

The background is a dark blue gradient with a complex pattern of white and light blue circular and linear elements. On the left side, there is a large circular scale with numerical markings from 140 to 260 in increments of 10. Several concentric circles and dashed lines with arrows are scattered across the background, suggesting a technical or data-related theme.

IT SECURITY FOR LIBRARIES PART 1: SECURING YOUR LIBRARY

BRIAN PICHMAN | EVOLVE PROJECT

AGENDA

- A high level overview of what to implement in your library to make it secure. With the rise of data breaches, identity theft, malicious hacking, it is important to implement measures to protect your patrons and staff.
- Topics/Agenda:
 - * Learn the "technical jargon" of IT Security
 - * Understand a typical network environment (infrastructure) and the tools needed to help with security
 - * Identify components of building a Security Plan
 - * Learn how to teach others to provide greater data and asset security in your library

Data Breaches by Industry



Healthcare

27%

263 INCIDENTS



Other

16%

159 INCIDENTS



Government

14%

137 INCIDENTS



Financial

12%

118 INCIDENTS



Education

11%

102 INCIDENTS



Retail

11%

102 INCIDENTS



Technology

9%

90 INCIDENTS

DATA RECORDS COMPROMISED IN FIRST HALF OF 2016

554,454,942

3,046,456
records lost or stolen
every day



126,936
records
every hour



2,116
records
every minute



35
records
every second



THE COSTS OF BREACHES

- This year's study found the average consolidated total cost of a data breach grew from \$3.8 million to \$4 million. The study also reports that the average cost incurred for each lost or stolen record containing sensitive and confidential information increased from \$154 to \$158

[IBM 2016 <http://www-03.ibm.com/security/data-breach/>]

• Data Breached Companies Experience...

- People loose faith in your brand
 - Loss in patrons
- Financial Costs
 - Government Requirements, Penalties, Fees, etc.
 - Sending of Notifications
 - Payment of Identity Protection or repercussions.

- Business Continuity



<https://betanews.com/2016/02/10/the-economic-cost-of-being-hacked/>

WHY DO PEOPLE ATTACK?

- Financial Gain
 - Stocks
 - Getting Paid
 - Selling of information
- Data Theft
 - For a single person
 - For a bundle of people
- Just Because
 - Malicious





YOU CAN ONLY MITIGATE RISK...NEVER PREVENT ALL RISK

Understanding your network and evaluating their risks; allows you to build plans around mitigating risk. You can never remove all risk. You aren't "un hackable"

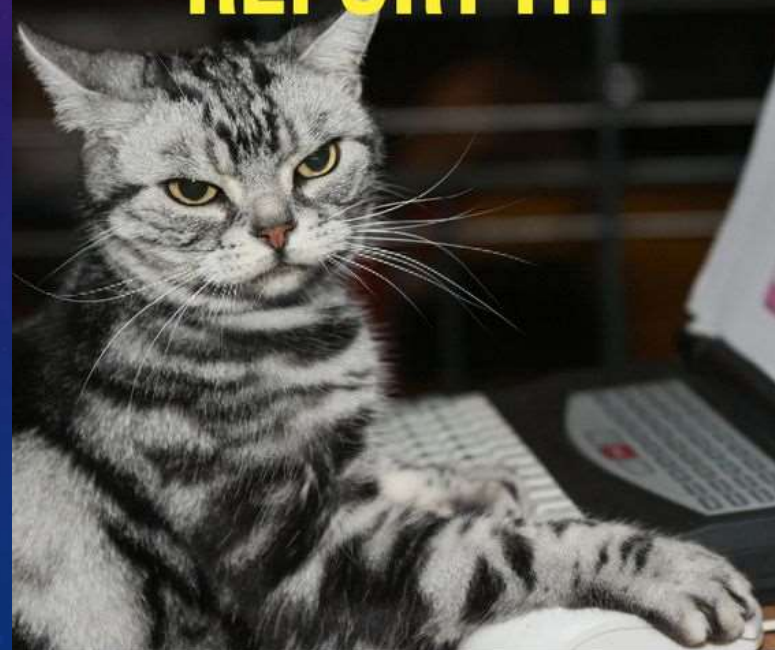
SO WHAT DO YOU NEED TO PROTECT?

- Website(s)
- ILS
- Staff Computers
 - And what they do on them
- Patron Computers
 - And what they do on them
- Network
 - And what people do on them
- Stored Data, Files, etc.
- Business Assets
- Personal Assets
-anything and everything that is plugged in...

YOU **CLICKED** ON THAT PHISHING LINK?
THIS DISPLEASES **SECURITY CAT**

BUT REMEMBER, IF YOU'VE MADE A MISTAKE

DON'T PANIC
REPORT IT!





