



# Non Profit IT Security

**What is it, why should I care, and what can I do?**

Presented by the Hartford Foundation for Public Giving  
Nonprofit Support Program

November 20, 2019

# Your Workshop Leader

**Linda Widdop**

TECH IMPACT

---

Director of Nonprofit Solutions

[linda@techimpact.org](mailto:linda@techimpact.org)



# Tech Impact: Your Technology Resource



Request Free  
Consult

Home Services ▾ Programs ▾ Resources ▾ Conference ▾ About ▾ Contact 🔍

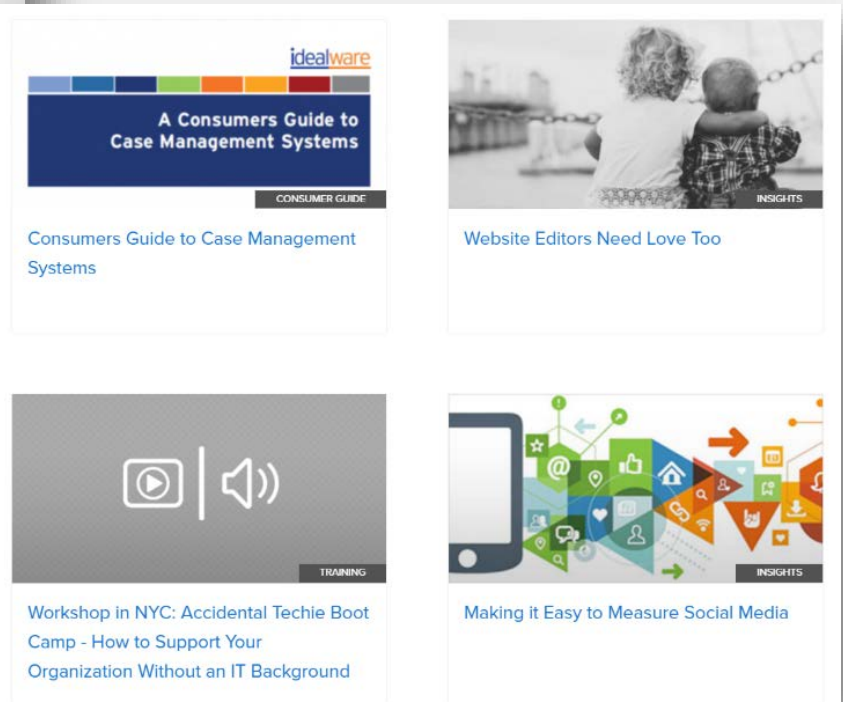
## Sensible Technology Solutions Exclusively for Nonprofits

### Tech Impact Nonprofit Technology Services

Tech Impact is a leading provider of nonprofit technology services and solutions. We are the place nonprofits can call to make sense of anything from large-scale technology projects, to technology maintenance and support. With more than a decade of experience working with a diverse group of nonprofits, we have the expertise and experience to deliver a wide range of services and support.

Request Free Consult

[www.techimpact.org](http://www.techimpact.org)  
[www.idealware.org](http://www.idealware.org)



# Tech Impact Services

Our continuum of services moves our community forward



education



workforce  
development



capacity  
building

## Free and Paid Online Training for Nonprofits and our Community

**CXWorks**  
call center training

**ITWorks**  
IT support training

**Stackable  
Credentials**  
continuous training for  
alumni

**PunchCode**  
programming Bootcamp

Managed Services

Cloud Identity & Device  
Management

Data Analysis &  
Visualization

Machine Learning &  
Artificial Intelligence

Cloud Migration

Security Monitoring &  
Assessment

Application Selection &  
Support

Community Integrated  
Design

**Productive**

**Secure**

**Informed**

**Innovative**

# Agenda

Overview of Cyber Security

Pieces of Security

Activity

How ED's Should Think About Security

Assessing Your Risk

Best Practices for Cyber Security

Configuration & Support

Costs of a Data Breach

Q&A / Conclusion





# 1

# Overview & Examples



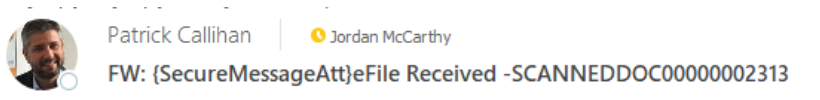
# What Is Cyber Security?

Cybersecurity refers to preventative methods used to protect information from being stolen, compromised or attacked.

This environment includes users, networks, devices, software, processes, information (in storage or transit), applications, services, and systems that can be connected directly or indirectly to networks.



# Example - Common Phishing Scams

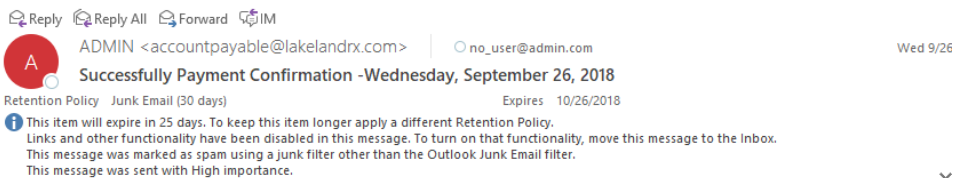


Looks **suspicious**.

**From:** \_Shar~File <[Liz@primaconstruction.net](mailto:Liz@primaconstruction.net)>  
**Sent:** Monday, May 14, 2018 10:50 AM  
**Subject:** {SecureMessageAtt}eFile Received -SCANNEDDOC00000002313

File Type - PDF : Size -710 KB

View your message Here [DOWNLOAD](#) To View Attachment, Sign in using your receiving email.



You have a secure document via One Drive pending your signature.

View File <[https://1drv.ms/w/s!Att1\\_hAx49EmgzK7\\_DUwhFoi3NvM](https://1drv.ms/w/s!Att1_hAx49EmgzK7_DUwhFoi3NvM)>

Your document is ready for download.

If you are having trouble signing the document, please visit the Help with Signing page on our Support Center.

<[http://www.avg.com/email-signature?utm\\_medium=email&utm\\_source=link&utm\\_campaign=sig-email&utm\\_content=webmail](http://www.avg.com/email-signature?utm_medium=email&utm_source=link&utm_campaign=sig-email&utm_content=webmail)>

Virus-free. [www.avg.com](http://www.avg.com) <[https://1drv.ms/w/s!Att1\\_hAx49EmgzK7\\_DUwhFoi3NvM](https://1drv.ms/w/s!Att1_hAx49EmgzK7_DUwhFoi3NvM)>

## Update status



Updates are available.

- 2018-05 Cumulative Update for Windows 10 Version 1709 for x64-based Systems (KB4103727)

**Status:** Awaiting restart

- 2018-05 Security Update for Adobe Flash Player for Windows 10 Version 1709 for x64-based Systems (KB4103729)

**Status:** Awaiting restart

[View installed update history](#)

Your device is at risk because it's out of date and missing important security and quality updates. Let's get you back on track so Windows can run more securely. Select this button to get going:

Restart now





## Example – Voicemail Attachment

 Reply  Reply All  Forward  IM




VOICEMAIL <pendingvoicemail\_noreply@simermeyer.onmicrosoft.com>

Scheduling

**Wmv received from (8328990209) (8328990209)**

Retention Policy Junk Email (30 days)

Expires 10/26/2018

 This item will expire in 25 days. To keep this item longer apply a different Retention Policy.  
Links and other functionality have been disabled in this message. To turn on that functionality, move this message to the Inbox.  
This message was marked as spam using a junk filter other than the Outlook Junk Email filter.  
We converted this message into plain text format.

Hi [scheduling@techimpact.org](mailto:scheduling@techimpact.org)

You Have a New Voice Message


From: WIRELESS CALLER (317) 696-0438

Received: Wednesday, August 26, 2018 at 03:20 PM

Length: 00:13

To: [scheduling@techimpact.org](mailto:scheduling@techimpact.org)

Play Voicemail <[<https://tinyurl.com/y8mqcdyp??==++%4b%4b%4b%>](https://tinyurl.com/y8mqcdyp??==++%4b%4b%4b%)>

Microsoft VMS 

Please consider the environment before printing this.

