Bill Connors presents Mastering Security in Blackbaud Raiser's Edge NXT® and Raiser's Edge®, sponsored by Blackbaud

The Webinar Series

In 2021, protecting the data of both your organization and your constituents is mission critical. In this three-part webinar series, Bill Connors, CFRE, bCRE-Pro, independent consultant and trainer on Blackbaud Raiser's Edge NXT® and Raiser's Edge®, in partnership with Blackbaud, dove into the most important things you need to know to master security, whether you're using Blackbaud Raiser's Edge NXT or Raiser's Edge. Regardless of your experience level using these solutions, this series is for you. Watch the recorded sessions on-demand here:

- Session 1: Creating a Culture of Security
- Session 2: Understanding Security in Blackbaud Raiser's Edge NXT® and Raiser's Edge®
- Session 3: Deep Dive into Blackbaud Raiser's Edge NXT® and Raiser's Edge® Security Options

Session slides, "handouts," and answers to two questions with long answers deferred by Bill during Session 3 are available for download on Bill Connors' website: https://billconnors.com/resources/

Frequently Asked Questions from the Webinars

We received 700+ questions over the course of the webinar series! We have compiled responses to the most frequently asked questions here, organized by session. Each question is hyperlinked to its response.

Session 1: Creating a Culture of Security

1. How frequently is our data backed up in Blackbaud Raiser's Edge or Raiser's Edge NXT?
2. What considerations do we have to keep in mind when we request a restore-to-backup?
3. What is a factory reset? What data is included in the reset?
4. What can I do if I am not eligible for restoring from a backup?
5. How can I tell if my organization is using automated recurring gifts?
6. Does Blackbaud require that you update your Blackbaud.com password periodically?
7. Is it okay to use a simple password as the temporary password when setting up a new user?
8. What about NIST password recommendations? I have not seen anyone implement them, but they seem like a good idea.
9. What about using the web browser to save passwords? Or saving them in a password-protected Excel spreadsheet?
10. Per our corporate policy, we cannot put our donor database in the cloud, so we cannot move to Raiser's Edge NXT. Is Blackbaud still committed to maintaining and upgrading Raiser's Edge, with regard to security?

11. Do you have examples of cybersecurity polices, such as Bring Your Own Device (BYOD) or an incident response plan?
12. Bill advised against sharing details about your organization on Facebook since there could be bad actors in the Facebook RE user group, for example. Is the Blackbaud community secure?
13. Is it safe to share…
    - Excel spreadsheets on a shared drive?
    - Documents using Google drive?
    - Documents using SharePoint/OneDrive?
    - Password-protected documents via email?
14. How should we securely transmit data to another entity, such as a mail house?
15. Do you send the phishing emails to your customers or just internally at Blackbaud?
16. What platform do you use for phishing tests?
17. Can you tell us more about what Bill mentioned about no longer sending constituent information in a gift notification email?
18. What should I do if I am asked by a Blackbaud employee to share my username and password?

Session 2: Understanding Security in Blackbaud Raiser's Edge NXT® and Raiser's Edge®

1. What data is encrypted in RE NXT?
2. I was unaware of separate security for Online Express. Where can I find more information on it?
3. How do I restrict database view to certain users?
4. Is there a way to print out the details of each security group?
5. What is the difference between two-factor authentication (2FA) and multi-factor authentication (MFA)?
6. What is the difference between single sign-on (SSO) and MFA? (And does using SSO by itself increase security?)
7. Is it possible to force all users to use MFA? We've had to have users enable MFA themselves, and then they are able to disable it, too. If not, can we monitor which users do not have MFA enabled?
8. What is going on with the BB ID change Bill mentioned? How is SSO affected?
9. As an Azure user – are we included/do we have to worry about this new hosting/ID change?
10. Is Blackbaud going to force all hosted clients to move to Azure?
11. What is the difference between Azure and Citrix?
12. What is the process of migrating from Blackbaud's self-hosted data centers to Azure?
13. What recommendations would Bill make for granting rights to consultants that need admin rights?
14. What recommendations do you have about what rights IT staff need?
15. How do you recommend small develop shops (less than 3 people) organize themselves?
16. You mentioned that only the DBA should have access to security. What is your recommendation for having one additional person with security access as the DBA "backup?"
17. How do I get someone to review my security setup individually and ensure it aligns with best practices?

