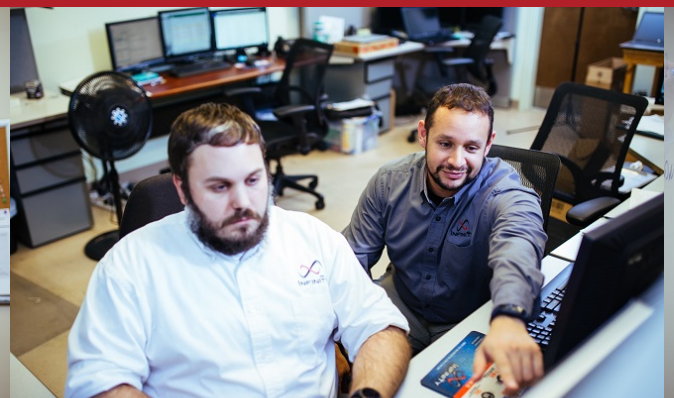
Infinity INC.

CyberSecurity

For the Rest of Us






Today's Presenter

Chuck Brown
CEO, Infinity, Inc.

What, exactly, is “Cybersecurity”?

Cybersecurity is the protection of internet-connected systems, including hardware, software and data, from cyberattacks.

In a computing context, security comprises **cybersecurity** and physical security – both are used by enterprises to protect against unauthorized access to data centers and other computerized systems.

Ok, so what's a "CyberAttack"?

A **cyberattack** is deliberate exploitation of computer systems, technology-dependent enterprises and networks.

Cyberattacks use malicious code to alter computer code, logic, or data, resulting in disruptive consequences that can compromise data and lead to cybercrimes, such as information and identity theft.

Ooops, your files have been encrypted!

English

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

About bitcoin

How to buy bitcoins?

bitcoin ACCEPTED HERE

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Copy

I’m a small business… who wants to attack me?


Who want to attack
me?

Small Business Risk

Just how big is the risk to small business?

- Big, very big.

Small Business Risk

Just how big is the risk to small business?

- Big, very big. According to the Verizon Data Breach Investigation Report, 61% of breaches hit smaller businesses last year, up from the previous year's 53%.