# Example – Action Needed on Account

Action Needed: Take action to keep getting emails



Sean from Microsoft <sean@office-notices.com>

To Linda Widdop



You forwarded this message on 9/3/2019 9:56 AM.

If there are problems with how this message is displayed, click here to view it in a web browser.

## Your Office 365 is flagged for login activity

Our records indicate that it has been more than 15 days since you logged into Office 365 through the web. For security reasons, this account will be locked due to inactivity.

To keep using your email, you must confirm that [Linda@techimpact.org](mailto:Linda@techimpact.org) is still in use by using the activation button below.

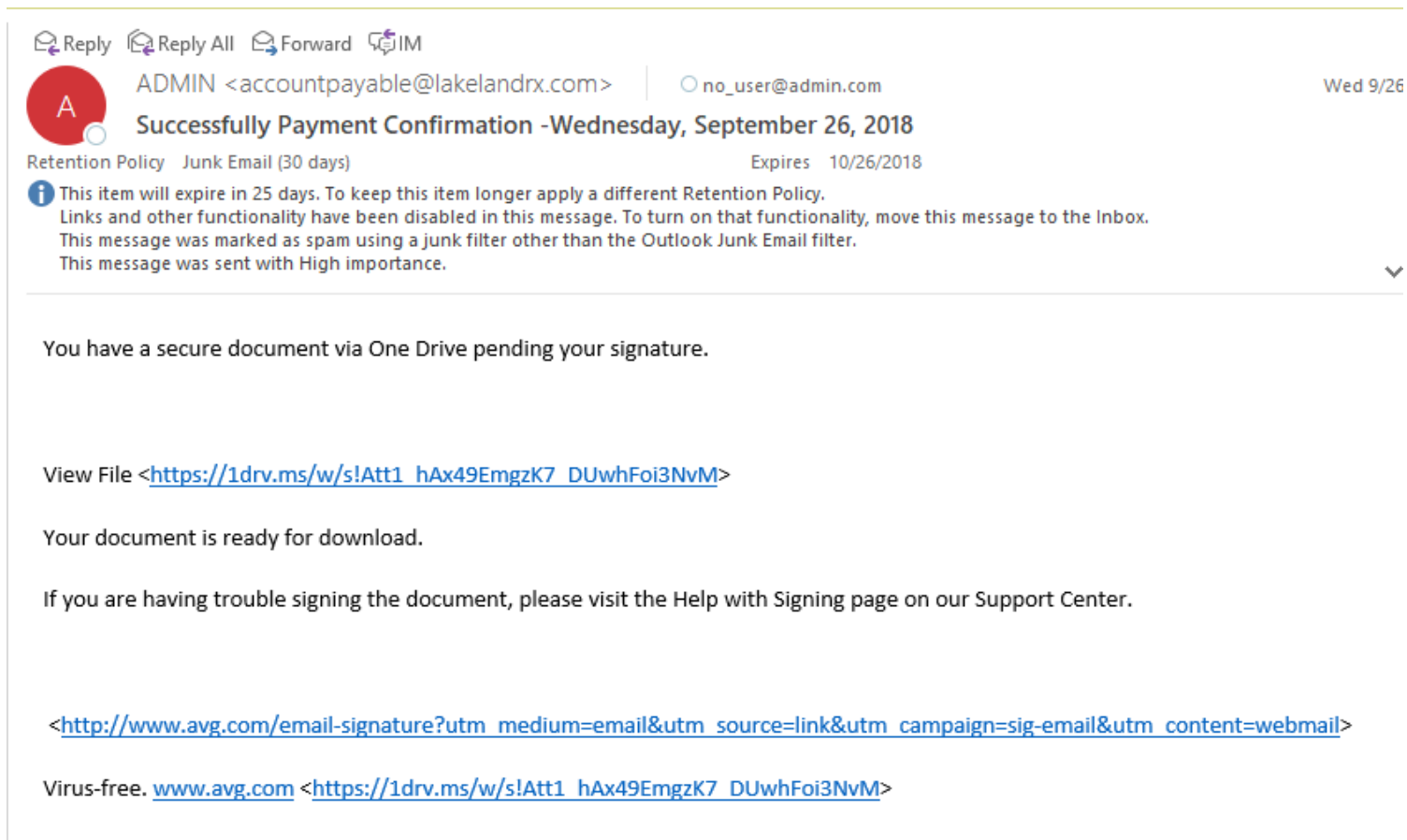
[Mark As Active](#)

You should use this button only if you want this account to remain active. If you no longer work at the company, please ignore this email.

Thanks for using Office 365!

2019 © Microsoft. All rights reserved

# Example – Payment Confirmation



# Example – Mailbox Spam Filter

RE: You have 6 Incoming Messages

MICROSOFT

Hi [info@twoten.org](mailto:info@twoten.org)

Attention: [info@twoten.org](mailto:info@twoten.org) We Detected you have [6] undelivered incoming emails on 21-Aug-2018, this is because your account storage is full, your action is required for them to be delivered

Kindly follow the self service instructions below to rectify the issue:

[Release Pending messages to inbox.](#)

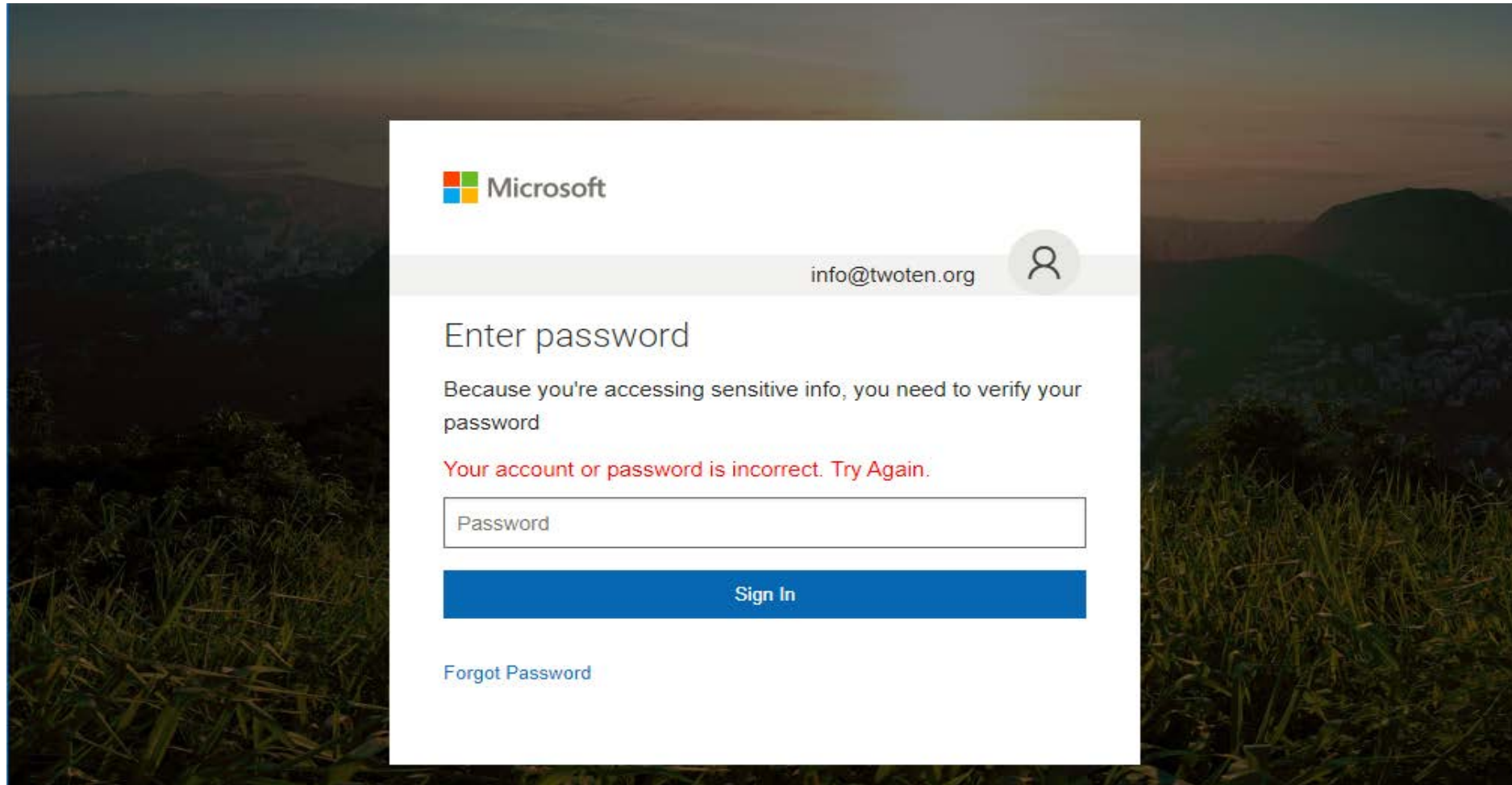
Source: [info@twoten.org](mailto:info@twoten.org) Office365 Support

Microsoft respects your privacy. Please read our online [Privacy Statement](#).

