SPIRION
200 Central Avenue, 19th Floor, St. Petersburg, FL 33701 | (646) 863-8301 | www.spirion.com

2020 Blackbaud Breach:
Quantifying Organizational Risk and Preparing Your Response

What Happened?

- **May 14th, 2020** cloud software company Blackbaud identified an intrusion by threat actors that exposed the personal information of donors to at least 200 educational and other nonprofit institutions around the world. Blackbaud is a South Carolina-based provider of cloud-based software and services designed for non-profit organizations.

- **July 16, 2020** The company disclosed the breach to customers and also indicated that it paid the actors to release personal and other data compromised by ransomware. In subsequent disclosures, the company cited Raiser's Edge and NetCommunity as involved in the compromise. Altru, Financial Edge NXT, and Raiser's Edge NXT have also been mentioned.

According to the British Broadcasting Corporation (BBC), "in some cases it (the breach) involved donors' details including:

- Names, ages and addresses
- Car license details
- Employers
- Estimated wealth and identified assets
- Total number and value of past donations to the organization in question
- Wider history of philanthropic and political gifts
- Spouses' identity and past gift-giving
- Likelihood to make a bequest triggered by their death"

The University of York, cited the following in their breach notice as personal data subject to the intrusion:

- Basic details (e.g. name, title, gender, date of birth, and student number, if applicable);
- Addresses and contact details (e.g. phone, email and LinkedIn profile URL);
- Course and educational attainment details (e.g. what qualification you received and some of the extracurricular opportunities you participated in while studying at York, if applicable);
- A record of your engagement with alumni and fundraising activities (e.g. inquiries, event participation, volunteering, donations, and any other interactions you have with us);
- Professional details (e.g. the profession you work in and your employer);
- Information about your interests you have provided to us (e.g. in response to one of our surveys)

What do I need to do?

The first things most organizations need to report on internally and externally is, "***what is our exposure and what is the impact?".***

This document will help Spirion clients answer those questions and allow them to:

- Minimize negative consequences of information security incidents, and improve the the ability to promptly restore operations.
- Enable prompt incident response decisions by appropriate stakeholders.
- Proactively reduce the exposure to information security incidents by employing consistent incident management processes that incorporate lessons learned from past incidents.
- Satisfy federal, state, and industry regulations that require improved protection of sensitive and private information, and timely disclosure of potential breaches to affected individuals.

Step by Step

Use of Spirion will be directed by your organization's Incident Response and/or Breach Notification policies, as applicable. Organizations that have reason to believe that their data was affected should take the following steps:

1) **Confirm directly with Blackbaud that your organization was in fact affected by the breach.** If you've received an email saying that your organization has been affected by the Blackbaud breach, that isn't enough to confirm your exposure — it could be from scammers posing as the potentially breached company in an effort to get your sensitive information. Don't respond to potentially fake emails. Contact Blackbaud directly to confirm the breach.

2) **Confirm what types of data were affected in the breach**. As part of your breach notification and reporting process it is important to validate the scope of affected data. Knowing which data types were affected will assist in the internal identification of the locations and controls currently in place. This will also assist in the accurate reporting of the scope of the breach.

3) **Contact your Blackbaud support representative and request the following:**
    - *A copy of your organization's databases for each product under license*
    - *A copy of the database schema*

4) **Identify scope of affected data and begin to formulate response.** Leveraging a combination of the techniques outlined below, Spirion and native database tools, evaluate scope of breach and identify affected parties.

5) **Based on the results of step 4, review with legal counsel** to determine, by jurisdiction, if notification to affected parties, law enforcement, and/or insurance carriers is required. If so, draft preliminary statements of fact and breach notices and review with upper management.

