Chaos, Complexity & Other Current Conundrums:

Inadvertent health care information breaches and identity theft – opportunities and challenges

John McClurg
Chief Security Officer

Achieving Excellence Together 2015
Atteindre l’excellence ensemble
Welcome to the world’s largest startup.

One year & counting
The World is Flat – 10th Anniversary

Traditional Boundaries of Delineated Interest Growing Ever-more Porous
“May you live in interesting times”

–Chinese Curse

I always thought it was a blessing!
cha·otic/adj ective
1. characterized by a state of utter confusion or disorder

com·plex/adj ective
1. composed of many interconnected parts

cou·nun· drum/noun
1. anything that puzzles
Chaos is inherent in all compounded things. Strive on with diligence.

Buddha

While not new concepts, their presence in our lives seem to be exponentially increasing....
I accept chaos, I'm not sure whether it accepts me.

Bob Dylan

...carrying with them no small quantities of ambiguity and general uncertainty...
The battlefield is a scene of constant chaos. The winner will be the one who controls that chaos, both his own and the enemies.

Napoleon Bonaparte

..which if not properly addressed can carry with them consequences of no small magnitude...

Potentially... even FATAL!
Civilization begins with order, grows with liberty and dies with chaos.

Will Durant

Chaos & Complexity then are not to be taken lightly.
There's chaos out there, and chaos means opportunity.

Marc Ostrofsky

Even in the dark clouds of chaos and complexity there's a sliver lining...even...an Opportunity!
Fools ignore complexity. Pragmatists suffer it. Some can avoid it. Geniuses remove it.

Alan Perlis

The questions of how we can best do that remains that about which rational minds can and do differ!

...More Art perhaps than it is Science
We need to shift the paradigm from reactive technologies to more integrative solutions that deal with the variety and complexity of the threats that are out there today.

John W. Thompson

--Chairman, Microsoft

“Quantum Security”... managing and mitigating in a realm of frequently non-discrete, evolving possibilities that can present themselves at any moment as either a potential harm or a benefit to an enterprise.
Myth: Real threats are few and far between.

Fact: 73% of organizations say they experienced a security breach in the last year.

Dell Global Security Study
The Reality: Cyber Security is a global issue

- 556 million people per year becoming victims of cybercrime
- 1.5 million per hour (Toronto)
- 18 people per second
- Annual price of $500 billion

Cybercrime costs the world more than the global black market in marijuana, cocaine & heroin combined
The Impact of Cyber Crime

Global costs of cyber crime is $500B

Translate costs into “hacker revenue”

Would be the largest company in the world

---

<table>
<thead>
<tr>
<th>Rank</th>
<th>Company Name</th>
<th>Revenues ($)</th>
<th>Profits ($)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Wal-Mart Stores</td>
<td>469.2</td>
<td>16,999</td>
</tr>
<tr>
<td>2</td>
<td>Exxon Mobil</td>
<td>449.9</td>
<td>44,880</td>
</tr>
<tr>
<td>3</td>
<td>Chevron</td>
<td>233.9</td>
<td>26,179</td>
</tr>
<tr>
<td>4</td>
<td>Phillips 66</td>
<td>169.6</td>
<td>4,124</td>
</tr>
<tr>
<td>5</td>
<td>Berkshire Hathaway</td>
<td>162.5</td>
<td>14,824</td>
</tr>
<tr>
<td>6</td>
<td>Apple</td>
<td>156.5</td>
<td>41,733</td>
</tr>
<tr>
<td>7</td>
<td>General Motors</td>
<td>152.3</td>
<td>6,188</td>
</tr>
<tr>
<td>8</td>
<td>General Electric</td>
<td>146.9</td>
<td>13,641</td>
</tr>
<tr>
<td>9</td>
<td>Valero Energy</td>
<td>138.3</td>
<td>2,083</td>
</tr>
<tr>
<td>10</td>
<td>Ford Motor</td>
<td>134.3</td>
<td>5,665</td>
</tr>
</tbody>
</table>

