



## Health Check Cyber Risk Assessment

2018 Final Report



Conference Call Findings for Client: Red Feather Mountain Library District

Client Vertical	Public Entity
Client Contact	Creed Kidd Library Director <a href="mailto:Director@RedFeatherLibrary.org">Director@RedFeatherLibrary.org</a> 970-881-2664
Date Prepared	3/28/2018
Report Author	Dave Chatfield

**NetDiligence Summary Findings**

**Subjective Grade and Opinion Statement (Covering Sections 1-8)**

Client's Posture	Grade Level	Opinion Statement
<input type="checkbox"/>	A+	Appears to have full suite of Superior Safeguards & Practices in place. (100% of below listed controls/ practices)
<input type="checkbox"/>	A	Appears to have full suite of 'best of class' network security technical safeguards in place that meet a baseline due care protection standard. Also, solid procedures, policies and processes exist to mitigate potential network-emanating liability events. This combined approach should serve to mitigate a direct loss as well as liability event.
X	B+	Appears to have the essential 'baseline' network security technical safeguards in place that meet a baseline due care protection standard. Also, some policies and processes exist to mitigate potential network-emanating liability events. This combined approach should serve to mitigate a direct loss as well as liability event.
<input type="checkbox"/>	C	Appears to have the majority of 'baseline' network security technical safeguards in place, but improvement is recommended. Also, some policies and processes exist to mitigate potential network-emanating liability events.
<input type="checkbox"/>	F	There appears to be some significant weaknesses in protecting the network. Some essential 'baseline' network security technical safeguards are NOT in place. Also, some policies and processes are NOT in place that might serve to increase the frequency or severity of potential network-emanating liability events.

**Breach Response Preparedness (Covering Sections 9-10)**

Client's Posture	Grade Level	Opinion Statement
<input type="checkbox"/>	A+	Best in class capabilities involving both incident response management and privacy/breach notification functions. Completeness, efficiency, and effectiveness have been maximized to the greatest possible extent. Best in class capabilities involving both incident response management and privacy/breach notification functions. Completeness, efficiency, and effectiveness have been maximized to the greatest possible extent.
X	A	Solid incident response management that follows industry standard practices. Strong integration between the technical (IT, IT Security) and compliance (Legal, Privacy, Compliance) teams to ensure effective end-to-end handling of incidents as they arise and prompt notifications where deemed necessary.
<input type="checkbox"/>	B	Functional incident response and privacy/compliance functions. Important emphasis placed upon breach notifications if that is where the evidence leads.
<input type="checkbox"/>	C	Uneven, weakly structured, and/or ad hoc-based capabilities involving incident response and/or subsequent privacy management capabilities. Greater emphasis here should be a high priority in the near term.
<input type="checkbox"/>	F	No evidence of an organized incident response capability or privacy management function, and no apparent corporate recognition of their importance at this time.

**Presence of Key Security Controls for This Vertical**

Key Security Controls	Present?
1. Experienced/credentialed information security management on staff	External Consultant
2. PCI-approved POS application used in retail locations	N/A
3. PCI data encrypted while at-rest and in-transit within company IT systems or eliminated entirely from production environment	N/A
4. IDS capabilities are reasonable	YES
5. Application level scan testing and programming practices insure against SQL injection and other well-known weaknesses	N/A
6. Proof of effective general vulnerability scanning and remediation efforts	NO
7. Redundancy of mission-critical systems	YES
8. Tested disaster recovery plans in place	Partial
9. Functioning change and patch management process in place	YES
10. Effective privacy policy and aligned IT procedures	YES

**Significant Findings / Recommendations**

1.	Section 2	We believe Red Feather needs to develop and implement a baseline vendor security management program.
----	-----------	--

**Additional Comments**

We believe that the Red Feather Mountain Library District (hereafter, Red Feather) maintains a moderately effective overall information security profile – relative in part to the nature, size, and IT footprint of the organization (and a few of our “Strong” opinions take these factors into account). We noted specific areas of maturity in system/network operations (Section 7), and within incident response and data privacy capabilities (Sections 9 & 10 combined). We also sensed what appears to be a lack of any present effort within vendor security management (Section 2), and recommend near-term efforts along these lines. Finally, we learned in our conversations with Library management that Red Feather appears to have significant external recourse to both an experienced consultant and the Colorado State Library in cases where additional expertise may be needed.

**Conclusion**

<input type="checkbox"/>	Acceptable – Appears to have <b>SUPERIOR BEST IN CLASS</b> practices overall
<input type="checkbox"/>	Acceptable – Based on information as received
<b>x</b>	Acceptable – With <b>COMPLIANCE TO RECOMMENATIONS ABOVE</b>
<input type="checkbox"/>	NOT ACCEPTABLE – <b>SIGNIFICANT UNRESOLVED WEAKNESSES OR UNKNOWNNS</b>

## Common Acronyms Used In This Report

Our reports often reference a number of acronyms common to the information technology, information security and privacy sectors. We have included here a brief list of those that may have been included in this report and their associated descriptions (and additional explanations where possible):

<b>Acronym</b>	<b>Full Description</b>
ASP	Application Service Provider (vendor who provides remote hosting of applications)
ASV	Approved Scan Vendor (must be chosen to perform PCI vulnerability scans in certain cases)
BYOD	Bring-Your-Own-Device (i.e., personal use smartphones with company email, usually via MDM)
CPO	Chief Privacy Officer (organizational leader responsible for privacy program effectiveness)
DLP	Data Loss Prevention (filtering program looking for instances of sensitive information, e.g. SSNs)
DR/BCP	Disaster Recovery and/or Business Continuity Plan (enterprise IT and business function restore plans)
EMV	Europay, MasterCard, Visa (entities requiring “chip & PIN” pay feature)
FTP, SFTP	File Transport Protocol / Secure File Transport Protocol (file sending programs)
HIPAA	Health Insurance Portability and Accountability Act (1996 U.S. health care law)
IDS/IPS	Intrusion Detection and/or Prevention System (technology to detect/prevent Internet-facing exploits)
IRP	Incident Response Plan or Program (documented procedures for dealing with incidents/breaches)
ISO 27001	International Standards Organization #27001 (international IT security standard)
MDM	Mobile Device Management (IT-team controlled application that manages remote smart devices)
MS SQL	Microsoft’s Structured Query Language database server product
MSSP	Managed Security Services Provider (vendor who typically provides 24x7 security services support)
NIST	National Institute of Standards and Technology (U.S. standards body)
OWASP	Open Web Application Security Project (global application security site, <a href="http://www.owasp.org">www.owasp.org</a> )
PCI	Payment Cardholder Industry (jointly supported by major card brands)
PCI DSS	PCI Data Security Standards (version 3.2 is latest as of 5/1/2018)
PHI	Protected Health Information (in U.S. HIPAA law, this is nearly all patient/dependent medical info)
PII	Personally Identifiable Information (typically, client or employee SSNs, DoB, addresses, etc.)
POS	Point-of-Sale (e.g., card swipe device)
RDP, VDI	Remote Desktop Protocol (Microsoft), Virtual Data Interface (VMware) remote session programs)
RTO, RPO	Recovery Time Objective / Recovery Point Objective (SLA recovery goals in minutes, hours, or days)
SANS	System Administration, Networking, and Security Institute ( <a href="http://www.sans.org">www.sans.org</a> )
SAQ	Self-Assessment Questionnaire (must be filled out annually by PCI Merchants)
SIEM	Security Information & Event Management (central platform that collects/analyzes security log info)
SLA	Service Level Agreement (i.e., determines compensation for service outages)
SSAE 16	Statement on Standards for Attestation Engagements #16 (typically, a large data center audit report)
SSL	Secure Sockets Layer (common encryption standard)
UPS	Uninterruptable Power Supply (short-term power, usually via battery source, until generator starts)
USB	Universal Serial Bus (data connector type for PCs, smartphones, printers, pads, etc.)
VPN	Virtual Private Network (allows encrypted remote connectivity sessions)
WEP	Wired Equivalent Privacy (older wireless encryption standard, now obsolete and easily compromised)
WPA, WPA2	Wi-Fi Protected Access (encryption standards for wireless local area networks, two versions exist)

## NetDiligence Detailed Findings

### 0. Nature of Environment and Types of Sensitive Customer Information Present

#### Topics Covered

##### Overall Environment

Total number of employees:	5
Total number of individual clients or transactions/year:	~2,200 Library Cards issued; 50K transactions/year
Total number of production servers being managed:	No production servers on-site; all 3 <sup>rd</sup> -party hosted
Dominant brands/versions of SQL databases in use:	Koha LibLime (built upon MySQL)
Total number of employee laptops; % encrypted:	2; none encrypted, no PII present
Total number of managed MDM/BYOD devices:	3 BYOD devices

##### Estimates of Sensitive Data Storage Hosted in Off-Premise Third Party and/or Cloud-Based Vendor Settings

Please identify each of your cloud services providers by name, *and to the extent possible, identify the presence and/or estimate the numbers for each type of record that is entrusted to the care of each vendor.*

Hosted or Cloud Services Vendor	CloudeAssurance** Published Score (Provisional or Validated)	Public/ Non-Sensitive Info	Personally Identifiable Info (PII)	Protected Health Info (PHI)	Payment Cardholder Info (PCI)	Competitive Business Info
Amazon	488	Yes				
Microsoft	596	Yes				
Google	N/A	Yes	Yes			
Koha LibLime	N/A	Yes	Yes			

\*\* For cloud-based vendors with current CloudeAssurance evaluation scores available, we have re-published them here and provided additional details at the end of this report.

