Cybersecurity: Risk Management & Mitigation

Sponsored by

POLSINELLI

#crewconvention
Rate Sessions
Excursions, etc.

Rate Speakers

In order to position their organizations to attract top talent, drive breakthroughs, and serve customers better, employers need to understand and prepare for the evolution of the workforce. The sooner organizations adopt the future-focused mindset, skills, and strategies needed to thrive in an increasingly virtual and flexible work environment, the sooner they will realize economic benefits. In this presentation, leaders will learn how to position their organization to be innovative and responsive for attracting and retaining workforce talent. In this session, you will:

- Learn how to capitalize on and manage changing employee-employee relationships and workplace attitudes
- Adapt your workplace to a commitment-based work model and reinforce a culture of learning
- Keep a blended, multi-generational, diverse, and global workplace engaged

Speakers
Sarah Sladek
PREMIER LEAD SPONSOR
Culbert

Maggie Coleman

Summary
Maggie Coleman is a Managing Director and Head of International Capital, Americas. In this role, Ms. Coleman leads a team that is primarily focused on cross-border capital deployment from global investors across Canada, EMEA and Asia Pacific. Ms. Coleman is responsible for placing capital from international investors into JLL’s direct transactions, structuring recapitalizations and joint-ventures, while also helping offshore capital acquire and finance JLL’s global investment portfolio and large single asset sales. Ms. Coleman maintains relationships with senior decision makers at a wide range of offshore capital sources ranging from institutional to private capital groups.

Ms. Coleman has been involved in over $20 billion in transactions and has directed the JLL platform that has executed over $30 billion in transactions since 2011, including over $10 billion in loan sales in the US, Europe and Asia. Further, Ms. Coleman is responsible for business development, client management and the execution of global transactions. She is a frequent speaker on global capital flows in the real estate sector.

PREMIER LEAD SPONSOR
JLL
Agenda

01 Risk discussion
02 Cyber threat briefing
03 The real world
04 The answer
05 Questions
Defining your risk envelope

1 Define risk
What defines my organization's risk boundaries?

2 Measure risk
How do I measure risk?
• Key stakeholder buy-in
• Enterprise-wide conversation

3 Path forward
How do I plot the most efficient path to get into my envelope?
• What is key to my “secret sauce”
• What is a “one time” exercise vs. ongoing (sustainment)
• What expertise do I need to have in house
• How do I leverage my staff, contractors, vendors…

Cybersecurity is a risk-based problem
The cyber threat briefing
Scams specifically directed at the real estate sector rose 1,100 percent from 2015 to 2017.

From June 2016 to May 2018, FBI data shows there was a loss of more than $1.6 billion in the U.S. alone.

Real estate was the second highest industry hit with malware events in the second quarter of 2018.

The basic motives – know your enemy

Adversaries’ tactics, techniques & procedures (TTP), intel, and outcomes vary

Warfare
Disrupt, degrade, deny, destroy

Espionage
Unauthorized access to information

Crime
Commit fraud or theft of information

Understanding the adversary’s motivation is key to making the best cyber governance decisions
Focus on major trends but don’t lose sight of emerging threats
Focus on major trends but don’t lose sight of emerging threats

1. Internet of Things
2. Supply chain attack
3. Phishing/social engineering
4. Insider threat
5. Ransomware
6. Advanced Persistent Threat (APT)
7. Cloud
8. Crime-as-a-Service (CaaS)

©2019 Baker Tilly Virchow Krause, LLP
Focus on major trends but don't lose sight of emerging threats.
What are you trying to protect?

Crown jewels
What are they?

Intellectual property

Delivery of your product or service
Attack surface

- People
- IT infrastructure
- Physical security
- Third parties
The real world
Phishing and pretexting represent 98% of social incidents and 93% of breaches. Email continues to be the most common vector (96%).

- 28% of attacks involved insiders
- 4% of people will click on any given phishing campaign
- Errors were at the heart of almost 1 in 5 breaches

Your people are the softest park of your attack surface

Keys to defense:

1. Minimize changes of an attack getting through
2. Build in resiliencies
Wire fraud – easy as 1, 2, 3

1. Compromise account
2. Watch and learn
3. Attack
Non-traditional attacks

Third parties

Industrial control systems (ICS)
The answer
Training and awareness

3 Laws of Real Estate

Location Location Location

3 Law of Training

Practice Practice Practice
Cybersecurity capability challenges

- Heavy demand driving up labor costs and churn
- Limited pipeline of new talent
- Process agility is the key to operationalizing the organization’s capabilities
- Constant evolution to meet changing threat
- Rapid evolution of technology
Security as part of the culture

- Test and challenge
- See something – say something
- Ask “why?”
Access to expertise

Know your resources

Ask for help
Cybersecurity is a risk-based problem

Defining your risk threshold is the first step – not deploying technology.

It starts and ends with your people

Your people are both your greatest threat and asset. Give them the context and training they need to be part of the solution.

Understand potential attack models

Know your enemy and how your organization looks from their perspective.

Access to cybersecurity expertise

Every organization needs access to expertise at both the tactical and strategic level to support decision making and operations.

Cybersecurity as part of your culture

Build security into your day-to-day process – do not just bolt it on.

Takeaways
WHO WE ARE

• Established Cyber Security Software and Service company with a strong pedigree and leadership

• Founded by NSA Cyber Operations experts and led by government and commercial luminaries

• Robust understanding of real-time cyber operations

Jon Murchison
Founder and CEO

BOARD AND STRATEGIC ADVISORS

Hamid Akhavan
Former CEO of T-Mobile Int.

Chris Inglis
Former Deputy Director of NSA

General Hayden
Former Director of NSA and CIA

Dr. Ronald Clark
Former DHS and NSC

Frank Fitzsimmons
Managing Director at Adelphi Capital

Dr. Rajendra Singh
CEO of Telecom Ventures, LLC

Tom Donahue Jr.
President of Adelphi Capital

Ambassador Dana Shell Smith
Former US Ambassador to Qatar
CYBER SECURITY CHALLENGES

• Growing # of IP-based devices
• Unsecured protocols and ports
• Mix of IT and OT equipment on the same network
• Remote access requirements
• Vendors with varying security experience and awareness
• Wide range of technician skill level
• Little to no visibility, monitoring, or threat detection
NUMEROUS ATTACK SURFACES

- Building Automation Systems (BAS)
- OT Devices (lighting, HVAC, access control, etc.)
- IoT Devices (smart TV, security cameras, Chromecast, etc.)
- IT Devices (laptops, desktops, servers, etc.)
- Vendors
- Personnel
THE RISKS

• Disruption of building operations
• Equipment damage
• Financial loss
• Insurance exposure
• Reputational damage
THE SOLUTION

• Protected from cyber threats
• Mitigate financial, equipment, and reputational risk
• Established cyber security platform and policy
• Real-time monitoring and threat detection by security experts
• Affordable
• Peace of mind
Jon Murchison
Blackpoint Security

David Ross
Baker Tilly
Principal—Cyber and Privacy Practice
Lead
David.ross@bakertilly.com
+1 (703) 923 8282
Rate Sessions

Excursions, etc.

Rate Speakers