



Cyberattack preparation: A basics refresher

Presenter: Chris Ellingwood

Learning objectives



- ▲ Better understand how and why NFPs must be more proactive in managing cybersecurity threats and events.
- ▲ Learn five basic things you can do to enhance your cyber controls and reduce the risk of a cyber event.

Cybersecurity in NFPs

- Historically, cybersecurity was a nice to have – now it's essential
- Microsoft's Digital Security Unit says NFPs are the most common target for cyber criminals – limited resources and valuable data
- Majority of NFPs don't believe hackers want their data – that they're under the radar

Cybersecurity is expensive. The typical for-profit corporation spends \$8,000 per employee per year on technology; charities typically spend \$3,000, according to research conducted by the Berkeley center. Of that amount, a nonprofit might spend only 5 to 10 percent on cybersecurity — or about \$225 per employee per year. Most experts say that's not nearly enough.

Microsoft



Verizon



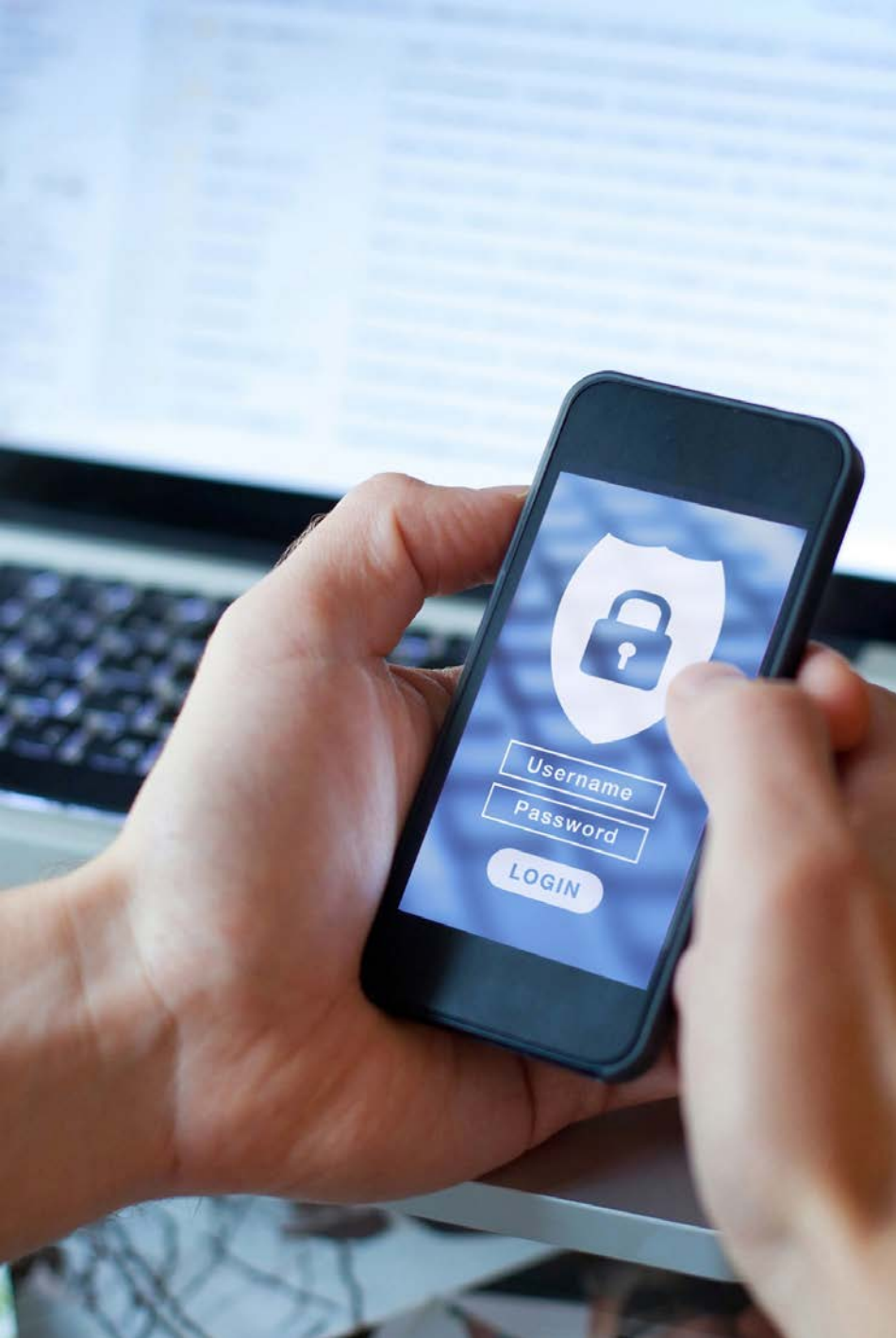
Polling question

How much per employee does the private sector spend on cybersecurity?

- a) \$ 300
- b) \$ 2,300
- c) \$ 3,500
- d) \$ 5,000



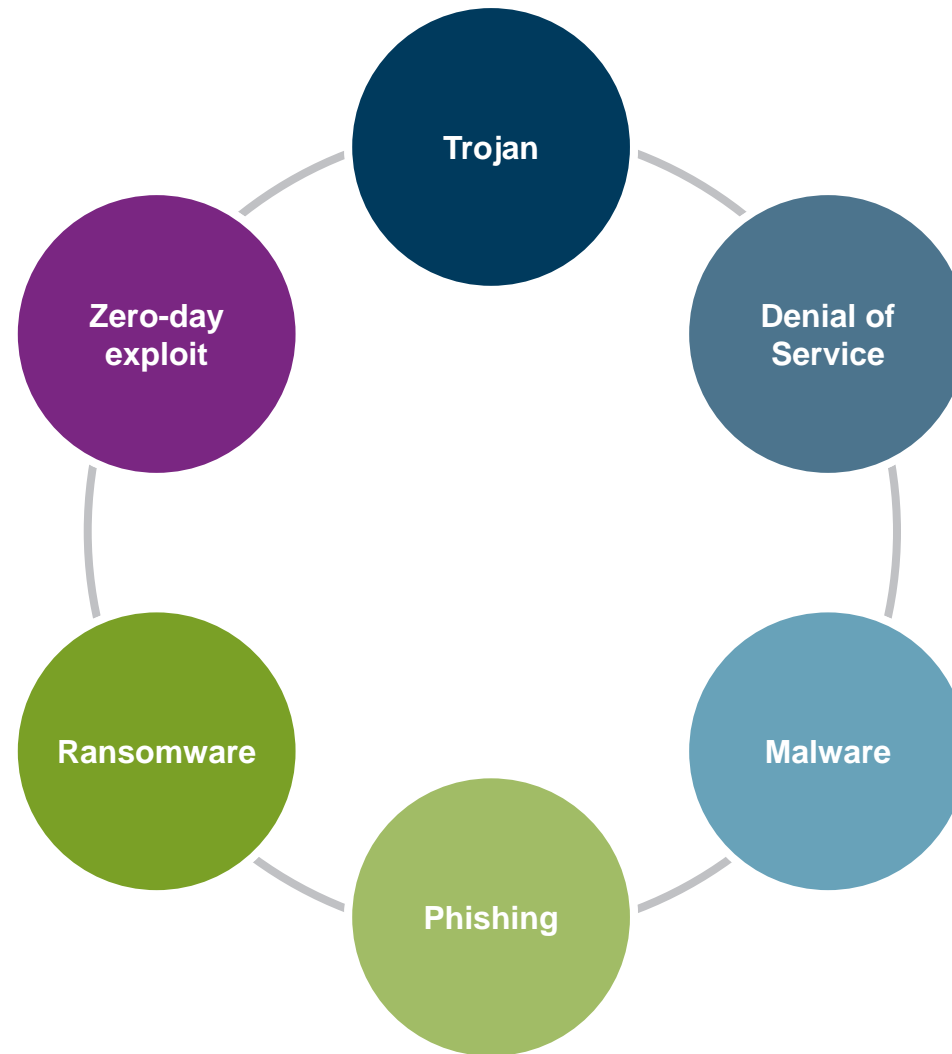
Cybersecurity should be part of your organizational culture and strategy



- ▲ **1** Just like you make sure your house or office is secure, same should go for IT systems.
- ▲ **2** Identify a framework – without a framework or strategy, you're treating security haphazardly.
- ▲ **3** IT strategy determines how you protect systems and data (on premise vs. in the cloud).
- ▲ **4** Technology changes, so should the plan to secure it.
- ▲ **5** Integrating security into your business planning makes it become part of the culture. It also avoids big surprises.

