Agenda Item 7a
Requested Action: Informational

Poudre River Public Library District

Cyber risk assessment and action items

Overview

The Library District participated in a cyber risk assessment in the fall of 2021 in conjunction with an increase in our cyber liability coverage. The questionnaire was designed to evaluate our current cyber security and data privacy practices and provide recommendations. The NetDiligence Cyber Health Check Assessment was sponsored by the Colorado Special Districts Insurance Pool.

Network infrastructure management is included in our IGA with the City of Fort Collins. The City IT department has committed personal and resources to evaluating and protecting the data network as well as working with 3rd party specialists to address security issues.

Following are key recommendations from the assessment and our plans to address areas of concern.

Implement a formal cyber security awareness training program for employees.
Action Item: The Library District will evaluate and select a training platform to be launched in the first quarter of 2023. In our experience, while staff are aware of email phishing attempts, there is often confusion in positively identifying malicious email and what actions to take. Interactive training, with live email testing, might have the greatest impact.

Develop a vendor security management program.
Action Item: We plan to utilize the NetDiligence resources to develop a vendor security checklist to be used with all existing and new vendors. An audit of our existing agreements will be completed by the end of the second quarter of 2023. The checklist will be used to evaluate new vendors.

Ensure primary system backups are encrypted at-rest in storage.
Action Item: Our Integrated Library System (ILS) backups are already encrypted. On premises file server backups will be converted to encrypted at-rest and the same will be done for employee laptops. This work is in progress and will be complete by December 31, 2022. Additionally, staff will be notified of the availability of email encryption options through Office 365.

Implement a data privacy program in concert with legal representation.
Action Item: The district requires 3rd party vendors to demonstrate they have protections in place to protect Personally Identifiable Information (PII) when data is exported from the ILS. In addition, we are careful to construct exports that disassociated PII whenever possible. We will review and update our privacy program to include customer and employee information.

Consideration of multi-factor authentication for Microsoft 365 accounts
Action Item: Particularly relevant given the transition to storing staff resources on Office 365. We plan to implement MFA by the end of June, 2023.

11/8/22

POUDRE RIVER PUBLIC LIBRARY DISTRICT

QuietAudit®

Health Check Cyber Risk Assessment

2021 Final Report

NetDiligence®

Conference Call Findings for Entity: Poudre River Public Library District

Client Vertical	**Public Entity**
Client Contact	**Mark Huber** **IT Manager** **MHuber@PoudreLibraries.org** **970-221-6662**
Date Prepared	**2/14/2022**
Report Author	**Dave Chatfield**

NetDiligence Summary Findings

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

Client's Posture	Grade Level	Opinion Statement
□	A+	Appears to have full suite of Superior Safeguards & Practices in place. (100% of below listed controls/ practices)
□	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.
□	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.
□	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
□	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.
□	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.
□	B	Functional incident response and privacy/compliance functions. Important emphasis placed upon breach notifications if that is where the evidence leads.
X	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.
□	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	Partial
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	YES
4. IDS capabilities are reasonable	Yes
5. Application level scan testing and programming practices insure against SQL injection and other well-known weaknesses	Partial
6. Proof of effective general vulnerability scanning and remediation efforts	YES
7. Redundancy of mission-critical systems	Partial
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	NO

Significant Findings / Recommendations

1.	Section 1	The District should promptly implement a formal cyber security awareness training program for its employees.
2.	Section 2	The District should develop a vendor security management program.
3.	Section 4	The District should ensure that their primary system backups are encrypted at-rest in storage.
4.	Section 10	The District should implement a data privacy program in concert with legal representation.
5.	Sections 1-10	We have offered a number of lesser suggestions that we believe merits management consideration for implementation in the near-to-medium term.

Additional Comments

Poudre River Public Library District (hereafter, "Poudre River" or "the District"), appears to have fairly modest in-house efforts directed specifically toward cyber security, although it also appears to benefit substantially in this respect from its relationship with the City of Ft. Collins (which provides a variety of technical services assistance, as mentioned throughout several Sections in this report). Management has a very good understanding of the areas in which improvement is still needed over the next year or so, within the context of existing resource constraints and consideration of the various elements that the District entrusts to the City vs. those which the District might wish to bring in-house going forward.

Conclusion

□	Acceptable – Appears to have **SUPERIOR BEST IN CLASS** practices overall
□	Acceptable – Based on information as received
X	Acceptable – With **COMPLIANCE TO RECOMMENATIONS ABOVE**
□	NOT ACCEPTABLE – **SIGNIFICANT UNRESOLVED WEAKNESSES OR UNKNOWNS**

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):

Acronym	***Full Description***
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, www.owasp.org)
PCI	Payment Cardholder Industry (jointly supported by major card brands)
PCI DSS	PCI Data Security Standards (version 3.2 is latest as of 5/1/2020)
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 (www.sans.org)
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:	130
Total number of individual clients or transactions/year:	~165,000 residents; 85,000 transaction users
Total number of production servers being managed:	14
Dominant brands/versions of SQL databases in use:	2
Total number of employee laptops; % encrypted:	10; 0% encrypted
Total number of managed MDM/BYOD devices:	0
Please identify your current cyber insurance carrier:	McGriff CSD
Do you have an active eRiskHub.com® account?	Registration information sent
Do you have an active Breach Plan Connect® account?	BPC brochure sent