Session 3: Deep Dive into Blackbaud Raiser's Edge NXT® and Raiser's Edge® Security Options

1. Where do I go to manage Blackbaud.com security?
2. Where do I go to manage database view security?
3. Where do I go to manage web view security?
4. Is it possible to test out a user's security before granting the privileges to them? What about if you are using single sign-on?
5. Bill pointed out how to grant access to Web Services, but I don't know what that even means. What does Web Services do?
6. Is it possible to give someone access to events without giving them any access to view gifts?
7. Can I give access to Lists in web view without giving access to Query in database view?
8. Are there any settings in the web view security that will override any security settings in the database view?

9. How do users know if they don't have access to something in web view or database view?
10. How do you set rights for moving gifts from one constituent to another in web view?
11. How extensive is the Security by Fund option? Does it affect fund selection during gift entry?
12. What is the difference between a solution admin, environment admin, and organization admin in web view? How can I tell who they are?
13. What do you recommend we do after a user leaves the organization?
14. Is there any further training available about Security in Raiser's Edge and Raiser's Edge NXT?

Answers

Session 1: Creating a Culture of Security

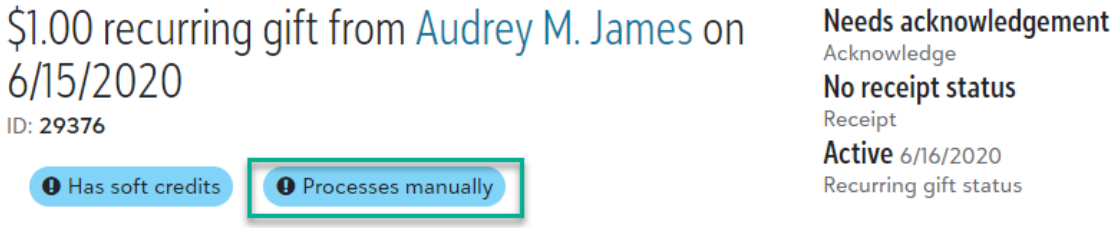
1. **How frequently is our data backed up in Blackbaud Raiser's Edge or Raiser's Edge NXT?** If your data is hosted by Blackbaud, a transaction log backup is run every 15 minutes. Check out the schedule of backups and backup storage here: https://kb.blackbaud.com/knowledgebase/Knowledge/40591/

2. **What considerations do we have to keep in mind when we request a backup of our database to be restored to production?** The answer to this question depends on whether you have 1) Raiser's Edge or 2) Raiser's Edge NXT. 1) When restoring a backup of your Raiser's Edge version 7 database, your current database is overwritten with the restored data: you will lose any and all information that has been entered in the database since the time of the backup. Only restore to a backup if you understand that any subsequent data will be lost. See more here. 2) If you are a Raiser's Edge NXT customer, the database view can be restored with the save caveat, but additionally the web view will undergo a factory reset. See more here. Further, as noted in the previous Knowledgebase article, there are some limitations around which databases *cannot* be restored: if you are using automated recurring gifts, your database cannot be restored from a backup. Additionally, Azure customers cannot restore their production database once they are live with Raiser's Edge NXT, Financial Edge NXT, or Blackbaud Church Management. To be clear, backups of the database view are still made and are available to restore elsewhere to consult, the limitation is that they cannot be restored to your live, production environment if your database meets either of these conditions.

3. **What is a factory reset? What data is included in the reset**? A factory reset creates a brand-new web view for your organization; only the database view will be fully restored. A complete list of web view fields that are reset can be found here**:** https://kb.blackbaud.com/knowledgebase/Article/96120**.**

4. **What can I do if I am not eligible for restoring from a backup?** Please see this Knowledgebase. We recommend manually re-entering the data in any situation where it is feasible. You can purchase a temporarily hosted database that can be used to export/import your deleted information. Your organization's site administrator must contact Customer Support.

