2:15 - 2:45 p.m.
Data Management – The Second Concern

**Moderator: David Tweedy**, CMC, MBA, Director, Risk Management Information Systems, Bickmore

**Mark E. Dorn, President & CEO, DAVID Corporation**
Learn how to securely and efficiently store, access and manage information. This session will cover cloud versus on premises, Commercial Off The Shelf Software (COTS) systems, MS Office, custom solutions, other tools and applications, user interfaces, protecting information and IP, secure storage, backup and recovery.
Question - Who Is Gregg Steinhafel?

- Resigned From:
- For His Executive Management Responsibility Of:
- Involved How Many People: 10,000 or 70M or 120M
- His Compensation For 2013:
<table>
<thead>
<tr>
<th>Resigned From</th>
<th>Target Department Stores</th>
</tr>
</thead>
<tbody>
<tr>
<td>For His Executive Management Responsibility Of</td>
<td>Data Breach</td>
</tr>
<tr>
<td>Involved How Many People</td>
<td>70,000,000</td>
</tr>
<tr>
<td>His Compensation For 2013</td>
<td>$20,600,000</td>
</tr>
<tr>
<td>Dog’s Compensation</td>
<td>Likely Ongoing</td>
</tr>
</tbody>
</table>

It’s Over

www.davidcorp.com
1. What Reports On Data Management Security Did You Review This Week?

2. What Is Your Funding Level For Data Management & Security?

3. If You Have A Data Breach (Lost/Stolen Data or Corrupted Data) Are You Sure You Are As Ready As Your Board & Members Expect?

   To Defend?

   To Respond?

   To Fix?
Data Center and Servers account for 67% of the hardware and infrastructure budget.
Many Of Us Have Info Security Programs (ISP)

But how well do we understand data management & security risk?

Graphic Source: https://www.harlandclarke.com/dv/0909/07.php
48% Of Employees Use Work PC’s For Personal
Pools Becoming A Borderless Enterprise

Data has moved beyond the enterprise firewall: Laptops / Home Offices USB Sticks / WiFi / VPN and more...
Insiders & Partners have direct access to your most sensitive data.

70% of all serious incidents are sparked by insiders.

Lost Laptops & Devices

Disgruntled Employees

File Sharing Software

How many of us use Drop Box? Where is Drop Box?
IT Resourcing Models At Pools

• **Do It Yourself On Premise**
  – Laptop/Workstation, WiFi Routers
  – On-premise server(s), data center

• **Hosting** *(use another’s resources)*
  – Shared or Dedicated
  – Various Forms of Cloud
  – Co-location
Data Center Management Solutions

**Configuration Management**
- Automated Provisioning and Updating of Physical and Virtual Environments
- Server Consolidation Through Virtualization

**End to End Monitoring**
- Proactive Platform Monitoring
- Application & Service Level Monitoring
- Interoperable and Extensible Platform

**Server Compliance**
- Configuration Controls and Reporting
- Centralized Security Auditing
- Comprehensive Security & Identity and Access Mgmt

**Data Protection and Recovery**
- Business Continuity Through Virtualization Mgmt
- Backup and Recovery of Physical and Virtual Resources
- Disaster Recovery
End to End Monitoring
Proactive platform, application and service-level monitoring

Challenges For Pools

• IT services, applications and servers must run smoothly
• Increasing pressure for service levels that ensure optimal uptime and responsiveness
• Proactively monitor availability, performance and configuration across heterogeneous platforms
• Perform deep application and service-level monitoring

Capabilities

- Databases
- Servers
- Web Servers
- Claims & Policy
- Other Apps
- Portals
- FROI
Concepts of ZERO Trust

All resources are accessed in a secure manner regardless of location.

Access control is on a “need-to-know” basis and is strictly enforced.

Verify and never trust.

Visibility: Inspect and log all traffic.

The network is designed from the inside out.
Zero Trust Data Protection

Policy-Based, Encryption-Enabled Data Protection.

- **Protect Data from Leakage and Theft**: Enforce usage policies for all removable devices and media.

- **Increase Data Security**: Define forced encryption policy for data flows onto removable devices / media. Flexible exception management. Ensure that data cannot be accessed if removable devices or media are lost or stolen.

- **Continuous Audit Readiness**: Monitor all device usage and data transfers. Track all transferred files and content. Report on all data policy compliance and violations.
Example Secured Web Access

- RSA SecurID® hardware tokens provide "hacker-resistant" two-factor authentication, for user identification. Based on time synchronization technology, this authentication device generates a simple, one-time authentication code that changes every 60 seconds.
Gardner Magic Quadrant

Magic Quadrant for Web Fraud Detection
Data Management Access - Questions

Q? - How do we (safely) provide access to, and maintenance of, all member data by both the pool and members? - Via Online & Portals

This includes claims data, contact information, policy information, certificates, completed training, completed inspections, exposures, underwriting processes, and more.