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.*

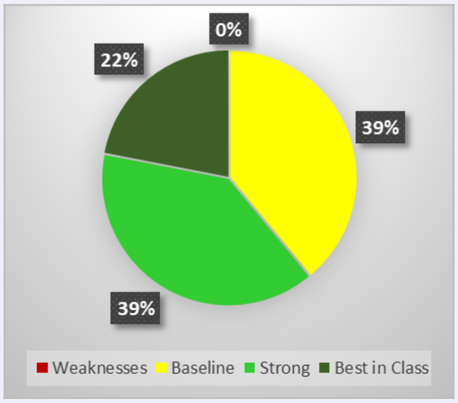
Hosted or Cloud Services Vendor	Public/ Non-Sensitive Info	Personally Identifiable Info (PII)	Protected Health Info (PHI)	Payment Cardholder Info (PCI)	Competitive Business Info
Amazon AWS	Yes				
Microsoft 365	Yes	Yes			
City of Ft. Collins, CO	Yes				
Innovative (LMS)	Yes	Yes			
eFile Cabinet (HR)	Yes	Yes			
Bamboo (HR)	Yes	Yes			

1. Security Organization, Personnel Security

Topics Covered

- Current FTE staffing & roles of dedicated information security team? If no ***dedicated*** security team, who is the named senior manager assigned CISO-level responsibility for information security program efforts within your organization?
- 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, NY DFS) 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 the past 2-3 years)?
- Does security associated with the Internet of Things (IoT) represent a key focus and/or business requirement for your organization? If so, please briefly discuss your efforts in this area.
- Please identify key information security projects and/or solution deployments for the next 12 months?

Findings

	Appears to have superior **BEST IN CLASS** practices	Findings for **ALL** clients 2017-2018:  2017-18 Client Population % by Sector: 10% Financial, Insurance & Legal 10% Healthcare 0% Retail 12% Technology, Consulting & Media 7% Manufacturing 2% Energy 54% Public Sector & Non-Profit 5% All Others
	Appears to have **STRONG** practices	
X	Appears to have minimum **BASELINE** practices	
	Appears to have one or more key **WEAKNESSES** noted	
Notes	Poudre River Public Library District (hereafter, "Poudre River" or "the District") relies upon their IT Manager for primary responsibility in implementing and enforcing the District's information security policies and capabilities. The District also benefits from ***broad-based*** additional assistance (via an Intergovernmental Agreement, or IGA) from the IT Department within the City of Fort Collins (please	

see: https://www.fcgov.com/it/), particularly in the areas of network administration, project management, application testing, and incident response services. Business acquisitions are not a factor for the District, so our question on security integration is not applicable. ***Management does not appear to map its information security practices to known standards (such as ISO 27001, NIST, etc.), and we would suggest adoption of one of these standards in the near-term (and/or seeking from the City awareness of their practices on the District's behalf)***. The District conducts criminal background checks for all new hires. Security awareness training is carried out on an informal basis, with periodic communication on phishing and other email compromise risks for employees. ***Within this area (and given that the District has had some recent experience with compromised email accounts as described in Section 9 below), we recommend implementing a formal security training program within the near-term (resources along these lines may be available through the City, as well as through CSD version of our eRiskHub at no cost to the District). Based upon our experience with other CSD pool members, KnowBe4 represents an online training solution worthy of consideration.*** Internet-of-Things (IoT) does not appear to represent an active area for the District, so our question here is not applicable at this time. Management advised of their current migrations to Microsoft 365 and Amazon AWS as notable current projects with cybersecurity implications, and also noted that some longer-term considerations include whether to rely somewhat less upon the City's services through the buildout/administration of the District's own Library network over the City's underlying fiber. ***We believe that a "Baseline" opinion for this Section is justified at the present time. Based upon our discussion, it appears that the District would likely need to either expand its own in-house hiring/resources for security-centric tasks, or ensure a greater level of agreed-upon services with the City, in order to achieve a "Strong" opinion here within the near-to-medium term.***

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.

Risk Manager Tools (Free):

- Vendor Security Due Diligence Checklist
- Sample eRisk Hub Policies:
  - Information Security Policy Template
  - Physical Security Policy Template
  - Security Awareness Training and Education Policy Template
  - Security Policy 101 – Essential Policies for Business

Articles & Whitepapers (Free):

- Seven Requirements for Successfully Implementing Information Security Policies and Standards

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 Outsourced Security Management, Tasks or Staffing:

- Citadel Information Group – see: www.citadel-information.com, Phone: 323.428.0441, Email: stan@citadel-information.com
- Integrity Technology Systems, Inc. – see: www.integritysrc.com, Phone: 515.528.0023, Email: Leslie.Matheson@IntegritySRC.com
- Emerald Data Networks – see: www.emeralddata.net, Phone: 678.302.3000, Email: drodgers@emeralddata.net
- Loricca, Inc. (HIPPA only) – see: loricca.com, Phone: 813.600.3005 x102, Email: mwhitcomb@loricca.com
- Integrated Systems Consultants (HIPPA only) – see: www.i-s-c.com, Phone: 231.492.0472, Email: tfairchild@i-s-c.com