Small Business Risk

And according to UPS Capital…

Cyber attacks cost
$84,000 - $148,000

Small Business Risk

And according to UPS Capital…

Cyber attacks cost $84,000 - $148,000

60% Businesses Close

Small Business Risk

And according to UPS Capital…

Cyber attacks cost $84,000 - $148,000

60% Businesses Close

90% Completely Unprotected

Small Business Risk

And according to UPS Capital…

Cyber attacks cost $84,000 - $148,000

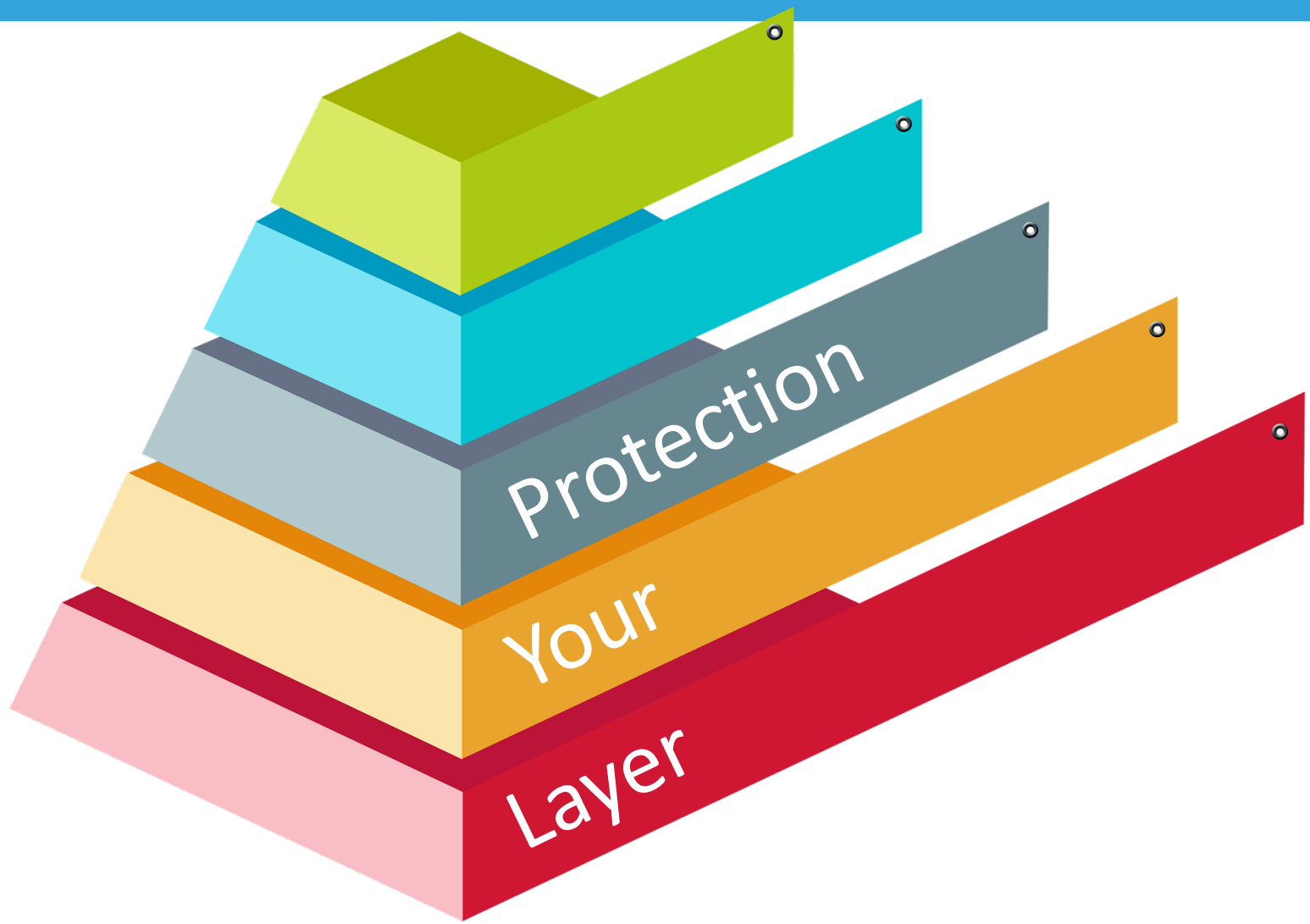
60% Businesses Close

90% Completely Unprotected

2/3

Attacks Directed at SMBs

Ok, I'm convinced. What can I do about it?


Protection
Your
Layer

Traditional Network Security

Layered approach for infrastructure

- Firewall
- Anti-virus
- Anti-Spam
- Group Policies

Company Policies

Layered approach for computing

- Password complexity
- BYOD procedures
- Screen savers/timeouts

Physical Security

Layered approach for access

- Server(s)
- Unused network ports/jacks

And then there's the really weak link…

People!

The Human Factor

- In their 2018 Human Factor Report, Proofpoint analyzed cyberattacks throughout 2017, looking into attempted attacks on nearly 6,000 organizations across the world. They found that **almost every industry suffered from a growth in the number of attacks**, ranging from phishing to ransomware and cloud application breaches.

The Human Factor

What can we do about it?

- Educate, educate, educate
- Phishing emails have a few things in common…

Phishing Flags

- Expect the unexpected
  - In a 2016 report from Wombat Security, organizations reported that the most successful phishing attacks were **disguised as something an employee was expecting**, like an HR document, a shipping confirmation or a request to change a password that looked like it came from the IT department.

From: HR@infinityinc.us

Reply-to: HR@infinityinc.us

Subject: Re: w-2

Please confirm that the w-2 is as it should be.

