Opening Remarks

Mark Wilson
CMO

John McClurg
CISO
<table>
<thead>
<tr>
<th>Time</th>
<th>Session Title</th>
<th>Speaker(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>11:00 am</td>
<td>Opening Remarks</td>
<td>Mark Wilson &amp; John McClurg</td>
</tr>
<tr>
<td>11:10 am</td>
<td>Protecting &amp; Managing Endpoints</td>
<td>Nigel Thompson</td>
</tr>
<tr>
<td>11:30 am</td>
<td>Protecting People</td>
<td>Ramon J. Pinero &amp; David Wiseman</td>
</tr>
<tr>
<td>11:50 am</td>
<td>Protecting Things</td>
<td>John Wall</td>
</tr>
<tr>
<td>12:10 pm</td>
<td>Technology Platform</td>
<td>Eric Cornelius</td>
</tr>
<tr>
<td>12:30 pm</td>
<td>Go-To-Market</td>
<td>David Castignola</td>
</tr>
<tr>
<td>12:45 pm</td>
<td>Closing Remarks</td>
<td>John Chen</td>
</tr>
</tbody>
</table>
Business Continuity during a Global Pandemic
I can’t communicate with my remote employees
Workers can’t go to the office
Phishing attacks are increasing
Volume of threats
New threat surfaces with mobile & IoT
The human factor
Complexity – number of vendors & solutions
We don’t have enough laptops to send to users
Our VPNs are overloaded
I need to keep my business running
Crisis communication for all employees everywhere
Unified Endpoint Security & Management for any device
Work remotely on any device – personal or corporate owned

Secure network access on a BYOL without needing a VPN
Intelligent Security that reduces friction and improves user experience
Future proof platform that will support the next generation of endpoints

ORDER
Business Continuity During Global Pandemic
Business Continuity

During Global Pandemic

Business Continuity Manager

Endpoint Security & Management

Working From Home

CIO | CISO

End User
Centers for Disease Control and Prevention
Global Pandemic Notice
March 1, 2020 10:13 AM

Warning - Level 3, Avoid Nonessential Travel—Widespread Ongoing Transmission.
Older adults and people of any age with serious chronic medical conditions are at increased risk for severe disease. There may be limited access to adequate medical care in affected areas.

California Department of Public Health
EXECUTIVE ORDER N-33-20
March 4, 2020 10:13 AM

The Director of the California Department of Public Health is ordering all individuals living in the State of California to stay home or at their place of residence, except as needed to maintain continuity of operation of the federal critical infrastructure sectors.

Business Continuity Plan
Crisis Communications System
Execute WFH Continuity Plan
InterCon Bank Inc.
Employee Welfare Check
March 1, 2020 10:13 AM

Your manager has started to make arrangements for you to travel back as soon as possible. We wish safe travels and speed during this pandemic.

How are you?
- I am safe
- I am not feeling safe
- I am not in the affected area

Global Pandemic Notice

Severity: High  Type: Other

The Director of the California Department of Public Health is ordering all individuals living in the State of California to stay home or at their place of residence, except as needed to maintain continuity of operation of the federal critical infrastructure sectors.

All employees are instructed to work from home until further notice.

For more info, click here.

Published on: 02/04/2020 15:54:01 (Pacific Time (US & Canada)) By: Ken Tanaka
Sent by AtHoc. To change your profile, add/delete contact numbers or email addresses, click here.

Copyright ©2020 Blackberry Limited. All Rights Reserved.
Notify Workers of WFH Options

Entitle Access with UEM
Secure Access to Work Apps

Corporate & Personal Devices

InterCon Bank Inc.