Options for Employee Security Awareness Training:

- Click 4 Compliance – see: www.click4compliance.com, Phone: 703.787.9492, Email: info@click4compliance.com
- Wombat Security Technologies, Inc. – see: www.wombatsecurity.com, Phone: 412-621-1484 x114, Email: r.massaro@wombatsecurity.com
- Supremus Group LLC (HIPPA only) – see: www.training-hipaa.net, Phone: 515.865.4591, Email: Bob@Training-HIPAA.net

Options for Network Security Software Solutions:

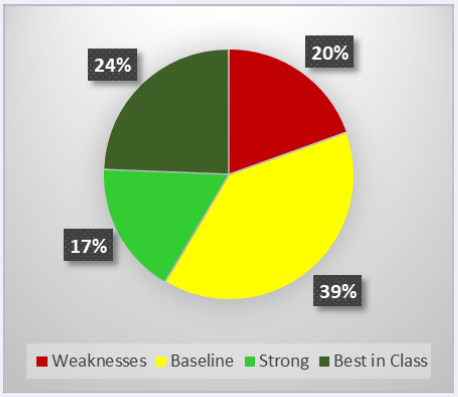
- General Dynamics Fidelis Cybersecurity Solutions – see: Phone: 703.286.5820, Email: barnaby.page@fidelissecurity.com
- Carbon Black – see: www.carbonblack.com, Phone: 610.639.1492, Email: michael.viscuso@getcarbonblack.com
- McAfee – see: www.mcafee.com/us, Phone: 408.346.5295, Email: Visshwanth_Reddy@McAfee.com

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?
- Have you documented – via your information asset inventory or similar mechanism – all instances where you entrust third-party vendors with sensitive PII/PHI or other types of customer/employee information? If so, do you hold these vendors to heightened data protection requirements as part of your contract terms?
- 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 **BEST IN CLASS** practices	Findings for **ALL** clients 2017-2018:  2017-18 Client Population % by Sector: 10% Financial, Insurance & Legal 10% Healthcare 0% Retail 12% Technology, Consulting & Media 7% Manufacturing 2% Energy 54% Public Sector & Non-Profit 5% All Others
	Appears to have **STRONG** practices	
	Appears to have minimum **BASELINE** practices	
X	Appears to have one or more key **WEAKNESSES** noted	
Notes	Based upon our discussion, it does not appear that the District has implemented a vendor security management program to any significant degree, ***and we recommend development of such a program in the near-term***. Management added that there may be some of these elements (particularly with respect to contracts involving indemnifications and/or cyber insurance coverage), but that these details have not been shared with the District to-date ***(and we would suggest seeking awareness of these elements).*** Management also welcomed a copy of our vendor security management questionnaire, for possible use going forward with new vendor selection. The District has not experienced any vendor-caused information security incidents or data privacy breaches during the past year. ***We believe a “Weaknesses” opinion is justified for this Section at the present time – and would further note that***	

	closer coordination with the City on vendor relationships that involve the District would be very helpful in the near-term while the District develops its own in-house capabilities.

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.

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, Phone: 813.600.3005 x102, Email: mwhitcomb@loricca.com

Options for Cloud-based Vendor Security Reviews:

- ISCA Labs – see: www.icsalabs.com Email: Management@NetDiligence.com

Options for Vendor Management Legal/Indemnification Reviews:

- Faruki Ireland & Cox P.L.L. - Ronald I. Raether, Esq. – see: www.ficlaw.com, Phone: 937.227.3733, Email: rraether@ficlaw.com
- InfoLawGroup – see: www.infolawgroup.com, Phone: 303.325.3528, Email: dnavetta@infolawgroup.com

Options for Cloud Encryption Solutions:

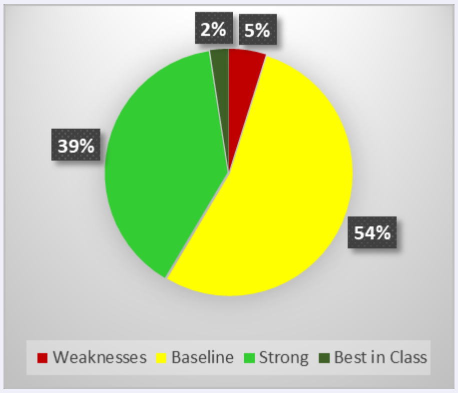
- Townsend Security – see: townsendsecurity.com, Phone: 360.359.4408, Email: luke.probasco@townsendsecurity.com
- Trend Micro, Inc. – see: www.trendmicro.com, Phone: 202.415.3955. Email: tom_kellermann@trendmicro.com
- Lockbox LLC – see: www.goironbox.com, Phone: 206.619.4226, Email: kevinlam@golockbox.com

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?
- 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?