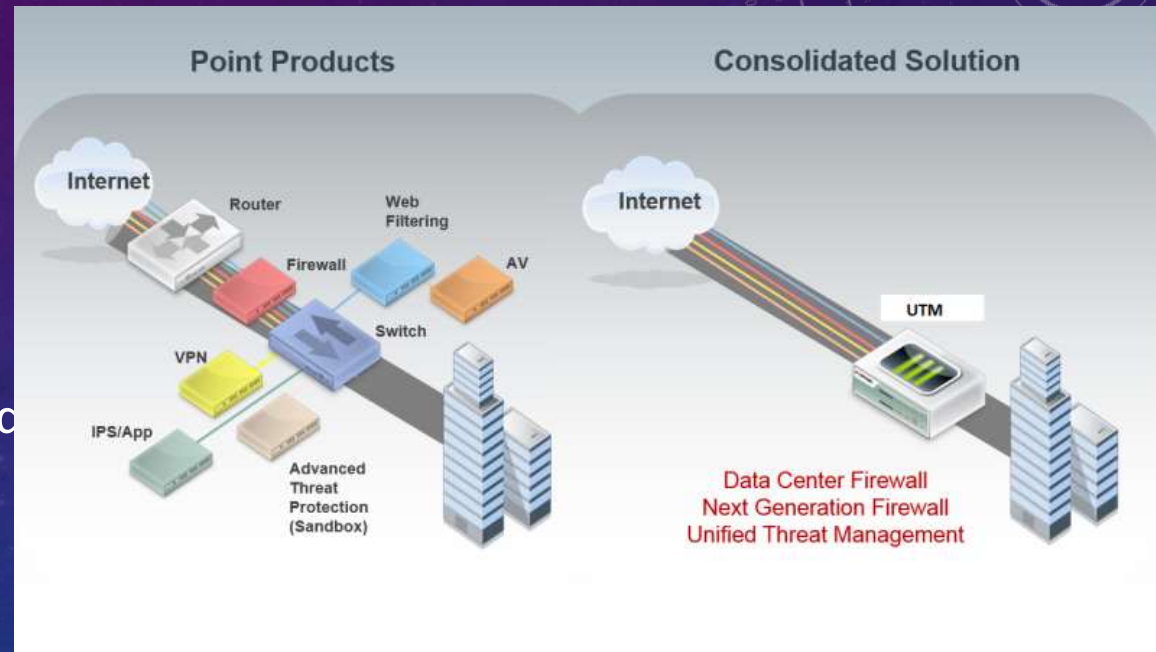
OUTER DEFENSES (ROUTERS/FIREWALLS)

- Site to Site Protection (Router to Router or Firewall to Firewall)
 - Encrypted over a VPN Connection
- Protection With:
 - IDS
 - IPS
 - Web filtering
 - Antivirus at Web Level
- Protecting INBOUND and OUTBOUND



UNIFIED THREAT MANAGEMENT

- Single Device Security
- All traffic is routed through a unified threat management device.



AREAS OF ATTACK ON OUTER DEFENSE

External Facing Applications

- Anything with an “External IP”
 - NAT, ONE to ONE, etc.
- Website
- EZProxy Connection
- Custom Built Web Applications or Services

Internal Applications

- File Shares
- Active Directory (usernames / passwords)
- Patron Records
- DNS Routing
- Outbound Network Traffic
 - Who is going where

ATTACKS

- Man in the Middle
 - Sitting between a conversation and either listening or altering the data as its sent across.
 - DNS Spoofing (<https://null-byte.wonderhowto.com/how-to/hack-like-pro-spoof-dns-lan-redirect-traffic-your-fake-website-0151620/>) set up a fake website and let people login to it.
- D/DoS Attack (Distributed/Denial of Service Attack)
 - Directing a large amount of traffic to disrupt service to a particular box or an entire network.
 - Could be done via sending bad traffic or data
 - That device can be brought down to an unrecoverable state to disrupt business operations.
- Sniffing Attacks
 - Monitoring of data and traffic to determine what people are doing.

- 01 - Information Gathering
- 02 - Vulnerability Analysis
- 03 - Web Application Analysis
- 04 - Database Assessment
- 05 - Password Attacks
- 06 - Wireless Attacks
- 07 - Reverse Engineering
- 08 - Exploitation Tools
- 09 - Sniffing & Spoofing
- 10 - Post Exploitation
- 11 - Forensics

Status	IP address	MAC address	Packets->	<-Packets	MAC address	IP address
poisoning	172.16.0.7	0022F849E288	2077	1620	002482BC1AAE	172.16.0.1

Status	IP address	MAC address	Packets->	<-Packets	MAC address	IP address
Full-routing	172.16.0.7	0022F849E288	40	41	002482BC1AAE	202.43.206.29
Full-routing	172.16.0.7	0022F849E288	46	50	002482BC1AAE	203.84.200.39
Full-routing	172.16.0.7	0022F849E288	6	4	002482BC1AAE	121.101.152.190
Full-routing	172.16.0.7	0022F849E288	24	14	002482BC1AAE	121.101.158.176
Full-routing	172.16.0.7	0022F849E288	237	344	002482BC1AAE	125.252.226.25
Half-routing	172.16.0.7	0022F849E288	4	0	002482BC1AAE	67.195.160.76
Full-routing	172.16.0.7	0022F849E288	2	1	002482BC1AAE	125.252.226.43
Full-routing	172.16.0.7	0022F849E288	5	4	002482BC1AAE	121.101.146.179
Full-routing	172.16.0.7	0022F849E288	10	9	002482BC1AAE	216.155.207.26
Full-routing	172.16.0.7	0022F849E288	5	4	002482BC1AAE	125.252.226.9
Full-routing	172.16.0.7	0022F849E288	40	37	002482BC1AAE	203.197.174.86
Full-routing	172.16.0.7	0022F849E288	3	4	002482BC1AAE	69.63.176.195
Full-routing	172.16.0.7	0022F849E288	21	24	002482BC1AAE	203.197.174.79
Full-routing	172.16.0.7	0022F849E288	79	63	002482BC1AAE	209.85.231.100
Full-routing	172.16.0.7	0022F849E288	22	28	002482BC1AAE	209.85.231.104
Full-routing	172.16.0.7	0022F849E288	58	59	002482BC1AAE	125.252.226.90
Full-routing	172.16.0.7	0022F849E288	28	31	002482BC1AAE	209.85.231.156
Full-routing	172.16.0.7	0022F849E288	70	70	002482BC1AAE	209.85.231.164
Full-routing	172.16.0.7	0022F849E288	7	4	002482BC1AAE	174.133.21.134
Full-routing	172.16.0.7	0022F849E288	194	204	002482BC1AAE	125.252.226.82
Full-routing	172.16.0.7	0022F849E288	11	5	002482BC1AAE	125.252.226.89
Full-routing	172.16.0.7	0022F849E288	7	6	002482BC1AAE	84.124.194.51
Full-routing	172.16.0.7	0022F849E288	75	73	002482BC1AAE	64.174.194.10

