

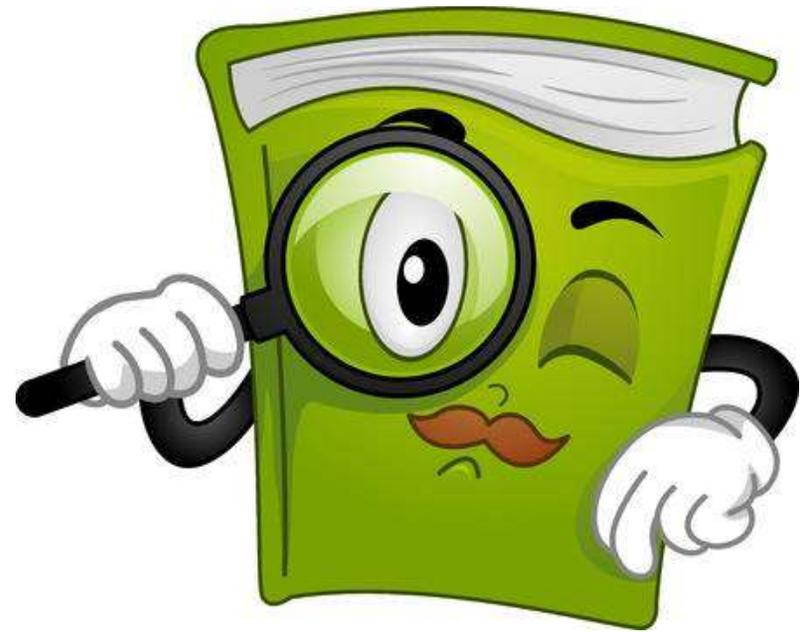
# Cyber Security



Presented by GC Information Systems  
August 13, 2019

Image Reference: <https://www.eweek.com/security/why-u.s.-firms-are-less-cyber-secure-than-they-think>

Want to read  
more about  
this topic?



Click here to view the Huddle Minutes:

<https://greencountymo.gov/dashboard/huddle/recap.php>

It's cheaper than ever to buy someone's stolen identity off the internet

BlueCross BlueShield hack may have exposed data for 10 million customers

Apr 7, 2016 at 4:12 PM

## Snapchat Hacked: Employee Payroll Details Leaked Following Phishing Scam

ON 02/29/16 AT 4:40 AM

02 Computer Virus Cripples UK Hospital System

NOV 16

## Hackers stole over 43 million Last.fm accounts in 2012 breach

September 1, 2016

IRS Caught Over 30,000 Tax Returns Involving ID Theft

WASHINGTON, D.C. (APRIL 21, 2016)

How one rent-a-botnet army of cameras, DVRs caused Internet chaos

10/25/2016, 3:45 PM

## Yahoo discovered hack leading to major data breach two years before it was disclosed

November 10

NOV 16, 2016 @ 08:12 AM

Mark Zuckerberg Hacked For The Third Time This Year

**Information**

**=**

**\$ \$ \$**

FREE

UKULELE

100

## ROYALTY FREE MUSIC STUDIO

CORPORATE UKULELE  
100 FREE DOWNLOAD -  
ROYALTY FREE MUSIC |  
HAPPY POSITIVE  
BUSINESS



Please support the artist to unlock your download

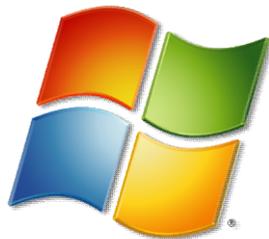
Email address

NEAT

By providing your email address, you agree that your email address will be shared with the author of this download and that you may receive emails from the author and Hypeddit.

You can withdraw your consent at any time by unsubscribing from any emails received.

