New Threats Mean New Challenges

(Especially since the old threats haven't left)

PRESENTER: Wayne Rash

Threats Seem to Be Everywhere

- Sony
- CentCom
- Home Depot
- Target
- Anthem Healthcare
- Banks

Home Depot data breach update: 56 million cards confirmed stolen

The Target security breach is a turning point for enterprises

Surviving the Sony Pictures hack: Is the company's future in jeopardy?

Threats Come from Everywhere

- Russian criminals
- Chinese hackers
- ISIS terrorists
- Maybe even North Korea
- Not to mention, your own employees

There Are Many Types of Threats

SPEARPHISHING

RANSOMWARE

DDOS

INSIDER THREATS

BRUTE-FORCE ATTACKS

DUMB MISTAKES

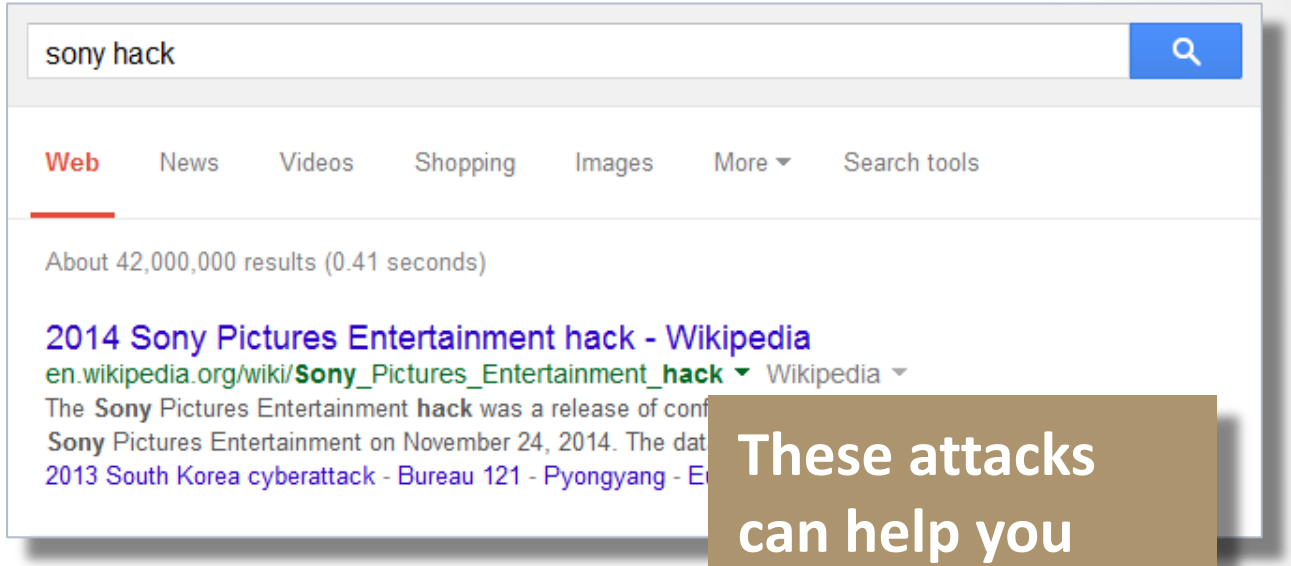
The Attack Atmosphere Changes Daily

- You need new or revised responses.
- New types of attacks mean you need new tools and approaches.

The bottom line: New attacks dictate a bigger quiver of arrows.

Many Attacks Are Getting Attention

- Sony
- Anthem
- Bank breaches
  - Carbanak Bank Breach



These attacks can help you learn what to expect.
New attacks help you make your case for support.

Some of the Worst Get Little Attention

- Attacks by state actors against U.S. or contractors
- Attacks that are detected before damage is done
- Attacks that are embarrassing to the victim

These attacks don't help you in terms of learning or support.

Some Attacks Can Go for Months

- Home Depot
- Target
- Sony
- Anthem

Security Has Become More Complex

- BYOD
- The cloud
- Mobile and remote workers
- Mobile and remote customers

- New requirements
  - Privacy
  - Legislation
  - Accounting rules
  - Competition
- And, of course, budgets are not getting bigger

