2

Planning Your Response

- 5 steps to minimize your exposure
- Assess your Readiness
- Lessons learned from Law Enforcement

3

Appendix Materials

- Cyber Maturity Assessment Areas of Focus

New "Vectors" of Threats are Accelerating the Concern

Yesterday…

Bad "Actors"

- Isolated criminals
- "Script Kiddies"

"Target of Opportunity"

Targets

- Identity Theft
- Self Promotion Opportunities
- Theft of Services

Today…

Bad "Actors"

- Organized criminals
- Foreign States
- Hactivists
- Insiders

"Target of Choice"

Targets

- Intellectual Property
- Financial Information
- Strategic Access

Dynamic World of Change

Traditional Approach

KPMG Approach

Business Delivery "Stack"

BUSINESS LAYER

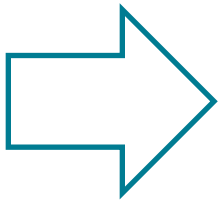
- Industry Leading Practices
- Geopolitical Drivers
- Business Process
- Corporate Objectives

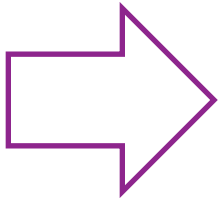
ENABLEMENT LAYER

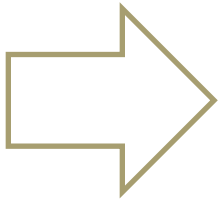
- Application
- Data

INFRASTRUCTURE LAYER

- Servers/Hosts
- Networks
- Physical Environment







Areas of Dynamic Change

- Driving Growth & Profitability
- New Products/Services
- Mergers/Acquisitions
- Globalization
- Strategic Sourcing
- Competitive Differentiation
- Increased Regulatory Scrutiny

- Mobile & Cloud Deployments
- "Big Data," BI & Analytics
- Self service & Consumerization

- Virtualization & Cloud Platforms
- Internetworking/VPNs
- New Operating Systems
- Low cost computing models
- Changing DataCenter models

Real Estate Cyber Security Risks

- Cash – wire transfer fraud
- Employee personal information
- Application data (tax returns, financial information, etc.)
- Tenant information – residential / senior living (HIPAA)
- Third-party vendor risks
- Building automation

The Five Most Common Cyber Security Mistakes

Mistake #1:

"We have to achieve 100 percent security."

Reality:

100 percent security is neither feasible nor the appropriate goal.

The Five Most Common Cyber Security Mistakes

Mistake #2:

"When we invest in best-in-class technical tools, we are safe."

Reality:

Effective Cyber Security is less dependent on technology than you think.

The Five Most Common Cyber Security Mistakes

Mistake #3:

"Our weapons have to be better than those of our attackers."

Reality:

The security policy should primarily be determined by your goals, not those of your attackers.

The Five Most Common Cyber Security Mistakes

Mistake #4:

"Cyber Security compliance is all about effective monitoring."

Reality:

The ability to learn is just as important as the ability to monitor.

The Five Most Common Cyber Security Mistakes

Mistake #5:

"We need to recruit the best professionals to defend ourselves against cyber crime."

Reality:

Cyber Security is not a department, but an attitude.

Planning Your Response
Example Cyber Security Framework

Planning Your Response
Five Steps to Minimize Your Exposure

1. **Assess your Readiness to Respond**

   Perform a cyber maturity assessment to look at areas such as Leadership and Governance, Human Factors, Information Risk Management, Business Continuity and Crisis Management.

2. **Hone in on your critical assets**

   Identify your critical assets but remember that what you consider to be of no value, may be considered valuable to an attacker. Take a look at the lifecycle of your critical information assets from creation all the way to destruction.

3. **Select your defense**

   Based on your assessment and your critical assets, select your defenses. Know what threats you are going to defend against – trying to prevent them all it gets very expensive

4. **Boost your security awareness and education**

   Everyone in the organization – from the boardroom to the mailroom – must understand the value and sensitivity of the information they possess and, more importantly, how to protect it.

5. **Enhance Monitoring & Incident Response**

   Being able to adequately respond to a security incident through established tested processes should not be taken lightly. Supported by a security monitoring platform and good threat intelligence, you can get a better grip on monitoring and responding to cyber crime.