Q?- How do we (safely) and most efficiently manage data…. program structures, excess coverages and reinsurance, and track retentions and then provide quick access to program participation and retention levels?
Q? - How do we feel better (safer) about our security and privacy? We have policies and technology in place, but there are so many regulations, and so many changes.

Security is an **All-or-Nothing** proposition
= You are as secure as your weakest link.

J. Bako, VP David Corp.
Today’s Agenda – Data Management

- Security 1
- Security 2
- Pool Questions
• Policy And Governance – Risks And Content
  • SOC II audits are generally the standard
  • Testing is against pre-defined security/trust principals
  • Governance is based upon higher standards

• Network & Device Security
  • Network layer N/S/E/W security in a cloud environment
  • Authentication within the VPN

• Staff & Data Security

• Common Deficiencies
Security – Part 2

- Application Content
- HIPAA & PII Data
- Access Management and Authentication
- Application Security
- Data Center / Host System & Vendor Security
Risks Of Policy Content

Without defined security policies and standards, it may be difficult to comply with legal, regulatory and industry requirements or ensure protection of sensitive data.
Risk based plans should reference and/or utilize industry accepted standards/practices such as ISO, COBIT, ISACA, ITIL or NIST.

Ex. National Inst. Of Standards And Technology

Security policies should be published, and accessible to appropriate employees and contractors.
For App Vendors, Hosting Sources & Client Personnel

- Is there a **written policy** for handling, storing and disposing of sensitive PHI/PII data?
- What **documented procedures** are in place for incident or similar security breech issues?
- What help desk or system administration procedures are in place for servicing user requesting **password resets, new access rights or change of privileges**?
- What policies exist for configuring servers or Virtual Machines (VM's)?
- What are the **policies for VPN** set up and access?
- What Network based **Intrusion Detection Systems** (NIDS) are part of the monitoring policy?
- What **vulnerability assessment plan** and schedule is in place?
- What **external penetration plan** and policy is in place? Without it you are non compliant.
# Security 1 – Policy And Governance

## Common Areas Of Policy Content Deficiency

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Patch Management</td>
</tr>
<tr>
<td>2.</td>
<td>Encryption Policy</td>
</tr>
<tr>
<td>3.</td>
<td>Human Resource Policy</td>
</tr>
<tr>
<td>4.</td>
<td>Access Control</td>
</tr>
<tr>
<td>5.</td>
<td>Incident Handling and Reporting</td>
</tr>
<tr>
<td>6.</td>
<td>Disposal of Resources</td>
</tr>
<tr>
<td>7.</td>
<td>System Backups</td>
</tr>
<tr>
<td>8.</td>
<td>Disaster Recovery</td>
</tr>
</tbody>
</table>
Define All Applications

Content Areas…….

1. Purpose & Risks
2. Users Profiles
3. Qty Of Users
4. Key Components (Web Servers, Server, Database, Appliances)
5. Personal Identifiable Information (PII) or Protected Health Information (PHI)
6. Host/Data Store
To Whom Does HIPAA Apply?

- **Business Associates** – TPA’s, Bill Reviewers, RMIS Vendors
  Provides a service that involves the disclosure of protected health information

Business Associates are now directly liable.....

Organizations that “create, receive, maintain or transmit,” PHI data are BAs
What is Protected Health Information (PHI)

<table>
<thead>
<tr>
<th>Individually Identifiable</th>
<th>Health Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>List of 18 Identifiers</strong></td>
<td></td>
</tr>
<tr>
<td>• Names</td>
<td>Health information means any information, including genetic information, whether oral or recorded in any form or medium, that:</td>
</tr>
<tr>
<td>• Geographic subdivisions smaller than State</td>
<td>(1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse;</td>
</tr>
<tr>
<td>• All elements of dates except year</td>
<td>and</td>
</tr>
<tr>
<td>• Phone &amp; Fax numbers</td>
<td>(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.</td>
</tr>
<tr>
<td>• Electronic mail addresses</td>
<td></td>
</tr>
<tr>
<td>• Social Security numbers (SSN)</td>
<td></td>
</tr>
<tr>
<td>• Medical record numbers</td>
<td></td>
</tr>
<tr>
<td>• Health plan beneficiary numbers</td>
<td></td>
</tr>
<tr>
<td>• Account numbers</td>
<td></td>
</tr>
<tr>
<td>• Certificate/license numbers</td>
<td></td>
</tr>
<tr>
<td>• Vehicle identifiers and serial numbers</td>
<td></td>
</tr>
<tr>
<td>• Device identifiers and serial numbers;</td>
<td></td>
</tr>
<tr>
<td>• Web Universal Resource Locators (URLs);</td>
<td></td>
</tr>
<tr>
<td>• Internet Protocol (IP) address numbers;</td>
<td></td>
</tr>
<tr>
<td>• Biometric identifiers</td>
<td></td>
</tr>
<tr>
<td>• Full face photographic images</td>
<td></td>
</tr>
<tr>
<td>• Any other unique identifying number</td>
<td></td>
</tr>
</tbody>
</table>