MAKING SENSE OF THE THREATS

Things You Can Handle with Technology

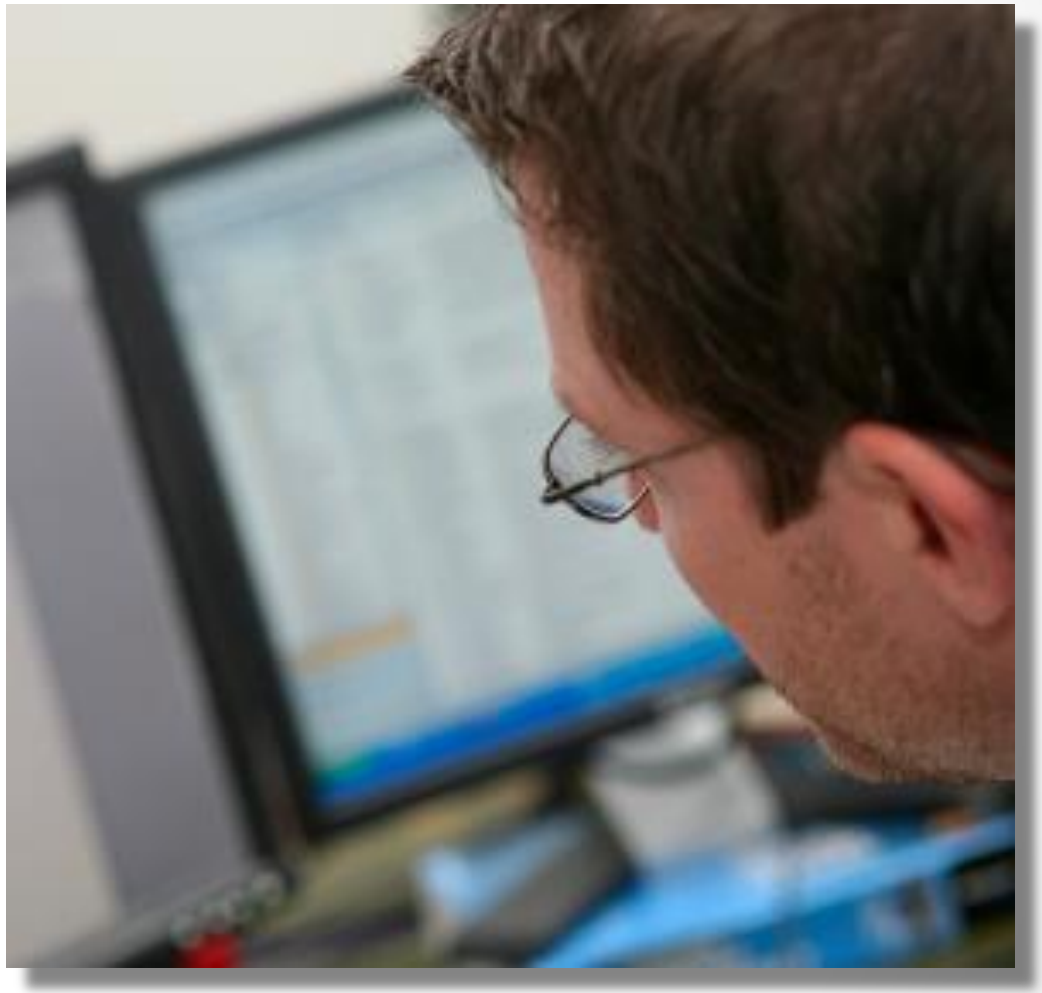
- Viruses
- Emailed malware
- Infected websites