Filter: tcp.stream eq 67

No.	Time	Source	Destination	Protocol	Length	Info
1036	9.243917	192.168.1.77	173.194.33.41	HTTP	758	G
1046	9.258497	173.194.33.41	192.168.1.77	HTTP	430	H
1048	9.258920	192.168.1.77	173.194.33.41	HTTP	1120	G
1059	9.273910	173.194.33.41	192.168.1.77	HTTP	430	H
1096	9.473301	192.168.1.77	173.194.33.41	TCP	54	6
2307	29.191953	192.168.1.77	173.194.33.41	TCP	1484	[
2308	29.191961	192.168.1.77	173.194.33.41	HTTP	55	G
2309	29.210835	173.194.33.41	192.168.1.77	TCP	60	H
2310	29.211104	173.194.33.41	192.168.1.77	HTTP	430	H
2374	29.411299	192.168.1.77	173.194.33.41	TCP	54	6

Frame 1036: 758 bytes on wire (6064 bits), 758 bytes captured (6064 bits) on interface 0
 Ethernet II, Src: Msi_74:82:e6 (00:16:17:74:82:e6), Dst: Actionte_d8:a3:88 (08:00:27:08:00:27:08:a3:88)
 Internet Protocol Version 4, Src: 192.168.1.77 (192.168.1.77), Dst: 173.194.33.41
 Transmission Control Protocol, Src Port: 63752 (63752), Dst Port: http (80), Seq: 311111111, Win: 65535, Len: 758
 Hypertext Transfer Protocol

```

0000  a8 39 44 d8 a3 88 00 16 17 74 82 e6 08 00 45 00  .9D....t...E.
0010  02 e8 23 8b 40 00 80 06 43 a4 c0 a8 01 4d ad c2  ..#.@...C....M.
0020  01 29 f9 08 00 50 f0 6c 54 ad 8f 0f 98 97 50 18  !)...P.l T....P.
0030  3f df 45 76 00 00 47 45 54 20 2f 5f 5f 75 74 6d  ?.Ev..GE T /__utm
0040  2e 67 69 66 3f 75 74 6d 77 76 3d 35 2e 32 2e 33  .gif?utm wv=5.2.3
0050  76 76 74 6d 77 74 71 76 75 74 6d 66 3d 27 20 20  utm=5.2.3
    
```



INNER DEFENSES (SWITCHES/SERVER CONFIGS)

- Protecting Internal Traffic, Outbound Traffic, and Inbound Traffic
 - Internal Traffic = device to device
 - Servers
 - Printers
 - Computers
- Protected By:
 - Software Configurations
 - Group Policy
 - Password Policy
 - Hardware Configurations
 - Routing Rules



Admincat



Limits Access

COMPUTER SECURITY AND POLICY

Why We Love It

- Protects the computers from accidental changes
- Protects Data
- Lots of things depend on the running operation of the network.
- Filtering helps with network efficiency

Why It Is A Barrier

- You need something done to improve your job (efficiency /performance)
- Patrons!
- Filtering limits access.

Local Group Policy Editor

File Action View Help

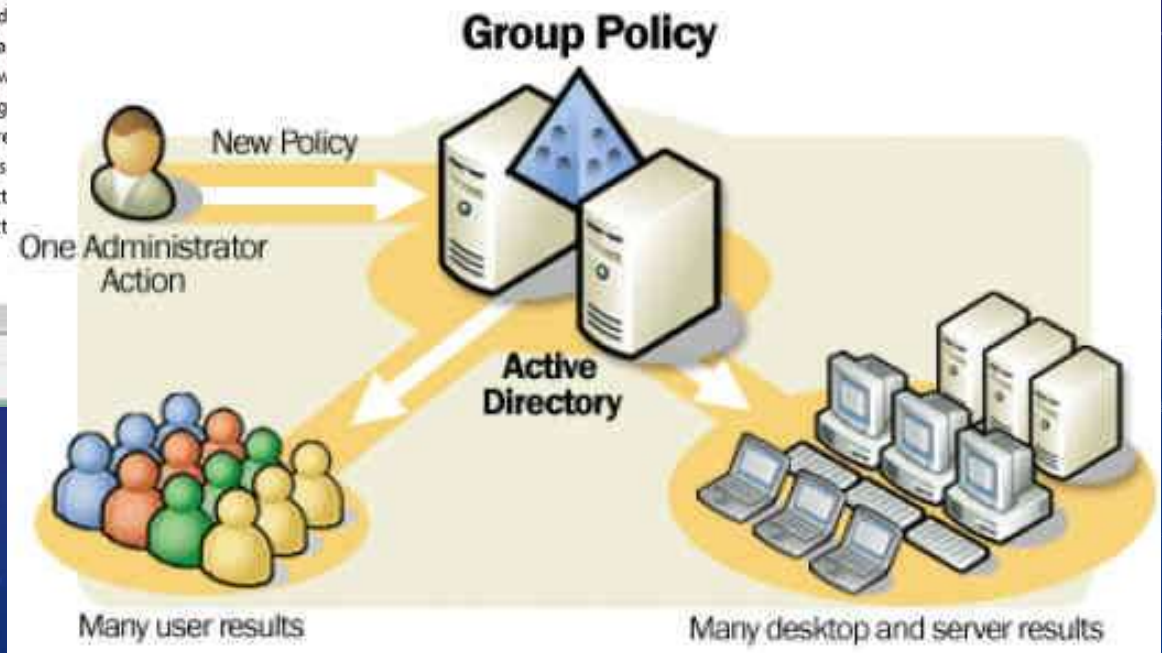
Computer Configuration

- Software Settings
- Windows Settings
- Administrative Templates
 - Control Panel
 - Network
 - Printers
 - Server
 - Start Menu and Taskbar
 - System
 - Windows Components
 - All Settings
- User Configuration
 - Software Settings
 - Windows Settings
 - Administrative Templates
 - Control Panel
 - Desktop
 - Network
 - Shared Folders
 - Start Menu and Taskbar
 - System
 - Windows Components
 - All Settings