www.davidcorp.com
Where Is The (PHI) Data In Your Pool

- Health Plan & Clearinghouse
- Health Care Provider (with electronic HIPAA transaction)
- Claims processing or administration
- Data analysis, processing or administration
- Utilization review
- Quality assurance
- Patient safety activities
- Billing
- Benefit & Practice management
- Repricing
- Legal
- Actuarial
- Accounting
- Data aggregation
- Management
- Administrative
- Accreditation
- Financial

“Chain of Trust”
A data storage company service provider that has access to protected health information (whether digital or hard copy) qualifies as a business associate, even if the entity does not view the information or only does so on a random or infrequent basis.

-HIPAA Omnibus
**Information system activity review (Required).** 45 CFR § 164.308 (a) (1) (ii) (D)
Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

**Standard: Documentation.** 45 CFR § 164.316 (b) (1)
(i) Maintain the policies and procedures implemented to comply with this subpart [SUBPART C – Security Standards for the Protection of Electronic PHI] in written (which may be electronic) form; and
(ii) If an action, activity or assessment is required by this subpart to be documented, *maintain a written (which may be electronic) record of the action, activity, or assessment.*

**Time limit (Required).** 45 CFR § 164.316 (b) (2) (i)
Retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of creation or date last was in effect, whichever is later.
Access Management & Authentication Content Areas

✔ Does the app or services allow ability to delegate user authentication or federated authentication?

✔ Does the app leverage enterprise authentication services (LDAP protocol, MS Active Directory)?

✔ Does the app support password policy requirements (password expiration at 60,90,120 days, lock a user account in x login attempts, prevent users from reusing passwords, set minimum password length or complexity upper/lower case, lock out time period enforcement, force new users to change new first login passwords, use new password reset questions?)

✔ Are usernames and passwords transmitted using encryption?

✔ Auto log off of a user based on inactivity?

✔ Limit concurrent access for the same user account?

✔ Restrict access rights to privileges, user Id’s, job roles, job functions?
Remote Access

- Does app have built-in functionality to provide remote access?
- Will remote app access by a vendor be required?
- Will remote app be ....web based, certified and non client involved?
- Can remote access users gain access to command line or script level access?
- Can the app or service restrict access to the app based on IP location?
- How does the remote hosting vendor test the application for SLA requirements?
Security 2 - Application Security

Personnel Security

✓ Are background checks done on personnel who will have administrative access to servers, applications and data. How frequently?

✓ Do support personnel have security certifications (CISSP, GIAC, VSA)

✓ Do the staff have 5-7 years or more in network security?

✓ Does the staff have HIPAA training for access to PHI?

✓ Are written policies and procedures in place to require notification in X Days to clients when sensitive data has been compromised?

✓ What policies and procedures are in place when a hosting employee is terminated or his/her access is terminated
Data Center Security

- Is the Datacenter SAS 70 or SOC2 Type 2 Certified?
  Controlled Access, UPS In Place, Server Racks Locked
  SOC2 Report Available For Review And Updated?

- Who/how has ability to install critical OS, Web, browser and database security patches?
- What access logs are created and reviewed…and how often?

- Video Coverage in place and Logs of all access to the infrastructure equipment
- Backup and Restoration of data, how is this accomplished and is the process audited?

- Does the app vendor or host store data segregated from other customer data?
- Does the app vendor only store the data in the United States?

- Does the app vendor completely delete data when a client officially deletes it from their web services? How many copies of my data are being collected?

- Is data encrypted before sending it over Internet or open network?
  What type of encryption is used? Is it (Government) FIPS 140-2 Compliant?
Penetration testing report provided?

Risk
Absence of penetration testing may lead to non-compliance as per regulatory requirement and non-identification of system vulnerabilities.

Recommendation
Penetration testing should be performed on regular basis to identify any potential weakness in the environment.
Application Security For Applications

Do **third parties conduct security assessments** on your application or service? When was the last review?

Are all web applications and web admin access programs developed based on secure coding guidelines like Open Web Application Security Project Guide, WASC Threat Classification or SANS Top 20?