* - Center for Strategic and International Studies (CSIS) 2013

---

#1 - Hacker’s Inc.
The Internet is “where the bad guys will go because that’s where our lives are, and our money, our secrets and our intellectual property,“

James Comey, FBI Director
## Identity Theft Market Value

<table>
<thead>
<tr>
<th>Service</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>US Based Credit Card</td>
<td>$1 - $2</td>
</tr>
<tr>
<td>Non-US Credit Card</td>
<td>$2 - $10</td>
</tr>
<tr>
<td>Prestige Credit Card</td>
<td>$200 - $400</td>
</tr>
<tr>
<td>PayPal account, verified balance</td>
<td>$2 - $200</td>
</tr>
<tr>
<td>Compromised Computer</td>
<td>$1 - $100</td>
</tr>
<tr>
<td>Healthcare Insurance Credentials</td>
<td>$50 - $2000</td>
</tr>
<tr>
<td>Skype Acct. Premium</td>
<td>$1 - $100</td>
</tr>
<tr>
<td>Game Accounts</td>
<td>$100 - $1000</td>
</tr>
<tr>
<td>Med. Health Record</td>
<td>$50</td>
</tr>
</tbody>
</table>
As a leader in our markets we are in the proverbial “thick of things”
.. all the more so when it comes to healthcare!

**#1** WW Healthcare IT Services Vendor for 5 consecutive years (Gartner)

**1st** FDA-approved personalized medicine clinical trial for pediatric cancer

**7B+** Medical images secured in the cloud

**17 of 18** Hospitals on the US News & World Report 2013 Honor Roll are Dell customers

**52B** Security events processed daily by Dell SecureWorks

**89%** of Hospital & Health Networks’ Most Wired Hospitals in 2013 are Dell customers

**71%** Of Stage 7 HIMSS EMR Adoption Model hospitals are Dell customers

**#1** VNA Vendor in KLAS 2013 Image Archive Performance Study* and 2013 Category Leader for VNA/Image Archive**

**4,000** Hospitals and 400,000+ physicians worldwide work with Dell

*KLAS  Research “Image Archive 2013: Finding out What is in Store for VNA?”, September 2013. ©2013 KLAS Enterprises, LLC. All rights reserved. www.KLASresearch.com

Cost to resolve issues from single cyberattack against Target in 2014

$148M

3M
Indications of malicious activity in US Government Civilian agency networks each year

$5.9M
Average cost of a data breach in 2013, according to Ponemon Institute research

100,000
New malware samples discovered by researchers every day, according to Georgia Tech

33%
Increase in number of cyber incidents reported by Federal agencies between fiscal years 2011 and 2013

19%
New malware samples detected by Antivirus solutions
Few sectors face the magnitude of challenges that healthcare does today

**Clinical challenges**
Increasing costs, decreasing budgets

**Lack of infrastructure**
Fewer than 1/4th of HC CIOs consider their existing infrastructure capable of supporting necessary technological advancements

**Shortage of skilled IT**
52% of HC CIOs are having trouble finding and hiring skilled IT workers

**Lack of standard platforms**

**Security**
The majority of HC providers have had at least one breach in the past two years
Powerful Disruptors:

Cloud: 85% of businesses said their organizations will use cloud tools moderately to extensively in the next 3 years.

Big Data: 35

Mobility: 5X

Security and risk: 79%

- By 2020 volume of data stored will reach 35 Zettabytes - KMGTPZEY
- Mobility source shifts from 62% corporate owned and 38% personal owned to 37% corporate owned and 63% personal owned
- of the surveyed companies experienced some type of significant security incident within the past year that resulted in financial and/or reputational impact
The New Dell Global Security Organization: Optimum positioning for 21st Century Risk

End-to-end transformation, characteristic of many of today’s corporations

- Implementing a Converged-House Security Model, Physical and Cyber integrated together, optimally positioned to address vulnerability interdependencies
- Leveraging the lessons learned from the Dark days at Lucent
- Minimally essential core - SecureWorks Integration Goal: “Be our own best customer”
- Together with new insights on the meaning of Holistic and Integrated

