PROTECTING YOUR ORGANIZATION’S DIGITAL ASSETS

HOW TO PROTECT YOUR ORGANIZATION, YOUR DONORS, YOUR CLIENTS & YOURSELF

TODAY’S PRESENTERS

Mike Estrich
Marketing Manager
TechWorx

Janelle Shollenberger
Account Manager
TechWorx
TOPICS

1. Identifying risk
2. Assets you need to protect
3. Understand who the “hackers” are
4. How to respond
5. Recovery
6. Questions and Answers

WHAT IS CYBERSECURITY AND WHY SHOULD I CARE?

Cybersecurity is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access
WHAT IS CYBERSECURITY AND WHY SHOULD I CARE?

Cybersecurity is the most critical job function that EVERY employee is responsible for…

Because one errant mouse click…
could be the downfall of your entire organization

WHAT ARE YOU PROTECTING?

….EVERY PIECE OF DATA that can be MONETIZED

**Your Organization's Data**
- Financial Information
- Debit/Credit Cards
- Donor Information
- Client Information
- HR Information
- PR/Social Media

**Your Personal Data**
- Social Security Number
- Debit/Credit Card Information
- Personal Information
- Medical Information
WHAT ARE YOU PROTECTING?

....EVERY PIECE OF DATA that can be MONETIZED

Financial data has a finite lifespan

It becomes worthless once the victim detects the fraud and cancels the card or account.

WHAT ARE YOU PROTECTING?

....EVERY PIECE OF DATA that can be MONETIZED

Information contained in health care records has a much longer shelf life and is rich enough for identity theft. Social Security numbers can’t easily be cancelled, and medical and prescription records are permanent.

There’s also a large market for health insurance fraud and abuse, which may be more lucrative than simply selling the records outright.
The F.B.I. now ranks cybercrime as one of its top law enforcement activities.

RECENT HACKS

Cyberattacks have become an ever-increasing threat.

• August 2018 – Facebook account of NC Animal Shelter
  Fraudulent GoFundMe campaign was posted to their 1.3 million followers

• August 2018 – PGA of America
  Ransomware virus encrypted files before the Rider Cup in France

• April 2017 – Cancer Services of East Central Indiana
  Ransomware attack that wiped all their data, $43,000 ransom requested. They didn't pay, then hackers posted all of the sensitive information they took online.
WHO ARE THE BAD ACTORS?

Nation-State

Criminal Syndicates

Hacktivism

Financial Gain
Information
Destruction of Data

Challenge
Boredom
Excitement
Political

Compensation Example...

Date: October 2013
Hacker: 12-year-old boy (5th Grader)
Target: Hack major government and police websites in Montreal for Anonymous.
Payment: Video Games
WHAT DOES A HACKER LOOK LIKE?

Patrick Murphy
Apr. 13
Male, 32
Favorite hobby: hiking
What he actually does: It's hard to say, but it involves a lot of clever thinking and picking locks.

Chris Dorn
Apr. 13
Jr. Hacker
Favorite hobby: music
What he actually does: Cassette tape hacking

Tolong Shang
Apr. 26
Jr. Hacker
Favorite hobby: painting
What he actually does: It's hard to say, but it involves a lot of creativity and color mixing.

Chris Valaske & Charlie Wilcox
Apr. 13, 47
Jr. Hackers
Favorite hobby: cooking
What they actually do: It's hard to say, but it involves a lot of recipe designing and taste testing.

CYBERSECURITY STATS

• 90% of all cyber attacks due to a human weakness

• Almost 50% of small companies have experienced a cyber attack

• 75+% percent of employees leave their computers unsecured

• More than 70% of attacks target small organizations with less than 100 employees
**CYBERSECURITY STATS**

Average initial cost to small/medium sized business

*Attack Costs*

- 2017: $20,753
- 2018: $34,604
- 2019: $79,841+

After an attack as much as **60%** of companies go out of business within **6 months**

---

**CYBERSECURITY STATS**

Average total cost cybersecurity data breach

**2018: $200,000+**

Average of **$148** per breached data record
WHY WOULD HACKERS ATTACK YOUR NONPROFIT, RATHER THAN A LARGE CORPORATION?

Most small to medium sized organizations aren’t fully prepared for a cyber attack!

Are you one of those nonprofits?

IDENTIFYING RISK

What is a possible risk?
IDENTIFYING RISK

What is a possible risk?

Windows Client Platforms

<table>
<thead>
<tr>
<th>Version</th>
<th>Mainstream Support End</th>
<th>Extended Support End</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows XP SP3</td>
<td>4/14/2009</td>
<td>4/8/2014</td>
</tr>
<tr>
<td>Windows Vista SP2</td>
<td>4/10/2012</td>
<td>4/11/2017</td>
</tr>
<tr>
<td>Windows 7 SP1</td>
<td>1/13/2015</td>
<td>1/14/2020</td>
</tr>
<tr>
<td>Windows 8 I</td>
<td>N/A*</td>
<td>N/A*</td>
</tr>
<tr>
<td>Windows 8.1</td>
<td>1/9/2018</td>
<td>1/10/2023</td>
</tr>
<tr>
<td>Windows 10</td>
<td>10/12/2011</td>
<td>10/13/2026</td>
</tr>
</tbody>
</table>