Using Spirion Sensitive Data Manager to confirm the scope of the affected data

Please refer to the following Spirion guide on how to search databases:

https://myguide.spirion.com/articles/Knowledgebase/How-to-Search-a-Database-27-3-2020

a. *Note: It is very common for sensitive data to be entered into free text fields and may be stored in file attachments within your database. Given the scale of the typical BlackBaud DB, it is not practical to manually search for sensitive data.*

Scanning Blackbaud Databases with Spirion

Option 1: For Blackbaud Database Administrators

For organizations that have a high-level understanding of the Blackbaud database and can quickly find the data subjects names column(s) on their respective tables and or has another internal database with donor information. *This* will provide a list of all donors who were affected by the breach and the data elements which were exposed.

1. Create a custom dictionary list by doing a SQL query on the database pulling the list of all the donors names.

2. Manipulate the names so you can account for variations in excel or SQL so there is: First Last; Last, First; First initial Last Name

    i. Note: Dictionary words are case insensitive. For example, if you have JOHN SMITH in your dictionary, it will match all of these:

        1. John Smith
        2. JOHN SMITH

3. John smith

ii. Note: The Name is read from the Header section of the dictionary itself and must be present in the dictionary file.
iii. Note: The file encoding needs to be in UTF-8 or ASCII.

3. Create a Sensitive Data Definition (SDD) similar to the following:

    1. Dictionary Names >= 1 total matches AND
    2. SSN Anyfind >= 1 total matches OR
    3. Bank Account Anyfind >= 1 total matches OR
    4. CCN Anyfind >= 1 total matches OR
    5. DOB Anyfind >= 1 total matches OR
    6. Personal Address Anyfind >= 1 total matches OR
    7. Telephone Number Anyfind >= 1 total matches OR
    8. Passport/dl/etc. Anyfind >= 1 total matches OR

4. Analyze database through SSMS and locate all FreeText Fields/Varchar(Max or >50)

5. Go to SearchColumnNames in your Spirion scheduled task policy and insert a list of the column names which are FreeText.

    Note: Format is important. No “[ ]” & no “dbo.”. It should be a single column name per line.

6. Run search on database

    Because it’ll be a fast search, one agent will suffice most likely.
    If you have multiple places where the database is deployed to; it’s reasonable to take agents away from disco teams to do dedicated single agent searches.

Scanning Blackbaud Databases with Spirion

Option 2: Blackbaud Database is Unknown

For organizations who lack a high-level understanding of the Blackbaud Database Schema.

This option will only tell you the data elements which were exposed. You will need to cross reference the results from this search with the known donors whose information was uploaded to Blackbaud.

1. Create an SDD which combines two unique data elements such as SSN and CCN and other AnyFinds.

    - The sensitive data definition should look like this:
        - AnyFind SSN >= 1 unique matches OR
        - AnyFind CCN >= 1 unique matches AND
            - DOB AnyFind >= 1 total matches OR
            - Personal Address AnyFind >= 1 total matches OR
            - Telephone Number AnyFind >= 1 total matches OR
            - Bank Account AnyFind >= 1 total matches OR
            - Passport/dl/etc. AnyFind >= 1 total matches OR

2. Run search on database using a discovery team.

Scanning Blackbaud Databases with Spirion

Option 3: Using Spirion's Command Line Interface

- Note: This option is only If your organization is using an older version of Spirion, i.e. IdentityFinder without a Console server.

