Blackbaud Cyber Security Incident: What Your Organization Needs to Know

What are the Blackbaud cybersecurity incident response options for your organization?

build
transforming nonprofits

Kyle Haines

Partner, Build Consulting

Get the most from your experience!

Interact

Ask questions using the available Q&A feature

Focus

Avoid multitasking. You may just miss the best part of the presentation!

Webinar Recording and Slides

Links to the recordings (video and MP3) will be shared via email after the webinar.

build
transforming nonprofits

Next Build webinar:

Microsoft Dynamics and Salesforce

A presentation of what you need to know
before choosing a platform

Wednesday, August 12
from 12 PM EDT

build
transforming nonprofits

build
transforming nonprofits

Invested

Work exclusively with nonprofit organizations; have served over 1,000

Strategic

Help our clients make IT and IS decisions that support mission

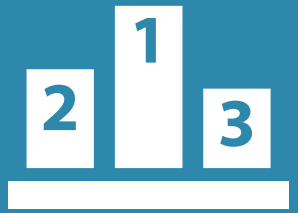
Collaborative

Empower you to make informed choices

build
transforming nonprofits

How Build leads in the social good sector:

Assessments and Roadmaps



Software Selections

Implementation Support

Interim or Part-Time CIOs

Outsourced CRM Management

build
transforming nonprofits

The information provided in this webinar does not, and is not intended to, constitute legal advice; instead, all information, content, and materials available in connection with this webinar are for general informational purposes only.

Attendees of this webinar should contact their attorney to obtain advice with respect to any particular legal matter.

build
transforming nonprofits

Three things we want to cover today

BACKGROUND

POTENTIAL RISKS

RESPONSE OPTIONS

build
transforming nonprofits

Background

What Blackbaud Disclosed

"In May of 2020, we discovered and stopped a ransomware attack. In a ransomware attack, cybercriminals attempt to disrupt the business by locking companies out of their own data and servers. After discovering the attempted attack, our Cyber Security team—together with independent forensics experts and law enforcement—successfully prevented the cybercriminal from blocking our system access and fully encrypting files; and ultimately expelled them from our system.

Prior to our locking the cybercriminal out, the cybercriminal removed a copy of a subset of data from our self-hosted environment. The cybercriminal did not access credit card information, bank account information, or social security numbers. Because protecting our customers' data was our top priority, we paid the cybercriminal's demand with confirmation that the copy they removed had been destroyed."

build
transforming nonprofits

$3,500,000,000 USD

FBI, *2019 Internet Crime Report*

build
transforming nonprofits

$8,965,847

LOSSES FROM RANSOMWARE ATTACKS IN 2019

FBI, *2019 Internet Crime Report*

build
transforming nonprofits

What Build has learned

- The breach occurred from 02/07/2020 to 05/20/2020
- The technical investigation has been completed
- The criminal investigation(s) are ongoing
- Blackbaud cannot provide a copy of the data that were removed
- The impact is wide-spread
  - Nearly all of Build's clients with Blackbaud products that were not in Azure or self-hosted by the client were affected
  - Blackbaud was experiencing long wait times for their incident response hotline
- A sophisticated criminal could easily make inferences about the organization for whom they have data.

build
transforming nonprofits

What Build does not know

- How did the breach occur?
- What remedies/changes were made?
- How long will Blackbaud monitor the dark web?
- How we can be sure that the data was actually destroyed?

build
transforming nonprofits

Trust the criminals?

build
transforming nonprofits

Potential Risks

Dear Beth and Mark,

On the behalf of the Board and staff of the Center for Researching we would like to thank you for your last gift of $25.00 made on May 20, 2020.

Without the support of supporters like you our mission would not be possible. In these uncertain times, Center for Researching needs your support more than ever. Can we count on your support [donate.centerforresaerching.org]?

Best,

Susan

P.S. If we don't have your most recent donation history, please call (202) XXX-YYYY

$300,478,433

LOSSES FROM SPOOFING ATTACKS IN 2019

FBI, *2019 Internet Crime Report*

build
transforming nonprofits

Dear Beth and Mark,

Persia Fischer asked that I reach out to you to see if we could schedule some time in the coming weeks to thank you for your support of the Center for Researching

She may not be able to join the call, but she wanted to be sure that you received some late-breaking news that would not be possible without your past support. She's hopeful that you can support us again and is excited to connect. Would you have any time in the next few days to schedule a call? Please let me know what times work for you and we'll get something scheduled!

