End User Cyber Security Training

By Jason Clause
IT Consultant
Endsight

A bit about me

Jason Clause

East Bay IT Consultant

San Francisco Bay Area

Information Technology and Services

500+
connections

Current	Endsight, The Jason Clause Show
Previous	Bravo! Marketing
Education	Kent State University
Recommendations	**14** people have recommended **Jason**
Websites	Podcast

LinkedIn iTunes

endsight Microsoft

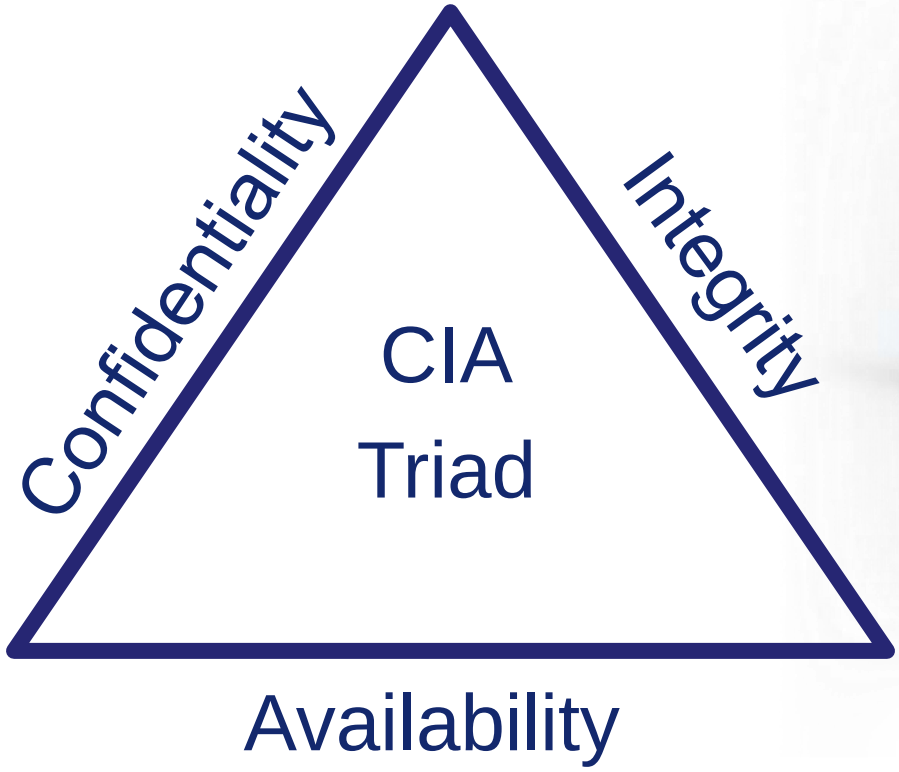
endsight

Survey Question: What is Cyber Security / IT Security?

1. Keeping sensitive information protected.
2. Protecting against malicious attacks on a computer system.
3. Assuring the validity of information.
4. All of the above

Answer: All of the above

A comprehensive plan includes:



- **Policy / Leadership**
- **Technology**
- **People**

endsight

Cybercrime is criminal activity involving the internet, a computer system, or computer technology.

http://news.microsoft.com/stories/cybercrime/index.html

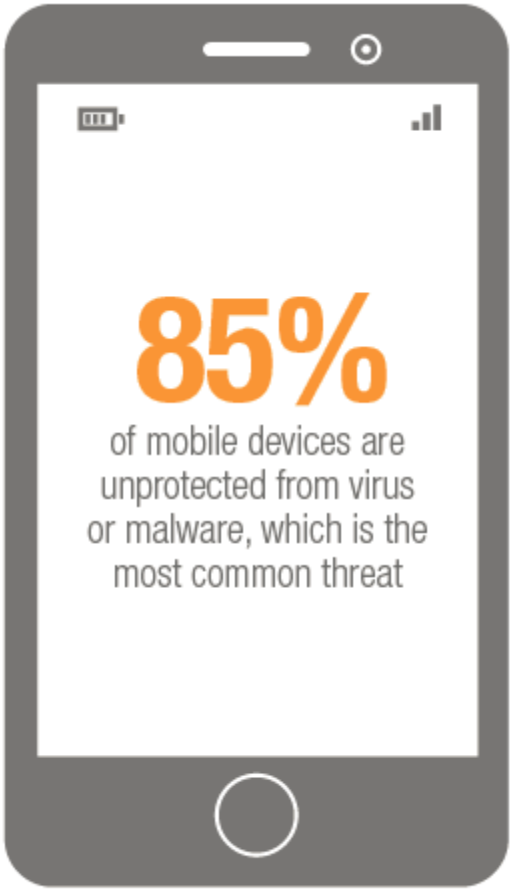
93 PERCENT OF ALL MONEY IS DIGITAL. THAT'S WHAT IS AT RISK HERE. –BILL NELSON

Bill Nelson, Financial Services Information Sharing & Analysis Center


Microsoft
40%
of small and medium-sized businesses that manage their own security will have their networks accessed by an attacker.