Technology Handles Part of the Problem

- Spearphishing
- Watering holes
- Social media
- Ransomware

No Obvious Technology Solutions

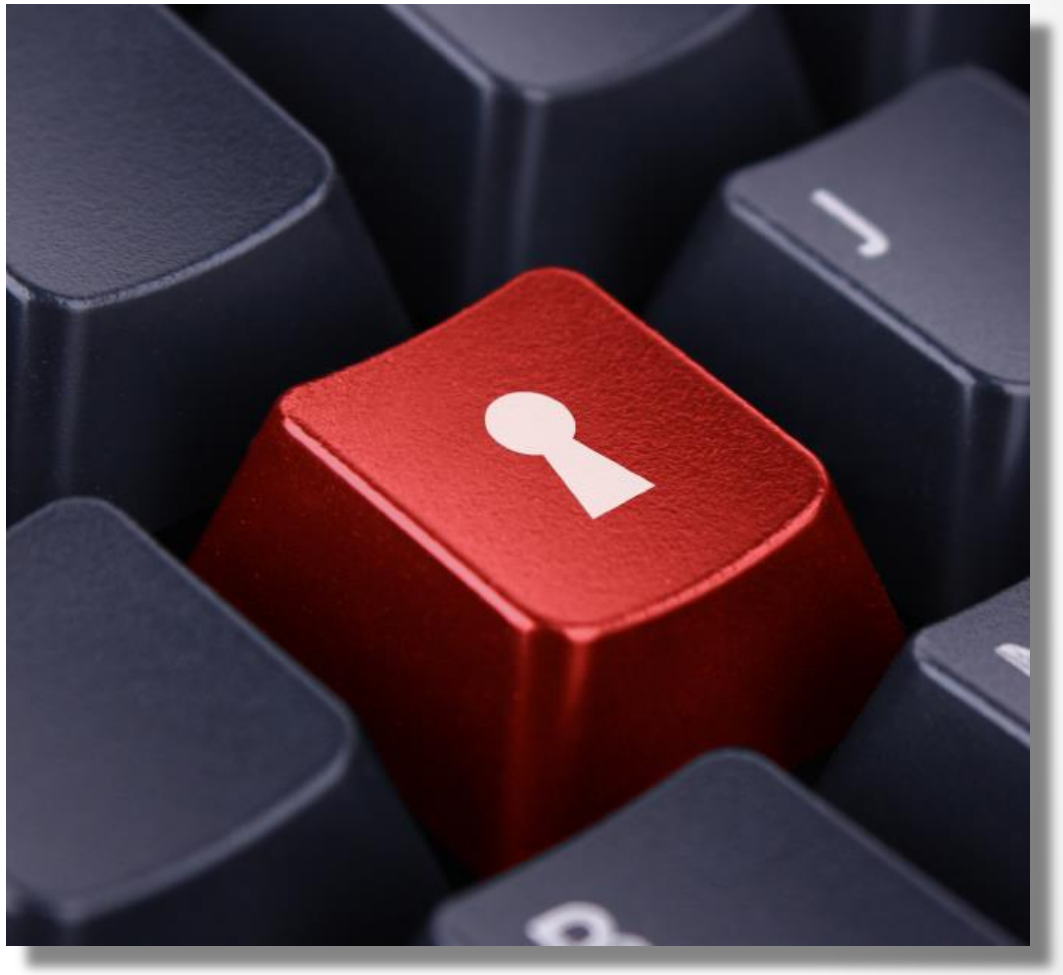
- DDOS attacks
- Dumb users
- Insiders



PRIORITIZING THE THREATS

Threats You Can Prevent (or Manage)