Microsoft Corporation, One Microsoft Way, Redmond, WA 98052

Send us [feedback](#).

## Example – Password Failure



The image shows a Microsoft login interface overlaid on a dark, scenic background of a field at dusk. The login box is white and contains the Microsoft logo in the top left. In the top right, the email address 'info@twoten.org' is displayed next to a user icon. The main heading is 'Enter password'. Below it, a message states: 'Because you're accessing sensitive info, you need to verify your password'. A red error message follows: 'Your account or password is incorrect. Try Again.' Below the error is a password input field with the placeholder text 'Password'. A blue 'Sign In' button is positioned below the input field. At the bottom left of the login box, there is a link that says 'Forgot Password'.

Microsoft

info@twoten.org

Enter password

Because you're accessing sensitive info, you need to verify your password

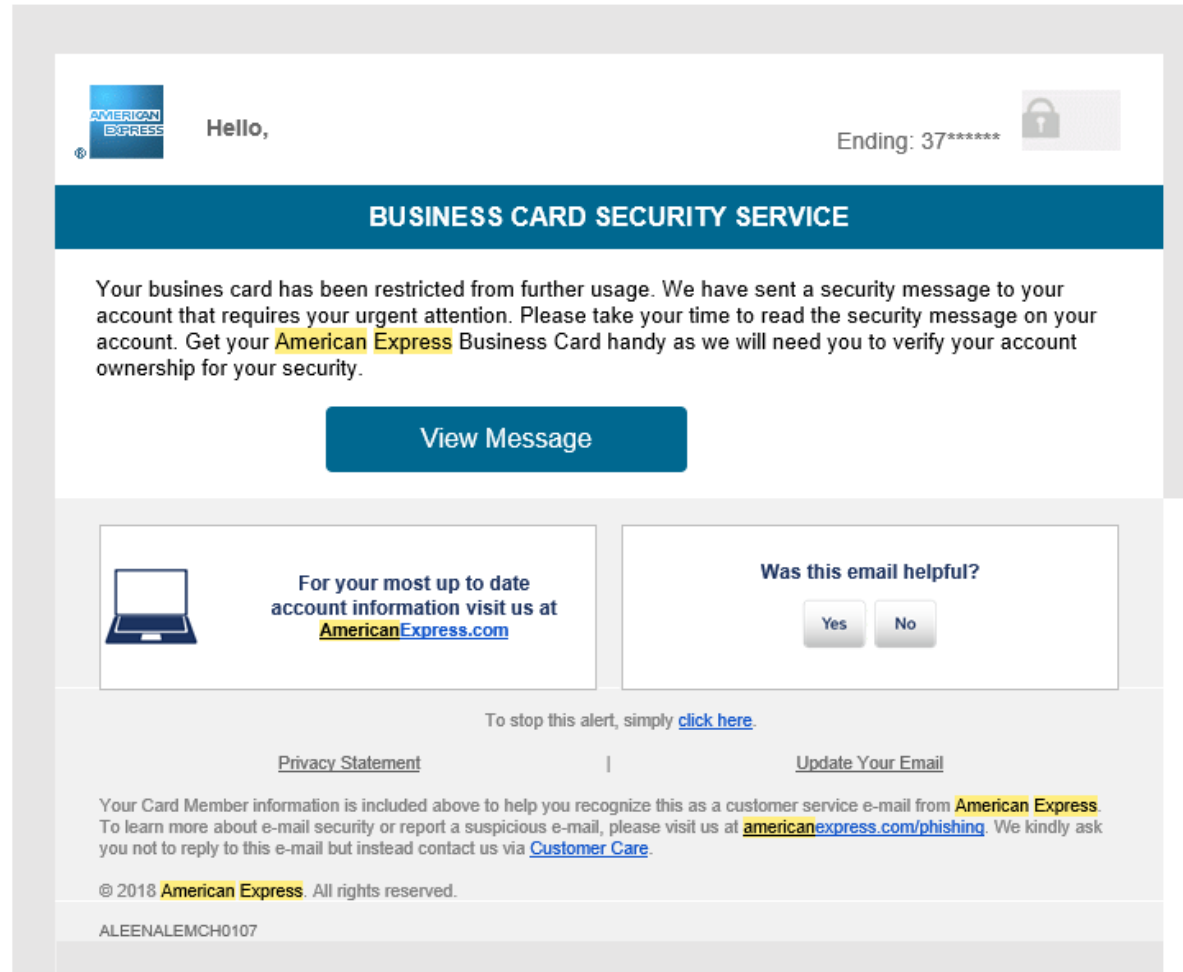
Your account or password is incorrect. Try Again.

Password

Sign In

[Forgot Password](#)

# Example – Credit Card Security Service





# Making the News

the two-way


BREAKING NEWS FROM NPR

AMERICA

Atlanta Working 'Around The Clock' To Fight Off Ransomware Attack

March 27, 2018 · 7:47 AM ET

DOREEN MCCALLISTER



Mayor Keisha Lance Bottoms speaks at a press conference in Atlanta in January. David Goldman/AP.

Officials in Atlanta say the city's computer systems are not yet fully operational after a ransomware attack hit the city last week and locked some city data behind a wall of encryption.

Tasnim Shamma of member station WABE in Atlanta tells our Newscast unit that cybersecurity experts are working around the clock to restore access to the city's data.

AT&T Live

Atlanta's Computers Held Hostage, With A \$50K Ransom

NOW · NEWSER BY JENN GIDMAN

f

t

e

Atlanta is being held hostage, by computer hackers who want more than \$50,000 in bitcoin to stop their siege. "This is much bigger than a ransomware attack, this really is an attack on our government," Mayor Keisha Lance Bottoms said at a Monday presser about the e-attack, per [Reuters](#), adding, "We are dealing with a [cyberhostage] situation." [Bitcoinist](#) reports the hack began Thursday morning, and it has taken down Atlanta's online bill payment system from some remote location, says Bottoms, who's staying mum over whether the ransom will be paid.

(Bitcoinist notes, however, the city has "no plans" to pay up.) The FBI, Homeland Security, Cisco, and Microsoft are all teaming up to help the city figure out what data has been breached and what steps to take next in what Bottoms has deemed a "massive inconvenience," reports [ABC News](#).

Atlanta still feeling the effects of ransomware cyberattack


f

t

G+

in

1



DAVID GOLDMAN/ASSOCIATED PRESS

mayor says the city continues to operate despite ongoing troubles caused by a cyberattack.

By Associated Press | MARCH 27, 2018

ATLANTA (AP) — Atlanta's mayor says the city continues to operate despite ongoing troubles caused by a cyberattack on its computer network last week.

City officials announced Thursday that the city's computer network had been attacked by ransomware that encrypted some city data.

