Cybersecurity in Low-Risk Organizations: Understanding Your Risks

February 19, 2019
Using ReadyTalk

Chat to ask questions

All lines are muted

If you lose your Internet connection, reconnect using the link emailed to you.

You can find upcoming and past webinars on the TechSoup website: www.techsoup.org/community/events-webinars

You will receive an email with this presentation, recording, and links

Tweet us @TechSoup and use hashtag #tswebinars
A Global Network
Bridging Tech Solutions and Services for Good

Where are you on the map?
Presenters

Sean Brooks
Director of the Citizen Clinic Center for Long-Term Cybersecurity
UC Berkeley

Sima Thakkar
Senior Manager, Content
TechSoup

Assisting with chat:
Zerreen Kazi, TechSoup

Sean Brooks
Director of the Citizen Clinic Center for Long-Term Cybersecurity
UC Berkeley

Sima Thakkar
Senior Manager, Content
TechSoup

Zerreen Kazi
Marketing Associate
TechSoup
Cybersecurity in Low-Risk Organizations

February 19, 2019

Sean Brooks
1. What is a “low risk” organization?
2. Common cybersecurity threats
3. The guide
   a. Controls
   b. Best Practices
   c. Building a Policy
   d. Implementation
4. Questions
What IS NOT a “Low Risk” Organization?

Consider the following questions:

● Do you believe your organization is actively at risk of a cyberattack?

● Does your work generate controversy, or is it viewed with hostility by government actors, government-backed organizations, or independent malicious actors?

● Are any individuals affiliated with your organization engaged in work or behaviors that might draw the attention of adversaries or malicious actors?

● Do you collect, generate, or otherwise handle sensitive information about a vulnerable population, or of interest to an oppressive government or malicious non-state actor?
What kind of common non-profit conditions create cybersecurity risk?
More than 10,000 Utah Food Bank donors notified of breach

August 31, 2015

Adam Greenberg

Utah Food Bank is notifying more than 10,000 individuals that their personal information – including payment card data – may have been exposed during a possible data security incident involving the donation webpage.

Pro-ISIS hackers hijack 800 US schools’ sites with Saddam Hussein photo, ‘I love Islamic State’ message

SchoolDesk, the Atlanta, Georgia-based web hosting company servicing these sites, confirmed the attack.

By Maximiliano Macau
November 7, 2017 10:31 GMT

Hacked! Crooks are Grabbing Nonprofit Websites and Demanding Ransom

Joy O’Neal, executive director of The Red Barn, received an unexpected telephone call from her brother early one April morning in 2015. He had been out with a friend talking about the Leeds, Ala.-based organization, when they visited the website. It had been hacked and taken over by a terrorist sympathizer group.

The organization was not specifically targeted, according to O’Neal. The server The Red Barn’s site

I LOVE ISIS

Hackers Algeria Opticent 2

Get News | Email Us | Contact Us | TEL: +212(0) 600925157 | Twitter: @Brick_Maillion | Site Map | HTML Validator | RSS Feed

Nonprofit Times

The Leading Business Publication for Nonprofit Management
1. What is a “low risk” organization?
2. Common cybersecurity threats
3. The guide
   a. Controls
   b. Best Practices
   c. Building a Policy
   d. Implementation
4. Questions
Common Threats
Username/Password ("account credentials") reuse

Most common tactic used to facilitate breaches

 Doesn’t require new hacking - just finding or buying already-stolen usernames/passwords
Phishing

“Hello! I am a Nigerian Prince...”

The goal? Share credentials, download malware, etc.

Low tech - but it WORKS!
Data Promiscuity

Not an “attack” - but very, very common.

All orgs have lots of data, easy to let it sprawl - across devices, accounts, cloud drives, etc.

But who do you want seeing HR files? Payroll? Donor lists?
Malware

“Malicious Software”

Take advantage of a known vulnerability in common software to make a device do something it isn’t supposed to.

Older software = more vulnerable

Specific concern: Ransomware
“All attackers are resource constrained”

@dinodaizovi

“All attackers have a boss and a budget”

@philvenables
1. What is a “low risk” organization?
2. Common cybersecurity threats
3. The guide
   a. Controls
   b. Best Practices
   c. Building a Policy
   d. Implementation
4. Questions
The Guide:


What is a cybersecurity “control”? 
Strong Authentication:
- Mitigates: Phishing, Account Takeovers
- Includes: Account monitoring, password managers, and MFA

HTTPS:
- Mitigates: Web-based attacks
- One-time setup, prevents reputational damage from “insecure” flags
- Not optional