You hear “cyberattack” – but what does that mean?

Types of attacks



Polling question

What is the most effective form of a cyberattack?

- a) Malware
- b) Denial of Service
- c) Ransomware
- d) Phishing



Impacts of a cyberattack



Cost



Reputation



Data loss



Regulatory failure

Cybersecurity and NFPs

CNN politics The Biden Presidency Facts First US Elections Audio Live TV Log In

FBI director blames Iran for 'despicable' attempted cyberattack on Boston Children's Hospital

By Sean Lyngaas, CNN
Updated 9:57 AM ET, Wed June 1, 2022

Statement: Cyberattack affecting International Committee of the Red Cross (ICRC)

CyberPeace Institute is committed to working with humanitarian NGOs to call for collective action against cyber threats and attacks.

A cyberattack against computer servers hosting information of the International Committee of the Red Cross (ICRC), announced in their [news release](#) on Wednesday, shows a shocking disregard for lives and suffering and the vital mission of this humanitarian organization. Such cyberattacks against organizations whose role is to help the most vulnerable must stop.

The NonProfit Times

The Hack Of Blackbaud: Damage Is Still Being Assessed

Donors to the Vermont Food Bank didn't rain email and phone calls down upon the organization when they found out data in the charity's...

Aug 6, 2020



PortSwigger

Chicago Public Schools data breach blamed on third-party ransomware attack

Cybercrooks compromised server containing student course ... The cyber-attack against Battelle for Kids, an Ohio-based non-profit with a...

1 week ago



Spectrum News

Scammers are taking advantage of Ukraine crisis to pose as ...

"Even if it's a charitable solicitation forwarded to you by someone you trust, it doesn't mean it's legit. They could have been hacked or fallen..."

Mar 4, 2022



Cybercriminals are charging anything from \$500 to \$7,000 for access to organizations' computers and morals appear to have gone out the window, as Doctors Without Borders and a U.S. hospital are targeted.

Forbes

CYBERSECURITY • EDITORS' PICK

Hackers Sell Backdoors Into A \$2 Billion Nonprofit, A Californian Hospital, And Michigan Government

BRIEFING ROOM

Statement by President Biden on our Nation's Cybersecurity

MARCH 21, 2022 • STATEMENTS AND RELEASES

This is a critical moment to accelerate our work to improve domestic cybersecurity and bolster our national resilience. I have previously warned about the potential that Russia could conduct malicious cyber activity against the United States, including as a response to the unprecedented economic costs we've imposed on Russia alongside our allies and partners. It's part of Russia's playbook. Today, my Administration is reiterating those warnings based on evolving intelligence that the Russian Government is exploring options for potential cyberattacks.

If you have not already done so, **I urge our private sector partners to harden your cyber defenses immediately by implementing the best practices we have developed together over the last year.** You have the power, the capacity, and the responsibility to strengthen the cybersecurity and resilience of the critical services and technologies on which Americans rely. We need everyone to do their part to meet one of the defining threats of our time — your vigilance and urgency today can prevent or mitigate attacks tomorrow.





What you can do

- ▲ Hackers are generally lazy and rely on unsuspecting people to do the work for them (click here now!).
- ▲ Before you worry about being hacked – there are five easy things you can do to dramatically help reduce the likelihood of an attack.
- ▲ Let's revisit the basics...

Cyberattack preparation

Access controls



▲ The use of passwords is changing

- Puts the onus on the security team, not the user
- Complexity is key (numbers, symbols, caps/lower case letter mix)
- 10+ characters – consider the use of a passphrase
- The need to change passwords frequently is no longer best practice

With some exceptions...