We uploaded it here: www.infinityinc.us/support@infinityinc.us

Use the last four of your social security number to download.

From: HR@infinityinc.us ← Message doesn't sound like our HR

Reply-to: HR@infinityinc.us

Subject: Re: w-2

Please confirm that the w-2 is as it should be.

We uploaded it here: www.infinityinc.us/support@infinityinc.us ← Wouldn't send a link like this

Use the last four of your social security number to download. ← Would NEVER do this

Phishing Flags

- Name check
  - If you receive an email or even an instant **message from someone you don't know directing you to sign in** to a website, be wary, especially if that person is urging you to give up your password or social security number. Legitimate companies never ask for this information via instant message or email, so this is a huge red flag. Your bank doesn't need you to send your account number -- they already have that information. Ditto with sending a credit card number or the answer to a security question.

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

TrustedBank™

Is that really your bank?

Dear valued customer of TrustedBank,

Generic, no name

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Go to bank's website on your own, NOT through this link to check

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Legitimate companies usually have a person sign off

Member FDIC © 2005 TrustedBank, Inc.

Phishing Flags

- Unrecognized links or attachments
  - Typically, phishing scams try to convince you to provide your username and password so they can gain access to your online accounts. From there, they can empty your bank accounts, make unauthorized charges on your credit cards, steal data, read your email and lock you out of your accounts. They can also try to install software by having you open **attachments with hidden scripts or code embedded in them**. Scripts that work without you having any idea something's happening.

From: reneeh@nationalbankofcommerce.banking.co
Reply-to: reneeh@nationalbankofcommerce.banking.co
Subject: Outstanding balance requiring attention
Invoice 1600075822.xlsm

Dear sir or madam,

Since we have not received the service termination letter, I'm assuming that you might have unintentionally overlooked our invoice 02/1600075822 (***Overdue***). If you decide to cancel the agreement, please let us know. Note that early withdrawal penalties will apply.

Refer to the attached document for billing information.

Regards,

Renee

Renee Hagen | Finance Compliance Department
National Bank of Commerce
1100 Henry Sq E, Suite 231, Township, New Mexico, 38542

From: reneeh@nationalbankofcommerce.banking.co
Reply-to: reneeh@nationalbankofcommerce.banking.co
Subject: Outstanding balance requiring attention ← Playing on fear
Invoice 1600075822.xlsm