5. **How can I tell if my organization is using automated recurring gifts?** You can differentiate between manual recurring gifts and automated recurring gifts in the web view because manual recurring gifts are notated like this:



Automated recurring gifts do not have this flag present on the record.

You can also tell if you have active automated recurring gifts by checking web view batches under Fundraising > Gift Management. If you are using automated recurring gifts, you will see batches titled "Installment payment transactions from [DATE] – [PAY METHOD] processed with Blackbaud Merchant Services."

6. **Does Blackbaud require that you update your Blackbaud.com password periodically?** After 180 days of inactivity, you will need to reset your password. Read more about this requirement here: https://kb.blackbaud.com/knowledgebase/articles/Article/43647

7. **Is it okay to use a simple password as the temporary password when setting up a new user?** Yes, however you should ensure that you enable forced password reset upon first logon. This will enable your user to ensure that they immediately change from the simple password to something more complex. Bear in mind that this example only applies to customers who are hosted by Blackbaud in a colocation data centers (e.g., "Boston" or "Vancouver").

8. **What about NIST password recommendations? I have not seen anyone implement them, but they seem like a good idea.** The NIST Password guidelines are certainly considered industry best practices. Blackbaud aligns to the NIST Cybersecurity Framework and is continuing evolving our controls and standards to align to these types of controls and exceed industry benchmarks.

9. **What about using the web browser to save passwords? Or saving them in a password-protected Excel spreadsheet?** It is important for every organization to assess their security risk in alignment with their organizational needs. While many of these functions offer great convenience, there are particular risks associated with those conveniences, and it is important to map those and understand your risks. However, due to the continued evolution and sophistication of cyber attacks, Blackbaud recommend the 'less is best'/'least privilege' model and try not to store anything that isn't absolutely necessary, including and especially passwords or other sensitive data.

10. **Per our corporate policy, we cannot put our donor database in the cloud, so we cannot move to Raiser's Edge NXT. Is Blackbaud still committed to maintaining and upgrading Raiser's Edge, with regard to security?** Absolutely, Blackbaud is committing to fortifying all of our systems with the same security controls and standards. For details on our fortification efforts, please reach out to your Blackbaud representative who can provide the latest installment of the bi-monthly Blackbaud Cybersecurity Updates and Resources document.

11. **Do you have examples of cybersecurity polices, such as Bring Your Own Device (BYOD) or an incident response plan?** There are a wealth of security best practice resources that have these types of examples of templates. Stay Safe Online has some great best practice information: National Cyber Security Alliance: Homepage (staysafeonline.org). However, for specific templates, you may also want to query other Security Industry resources, such as SANS, which has a wealth of templates. (Resource here: Information Security Policy Templates | SANS Institute)

12. **Bill advised against sharing details about your organization on Facebook since there could be bad actors in the Facebook RE user group, for example. Is the Blackbaud community secure?** The Blackbaud Community is secured in alignment with Blackbaud's Global Trust & Security Program and standards. However, it is important for every organization to assess their security risk in alignment with benefit of sharing data, both personally and professionally. Due to the continued evolution and sophistication of cyber attacks, Blackbaud recommends the

'less is best'/'least privilege' model and try not to share anything that isn't absolutely necessary.

13. **Is it safe to share…**
    - **Excel spreadsheets on a shared drive?**
    - **Documents using Google drive?**
    - **Documents using SharePoint/OneDrive?**
    - **Password-protected documents via email?**

    It is important for every organization to assess their security risk in alignment with benefit of sharing data, both personally and professionally. However, due to the continued evolution and sophistication of cyber attacks, Blackbaud recommends the 'less is best'/'least privilege' model and try not to share anything that is not absolutely necessary.

14. **How should we securely transmit data to another entity, such as a mail house?** The best practice is to use a secure file transfer protocol (SFTP).

15. **Do you send the phishing emails to your customers or just internally at Blackbaud?** We conduct these exercises routinely as part of our Security Awareness program for Blackbaud employees. These exercises are not used with customers.