Converged, Cored and Connected
The Emergence of a New Model

- Dark Dante – Physical vulnerabilities undermine Cyber interests & Cyber vulnerabilities undermine Physical
- Aspects of the, Dark Dante, Nicholson, & Hanssen affairs subsequently validated the assumption that dimensions of the 21st century threat vectors could be optimally addressed by a converged model.
- Conversations with Bob
Dell Global Security – *Converged, Cored and Connected*

**Mission remains**

“To assure & enhance the integrity, people, processes, and assets by which Dell achieves its greater mission.”

by managing unacceptable risk to the Corporation under the **protective umbrella** of a “converged” security organization – including both Cyber & Federal Security

**Vision remains**

“To see DGS and its services engaged as both an *inextricable* and *indispensible* aspect of advancing the business.”

by grounding our security policies and practices not only in the most current voice of the Threat, but in the laws and regulations of the countries we do business at a price point that enhances our bottom line.

Not just your traditional “Guns, Gates, Guards & Geeks…”

Nor “Distasteful cost”… but “Aspect of Advancing”

**BUSINESS ASSURANCE**
Exposure

Supply Chain: complex processes subject to country specific regulations and vulnerable to disruptions

Emerging Markets: highly interconnected geopolitical risks such as terrorism, nuclear proliferation, corruption & organized crime.

Cyber Espionage (APT): advanced clandestine activities to gain persistent intelligence on an individual, group of individuals, companies and governments.

Transnational Crime: organized crime and narco-terrorism weaken states’ authority

Regulatory & Compliance Diversity: if not balanced, regulation can have unintended consequences for industry structures and market competition.

M&As, JVs: these activities represent significant opportunities and risk if not properly managed. Due diligence is key.

Contract/Procurement Security: increased dependence on external suppliers and sole source suppliers; assuring contract language related to internal controls and compliance has impact.

Work Place Violence: however it manifests itself, is disruptive to Dell operations.

BCM: natural disasters continue to impact production, disrupt supply chains.

Mitigation Strategy

DGS Service: Policy and Standards; Risk Management and Assessments; Physical Security - Assure distribution centers & channels are properly secured

DGS Service: Assure adequate regional staffing; monitor high risk travel; integrate risk reduction activities; leverage global contracts.

DGS Service: CI Pilot – Federal Enclave; Cyber Threat Team; Coordinate cyber-intrusion, counterintelligence, and espionage investigations; advance self-inspections and audits.

DGS Service: Physical Security; Risk Management and Assessment; Investigations; Awareness and Training; Collaboration with the Anti-corruption Team;

DGS Service: Policy and Standards; Classified Security Management; Perennial Policy review.


DGS Service: Contract & Procurement Security Services; Policy & Standards; Risk Management & Assessments

DGS Service: Investigations; Contract Guards; Policy and Standards; Awareness products; training tools.

DGS Collaboration: BCM - Standardize and simplify requirements to develop, test and maintain emergency response and recovery capabilities.
A Good Year: From Obscurity to 4th to 2nd to 1st

Minimally Essential Core
Surrounded by a Constellation of Trusted Partners
“Dell’s security vision is one that sees the need to shift our paradigm from reactive technologies to more integrative solutions that deal with the variety and complexity of the threats poised against us today. To that end he’s brought Physical and Cyber security initiatives together under one converged organizational umbrella internally within Dell and has positioned around that indigenous core a constellation of security-focused acquisitions, the prowess of which is also being offered to external customers in a manner that “connects” traditionally silo-ed solutions. While individual domains may have provided adequate security to date, they have left gaps that threat actors can (and do) exploit. The time is ripe, then, for a more coordinated, connected approach to security, enhancing our contextual awareness as we do battle, leveraging the richness inherent in the data stores of these historically silo-ed solutions. Not only does Dell now offer his customers end-to-end IT solutions, he’s overlaying across that infrastructure commensurate security solutions that will no longer operate in isolated silos.”
Dell security evolution