Setting

Setting	State	Co
Path Exclusions	Enabled	
Turn off automatic learning	Enabled	
Allow input personalization	Enabled	
Force a specific default lock screen and logon image	Not configured	
Prevent changing lock screen and logon image	Not configured	
Prevent changing start menu background	Not configured	
Do not display the lock screen	Not configured	
Prevent enabling lock screen camera	Not configured	
Prevent enabling lock screen slide show	Not configured	
Force a specific background and accent color	Not configured	
Force a specific Start background		
Block clean-up of unused langua		
Restricts the UI language Window		
Force selected system UI languag		
Apply the default account picture		
Do not allow the BITS client to us		
Do not allow the computer to act		
Do not allow the computer to act		
Allow BITS Peercaching		
Timeout for inactive BITS jobs		

2281 setting(s)



UPDATES, PATCHES, FIRMWARE

- Keeping your system updated is important.
 - Being on the latest and greatest [software/update/firmware] isn't always good.
 - Need to test and vet all updates before implementation
 - If you can – build a dev environment to test and validate.



**99 little bugs in the code.
99 little bugs in the code.
Take one down, patch it around.
127 little bugs in the code...**

The screenshot displays the Jamf Pro web interface. At the top, there are navigation tabs for 'Computers', 'Mobile Devices', 'Users', and 'Notifications'. The user is logged in as 'admin'. The main content area is titled 'MKT-DMPNRS1WG5VT' and has three tabs: 'Inventory', 'Management', and 'History'. The 'Management' tab is active, showing a list of management commands on the left and a grid of command icons on the right. The commands include Update Inventories, Lock Device, Clear Passcode, Clear Restrictions, Unmanage Device, Wipe Device, Send Blank Push, Set Wallpaper, and Enable Lost Mode. A 'No Pending Commands' message is displayed at the bottom of the command grid. At the very bottom of the interface, there are buttons for 'Done', 'History', and 'Delete'.

Computers Mobile Devices Users Notifications 1 admin

MKT-DMPNRS1WG5VT

Inventory Management History

Management Commands
4 Pending Commands

- Configuration Profiles
5 in scope
- Activation Lock Bypass
Not Configured
- Apps
2 in scope
- eBooks
0 in scope
- Mobile Device Groups
1 smart, 0 static

Management Commands

- Update Inventories
- Lock Device
- Clear Passcode
- Clear Restrictions
- Unmanage Device
- Wipe Device
- Send Blank Push
- Set Wallpaper
- Enable Lost Mode

No Pending Commands

Done History Delete

System Center 2012 Configuration Manager (Connected to P01 - Primary Site)

Home | Collection | Close

Add Selected Items |
 Install Client |
 Manage Affinity Requests | Update Membership | Copy |
 Manage Out of Band | Add Resources | Delete |
 Clear Required PXE Deployments | Export |
 Deploy | Properties

Assets and Compliance > Overview > Devices > AutoCAD 2013 x86

Assets and Compliance

- Overview
- Users
- Devices
 - AutoCAD 2013 x86
- User Collections
- Device Collections
 - Application Installs
 - Departments
- User State Migration
- Asset Intelligence
- Software Metering
- Compliance Settings
- Endpoint Protection

AutoCAD 2013 x86 1 items

Search [] Search Add Criteria

Icon	Name	Client Type	Client	Site Code	Client Activity
	CL1	Computer	Yes	P01	Inactive

+ Add Selected Items
 - Remove from Collection
 Install Client
 Start
 Approve
 Block
 Unblock
 Manage Out of Band
 Clear Required PXE Deployments
 Endpoint Protection
 Edit Primary Users
 Refresh F5
 Delete Delete
Properties
 Client Actions
 Client Logs
 Client Tools

Application Deployment Evaluation Cycle
 Discovery Data Collection Cycle
 File Collection Cycle
 Hardware Inventory Cycle
 Machine Policy Evaluation and Update Cycle
 Software Updates Scan Cycle
 Software Updates Deployment Evaluation Cycle
 Software Inventory Cycle
 User Policy Retrieval and Evaluation Cycle
 Windows Installer Source List Update Cycle

Active Directory

Summary | Client Activity Detail | Client Check Detail | Endpoint Protection | Malware Detail

Ready

Start | Internet Explorer | Mail | Windows Explorer | Taskbar | System Tray: 10:10 PM 11/7/2012

SCCM tools



SWITCH CONFIGURATIONS

- Routing Rules
 - Split networks into
 - Public: 10.0.10.X
 - Staff: 10.0.20.X / :: Wireless Staff
 - Servers: 10.0.30.X
 - Wireless Public
 - Route traffic so Public LAN cannot see Staff LAN
- Access Restrictions
 - Limit devices connecting to LAN
 - MAC Address Filtering
- Limit Port Scanning, IP Scanning, etc on network.
- Limit which networks have access to which ports.

PROTECTING END DEVICES

- Protecting Assets
 - Business Assets
 - Thefts
 - Hacking
 - Personal Devices
 - Security Risk
- Usually pose an INBOUND threat to your network



Policies

- AV Not U...
- Compliant (0)
- AntiVirus Compliance 2 (0)
- Asset Classification 1 (2,845)
 - NAT Devices (0)
 - Windows (2,817)
 - Printers (0)
 - Linux/Unix (18)
 - Macintosh (0)
 - VoIP Devices (0)
 - Network Devices (1)
 - Unclassified (0)

Matched
 Unmatched
 Pending
 Irresolvable
 Hide Offline
 Filter by: All | Hosts: 2,817

Online Host	Host IP	Segment	Policy Asset Cla	MAC Address	Display Name	Actions
DOM37AQ37DC	10.37.1.1	Env 37	Windows	000c29f10fe9		
DOM37יבדן_אירנה...	10.37.1.126	Env 37	Windows	0007e96e428d	Admin	
RSAIGLTA	10.37.100.1	dash 37 100-101	Windows	000010371001	hugu pinam	
RSIAERPA	10.37.100.2	dash 37 100-101	Windows	000010371002	adonell vivyn	
RS	sh 37 100-101	sh 37 100-101	Windows	000010371003	kezawne pelgann	
RS	sh 37 100-101	sh 37 100-101	Windows	000010371004	bead laod	
GU	sh 37 100-101	sh 37 100-101	Windows	000010371005	anachri linel	
RS	sh 37 100-101	sh 37 100-101	Windows	000010371006	ranki cretta	
RS	sh 37 100-101	sh 37 100-101	Windows	000010371007	rogerel qual	
RS	sh 37 100-101	sh 37 100-101	Windows	000010371008	hlognu edien	

Window

IP Address: 000010371002

Actions

- Sub-R...
- 1. U...
- 2. M...