## Nonprofits are especially at risk

Operate heavily on trust

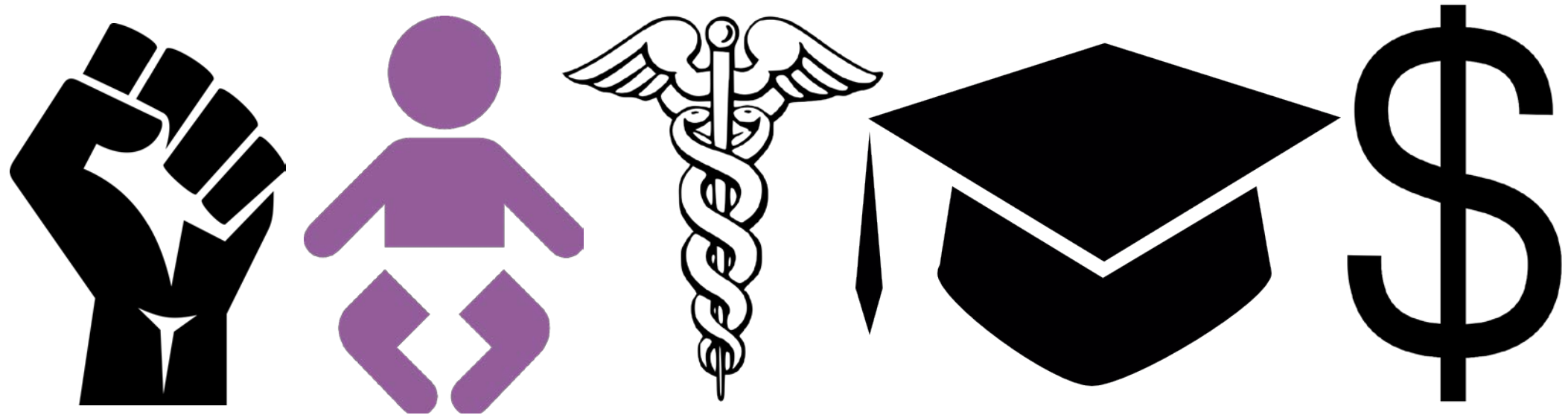
Often have tons of sensitive data

Stepping stones into bigger targets

Too busy with meaningful work to  
divert time/energy/money to  
overhead



Certain types of nonprofits are at particularly high risk





# 2

## The pieces of your security landscape

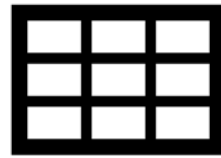
What do you have (assets) that someone wants?



**Things**



**Money**



**Data**



**Information**

## Assets



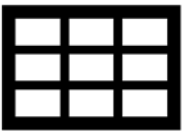
Things

Usually they want *access* to computers and servers in order to launch scams and attacks on other organizations



Money

Nothing shocking here – looking for quick cash transfers



Data

Standard information like medical records, credit numbers have commodity pricing information on the black market. \$x/record



Information

If they are against your mission, they might want damaging information or internal communications, but this is extremely unlikely.



Who wants those assets (adversaries)?



**External  
Attackers**



**Staff**



**Concerned  
Citizens**

# EXTERNAL ATTACKERS

Ransomware

Phishing

DDoS (distributed denial of service)

Malicious software & spam

Online fraud

Installing Botnets

Software piracy



# INTERNAL STAFF

Careless with data

Careless with credentials

Stealing information

Coverup

Installing inappropriate software

Falling for Phishing



## CONCERNED CITIZENS

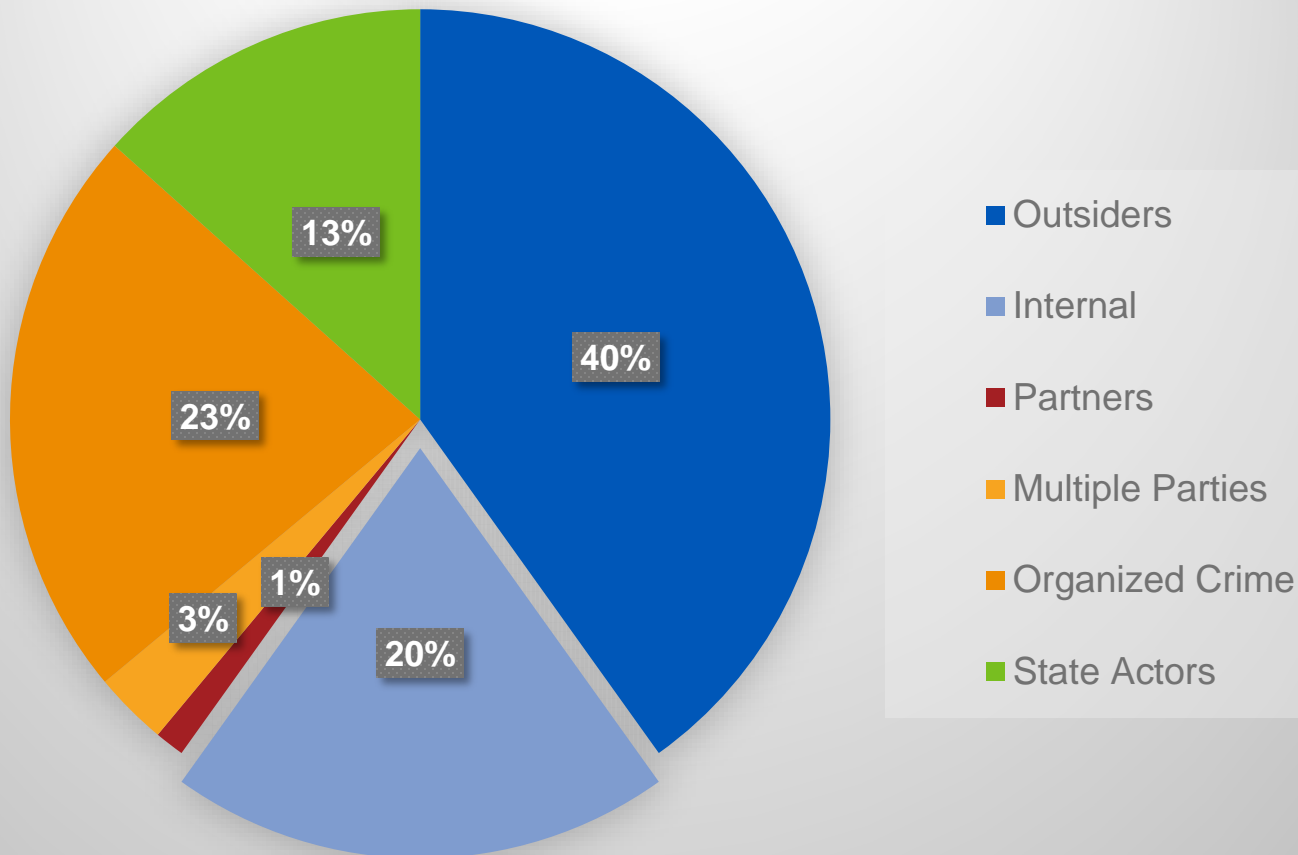
Might go public, or submit what they found to the authorities. This would present a significant ***reputational*** or ***regulatory*** risk to you.

Are against your mission and want to disrupt your ability to deliver programs or smear your reputation.



# Data Breach Investigations Report (2019)

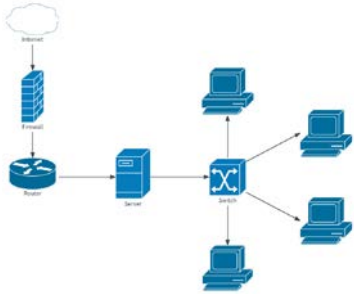
## Who's Responsible



Verizon's DBIR analyzes 41,600+ security incidents and 2,000+ breaches across 65 countries.

The report draws its findings from an analysis of real-world data breaches investigated by Verizon and an extensive range of third-party contributors during the last 12 months.

## Threat Vectors: (AKA How do they get in?)



Network Penetration



Phishing Scams



Lost / Stolen  
Malware / Virus



User Error



## Common Threat Vectors



Compromising a valid **identity** by stealing credentials or social engineering



Exploiting vulnerabilities in **software** or **firmware** used by your organization (Zero-day exploits)



Take advantage of normal **data-leakage** caused by common poor security hygiene



Use **physical access** to steal data or compromise systems



Spy on **communication** between staff or between your systems and the internet



# 3

## How ED's Should Think About Security

# Security is probably part of your mission

Do you...

...work with / advocate for sensitive populations?