## 1. Security Organization, Personnel Security

### Topics Covered

- Current FTE staffing & roles of dedicated information security team; planned near-term additions?
- Current or anticipated reliance upon outsourcing of security tasks to third-party vendors?
- Any significant business acquisitions underway/completed? How have information security practices been evaluated – and what integration plans exist for these new business units?
- What well-known security standards (e.g., ISO 27001/2, NIST, HIPAA, PCI) do you rely upon in developing/implementing/enforcing organization-wide information security policies and practices?
- Pre-employment screening for ALL new hires to include criminal checks?
- Security awareness training: new hire orientation AND annual refresher requirements? How delivered?
- Have you focused recent employee training emphasis on ransomware and targeted phishing efforts (both of which represented especially frequent breach incidents during 2016)?
- Please identify key information security projects and/or solution deployments for the next 12 months?

### Findings

	Appears to have superior <b>BEST IN CLASS</b> practices	<p>Findings for <b>ALL</b> clients 01/2015-06/2016:</p>  <p>2015-16 Client Population % by Sector:</p> <ul style="list-style-type: none"> <li>22% Financial, Insurance &amp; Legal</li> <li>19% Healthcare</li> <li>17% Retail</li> <li>11% Technology, Consulting &amp; Media</li> <li>11% Manufacturing</li> <li>6% Energy</li> <li>3% Public Sector &amp; Non-Profit</li> <li>11% All Others</li> </ul>
<b>X</b>	Appears to have <b>STRONG</b> practices	
	Appears to have minimum <b>BASELINE</b> practices	
	Appears to have one or more key <b>WEAKNESSES</b> noted	
Notes	<p>With only 5 total employees, Red Feather Mountain Library District (henceforth, “Red Feather”) entrusts shared responsibility for information security between its Director and Financial Officer – and, by extension, among the outsourced IT/application vendors upon whom the District relies upon for online services – which notably includes the Colorado State Library. Red Feather also has access to an experienced network consultant (Carson Block) who has worked with library entities throughout the State. Business acquisition is not a foreseeable task for Red Feather, so our security integration question is N/A. As for security-related standards, management noted that they are well-versed in the State’s statute on user confidentiality, as well as HIPAA (the latter for the benefit of employee data</p>	

	<p>protection). Employee candidates and volunteers each undergo a full criminal background check prior to hire. Security and user privacy are topics reportedly covered frequently in employee/volunteer meetings. Ransomware has been a recent priority topic for Red Feather, and toward this end, management has both informed employees of the risks and installed anti-ransomware software (Cybereason RansomFree, see: <a href="https://ransomfree.cybereason.com/">https://ransomfree.cybereason.com/</a>) on workstations. Recent projects for Red Feather have included the evaluation and use of several endpoint protection tools (e.g., PrivacyBadger, SSEverywhere, AdBlocker). <b>Given Red Feather's size, mission, availability of resources, and management focus on security/privacy-centric topics, we believe it is reasonable to offer a "Strong" opinion for this Section at the present time.</b></p>
	<p>We recommend you utilize the following resources available in the eRisk Hub. Don't have access to the <a href="#">eRisk Hub</a>? Come see what you are missing – ask your broker/underwriter for your free membership access as part of your cyber insurance policy coverage. Or please email <a href="mailto:Management@NetDiligence.com">Management@NetDiligence.com</a>.</p> <p><b>Risk Manager Tools (Free):</b></p> <ul style="list-style-type: none"> <li>• <a href="#">Vendor Security Due Diligence Checklist</a></li> <li>• Sample eRisk Hub Policies:             <ul style="list-style-type: none"> <li>▪ <a href="#">Information Security Policy Template</a></li> <li>▪ <a href="#">Physical Security Policy Template</a></li> <li>▪ <a href="#">Security Awareness Training and Education Policy Template</a></li> <li>▪ <a href="#">Security Policy 101 – Essential Policies for Business</a></li> </ul> </li> </ul> <p><b>Articles &amp; Whitepapers (Free):</b></p> <ul style="list-style-type: none"> <li>• <a href="#">Seven Requirements for Successfully Implementing Information Security Policies and Standards</a></li> </ul>
	<p>Several vendors provide remediation and/or outsourced services for suggestions or recommendations identified in the "Notes" for this Section. We list some of these below <b>without specific endorsement from NetDiligence</b> (although some may be listed in the eRisk Hub).</p> <p><b>Options for Outsourced Security Management, Tasks or Staffing:</b></p> <ul style="list-style-type: none"> <li>• Citadel Information Group – see: <a href="http://www.citadel-information.com">www.citadel-information.com</a>, Phone: 323.428.0441, Email: <a href="mailto:stan@citadel-information.com">stan@citadel-information.com</a></li> <li>• Integrity Technology Systems, Inc. – see: <a href="http://www.integritysrc.com">www.integritysrc.com</a>, Phone: 515.528.0023, Email: <a href="mailto:Leslie.Matheson@IntegritySRC.com">Leslie.Matheson@IntegritySRC.com</a></li> <li>• Emerald Data Networks – see: <a href="http://www.emeralddata.net">www.emeralddata.net</a>, Phone: 678.302.3000, Email: <a href="mailto:drodgers@emeralddata.net">drodgers@emeralddata.net</a></li> <li>• Loricca, Inc. (HIPPA only) – see: <a href="http://loricca.com">loricca.com</a>, Phone: 813.600.3005 x102, Email: <a href="mailto:mwhitcomb@loricca.com">mwhitcomb@loricca.com</a></li> <li>• Integrated Systems Consultants (HIPPA only) – see: <a href="http://www.i-s-c.com">www.i-s-c.com</a>, Phone: 231.492.0472, Email: <a href="mailto:tfairchild@i-s-c.com">tfairchild@i-s-c.com</a></li> </ul> <p><b>Options for Employee Security Awareness Training:</b></p> <ul style="list-style-type: none"> <li>• Click 4 Compliance – see: <a href="http://www.click4compliance.com">www.click4compliance.com</a>, Phone: 703.787.9492, Email: <a href="mailto:info@click4compliance.com">info@click4compliance.com</a></li> <li>• Wombat Security Technologies, Inc. – see: <a href="http://www.wombatsecurity.com">www.wombatsecurity.com</a>, Phone: 412-621-1484 x114, Email: <a href="mailto:r.massaro@wombatsecurity.com">r.massaro@wombatsecurity.com</a></li> <li>• Supremus Group LLC (HIPPA only) – see: <a href="http://www.training-hipaa.net">www.training-hipaa.net</a>, Phone: 515.865.4591, Email: <a href="mailto:Bob@Training-HIPAA.net">Bob@Training-HIPAA.net</a></li> </ul> <p><b>Options for Network Security Software Solutions:</b></p> <ul style="list-style-type: none"> <li>• General Dynamics Fidelis Cybersecurity Solutions – see: Phone: 703.286.5820, Email: <a href="mailto:barnaby.page@fidelissecurity.com">barnaby.page@fidelissecurity.com</a></li> <li>• Carbon Black – see: <a href="http://www.carbonblack.com">www.carbonblack.com</a>, Phone: 610.639.1492, Email: <a href="mailto:michael.viscuso@getcarbonblack.com">michael.viscuso@getcarbonblack.com</a></li> <li>• McAfee – see: <a href="http://www.mcafee.com/us">www.mcafee.com/us</a>, Phone: 408.346.5295, Email: <a href="mailto:Visshwanth.Reddy@McAfee.com">Visshwanth.Reddy@McAfee.com</a></li> </ul>

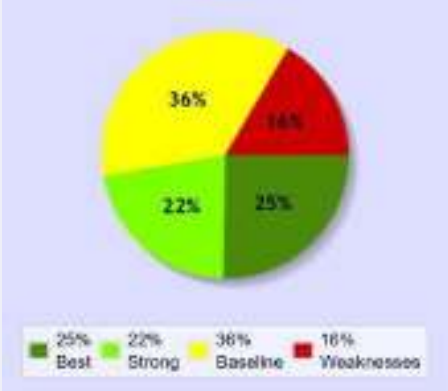


## 2. Vendor Security Management

### Topics Covered

- Do you have a program to review the security/privacy practices of key third-party vendors/prospects?
- Do you require the completion of a security practices questionnaire and negotiate gap remediation?
- Do you review vendor submitted copies of SSAE 16, PCI, and/or other types of audit reports?
- Do you enforce any special requirements for entrusting vendors with sensitive PII/PCI/PHI information?
- Do you require indemnification in your favor in service contracts addressing vendor breaches/failures?
- Do you require vendors to carry cyber risk insurance policy coverage as a contract condition?
- Have you experienced any significant vendor-caused data breaches or service failures in the past year?