Planning Your Response
Assess Your Readiness – Cyber Maturity Assessment

LEGAL AND COMPLIANCE

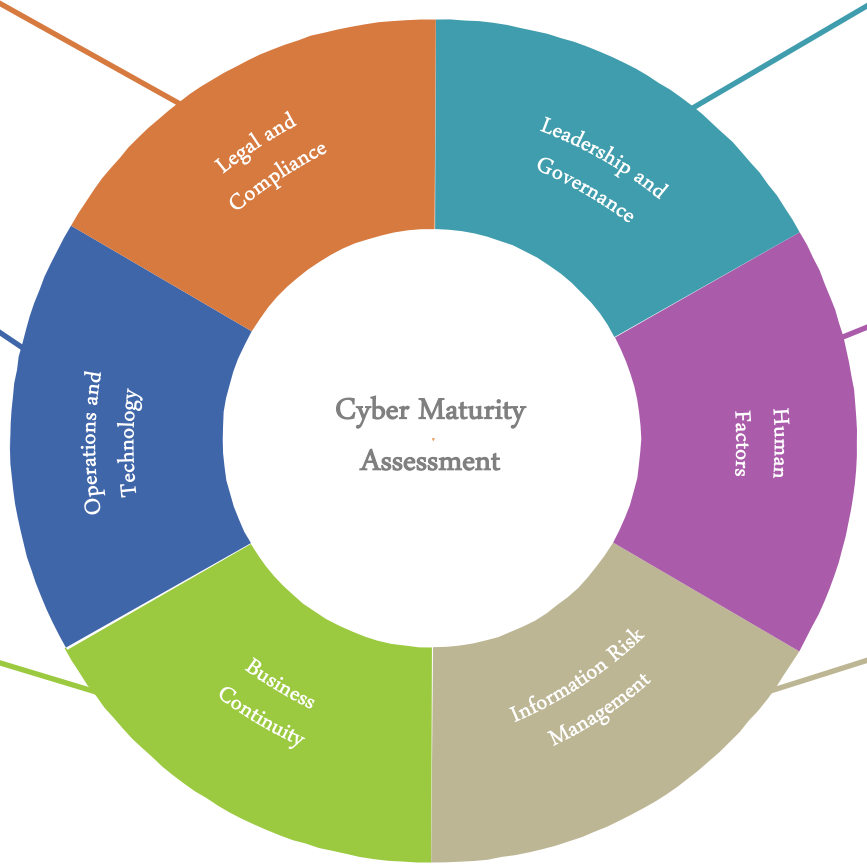
Regulatory and international certification standards as relevant

OPERATIONS AND TECHNOLOGY

The level of control measures implemented to address identified risks and minimize the impact of compromise

BUSINESS CONTINUITY AND CRISIS MANAGEMENT

Preparations for a security event and ability to prevent or minimize the impact through successful crisis and stakeholder management



LEADERSHIP AND GOVERNANCE

Board demonstrating due diligence, ownership and effective management of risk

HUMAN FACTORS

The level and integration of a security culture that empowers and ensures the right people, skills, culture and knowledge

INFORMATION RISK MANAGEMENT

The approach to achieve comprehensive and effective risk management of information throughout the organization and its delivery and supply partners

Planning Your Response
Assess Your Readiness – Cyber Maturity Assessment

Leadership and Governance
Board demonstrating due diligence, ownership and effective management of risk

Topics
Understanding of Cyber
Board Involvement
Third-Party Supplier Relationships
Identification of Critical Data
Ownership and Governance for Data Protection
Program Management

Human Factors
The level and integration of a security culture that empowers and ensures the right people, skills, culture and knowledge

Topics
Training and Awareness
Culture
Personnel Security Measures
Talent Management
Organizational Roles and Responsibilities

Planning Your Response
Assess Your Readiness – Cyber Maturity Assessment

Information Risk Management
The approach to achieve comprehensive and effective risk management of information throughout the organization and its delivery and supply partners

Topics
Risk Management Approach and Policies
Risk Tolerance Identification
Risk Assessment and Measures
Asset Management
Information Sharing
Third Party Accreditation
Ability to Detect Attacks & Integrate Improvements

Business Continuity and Crisis Management
Preparations for a security event and ability to prevent or minimize the impact through successful crisis and stakeholder Management

Topics
Ability to Manage Cyber Events
Financial Ramifications & Budget
Resources Required & Training
Robust Plans
Communications
Testing

Planning Your Response
Assess Your Readiness – Cyber Maturity Assessment

Operations and Technology
The level of control measures implemented to address identified risks and minimize the impact of compromise

Topics
Threat and Vulnerability Management
Logical Security Controls
Physical Security Controls
Security Monitoring
Incident Response
Integration with IT Service Management

Legal and Compliance
Regulatory and international certification standards as relevant

Topics
Inventory of compliance requirements
Compliance program components
Role of the Audit Committee
Litigation inventory
Cyber insurance

Tony Buffomante
KPMG LLP
Principal, Information Protection Services

200 E. Randolph
Chicago, IL 60601

abuffomante@kpmg.com
312-665-1748