Windows Server Platforms

<table>
<thead>
<tr>
<th>Version</th>
<th>Mainstream Support End</th>
<th>Extended Support End</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 2003 SP2</td>
<td>7/13/2010</td>
<td>7/14/2015</td>
</tr>
<tr>
<td>Windows 2008 SP2</td>
<td>1/13/2015</td>
<td>1/14/2020</td>
</tr>
<tr>
<td>Windows 2008 R2 SP1</td>
<td>1/13/2015</td>
<td>1/14/2020</td>
</tr>
<tr>
<td>Windows 2012</td>
<td>10/9/2018</td>
<td>1/10/2023</td>
</tr>
<tr>
<td>Windows 2012 R2</td>
<td>10/9/2018</td>
<td>1/10/2023</td>
</tr>
<tr>
<td>Windows 2016</td>
<td>1/11/2022</td>
<td>1/12/2027</td>
</tr>
<tr>
<td>Windows 2019</td>
<td>1/9/2024</td>
<td>1/9/2029</td>
</tr>
</tbody>
</table>
IDENTIFYING RISK – WHO CAN GIVE ACCESS?

People

Site Disasters

Outside Users

PROTECT - BASIC

System Patches

Software Updates

Access Control

Email Filter

Firewall
PROTECT - ADVANCED

Multi Factor Authentication (MFA)

Data & Email Encryption

DNS (Website) Filters

PROTECT – MITIGATE RISK

Identify Weakest Link

Recognize Threats

Create a Plan
DETECT – MALICIOUS SOFTWARE

• Virus
• Ransomware
• Spyware (not Adware)

DETECT – CAT AND MOUSE GAME

• Always a response to a threat
• Will never be 100% guaranteed
DETECT – TYPES OF PROTECTION

• Anti-Virus
• Anti-Malware
• Firewall
• Updated security patches

DETECT – NOT ALL ANTIVIRUS IS CREATED EQUAL
DETECT – LOGIN

• Forget Passwords
• Think Passphrase
• Change often
• Create Domain

DETECT – SOCIAL ENGINEERING

Social engineering bypasses all technologies, including firewalls.

— Kevin Mitnick —

Once feared by security experts as the “World’s most feared hacker”
Author of “Ghost in the Wires”

AZ QUOTES
DETECT – SOCIAL ENGINEERING

This is why it's important to teach employees the dangers of social engineering…
DETECT – SOCIAL ENGINEERING

- Attackers use social skills
- Can obtain company information
- Can obtain personal information
- Can obtain computer systems information
- Get around any cybersecurity safeguards

DETECT – SOCIAL ENGINEERING

- Utility Service
- Telecom Engineer
- Pest control
- IT contractor
- Fake employee
- Consultant
- Courier / Deliveryman
DETECT – SOCIAL ENGINEERING - SPOOFING

Michael Estrich

From: Greg Coleman <gcoleman@seawolves.com>
Sent: Friday, July 8, 2016 12:58 PM
To: Michael Estrich
Subject: Important !!!

Hello Mike,

I’ll need you to cut out a check payment of $3,650 and mail it out today via next day delivery. Let me know when you’re ready so I can send the details.

Thanks,
Greg

Sent from my iPhone

---

DETECT – SOCIAL ENGINEERING - SPOOFING

From: Greg Coleman <gcoleman@seawolves.com>
Sent: Friday, July 8, 2016 12:58 PM
To: Michael Estrich <mike.estrich@decisionassociates.net>
Subject: Important !!!

Thanks,
Mike

From: Greg Coleman [mailto:gcoleman@seawolves.com]
Sent: Friday, July 8, 2016 12:58 PM
To: Michael Estrich <mike.estrich@decisionassociates.net>
Subject: Important !!!
**DETECT – SOCIAL ENGINEERING – PHISHING**

Vincent R. Cappucci <vcappucci@ent-law.com>

**RE: divorce papers**

My name is Vincent Cappucci and I am a senior partner at ENTWISTLE & CAPPUCI LLP. Your spouse has contracted me to prepare the divorce papers. Here is the first draft, please contact me as soon as possible:

http://www.entwistle-law.com/papers/divorce_joy.doc

Thank you
Vincent R. Cappucci
Senior Partner
vcappucci@ent-law.com
Phone: 312-594-3678
Fax: 312-594-1151

**DETECT – SOCIAL ENGINEERING**
RESPOND – PLANNING

Proactive vs Reactive

What are your nonprofit’s...
1. Policies
2. Processes
3. Procedures

RESPOND – PLANNING: WHAT HAPPENS IF...

• Employee steals data
• Employee unwittingly gives out data
• Server crash
• Site compromised by fire/flood
• Data gets hacked/locked down
• Data gets deleted accidentally or maliciously
RECOVERY TYPES

Good, Better, Best

$ Tapes
$$ Onsite – NAS Unit
$$$ Offsite – Rotating Drives
$$$$ Cloud – Onsite & Offsite

RECOVER - INSURANCE

• Cyber Insurance
• Good and Bad
QUESTIONS

FOLLOW UP

To schedule a free cybersecurity assessment please contact

Mike Estrich or Janelle Shollenberger
sales@techworx.io
814.806.3228