### Findings

	Appears to have superior <b>BEST IN CLASS</b> practices	<p>Findings for <b>ALL</b> clients 01/2015-06/2016:</p>  <p>2015-16 Client Population % by Sector:</p> <ul style="list-style-type: none"> <li>22% Financial, Insurance &amp; Legal</li> <li>19% Healthcare</li> <li>17% Retail</li> <li>11% Technology, Consulting &amp; Media</li> <li>11% Manufacturing</li> <li>6% Energy</li> <li>3% Public Sector &amp; Non-Profit</li> <li>11% All Others</li> </ul>
	Appears to have <b>STRONG</b> practices	
	Appears to have minimum <b>BASELINE</b> practices	
<b>X</b>	Appears to have one or more key <b>WEAKNESSES</b> noted	
Notes	<p>Based upon our conversation, management does not appear to have participated in vendor security management to any significant degree to-date, <b>and Red Feather appears to have enough interaction with external vendors to warrant at least a baseline effort here going forward.</b> That having been said, it appears likely that Red Feather benefits to some extent in this area from their relationship with the Colorado State Library, who may well have additional bandwidth and resources to conduct vendor security reviews as part of their overall mission. <b>Within Red Feather's more immediate setting, we would suggest that management begin implementing the following tasks as they review present and future vendor relationships: (a) request completion of a basic information security questionnaire (and management welcomed a copy of our sample template), (b) in applicable cases, request current copies of SSAE 16 data center audits, PCI compliance statements, and/or security practices summaries and ensure that the results are consistent with Red Feather's expectations for effective protections, (c) to the extent that any customer/employee PII/PHI/PCI data is entrusted with a</b></p>	

*vendor, request specific assurances as to data privacy protection efforts, (d) as a hedge against both service resiliency and data privacy incidents caused by vendors, require inclusion of indemnification terms in service contracts that make Red Feather whole following such events, and (e) requiring evidence that each vendor carries current cyber insurance policy coverage. We should also note the likely possibility that the Colorado State Library and/or other CO-led agencies that benefit Red Feather’s mission may already have some of these elements in place at a State-wide level (e.g., via State purchasing contracts) – and management will want to familiarize itself with any such efforts.*

Management advised that Red Feather has never suffered a vendor-caused data privacy breach, but also noted that that periodic vendor service interruptions do take place periodically, mostly temporary in nature and often in response to poor weather conditions.

We recommend you utilize the following resources available in the eRisk Hub. Don’t have access to the [eRisk Hub](#)? Come see what you are missing – ask your broker/underwriter for your free membership access as part of your cyber insurance policy coverage. Or please email [Management@NetDiligence.com](mailto:Management@NetDiligence.com).

Risk Manager Tools (Free):

- [Cloud Risk Considerations](#)

Articles & Whitepapers (Free):

- [Quiz: Cloud Computing Security Awareness](#)
- [Eight Security Concerns Before Jumping Into the Cloud](#)
- [Protecting Your Data in the Cloud in 2013, Remember D.A.R.T](#)
- [Cloud Security: Pulling Back the Curtain](#)
- [The Dos and Don’ts of Navigating The Cloud: A Business Guide For Cloud Computing](#)

Several vendors provide remediation and/or outsourced services for suggestions or recommendations identified in the “Notes” for this Section. We list some of these below *without specific endorsement from NetDiligence* (although some may be listed in the eRisk Hub).

Options for Vendor Security Program Development:

- Loricca, Inc. (HIPPA only) – see: [loricca.com](http://loricca.com), Phone: 813.600.3005 x102, Email: [mwhitcomb@loricca.com](mailto:mwhitcomb@loricca.com)

Options for Cloud-based Vendor Security Reviews:

- ISCA Labs – see: [www.icsalabs.com](http://www.icsalabs.com) Email: [Management@NetDiligence.com](mailto:Management@NetDiligence.com)

Options for Vendor Management Legal/Indemnification Reviews:

- Faruki Ireland & Cox P.L.L. - Ronald I. Raether, Esq. – see: [www.ficlax.com](http://www.ficlax.com), Phone: 937.227.3733, Email: [rraether@ficlaw.com](mailto:rraether@ficlaw.com)
- InfoLawGroup – see: [www.infolawgroup.com](http://www.infolawgroup.com), Phone: 303.325.3528, Email: [dnavetta@infolawgroup.com](mailto:dnavetta@infolawgroup.com)

Options for Cloud Encryption Solutions:

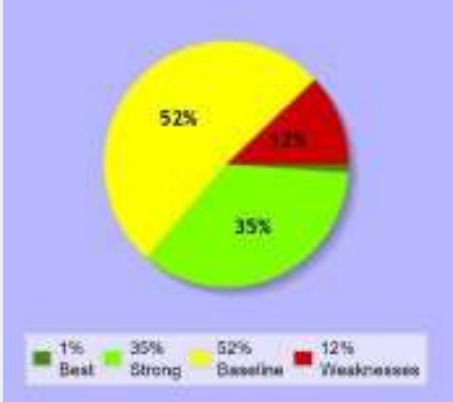
- Townsend Security – see: [townsendsecurity.com](http://townsendsecurity.com), Phone: 360.359.4408, Email: [luke.probasco@townsendsecurity.com](mailto:luke.probasco@townsendsecurity.com)
- Trend Micro, Inc. – see: [www.trendmicro.com](http://www.trendmicro.com), Phone: 202.415.3955. Email: [tom\\_kellermann@trendmicro.com](mailto:tom_kellermann@trendmicro.com)
- Lockbox LLC – see: [www.goironbox.com](http://www.goironbox.com), Phone: 206.619.4226, Email: [kevinlam@golockbox.com](mailto:kevinlam@golockbox.com)

### 3. PCI DSS Compliance

#### Topics Covered

- Date and compliance status of most recent PCI DSS v3.2 SAQ (or QSA-certified ROC)? ASV Scans?
- If payment processing is outsourced, do you request/review PCI compliance statements from each of the processors on an annual basis?
- Identify PCI-Validated Point-of-Sale solutions used in retail and online e-commerce sites?
- Do you have plans to migrate to Point-to-Point Encryption (P2PE) for your Point-of-Sale platforms?
- Full at-rest encryption of PCI cardholder data or total elimination from environment?
- If relevant to your e-commerce settings, have you fully addressed/resolved the SSL/early TLS exposure issues that PCI has mandated for resolution in 2018?

#### Findings

	Appears to have superior <b>BEST IN CLASS</b> practices	<p>Findings for <b>ALL</b> clients 01/2015-06/2016:</p>  <p>2015-16 Client Population % by Sector:</p> <ul style="list-style-type: none"> <li>22% Financial, Insurance &amp; Legal</li> <li>19% Healthcare</li> <li>17% Retail</li> <li>11% Technology, Consulting &amp; Media</li> <li>11% Manufacturing</li> <li>6% Energy</li> <li>3% Public Sector &amp; Non-Profit</li> <li>11% All Others</li> </ul>
	Appears to have <b>STRONG</b> practices	
<b>X</b>	Appears to have minimum <b>BASELINE</b> practices	
	Appears to have one or more key <b>WEAKNESSES</b> noted	
Notes	<p>Management advised that Red Feather does not accept credit/debit cards for payment of fees/fines associated with library operations, and has no expectations of doing so at any point in the near-to-medium term. All such transactions are conducted by cash or check only. Within this context, Red Feather appears to have no compliance obligations under PCI DSS at this time – <b>and we assign a default “Baseline” opinion in this section for all similarly situated assessment clients.</b> For management’s educational benefit, we provided a recent copy of the PCI DSS compliance standards so that they can get a working familiarity with the nature of their obligations should Red Feather ever choose to accept card payments at some future date.</p>	
<p>We recommend you utilize the following resources available in the eRisk Hub. Don’t have access to the <a href="#">eRisk Hub</a>? Come see what you are missing – ask your broker/underwriter for your free membership access as part of your cyber insurance policy coverage. Or please email <a href="mailto:Management@NetDiligence.com">Management@NetDiligence.com</a>.</p>		

Risk Manager Tools (Free):

- [Sensitive Information Handling Policy](#)
- [State Security Breach Laws Response Guide](#)

Articles & Whitepapers (Free):

- [Revisiting PCI](#)
- Credit Card Data Security Standard Updates, Is Your Organization Aware?
- [When It Comes to PCI Data Breach Investigations, Organizations Are Well Served to “Declare Their Independence”](#)
- [Payment Cards and Data Breaches with Grayson Lenik, Trustwave](#)

Several vendors provide remediation and/or outsourced services for suggestions or recommendations identified in the “Notes” for this Section. We list some of these below **without specific endorsement from NetDiligence** (although some may be listed in the eRisk Hub).

Options for PCI Compliance Assessments and Support:

- Trustwave – see: [www.trustwave.com](http://www.trustwave.com), Phone: 406.422.5107, Email: [glenik@trustwave.com](mailto:glenik@trustwave.com)
- Crimson Security – see: [crimsonsecurityinc.com](http://crimsonsecurityinc.com), Phone: 631.265.3564, Email: [narender.mangalam@crimsonsecurity.com](mailto:narender.mangalam@crimsonsecurity.com)
- 360 Advanced – see: [www.360advanced.com](http://www.360advanced.com), Phone: 866.418.1708 x710 Email: [eratcliffe@360advanced.com](mailto:eratcliffe@360advanced.com)
- Schneider Downs – see: [www.schneiderdowns.com](http://www.schneiderdowns.com), Phone: 614.586.7108 Email: [cdebo@schneiderdowns.com](mailto:cdebo@schneiderdowns.com)

## 4. Encryption-Related Capabilities

### Topics Covered

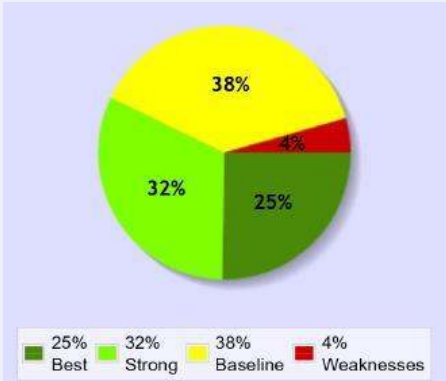
In-transit encryption for: *(Please Identify deployed solutions for each setting)*

- VPNs and/or dedicated lines to partners, customers, service providers?
- Secure FTP, vendor cloud, or file-level encryption for transmission over the Internet?
- E-mail transmission?
- Wireless via WPA/WPA2 or other advanced protocols (and elimination of WEP)?

