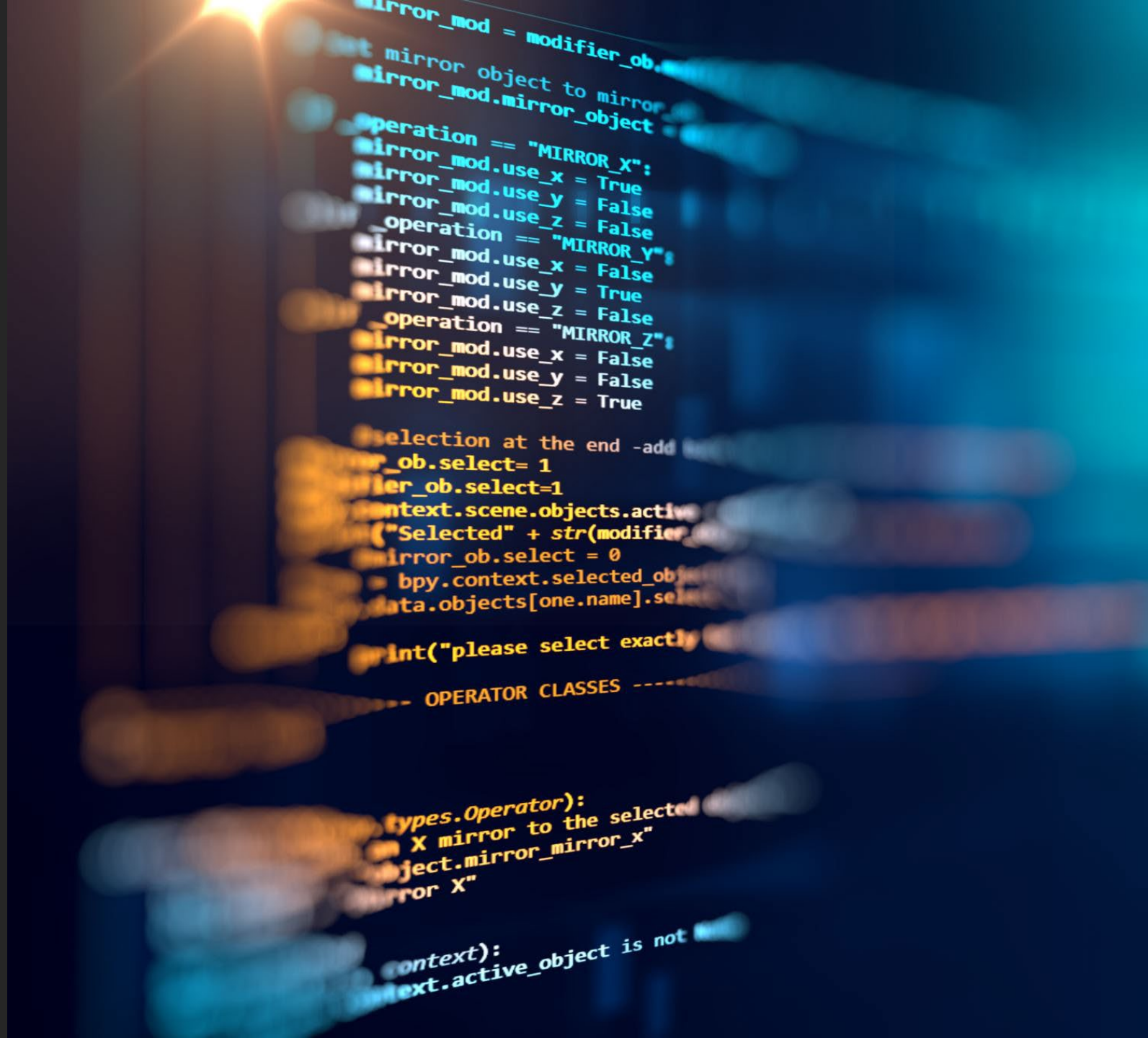
# PLANNING FOR A CYBER CRISIS

ROBERT FOX

ALCOVY RESOURCE COURT



# WHY ARE WE HERE?

## BE AFRAID. BE VERY AFRAID.

- **We're here to learn how to be better at managing and protecting program information.**
- **We have a moral and ethical responsibility to safeguard sensitive participant information.**
- **We have a professional responsibility to mitigate risk.**
- **We have a responsibility to lead in a time of 'crisis'.**
- **We want to avoid embarrassment.**
- **We want to avoid or minimize program and service disruption.**
- **We want to feel more in control.**
- **We want an easy solution to 'hacking'.**

# AUDIENCE POLL:

WHAT DO YOU FEAR THE MOST?