Software Updates:
- Mitigates: Malware
- Easy to set once
- Includes: software updates, license renewal
The Cloud:
- Mitigates: Malware, Phishing, Web-Based Attacks, Data Theft, etc.
- “The Cloud” = Someone else’s computer
- Includes ongoing costs, often behavioral shifts
- Offloads many difficult security issues to highly-qualified service providers

Data Security:
- Mitigates: Data Theft and Loss
- Includes end-to-end encryption, file and disk-based encryption, access management
- Some risks (lost keys = lost data) - but an important step to preventing data loss
Should you spend the time, money, and energy to deploy all controls listed in this guide?
Using the Guide

1. **Read** through the controls (in Section 2) and best practices (in Section 3)

2. **Select** the level of controls appropriate for your organization, and use those controls and best practices described in Section 3 to build your security policy.

3. **Implement** security controls within your organization based upon your new security policy.

You can jump between the control descriptions in Section 2, the policy assistance in Appendix A, and the implementation guidance in Appendix B by using the links below each headline.
## Using the Guide

### Strong Authentication

Set policy for this control here.

Additional implementation guidance can be found here.

<table>
<thead>
<tr>
<th><strong>Baseline:</strong> Require multi-factor authentication for all organization-managed accounts. Turn on login alerts where offered.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>What time and technical sophistication is required to set up this control?</strong></td>
</tr>
<tr>
<td>Low Sophistication</td>
</tr>
<tr>
<td>Less than 1 hour</td>
</tr>
<tr>
<td>Baseline +: Require multi-factor authentication for all organization-managed accounts. Require the use of password managers. Turn on account monitoring where offered.</td>
</tr>
<tr>
<td>Moderate Sophistication</td>
</tr>
<tr>
<td>Less than 1 day</td>
</tr>
</tbody>
</table>

**NOTE:** As a general rule, do not recycle the same password across multiple accounts. When choosing a password, pick something unique, and make it long. You should focus more on length than on adding in hard-to-remember characters or complex upper/lower case combinations. The use of a "passphrase" - a string of at least 4 unrelated words - instead of a password is encouraged.

### Multi-factor Authentication

Multi-factor authentication (MFA) is a tool that offers additional security online accounts by requiring an extra layer of user verification. When MFA is enabled for an account, a user must not only enter a username and password, but they must also verify additional "factors" – like a code texted to their phone – that prove they are the true owner of the account. When accounts have MFA enabled, attackers who attempt to log in using stolen usernames and passwords will have a much harder
## Using the Guide

### Strong Authentication

Set policy for this control here.

Additional implementation guidance can be found here.

| Baseline: Require multi-factor authentication for all organization-managed accounts. Turn on login alerts where offered. |
|---|---|---|
| **What time and technical sophistication is required to set up this control?** | **Who enables this control?** | **What risks does this control mitigate?** |
| Low Sophistication Less than 1 hour | System administrators and individuals set it up | Phishing/Account Takeovers |

**Baseline +**: Require multi-factor authentication for all organization-managed accounts. Require the use of password managers. Turn on account monitoring where offered.

| Moderate Sophistication Less than 1 day | System administrators and individuals set it up | Phishing/Account Takeovers |

**NOTE**: As a general rule, do not recycle the same password across multiple accounts. When choosing a password, pick something unique, and make it long. You should focus more on length than on adding in hard-to-remember characters or complex upper/lower case combinations. The use of a “passphrase” - a string of at least 4 unrelated words - instead of a password is encouraged.

### Multi-factor Authentication

Multi-factor authentication (MFA) is a tool that offers additional security online accounts by requiring an extra layer of user verification. When MFA is enabled for an account, a user must not only enter a username and password, but they must also verify additional “factors” – like a code texted to their phone – that prove they are the true owner of the account. When accounts have MFA enabled, attackers who attempt to log in using stolen usernames and passwords will have a much harder
Using the Guide

**Strong Authentication**

Set policy for this control here.

Additional implementation guidance can be found here.

<table>
<thead>
<tr>
<th>What time and technical sophistication is required to set up this control?</th>
<th>Who enables this control?</th>
<th>What risks does this control mitigate?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low Sophistication</td>
<td>System administrators and individuals set it up</td>
<td>Phishing/Account Takeovers</td>
</tr>
<tr>
<td>Less than 1 hour</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Baseline +**: Require multi-factor authentication for all organization-managed accounts. Require the use of password managers. Turn on account monitoring where offered.

| Moderate Sophistication | System administrators and individuals set it up | Phishing/Account Takeovers |
| Less than 1 day | | |

**NOTE**: As a general rule, do not recycle the same password across multiple accounts. When choosing a password, pick something unique, and make it long. You should focus more on length than on adding in hard-to-remember characters or complex upper/lower case combinations. The use of a “passphrase” - a string of at least 4 unrelated words - instead of a password is encouraged.