Pre-2010
- BIOS, driver and embedded security for endpoints

2010 Q1
- Endpoint security, patch management
- Mobile Device Management

2011 Q1
- Managed security services
- Security & risk consulting
- Incident response
- Threat intelligence

2012 Q2
- Next-generation firewall, UTM
- SSL VPN for mobile security
- Email & web security

2012 Q3
- AD consolidation & migration
- Identity & access management

2012 Q4
- Data encryption & protection

2013 Q3/4
- Launch Connected Security starting in North America
# Dell SecureWorks Security Services

## Managed Security
- 24/7 security monitoring
- Security device mgmt.
- Log Management
- SIM On-demand
- Vulnerability management
- Web application scanning
- Managed SIEM
- Managed Advanced Malware Protection

## Security and Risk Consulting
- Testing & assessments
- Mobile & cloud security
- Compliance and certification
- Program development & governance
- Architecture design and implementation
- Expert residency
- Physical Security
- Wireless security testing
- Social engineering

## Threat Intelligence
- Threat, vulnerability & advisory feeds
- Emerging threat bulletins
- Targeted Threat Intelligence
- Microsoft update analysis
- Weekly intelligence summary
- Cybersecurity news roundup
- Live intelligence briefings
- CTU support
- Attacker database feed

## Incident Response
- CIRP development
- CIRP Gap Analysis
- CIRP training
- Tabletop exercises & “War Gaming”
- Incident handling
- Digital forensics
- Incident management
- Malware analysis
- Eradication & recovery
- Postmortem analysis
- Documentation
Security leadership, scale and recognition

- **Dell SecureWorks**
  - 60B+ security events analyzed daily
  - Detects 3B security events of interest daily
  - 2M devices WW reporting on 40m users
  - 3,000 security incidents escalated daily
  - Over 18 Trillion applications controlled
  - $14 Trillion in assets protected daily

- **Dell SonicWALL**
  - 110M managed identities
  - 15,000 malicious events analyzed daily
  - 2,000+ security professionals worldwide

- **Dell Data Protection Encryption**
  - Data encrypted & protected on 7M devices
  - 110M managed identities
  - 2,000+ security professionals worldwide
Securing Dell with Dell – Leveraging our Strengths

• Managed Security Services offering – All Dell Firewalls & IPS
• Monthly average of 22 billion events – 148 escalations back to Dell IT Security team for investigation (top 10% of SecureWorks customer base)

• Deployed the Aventail solution to replace incumbent
• Started joint development with Firewall business unit.

• KACE K1000 Management Appliance
• Deployed in Dell’s highly secure, segmented PKI environment for full patch management

• Deploying on Dell internal notebooks
• Pilot started in March, with a deployment starting in Q2

• Quest Authentication Services & Recovery Manager
• Partnering to displace incumbent for Quest account provisioning
Securing a more cloud-based and mobile world

Network
Deep protection and control
- Next Gen Firewall
- Secure Mobile Access
- Email Security
Dell SonicWALL

Data & Endpoints
Protect data wherever it goes
- Encryption
- Configuration and Patch Management
- Secure Cloud Client
- Protected Workspace
Dell Data Protection | Encryption, Dell KACE

User
Identity and access management
- Identity Governance
- Privileged Management
- Access Management
- Compliance and IT Governance
Dell One Identity Solutions

Services
Protect, predict and respond to threats
- Incident Response
- Managed Security Services
- Security and Risk consultation
- Threat Intelligence
Dell SecureWorks
The Dell Security difference

**Connected end-to-end**
- Closes gaps, reduces complexity and mitigates risk
- Secure your business from device to datacenter to cloud

**Shared, context-aware intelligence**
- Enables proactive protection everywhere
- Share real-time threat information system-wide

**Built for humans**
- Makes it easy for people to do the right thing
- Stands in the way of threats, not people and productivity

Secure your business from device to datacenter to cloud.
The security program your organization needs
A different way to approach the security challenge