16. **What platform do you use for phishing tests?** Blackbaud currently leverages Phish Labs for phish simulations. Additionally, we use KnowB4 for security awareness training videos. However, there are a wealth of platforms designed to help organizations with these types of simulations and training exercises. Our recommendations would be to investigate platforms that best meet your requirements and organization needs. SANS and Wombat are some other examples. You can also query the web for other free resources as well.

17. **Can you tell us more about what Bill mentioned about no longer sending constituent information in a gift notification email?** We announced in the December 15 What's New in Raiser's Edge NXT blog that notification emails from RE NXT donation forms no longer include personal data. You can read more about this change in the blog post.

18. **What should I do if I am asked by a Blackbaud employee to share my username and password?** If a Blackbaud employee is ever asking for your password, please feel free to ask for their supervisor or report the issue to security@blackbaud.com for us to investigate. Our employees have appropriate access granted on an as-needed basis and should never be asking a customer for their credentials/passwords.

Session 2: Understanding Security in Blackbaud Raiser's Edge NXT® and Raiser's Edge®

1. **What data is encrypted in RE NXT?** You can review this knowledgebase for a full list of encrypted fields in Raiser's Edge NXT: https://kb.blackbaud.com/knowledgebase/Article/47633

2. **I was unaware of separate security for Online Express. Where can I find more information on it?** Here is a detailed knowledgebase on the subject, including a video demo. It is *not* necessary or recommended to require all Online Express users to be supervisors. The first user of Online Express must be a supervisor user, but then additional security groups can be "invited" to use Online Express.

3. **How do I restrict database view to certain users?** If you are hosted in one of Blackbaud's colocation data centers (e.g., "Boston" or "Vancouver"), you could restrict access by not assigning the user a Blackbaud Hosting Services account. However, if you are hosted in Azure, this is not possible single database view access is

authenticated using Blackbaud ID. In this case, you can prevent users from accessing specific database view modules and functionality within their database view security group.

4. **Is there a way to print out the details of each security group?** You can print a group profile in database view using these steps: https://kb.blackbaud.com/knowledgebase/Article/52784. In the web view, use your browser to print the screen.

5. **What is the difference between two-factor authentication (2FA) and multi-factor authentication (MFA)?** The difference between the two is that 2FA is 2 factors and MFA is 2 or more factors. If you were to draw a Venn diagram of 2FA and MFA, 2FA would entirely be within MFA.

6. **What is the difference between single sign-on (SSO) and MFA? (And does using SSO by itself increase security?)** Customers establish an SSO connection with Blackbaud in order to manage authentication for their organization through their Identity Provider (IdP). This allows the customer to have their users sign in with the same authentication to their email, file sharing, and other applications in addition to their Blackbaud solutions. The authentication measures in place with the IdP may or may not include MFA. Managing authentication through a single IdP is generally more secure as it provides greater insight and control over user management and authentication across an organization.

   MFA is one of many authentication measures that can be in place when a user authenticates to an application. MFA is the #1 way users can increase the security of their account.

7. **Is it possible to force all users to use MFA? We've had to have users enable MFA themselves, and then they are able to disable it, too. If not, can we monitor which users do not have MFA enabled?** Today, in order to require or monitor users in this way, a SSO connection is required when MFA is enforced through the IdP.

8. **What is going on with the BB ID change Bill mentioned? How is SSO affected?** The change we are making is to allow organizations to utilize MFA and/or SSO in the non-Azure datacenters. Read here for more details: https://community.blackbaud.com/blogs/13/7533

9. **As an Azure user – are we included/do we have to worry about this new hosting/ID change?** Azure is excluded from this update. Users who are hosted in Azure already leverage BBID for the full login experience.

10. **Is Blackbaud going to force all hosted clients to move to Azure?** No. We would love for everyone to be in Azure, but currently there are some applications and integrations that prevent some sites from being qualified for the move.

11. **What is the difference between Azure and Citrix?** Azure is a hosted environment; Citrix is a third-party virtualization mechanism. In simpler terms, Azure is where your data lives, while Citrix is the software that enables you to connect to the data in that location. Azure still leverages Citrix for accessing the database view.