Findings

	Appears to have superior **BEST IN CLASS** practices	Findings for **ALL** clients 2017-2018:  2017-18 Client Population % by Sector: 10% Financial, Insurance & Legal 10% Healthcare 0% Retail 12% Technology, Consulting & Media 7% Manufacturing 2% Energy 54% Public Sector & Non-Profit 5% All Others
	Appears to have **STRONG** practices	
X	Appears to have minimum **BASELINE** practices	
	Appears to have one or more key **WEAKNESSES** noted	
Notes	Management advised that the District has no on-premise card processing capabilities, but noted that customer self-service features exist through PayPal's PayFlow Pro service. While it is highly likely that PayPal maintains a PCI Service Provider fully-compliant status on behalf of its clients, it is also the responsibility of the District (as an accepting PCI Merchant) to complete an annual PCI DSS Self-Assessment Questionnaire ("SAQ") that encompasses the District's oversight of their payment operations. Based upon our conversation, it appears that the District will be able to complete the easiest version, known as SAQ Form "A" (all payment operations outsourced). For further details, please see: https://www.pcisecuritystandards.org/pci_security/completing_self_assessment. The SAQ Form "A" template can be downloaded at: https://www.pcisecuritystandards.org/document_library. ***Contingent upon completing an initial annual PCI DSS SAQ form, we believe a "Baseline" opinion is justified at this time.***	

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.

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

4. Encryption-Related Capabilities

Topics Covered

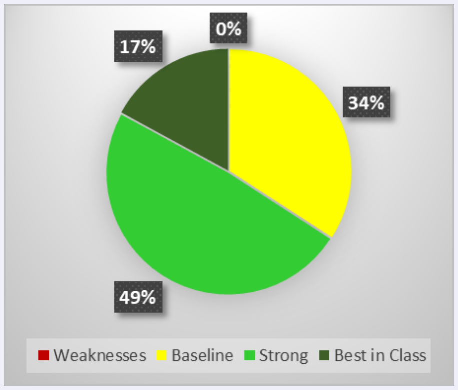
In-transit encryption for: *(Please Identify deployed solutions for each setting)*

- 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, cloud storage, and/or 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 **BEST IN CLASS** practices	Findings for **ALL** clients 2017-2018:  2017-18 Client Population % by Sector: 10% Financial, Insurance & Legal 10% Healthcare 0% Retail 12% Technology, Consulting & Media 7% Manufacturing 2% Energy 54% Public Sector & Non-Profit 5% All Others
	Appears to have **STRONG** practices	
X	Appears to have minimum **BASELINE** practices	
	Appears to have one or more key **WEAKNESSES** noted	
Notes	In-transit capabilities include: Microsoft Windows Server client VPN for encrypted remote connectivity; SFTP for secure file transmission (provided by the City of Ft. Collins) for HR-related purposes; standard Microsoft 365 email transmission (***but apparently not offering voluntary attachment encryption, which we suggest also be considered***); and WPA-level encryption for wireless LAN settings. At-rest capabilities include: Management advised that no at-rest capabilities currently exist. ***We would recommend that at least the District's backup images be encrypted (via external USB drives, as***	

advised, or via cloud-based commercial backup services). We would also suggest that employee laptops for sensitive employees within the District (most notably, for HR and IT) be considered for encryption deployment in the near-to-medium term.

We believe a "Baseline" opinion is justified for this Section at the present time, and further suggest that timely adoption of an encrypted backup solution would move the District closer to a "Strong" level of capabilities.

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.

Risk Manager Tools (Free):

- Small Business Cyber Security Planning Guide
- HIPAA Security Rule: Frequently asked questions regarding encryption of PII
- Acceptable Use Policy (Sample Policy)

Articles & Whitepapers (Free):

- Encryption & Key Management – Best Practices
- Encrypting Email for Data Security

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 Enterprise Encryption Solutions:

- Symantec – see: www.symantec.com
- McAfee – see: www.mcafee.com
- Sophos – see: www.sophos.com

Options for Secure Email Encryption:

- Zix Corporation – see: www.zixcorp.com
- Tumbleweed/Axway – see: www.axway.com

Options for Backup Tape Encryption:

- IBM Tivoli Storage Manager (TSM) – www.ibm.com

Options for Database Encryption:

- Microsoft SQL Server – see: www.microsoft.com
- Oracle – see: www.oracle.com

Options for Laptop Encryption:

- PGP – see: www.pgp.com
- Pointsec – see: www.checkpoint.com
- TrueCrypt – see: www.truecrypt.com

Options for USB Encryption:

- IronKey – see: www.ironkey.com

Options for Cloud Encryption:

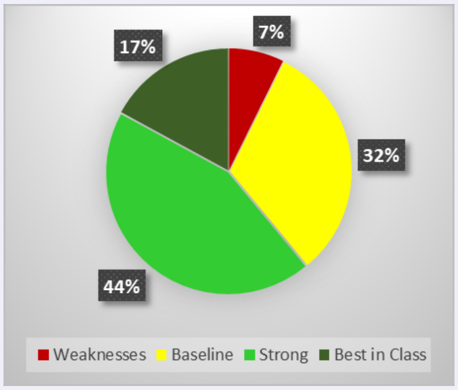
- Townsend Security – see: townsendsecurity.com, Phone: 360.359.4408, Email: luke.probasco@townsendsecurity.com
- Trend Micro, Inc. – see: www.trendmicro.com, Phone: 202.415.3955. Email: tom_kellermann@trendmicro.com
- Lockbox LLC – see: www.goironbox.com, Phone: 206.619.4226, Email: kevinlam@golockbox.com