Work Access Notification

March 5, 2020 10:13 AM

Work From Home Enabled

You've been entitled to work from home. Learn more details about how to access your company files and applications.
Business Continuity

During Global Pandemic

Business Continuity Manager

Endpoint Security & Management

CIO | CISO

Working From Home

End User

During Global Pandemic
Phishing Attacks Increasing
Targeting Workers at Home

Security Attacks Increasing
Targeting Corp & Personal Devices
Users on Home Networks
Unified Endpoint Security Console

Protecting Personal & Corp Device

AI Prevention Stopping 100% Phishing
Mobile Threat Defense
Continuous Authentication
Endpoint Protection
Detection & Response
Continuous Authentication
Multiple Telemetry Objects
Intelligent Security
AI Driven Risk Model
Adaptive Security Policies
Business Continuity

During Global Pandemic

Business Continuity Manager

Endpoint Security & Management

CIO | CISO

Working From Home

End User
Secure Documents
Secure Intranet Access
One Secure Application
Secure Email & Calendar
BlackBerry

User Behavioral Analytics
Intelligent Security
Continuous Authentication
Protecting the Vehicle
Control & Safety Systems
Secure Connectivity
Unified Endpoint Management & Security

Nigel Thompson
Vice President, Product Marketing, BlackBerry Spark Division
Business believe that WFH will likely be long term or permanent.

Increased attacks targeting corporate data on mobile & personal devices continues to grow.

Increase demand for products that support & secure unmanaged devices.

Work from Office

Work from Home | Remote
Secure Network Access & Secure Web Gateway

Secure Email Calendar, Web & Secure Integration with 3rd Party Apps

Advanced Data Loss Protection & Data Rights Management

AI Driven Endpoint Protection & Mobile Threat Defense

Endpoint Detection & Response with Intelligent Actions

Mobile Device Management & Modern Management

Corporate Mobile Devices

Personal Devices
Order is achieved through the BlackBerry’s AI-powered Unified Endpoint Security Platform.
Protecting People

**Ramon J. Pinero**
Vice President, Services,
BlackBerry AtHoc

**David Wiseman**
Vice President, Secure Communications
PROTECT MOBILE COMMUNICATIONS – VOICE AND MESSAGES

- Tapping of networks to capture content of calls and messages
- Identity spoofing and hijacking
- Loss of control and ownership of metadata

INNOVATION THIS YEAR

- Updated NIAP/CSfC – certifications with Top Secret usage crypto package
- Partnership CACI for US FedRAMP service – SteelBOX
- Enhanced messaging and PBX integration capabilities
BlackBerry® AtHoc

Secure    |    Unified    |    Flexible

Situation Response
Plan, respond, & collaborate

Alert
Notify anyone, anywhere, on any device

Collect
Capture critical information to achieve situational awareness

Account
Gain real-time visibility into the safety and status of your personnel

Connect
Inter-agency critical communications
Joseph Shearer-Rust, MBCI
Resilience Officer
BlackBerry AtHoc: Real Customer Usage

Terror Attack
BlackBerry, major global media company, major defense organizations, activated personnel accountability event to obtain real-time safety status of workers and travelers in London (and previous attacks in Paris and Brussels)

Cyber Security Breach
G8 Government was victim of cyber attack and reduced time of sharing critical information from 90 minutes to less than 90 seconds

Communication Outage
Major manufacturer’s typical communication channels went offline; integration with non-IP mass communication devices were activated

Severe Weather
City building inspectors created situational awareness via rich media communication of damaged buildings post Mexico earthquake
Why BlackBerry

Gas Sensor

Internal Notification

Contra Costa County Office of Emergency Services

Fire

Police

Etc.

Accountability event

Internal Notification

External Health orgs.

Citizens

External Notification

Other input
Why BlackBerry? Why Now?

- Competitive Pricing -
  - Public Safety -
  - Enterprise -

- Blue Light -
  - Healthcare -
  - SLED -

- Amazon Web Services -
  - Microsoft Azure -
  - Dedrone -

- Infrastructure -
  - Product -
  - People -

Broadening Our Reach
Protecting Things

John Wall
Senior Vice President, Head of BTS Operations
150M+  MILLION CARS ON THE ROAD

45+  AUTOMAKERS

270+  MAKES & MODELS

7 of 7  TOP TIER1s USE BLACKBERRY QNX

9 of 10  AUTOMAKERS USE BLACKBERRY QNX

100%  START OF PRODUCTION SUCCESS RATE
Software Trends in Automotive

Safety – Security – Trust

Secure Gateways
Telematics
Complex Domain Controllers

Acoustics
Digital Cockpit
Infotainment
Instrument Clusters
OTA
ADAS, Active Safety
Control Systems
V2X