At-rest encryption for: *(Please identify deployed solutions for each setting)*

- Backup tapes and other archival media?
- Production databases and unstructured file servers?
- Employee laptops and other mobile computing devices?
- USB Thumb Drives and other mobile storage devices?

### Findings

	Appears to have superior <b>BEST IN CLASS</b> practices	<p>Findings for <b>ALL</b> clients 01/2015-06/2016:</p>  <p>2015-16 Client Population % by Sector:</p> <ul style="list-style-type: none"> <li>22% Financial, Insurance &amp; Legal</li> <li>19% Healthcare</li> <li>17% Retail</li> <li>11% Technology, Consulting &amp; Media</li> <li>11% Manufacturing</li> <li>6% Energy</li> <li>3% Public Sector &amp; Non-Profit</li> <li>11% All Others</li> </ul>
	Appears to have <b>STRONG</b> practices	
<b>X</b>	Appears to have minimum <b>BASELINE</b> practices	
	Appears to have one or more key <b>WEAKNESSES</b> noted	
Notes	In-transit capabilities include: TLS/SSL-supported use of Google Drive for some business requirements, and WPA2 for WiFi for staff and public use in segregated LAN segments. Red Feather has not yet demonstrated a business need for VPN technology, and use of e-mail for transmission of sensitive files is highly discouraged ( <b>and we would suggest mandated use of file-level password protection – at a minimum – in such cases</b> ; management advised that they will investigate current use of e-mail transmission by Red Feather’s CPA and adjust accordingly if needed).	

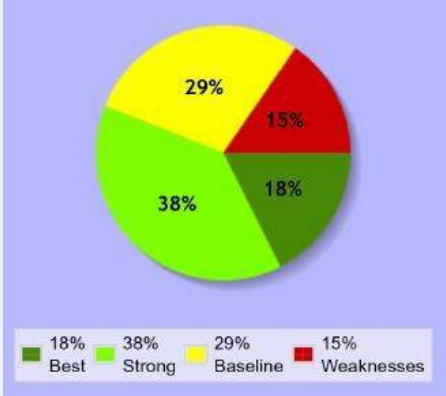
	<p>At-rest capabilities include: Weekly backups to a portable drive are encrypted, and the financial officer’s workstation is also encrypted. The Library’s two laptops (and any associated USB devices) are not encrypted, with management advising that no sensitive data resides on either of these devices – <b><i>and we would suggest continued review of such devices in evaluating whether cyber exposure risks might necessitate use of encryption in these cases.</i></b></p>
<p>We recommend you utilize the following resources available in the eRisk Hub. Don’t have access to the <a href="#">eRisk Hub</a>? Come see what you are missing – ask your broker/underwriter for your free membership access as part of your cyber insurance policy coverage. Or please email <a href="mailto:Management@NetDiligence.com">Management@NetDiligence.com</a>.</p> <p><u>Risk Manager Tools (Free):</u></p> <ul style="list-style-type: none"> <li>• <a href="#">Small Business Cyber Security Planning Guide</a></li> <li>• <a href="#">HIPAA Security Rule: Frequently asked questions regarding encryption of PII</a></li> <li>• <a href="#">Acceptable Use Policy (Sample Policy)</a></li> </ul> <p><u>Articles &amp; Whitepapers (Free):</u></p> <ul style="list-style-type: none"> <li>• <a href="#">Encryption &amp; Key Management – Best Practices</a></li> <li>• <a href="#">Encrypting Email for Data Security</a></li> </ul>	
<p>Several vendors provide remediation and/or outsourced services for suggestions or recommendations identified in the “Notes” for this Section. We list some of these below <b><i>without specific endorsement from NetDiligence</i></b> (although some may be listed in the eRisk Hub).</p> <p><u>Options for Enterprise Encryption Solutions:</u></p> <ul style="list-style-type: none"> <li>• Symantec – see: <a href="http://www.symantec.com">www.symantec.com</a></li> <li>• McAfee – see: <a href="http://www.mcafee.com">www.mcafee.com</a></li> <li>• Sophos – see: <a href="http://www.sophos.com">www.sophos.com</a></li> </ul> <p><u>Options for Secure Email Encryption:</u></p> <ul style="list-style-type: none"> <li>• Zix Corporation – see: <a href="http://www.zixcorp.com">www.zixcorp.com</a></li> <li>• Tumbleweed/Axway – see: <a href="http://www.axway.com">www.axway.com</a></li> </ul> <p><u>Options for Backup Tape Encryption:</u></p> <ul style="list-style-type: none"> <li>• IBM Tivoli Storage Manager (TSM) – <a href="http://www.ibm.com">www.ibm.com</a></li> </ul> <p><u>Options for Database Encryption:</u></p> <ul style="list-style-type: none"> <li>• Microsoft SQL Server – see: <a href="http://www.microsoft.com">www.microsoft.com</a></li> <li>• Oracle – see: <a href="http://www.oracle.com">www.oracle.com</a></li> </ul> <p><u>Options for Laptop Encryption:</u></p> <ul style="list-style-type: none"> <li>• PGP – see: <a href="http://www.pgp.com">www.pgp.com</a></li> <li>• Pointsec – see: <a href="http://www.checkpoint.com">www.checkpoint.com</a></li> <li>• TrueCrypt – see: <a href="http://www.truecrypt.com">www.truecrypt.com</a></li> </ul> <p><u>Options for USB Encryption:</u></p> <ul style="list-style-type: none"> <li>• IronKey – see: <a href="http://www.ironkey.com">www.ironkey.com</a></li> </ul> <p><u>Options for Cloud Encryption:</u></p> <ul style="list-style-type: none"> <li>• Townsend Security – see: <a href="http://townsendsecurity.com">townsendsecurity.com</a>, Phone: 360.359.4408, Email: <a href="mailto:luke.probasco@townsendsecurity.com">luke.probasco@townsendsecurity.com</a></li> <li>• Trend Micro, Inc. – see: <a href="http://www.trendmicro.com">www.trendmicro.com</a>, Phone: 202.415.3955. Email: <a href="mailto:tom_kellermann@trendmicro.com">tom_kellermann@trendmicro.com</a></li> <li>• Lockbox LLC – see: <a href="http://www.goironbox.com">www.goironbox.com</a>, Phone: 206.619.4226, Email: <a href="mailto:kevinlam@golockbox.com">kevinlam@golockbox.com</a></li> </ul>	

## 5. Technical Compensating/Contributing Controls

### Topics Covered

- In addition to perimeter firewalls, do you also enforce internal segregation of sensitive file servers/databases to ensure restricted access from within the organization?
- What branded solutions are you currently using for multi-factor authentication? In what settings?
- Have you deployed remote session serving software (e.g., Citrix, MS RDP, VMWare VDI) to reduce or eliminate reliance upon locally stored data on employee workstations/laptops?
- Strong user account provisioning/termination, role-based access assignments, password management?
- How do you regularly monitor/audit regular and administrative user account activity?
- What data loss prevention (DLP) solutions have you deployed at the e-mail gateway, internal network, and/or server/endpoint settings? How have these helped with detection efforts?
- What vulnerability scanning solutions (in-house, ASP, and/or cloud-based) are currently used for both public-facing and internal network environments? How are findings addressed?
- In addition, who performs independent/third-party penetration testing against your environments?

### Findings

	Appears to have superior <b>BEST IN CLASS</b> practices	<p>Findings for <b>ALL</b> clients 01/2015-06/2016:</p>  <p>2015-16 Client Population % by Sector:</p> <ul style="list-style-type: none"> <li>22% Financial, Insurance &amp; Legal</li> <li>19% Healthcare</li> <li>17% Retail</li> <li>11% Technology, Consulting &amp; Media</li> <li>11% Manufacturing</li> <li>6% Energy</li> <li>3% Public Sector &amp; Non-Profit</li> <li>11% All Others</li> </ul>
	Appears to have <b>STRONG</b> practices	
<b>X</b>	Appears to have minimum <b>BASELINE</b> practices	
	Appears to have one or more key <b>WEAKNESSES</b> noted	
Notes	<p>Management advised that Red Feather makes use of some of the above-listed controls within its environment. Notable examples include: (a) VLAN segregation of WiFi segments according to function and employee/public use requirements, (b) use of a remote-session serving package by Red Feather's CPA in order to get to their office-based workstation from remote locations via firewall policy rules and workstation-level authentication (and we would suggest augmentation of this access function via a two-factor authentication requirement and/or full-featured VPN implementation in the near-to-medium term), (c) management maintains localized/locked lists of passwords for both regular and</p>	