...work with / advocate for minors?

...help people with financial, health,  
or educational matters?



If you answered yes to any of the above, practicing and advocating for responsible data storage and sharing practices is actually a core part of your mission.



## Letters and more letters

### GDPR: General Data Protection Regulation

Data protection framework across EU, imposes strict rules on hosting, processing EU citizen data anywhere in the world.

### PCI: Payment Card Industry

Set of security standards designed to ensure that ALL companies that accept, process, store or transmit credit card information maintain a secure environment

### HIPAA: Health Insurance Portability and Accountability Act

National standards for electronic health care data and national identifiers for providers, health insurance plans, and employers

### PII: Personally Identifiable Information

Information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context.

## Some important and under-appreciated principles

IT Security is:

...not overhead, and not optional.  
It's a core element of your  
operational mandate.

...an ongoing process, not an  
achievement.

...not something you can do  
perfectly, and something that you  
can overdo.





Your goal is not to fix everything

Perfect security isn't possible

Trying to implement perfect security is a waste of resources that hamstrings and frustrates your team and actually makes you less safe

The goal here is balance



# Most Common Threats

External Attackers stealing email account credentials for spam or fraud

External Attackers repurposing servers, computers, or networking equipment for botnets or fraud

External Attackers phishing to make money

Protecting against these is a matter of making it harder for the attacker to get in. They often go after someone else





And those are just the basic threats that everyone worries about

Advanced adversaries are those that specifically target you and have the technical means to pull it off. Usually their aim is espionage and/or damaging your reputation.

Protecting yourself is possible but difficult. You need to be hardened not just harder. That probably means compromises for your staff.

Protecting against government actors is even harder because you often can't use cloud-based services.



## Focusing efforts

We only want to worry about the threats that are actually relevant to your organization

Too much security = no security at all

- at the planning stage (because you'll be too overwhelmed to ever get started)

- at the deployment stage (because your staff will be too overwhelmed and frustrated to follow your directives)

Why protect against the loss of medical information if you don't have any or the stealing of internal communications if you make everything public?

What would the **impact** be of Staff getting access to HR Data?

## Activity

### Let's fill out the DIY Security Assessment Worksheet

Enter "Low", "Medium" or "High" in the Impact Self-Assessment table

Use blank lines for additional systems

### Let's evaluate our Priorities

Circle any boxes that are High Priority in the Impact Self-Assessment Table

Rate those using #1 as highest priority in the Prioritization Self-Assessment table

### Let's discuss





# Your Impact

On Page 1 of your worksheet, answer the following question for each box:

What would the **impact** be of \_\_\_\_\_ getting access to \_\_\_\_\_?

	External Attacker	Internal Attacker	Concerned Citizen
Org financial account information	High	Low	Low
Staff HR data (salaries, SSN, <u>etc</u> )			
Internal communications			
Internal intellectual property			
Constituent medical info			
Constituent financial info			
Donor or constituent contact info			

## We can't do everything

- Unless you're a bank, you're going to have to pick and choose which of these vectors you focus on
- The *likelihood* of a particular kind of attack can help, but we should combine that with the *impact to your specific organization we determined in part 1*.

	External Attacker	Internal Attacker	Concerned Citizen
Org financial account information	High	Low	Low
Staff HR data (salaries, SSN, etc)			
Internal communications			
Internal intellectual property			
Constituent medical info			
Constituent financial info			
Donor or constituent contact info			

+

### *Likelihood*

Very Rare

Unusual

Common



# Prioritization

	External Attacker	Internal Attacker	Concerned Citizen
Org financial account information	1	5	
Staff HR data (salaries, SSN, etc.)		4	3
Internal communications			
Internal intellectual property			
Constituent medical info	2		
Constituent financial info			
Donor or constituent contact info			

## Likelihood

Very Rare
Unusual
Common


- Look back to your impact assessment and review your highest-impact outcomes
- Circle these cells on the second page of your workbook
- Rank them starting at 1 (highest priority) by looking at the *likelihood* of something happening

# Cyber Security Threat Vectors



## Device Security

Ensure our devices are safe and that their loss will not endanger the organization




## Data Loss Controls

Ensure that sensitive information doesn't intentionally or accidentally get put somewhere unsafe, or sent to someone who shouldn't have it



## Item-level Encryption

Provide extra protection to specific highly sensitive information to prevent sharing



## Account Security

Ensure that people have only the level of access they really need, and that we know who is accessing what



## Malware Controls

Minimize the exposure of our devices to risky software and websites, and ensure that active protections are in place to defend against new and unknown malware



## Network Controls

Monitor our networks and protect them from direct penetration attempts





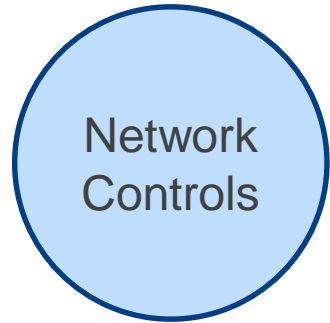
## What is Device Security?

- Allows organizations to limit which devices are accessing data
- Allows organizations to enforce settings on devices that are exposed to sensitive information
- Allows organizations to manage updates, anti-virus, and other key features of mobile devices
- Allows organizations to wipe sensitive data from devices when employees leave or devices are lost



## What is Malware Controls?

- Ensure that all workstations have antivirus and antimalware applications installed
- Ensure that all AM/AV is updated
- Run full scans regularly
- Address any suspicious results immediately



## What are Network Controls?

- Network firewall is installed and configured properly (do not just use the Internet modem)
- Firewalls are patched and updated regularly
- Log files are regularly monitored for suspicious activity (DDoS)
- Wireless access points are configured with passwords
- Wireless guest network is separate from business network



## What is Account Security?

- Ensure that each account is used by one user
- Ensure that each account is used by the correct user
- Monitor for suspicious login activity



## What are Data Loss Controls?

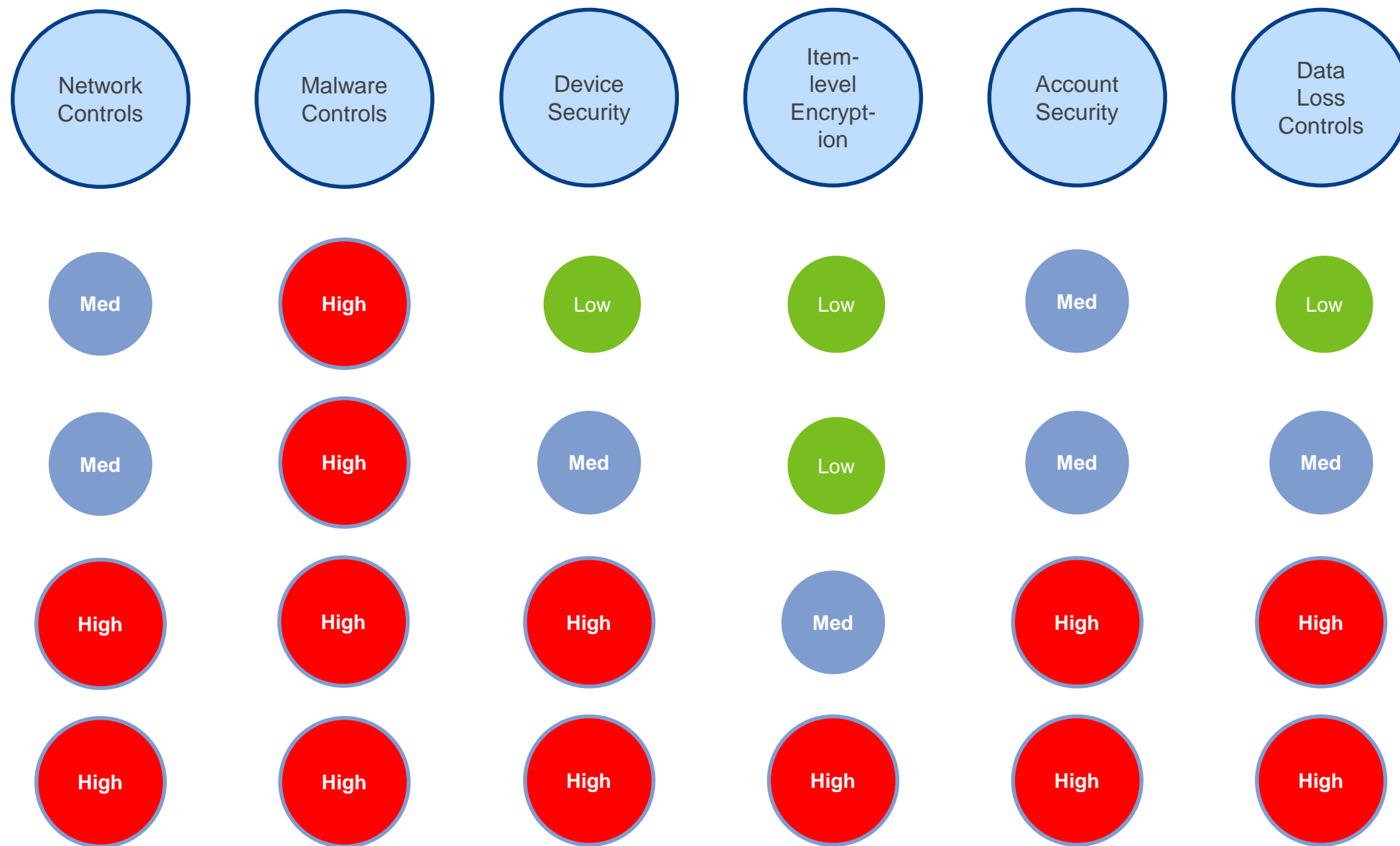
- Monitor for the accidental or intentional sharing of sensitive information like Social Security Numbers and other PII
- Monitor the location of sensitive information
- Use heuristic analysis to identify suspicious patterns of behavior that might indicate compromise or intentional removal of data