Secure Lifecycle Management

Traditional
Growth

OTA, Jarvis
Connected Services
Growing Demand for Secure and Safety Certified Products

- Control systems in autonomous vehicles
- Safety & ADAS systems
- Digital & hybrid instrument clusters
- High-speed rail
- Factory automation & industrial control
- Energy generation
Embedded Software Market - 2019

Vertical Split

- Aerospace & Defense: 22%
- Automotive/Rail/Transportation: 22%
- Industrial Automation: 20%
- Medical Devices: 19%
- Communications/Networking: 10%
- Other: 6%

Data from VDC Research

- Microsoft share predicted to drop faster than previously forecast
- Commercial Linux shrinking while RTOS growing
- BTS-QNX SAM as percent of TAM is much higher in Medical than in the A&D vertical
Why We Win – Foundational Value

Safety
- Broadest safety certified software portfolio
- Significant ongoing investment in safety roadmap
- Safety certified custom engineering and training

Security
- BlackBerry / QNX brand value and reputation
- BlackBerry / QNX embedded security technology
- BlackBerry / QNX security services

Reliability
- Decades of proven reliability in mission critical systems
- Proven microkernel system architecture
- Trusted people and proven long term customer support

Note: These attributes and associated value apply equally to segments within GEM and Automotive markets
Why We Win – Foundational Value

Scale
- Scalable product licensing and business models
- Deeply embedded to high-end complex system pedigree
- Linux compatibility to leverage talent and technology

Realtime
- Decades of success powering real-time critical systems
- Realtime OS pedigree and adherence to standards
- Best in class system performance and analysis tools

Trust
- Trusted to deliver on commitments (100% SOP success)
- Impeccable reputation for world’s best engineering talent
- Mission - Life - Safety - Critical device foundation

Note: These attributes and associated value apply equally to segments within GEM and Automotive markets
Secure & Safety Certified Software Portfolio

QNX Certified Operating System

Certified Hypervisor
Certified Graphics
Certified Board Support
Certified System Libraries
Certified Tools
Certified Comms
Functional Safety Consulting

ISO
IEC
Beachhead Strategy for Products and Services

1. New Value-Add Embedded Products
   - Deliver new value-add products that build on our proven Foundational Products to meet customers’ needs to increase our stickiness and revenue

2. New Value-Add Connected Services Products
   - Augment the portfolio to include new Connected Services Products: Lifecycle endpoint management leveraging BlackBerry’s extensive portfolio.

3. Expand Professional Services
   - Scale and expand the Engineering Services portfolio globally building on our existing trusted and proven Engineering Services to increase stickiness and revenue

4. New Synergistic Market Segments
   - Enter new synergistic market segments (e.g. A&D) leveraging our value proposition, product and services portfolio and channel reach with an initial focus on awareness and early customer wins
Victor Salmons
Vice President Engineering, Speciality Printers
BlackBerry Technology Platform

Eric Cornelius
Chief Product Architect
The New Normal: Work from Any Location, Any Device
Explosion of Interconnected Devices
Leverage the rich data access across the BlackBerry security portfolio to bring unified services, analytics, and holistic automated remediation by using a common data framework and shared insights amongst all products.
BlackBerry Data for Intelligent Action

- **Desktop**
  - Traditional Security
  - Rules & Signatures

- **Desktop or Mobile**
  - Next Gen Security
  - Rules, Signatures, ML Models, Threat Hunting

- **Industrial IoT & Automotive**

- **BlackBerry Security**
  - Complete 360 Security Insights, Automated Hunt & Remediate, Advanced Threat Prioritization, Rich Cross-Platform Querying, Proactive Detection, Standardized Data-
  - Ingestion
  - Transmission
  - Formatting
  - Storage
  - Processing
  - Generation