- Spearphishing
- Insiders (sometimes)
- Social media

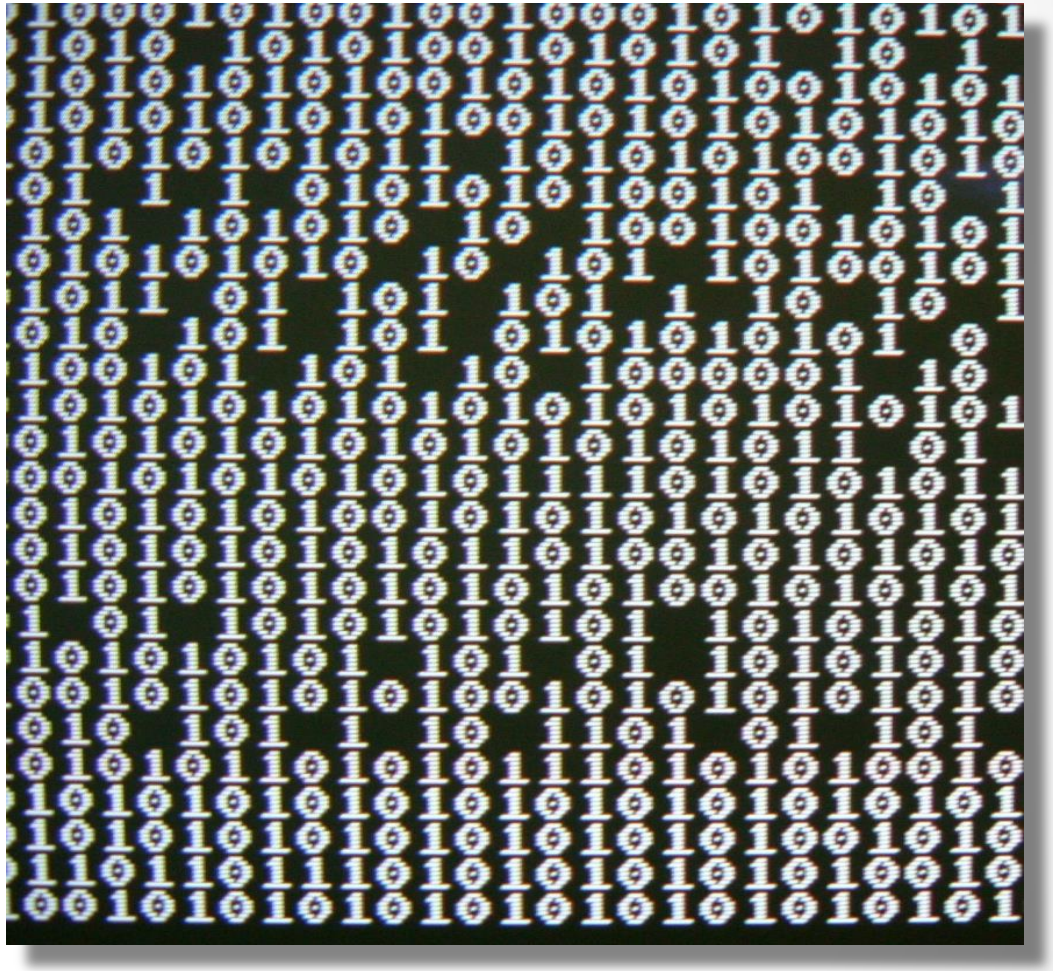


What You Need Help For

- Denial of service
- Viruses and malware
- Improper design
- Following best practices

You Can Hope to Limit Damage From

- DDOS
- Brute force
- Physical attacks (theft or loss of hardware or data)



PREVENTING A MAJOR BREACH

Know the Common Attacks

- Usually spearphishing
- Normally accompanied with some other action or attack

Prevent the Spread

- Segment your network
- Don't keep data you don't need
- Encrypt everything
- Limit access

Work Smarter

- Really train your staff
  - We’re not talking about the annual security meeting here, but real training
- Review your plans continuously
- Learn everything you can about other breaches

DETAILS OF COMMON ATTACKS

Spearphishing

- Nearly all major breaches have spearphishing as a major component
- Many also have some failure of trusted access
- Ultimately, most major breaches have a personnel failure

How a Spearphishing Attack Works

- Targeted email is received
  - Aimed at one or more specific people with desired access
- The email may contain malware, but normally does not
  - Usually has social engineering content driving action
  - The action may be clicking on a link that contains malware
  - The action is more often a way to harvest credentials
  - The social engineering is often not a key individual, but some-one at a low level with access
  - The target may also be an outsider with access (Target)
  - Spearphishing email can be very difficult to spot, with camouflaged links, etc.
- Normally, spearphishing depends on inside information, but sometimes enough data is available in public

The Victims of Spearphishing

- An unknown number of banks
- Anthem
- Sony
- Target
- ICANN
- Microsoft

Social Engineering

Social media

- Used to get people to become infected with malware
- Also used to harvest information needed for spearphishing

Watering holes

- Popular websites for professions, including social media
- May be infected with malware
- May also be used to harvest personal information

Drives/media

- Attacker will leave infected USB drives where employees can find them
- May also work with infections delivered to smartphones

Insider Threats

- Disgruntled employees
- Dissatisfied contractors
- Dumb moves

Ransomware

- Encrypts the victim's hard drive
- Demands a ransom to unlock it:
  - Normal demand is about $500 in Bitcoins
  - Normally, there's a 24-hour time limit
  - An unlock key will be provided once ransom is received
- May also lock external hard drives or network drives
- Latest encryption methods are very strong

Dealing with Ransomware

- Used to be spread by spearphishing; new methods are appearing, including file-less attacks and advertising attacks
- Good, updated anti-malware and antivirus software will usually catch it, as will updated security hardware
- Recovery is possible, if you have good backups
- Ransomware is normally run as a business enterprise

Why These Threats Are so Hard to Fight

- They frequently bypass corporate security
- Many (perhaps most) spearphishing, social engineering and Web threats are aimed at personally owned devices
- Employees are off-guard when they're not at the office
- BYOD policies can make this worse
- A typical attack goes after personal email or social media sites
- Information gathered from public sources helps make it all seem real

What You Can Do

- Take advantage of current visibility
- Use lessons of others to learn before it happens to you
- Put together a multi-discipline working group
  - This means IT, security and management need to cooperate
- Create best practices based on your organization's needs
- Where possible, allocate or add staff

Why You Care

- Avoid damage to the organization
- It's required by law, in many cases
- There may be civil consequences, in many cases
- You may get to keep your job

In Closing

- The vast majority of breaches are personnel-related
- The single most important thing you can do is to train your people:
  - This should include real-world, hands-on training
  - Training should be a required part of onboarding
  - Training should be frequent and in person
  - One-on-one training in the employee's work area is best
- Run tests to make sure your training is effective:
  - This can include simulated spearphishing
  - Simulated social media attacks are also important
- While you're at it, leave a few bait USB sticks around

QUESTIONS?