	<p>privileged users (with permitted access on a restricted basis, including for the Board of Trustees if an emergency dictates), and (d) use of LastPass to compel password composition/change non-repeat rules. <b><i>Going forward, we would also suggest consideration of the following capabilities for the near-term: (a) consider two-factor/VPN capabilities for the CPA scenario described above, and (b) periodic use of external vulnerability scanning to guard against undetected weaknesses in Red Feather’s public-facing environment.</i></b></p>
<p>We recommend you utilize the following resources available in the eRisk Hub. Don’t have access to the <a href="#">eRisk Hub</a>? Come see what you are missing – ask your broker/underwriter for your free membership access as part of your cyber insurance policy coverage. Or please email <a href="mailto:Management@NetDiligence.com">Management@NetDiligence.com</a>.</p> <p><u>Risk Manager Tools (Free):</u></p> <ul style="list-style-type: none"> <li>• <a href="#">Expanded eRisk Self-Assessment</a></li> <li>• <a href="#">Quick eRisk Assessment</a></li> </ul>	
<p>Several vendors provide remediation and/or outsourced services for suggestions or recommendations identified in the “Notes” for this Section. We list some of these below <b><i>without specific endorsement from NetDiligence</i></b> (although some may be listed in the eRisk Hub).</p> <p><u>Options for IT Management Services/Consulting:</u></p> <ul style="list-style-type: none"> <li>• LWG Consulting, Inc. – see: Phone: 847-559-3000 x7076, E-Mail: <a href="mailto:tchrist@lwgconsulting.com">tchrist@lwgconsulting.com</a></li> <li>• Mandiant Corporation – see: Phone: 703-683-3141, E-Mail: <a href="mailto:investigations@mandiant.com">investigations@mandiant.com</a></li> <li>• Emerald Data Networks – see: Phone: 678.302.3000, Email: <a href="mailto:drodgers@emeralddata.net">drodgers@emeralddata.net</a> (Georgia)</li> <li>• Integrity Technology Systems, Inc. – Phone: 515.528.0023, Email: <a href="mailto:Leslie.Matheson@IntegritySRC.com">Leslie.Matheson@IntegritySRC.com</a> (Iowa)</li> </ul> <p><u>Options for Two-Factor Authentication Solutions:</u></p> <ul style="list-style-type: none"> <li>• RSA SecureID – see: <a href="http://www.emc.com">www.emc.com</a></li> </ul> <p><u>Options for Remotely Served Session Solutions:</u></p> <ul style="list-style-type: none"> <li>• Citrix – see: <a href="http://www.citrix.com">www.citrix.com</a></li> </ul> <p><u>Options for Privileged Account Management:</u></p> <ul style="list-style-type: none"> <li>• Cyber-Ark – see: <a href="http://www.cyber-ark.com">www.cyber-ark.com</a></li> </ul> <p><u>Options for Data Loss/Leak Prevention (DLP) Solutions:</u></p> <ul style="list-style-type: none"> <li>• Cisco IronPort – see: <a href="http://www.ironport.com">www.ironport.com</a></li> </ul> <p><u>Options for Vulnerability Scanning:</u></p> <ul style="list-style-type: none"> <li>• Qualys – see: <a href="http://www.qualys.com">www.qualys.com</a></li> <li>• Nessus – see: <a href="http://www.nessus.org">www.nessus.org</a></li> </ul> <p><u>Options for Social Media Legal Guidance:</u></p> <ul style="list-style-type: none"> <li>• Baker Hostetler – see: <a href="http://www.bakerlaw.com">www.bakerlaw.com</a></li> </ul>	



## 6. Application/Systems Development and Maintenance

### Topics Covered

- Do you develop original application code for internal or public-facing settings? If so, who is responsible for ensuring that effective security architecture, coding, and testing tasks are followed?
- Developer knowledge of secure coding techniques (OWASP) and formal/ongoing developer training?
- Application-based vulnerability testing to identify/eliminate application-level weaknesses (e.g., through packages such as IBM’s AppScan, HP’s WebInspect, Qualys’ WAS, or Rapid7’s Metasploit Pro?)

### Findings

	Appears to have superior <b>BEST IN CLASS</b> practices	<p>Findings for <b>ALL</b> clients 01/2015-06/2016:</p> <p>2015-16 Client Population % by Sector:                  22% Financial, Insurance &amp; Legal                  19% Healthcare                  17% Retail                  11% Technology, Consulting &amp; Media                  11% Manufacturing                  6% Energy                  3% Public Sector &amp; Non-Profit                  11% All Others</p>
	Appears to have <b>STRONG</b> practices	
<b>X</b>	Appears to have minimum <b>BASELINE</b> practices	
	Appears to have one or more key <b>WEAKNESSES</b> noted	
Notes	Management advised that Red Feather does not engage in any type of original application development, and further noted that their public Web site is managed through the Colorado State Library (as a WordPress-authored site). <b><i>We suggested that management query the Colorado State Library as to their reliance upon the application security best practices identified in this section.</i></b>	
We recommend you utilize the following resources available in the eRisk Hub. Don't have access to the <a href="#">eRisk Hub</a> ? Come see what you are missing – ask your broker/underwriter for your free membership access as part of your cyber insurance policy coverage. Or please email <a href="mailto:Management@NetDiligence.com">Management@NetDiligence.com</a> . <b>Risk Manager Tools (Free):</b> <ul style="list-style-type: none"> <li>• <a href="#">Privacy Policy Template For Mobile Applications</a></li> </ul> <b>Articles &amp; Whitepapers (Free):</b> <ul style="list-style-type: none"> <li>• <a href="#">The Hidden Privacy and Security Risks of Apps</a></li> </ul>		
Several vendors provide remediation and/or outsourced services for suggestions or recommendations identified in the “Notes” for this Section.		

We list some of these below *without specific endorsement from NetDiligence* (although some may be listed in the eRisk Hub).

Options for Secure Coding Awareness/Training:

- The Open Web Application Security Project (OWASP) – see: [www.owasp.org](http://www.owasp.org)

Options for Application Security Scanning Tools:

- IBM AppScan – see: [www.ibm.com](http://www.ibm.com)
- HP WebInspect – see: [www.hp.com](http://www.hp.com)

Options for Application Security Penetration Testing:

- iViz – see: [www.ivizsecurity.com](http://www.ivizsecurity.com), Phone: 617.391.0176, Email: [varun.sharma@ivizsecurity.com](mailto:varun.sharma@ivizsecurity.com)
- Trustwave – see: [www.trustwave.com](http://www.trustwave.com), Phone: 312.873.7474, Email: [CPogue@trustwave.com](mailto:CPogue@trustwave.com)
- Mandiant Corporation – see: [www.mandiant.com](http://www.mandiant.com), Phone: 703.683.3141, Email: [investigations@mandiant.com](mailto:investigations@mandiant.com)

Options for Mobile Application Testing:

- ICSA Labs – see: [www.icsalabs.com](http://www.icsalabs.com), Phone: 717.790.8143, Email: [Management@NetDiligence.com](mailto:Management@NetDiligence.com)

## 7. System & Network Operations

### Topics Covered

- Identify deployed firewall solutions and other perimeter security components?
- Identify deployed anti-virus and other malware prevention solutions?
- Identify automated server/desktop patch management tools?
- Identify overall change management process and deployed tracking solution?
- Identify mobile device management (MDM) solutions currently in use (e.g., AirWatch, BlackBerry BES, Good Technology, MS ActiveSync, MobileIron)?
- Does your organization permit “Bring Your Own Device” (BYOD) use by your employees? If so, please discuss the nature of the additional protections you have implemented to guard against the added risks inherent in allowing the on premise/on-network utilization of personal PC/laptop/tablet/smartphone devices.

### Findings

<p><b>X</b></p>	<p>Appears to have superior <b>BEST IN CLASS</b> practices</p>	<p>Findings for <b>ALL</b> clients 01/2015-06/2016:</p> <p>2015-16 Client Population % by Sector:                  22% Financial, Insurance &amp; Legal                  19% Healthcare                  17% Retail                  11% Technology, Consulting &amp; Media                  11% Manufacturing                  6% Energy                  3% Public Sector &amp; Non-Profit                  11% All Others</p>
	<p>Appears to have <b>STRONG</b> practices</p>	
	<p>Appears to have minimum <b>BASELINE</b> practices</p>	
	<p>Appears to have one or more key <b>WEAKNESSES</b> noted</p>	
<p>Notes</p>	<p>Red Feather currently relies upon a Cisco Meraki MX60 firewall, and upon a combination of several deployed solutions for AV and malware preventions – including Avast, Malwarebytes, and RansomFree. For system patching, Red Feather applies a two-pronged approach: (a) for employee workstations – patching/updating is a manual process, undertaken carefully at periodic intervals, and (b) for public PCs, these are auto-wiped and reimaged upon each re-boot using DeepFreeze. Change management, within the context of Red Feather’s modest-sized IT footprint, is properly recorded in a change log that is kept in an Excel spreadsheet (which also incorporates Red Feather’s information asset inventory). For mobile device management (MDM), Red Feather maintains a small population of tablets that are designated for public e-reader use – along with one specialized device helps process ACH transactions; this latter device is restricted for use on Red Feather’s secure VLAN segment.</p>	