Cyberattack preparation

Access controls



- ▲ The use of multi-factor authentication (MFA)
 - Tokens, Microsoft/Google Authenticator, texts to codes, etc.
 - If that is enabled and used, no need to require password changes unless there is a risk that a password was compromised
- ▲ Service accounts
 - Longer, more complex passwords than standard users
 - Password is stored in secure spot or password vault. Only changed when there is a change in IT personnel or a risk it was compromised
- ▲ Administrator accounts
 - Longer, more complex passwords
 - Require MFA
 - Users should have a day-to-day account and only use the admin account when needed



56% of nonprofits don't require multi-factor authentication (MFA) to log into online accounts.

Polling question

How much less likely are you to be a victim of a cyberattack if you have MFA enabled for system access?

- a) 29%
- b) 49%
- c) 75%
- d) 99%



Cyberattack preparation

Patching

- ▲ Patching is a critical function for IT teams
- ▲ Ensure you have a complete inventory of hardware/software
- ▲ Centrally manage workstations and servers
- ▲ Smaller NFPs may have a challenge with this
 - Remote workforce
 - Employees/volunteers/board members often using own devices
- ▲ Run regular vulnerability scans of systems
- ▲ Patch Tuesday – everyone's favorite day



60% of successful data breaches in 2019 were associated with an unpatched system

More than 70% of nonprofits have not run even one vulnerability assessment

Cyberattack preparation

Logging

Knowing what's going on is half the battle

- ▲ Logging of privileged accounts helps detect changes
- ▲ Logging can coincide with alerting and notify you of possible security events
- ▲ Logging activity is important for triage and troubleshooting post-events
- ▲ Properly setting up logging can be challenging
- ▲ Smaller organizations may seek to outsource
- ▲ Being proactive is key



Only 26% of nonprofits
actively monitor their
network environments.

Cyberattack preparation

Test backups and more



- ▲ Backups can come to the rescue after an attack
- ▲ Testing the functionality of backups and restoration is critical
- ▲ Full system failovers should be conducted
- ▲ Backups should be scanned for ransomware/malware
- ▲ Just as important to back up hardware configurations

Cyberattack preparation

Incident Management Plan

- ▲ Understand what defines an incident
- ▲ Helps provide direction
- ▲ Contact information of those who should be involved
- ▲ Documents standards for recovery time
- ▲ Conduct training exercises so that management knows what to do – think like a fire drill
- ▲ Update frequently to address changes in the environment



Only 20% of nonprofits
have a policy in place to
address cyberattacks.

Cyberattack preparation

Training – phishing attacks

- ▲ Phishing is most common way hackers get ransomware and malware installed
- ▲ It only takes one click
- ▲ Frequent training is key – questioning emails becomes habit/culture
- ▲ You are not hurting feelings by testing
- ▲ Other controls should also be in place
 - Prevent users from being able to install software (local administrator rights)
 - Allow and deny list for software
 - Disable macros in email




59% of nonprofits
do not provide any
cybersecurity training to
staff on a regular basis.

Phishing – a note for charitable organizations

Beware of the fake campaign

- ▲ Highly recommend that you have tools in place, such as Google alerts, for your organization
 - We see this with tragedy after tragedy – hackers phishing for personal information and money as a fake (or pretending to be a real) charitable organization that is raising funds for a cause.
- ▲ Should also have a communication plan for donors
- ▲ Treat your donor lists like you would a credit card number


 MakeUseOf

Is It Safe to Donate Money to Ukraine Online? How to Avoid Charity Scams

The Red Cross, for example, has warned people to be wary of scams on its ... This is not only safer but will also ensure that your money is...

5 days ago



 NBC News

Donors warned to be cautious of scams following mass shootings

With the Texas attorney general and state lawmakers warning about fraudulent fundraising in the wake of the school shooting in Uvalde,...

53 mins ago



Final thoughts

The basics go a long way

1

Sticking to the basics helps your organization

2

Understand your organization and the risk that is present

3

Leverage third-party support and expertise where you are able

4

Leverage third-party support and expertise where you are able



Thank you

Chris Ellingwood

CISA | Senior Manager
cellingwood@berrydunn.com
802.310.0361

Josh Clark

CISA | Manager



berrydunn.com