Dear sir or madam,

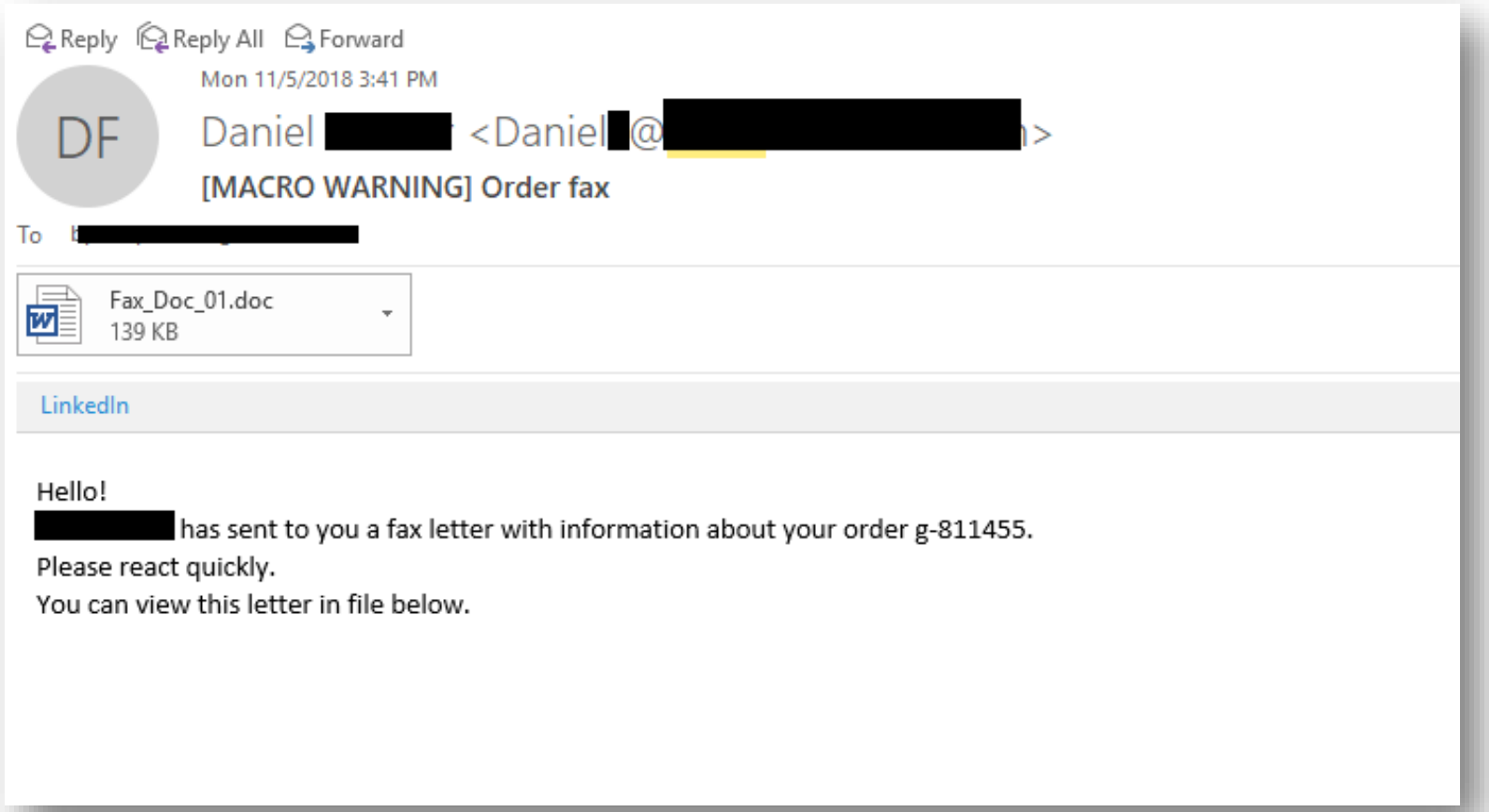
Since we have not received the service termination letter, I'm assuming that you might have unintentionally overlooked our invoice 02/1600075822 (***Overdue***). If you decide to cancel the agreement, please let us know. Note that early withdrawal penalties will apply. ← Playing on fear

Refer to the attached document for billing information. ← Always be suspicious of attachments; log in to your bank independently

Regards,

Renee

Renee Hagen | Finance Compliance Department
National Bank of Commerce
1100 Henry Sq E, Suite 231, Township, New Mexico, 38542


Reply
Reply All
Forward
Mon 11/5/2018 3:41 PM
DF
Daniel [redacted] <Daniel[redacted]@[redacted]>
[MACRO WARNING] Order fax
To [redacted]
Fax_Doc_01.doc
139 KB
LinkedIn
Hello!
[redacted] has sent to you a fax letter with information about your order g-811455.
Please react quickly.
You can view this letter in file below.

Reply Reply All Forward

Mon 11/5/2018 3:41 PM

DF

Daniel [redacted] <Daniel[redacted]@[redacted]>

[MACRO WARNING] Order fax ← Our program warns us of Macros

To [redacted]

Fax_Doc_01.doc
139 KB

LinkedIn

Hello!

[redacted] has sent to you a fax letter with information about your order g-811455.

Please react quickly. ← Playing on fear

You can view this letter in file below.

Phishing Flags

- Poor spelling and/or grammar
  - It's highly unlikely that a corporate communications department would send messages to its customer base without going through at least a few rounds of spelling and grammar checks, editing, and proofreading. If the email you receive is **riddled with these errors** or sounds like an awkward translation, it’s most likely a scam.