**Anything or Anyone that  
connects to the Internet is  
a possible target**



# **Types of Attack**

**Targeted vs Opportunistic**

# **Public Sector**

**Public sector ransomware attacks  
are trending up**

53 known attacks in 2018

21 known public-sector attacks as of April

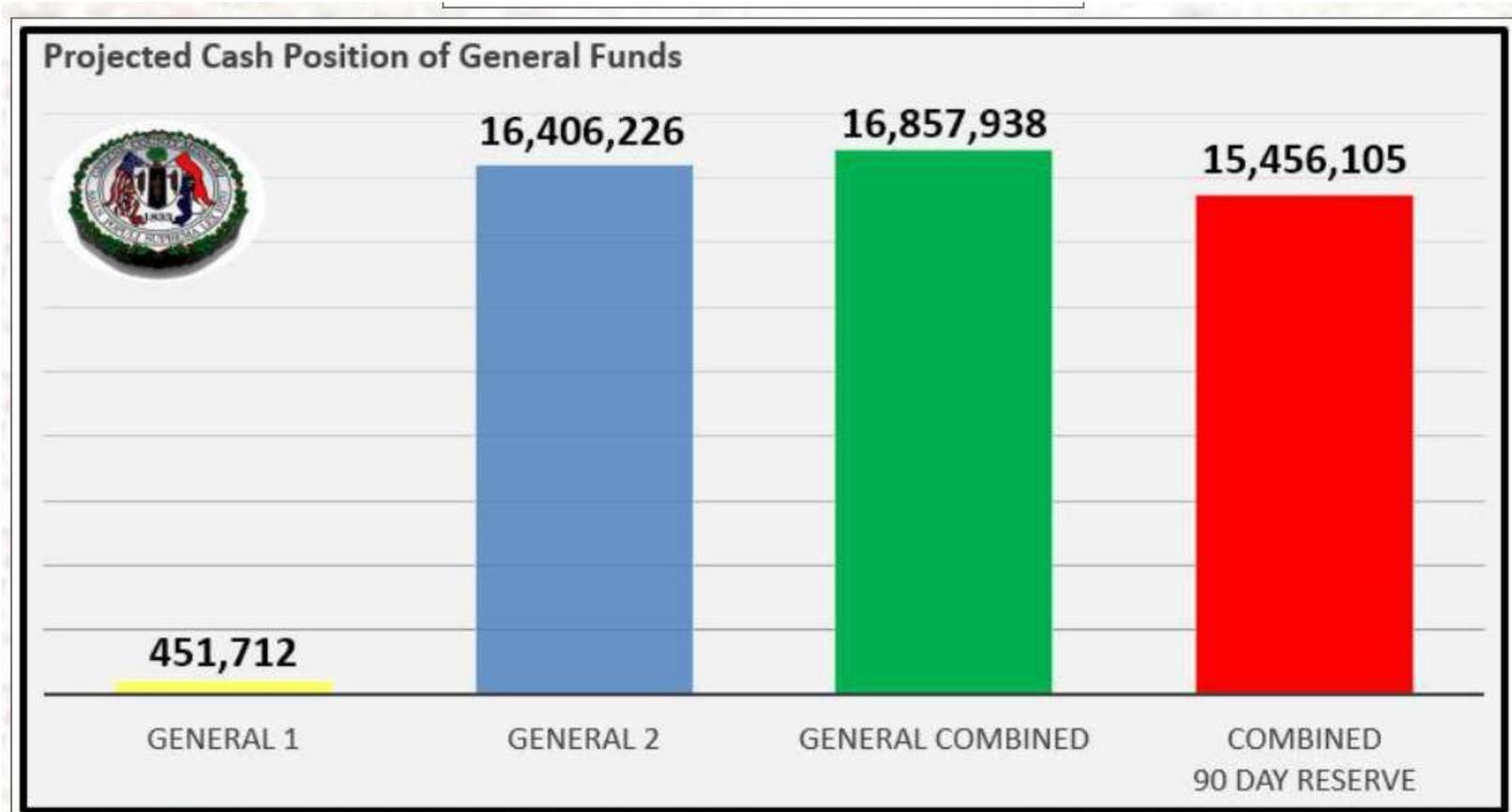
# **Ransomware**

## **Paying the ransom:**

Public sector victims paid an average of \$338,700, which is ten times more than the average paid by the private sector

**You still have to rebuild the network!**

# Ransomware



# **Ransomware**

## **Not paying the ransom:**

Atlanta – \$17 million

Baltimore – \$18.2 million

Imperial County, CA – \$1.6 million

# **Not just Ransomware**

## **Average cost of data breach:**

For public sector organizations specifically, the total average cost of a data breach was **\$2.3 million**, with an average cost of **\$75 per record**

**-Ponemon Institute 2018 study**

# **Not just Ransomware**

## **Latest estimates for us:**

\$2 million... Just to purchase credit monitoring!

## **Local example:**

Small breach of 1000 records at local LEA cost over \$100,000

# **We are a target**

**We block on average 1400  
Malicious connections and  
Intrusion attempts every day**

# **You are a target**

**Leadership – your face is on the website  
and everyone wants to land a whale**

**Anyone with a phone or email**

# **Tactics**

# Phishing

Over 90 percent of significant breaches involve phishing attacks

-Michael Roling

Former State of Missouri CISO

# Phishing Messages Are:

- Email
- Texting
- Chat/IM
- Phone Calls aka Vishing
- Facebook/Social Media posts/messages
  - Forum/Article comments
  - Traditional Mail
- ANY communication, including face-to-face

# **How do they Phish effectively?**

## Social Engineering

- Confident
- Friendly/Helpful
- Make it personal
- Do their homework

# File Types Used:

Know which common file extensions are likely safe ✓ and which can be harmful ✗:

✓ .jpg	✗ .exe	✗ .scr
✓ .png	✗ .msi	✗ .pif
✓ .pdf	✗ .bat	✗ .reg
✓ .docx	✗ .com	✗ .js
✓ .xlsx	✗ .cmd	✗ .vbs
✓ .pptx	✗ .hta	✗ .wsf
	✗ .cpl	✗ .jar

# Tailgating

Tailgating, sometimes referred to as piggybacking, is a physical security breach in which an unauthorized person follows an authorized individual to enter a secured premise.

# Recent Incidents:

- Social Engineering: compromised County account to order hardware
- Social Engineering: fake tech support call; remote access
  - Social Engineering: Payroll attack
- Compromised accounts: Typically data breaches elsewhere

# People-centric Cybersecurity Strategy

Our people are your greatest ~~risk~~ asset;  
use them!

# What can we do right now?

- **Training** – We will come to you!
- **Trust but verify** – Social Engineering killer; make it a process
- **Automatic Lock Screens** – Don't leave things unattended
- **Standard User Accounts** – Mitigates over 80% of Microsoft vulnerabilities (BeyondTrust, Microsoft Vulnerabilities Report 2019)
- **Passphrases** – Easy to remember, super secure
- **Security Updates** – Don't postpone me
- **Attachments** – if there's doubt, there is no doubt
- **If concerned, don't be embarrassed to ask**