# INFORMATION SECURITY FAILURES

## I LOVE A GOOD HORROR STORY

- **Veteran's Administration:** 26.5 million veterans' records including personally identifying information stolen from the home of an employee who 'improperly took the material home'.
- **Boston Globe:** Exposed 240,000 records including credit card and checking account information by using recycled records for printing and wrapping newspapers for distribution.
- **GA Dept. of Community Health:** Claims contractor lost CD containing the names, DOBs, SSNs, addresses, and Medicaid numbers of 2.9 million claimants.
- **Equifax:** In 2017, the credit-monitoring agency allowed third-party software to expose the private records of 147.9 million Americans.

# WHAT IS THE GOAL?

## PROBABLY NOT WHAT YOU THINK

- **Success is not a future without information security risks or outside attacks.**
- **Success isn't even a future without being the victim of a successful attack or other information loss.**
- **Success is competent preparation, knowing what to do when things go sideways, and having an effective plan to repair the damage and move on.**
- **We're going to get there with a conceptual framework, basic information security practices, and checklists.**

# PREVENT – DETECT - RECOVER

## CONCEPTUAL FRAMEWORK SOUNDS COOL

- **Prevent**
  - Everything you do on the front end to reduce the likelihood of an information leak or the success of a random attack. Includes authentication, encryption, physical access controls, security audits, information technology policies, device protections, and a lot of sysadmin work for someone else.
- **Detect**
  - Most threat detection is out of your control. The good news is what is in your control is relatively easy. Make friends with County IT.
- **Recover**
  - The most important, controllable component – Crisis Management. The entire focus is on restoring what was lost and quickly returning to normal. The 'secret' is taking easy, measurable actions beforehand.

# PREVENT

# BEST PRACTICES

## AKA, HOW NOT TO MAKE THE NEWS

- **Identify Information Threats:**
  - Physical Access Control – How is information accessed, by whom, and how is it protected?
  - Device Security – Every device that accesses information is a target that needs to be hardened.
  - User Error – Face it, we are the worst.
- **Establish or Train on Standards:**
  - Know and adhere to your organization's IT policy.
  - Frequent training on basic security practices: passwords, authentication, document control (especially for remote workers), VPNs, communication encryption, recognizing common attacks.
- **Conduct an IT Security Audit:**
  - Once a year, go down the list. Identify areas at risk, identify what you need to improve, and identify where you need to ask questions.
  - Ask for what you need.

# WHAT IS AN IT AUDIT AND WHY DO IT?

## BASICALLY, A CHECKLIST ON STEROIDS

- **By Definition:** An official inspection and accounting of your IT assets – physical and digital.
- **Purpose:** Know what you have, what you need, what works, and what's broken. Take a large problem and break it into simple problems.
- **Physical Audit:** See Handout 1. Most of these things are already taken care of by your county or court, you're looking for glaring, obvious holes or smaller gaps unique to your program.
- **Digital Audit:** See Handout 2. In reality, all of the high-level network security is someone else's job. Your goal is to understand your backup, redundancy, and recovery assets, and to identify additional ways to safeguard your critical information.
- **End Result:** You have a list of needs and problems that will guide your recovery planning. Not too big, not too small… just right.