Subject: Mailbox Shutdown Notification

From: "Webmaster"
Date: March 26, 2009 12:09:58 PM EDT
To: undisclosed-recipients:;
Reply-To:

You are expected to verify your email account to avoid mailbox shutdown by furnishing us with the following detials :
Login Username:
Login password: **********

To avoid shutting down of your mailbox which could lead to loss of your important files on our server,you must send these details on receipt of this message.
Thank you very much.

Webmaster

Subject: Mailbox Shutdown Notification

From: "Webmaster"
Date: March 26, 2009 12:09:58 PM EDT
To: undisclosed-recipients:;
Reply-To:

You are expected to verify your email account to avoid mailbox shutdown by furnishing us with the following detials :
Login Username:
Login password: **********

To avoid shutting down of your mailbox which could lead to loss of your important files on our server,you must send these details on receipt of this message.
Thank you very much.

Webmaster

What program nowadays wouldn't catch "detials"?

Clunky language and no space around comma

Phishing Flags

- Are you threatening me?!
  - “Urgent action required!" "Your account will be closed!" "Your account has been compromised!" These intimidation tactics are becoming more common than the promise of "instant riches," **taking advantage of your anxiety and concern to get you to provide your personal information**. Don't hesitate to call your bank or financial institution to confirm if something just doesn't seem right.

From: notice@netflicsx-alerts.com
Reply-to: no-reply@netflicsx-alerts.com
Subject: Your Netflix account is on hold!

NETFLIX

! Your account is on hold.

Please update your payment details

Hi User,

We're having some trouble with your current billing information. We'll try again, but in the meantime you may want to update your payment details.

UPDATE ACCOUNT NOW

Need help? We're here if you need it.
Visit the Help Center or contact us now.

- Your friends at Netflix

From: notice@netflicsx-alerts.com
Reply-to: no-reply@netflicsx-alerts.com
Subject: Your Netflix account is on hold!

Playing on fear

NETFLIX

Strange punctuation, playing on fear

! Your account is on hold.

Please update your payment details

Hi User,

"User"? They know your name.

We're having some trouble with your current billing information. We'll try again, but in the meantime you may want to update your payment details.

UPDATE ACCOUNT NOW

Log in independently

Need help? We're here if you need it.
Visit the Help Center or contact us now.

- Your friends at Netflix

But What If…

If your network is compromised despite your best efforts, you still don't have to panic.

But What If…

If your network is compromised despite your best efforts, you still don't have to panic.

1. Have a plan.
   - If you currently do, review it; it could probably use updating. If you don't have one, start it. It's easier than you think.
   - Find out if you are subject to regulatory requirements—there may be substantial penalties for not reporting breaches to the appropriate agencies/customers.

But What If…

If your network is compromised despite your best efforts, you still don't have to panic.

1. Have a plan.
   - If you currently do, review it; it could probably use updating. If you don't have one, start it. It's easier than you think.
   - Find out if you are subject to regulatory requirements—there may be substantial penalties for not reporting breaches to the appropriate agencies/customers.
2. Tell your IT team.
   - Whether you clicked on something suspicious, want them to check if a message is suspicious, or are already suffering from system errors or ransomware, your IT providers should be available to help you and they'll want to know.
   - And now a word about backups…

Backups: Your last line of defense

- Know your policies
  - How frequent are your backups?
  - What are you backing up?
  - Where are your backups going?
  - Are you sure you can recover from your backups, have they been tested?

Backups: Your last line of defense

- Know your policies
  - How frequent are your backups?
  - What are you backing up?
  - Where are your backups going?
  - Are you sure you can recover from your backups, have they been tested?

3. But the BEST way to protect your network:

Better than a cure…

Next Steps

Request information about employee cyber awareness training

Let's Talk

Subscribe to receive more tips and information like this

Keep in Touch

See more phishing examples

Show Me

Thank You!