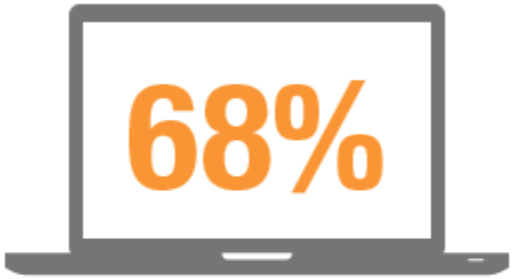

50%
of them won’t even know they were attacked.

endsight



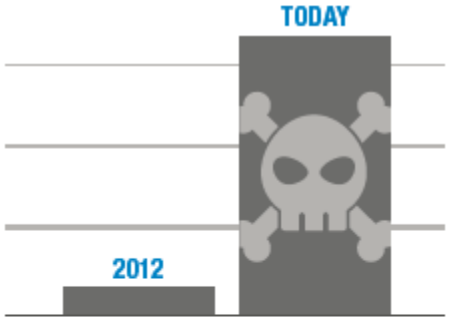
85%

of mobile devices are unprotected from virus or malware, which is the most common threat

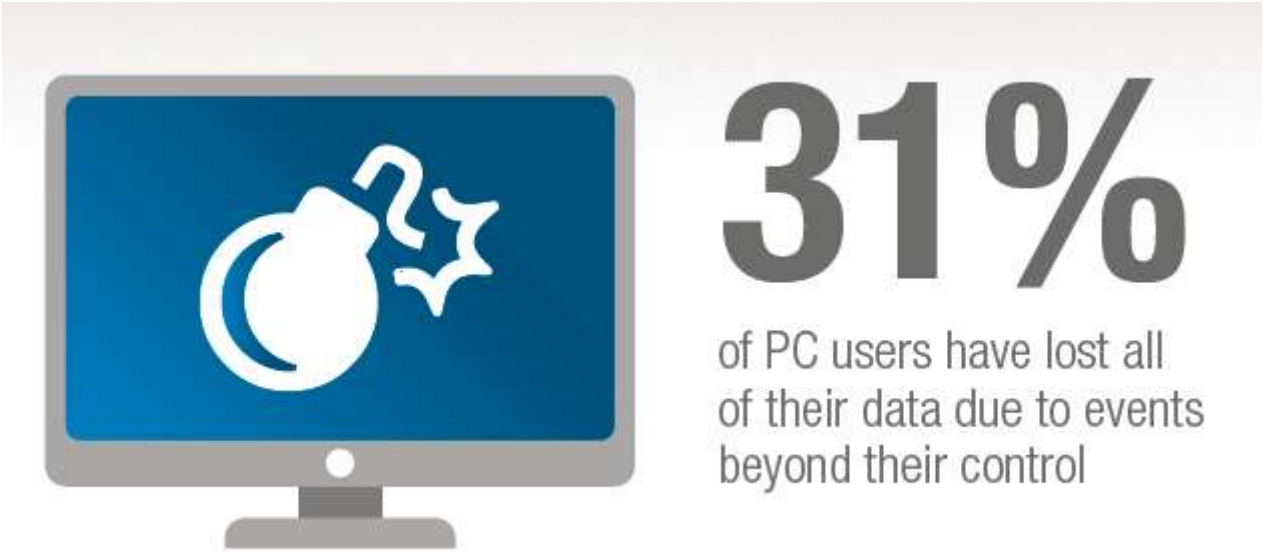


68%

of U.S. companies permit employee-owned devices in the workplace



400% jump in mobile malware since 2012


31%
of PC users have lost all
of their data due to events
beyond their control

endsight

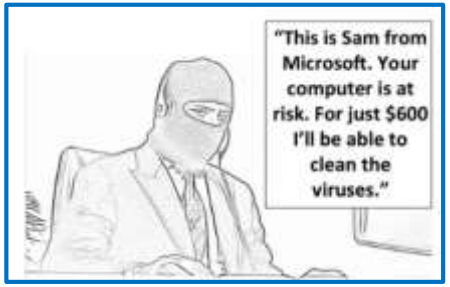

78%
of malware cyber espionage is related to email attachments

endsight

The cybercrime problem is broad

and getting worse

- More professional cybercrime services make it easier for would-be attackers to become cybercriminals
  - Many cybercriminals don't need technical abilities when entering the world of cybercrime
- In many regions, it is socially acceptable to steal from victims on the Internet



