Small/Medium-sized Business

And The Cyber Challenges They Face

Objectives

- Define the Cybersecurity Problem facing Small/Medium-sized Businesses
- Unpack a Ransomware Attack
- Response to Attack

Cybersecurity Defined

- Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information. (CISO)
- Long definition – short : Measures taken to protect a computer system against unauthorized access or attack
- Even shorter: Protection of any device that touches the internet.

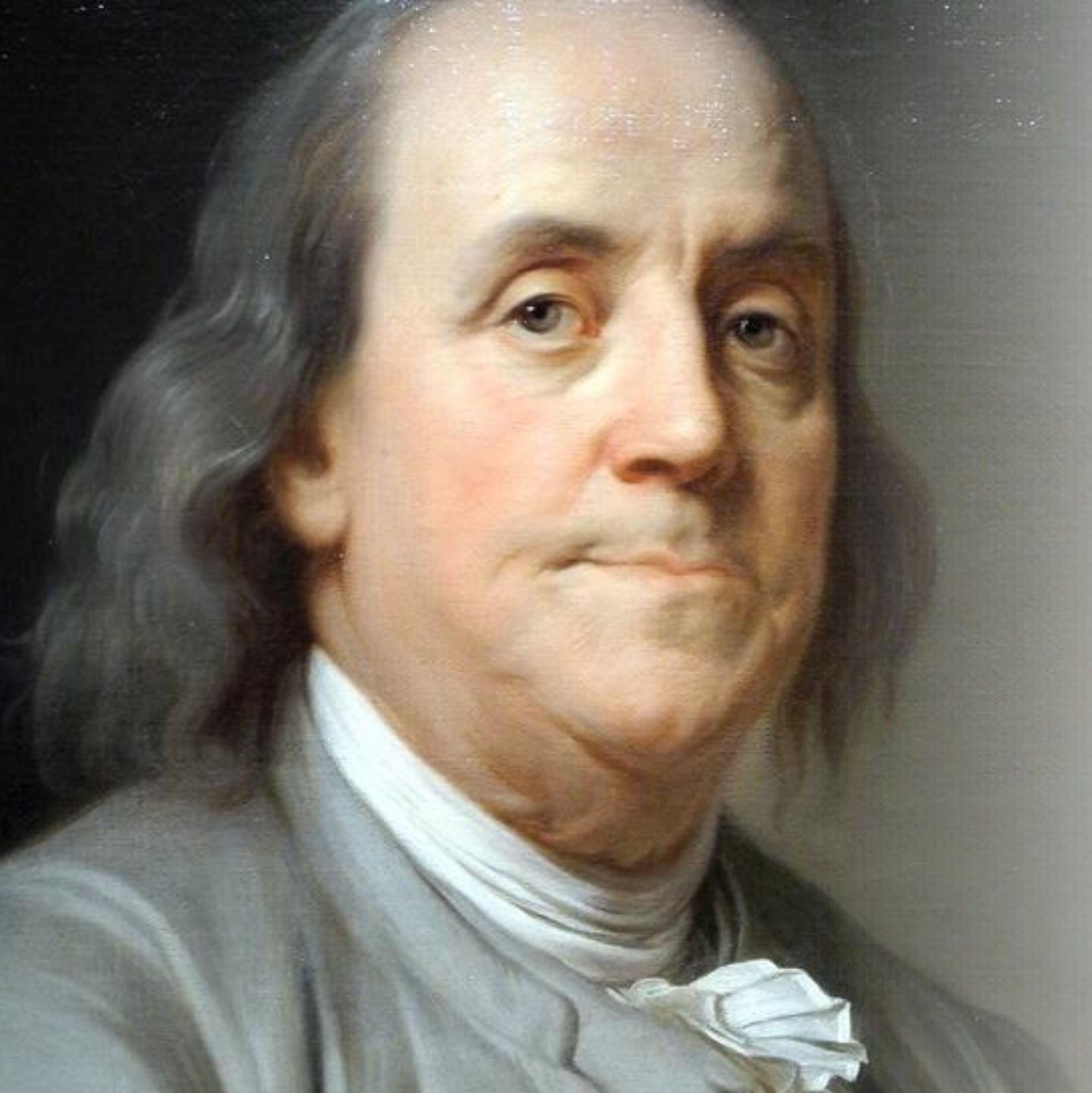
Goals of Cybersecurity

- Confidentiality – Information is restricted to only those who need to know
- Integrity – Information you receive and send is not interfered with or tainted
- Availability – Information is available when needed
- Response Plan – Develop incident response to potential cyber attacks
- Training Plan– Train your employees to “pause before you cause …a problem to your employer’s network.”

- When considering cybersecurity, Hope should not be your only plan.

- “They (small business owners) mistakenly think they do not have the data the bad guys would want, are not big enough, or are not located in a big city where such hacks occur. **A company’s size and location are often irrelevant to why an attack is launched.”**

Scot Ganow, co-chairman of the Privacy and Data Security practice group at Taft Stettinius & Hollister LLP



Preparation

“By failing to prepare, you are preparing to fail.”
— Benjamin Franklin

The Problem for Small/Medium-sized Business

Cyber crime has increased 600% during the pandemic

Cyber attacks against Small/Medium-sized Businesses mall are becoming increasingly common.