# DETECT

# DETECTION

## DANGER, WILL ROBINSON

- **Network Threat Detection –** Not our problem. What you can do is make sure your sysadmin has an accurate picture of who should be accessing your digital information, when, and from where.
- **Common Sense Detection –** Do you know where your physical files are, would you recognize tampering or theft? Do you know what your digital assets should look like, do you know who has access and why?
- **Have I Been Hacked? –** You'll know because you'll see something like this:

SOLERA NETWORKS

DeepSee | Capture | Statistics | Settings | Profile | Log Out

THE FIREWALL OF THE UNITED STATES

# COMPUTER BLOCKED

This computer has been blocked to Americans by the US Goverment Firewall

**ALL ACTIVITY OF THIS COMPUTER HAS BEEN RECORDED**

**If you use webcam, videos and pictures were saved for identification. You can be clearly identified by resolving your IP address**

**Illegally downloaded material (audio, videos or software) has been located on your computer**

By downloading, those were reproduced, thereby involving a criminal offense under Section 106 of Copyright Act.

The downloading of copyrighted material via the Internet or music sharing networks is illegal and is in accordance with Section 106 of the Copyright Act subject to a fine or imprisonment for a penalty of up to 3 years.

Furthermore, possession of illegally downloaded material is punishable under Section 184 paragraph 3 of the Criminal Code and may also lead to the confiscation of the computer, with which the files were downloaded.

To perform the payment, enter the acquired **GreenDot MoneyPack** code in the designated payment field and press the „OK" button.