**Multi-factor Authentication**

Multi-factor authentication (MFA) is a tool that offers additional security online accounts by requiring an extra layer of user verification. When MFA is enabled for an account, a user must not only enter a username and password, but they must also verify additional “factors” - like a code texted to their phone - that prove they are the true owner of the account. When accounts have MFA enabled, attackers who attempt to log in using stolen usernames and passwords will have a much harder time.
### Strong Authentication

Set policy for this control here.
Additional implementation guidance can be found here.

<table>
<thead>
<tr>
<th>Baseline: Require multi-factor authentication for all organization-managed accounts. Turn on login alerts where offered.</th>
<th>What time and technical sophistication is required to set up this control?</th>
<th>Who enables this control?</th>
<th>What risks does this control mitigate?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low Sophistication</td>
<td>Less than 1 hour</td>
<td>System administrators and individuals set it up</td>
<td>Phishing/Account Takeovers</td>
</tr>
</tbody>
</table>

**Baseline +**: Require multi-factor authentication for all organization-managed accounts. Require the use of password managers. Turn on account monitoring where offered.

| Moderate Sophistication | Less than 1 day | System administrators and individuals set it up | Phishing/Account Takeovers |

**NOTE**: As a general rule, do not recycle the same password across multiple accounts. When choosing a password, pick something unique, and make it long. You should focus more on length than on adding in hard-to-remember characters or complex upper/lower case combinations. The use of a "passphrase" - a string of at least 4 unrelated words - instead of a password is encouraged.

### Multi-factor Authentication

Multi-factor authentication (MFA) is a tool that offers additional security online accounts by requiring an extra layer of user verification. When MFA is enabled for an account, a user must not only enter a username and password, but they must also verify additional "factors" – like a code texted to their phone – that prove they are the true owner of the account. When accounts have MFA enabled, attackers who attempt to log in using stolen usernames and passwords will have a much harder
Using the Guide

**Strong Authentication**

Set policy for this control here.

Additional implementation guidance can be found here.

**Baseline:** Require multi-factor authentication for all organization-managed accounts. Turn on login alerts where offered.

- **Low Sophistication**
  - Less than 1 hour
  - System administrators and individuals set it up
  - Phishing/Account Takeovers

- **Baseline +:** Require multi-factor authentication for all organization-managed accounts. Require the use of password managers. Turn on account monitoring where offered.
  - Moderate Sophistication
  - Less than 1 day
  - System administrators and individuals set it up
  - Phishing/Account Takeovers

NOTE: As a general rule, do not recycle the same password across multiple accounts. When choosing a password, pick something unique, and make it long. You should focus more on length than on adding in hard-to-remember characters or complex upper/lower case combinations. The use of a "passphrase" - a string of at least 4 unrelated words - instead of a password is encouraged.

**Multi-factor Authentication**

Multi-factor authentication (MFA) is a tool that offers additional security online accounts by requiring an extra layer of user verification. When MFA is enabled for an account, a user must not only enter a username and password, but they must also verify additional "factors" – like a code texted to their phone – that prove they are the true owner of the account. When accounts have MFA enabled, attackers who attempt to log in using stolen usernames and passwords will have a much harder time accessing them.
Using the Guide

**Strong Authentication**

Set policy for this control here.

Additional implementation guidance can be found here.

**Policy Selection:**
- **Baseline:** Require multi-factor authentication for all organization-managed accounts. Turn on login alerts where offered.
- **Baseline +:** Require multi-factor authentication for all organization-managed accounts. Require the use of password managers. Turn on account monitoring where offered.
- **No Policy**

**Policy Details:** Person(s) responsible for implementing this policy:

(Name)

This individual is responsible for ensuring multifactor authentication is enabled on all critical accounts, and will serve as a resource for other staff who need assistance with MFA setup or recovery. This individual is also responsible for ensuring that backup MFA codes for organization-owned accounts are stored in a safe, secure place - such as an external USB drive in a locked cabinet.

What accounts are considered critical?

<table>
<thead>
<tr>
<th>Account</th>
<th>MFA Forced?</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Account Name)</td>
<td>(yes/no)</td>
</tr>
</tbody>
</table>

**NOTE:** As a general rule, do not recycle the same password across multiple accounts. When choosing something unique, and make it long. You should focus more on length than on adding in hard-to-guess or complex upper/lower case combinations. The use of a "passphrase" - a string of at least 4 unique words - or a password is encouraged.