Bob
Executive Assistant
Center for Researching

$57,836,379

LOSSES FROM SPEARFISHING ATTACKS IN 2019

FBI, *2019 Internet Crime Report*

build
transforming nonprofits

Unencrypted data to aid in confidence schemes and exploits

WEALTH RATINGS

PHONE

DATE OF BIRTH

GIFTS

EMAIL

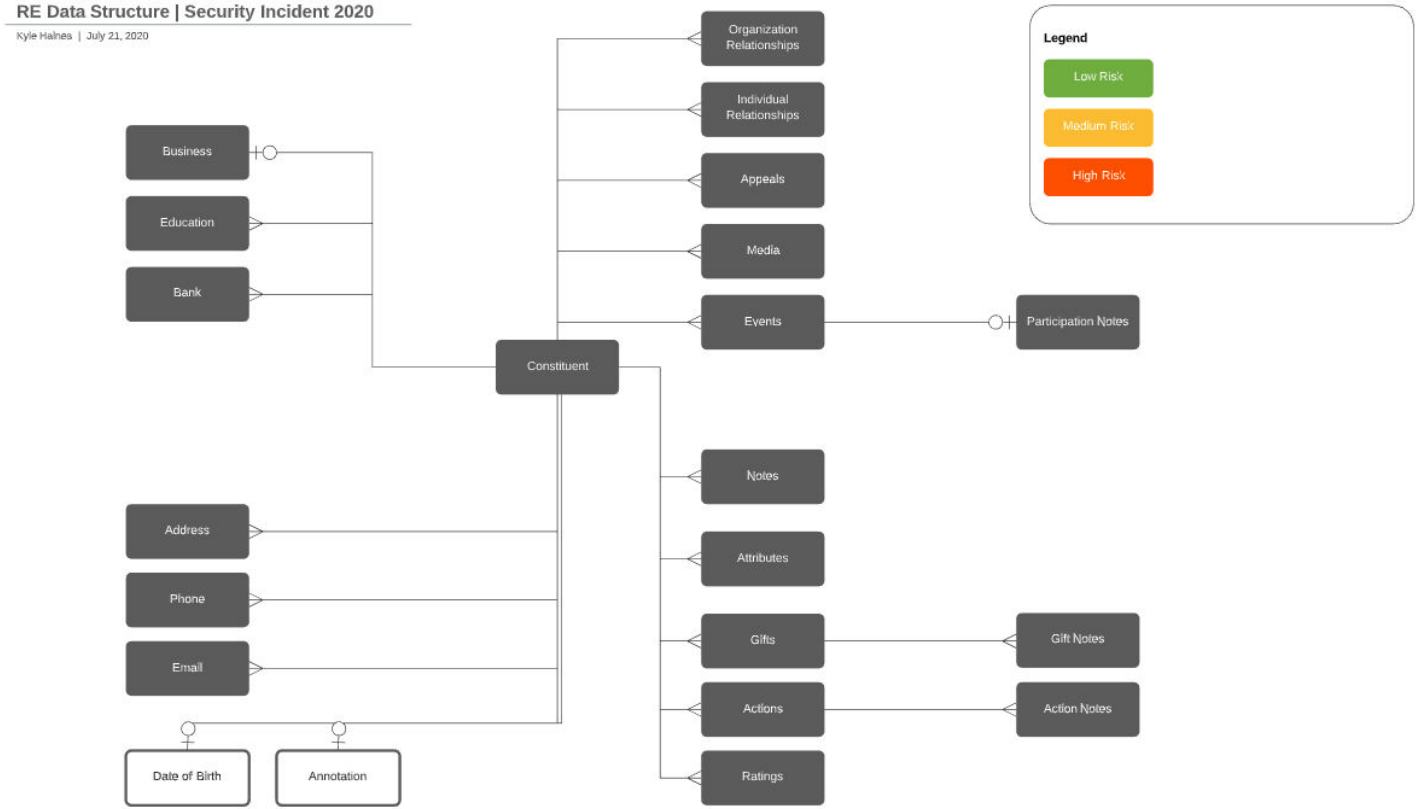
RELATIONSHIPS

NOTES

INTERACTIONS

build
transforming nonprofits

Sample Risk Assessment



build
transforming nonprofits

Response Considerations

Decision Framework

1. What are you required by federal, state, territory, etc. required to disclose?
2. What is the right thing to do?

build
transforming nonprofits

If you choose **not** to disclose

- Organizations have already started to notify their constituents – your constituents may already know.
- What if the data is later used by these, or other criminals? Who is responsible?
- If you chose not to disclose, is there a brand reputation risk?

build
transforming nonprofits

If you choose to disclose

- How will you respond to inbound questions from?
  - Constituents
  - VIPs
  - Media
- How will you respond to requests from constituents to have their entire record provided to them?
- How will you respond to requests to have data deleted and provide confirmation to constituents?

build
transforming nonprofits

Potential silver linings for your organization

- Perform a comprehensive information system and technology security audit.
- Revisit usage standards – what constitutes data that should not be stored?
- Revisit audit practices – scrub data that should not be stored in unencrypted fields.
- Revisit all manners of data governance and usage.
- Implement data use polices for staff, volunteers, etc.
- Roll out multi-factor authentication on every application you can (many Blackbaud products don’t support MFA).

build
transforming nonprofits

Our advice: Don’t be passive.

build
transforming nonprofits

Q&A