Actions:

- Disable External Device
- Get Microsoft SMS Updates
- Kill Instant Messaging
- Kill Peer to Peer
- Kill Process on Linux
- Kill Process on Macintosh
- Kill Process on Windows
- Run Script on Linux
- Run Script on Macintosh
- Run Script on Windows
- Set Registry Key
- Start AntiVirus
- Start Macintosh Updates
- Start Windows Updates
- Update AntiVirus
- Windows Self Remediation

The host is not inspected by the

- 3. NA Printers
- 4. NA Linux/Unix
- 5. NA Macintosh
- 6. NA VoIP Devices
- 7. NA Network Devices
- 8. NA Unclassified

PASSWORDS

- Let's talk about Passwords
 - Length of Password
 - Complexity of password requirements
 - DO NOT USE POST IT NOTES
- A person's "every day account" should never have admin rights to machines.
 - That includes your IT Folks!

The comic strip is divided into four panels. The top-left panel shows a password 'Tr0ub4dor &3' with annotations: 'UNCOMMON (NON-GIBBERISH) BASE WORD' for 'Troubador', 'ORDER UNKNOWN' for the mixed case, 'CAPS?' for 'T', 'COMMON SUBSTITUTIONS' for 'r', 'NUMERAL' for '4', and 'PUNCTUATION' for '&3'. A note says '(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)'. The top-right panel shows a password represented by 28 boxes, with a calculation $2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$ and a note: '(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE: YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)'. The difficulty to guess is 'EASY' and to remember is 'HARD'. The bottom-left panel shows the password 'correct horse battery staple' with a note: 'FOUR RANDOM COMMON WORDS'. The bottom-right panel shows a stick figure thinking 'THAT'S A BATTERY STAPLE.' and 'CORRECT.' with a battery icon. The difficulty to guess is 'HARD' and to remember is 'YOU'VE ALREADY MEMORIZED IT'. A final caption at the bottom reads: 'THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.'

TOOLS TO HELP



LastPass ****

ENGLISH

FEATURES HOW IT WORKS GO PREMIUM ENTERPRISE LOG IN

The Last Password You Have to Remember

[Get LastPass Free](#)

✳ The Secure and Trusted Way to Store Passwords



Leading Encryption Technology

We've implemented AES 256-bit encryption with routinely-increased PBKDF2 iterations. That's tech speak for strong protection for the data you store in LastPass.



Local-Only Decryption

All sensitive data is encrypted and decrypted locally before syncing with LastPass. Your key never leaves your device, and is never shared with LastPass. Your data stays accessible only to you.



Add Multifactor Authentication

Want to up your online security? Add one of our many multifactor authentication options. By adding a second login step, you're better protecting your account - and the information you've stored in it.

CRYPTO LOCKERS

Cryptolocker 2.0

Your personal files are encrypted



Your files will be lost
without payment on:

11/24/2013 3:16:34 PM

Info

Your **important files were encrypted** on this computer: photos, videos, documents, etc. You can verify this by click on see files and try to open them.

Encryption was produced using **unique** public key **RSA-4096** generated for this computer. To decrypt files, you need to obtain **private** key.

The single copy of the private key, which will allow you to decrypt the files, is located on a secret server on the Internet; **the server will destroy the key within 72 hours after encryption completed**. After that, nobody and never will be able to restore files.

To retrieve the private key, you need to pay 0.5 bitcoins.

Click **proceed to payment** to obtain private key.

Any attempt to remove or damage this software will lead to immediate private key destruction by server.

See files

<< Back

Proceed to payment >>

Advanced setup

ANTIVIRUS

UPDATE

PERSONAL FIREWALL 3

WEB AND EMAIL 1

DEVICE CONTROL

TOOLS 2

USER INTERFACE 1

+ BASIC

- ADVANCED

Filtering mode

Automatic mode is the default one. It is suitable for users who have no need to define rules. Automatic mode allows all outgoing and incoming connections from the network side unless otherwise specified.

Evaluate also rules from Windows Firewall

eset

SMART SECURITY

See ESET Smart Security in action in our overview video



Learning mode

Rules	Edit	i
Zones	Edit	i
IDS and advanced options	Edit	i
IDS exceptions	Edit	i

+ KNOWN NETWORKS > i

+ FIREWALL PROFILES > i

Default

OK

Cancel



Malwarebytes Anti-Malware

Malwarebytes ANTI-MALWARE

Dashboard Scan Settings History Activate Buy Premium

General Settings

Malware Exclusions

Web Exclusions

Detection and Protection

Update Settings

History Settings

Access Policies

Advanced Settings

Automated Scheduling

About

General Settings

Customize the basic options in Malwarebytes Anti-Malware. Control options such as: notifications, language, and explorer integration.

