Who Turned Out the Lights?

Foiling Wily Hackers to Protect Critical Business Functions and Data
Who am I?

✓ How do you know?
✓ How do I prove it to you?
✓ Without compromising my privacy?

Identity Paradox

“On the Internet, nobody knows you’re a dog.”

Written by Peter Steiner and published by The New Yorker on July 5, 1993
Who am I?

Ron Woerner, CISSP, CISM

• Cybersecurity Professor, Bellevue University
• Chief Security Evangelist, RWX Security Solutions
What the $%$#$ are we doing here?
Agenda

• What’s going on?
• Attack methods
• Solutions
  • Awareness
  • Simple security measures
  • NIST Cybersecurity Framework
• Where to go from here
Breaches Continue to Rise

Source: 2016 BakerHostetler Data Security Incident Response Report
The Internet of ransomware things...

HUNGRY? PAY UP AND I'LL UNLOCK MY DOOR!

ON STRIKE UNTIL YOU SEND MONEY TO MY HACKERS.

20 BUCKS IN MY PAYPAL ACCOUNT OR I'LL ONLY BREW DECAF!

I'LL BE BURNING THE TOAST IF YOU DON'T GET ME SOME DOUGH!

THE NEXT TIME YOU LEAVE, IT'LL COST YOU 100 BUCKS TO GET BACK INTO THE HOUSE, UNLESS YOU GIVE ME $75 NOW!

MY ALARM SYSTEM IS GOING TO GO OFF RANDOMLY THROUGHOUT THE NIGHT, UNLESS YOU "DONATE".

YOUR DIRTY DISHES CAN WAIT, I'M BUSY MINING BITCOINS.

EXCUSE US WHILE WE PARTICIPATE IN A DDOS ATTACK.

I'M TURNING OFF THE HEAT UNTIL YOU WARM UP MY BANK ACCOUNT!

I'LL START YOUR CAR, BUT ONLY TO TAKE YOU TO YOUR BANK TO MAKE A TRANSFER.

SEND ME $25 OR I'LL TELL EVERYONE ON YOUR SOCIAL NETWORK THAT YOU WERE STUPID ENOUGH TO BUY AN INTERNET-CONNECTED BROOM!

IF YOU DON'T SEND US CASH, YOUR REPUTATION WILL BE IN THE TRASH.

WIRE MY HACKER $100 OR I'LL REVERSE MY MOTOR AND BLOW DIRT ALL OVER THIS PLACE!
The Most Common And Insecure Password Revealed—It’s Not 123456 Or Admin

What keeps you up at night?

Business
Email
Compromise

Ransomware

Stolen
Credentials
Phishing & Business Email Compromise (BEC)

Worldwide Sweep Targets Business Email Compromise
Criminal Cases Show Need to Verify Before Wiring Funds

Operation reWired
The FBI worked with partner agencies domestically and in multiple countries around the world in a large-scale, coordinated effort to dismantle international BEC schemes.
Variety of BEC

• Vendor Fraud – Invoice Payments

• Compromised or spoofed email accounts requesting a wire (ACH) transfer

• HR Requests
  • W2 or other PII
  • Changes to payroll
How they find victims
How they communicate with victims

Spoofed email:
From: john.smith@domain.com
Reply-To: bad.guy@scammer.com

Look-alike domain registered:
john.smith@domain.com legitimate
john.smith@dornain.com fraudulent

Compromised email account:
Phishing or malware used to steal credentials for
john.smith@domain.com
Phishing
Business Email Compromise (BEC)

• Finding email addresses is trivial
• Inherently insecure
• Phishing, Spear Phishing, Whaling
Ransomware

**ransomware**, ransəmˌwe(ə)r/ *noun*

A type of malicious software designed to block access to a computer system until a sum of money is paid.
Ransomware Defenses

- Patch
- Backup data
- Active Spam & Internet filters
- Update Anti-Virus
- Employee discretion
- Incident Response Plan