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?
- Have you implemented strong user account provisioning/termination, role-based access assignments, password management?
- What is your minimum retention rate (in days) for user activity logs for audit/investigation purposes? Are there any notable exceptions?
- 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 **BEST IN CLASS** practices	Findings for **ALL** clients 2017-2018:  2017-18 Client Population % by Sector: 10% Financial, Insurance & Legal 10% Healthcare 0% Retail 12% Technology, Consulting & Media 7% Manufacturing 2% Energy 54% Public Sector & Non-Profit 5% All Others
X	Appears to have **STRONG** practices	
	Appears to have minimum **BASELINE** practices	
	Appears to have one or more key **WEAKNESSES** noted	
Notes	Management advised that the District has implemented some of the above-listed capabilities. Examples include: (a) segregation of traffic via staff/public VLANs that are managed by the City of Ft. Collins, (b) current consideration of multi-factor authentication (MFA) for Microsoft 365 accounts ***(and we strongly suggest near-term deployment in order to reduce ransomware infection risks)***, (c) enforcement of contemporary MS Active Directory group assignments and password	

	composition/change rules, and (d) periodic scanning of the District's environment by the City of Ft. Collins via their BitSight subscription. We did not learn of any regular user account audit tasks, ***and would suggest undertaking such efforts in the near-term (and/or ensuring that the City of Ft. Collins does so on the District's behalf)***. ***Contingent upon near-term deployment of multi-factor authentication (MFA) as indicated above, we believe a "Strong" opinion is justified for this Section at the present time.***

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.

Risk Manager Tools (Free):

- Expanded eRisk Self-Assessment
- Quick eRisk Assessment

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 IT Management Services/Consulting:

- LWG Consulting, Inc. – see: Phone: 847-559-3000 x7076, E-Mail: tchrist@lwgconsulting.com
- Mandiant Corporation – see: Phone: 703-683-3141, E-Mail: investigations@mandiant.com
- Emerald Data Networks – see: Phone: 678.302.3000, Email: drodgers@emeralddata.net (Georgia)
- Integrity Technology Systems, Inc. – Phone: 515.528.0023, Email: Leslie.Matheson@IntegritySRC.com (Iowa)

Options for Two-Factor Authentication Solutions:

- RSA SecureID – see: www.emc.com

Options for Remotely Served Session Solutions:

- Citrix – see: www.citrix.com

Options for Privileged Account Management:

- Cyber-Ark – see: www.cyber-ark.com

Options for Data Loss/Leak Prevention (DLP) Solutions:

- Cisco IronPort – see: www.ironport.com

Options for Vulnerability Scanning:

- Qualys – see: www.qualys.com
- Nessus – see: www.nessus.org

Options for Social Media Legal Guidance:

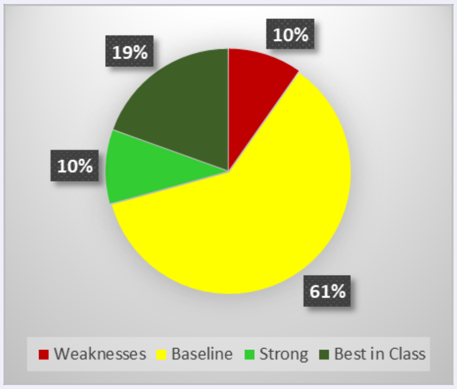
- Baker Hostetler – see: www.bakerlaw.com

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 (and/or third-party vendor) 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 **BEST IN CLASS** practices	Findings for **ALL** clients 2017-2018:  2017-18 Client Population % by Sector: 10% Financial, Insurance & Legal 10% Healthcare 0% Retail 12% Technology, Consulting & Media 7% Manufacturing 2% Energy 54% Public Sector & Non-Profit 5% All Others
X	Appears to have **STRONG** practices	
	Appears to have minimum **BASELINE** practices	
	Appears to have one or more key **WEAKNESSES** noted	
Notes	Management advised that the District engages in some original application development. Notably, this involves Cold Fusion development for the read.poudrelibraries.org website. The District's web application developer is reportedly well aware of security-centric considerations as part of her role (and that some amount of client name/address information is included in the database associated with this application. ***We would suggest that the developer – if she hasn't already done so – take Cold Fusion security training modules as part of her ongoing development plan.*** ***Contingent upon confirmation of the developer's completion of Cold Fusion security module training, we believe a "Strong" opinion for this Section is justified at the present time.***	

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.