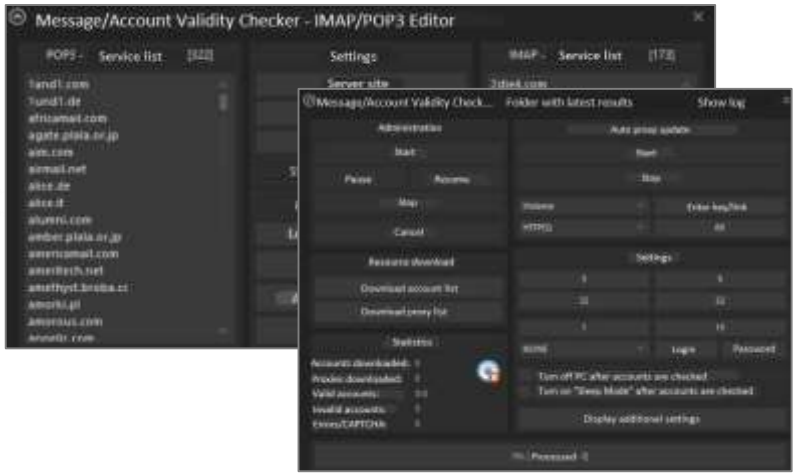
It has never been easier for new entrants into the market

Example of crimekits and services

Remote Control Trojan (RAT)

Chinese tool **Phone Remote Management. It is** used to remotely control Android devices. It can remotely monitor and control many of the features on a user's mobile device from anywhere on the Internet

Account Checkers



Russian checker **Private Keeper**. It is a universal checking tool supporting 17 different web services (PSN, PayPal, Skype, Twitter, etc.) and many email providers. It has an IMAP/POP3 server editor that supports "almost any email service" and allows users to parse the content of messages and check email accounts validity

Sources: Various

endsight

The Many Types of Security Threats

Antivirus, malware scanners, threat detection… there is no one solution to all these threats:

- Malware
- Spyware
- Adware
- Phishing
- Data Theft
- Trojans
- Viruses
- Password Hacking
- Vulnerability Scanners
- Packet Sniffers

endsight

Ransomware

The Growing Enemy of Businesses

- Over 500,000 businesses* have been hit by ransomware
- Once hit, the only way to get rid of it is to pay the ransom
- Criminals are constantly developing new techniques to attack businesses


• Patch management
• Policy enforcement
• DNS filtering
• Encryption
• Anti-virus
• SPAM filtering
• Data backup
• Reactive support
• Long term planning

endsight

Tips to keep you safe

endsight

Nelson Mandela walks into this room right now and offers you this glass of water….

Will you accept it?

endsight

This man walks into this room right now and offers you this glass of water....

Will you accept it?

endsight

Were you checking the water or the person serving the water?

People decide what is good and what is bad based on “trust”
Perception is influenced by Trust

endsight

"I can't always do things right. But I can always try to do the right things."

endsight


To better protect your users we've compiled a security 101 checklist in the following key areas:
Password security
Email security
Web browser security
Smartphone security
Workstation security
Network security
Personal & "social" security

endsight

PASSWORD SECURITY

- Never share your password with anyone, ever
- Use a passphrase (a short sentence that's easy to remember) instead of a password
- Combine your passphrase with two-factor authentication

endsight

Create strong passwords

Which passwords are strong?

Title Here

Subtitle Here

$w0rd

STRONG

My son Aiden is three years old in December

endsight

Strong passwords are not enough

Protect your accounts and passwords

- Use unique passwords for different websites
- Limit use of corporate e-mail accounts as your identifier on third-party website

Endsight has a video on how to create strong passwords:

https://youtu.be/UnmdxReVoNc

endsight

EMAIL SECURITY

- Never respond to an email from strangers
- Don't open any attachments that you haven't scanned first
- Don't open any links you haven't checked (hint, hover over the link to ensure it's really going where it's supposed to go)
- Always back up your email