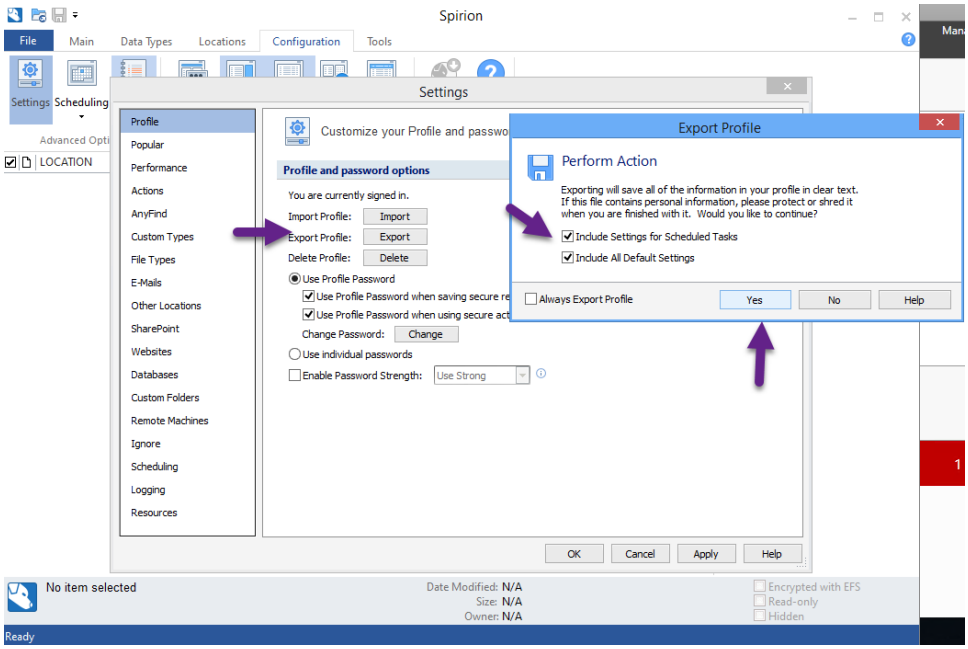
Agent only scanning - Adding customized search to the Agent using Command Line and Custom configuration.

Steps for adding a customized search to the Agent using Command Line:

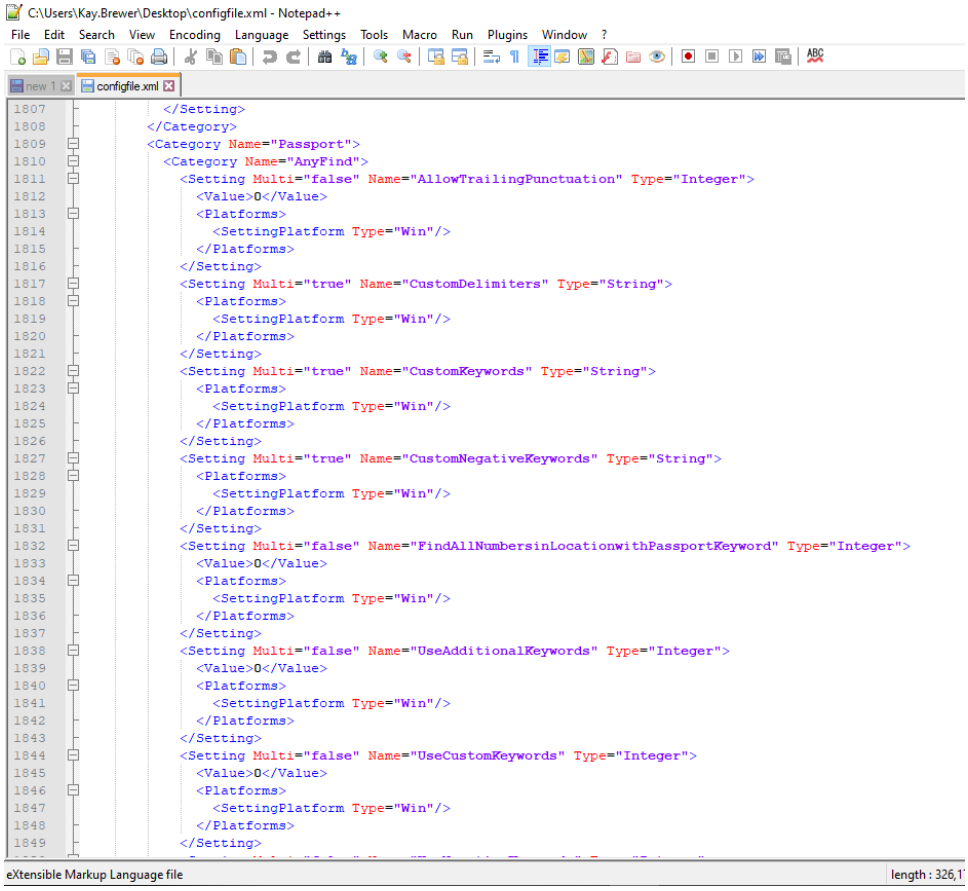
1. Open the Agent on an Endpoint

2. Go to Configuration > Settings > Profile

3. Export your profile to a .xml



4. Once the .xml is created open the configuration file and edit the settings you would like to customize for this search. A helpful tool to review the available settings is the Settings Viewer Tool located on our knowledge base.