43 to 61% of Cyber Attacks target Small/Medium-sized Businesses

70% of Small/Medium-sized Businesses are not ready to deal with a Cyber Attack

3 out of 4 Small/Medium-sized Businesses say they don't have sufficient IT personnel

51% of Small/Medium-sized Businesses say they can't afford Cybersecurity

Small/Medium-sized Businesses are not prepared for the consequences of the operational disruption that generally follows a cyber attack

You Should Know…

- There is no 100% protection against Cyber Criminals
- It is not IF you will be attacked but when
- Tree of Survival
- Who are you working for?

Why You Should Implement Cyber Security

- Protecting your network and business assets is as important as protecting your home
- Customers/Vendors/Partners expect you to care about their information and intellectual property
- State and Federal Governments are passing legislation pertaining to reporting requirements for businesses who experience a breach
- Depending on your industry you could have fines and sanctions
- Legal Considerations such as exposure to class-action lawsuit or damages to individuals
- Ensure Cyber Insurance Pays
- Compliance Frameworks

Biggest Cyberthreats to Small/Medium sized Businesses

- Phishing Attacks
- Malware
- Ransomware
- Password Issues
- Insider Threat

Suspicious Email

From: John Doe <abc@voostg.com
Sent: Monday May1, 2022 10:50 AM
To: Joey Bag O'Donuts Joey.Bagodonuts@drywater.com
Subject: Change of Bank Account

I have recently switched banks hence, wish to change my current Payroll Info to my new account,

Kindly get back to me with what info I need to forward.
Regards,

John Doe
Chief Executive Officer at Dry Water Company.

(This is not John Doe's usual signature line and the company logo is missing which is on all other John's emails which a frequent recipient of email from John would know.)

From: "SunTrust"<secure@suntust.com>
To: -
Subject: Account Temporarily Suspended
Date: 2017-08-25 10:09AM

Dear SunTrust Client,

As part of our security measures, we regularly screen activity in the suntrust Online Banking System. We recently contacted you after noticing on your online account, which is been accessed unusually.

To view your Account,

1. Visit suntrust.com
2. Sign on to Online Banking with your user ID and password
3. Select your account

We appreciate your business and are committed to helping you reach your financial goals. call us at 800-SUNTRUST (786-8789), or stop by your local branch to learn more about our helpful products and services.

Thank you for banking with SunTrust.

Sincerely,
SunTrust Customer Care

bit.ly/2gbylhc
racuda Networks, Inc. All rights reserved. | Privacy Policy | Terms of Service

How to avoid Phishing/Ransomware/Malware

- Do not open emails from unknown senders
- Do not visit websites that do not pertain to the employee's specific work needs and requirements
- Do not download information from websites or click on links that do not pertain to an employee's specific work requirement
- Do not provide personal information when answering an email, unsolicited phone call, text message or instant message.

Vulnerabilities

- Vendors/Down Chain
- Network, cloud services, and device misconfigurations
- No encryption or poor encryption
- Non-patched systems or delayed patching
- Technical Vulnerabilities

Myths vs Reality

“I am too small to be a target”	“I don’t have anything anyone would want to steal”
”I don’t have time to understand all that technical stuff”	IT will get us back up and running soon, right?
“I can’t afford Cybersecurity protection”	”I have Cyber Insurance, so I am good.”

Reality

- Criminals want you to think that
- If you have something to sell, you have something to steal
- You don’t have to
- Wrong, it can take days, weeks, or months to get back to normal
- You can’t “not” afford it
- Having Cyber Insurance does not equal getting paid for an event!

What does Cybersecurity for a business look like?

- Network/Security/Vulnerability Scans
- Firewall
- Antivirus /Anti-malware
- Backup System
- Email/Spam Filtering
- Multi-Layered Email Security
- Password Management
- Multi Factor Authentication

What does Cybersecurity for a business look like?

- Monitor Network Traffic Flow
- 24/7 SOC Monitoring
- Mobile Device Management
- Phishing Training for Employees
- Dark Web Scans
- Compliance Framework
- Policies and Procedures

Unpacking a Ransomware Attack

Paul’s Nightmare Begins

Paul's Company

- Paul returned from lunch
  - Paul signs back in
  - Indicators of Compromise
  - Restarted his programs
  - Paul elected to restart his computer
  - Noticed another session running in the background which was unusual
  - Left the office for a meeting
  - The next morning it became apparent that his company network had been attacked by ransomware

Ooops, your files have been encrypted!