endsight

Don’t be tricked into downloading malware


AO 88(Rev. 11/94) Subpoena in a Civil Case

Issued by the
UNITED States District Court

Issued to: Michael Krause
Northwind Traders
387-555-1212

SUBPOENA IN A CIVIL CASE
Case Number: 28-755-YCM
United States District Court

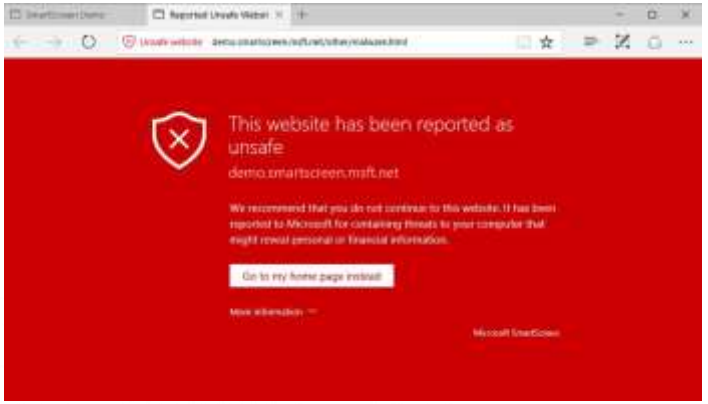
YOU ARE HEREBY COMMANDED to appear and testify before the Grand Jury of the United States District Court at the place, date, and time specified below.

Place: United States Courthouse
880 Front Street
San Diego, California 92101

Date and Time: May 7, 2011
9:00 a.m. PST

Room: Grand Jury Room

- Use malware and phishing protection in their browsers.
- Keep Antivirus on and updated



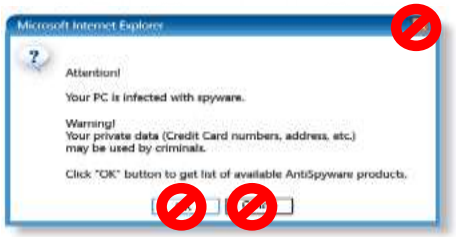
endsight

WEB BROWSER SECURITY

- Only install from safe sources (hint, the vendor's download site or your browser's add-in store)
- Look for the lock and ensure you see the icon before entering your personal information into a website
- Save and sync selectively when asked "Would you like to store this password?" The best answer is NO.
- If you log in then you should also log out - always
- Clear and back up everything

endsight

Don’t be tricked into downloading malware



endsight

SMARTPHONE SECURITY

- Always use a lock screen - every smartphone and tablet have one. Use it.
- Nobody should ever borrow your smartphone
- Don't respond to a text from a stranger
- Don't answer calls from strange phone numbers - it's better to screen these calls. Let voicemail handle it.
- Back up everything

endsight

WORKSTATION SECURITY

- Use an active security suite, aka an antivirus program to protect your system from viruses such as malware, spyware, and network attacks
- Update your software - keep your operating system, security suite, and programs up-to-date
- Leave it? Lock it. Don't leave your system logged in and unattended
- Don't share your system with anyone unless specifically told by your IT team
- Back up your data

endsight

NETWORK SECURITY

- Never connect to Wi-Fi that you don't own
- Don't connect to Wi-Fi without a password
- Always use a firewall
- Always use SSL in your web browser

endsight

Guard company data when you're on the go

- Connect securely
  - Save sensitive activities for trusted connections
- Confirm the connection HLTONHOTELS.NET
- Encrypt storage on mobile devices
- Flash drives: watch out for unknowns and disable auto run

endsight

PERSONAL & "SOCIAL" SECURITY

- Don't talk to strangers online
- Only give out data on the phone calls that you started
- Watch your back - literally. Be aware of your surroundings when in public and logged on to your computer
- Everybody you just met is a stranger, no matter what they claim to "know" - the best advice for online and in person as well.

endsight

Social Engineering

Phishing

- Attacker sends a generic email to millions of people
- The goal is to trick them into doing something
  - Opening an infected attachment
  - Visiting a malicious website.

Spear Phishing

- Attacker sends a custom email targeting a very small, select number of people.
- Emails are extremely realistic looking and hard to detect.
- They often appear to come from someone you know. (Like your boss)
- They may use your industry's jargon
- Often create a tremendous amount of urgency

How to evade scams

- Look for telltale signs www.snopes.com
- Think before you Link
- Keep sensitive information private
- Identify socially engineered attacks
  - Unreasonable urgency
  - Secrecy
  - Signature not quite right
  - Tone that just doesn't seem right
  - Using a correct but unfamiliar name or nickname
- When in doubt, pick up the phone
- Scrutinize any attempt to bypass security policies or procedures.

endsight

Use two local accounts

Local User Account

- Daily use account - does not have permission to install software on the local machine

Local Admin Account

- Local Admin - has permission to install software on the local machine

Thank You!

Jason Clause
510-823-4604
jclause@endsight.net
https://www.linkedin.com/in/jasonclause/
www.jasonclause.com

endsight