5. When the xml is finished saved the xml and load an elevated command line and run a command like the one below.
   IdentityFinderCmd /jobmode /configurationfile="c:\myconfigfiles\profile1.xml"

    a. For more information on the command line interface see this article: https://myguide.spirion.com/articles/Knowledgebase/Endpoint-Software-Command-Line-Interface-31-3-2020?lId=00h00000000001C00ii&lname=General

200 Central Avenue, 19th Floor, St. Petersburg, FL 33701 | (646) 863-8301 | www.spirion.com

Leveraging Spirion's Senstive Data Manager as part of your breach response process

As part of your breach notification response protocol, notifying your data subjects will require:

1. Knowing which data subjects to notify
2. Knowing which jurisdictions (Countries/States) those data subjects reside within

Scanning Blackbaud databases with Spirion Sensitive Data Manager to assist with breach notification

After collecting the information from the results using technique one or two. Running a secondary search utilizing the technique below can assist in notifying the donors of exactly what information of theirs was breached.

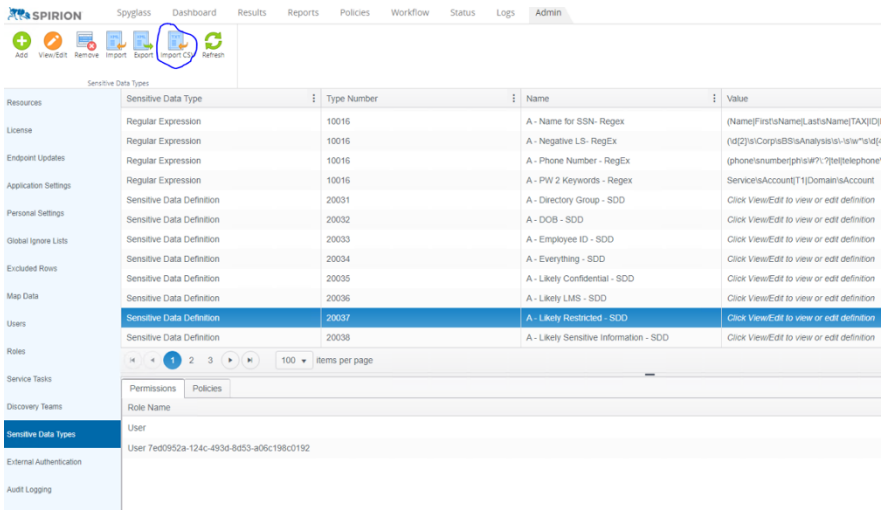
1. Write a query to return two or more data elements of a possibly affected subject. Ideally 4-5 data element points on each donor in database.

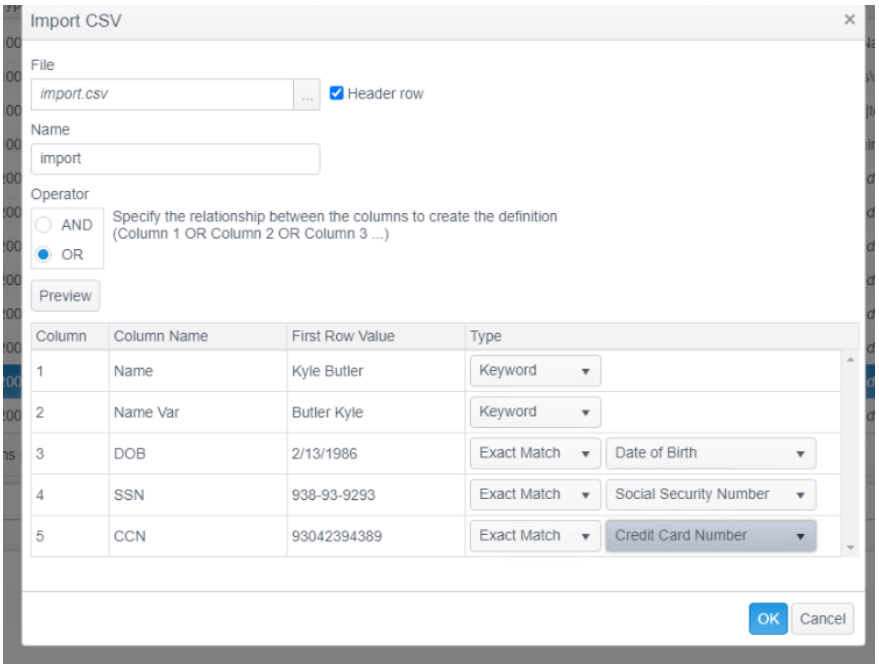
2. Export the query results to csv as outlined below:

   Note: Data types DO NOT have to exist in Spirion Console

A	B	C	D	E	F	G	H
Name	Name Var	DOB	SSN	CCN			
Kyle Butler	Butler Kyle	2/13/1986	938-93-9293	93042394389			

3. Use the Spirion DSAR Excel import functionality to quickly create multiple SDD's which are specific to a donor. This can be found under the "Admin Tab" within the Sensitive Data Types Section. The import button is circled in the ribbon bar in the picture below.





4. Run search on entire database searching only tables and columns discovered using technique 1 or 2.

Additional Resources

Spirion Resources:

- A Mid-Year Review and Look Ahead for 2021 - http://spirion.com/blog/data-privacy-and-compliance-ccpa-cprea-gdpr-a-look-ahead-for-2020/

- U.S. State Data Protection Laws Enforceable in 2020 - https://www.spirion.com/wp-content/uploads/2020/04/SPIRION-Datasheet-US-State-Data-Protection-Laws-2019-WEB.pdf

- How to use Sensitive Data Definitions –
  - https://myguide.spirion.com/articles/Knowledgebase/How-To-Use-Sensitive-Data-1-4-2020
- Using custom dictionaries - https://myguide.spirion.com/articles/Knowledgebase/Using-Dictionaries-6-4-2020LoginLogin to Spirionmyguide.spirion.com

- Creating reports - https://my.spirion.com/Help/EnterpriseConsole/index.htm#3284.htm%3FTocPath%3DReports%7C 0

Data Protection Laws Implicated:

Throughout the world, information security and data privacy laws – data protection laws – almost universally mandate (1) identification of personal information in an organization's information ecosystem; (2) establishment of controls to protect that information; and (3) timely notification to affected persons and to law enforcement in the event of a breach. Spirion assists in all three areas, and with respect to the third, can help the victim organization complete a breach notice. Under the EU General Data Protection Regulation (GDPR) Art. 33(3)(a), a breach notice must "describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned[.]" California's breach notification statute[1] requires disclosure of a "list of the types of personal information that were or are reasonably believed to have been the subject of a breach."

- **Canada.** Canada's federal data protection statute is the *Personal Information Protection and Electronic Documents Act* (PIPEDA). Section 10.1 addresses breach notification.
- **European Union.** The *General Data Protection Regulation 2016/679* (GDPR) is the primary data protection law for the European Union. Articles 33 and 34 address breach notification.

- **United Kingdom.** The United Kingdom's Data Protection Act 2018 (DPA) is the U.K.'s implementation of the GDPR. As a consequence, breach notification requirements will be the same as those of the GDPR.
- **United States.** While there is no generally-applicable federal data protection law, multiple sectoral data protection laws require breach notification, such as HIPAA/HITECH (healthcare; 45 CFR §§ 164.400-414) and GLBA (financial; 12 C.F.R. § Pt. 225, App. F.). All individual U.S. states have breach notification laws.

[1] Cal. Civ. Code § 1798.82(d)(2)(B).

If you have any questions or would like additional information, please contact a member of our Privacy and Data Security team: Support@Spirion.com