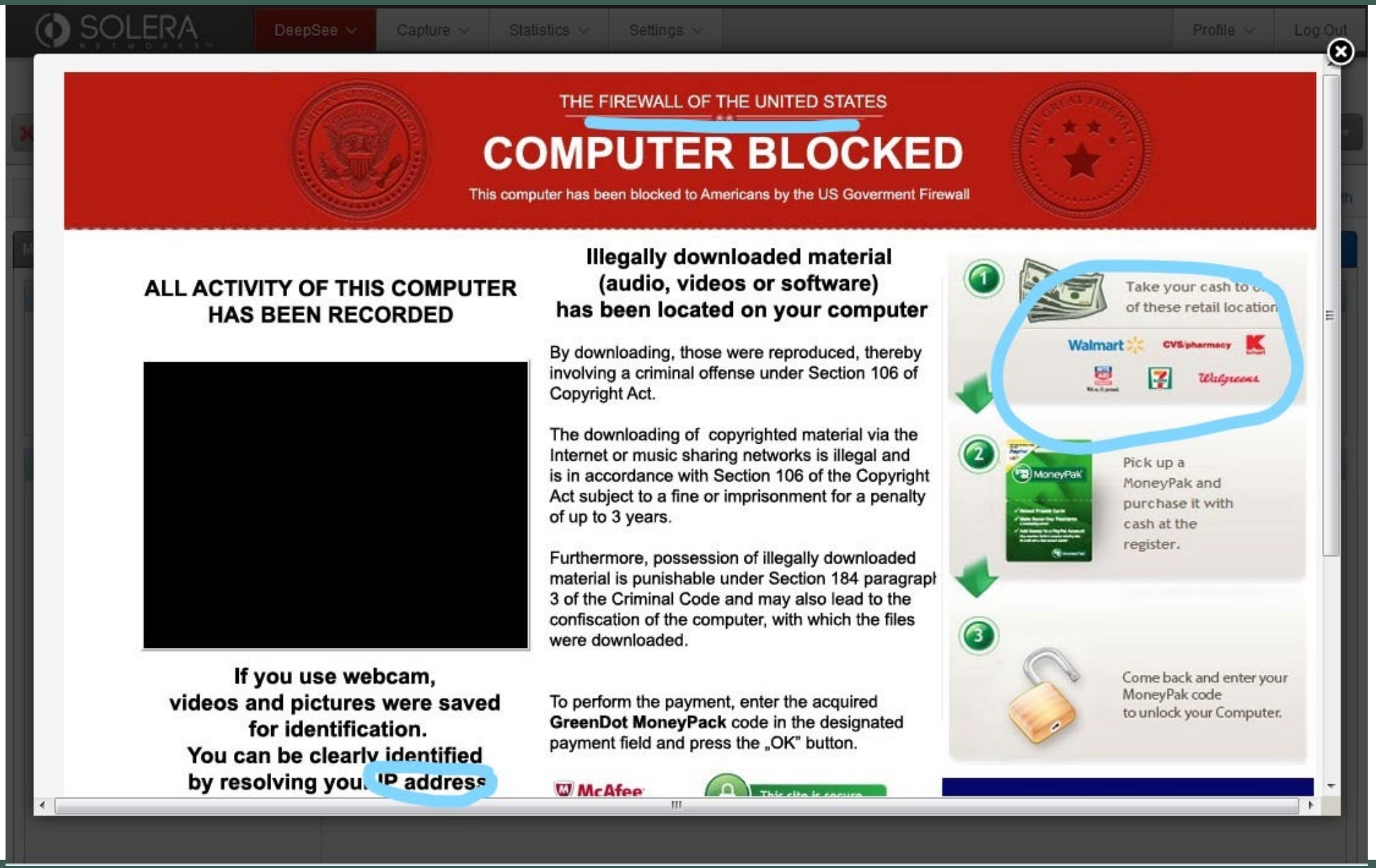
McAfee

1. Take your cash to one of these retail locations:

Walmart | CVS pharmacy | Walgreens

2. Pick up a MoneyPak and purchase it with cash at the register.

3. Come back and enter your MoneyPak code to unlock your Computer.


SOLERA
DeepSee
Capture
Statistics
Settings
Profile
Log Out
THE FIREWALL OF THE UNITED STATES
COMPUTER BLOCKED
This computer has been blocked to Americans by the US Goverment Firewall
ALL ACTIVITY OF THIS COMPUTER HAS BEEN RECORDED
If you use webcam, videos and pictures were saved for identification.
You can be clearly identified by resolving your IP address
Illegally downloaded material (audio, videos or software) has been located on your computer
By downloading, those were reproduced, thereby involving a criminal offense under Section 106 of Copyright Act.
The downloading of copyrighted material via the Internet or music sharing networks is illegal and is in accordance with Section 106 of the Copyright Act subject to a fine or imprisonment for a penalty of up to 3 years.
Furthermore, possession of illegally downloaded material is punishable under Section 184 paragraph 3 of the Criminal Code and may also lead to the confiscation of the computer, with which the files were downloaded.
To perform the payment, enter the acquired GreenDot MoneyPack code in the designated payment field and press the „OK" button.
McAfee
Take your cash to
of these retail location
Walmart
CVS pharmacy
Walgreens
MoneyPak
Pick up a MoneyPak and purchase it with cash at the register.
Come back and enter your MoneyPak code to unlock your Computer.

# RECOVER

# RECOVER, PART 1

## CRISIS MANAGEMENT THROUGH CHECKLISTS

- **Only Concerns:** What did we lose, who does it harm, and how to we get it back?
- **Step One – Stop the Bleeding:**
  - Make sure the threat, whatever it is, is over and the vulnerability is fixed.
  - Know who is responsible for recovery process. That person should clearly communicate the plan to everyone affected.
- **Step Two – Document the Damage:**
  - Assume all compromised devices are bricked.
  - Check integrity of backups, identify the date of the last full backup/redundancy.
  - Identify all services that are affected. In our world, this could range from everything to almost nothing. First focus should be on service delivery to participants, second program operations and obligations, last is everything that makes your job easier.

# RECOVER, PART 2

## CRISIS MANAGEMENT THROUGH CHECKLISTS

- **Step Three – Repairing the Damage:**
  - Should be careful, thorough, and involve the IT department.
  - Replace or remediate devices, most likely through a factory wipe and restore process.
  - Use your critical items list to identify any items missed by a backup and plan for how to restore or recreate them. This is where most organizations fail in the prevention stage, and remediation is timely and expensive.
  - Roll out the critical items to key users one at a time in an organized manner. IT may control this process.
- **Step Four – Conduct a New Audit:**
  - At this point, you should have a pretty good idea of what worked and what didn't.
  - Update your checklists and plans accordingly.
  - Gloat over a job well done!

# CONTACT INFO

Robert Fox
rfox@co.newton.ga.us
678-209-3618