- Does the app verify all parameters are validated or encoded before being included on a web page (XXS)

- Does the application check for **SQL injection flaws** when user data is entered

- Does the app check and prevent **remote file inclusion** (RFI)

- Does the app prevent attacker from direct manipulation of object references like files, directories, database records via the url
MITRE maintains the CWE (Common Weakness Enumeration) web site, with the support of the US Department of Homeland Security's National Cyber Security Division, presenting detailed descriptions of the top 25 Software errors along with authoritative guidance for mitigating and avoiding them.

That site also contains data on more than 700 additional Software errors, design errors and architecture errors that can lead to exploitable vulnerabilities.
Use our free security engineering training programs as the building blocks for your custom training program.
Application Security For Web Applications

✓ Does the app **check for and require authorization token** submission by the browser

✓ Is the app tested to make sure **info not leaked via error messages**

✓ Does the app or service support SSL v3/TLS

✓ Does the app use IP ports 80 and 443 http / https

✓ Does the app have controls to prevent direct data manipulation

✓ Does the **app record in an audit file all direct access** to the database

✓ Is a web scanning tool run on the app regularly

✓ Is the app supported by certified web programmers – GSSP Secure Software Programmer
Host Security

- Is enterprise antivirus, anti-spyware and host intrusion prevention software installed

- How/who is installing critical O/S, web, browser and database security patches within x days of release?

- Who/how are local administrator level rights managed?

- **Who/how are clients notified if a security breach occurs with application or hosting service?**

- How much up time is expected? What is the typical down time and recovery time?

- **Is the app hosted with other app clients on the same server** or is the server single tenant?

- Is the hosting service security program audited and certified?
Negative Issues With SaaS

- Doesn’t Make Integration Work Easier (HR/WC)
- Doesn’t Auto Integrate With Other SaaS Apps
- Costs Are Not Always Less Than Licensed or Hosted
- Organization Integration Needs
- Often Consumer Oriented Functionality
  (Ex. Facebook Login)

Positive Issues With SaaS

- Common Code Base & Easier Upgrades
- Mobile & Easy Initial Deployment
- Pay As You Go Model
- Scalability
- Simple Disaster Recovery
- Geo Replication
Data Management In Pools – Top Goals

Find Your Blend

- High Performance
- Security
- Privacy
- Compliance

Don’t Be A Target

www.davidcorp.com
Disaster Recovery

Q? How do we really give Disaster Recovery a good test?

- Disaster Recovery Testing is not a single occurrence or event; it is an ongoing process.
- Test for system failure, data theft and data corruption.
- In some cases, the cost of maintaining a Disaster Recovery mindset and performing Simulation Testing can actually outweigh the risk and cost of an actual disaster.
- Focus on the anticipated types of disasters, probability of occurrence, and projected damage associated to better understand the actual financial impact. The results can then be weighed against the cost of an accommodating Disaster Recovery Plan to ensure financial feasibility.
Q. How do we keep personal identifiable information (PII) out of the e-mail system?

Reduce the risk of exposure is to look towards alternate communication mechanisms altogether, understanding email is a highly insecure platform by nature and often overused.

When there is no alternative but to email PII, measures should be taken to use either message- or transport-based encryption.
Are there solutions to better help support the following member management activities?

<table>
<thead>
<tr>
<th>Manage program membership</th>
<th>Manage and track participation in training, return to work or triage programs, EAP programs, or other pool activities</th>
<th>Manage and track member contributions; and determine and provide ex-mods</th>
</tr>
</thead>
<tbody>
<tr>
<td>start and stop dates, retentions, locations and contacts</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Data Management Risk Questions

• Are there new **Threats**?
• Do I have new **Vulnerabilities**?
• Is there an increased **Likelihood** of Occurrence?
• Has the **Impact** increased?
Q? - Guidance on When to Use Cloud?

• **Cloud can also be a way to increase IT resources in line with your business needs.**
  – Ramp up resources when you need more
  – Ramp down resources when not needed
  – Avoid on-going capital outlays

• **Cloud Can Be A Tool for Risk Management**
  – Assume
  – Reduce/Control/Mitigate
  – Transfer
  – Avoid
When to Use IT Data Architecture?

Combination of Risk Transfer, Control/Mitigation, Avoidance, or Assumption

Combination of Risk Transfer, Control/Mitigation, Avoidance, or Assumption

Default

Combine of Risk Transfer, Control/Mitigation, Avoidance, or Assumption

Combination of Risk Transfer, Control/Mitigation, Avoidance, or Assumption

Depends on Organizational Capabilities and Risk Tolerance

Transfer

Low

High

Impact

Low

High

Likelihood

Depends on Organizational Capabilities and Risk Tolerance

Assume

Transfer

Avoid

Control/Mitigate

Assume

Transfer

Avoid