## What is Item-Level Encryption?

- Allows organizations to protect sensitive data regardless of its location. Protected files can be stored on thumb drives or emailed outside of the organization without fear of data loss.
- Prevents users from sharing content unless permitted by the organization. Protected files can't be forwarded and some control is provided over printing, copy/paste, etc.

## Levels of Concern Vary



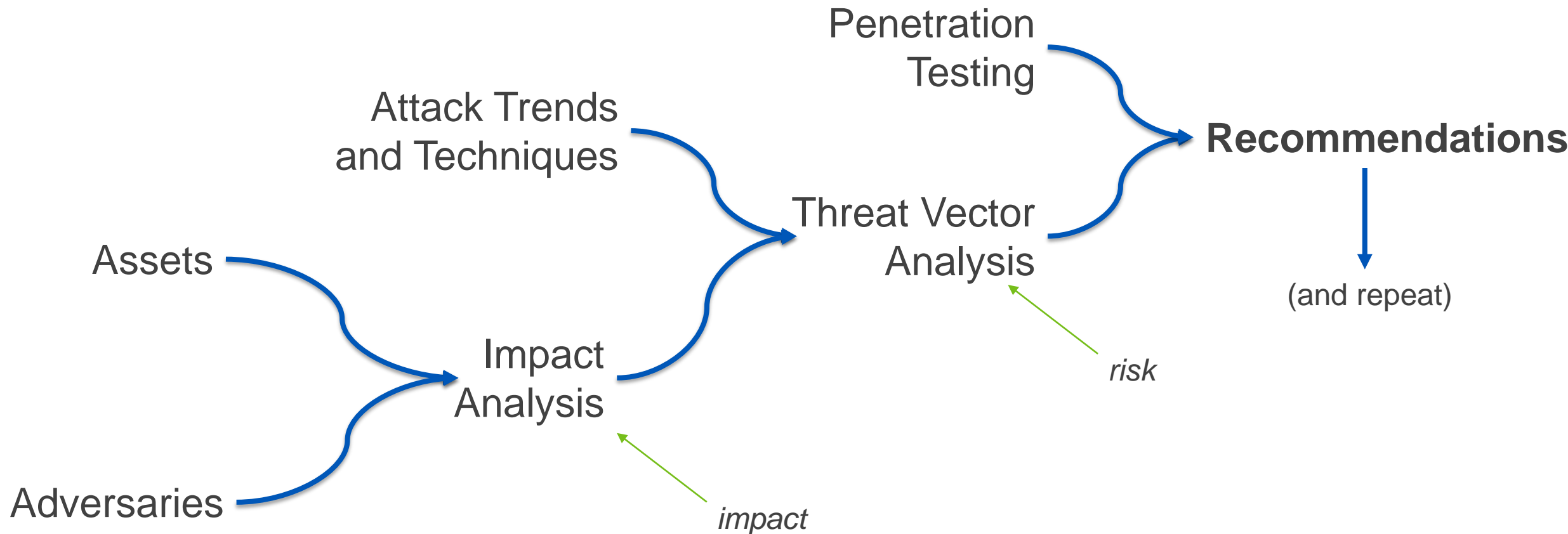


# 4

## Assessing Your Risk



## What's our process?





# Security Assessment (DIY)

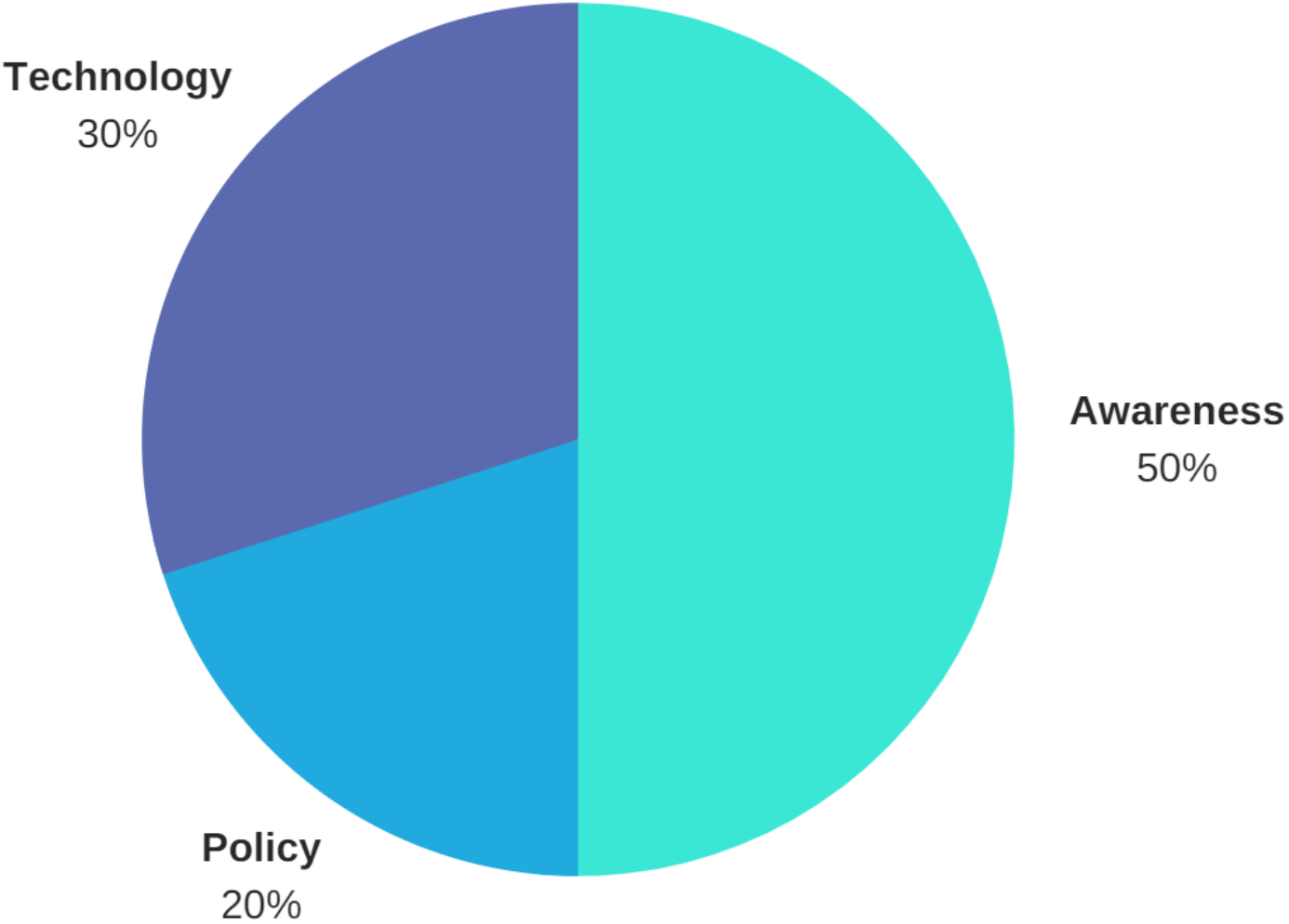
Security Worksheet		
BENCHMARKS	standard security areas, add to list if needed	
ASSESSMENT	details of current state with gap and score (see scoring chart)	
PROJECTS	any mitigation projects with timeline/priority	
COSTS	costs of mitigation and ongoing support if needed	