**Protect**
Protect your whole enterprise including the people that use it – efficiently and proactively.

**Comply**
Comply with regulations and achieve consistent, reliable and easy governance across the board.

**Enable**
Enable your organization to take advantage of new technologies and innovate faster in an evolving world.

### Benefits

<table>
<thead>
<tr>
<th>Protect</th>
<th>Comply</th>
<th>Enable</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Assess your risk posture and vulnerabilities</td>
<td>• Meet Meaningful Use Stage 1 and 2</td>
<td>• Secure the organization for mobility (BYOD), cloud, and the Internet of Things</td>
</tr>
<tr>
<td>• Stay ahead of evolving threats (both from insiders and outside malware)</td>
<td>• Prepare the organization for HIPAA audits</td>
<td>• Protect innovations and secure access to PHI from business associates</td>
</tr>
<tr>
<td>• Monitor and mitigate threats in real time</td>
<td>• Incorporate guidelines such as NIST and FIPS</td>
<td></td>
</tr>
</tbody>
</table>

### How Dell Addresses the Challenges

<table>
<thead>
<tr>
<th>Initial Assessments</th>
<th>Security Infrastructure</th>
<th>Monitoring Program</th>
<th>Other Critical Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Security Architecture Assessment</td>
<td>Perimeter, Application and Endpoint</td>
<td>• 24x7 Monitoring</td>
<td>• Identity and Access Management (IAM)</td>
</tr>
<tr>
<td>• Security Program Review</td>
<td>• Firewall</td>
<td>• Security Devices</td>
<td>• Dell Data Protect and Encryption (DDP</td>
</tr>
<tr>
<td>• HIPAA Gap Analysis</td>
<td>• IDS / IPS</td>
<td>• Log Monitoring</td>
<td>• Incident Response and Forensics</td>
</tr>
<tr>
<td>• Meaningful Use Risk Analysis</td>
<td>• Malware Detection</td>
<td>• Threat Protection</td>
<td>• Next Gen Firewalls</td>
</tr>
<tr>
<td></td>
<td>• Web Application Firewall</td>
<td>• Threat Intelligence</td>
<td>• E-mail security</td>
</tr>
<tr>
<td></td>
<td>• Identity Management</td>
<td>• Incident Management</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Access Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Security silos create risk that impedes business innovation

Opportunities
- Cloud
- Mobility
- Virtualization
- Web 2.0
- Big Data

Challenges
- Threats
- Compliance
- Lack of Resources
- Complexity

Risky
Expensive
Inefficient
Use case: Secure Mobility for Clinicians

**Challenge**

- Clinicians need to **access and share** patient data online from multiple locations and devices
- The need for **Mobility/BYOD, Cloud** introduces multiple points of failure and increases the risk for a data loss / breach

**Solution**

- End Point Security and Management
- Data Encryption at Rest and Motion
- Network policy enforcement/ controls
- User Identity validation
- Security monitoring and Audit services (IDS, IPS)

Dell Next-Generation Firewalls + Dell Data Protection + Dell One Identity + Network policy enforcement = **Secure Clinical**
Welcome to the Age of Context

Breaking, at last, the Insider Threat Conundrum
...through BIG DATA analytics

Viktor Mayer-Schönberger & Kenneth Cukier

Moving from Reactive to Proactively Predictive
**Risk Scoring Methodology**

**Summary**

The risk scoring methodology will provide Dell visibility into specific components (Composite Risk Score, Domains and Business Logic) that contribute to the overall individual risk score.

I. **Composite Score**: Represents the highest level risk designation and factors risk scores from across the domains.

II. **Domain**: A level below the composite score, the domain includes business logic categorized into similar categories. (i.e., 8 domains are displayed to the right).

III. **Business Logic / Rules**: Statements that measure virtual, non-virtual behavior and contextual factors and assign a predetermined risk score (e.g., if individual receives a failed access attempt, then business rule score is high).