[Restore Default Settings](#)

Notifications: Enabled

Language: English

Close Notification: After 7 seconds

Explorer context menu entry: Yes No

FileHippo.com

Absolute[®]
CUSTOMER CENTER

COMPUTRAGE[®]
LO/JACK[®]
FOR LAPTOPS

MY COMPUTER

MY PROFILE

HELP

Locate

Enable Protection Services

Recover Computer

Lock / Unlock

Computer Name:
Jane [\(Edit\)](#)

Make:
Dell

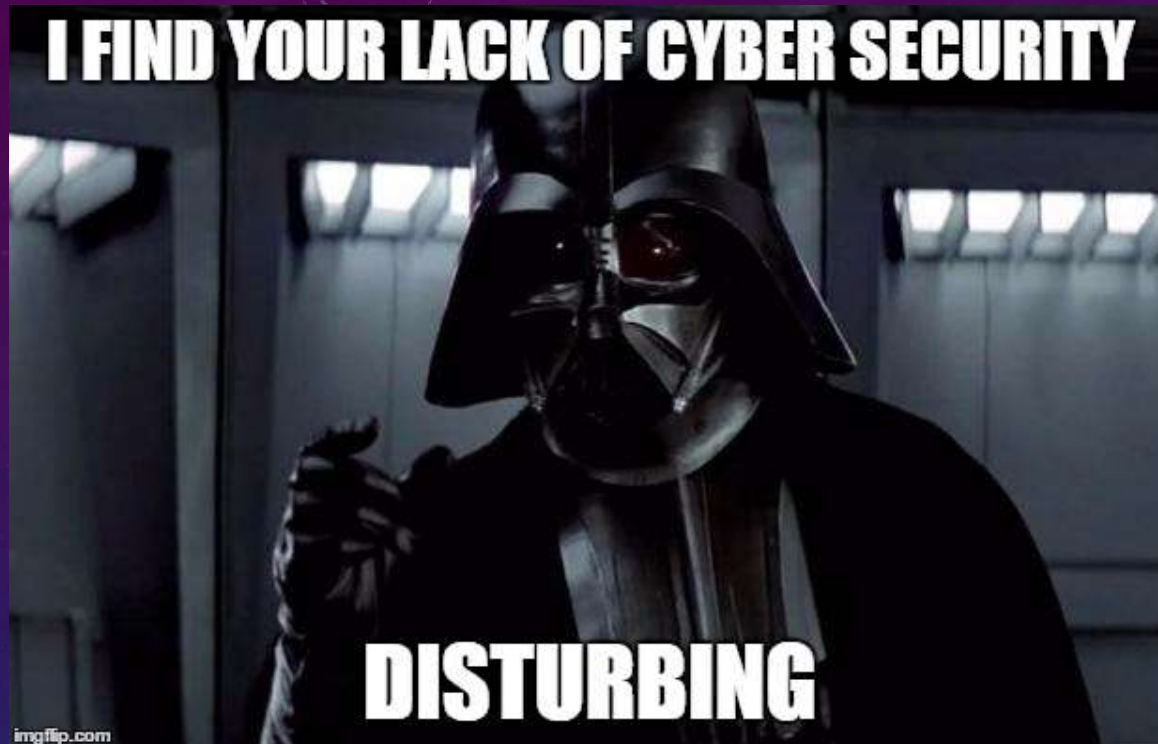
Last Call Date:
7/30/2010

Registration Code:
000000000

Model:
MXC062

Expiry Date:
7/30/2010

PRINT LICENSE



TRAINING

Staff and ?Patrons? Should all be required to attend Training

MYTHS

- I'm not worth being attacked.
- Hackers won't guess my password.
- I have anti-virus software.
- I'll know if I been compromised.



BEST KIND OF TRAINING

- Awareness
 - Reporting Issues Immediately
- Precautions
 - Being smart about links, emails, and phone calls.
 - Don't know the person – probably not legit.
 - Site doesn't look familiar – probably not legit
- Checking Others
 - Seeing someone doing something “suspicious?”
 - Seeing someone not following the “security training?”
- Acting as “owners” to data and assets.



FAKE EMAILS

From: AT&T Yahoo! Mail brucewm310@sbcglobal.net

To: undisclosed recipients:

Cc:

Subject: AT&T E-mail Update



Dear Customer,

Your E-mail account n... <http://hjnjb.....ghghghghghghghg.3owl.com/>

[Click Here To Verify Your AT&T Now](#)

Thank you
Customer Care
Copyright ? 2013 Yahoo! Inc. All rights reserved
Thanks

How to tell an email is a FAKE the From: email address, this is from an official at AT&T or Yahoo!

Also HOVER over the place it click -- do NOT click, but hover over and it will show you the link. In this case a bogus link likely leading to spyware or worse.

Gmail Team <mail-noreply@google.com>

to me

from: Gmail Team <mail-noreply@google.com>

to: Aseem Deen <aseem1234@gmail.com>

date: Sat, May 21, 2016 at 12:20 PM

subject: Your Gmail address, aseemd4@gmail.com, has been created

mailed-by: google.com

signed-by: google.com

encryption: Standard (TLS) [Learn more](#)

Welcome

Here a

Should

Enjoy!

The G

SSL

How does HTTPS work: SSL explained

This presumes that SSL has already been issued by SSL issuing authority.



https://evolveproject.org

Getting Started Cisco Unified Intel CCX Admin Basmussen Collec

Page Info - https://evolveproject.org/

General Media Permissions Security

Website Identity

Website: **evolveproject.org**
Owner: **This website does not supply ownership information.**
Verified by: **COMODO CA Limited**

View C

General Details

This certificate has been verified for the following uses:

SSL Client Certificate
SSL Server Certificate

Issued To

Common Name (CN) www.evolveproject.org
Organization (O) <Not Part Of Certificate>
Organizational Unit (OU) Domain Control Validated
Serial Number 00:F0:35:8D:87:EC:03:0E:97:3B:CF:0C:F8:C4:9B:F3:3A