# 5

## Best Practices for Cyber Security

# Cyber Security Best Practices – Areas to Address



## Awareness - Policy



Clear and updated policy for computer use



Documented methods for storing, sharing and handling information



Communicated and signed by staff

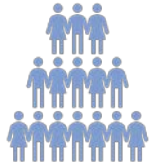


Protects the organization from liabilities

<https://www.sans.org/security-resources/policies/general#acceptable-use-policy>

<https://www.sans.org/security-resources/policies/general/>

# Awareness - Culture



The *culture* of security in your organization



Are people likely to think about security before taking action?



Know there are **consequences** to poor security practices



Trust that you care more about them **getting work done** than fear mongering



Have **usable** tools to be secure

## Awareness - User Education

Regular security briefs and educational content – threats are always changing

Educate – use KnowBe4 to simulate phishing attacks and provide education. Will protect organization but extra benefit to protect employee personal information.

Accountability – keep users accountable



## Awareness – Liability and Recovery



- **Investigation** – determine what occurred and how to recover. May involve 3<sup>rd</sup> party or FBI
- **Business Losses** – monetary losses, downtime, and costs to manage the crisis
- **Privacy/Notification** – send data breach notifications to customers or affected parties
- **Lawsuits/Extortion** – legal expenses associated with release of confidential data. Also includes ransomware costs



## Technology Mitigations



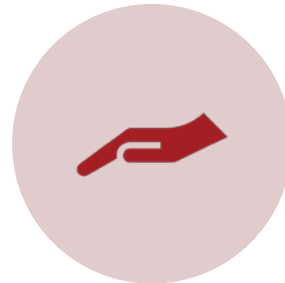
Helpful where policy is difficult to apply and/or follow (protecting against technical external attacks)



**Enforces** policy and culture and provides feedback about what is working and what isn't



Gives staff tools to **enable** them to do what is right (send data securely, store safely, etc)



Not a panacea, but a *safety net*



## Technology - Password Practices

01

Make passwords as long as possible: 20+ characters

02

Don't reuse passwords – ever

03

Don't share passwords unless you absolutely have to. Use a password manager

04

Use multi-factor authentication

# Technology - Multi-Factor Authentication

Use one centralized system as an identity / MFA provider

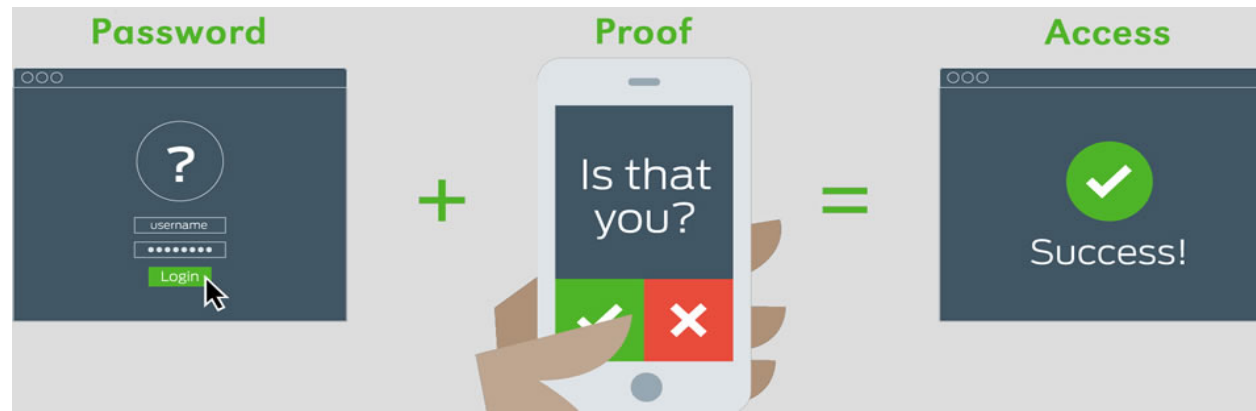
Users are prompted on phone using mobile app

Users receive phone call or text message verifying identity

“Remember” devices for configurable period of time to prevent the need for entering two-factor during that time

Exempt certain physical locations (ie, your offices) from enforcement

Examples of MFA providers include Google, Office 365, Duo, Okta, OneLogin



## Technology - Software Update & Antivirus enforcement

Use a centralized tool to check for and apply software updates to all of your PCs

Use a centralized tool to check for and enforce the presence of up-to-date antivirus tooling on all PCs

Have policies requiring staff to apply updates / restart PCs when prompted

Examples of RMM tools include Kaseya, Solar Windows, Comodo, AutoTask



## Technology - Mobile Device Management

Enrolled devices have configuration policies applied

View compliance with your policies using Compliance policies

Remote wipe

Device geolocation

Allow users to enroll personal devices, preferably at the application level



# Technology - Data Backup & Recovery



Scheduled and Automated  
Offsite  
Tested

## Next Steps



# Key Recommendations

1	<p>“Quick wins” Do these first</p> <p>Fast Enablement Minimum user impact and cost</p>	<ol style="list-style-type: none"><li>1. Create/Update Computer Policy</li><li>2. Update software, and keep it updated</li><li>3. Block access to known-dangerous sites</li></ol>
2	<p>Do these next</p> <p>Base protections Moderate user impact and cost</p>	<ol style="list-style-type: none"><li>1. Protect all accounts with MFA</li><li>2. Use a password manager</li><li>3. Encrypt devices</li><li>4. Fully manage your devices</li></ol>
3	<p>Do these last</p> <p>Best protections Additional investments required</p>	<ol style="list-style-type: none"><li>1. Know who is doing what in your systems</li><li>2. Monitor and proactively prevent data loss</li><li>3. Protect network traffic</li></ol>





5a

Microsoft Office 365



# 365 E3 Security Features



## Advanced email

Use archiving and legal hold capabilities, plus unlimited storage, for compliance needs. And use data loss prevention (DLP) policies and policy tips that educate your users for additional compliance enforcement in email.



## Document and email access control

Rights Management Services enable you to restrict access to documents and email to specific people and to prevent anyone else from viewing or editing them, even if they are sent outside the organization.



## Message Encryption

Apply flexible out-of-the-box encryption policies like Encrypt Only and Do Not Forward, and read protected messages in Outlook while messages sent to non-Office 365 users can be read using Google, Yahoo or a Microsoft identity. Plus, control your encryption keys in Azure Key Vault. [Learn more](#) ➔



## Advanced compliance tools

With the unified eDiscovery Center, you can search across Exchange, Skype for Business, OneDrive for Business, and SharePoint mailboxes.



## Information protection

Rights management, data loss prevention, and encryption for Exchange Online, Skype for Business, and SharePoint Online help keep your content safe in email, IM and meetings, and team sites.



## 365 E5 Advanced Security Features

### O365 E3 + :



#### Advanced information protection

Data loss prevention and encryption across Exchange Online, Skype for Business, and SharePoint Online help keep your content safe in email, IM, meetings, and team sites.



#### Threat intelligence

Threat intelligence provides broad visibility into the threat landscape, which helps deliver actionable insights, and enables proactive cybersecurity to ultimately help reduce your costs.