**Multi-factor Authentication**

Multi-factor authentication (MFA) is a tool that offers additional security online accounts by requiring verification. When MFA is enabled for an account, a user must not only enter a username and password, but also verify additional "factors" - like a code texted to their phone - that prove they are the true owner of the account. If accounts have MFA enabled, attackers who attempt to log in using stolen usernames and passwords are far less likely to succeed.

**Account Inventory**

What online accounts does your organization consider important to your mission? This could include email, social media, financial, online storage, etc.:

<table>
<thead>
<tr>
<th>Account</th>
<th>Purpose</th>
<th>Impact on organization if access is lost</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>(High, Medium, Low)</td>
</tr>
</tbody>
</table>

What staff members have access to which account? Include if they "own" the account and are responsible for its activity.

<table>
<thead>
<tr>
<th>Account</th>
<th>Staff</th>
<th>MFA Enabled?</th>
</tr>
</thead>
</table>
Using the Guide

**Strong Authentication**

Set policy for this control here.

Additional implementation guidance can be found here.

**Policy Selection:**
- **Baseline:** Require multi-factor authentication for all organization-managed accounts. Turn on login alerts where offered.
- **Baseline +:** Require multi-factor authentication for all organization-managed accounts. Require the use of password managers. Turn on account monitoring where offered.
- **No Policy**

**Policy Details:** Person(s) responsible for implementing this policy:

**What time and technical sophistication is required to set up this control?**

- **Low Sophistication**
  - Less than 1 hour
- **Moderate Sophistication**
  - Less than 1 day

**Who enables this control?**

- System administrators and individuals set it up
- Phishing Takeover

**What notifies control is enabled?**

- Phishing Takeover

**What accounts are considered critical?**

<table>
<thead>
<tr>
<th>Account</th>
<th>MFA Forced?</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Account Name)</td>
<td>(yes/no)</td>
</tr>
</tbody>
</table>

**Multi-factor Authentication**

Multi-factor authentication (MFA) is a tool that offers additional security online accounts by requiring verification. When MFA is enabled for an account, a user must not only enter a username and password, but verify additional "factors" – like a code texted to their phone – that prove they are the true owner of the account. Having accounts enabled, attackers who attempt to log in using stolen usernames and passwords.

**The below chart is a basic way to determine which accounts should be considered "critical" to an organization. By rating the accounts and mapping them to the staff with access, organization can determine which staff members need to prioritize enabling strong authentication.**

<table>
<thead>
<tr>
<th>Account Inventory</th>
</tr>
</thead>
<tbody>
<tr>
<td>What online accounts does your organization use in order to do business, or account you own, such as email, social media, financial, online storage, etc.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Account</th>
<th>Purpose</th>
<th>Impact on organization if access is lost</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Account Name)</td>
<td>(High, Medium, Low)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Account</th>
<th>Staff</th>
<th>MFA Enabled?</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Account Name)</td>
<td>(Staff)</td>
<td>(MFA Enabled?)</td>
</tr>
</tbody>
</table>
Best Practices

Guide also includes template policies or best practices on...

- “Fleet” Management
- Travel Policies
- Incident Response
- Social Media Use
- Payment Card Security

These can be used, edited, or expanded as needed based on what suits your organization’s needs and concerns.
Thank you.

If you have any additional questions, you are welcome to contact me: swb@berkeley.edu

Special thanks to the MacArthur Foundation for supporting this project.

Thank you to TechSoup.
Share and Learn

Chat in one thing that you learned in today’s webinar.

Please complete our post-event survey. Your feedback really helps.

Follow TechSoup on social media (FB, Instagram, Twitter)

Visit the TechSoup Blog at blog.techsoup.org
Join us for our upcoming webinars.

2/21
Maximize Spring Fundraising and Maintain Donors Through 2020

2/28
How to Drive Social Media Engagement with Nonprofit Storytelling

3/05
QuickBooks Premier for New Desktop Users

3/11
How to Be a Data-Driven Organization with Power BI

Archived Webinars:
www.techsoup.org/community-events
TechSoup Courses

Access on-demand content built specifically for nonprofit and library staff.

Topics include:
• Google Analytics
• Facebook Advertising for Nonprofits
• Design
• Tech Training
• Technology Planning
• Microsoft Office 365
• And more

https://techsoup.course.tc/catalog/

TechSoup Services

From basic help-desk-style case support, to more complex managed IT and cloud implementation solutions, TechSoup can help.

Services include:
• Help Desk
• Managed IT
• Cloud Implementation
• Office365 Support

https://www.techsoup.org/services

FY19WEB10 - 10% off a TechSoup Course of Your Choice
Thank you to our webinar sponsor!

Please complete the post-event survey that will pop up once you close this window.