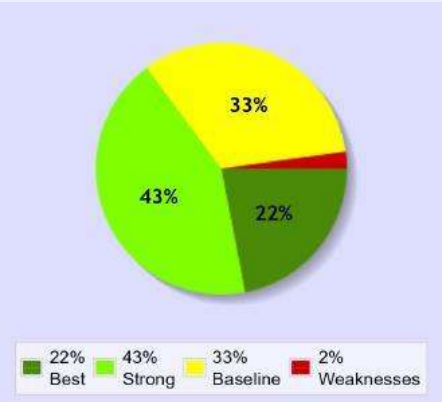
	<p><b><i>Keeping in mind the scope and IT footprint of the Red Feather environment, we believe that management’s use of capable solutions for each of the topics included in this Section justifies a “Best in Class” opinion at this time.</i></b></p>
<p>We recommend you utilize the following resources available in the eRisk Hub. Don’t have access to the <a href="#">eRisk Hub</a>? Come see what you are missing – ask your broker/underwriter for your free membership access as part of your cyber insurance policy coverage. Or please email <a href="mailto:Management@NetDiligence.com">Management@NetDiligence.com</a>.</p> <p><u>Risk Manager Tools (Free):</u></p> <ul style="list-style-type: none"> <li>• <a href="#">Personal Device Use (BYOD) Policy</a></li> </ul>	
<p>Several vendors provide remediation and/or outsourced services for suggestions or recommendations identified in the “Notes” for this Section. We list some of these below <b><i>without specific endorsement from NetDiligence</i></b> (although some may be listed in the eRisk Hub).</p> <p><u>Options for Firewall Solutions:</u></p> <ul style="list-style-type: none"> <li>• Cisco – see: <a href="http://www.cisco.com">www.cisco.com</a></li> <li>• Juniper Networks – see: <a href="http://www.juniper.net">www.juniper.net</a></li> </ul> <p><u>Options for Antivirus (AV) And Malware Prevention:</u></p> <ul style="list-style-type: none"> <li>• Trend Micro, Inc. – Phone: 202.415.3955, Email: <a href="mailto:tom_kellermann@trendmicro.com">tom_kellermann@trendmicro.com</a></li> <li>• Symantec – see: <a href="http://www.symantec.com">www.symantec.com</a></li> <li>• McAfee – see: <a href="http://www.mcafee.com">www.mcafee.com</a></li> <li>• Kaspersky Lab – see: <a href="http://www.kaspersky.com">www.kaspersky.com</a></li> </ul> <p><u>Options for Patch Management:</u></p> <ul style="list-style-type: none"> <li>• Microsoft WSUS/SCCM – see: <a href="http://www.microsoft.com">www.microsoft.com</a></li> <li>• Altiris (Symantec) – see: <a href="http://www.altiris.com">www.altiris.com</a></li> </ul> <p><u>Options for Change Management:</u></p> <ul style="list-style-type: none"> <li>• BMC Remedy – see: <a href="http://www.remedy.com">www.remedy.com</a></li> </ul> <p><u>Options for Systems Remediation &amp; Managed Services:</u></p> <ul style="list-style-type: none"> <li>• Integrity Technology Systems, Inc. – see: <a href="http://www.integritysrc.com">www.integritysrc.com</a>, Phone: 515.528.0023, Email: <a href="mailto:Leslie.Matheson@IntegritySRC.com">Leslie.Matheson@IntegritySRC.com</a></li> <li>• Emerald Data Networks – see: <a href="http://www.emeralddata.net">www.emeralddata.net</a>, Phone: 678.302.3000, Email: <a href="mailto:drodgers@emeralddata.net">drodgers@emeralddata.net</a></li> </ul>	

## 8. Business Continuity and Disaster Recovery

### Topics Covered

- Who owns organization-wide responsibility for DR/BCP program oversight/execution?
- Are DR plans based upon regularly updated business impact analysis (BIA) exercises?
- Existing DR plans and testing schedules? Recent DR test results?
- Reliance on vendors (e.g., SunGard, IBM) vs. internal resources/facilities for DR tasks/functions?
- Identify the organization’s production/DR data center locations? Planned enhancements going forward?
- Presence of sufficient UPS and longer-term generator capacity and regular testing of same?
- Do you maintain awareness of key vendor DR capabilities and/or test events?

### Findings

	Appears to have superior <b>BEST IN CLASS</b> practices	<p>Findings for <b>ALL</b> clients 01/2015-06/2016:</p>  <p>2015-16 Client Population % by Sector:</p> <ul style="list-style-type: none"> <li>22% Financial, Insurance &amp; Legal</li> <li>19% Healthcare</li> <li>17% Retail</li> <li>11% Technology, Consulting &amp; Media</li> <li>11% Manufacturing</li> <li>6% Energy</li> <li>3% Public Sector &amp; Non-Profit</li> <li>11% All Others</li> </ul>
<b>X</b>	Appears to have <b>STRONG</b> practices	
	Appears to have minimum <b>BASELINE</b> practices	
	Appears to have one or more key <b>WEAKNESSES</b> noted	
Notes	<p>Given that some of Red Feather’s key applications are hosted by reputable third-party vendors, management’s responsibility with regard to these platforms includes keeping abreast of vendor DR and resiliency capabilities as part of Red Feather’s overall vendor security management program (please see our general discussion on this topic in Section 2 above). Regarding local IT systems, management follows a backup regimen that includes multiple levels of data replication with copies stored at the Library, at the Director’s home, on Google storage, and at a community bank (vault storage). As noted in Section 4, off-site copies of data are encrypted prior to transport using VeraCrypt. Recovery testing does not take place on a regular basis (<b>and we would suggest periodic test restores going forward</b>). Management additionally noted that backups are primarily of data only, and that application recovery would typically be accomplished through licensed DVD copies and/or other master code sources. Management advised that the Library currently relies upon individual UPS units for local-hosted IT servers – but also noted that they are currently looking into the prospect of</p>	

	<p>adding a longer-term generator. <b><i>Contingent upon commencement of some type of periodic test restore procedure being developed and implemented, we believe a Strong opinion is justified for this section.</i></b></p>
<p>We recommend you utilize the following resources available in the eRisk Hub. Don't have access to the <a href="#">eRisk Hub</a>? Come see what you are missing – ask your broker/underwriter for your free membership access as part of your cyber insurance policy coverage. Or please email <a href="mailto:Management@NetDiligence.com">Management@NetDiligence.com</a>.</p> <p><u>Risk Manager Tools (Free):</u></p> <ul style="list-style-type: none"> <li>• <a href="#">Business Interruption Cost Calculator</a></li> </ul> <p><u>Articles &amp; Whitepapers (Free):</u></p> <ul style="list-style-type: none"> <li>• <a href="#">Preventing eBusiness Interruption</a></li> <li>• <a href="#">21st Century Incident Response - Incident Response Process Automation</a></li> <li>• <a href="#">The Intersection of Business Continuity and Data Breach Preparedness</a></li> <li>• <a href="#">Business Continuity in Healthcare – External Service Providers, Personal Health Records, and ePrescriptions</a></li> <li>• <a href="#">Business Continuity in Healthcare – Healthcare Reform</a></li> <li>• <a href="#">Business Continuity in Healthcare–Electronic Medical Records</a></li> </ul> <p>Several vendors provide remediation and/or outsourced services for suggestions or recommendations identified in the “Notes” for this Section. We list some of these below <b><i>without specific endorsement from NetDiligence</i></b> (although some may be listed in the eRisk Hub).</p> <p><u>Options for Disaster Recovery Consulting And Service Providers:</u></p> <ul style="list-style-type: none"> <li>• SunGard – see: <a href="http://www.sungard.com">www.sungard.com</a></li> <li>• IBM Business Recovery Services – see: <a href="http://www.ibm.com">www.ibm.com</a></li> <li>• Avalution – see: <a href="http://www.avalution.com">www.avalution.com</a> Phone: 866.533.0575, Email: <a href="mailto:contactus@avalution.com">contactus@avalution.com</a></li> <li>• Concept Analysis and Integration – see: <a href="http://caaii.com">caaii.com</a> Phone: 301.997.2177 x7011, Email: <a href="mailto:dholloway@caaii.com">dholloway@caaii.com</a></li> <li>• Integrated Systems Consultants – see: <a href="http://www.i-s-c.com">www.i-s-c.com</a>, Phone: 231.492.0472, Email: <a href="mailto:tfairchild@i-s-c.com">tfairchild@i-s-c.com</a></li> <li>• Loricca, Inc. – see: <a href="http://loricca.com">loricca.com</a> Phone: 813.600.3005 x102, Email: <a href="mailto:mwhitcomb@loricca.com">mwhitcomb@loricca.com</a></li> </ul> <p><u>Options for Datacenter Power Solutions:</u></p> <ul style="list-style-type: none"> <li>• APC – see: <a href="http://www.apc.com">www.apc.com</a></li> </ul>	

## 9. Incident Response Procedures & Functions

### Topics Covered

- Please describe your organization-wide computer incident response team (CIRT) program?
- How are employees directed to report suspected information security incidents? How escalated?
- Who within the CIRT function is responsible for external research on evolving threats/capabilities?
- Do you conduct any type of periodic “table-top” incident response exercises (touching upon different types of scenarios) to ensure that IRP plans are well understood and followed?
- Do you rely upon any vendor managed security services provider (MSSP) relationships?
- Identify deployed IDS/IPS solutions to provide monitoring/alert functions for suspicious activities?
- Identify deployed centralized Security Information and Event Management (SIEM) solution?
- Depth of existing data forensics expertise in-house and/or on stand-by with established vendor(s)?
- Identify significant security incidents during the past year that either consumed significant security team time to address/resolve or involved a negative business/customer impact? How resolved?