12. **What is the process of migrating from Blackbaud's self-hosted data centers to Azure?** If you would like to request an evaluation for your site to be relocated to the Azure cloud environments, please review the system and environment requirements and the preparations required for a relocation. If your system meets the relocation criteria, please reach out to your Customer Success Manager and from there they will work with you to discuss scheduling.

13. **What recommendations would Bill make for granting rights to consultants that need admin rights?** It depends on what the consultant is doing for you. With many of Bill's clients, he never has any access to their database at

all, let alone admin access. When he does need access (and he does often need admin access) but it should be temporary: only give the consultant access for as long as they need it, then revoke it. It's easy enough to give the rights back if necessary, again later. And some "consultants" are really "contractors," so consider their role and work accordingly: someone helping with gift entry or reporting doesn't need admin rights, someone who is an interim DBM for you likely does. The bottom line: only give consultants what they need to do the work they're hired to do and then revoke those rights when they leave. "Consultants" don't automatically get admin rights. (This answer applies to those who are "Raiser's Edge consultants," but the same principle applies to IT and fundraising consultants: "consultant" is not a pedestal deserving of admin rights, give rights relevant to the scope of their work, RE training, knowledge, and ability, just like your staff users.)

14. **What recommendations does Bill have about what rights IT staff need?** We really love and appreciate the hard and usually underappreciated work that IT staff do for us – we certainly couldn't do our work without them. However, what Bill said during the webinar about managers is usually true of IT staff: they don't have the training, knowledge, or need to have admin rights just because they're IT. Every account with rights is a security risk, and accounts with full admin rights are the biggest security risks. Bill prefers for IT to know about the backup account in the safe he mentioned for managers and not to have admin rights to RE. In the RE NXT cloud environment, there is usually little to nothing we need IT staff to do for us, nor that they know how to do in RE. If your IT staff is doing real work in RE for you and has the training and knowledge to do it, then they should have rights relevant to the work they're doing. For Bill, "IT" doesn't automatically equate to "admin rights," but it's not a sign of disrespect or distrust; it's just better security.

15. **How does Bill recommend small develop shops (less than 3 people) organize themselves?** With regard to security, a small staff is an example of "one user per security group." Create a group appropriate to each user's training, role, and aptitude. Someone will need to be the supervisor/admin in RE, although certainly wearing the DBM hat as one of several hats, not the only one. Just be careful when doing daily work with that level of rights.

16. **Bill mentioned that only the DBA should have access to security. What is his recommendation for having one additional person with security access as the DBA "backup"? I'm concerned about coverage for emergencies, vacations, etc.** We talked about this later in the webinar, but here is a summary of Bill's recommendation: There should be a DBM backup person. Cross-training is definitely encouraged. But the backup person does not need full supervisor/admin rights every day to do that. If the DBM is going to be out on planned time – vacation, conference, parental leave, scheduled medical procedure, etc. – the backup person's rights can be changed before the DBM leaves and changed back when the DBM returns. For emergency purposes, Bill recommended a backup account with credentials locked in a safe. A backup person should be encouraged, definitely, but that person does not need daily, full admin rights to have the knowledge and ability to step in if needed.

17. **How do I get someone to review my security setup individually and ensure it aligns with best practices? Does Bill do this?** Thanks for asking, he does. A consultant, whether independent like Bill or someone from Blackbaud, should be able to help you with this if you have properly vetted them. Not every "RE consultant" is qualified to do an RE security audit, so check their experience and credentials first.

Session 3: Deep Dive into Blackbaud Raiser's Edge NXT® and Raiser's Edge® Security Options

1. **Where do I go to manage Blackbaud.com security?** As a Blackbaud.com organization administrator, you can manage your organization's Blackbaud.com users from the Admin Console, and then clicking on Users and Admins. Here are more FAQs about managing your Blackbaud.com accounts.

2. **Where do I go to manage database view security?** You will log into database view and navigate to Admin > Security. You can find a more detailed user guide here.

3. **Where do I go to manage web view security?** You will log into web view and navigate to Control Panel > Security. Read more about web view security here.