Risk Manager Tools (Free):

- Privacy Policy Template For Mobile Applications

Articles & Whitepapers (Free):

- The Hidden Privacy and Security Risks of Apps

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

Options for Application Security Scanning Tools:

- IBM AppScan – see: www.ibm.com
- HP WebInspect – see: www.hp.com

Options for Application Security Penetration Testing:

- iViz – see: www.ivizsecurity.com, Phone: 617.391.0176, Email: varun.sharma@ivizsecurity.com
- Trustwave – see: www.trustwave.com, Phone: 312.873.7474, Email: CPogue@trustwave.com
- Mandiant Corporation – see: www.mandiant.com, Phone: 703.683.3141, Email: investigations@mandiant.com

Options for Mobile Application Testing:

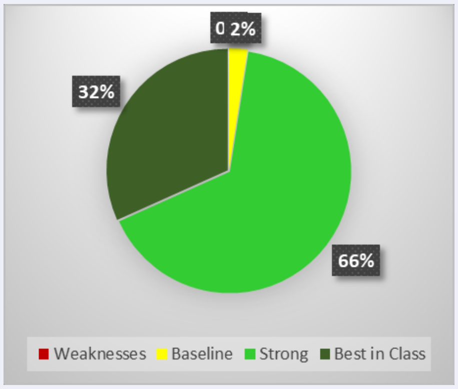
- ICSA Labs – see: www.icsalabs.com, Phone: 717.790.8143, Email: Management@NetDiligence.com

7. System & Network Operations

Topics Covered

- Identify deployed firewall solutions and other perimeter security components?
- Identify deployed anti-virus (AV), advanced endpoint detection & response (EDR) 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

	Appears to have superior **BEST IN CLASS** practices	Findings for **ALL** clients 2017-2018:  2017-18 Client Population % by Sector: 10% Financial, Insurance & Legal 10% Healthcare 0% Retail 12% Technology, Consulting & Media 7% Manufacturing 2% Energy 54% Public Sector & Non-Profit 5% All Others
X	Appears to have **STRONG** practices	
	Appears to have minimum **BASELINE** practices	
	Appears to have one or more key **WEAKNESSES** noted	
Notes	The District reportedly relies upon Cisco firewall solutions (maintained by the City), and upon Microsoft's Windows Defender for antivirus and malware prevention. System patching is primarily manual. Change management, to a significant degree is managed on the District's behalf by the City through their centralized IT ticketing system. Mobile device management (MDM) is supported through a Meraki solution that is used for iPad devices within the public programs areas. Bring your own device (BYOD) is not supported within the District at this time. ***We believe a "Strong" opinion is justified for this Section at the present time.***	
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.		

Risk Manager Tools (Free):

- Personal Device Use (BYOD) Policy

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 Firewall Solutions:

- Cisco – see: www.cisco.com
- Juniper Networks – see: www.juniper.net

Options for Antivirus (AV) And Malware Prevention:

- Trend Micro, Inc. – Phone: 202.415.3955, Email: tom_kellermann@trendmicro.com
- Symantec – see: www.symantec.com
- McAfee – see: www.mcafee.com
- Kaspersky Lab – see: www.kaspersky.com

Options for Patch Management:

- Microsoft WSUS/SCCM – see: www.microsoft.com
- Altiris (Symantec) – see: www.altiris.com

Options for Change Management:

- BMC Remedy – see: www.remedy.com

Options for Systems Remediation & Managed Services:

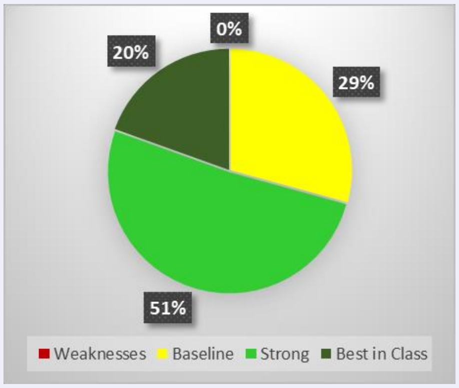
- Integrity Technology Systems, Inc. – see: www.integritysrc.com, Phone: 515.528.0023, Email: Leslie.Matheson@IntegritySRC.com
- Emerald Data Networks – see: www.emeralddata.net, Phone: 678.302.3000, Email: drodgers@emeralddata.net

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?
- Please briefly summarize your overall approach for data backup management in terms of relying upon cloud-based solutions vs. retaining on-premise capabilities? Do you have plans for changing the current mix within the next couple years?
- In light of the heavy impacts that ransomware has had on organizations during the past few years, we have learned that organizations that include at least one “air gap” style segregation element in their backup strategy fare better in such events. Have you implemented any “air gap” storage protections that include either physical (e.g., off-site lockbox, use of write-once-read-many (WORM)) or digital (e.g., custom cloud backup access control, multi-generation version management) features?
- 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 **BEST IN CLASS** practices	Findings for **ALL** clients 2017-2018:  2017-18 Client Population % by Sector: 10% Financial, Insurance & Legal 10% Healthcare 0% Retail 12% Technology, Consulting & Media 7% Manufacturing 2% Energy 54% Public Sector & Non-Profit 5% All Others
	Appears to have **STRONG** practices	
X	Appears to have minimum **BASELINE** practices	
	Appears to have one or more key **WEAKNESSES** noted	
Notes	The District does not appear to have a formal disaster recovery & business continuity plan (DR/BCP) program or document in place today, ***and we strongly suggest developing one in the near-to-medium term.*** That having been said, management did share with us several task-level elements of such a program that exist today, including: (a) an on-premise dedicated backup server for their primary file server that runs regular snapshots and is used for periodic file recovery requests, (b) cloud-based	

backup for their on-premise Innovative (ILS) server through Innovative (although management noted that recovery tests have not been performed – ***and we would suggest such an effort in the near-term***), and (c) 20-minute UPS capacity for District servers and network switches. Full server recovery, if/when needed, would involve reinstallation onto spare server equipment. Network equipment issues will often require assistance from the City in case of unit failures. ***We believe a "Baseline" opinion is justified for this Section at the present time, and would further suggest that developing (and maintaining) a formal DR/BCP document would move the District toward a "Strong" level of capability.***

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.