### Findings

	Appears to have superior <b>BEST IN CLASS</b> practices	<p>Findings for <b>ALL</b> clients 01/2015-06/2016:</p> <p>2015-16 Client Population % by Sector:</p> <ul style="list-style-type: none"> <li>22% Financial, Insurance &amp; Legal</li> <li>19% Healthcare</li> <li>17% Retail</li> <li>11% Technology, Consulting &amp; Media</li> <li>11% Manufacturing</li> <li>6% Energy</li> <li>3% Public Sector &amp; Non-Profit</li> <li>11% All Others</li> </ul>
<b>X</b>	Appears to have <b>STRONG</b> practices	
	Appears to have minimum <b>BASELINE</b> practices	
	Appears to have one or more key <b>WEAKNESSES</b> noted	
Notes	<p>Management’s approach to incident response, given the modest size of the Red Feather staff, is very direct: employees are directed to report any actual or suspected incidents to the Director immediately upon discovery. The Director, in turn, will attempt to resolve the incident within his level of technical capabilities – or, alternatively, reach out to their network consultant (Carson Block), the Colorado State Library, or to McGriff/CSD as appropriate. In addition to keeping abreast with McGriff/CSD’s available resource assistance in this area, we also suggested (and sent registration instructions) that management take advantage of the McGriff/CSD version of our eRiskHub® cyber risk management portal. As for recent incidents, management noted that Red Feather itself has not experienced any</p>	

	<p>such events within the past year – but also advised that members of the community periodically visit and ask for assistance with personal virus infections on their PCs and devices. Within reason, Red Feather provides one-on-one assistance here – but also has a keen sense for when they should recommend that individuals seek more advanced technical assistance from a local computer repair shop.</p>
<p>We recommend you utilize the following resources available in the eRisk Hub. Don't have access to the <a href="#">eRisk Hub</a>? Come see what you are missing – ask your broker/underwriter for your free membership access as part of your cyber insurance policy coverage. Or please email <a href="mailto:Management@NetDiligence.com">Management@NetDiligence.com</a>.</p> <p><u>Risk Manager Tools (Free):</u></p> <ul style="list-style-type: none"> <li>• <a href="#">State Security Breach Laws Response Guide</a> (50-state map of breach duties)</li> <li>• <a href="#">Data Breach Cost Calculator</a></li> <li>• <a href="#">Notification Cost Calculator</a></li> <li>• <a href="#">A Guide to Data Breach Incident Response Planning</a></li> <li>• <a href="#">Data Breach Incident Response Workbook</a></li> <li>• <a href="#">Data Breach Response Guide</a></li> <li>• <a href="#">Incident Response Plan</a></li> </ul> <p><u>Articles &amp; Whitepapers (Free):</u></p> <ul style="list-style-type: none"> <li>• <a href="#">Crisis Data Breach Response: Notification</a></li> <li>• <a href="#">Crisis Data Breach Response: Credit Monitoring and ID Restoration</a></li> <li>• <a href="#">Crisis Data Breach Response: Computer Forensic Services</a></li> <li>• <a href="#">Crisis Data Breach Response: Legal Counsel</a></li> </ul>	
<p>Several vendors provide remediation and/or outsourced services for suggestions or recommendations identified in the “Notes” for this Section. We list some of these below <b>without specific endorsement from NetDiligence</b> (although some may be listed in the eRisk Hub).</p> <p><u>Options for Incident Response Planning Assistance:</u></p> <ul style="list-style-type: none"> <li>• Immersion, Ltd. – see: <a href="http://www.immersionltd.com">www.immersionltd.com</a>, Phone: 814.272.0574 x3304, Email: <a href="mailto:shawn.melito@immersionltd.com">shawn.melito@immersionltd.com</a></li> </ul> <p><u>Options for Intrusion Detection/Prevention Systems (IDS/IPS):</u></p> <ul style="list-style-type: none"> <li>• Snort – see: <a href="http://www.snort.org">www.snort.org</a></li> <li>• TippingPoint (HP) – <a href="http://www.tippingpoint.com">www.tippingpoint.com</a></li> </ul> <p><u>Options for Security Information And Event Management (SIEM) Solutions:</u></p> <ul style="list-style-type: none"> <li>• ArcSight – see: <a href="http://www.arcsight.com">www.arcsight.com</a></li> <li>• RSA enVision (EMC) – see: <a href="http://www.emc.com">www.emc.com</a></li> </ul> <p><u>Options for Incident Response And Data Forensics Services:</u></p> <ul style="list-style-type: none"> <li>• Navigant – see: <a href="http://www.navigant.com">http://www.navigant.com</a> Phone: 215.832.4485, Email: <a href="mailto:dbielby@navigant.com">dbielby@navigant.com</a></li> <li>• Verizon Business – see: <a href="http://www.verizonbusiness.com/products/security/risk/forensics">www.verizonbusiness.com/products/security/risk/forensics</a> Phone: 914.574.2805, Email: <a href="mailto:chris.novak@verizonbusiness.com">chris.novak@verizonbusiness.com</a></li> <li>• Kroll Cyber Security – see: <a href="http://www.krollcybersecurity.com">www.krollcybersecurity.com</a>, Email: <a href="mailto:blapidus@kroll.com">blapidus@kroll.com</a></li> <li>• Kivu Consulting – see: <a href="http://kivuconsulting.com">kivuconsulting.com</a>, Email: <a href="mailto:wkrone@kivuconsulting.com">wkrone@kivuconsulting.com</a>, <a href="mailto:mbell@kivuconsulting.com">mbell@kivuconsulting.com</a></li> </ul>	

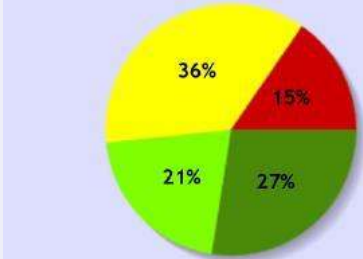


## 10. Privacy

### Topics Covered

- Who serves as your chief privacy officer (CPO), either in title and/or operational function?
- Do you have pre-approved procedures and templates for use in responding to a **data privacy breach**?
- External vendor(s) lined up to assist with volume-based privacy breach remediation activities?
- **If you author/provide consumer mobile applications (e.g., “app store” offerings)** – Have you ensured that your mobile app(s) fully comply with applicable laws requiring effective privacy policy adherence, such as California’s Online Privacy Protection Act?
- Identify notable (i.e., volume-based) privacy breach notifications required during the past year? How were these carried out and what changes to existing practices/solutions (if any) as a result?

### Findings

	Appears to have superior <b>BEST IN CLASS</b> practices	<p>Findings for <b>ALL</b> clients 01/2015-06/2016:</p>  <p>2015-16 Client Population % by Sector:</p> <ul style="list-style-type: none"> <li>22% Financial, Insurance &amp; Legal</li> <li>19% Healthcare</li> <li>17% Retail</li> <li>11% Technology, Consulting &amp; Media</li> <li>11% Manufacturing</li> <li>6% Energy</li> <li>3% Public Sector &amp; Non-Profit</li> <li>11% All Others</li> </ul>
<b>X</b>	Appears to have <b>STRONG</b> practices	
	Appears to have minimum <b>BASELINE</b> practices	
	Appears to have one or more key <b>WEAKNESSES</b> noted	
Notes	Beyond the sensitive information that Red Feather maintains on its team of employees and volunteers (protection of which is governed by policies enacted by the Board of Trustees, and paper copies of same kept in a locked drawer), management also noted that the personal data collected on clients (i.e. for issuance of Library membership cards) is fairly modest – and typically only includes name, gender, mailing/physical address, and e-mail address. Client information in this latter case is stored not at the Library, but within the LibLime application hosted by the Colorado State Library (and therefore, subject to the data privacy protections exerted at that level). In responding to a suspected data privacy breach event, management noted that they would likely refer the matter to their legal counsel – who in turn would contact McGriff/CSD for further assistance. While it appears that Red Feather has a good handle on their privacy remediation tasks, we might also suggest that they consider adoption of our Breach Plan Connect® incident response plan offering (see: <a href="http://www.breachplanconnect.com">www.breachplanconnect.com</a> ).	

	<p>Management advised that Red Feather has not experienced any data privacy breach events within recent memory.</p>
<p>We recommend you utilize the following resources available in the eRisk Hub. Don't have access to the <a href="#">eRisk Hub</a>? Come see what you are missing – ask your broker/underwriter for your free membership access as part of your cyber insurance policy coverage. Or please email <a href="mailto:Management@NetDiligence.com">Management@NetDiligence.com</a>.</p> <p><u>Risk Manager Tools (Free):</u></p> <ul style="list-style-type: none"> <li>• <a href="#">Publicized Breach Events</a></li> <li>• <a href="#">Privacy Case Law</a></li> <li>• <a href="#">Web Site Privacy Policy</a> (Sample Policy)</li> <li>• <a href="#">Privacy Policy Template For Mobile Applications</a></li> <li>• <a href="#">Security and Privacy Controls for Federal Information Systems and Organizations</a></li> </ul> <p><u>Articles &amp; Whitepapers (Free):</u></p> <ul style="list-style-type: none"> <li>• <a href="#">The New Year May Mean You Need a New Privacy Policy: Recent Changes in Laws Require Attention</a></li> <li>• <a href="#">California Passes Three Privacy and Data Security Laws that Affect Many Companies</a></li> <li>• <a href="#">The Hidden Privacy and Security Risks of Apps</a></li> <li>• <a href="#">Understanding the Final HIPAA Security and Privacy Rules</a></li> <li>• <a href="#">Protecting Personal Information – A Guide For Business (FTC)</a></li> </ul>	
<p>Several vendors provide remediation and/or outsourced services for suggestions or recommendations identified in the “Notes” for this Section. We list some of these below <b>without specific endorsement from NetDiligence</b> (although some may be listed in the eRisk Hub).</p> <p><u>Options for Privacy Consulting &amp; Breach Investigation Services:</u></p> <ul style="list-style-type: none"> <li>• Nelson Levine de Luca &amp; Hamilton – see: <a href="http://www.nldhlaw.com">www.nldhlaw.com</a> Phone: 215.358.5154, Email: <a href="mailto:jmullen@nldhlaw.com">jmullen@nldhlaw.com</a></li> <li>• Baker Hostetler – see: <a href="http://www.bakerlaw.com">www.bakerlaw.com</a> Phone: 513.929.3491, Email: <a href="mailto:cahoffman@bakerlaw.com">cahoffman@bakerlaw.com</a></li> <li>• Faruki Ireland &amp; Cox – see: <a href="http://www.ficlaw.com/">http://www.ficlaw.com/</a>, Phone: 937.227.3733, Email: <a href="mailto:rraether@ficlaw.com">rraether@ficlaw.com</a></li> <li>• McDonald Hopkins – see: <a href="http://www.mcdonaldhopkins.com">www.mcdonaldhopkins.com</a>, Phone: 248.220.1354, Email: <a href="mailto:jgiszczak@mcdonaldhopkins.com">jgiszczak@mcdonaldhopkins.com</a></li> <li>• Edwards Wildman Palmer – see: <a href="http://www.edwardswildman.com">www.edwardswildman.com</a> Phone: 617.239.0585 Email: <a href="mailto:mschreiber@edwardswildman.com">mschreiber@edwardswildman.com</a></li> </ul> <p><u>Options for Privacy Breach Notification &amp; Credit Monitoring Services:</u></p> <ul style="list-style-type: none"> <li>• Immersion, Ltd. – see: <a href="http://www.immersionltd.com">http://www.immersionltd.com</a> Email: <a href="mailto:elito@immersionltd.com">elito@immersionltd.com</a></li> <li>• Experian – see: <a href="http://www.experian.com">http://www.experian.com</a> Email: <a href="mailto:ozzie.fonseca@experian.com">ozzie.fonseca@experian.com</a></li> </ul>	