Issued By

CALL SPOOFERS

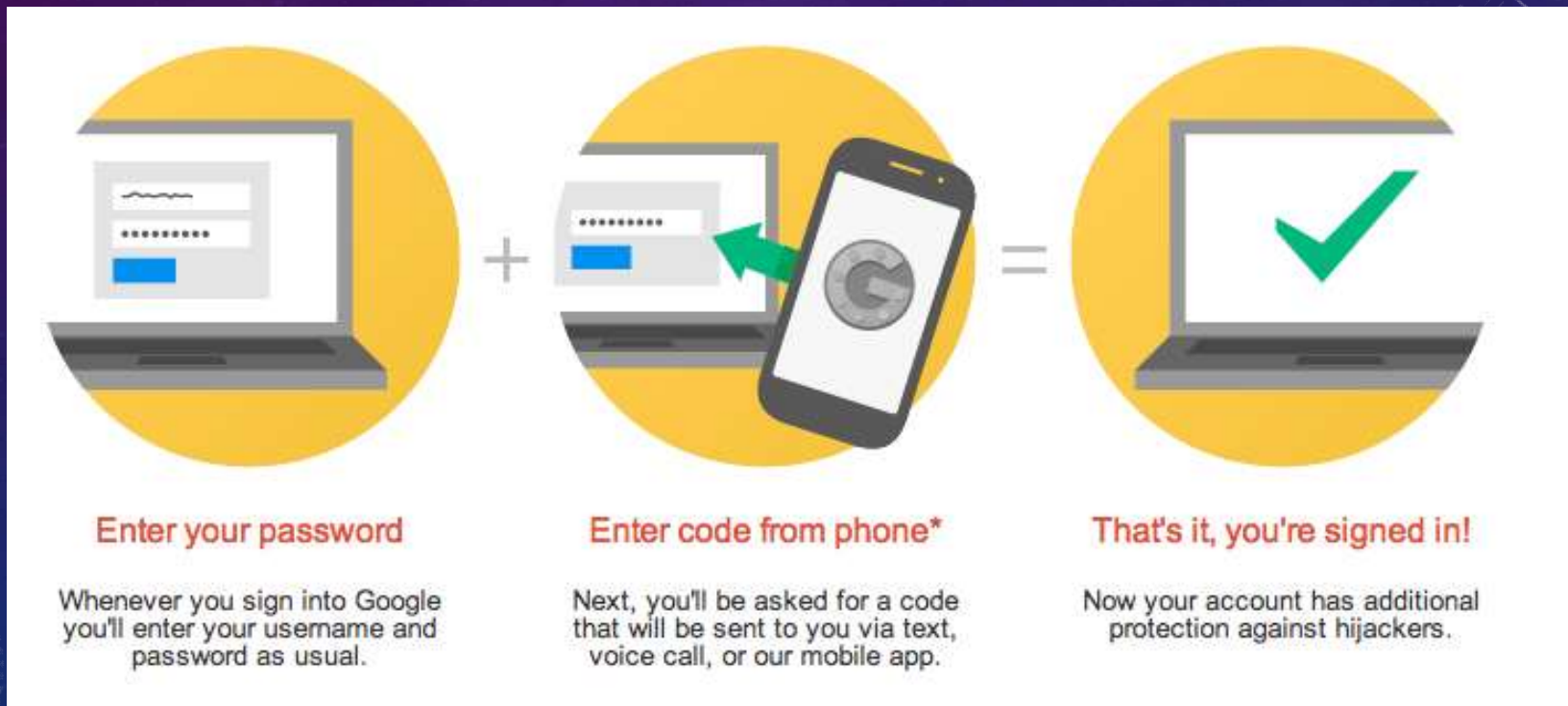
- Phone calls from “Microsoft”
 - Wanting to remote in and fix your computer.
- Phone calls from your “Bank”
 - Wanting to talk to you about your credit card
- Rule:
 - Just. Hang. Up. Then call the number on the back of the card or directly off their actual website.

GOOGLE ISN'T ALWAYS YOUR FRIEND



DUAL FACTOR AUTHENTICATION

- After logging in; verify login via Email, SMS, or an app with a code.



AD BLOCKING



Phishing










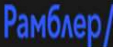





Social Engineering

SITES TO HELP

- Haveibeenpwnd.com
 - Sign up and check to see if your data appears after a hack is released
- <https://krebsonsecurity.com/>
 - Great blog to stay informed of what is happening with IT Security
- LifeLock, Identify Guard
 - Monitoring Your Data and Privacy

Top 10 breaches

 myspace	359,420,698	MySpace accounts
 NETEASE www.163.com	234,842,089	NetEase accounts 
 in	164,611,595	LinkedIn accounts
	152,445,165	Adobe accounts
 badoo	112,005,531	Badoo accounts  
	93,338,602	VK accounts
 Рамблер/	91,436,280	Rambler accounts
	68,648,009	Dropbox accounts
 tumblr.	65,469,298	tumblr accounts
 Modern Business Solutions	58,843,488	Modern Business Solutions accounts

RECAPPING

- Protect Outer Perimeter with Hardware
 - Filtering, IPS/IDS, Antivirus
- Protect Inner Perimeter with Configurations
 - Group Policy, Switch Configurations, Routing
- Protect End Devices with Software
 - Antivirus, Firewalls
- Protect Users with Training
 - Passwords



COMPLIANCE STANDARDS

- **CIPA**

- The Children's Internet Protection Act (CIPA) is a federal law enacted by Congress to address concerns about access to offensive content over the Internet on school and library computers

- **FERPA**

- The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C 123g: 34 CFR Part 99) is a Federal Law that protects the privacy of student educational records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.

- **PCI**

- The Payment Card Industry Data Security Standard (**PCI DSS**) applies to companies of any size that accept credit card payments. If your company intends to accept card payment, and store, process and transmit cardholder data, you need to host your data securely with a **PCI compliant** hosting provider.

- **SOX / Sarbanes Oxley Act**

- This act requires companies to maintain financial records for seven years.