Risk Manager Tools (Free)*:*

- Business Interruption Cost Calculator

Articles & Whitepapers (Free):

- Preventing eBusiness Interruption
- 21st Century Incident Response - Incident Response Process Automation
- The Intersection of Business Continuity and Data Breach Preparedness
- Business Continuity in Healthcare – External Service Providers, Personal Health Records, and ePrescriptions
- Business Continuity in Healthcare – Healthcare Reform
- Business Continuity in Healthcare–Electronic Medical Records

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 Disaster Recovery Consulting And Service Providers:

- SunGard – see: www.sungard.com
- IBM Business Recovery Services – see: www.ibm.com
- Avalution – see: www.avalution.com Phone: 866.533.0575, Email: contactus@avalution.com
- Concept Analysis and Integration – see: caaii.com Phone: 301.997.2177 x7011, Email: dholloway@caaii.com
- Integrated Systems Consultants – see: www.i-s-c.com, Phone: 231.492.0472, Email: tfairchild@i-s-c.com
- Loricca, Inc. – see: loricca.com Phone: 813.600.3005 x102, Email: mwhitcomb@loricca.com

Options for Datacenter Power Solutions:

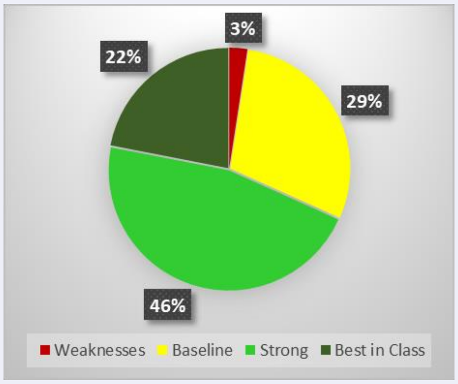
- APC – see: www.apc.com

9. Incident Response Procedures & Functions

Topics Covered

- Please describe your organization-wide Information Response Plan (IRP) program – and the extent to which it is formally documented.
- 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?
- Have you investigated the extent to which (if any) the “Dark Web” has obtained unauthorized access to your systems, customer/employee data, or proprietary intellectual property?
- 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?
- (Only if you rely on SolarWinds SIEM) Have you confirmed any impact and/or completed remediation efforts arising from the SolarWinds cyber exploit from 2020?
- 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

<table>
<tr><td></td><td>Appears to have superior <b>BEST IN CLASS</b> practices</td><td rowspan="4">Findings for <b>ALL</b> clients 2017-2018:


2017-18 Client Population % by Sector:
10% Financial, Insurance & Legal
10% Healthcare
0% Retail
12% Technology, Consulting & Media
7% Manufacturing
2% Energy
54% Public Sector & Non-Profit
5% All Others</td></tr>
<tr><td></td><td>Appears to have <b>STRONG</b> practices</td></tr>
<tr><td>X</td><td>Appears to have minimum <b>BASELINE</b> practices</td></tr>
<tr><td></td><td>Appears to have one or more key <b>WEAKNESSES</b> noted</td></tr>
<tr><td>Notes</td><td colspan="2">The District relies to a significant extent upon the City to assist with incident response plan (IRP) requirements and needs in the normal course. <b><i>To further strengthen their capabilities in this area, we would very much suggest that the District formulate its own documented IRP – integrating, as needed, references to the services and assistance being provided explicitly by the City, and ensuring that the District can address any gaps that might exist</i></b>. Our Breach Plan Connect IRP hosted service might well contribute to this effort (please see: https://netdiligence.com/solutions/breach-plan-</td></tr>
</table>

connect/). Within the context of City support, we learned that District employees are able to open a ticket with the City (or if more urgent, contact them directly) in case of a suspected information security incident. The City is also responsible for maintaining intrusion detection/prevention system (IDS/IPS) capabilities on behalf of the District as part of their overall responsibility in maintaining network and firewall connectivity. ***Management advised of two notable recent information security incidents that impacted the District's operations. The first involved their recently-retired, former Executive Director, who fell for a phishing email and had his email account compromised. Another employee suffered a similar fate more recently, but Microsoft 365's artificial intelligence engine picked up the subsequent exploit attempts from Asia and blocked them while also notifying staff of the issue. Given the City's ongoing contribution to the District's modest efforts in this area, we believe a "Baseline" opinion is justified for this Section – but we would also urge significant additional effort in this area by District management in the near-term.***

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.