English

Payment will be raised on

5/18/2017 19:40:10

Time Left

01:20:04:50

Your files will be lost on

5/22/2017 19:40:10

Time Left

05:20:04:50

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
GMT from Monday to Friday


PETYA RANSOMWARE - St...
petya37h5tbhyvki.onion/LqPmoG
Search
PETYA RANSOMWARE
Start
Payment
FAQ
Support
English
Your computer has been encrypted
The hard disks of your computer have been encrypted with an military grade encryption algorithm. It's impossible to recover your data without an special key. This page will help you with the purchase of this key and the complete decryption of your computer.
The price will be doubled in:
6 days 12 hours 9 minutes 18 seconds
Start the decryption process
News
24.03.2015
WARNING

Payment for private key

Private key will be destroyed on
9/20/2013
6:48 PM

Time left
71 : 57 : 22

Choose a convenient payment method:

Bitcoin (most cheap option)

bitcoin

Bitcoin is a cryptocurrency where the creation and transfer of bitcoins is based on an open-source cryptographic protocol that is independent of any central authority. Bitcoins can be transferred through a computer or smartphone without an intermediate financial institution.

You have to send below specified amount to Bitcoin address **1KP72fBmh3XBRfuJDMn53APaqM6iMRspCh** and specify the transaction ID, which will be verified and confirmed.

Home Page
Getting started with Bitcoin

Now What?
Ransomware Response

This is where Hope has left the building!

IT will get us back up and running soon, right?

"Organizations have become so used to IT fixing things or getting things back up and running in short order that they don’t really plan for complete loss, or long-term loss, or corruption of systems, services or data."
—Mac McMillan, CynergisTek

Timeline (Hour One)

- Hour One
  - Initial discovery
  - Obtain Basic intelligence
  - Activate Incident Response Plan and Team
  - Begin Documentation of Event
  - Triage Event
  - Get Help

Timeline (12+ Hours)

- 12+ hours
  - Notify Insurance Carrier
  - Notify Law Enforcement
  - Notify key business partners/Board of Directors
  - Begin Data Recovery/Restoration
  - Confirm it is a breach and not just an incident

Timeline (12-72+ Hours)

- 12-72+ hours
  - Negotiate with threat actors
  - Threat actors often request payment in Bitcoin and crypto-currency
  - Forensic experts begin forensic examinations
  - Need to plan news releases and PR campaign
  - Begin notification to regulatory/compliance authorities/customers

How is Paul's Company Doing?

- Remained calm
- Contacted IT Department
- Reported the attack to LE
- Decided to pay the Ransom
- Insurance Carrier

Timeline (12-72+ hours)

Before Ransom Payment

- "Proof of Life"

After the Ransom Payment

- Confirm threat actors have sent decryption codes after payment
- Experts should "sandbox" the decryption code for malware

12-72+ hours

- Begin decryption of data, MSP can assist
- If you have problems with decryption, you may have to "purchase" additional decryption keys from threat actors
- Ensure documentation is being completed

Timeline (2-4 Weeks)

- 2-4 weeks +
  - Hopefully, operations have been restored
  - Conduct after action review
  - Implement additional security measures
  - Complete forensic examination and obtain reports
  - Confirm if Incident or Breach

Timeline – Post Event Fallout

- 1 month-48 months
  - Individual notifications (credit monitoring)
  - Lawsuits
  - Media inquiries
  - Regulatory investigations
  - After action review
  - Update Plan

Documentation

- Have a copy of existing plan handy
- Appoint someone to document event (best)
- Track event through timeline on paper and on whiteboard
- Include screenshots of the ransomware warnings
- Have a one-person control information outflow
- Document personnel/roles
- Notification diary (time/date/who was notified)
  - Law Enforcement
  - Insurance Company
  - Experts
  - Business Partners
  - Customers

Documentation

- Have documentation of what was on your network before threat attack (mitigation)
- Important to document what happened, response to cyber event, personnel involved, outside resources utilized, toolsets needed, etc.
- Documentation must be comprehensive for law enforcement, criminal court and civil lawsuits, insurance carrier, BOD etc.
- Documentation may be needed to mitigate or refute federal/state/regulatory authorities' fines and sanctions
- Have a means to securely store documentation for years
- You have only one opportunity to do it right

The Most Painful Thing….

“This was the most painful thing that I have ever experienced in my personal or professional life.”

“Education President” who engaged Nomerel after experiencing a cyber breach stated after 8 months of ongoing recovery, remediation, reporting and attempting to repair his institution’s reputation.

Strategy Going Forward

- You cannot eliminate 100% of the possibility that you will be a victim of ransomware, but you can diminish the probability by acting proactively.
- Need to have robust backups
- Train and educate your employees about email phishing and best security practices
- Keep your system patched and your anti-virus and anti-malware automatically updated
- Manage access control to files and restrict privileges
- Prioritize what needs to be protected
- Utilize Whitelisting as well as Blacklisting

Strategy Going Forward

- Critical to detect the attacker as quickly as you can after they penetrate the network
- Mitigation of Damage through Real-Time Detection
- Utilize Cybersecurity Tools
- Train Employees to Look for Insider Threat
- Have a Plan
- Practice the Plan

Nomerel can Help!

Give us a call:

Ann-Margaret Hinkle

Director of Security Services

918.806.7628 Mobile

Ann.Hinkle@nomerel.com