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)
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 lose 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

SHAZAM!!!
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...
Outside
- Modem

Router

Firewall
- Servers

Switches

End User
- Phones
- Computers
- Laptops

Outside
- Modem

Router

Firewall
- Servers

Switches

End User
- Phones
- Computers
- Laptops
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 it's sent across.

• 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.
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
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.
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...

<table>
<thead>
<tr>
<th>Inventory</th>
<th>Management</th>
<th>History</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Configuration Profiles</strong></td>
<td><strong>Configuration Profiles</strong></td>
<td></td>
</tr>
<tr>
<td>- <strong>Activation Lock Bypass</strong></td>
<td>- <strong>Update Inventory</strong></td>
<td></td>
</tr>
<tr>
<td>- <strong>Apps</strong></td>
<td>- <strong>Lock Device</strong></td>
<td></td>
</tr>
<tr>
<td>- <strong>eBooks</strong></td>
<td>- <strong>Clear Passcode</strong></td>
<td></td>
</tr>
<tr>
<td>- <strong>Mobile Device Groups</strong></td>
<td>- <strong>Clear Restrictions</strong></td>
<td></td>
</tr>
<tr>
<td>- <strong>Enable Lost Mode</strong></td>
<td>- <strong>Unmanage Device</strong></td>
<td></td>
</tr>
<tr>
<td>- <strong>Wipe Device</strong></td>
<td>- <strong>Seed Blank Push</strong></td>
<td></td>
</tr>
<tr>
<td>- <strong>Set Wallpaper</strong></td>
<td>-</td>
<td></td>
</tr>
</tbody>
</table>

**No Pending Commands**
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
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!
TOOLS TO HELP

The Last Password You Have to Remember

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 step, you’re better protecting your account - and the information you’ve stored in it.
Your personal files are encrypted

Info
Your important files were encrypted on this computer: photos, videos, documents, etc. You can verify this by clicking 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.
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: No
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 (brucewm210@docglobal.net)
To: undisclosed recipients
CC: 
Subject: AT&T Email Update

Dear Customer,

Hover over this to see this: http://hjhijgjggjggjgggjgggsgjggggjggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggg
How does HTTPS work: SSL explained

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

1. User accessing secure site.
2. Check DNS records for IP address to find website host.
3. Website records found. Going to the host web server.
4. Requesting secure SSL connection from website host.
5. Host responds with valid SSL certificate.
6. Secure connection is now established. Transferred data is encrypted.

SSL Client Certificate
SSL Server Certificate

This certificate has been verified for the following uses:

- Issued To
  - Common Name (CN): evolveproject.org
  - Organization (O): <Not Part Of Certificate>
  - Organizational Unit (OU): Domain Control Validated
- Serial Number: 00:F0:35:8D:B7:EC:03:0E:97:3B:CF:0C:F8:C4:98:F3:3A
- Issued By:

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

SHOULDN'T HAVE GOOGLED THAT

I SHOULD NOT HAVE GOOGLED THAT
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
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

• Vulnerabilities exist in people, processes, and technologies.

• Risks are possible events or conditions that could have undesirable outcomes for the organization. Risks occur at the intersection of threats and vulnerabilities.
Validation through security auditing, fake attacks
Security Assessment

Risk Assessment

Access control, access monitoring, access records, virus protection, compartmentalized management, document security, etc.

Preventative Measures (*1-4)

Security Policy

Personal information not anticipated by the rules: not produced, possessed, or allowed entry

Systematic Measures (*1)

Security management system (education, personal management, etc.)

Technological Measures (*2-3)
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

QUESTIONS?

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