Risk Manager Tools (Free):

- State Security Breach Laws Response Guide (50-state map of breach duties)
- Data Breach Cost Calculator
- Notification Cost Calculator
- A Guide to Data Breach Incident Response Planning
- Data Breach Incident Response Workbook
- Data Breach Response Guide
- Incident Response Plan

Articles & Whitepapers (Free):

- Crisis Data Breach Response: Notification
- Crisis Data Breach Response: Credit Monitoring and ID Restoration
- Crisis Data Breach Response: Computer Forensic Services
- Crisis Data Breach Response: Legal Counsel

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 Incident Response Planning Assistance:

- Immersion, Ltd. – see: www.immersionltd.com, Phone: 814.272.0574 x3304, Email: shawn.melito@immersionltd.com

Options for Intrusion Detection/Prevention Systems (IDS/IPS):

- Snort – see: www.snort.org
- TippingPoint (HP) – www.tippingpoint.com

Options for Security Information And Event Management (SIEM) Solutions:

- ArcSight – see: www.arcsight.com
- RSA enVision (EMC) – see: www.emc.com

Options for Incident Response And Data Forensics Services:

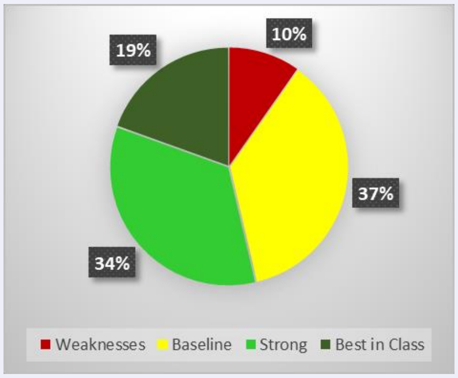
- Navigant – see: http://www.navigant.com Phone: 215.832.4485, Email: dbielby@navigant.com
- Kroll Cyber Security – see: www.krollcybersecurity.com, Email: blapidus@kroll.com
- Kivu Consulting – see: kivuconsulting.com, Email: wkrone@kivuconsulting.com, mbell@kivuconsulting.com

10. Privacy

Topics Covered

- Who serves as your chief privacy officer (CPO), either in title and/or operational function?
- Have you sought to minimize the collection of sensitive personal data in your organization, and providing confirmed proper business justification in writing/policy for all such required instances?
- If your business operations incorporate multi-national jurisdictions, have you ensured/confirmed compliance with various global data privacy standards such as GDPR (E.U.), PIPEDA (Canada), or others?
- 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?
- 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 **BEST IN CLASS** practices	Findings for **ALL** clients 2017-2018:  2017-18 Client Population % by Sector: 10% Financial, Insurance & Legal 10% Healthcare 0% Retail 12% Technology, Consulting & Media 7% Manufacturing 2% Energy 54% Public Sector & Non-Profit 5% All Others
	Appears to have **STRONG** practices	
	Appears to have minimum **BASELINE** practices	
X	Appears to have one or more key **WEAKNESSES** noted	
Notes	Management advised that the District has not been actively engaged in the data privacy area for at least the past six years, and has no formal documentation in support of such a program – ***and given that Library operations would tend to maintain at least some level of client personal information in their systems, we recommend the development of a data privacy program in the near-term.*** To the extent that any such issues would arise involving a data privacy breach, they would be referred to the District's attorney at the law firm of Seter & Vander Wall (please see: https://svwpc.com/). Management is also aware that they can rely upon McGriff Colorado Special Districts for specific referrals and assistance from support vendors in case of need (including if a possible cyber insurance policy claim is involved). The District reportedly has not experienced a data privacy breach event within the past year. ***We believe a "Weaknesses" opinion is justified for this Section at the present time, and we urge the District to implement a data privacy program.***	

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.

Risk Manager Tools (Free):

- Publicized Breach Events
- Privacy Case Law
- Web Site Privacy Policy (Sample Policy)
- Privacy Policy Template For Mobile Applications
- Security and Privacy Controls for Federal Information Systems and Organizations

Articles & Whitepapers (Free):

- The New Year May Mean You Need a New Privacy Policy: Recent Changes in Laws Require Attention
- California Passes Three Privacy and Data Security Laws that Affect Many Companies
- The Hidden Privacy and Security Risks of Apps
- Understanding the Final HIPAA Security and Privacy Rules
- Protecting Personal Information – A Guide For Business (FTC)

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 Privacy Consulting & Breach Investigation Services:

- Nelson Levine de Luca & Hamilton – see: www.nldhlaw.com Phone: 215.358.5154, Email: jmullen@nldhlaw.com
- Baker Hostetler – see: www.bakerlaw.com Phone: 513.929.3491, Email: cahoffman@bakerlaw.com
- Faruki Ireland & Cox – see: http://www.ficlaw.com/, Phone: 937.227.3733, Email: rraether@ficlaw.com
- McDonald Hopkins – see: www.mcdonaldhopkins.com, Phone: 248.220.1354, Email: jgiszczak@mcdonaldhopkins.com
- Edwards Wildman Palmer – see: www.edwardswildman.com Phone: 617.239.0585 Email: mschreiber@edwardswildman.com

Options for Privacy Breach Notification & Credit Monitoring Services:

- Immersion, Ltd. – see: http://www.immersionltd.com Email: elito@immersionltd.com
- Experian – see: http://www.experian.com Email: ozzie.fonseca@experian.com

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 or visit us at 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 or visit us at 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