- **SOC / Service Organization Controls**

- The **SOC 2** report focuses on a business's non-financial reporting controls as they relate to security, availability, processing integrity, confidentiality, and privacy of a system, as opposed to **SOC 1/SSAE 16** which is focused on the financial reporting controls

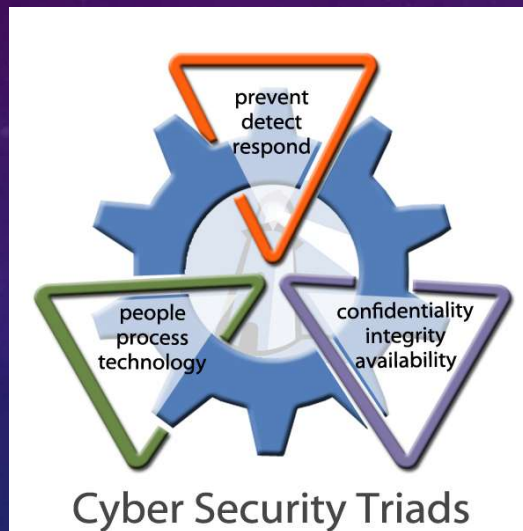
BUILDING A PLAN

- Risk Assessments
- Training Plans
- Policies, Policies, Policies!
 - Training
 - Breaches
 - Asset
 - Computer Use
- Back Up Plans
 - Data Recovery from Threats
 - System Recovery from Threats



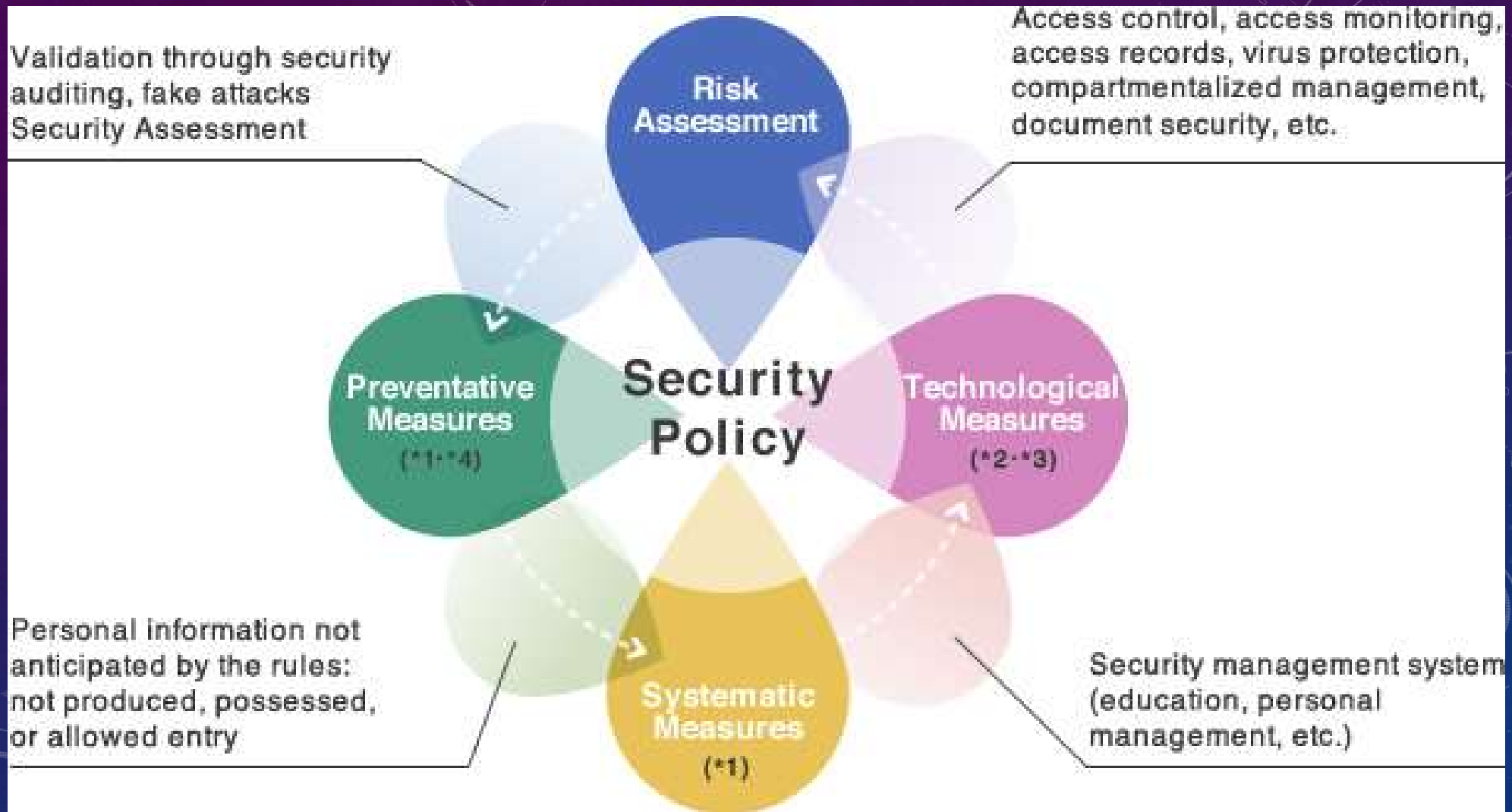
RISK ASSESSMENT

- Threats are sources of danger to information assets



- Risks are possible events or conditions that could have undesirable outcomes for the organization. Risks occur at the intersection of threats and vulnerabilities.

- Vulnerabilities exist in people, processes, and technologies.



SECURITY PLANS

- Are tested and audited.
 - Audit account usage, audit network logs, check computers for malicious software, check if computers aren't receiving updates.
 - Test staff's ability to follow basic security rules and principles.
- Refined
 - As your infrastructure grows or as things change, you will need to continually refine and update your security plan and policy.
- Plans are followed.
 - There shouldn't be exceptions to rules.

EMPLOYEE TIP SHEET - SECURITY IS EVERYONE'S RESPONSIBILITY

- **Ignoring cybersecurity is not an option.**
- **Think Security, First and Always.**
- **Protect What Matters**
- **Think Like An Attacker**
- **Knowledge is Power**
- **Cybersecurity Never Stands Still**
- **Good Security Has Many Layers**

<http://www.mgeutc.com/news/cybersecurity/a-proactive-approach-to-cybersecurity-2/>

QUESTIONS?

- Brian Pichman
- Twitter: @bpichman
- Cell: 815-534-0403
- Email: bpichman@evolveproject.org