**Methodology Overview**

**I. Composite Risk Score Level**

<table>
<thead>
<tr>
<th>Business Policy Violations</th>
<th>Business Expenses Paid by Credit Card or Cash Alert</th>
<th>Business or First Class Travel Alert</th>
<th>Group Meals Alert</th>
<th>Recurring Expenses Alert</th>
<th>Tips Alert</th>
</tr>
</thead>
<tbody>
<tr>
<td>Terminatio n Date (i.e., Date Employee is Separating From Dell)</td>
<td>6</td>
<td>40%</td>
<td>3.6</td>
<td>9</td>
<td>10%</td>
</tr>
</tbody>
</table>

**Risk Scoring Framework**

**Dell BAP Pilot Domains**

Insider threats are influenced by a combination of virtual, non-virtual, and organizational factors (e.g., access and clearance level). In order to quantify risk, an individual’s behavior across each landscape must be evaluated and weighted, based on the drivers of risk. The following eight domain areas have been identified for the pilot.

**I. Financial Policy Violations**

- Business Expenses Paid by Credit Card or Cash Alert
- Business or First Class Travel Alert
- Group Meals Alert
- Recurring Expenses Alert
- Tips Alert

**II. Separation Status**

- Terminatio n Date (i.e., Date Employee is Separating From Dell)

**III. Foreign Travel**

- Destinatio n Country
- Pre-Travel Brief (Yes/No)

**IV. Physical Security Alerts**

- Access Granted Anomalies
- Access Denied Anomalies
- Invalid Access Level
- Invalid Card Format
- Invalid Pin #
- Invalid Facility Code

**V. Specialized Access Levels**

- Security Clearance Level
- Special Access Level
- Classification of Safe Combinati on
- Physical Access Privilege

**VI. Security Incidents**

- Issue Summary
- Report Type
- Primary and Secondary Allegation Classificati on (8 total)
- Primary and Secondary Allegation Type (31 total)

**VII. Ethics Incidents**

- Issue Summary
- Report Type
- Primary and Secondary Allegation Classificati on (8 total)
- Primary and Secondary Allegation Type (31 total)

**VIII. Performance History**

- Performance Rating
- Employee Review – Dimension Comments (Parts 1 - 4)
- Manager Performance Improvement Plan

**IX. Additional Risk Indicators**

- As Dell decides to expand the pilot to all Federal business segments, additional data sources and PRIs will be critical to the success of the detection capability.

**Risk Scoring Principles**

Varying Degrees of Risk: Based on patterns of behaviors, certain individuals have an elevated risk and will be the focus of risk mitigation efforts.

Risk-Based Monitoring: As the perceived risk increases, the amount of technical and behavioral monitoring also increases.

Continuous Improvement: Dell will routinely evaluate its risk scoring business rules as new threats arise from historical cases, Dell SME input, and technology as workplace practices evolve.

**Next Step**

In order to refine and institutionalize the analytical capabilities, Dell will focus on the following next steps:

1. Facilitate conversations with Dell data owners to identify key data sources
2. Document data capture process and data availability for key Dell systems
3. Evaluate decision to expand to all Federal business segments
4. Prioritize additional PRIs that should be considered for the advanced analytics tool
5. Validate the use of PRIs with Dell privacy and legal personnel on the ITWG
6. Capture lessons learned and business reqs to expand to all Federal business segments
7. Integrate future data sources once the Dell Federal Network is established in November
8. Move forward with the decision to incorporate all Federal business segments

*Insider Threat Program for a large defense contractor uses upwards of 25 data sources for their advanced analytics capability. Dell is currently utilizing seven data sources in the proof of concept pilot.
Social Media – Exploiting growing connectivity
Yet another Conundrum... the re-emergence of an “old Friend”

Before

Steganography

After
The result: successful collaboration

Tools and technology powered with human intelligence

The world’s best security minds researching our protection

Complete lifecycle protection from device to cloud

Security for what’s next, not just for today

Security is no longer a distasteful cost of doing business... it is now an indispensable aspect of advancing business
Thank you

John E. McClurg
CSO & Vice-President
Dell Inc.
John_Mcclurg@dell.com