- DHS CISA: https://www.us-cert.gov/Ransomware
- CIS Primer: https://www.cisecurity.org/white-papers/ms-isac-security-primer-ransomware/
Trust, but Verify

• If it seems too good to be true... Trust your gut

• When in doubt, ask someone #1 way to defeat social engineering

• Verify files & websites using Virus Total: virustotal.com
Stolen Credentials

Multi-Factor Authentication
What You Can (Should) Do

Only You can Protect Yourself and Others
Securing Internet of Things (IoT) Devices

What is it?
What does it do?
Who can see or change it?
What can go wrong & Why?
What happens when it breaks?
NIST CSF Five Steps / Functions

1. Identify
2. Protect
3. Detect
4. Respond
5. Recover

https://www.nist.gov/cyberframework
NIST CSF Five Steps / Functions

1. **Identify** valuable company assets and data.
2. **Protect** valuable company assets and data from threats.
3. **Detect** when a cyber incident occurs.
4. **Respond** quickly and efficiently to a cyber incident.
5. **Recover** from an incident and get back to business.

[https://www.nist.gov/cyberframework](https://www.nist.gov/cyberframework)
Simple Steps for Cyber Security

• If I can touch it, I own it
  Physical Security

• Account Security
  Lock Down Your Login
  Multi-Factor Authentication
  Password Keepers

• Procedures for transferring $ Confirmation

• “Be Prepared”
  It’s not if, but when...
  Know what to do if...
Going for Help

• FBI Internet Crimes Complaint Center (IC3): https://www.ic3.gov/default.aspx

• The Cybersecurity and Infrastructure Security Agency (CISA)


• State and Local Police

• Your bank
Resources

http://www.dhs.gov/stophinkconnect

http://staysafeonline.org/

Resources

• NIST Small Business Cybersecurity Corner: https://www.nist.gov/itl/smallbusinesscyber

• FTC: Cybersecurity for Small Business: https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity

• SBA: https://www.sba.gov/managing-business/cybersecurity

• StaySafeOnline (NCSA): http://staysafeonline.org/

• StopThinkConnect (DHS CISA): https://stopthinkconnect.org/
The vast majority of smaller businesses rely on information technology to run their businesses and to store, process, and transmit information. Protecting this information from unauthorized disclosure, modification, use, or deletion is essential for those companies and their customers.
Protect your small business

Learn the basics for protecting your business from cyber attacks. The business cybersecurity resources in this section were developed in partnership with the National Institute of Standards and Technology, the U.S. Small Business Administration, and the Department of Homeland Security.

https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity
Management and Cybersecurity

Managing a Business
- Running a Business
- Leading Your Business
- Growing Your Business
- Business Law & Regulations
- Business Guides by Industry
- Exporting
- Closing Down Your Business
- Cybersecurity

Cybersecurity
Is your business prepared in the event of a cybersecurity breach? Now is the time to take stock of your cybersecurity health, including the importance of securing information through best cybersecurity practices, identifying your risks and the types of cyber threats, and learning best practices for guarding against cyberattacks.

Introduction to Cybersecurity
Small businesses often don't consider themselves targets for cyberattacks due to their size or the perception that they don't have anything worth stealing. However, small businesses have valuable information.

Top Ten Cybersecurity Tips
Cybersecurity threats are real and small businesses are often an attractive target. As a small business owner, it's critical to implement the best tools and tactics you can to protect your...

Protect Against Ransomware
Ransomware is a type of malicious software that infects and restricts access to a computer until a ransom is paid. Although there are other methods of delivery, ransomware is frequently delivered...

https://www.sba.gov/managing-business/cybersecurity
Who owns the Headache?
Questions???

Ron Woerner, CISSP, CISM
Ron. Woerner @ rwxsecurity.com
Rwoerner @ Bellevue.edu
LinkedIn:
https://www.linkedin.com/in/ronwoerner/
Twitter: @ronw123
By working together, we all become safer and more secure