#### Advanced security

Advanced Threat Protection helps defend users against sophisticated threats hidden in emails, attachments, and links. Customer Lockbox lets you limit data access to only pre-assigned, two-factor-authenticated administrator approvals for greater control and transparency. And the built-in features of Office 365 Cloud App Security give you enhanced visibility and control of your Office 365 environment.



#### Analytics tools

With the live dashboards and interactive reports of Power BI Pro non-technical users can visualize and analyze data with greater speed, efficiency, and understanding. With its interactive dashboards, Microsoft MyAnalytics enables you to surface personal and organizational insights based on information across Office 365.

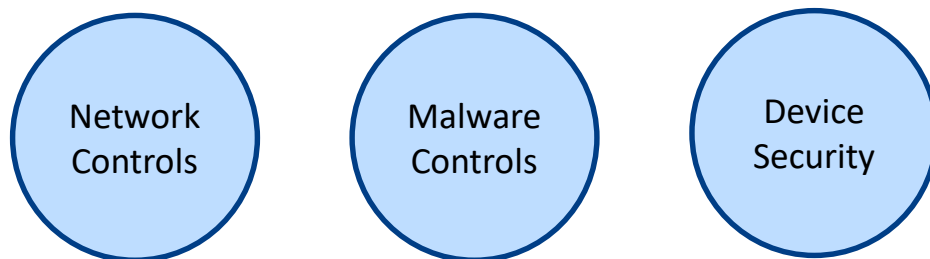


# 6

## Configuration & Support

How can we protect ourselves?

# Do This First!



Antivirus/Antimalware

Available through TechSoup or MSP

Content Filtering Tools

Subscribe (DNS Umbrella, Barracuda, etc)

















Firewalls/VPNs

Install/Configure a good firewall

OS Version/updates

Windows 10 PRO – a must!

# Levels of Professional Support Needed

	Device Security	Item-level Encryption	Account Security	Data Loss Controls
Any Nonprofit				
Orgs with standard regulatory requirements (HIPAA, FIRMA, etc)				
Orgs with stringent regulatory requirements (Banking, GDPR)				
Orgs with resourced political enemies				

## Professional Help is Available



### Planning

For licensing and features



### Email migration

From any existing system



### File sharing and collaboration

We can customize your cloud storage space for your modern day teams



### Communication & teamwork

To work with internal and external users quickly and cost effectively



### Support

For admins and users



### Compliance & Security

Manage access and maintain compliance

## Cost of a Data Breach: Actual Costs

Estimates an average of \$221 per lost record, and \$7 million average total cost. Costs may include:

- legal guidance
- breach notification
- forensics
- credit monitoring

Source: Ponemon Institute 2018 Cost of Data Breach Study ([www.ibm.com/downloads/cas/861MNWN2](http://www.ibm.com/downloads/cas/861MNWN2))







## Cost of a Data Breach: Intangible Costs

The lost trust that nonprofits experience from donors, volunteers and the community can affect

- fundraising activities
- volunteer engagement
- partnerships with other organizations

Source: Ponemon Institute 2018 Cost of Data Breach Study ([www.ibm.com/downloads/cas/861MNWN2](http://www.ibm.com/downloads/cas/861MNWN2))

# Different Levels of Data Breach Insurance Coverage

First-party data breach insurance provisions include:

- Data breach investigation costs
- Hardware and software damage costs
- Fines incurred by lost data
- Lost revenue

Third-party data breach insurance provisions include:

- Lawsuits from individuals due to data loss
- Fees incurred for aiding individuals in the event of data loss



## Bad News – It's Not “IF”, It's “WHEN”

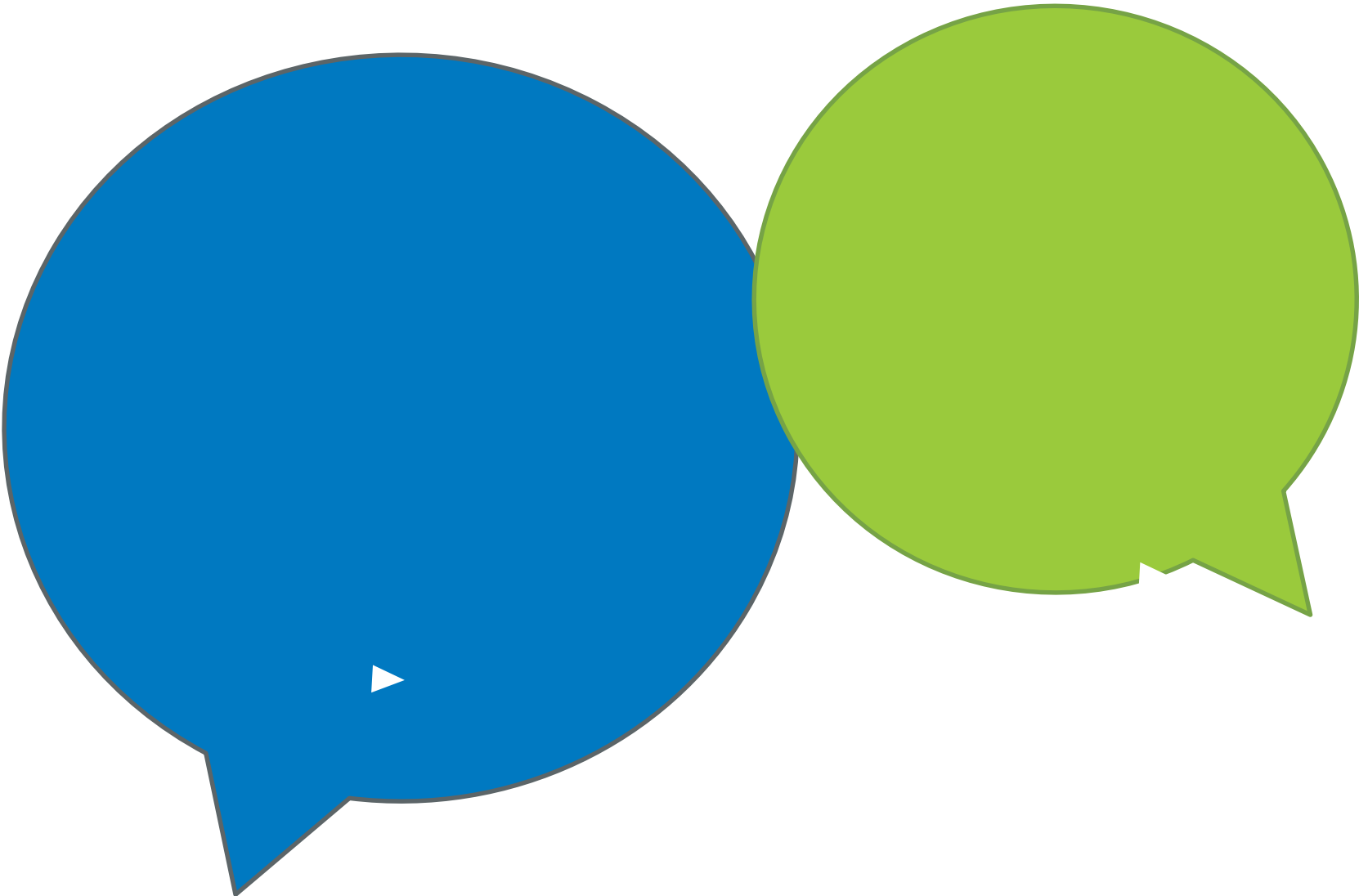


Security Breaches are going to happen even if your organization has taken steps to secure the environment and train users.

- Act Quickly – contact your IT professional at the first hint of trouble
- Follow the Plan – know what to do, how to communicate
- Recover Losses – invoke your insurance plan



Questions?





## Acknowledgments

Linda Widdop

Colin Murphy

Amy Studwell

Meher Shulman

All presentation materials copyright Tech Impact except where indicated. All images are used under a Creative Commons royalty-free non-attribution license, except for speaker headshots which were provided by the speakers.

# Thank You!



Contact Linda Widdop, Director of Technology Services for more information  
[linda@techimpact.org](mailto:linda@techimpact.org) | (215) 557-1559 x 111