4. **Is it possible to test out a user's security before granting the privileges to them? What about if you are using single sign-on?** There is no native test functionality, but you can functionally test the account by having another supervisor-level user assign you to the groups and roles that the user would belong to and visualizing these privileges from your own account.

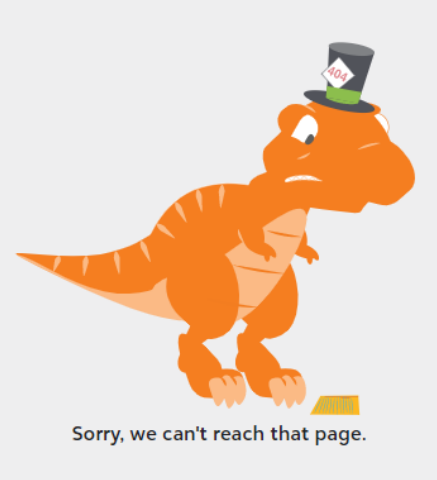
5. **Bill pointed out how to grant access to Web Services but I don't know what that even means. What does Web Services do?** Web Services was used for the former Raiser's Edge mobile apps and is still used for some integrations (RELO, ResearchPoint, etc.). Changes made to Web Services can affect these integrations, so assign privileges to this feature sparingly.

6. **Is it possible to give someone access to events without giving them any access to view gifts?** Yes! This can be accomplished by creating a database view security group that grants Event and Participant privileges, but not does not grant privileges to view, add, or edit gifts.

7. **Can I give access to Lists in web view without giving access to Query in database view?** Yes – their database view security group needs to exclude Query privileges, but the web view fundraising role will include List privileges. This also aligns with Bill's recommendation to be very limited about when you grant export privileges. In web view, you can grant List view rights without granting export rights; with Query, view and export rights are bundled. Bear in mind that a web view user without rights to Query will not be able to open a static query to make a list or save a list as a static query.

8. **Are there any settings in the web view security that will override any security settings in the database view?** There are no web view security settings that will affect a user's experience in the database view. There are some web view security settings that might seem to "override" or "contradict" database view security settings, but they are intended instead to think of and treat the web view functionality as similar *but different* functionality with their own security settings, not "overriding" settings. See the "Exceptions" slide on this topic in Session 2 of the series.

9. **How do users know if they don't have access to something in web view or database view?** In database view, the module or record type that the user cannot view is hidden, so they cannot even view areas of the database to which they have not been granted access. In web view, this the case for features (such as Email or Lists – if you are not given access to these features, the navigation menu items do not appear at all). In a few cases, such as a when a user has access to web view reports but not to view gift records, they see this warning if they attempt to access a record type not available to them:



10. **How do you set rights for moving gifts from one constituent to another in web view?** If a user can edit a gift in database view, they can edit the gift's constituent (or move it from one constituent record to another) in web view.

11. **How extensive is the Security by Fund option? Does it affect fund selection during gift entry?** Yes, if a user does not have access to view a fund in Fund by Security, it will not be available during gift entry.

12. **What is the difference between a solution admin, environment admin, and organization admin? How can I tell who they are?** A solution admin has full access to a single solution, such as Raiser's Edge NXT. An environment admin is an admin for multiple solutions. You can read more about managing solution and environment admins here. Organization administrators, on the other hand, can manage their organization's profile and blackbaud.com users. You can see who your organization administrators are by following these steps.

13. **What do you recommend we do after a user leaves our organization?** In session #2, Bill recommended that you prefix their user account in database view with "zz", remove all of their groups, and change their password in database view. You may choose to delete the user account, but consider these implications of deleting a user. In sessions 1 and 2 Bill offered a free "handout" on all the steps he recommends to consider when adding and removing a user. A copy of it can be found on his website at https://billconnors.com/resources.

14. **Is there any further training available about Security in Raiser's Edge and Raiser's Edge NXT?** Yes, you can take Raiser's Edge NXT Database Health and Administration (course abstract here) for web view security or Raiser's Edge Effective Database Administration (course abstract here) for database view security. Both courses are included in the *Learn More* and *Learn Everything* subscriptions.