Explanation of Supplemental Scores



In the course of our assessment, if we identify one or more cloud-based vendors currently being utilized that have been assessed independently by CloudeAssurance we include that information in our report. For each instance, we provide the most recently reported scores, as reflected by application of CloudeAssurance’s proprietary evaluation methodology against either (a) publicly published, self-reported vendor practices (“Provisional”), or (b) independent cloud security assessor determination of practices (“Validated”).

The scores reported by CloudeAssurance conform to the following scale:

Rating System Score	Maturity Level	Scoring Scale	Color Code
> 850	5	Optimized Score	
751 – 850	4 - 5	Excellent Score	
601 – 750	3 - 4	Great Score	
401 – 600	2 - 3	Fair Score	
201 – 400	1 - 2	Poor Score	
0 – 200	0 - 1	Very Poor Score	

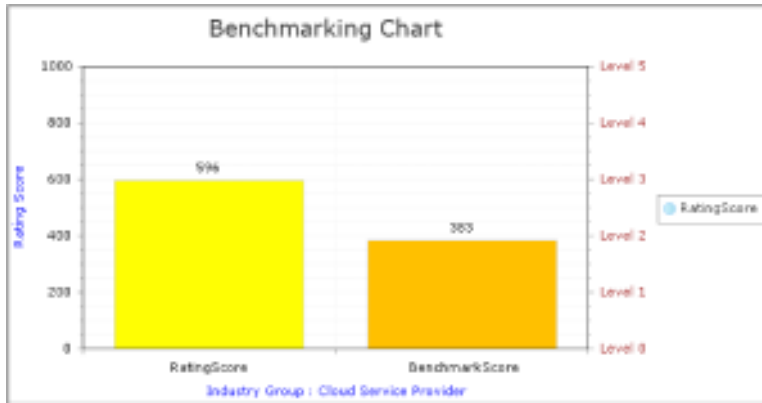
From CloudeAssurance relating to their determination of “Provisional” vs. “Validated” cloud-based ratings:

*CloudeAssurance provisional scores delivered through the SaaS platform and the AlertApp! Mobile Application are derived from licensed content owned by NetDiligence alliance partner CloudeAssurance, Inc. which service scores various cloud service providers based on self-assessment data publicly disclosed by each cloud service provider on web sites such as the Cloud Security Alliance (CSA) STAR registry and their publicly disclosed security certification such as ISO 27001.*

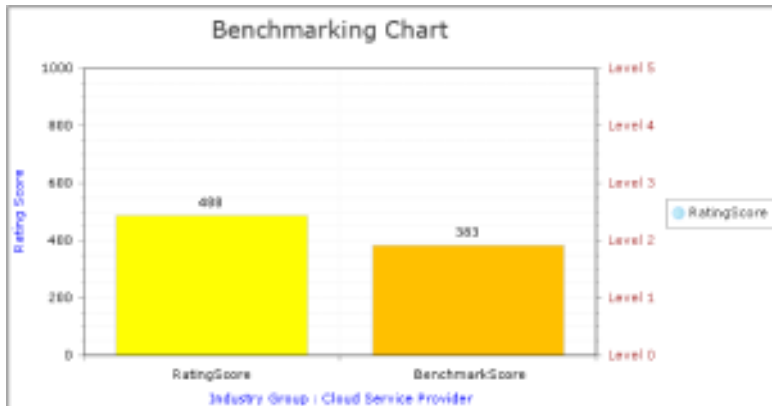
*The purpose of this **Provisional** score is to reveal the self-assessed level of reasonable and prudent safeguard controls in place within a cloud service provider’s operations in relation to CSA industry security standards. This score has not been **Validated** by an independent cloud security assessor approved by the HISP Institute through their Cloud Assurance Assessor Program (CAAP), so it is somewhat subjective but included in this report for added detail and customer education and awareness.*

On the next page, we reproduce the summary details associated with the most recently reported CloudeAssurance scores and comparison data for cloud-based vendors currently being utilized.

**Microsoft Office 365: 596 – Fair Score (Q4, 2016) \*\*TOP 10\*\***



**Amazon Web Services: 488 – Fair Score (Q4, 2016)**



## About NetDiligence®

NetDiligence® is a cyber risk assessment company that offers due-diligence services to help organizations determine how well their network security and privacy practices measure up against known industry standards, as well as regulatory and insurance carrier requirements.

Using proprietary methodologies and tools anchored in proven risk management principals, NetDiligence provides a full range of enterprise-level information security, e-risk insurability and regulatory compliance assessment and testing services. NetDiligence supports and is endorsed by some of the world's largest network liability insurance underwriters.



For more information about how NetDiligence can help your organization assess and protect its network against cyber losses, contact us at [Management@NetDiligence.com](mailto:Management@NetDiligence.com) or visit us at [www.NetDiligence.com](http://www.NetDiligence.com).

## About eRiskHub®

The eRiskHub, powered by NetDiligence, is a licensed service that positions insurers and brokers to effectively assist clients with loss control. The eRiskHub cyber risk management web portal provides general information about sound security practices *before* a breach occurs, and facilitates appropriate reporting and recovery efforts *after* a breach. It provides tools and resources to help clients understand their exposures, establish response plans and minimize the effects of a breach on their organizations.

***Ask your agent if you qualify for eRiskHub membership as an adjunct of your policy.***

For more information about the eRiskHub, contact us at [Management@NetDiligence.com](mailto:Management@NetDiligence.com) or visit us at [www.eRiskHub.com](http://www.eRiskHub.com).

## About Breach Plan Connect®

### ***Data breach response planning.***

Having a data breach plan today is paramount for prudent cyber risk management and can help put an organization in good standing with many cyber risk insurers and state/federal regulators who are increasingly asking about *data breach* response plans. **Breach Plan Connect™** (BPC) is a NetDiligence cloud-based solution which creates a customized **data breach crisis response plan** for your organization. Moreover, BPC is securely hosted to provide you with easy, fast and secure access to your data breach crisis plan whenever needed 24 x 7. And you can also print your plan for your regulator if needed. Finally, BPC includes access to leading Breach Coach® lawyers for a free call, and other experts. Contact us for more information at [Management@NetDiligence.com](mailto:Management@NetDiligence.com)

## About Partner Services

### NPC's Immersion Data Breach Response – Onsite Training & Plan Creation

You hold vital confidential information about your customers and your employees. Should that information be lost or stolen, you are facing costly legal requirements, negative publicity and possible permanent damage to your brand. Have you done everything possible to avoid a devastating data breach? Is your organization fully prepared to respond in the right way if the “worst does happen”? If not, talk to the breach response specialists at NPC's Immersion Data Breach Response. (<http://www.npcweb.com/services/Data-Breach-Response.aspx>). NPC will use its “in the trenches” experience to help you design an incident response plan that fills any gaps which may exist. Example services include:

- Incident Response Plan Development
- Web-based & Onsite IRP Training
- Customer Call Center
- Breach Notification Mailing

Contact NetDiligence 610.525.6383 [Management@NetDiligence.com](mailto:Management@NetDiligence.com) for further information on NPC's Immersion Data Breach Response services.

---

### ICSA Labs – Mobile Application Testing Program

ICSA Labs delivers mobile application testing for companies that have developed custom-made mobile apps in-house or through the use of a third party. During a mobile app testing engagement, ICSA Labs examines a mobile app across more than twenty high-level assessment objectives mapping back to five key categories: maliciousness, vulnerability, authentication, reliability, and privacy.

Contact NetDiligence 610.525.6383 [Management@NetDiligence.com](mailto:Management@NetDiligence.com) for further information on ICSA Labs services.

---

### SecurityScorecard Inc. – External Cyber Risk Profiling Services

SecurityScorecard™ grading service gives you continuous insight into the security posture and key risks of your company and of your business partners, as understood by cybercriminals who are performing reconnaissance on your company's infrastructure. SecurityScorecard™ collects and contextualizes millions of signals across key risk categories into our big-data analysis engine, providing real-time threat intel and actionable intelligence to improve security posture of your company and your partner ecosystem.

Contact NetDiligence 610.525.6383 [Management@NetDiligence.com](mailto:Management@NetDiligence.com) for further information on ICSA Labs services.