- **Common Data Lake**

- **Threat Intelligence**

- **Desktop**

- **Mobile**

- **Next Gen Security**

**#BlackBerrySecure**
### Zero Trust/Zero Touch Vision

- Expand BlackBerry Persona platform across BlackBerry Spark portfolio
- Open BlackBerry Persona platform to third parties
- Leverage context correlation for generating risk score to improve Zero Touch user experience

#### Intelligent Security Action Orchestrator

<table>
<thead>
<tr>
<th>Component</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Score Aggregator</td>
<td>Identity &amp; Behavior Learned Locations, Continuous Auth (anomaly detection and passive biometrics), Geo-velocity, IP Address Reputation, Persona Desktop Scores, 3rd Party Risk Engines</td>
</tr>
<tr>
<td>ML Model Training</td>
<td>Behavioral Locations (bLoc), Application Usage Anomaly, Passive Biometrics</td>
</tr>
</tbody>
</table>

#### Event Streams
- Audit Log
- Action Rule Template
- IP Whitelist/Blacklist
- Risk Engine Config
- Geo Zone Definition

#### Admin API Layer

<table>
<thead>
<tr>
<th>Module</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Persona Portal</td>
<td>Zero Trust Console (Future)</td>
</tr>
</tbody>
</table>

#### Runtime API Layer

<table>
<thead>
<tr>
<th>Module</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile App</td>
<td>Persona SDK, Trust Score (Optional Actions)</td>
</tr>
<tr>
<td>Web App</td>
<td>EID, Trust Score (Optional Actions)</td>
</tr>
<tr>
<td>BIG</td>
<td>Trust Score (Optional Actions)</td>
</tr>
<tr>
<td>Third Party</td>
<td>Trust Score (Optional Actions)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Event Flow</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event data</td>
</tr>
<tr>
<td>Training data</td>
</tr>
</tbody>
</table>
Applying AI to Automotive

Concept framework concept at CES showing software management & cybersecurity across the vehicle fleet.

Enhance automotive SW security posture by providing insights into binaries and continuous protection against CVEs

BlackBerry OTA to manage software lifecycle for connected vehicles

ML technology to prevent vulnerabilities into the vehicle Android IVI system in a QNX hypervisor

ML technology to manage vehicle health

ML technology to identify driver via driving patterns

Build

Binary Scanning

Deploy

OTA

Operate

BlackBerry Protect

Vehicle Health Monitoring

BlackBerry. Persona

© 2020 BlackBerry. All Rights Reserved.
Applying AI to Automotive

Next: An intelligent vehicle platform to develop, deploy, and manage a new generation of in-vehicle services.
Applying AI to Healthcare

New concept under evaluation: Extensibility of software management & cybersecurity for healthcare deployments. Combination of new technologies and services.

Build
Software Scanning
Build secure health equipment via secure boot, insights into binaries, and continuous protection against CVEs

Deploy
OTA
BlackBerry OTA for certificate & key management, manage software for connected equipment

Operate
Equipment Health Monitoring
ML technology & network monitoring to manage health of equipment and devices

BlackBerry Protect
ML technology to prevent vulnerabilities into systems and connected equipment

BlackBerry. Persona
ML technology to identify patients or other users via usage patterns

New concept under evaluation: Extensibility of software management & cybersecurity for healthcare deployments. Combination of new technologies and services.
Go-To-Market

David Castignola
Head of BlackBerry Spark Field Operations & Marketing
CUSTOMER GOAL

Reduce Risk & Improve Security Posture to Enable the Business
TOP PRIORITIES

1. Rationalize & Optimize
2. Drive Productivity
3. Business Continuity/Secure WFH
PLAN FOR GROWTH

1. Awareness
2. Execution
Awareness
Unified GTM Strategy
Protect the Base – Grow New Logos...Take Market Share

Unified Distribution & Channel Management Operating Rhythm

EXECUTION

Unified Sales Organization

THECHANNELCO
CRN
PARTNER PROGRAM GUIDE 2017
WINNER 2018
WINNER 2019
Closing Remarks

John Chen
Executive Chairman & CEO
THANK YOU!

We appreciate your feedback.
Please complete the survey on the next screen.