Cyber Security and Small State and Local Government Agencies

NETWATCHER™
By Defensative

Scott B. Suhy
Scott.Suhy@Defensative.com

NASCIO - STATE CIO PRIORITIES FOR 2016

PRIORITY #1 - SECURITY AND RISK MANAGEMENT

CYBER THREATS ARE NOT INCREASING IN COMPLEXITY AND INTENSITY

They are!

FUNDING FOR CYBERSECURITY INITIATIVES IS INSUFFICIENT

FOR A SMALL GROUP
SECURITY TALENT IS EASY
TO FIND AND NOT VERY
EXPENSIVE

They are hard to find and expensive

✓Fact…

LACK OF CYBERSECURITY
VISIBILITY AND CONTROL

ALERT OVERLOAD!

SMALLER AGENCIES AND
SMB'S HAVE NOT BECOME
THE NEW TARGET

They have become the target!

✓Just ask these groups…

http://www.databreaches.net/
https://www.privacyrights.org/data-breach
http://www.heritage.org/research/reports/2014/10/cyber-attacks-on-us-companies-in-2014

San Diego County Employees Retirement Association
State of Rhode Island website
New Hampshire Department of Motor Vehicles
Georgia Technology Authority
Oregon Department of Revenue
Nebraska Treasurer's Office
Los Angeles County, Community Development Commission
City of Lubbock
City of Wickliffe
Vermont Agency of Human Services
State of Indiana Official Website
Iowa Department of Education
Eastern Suffolk BOCES
Georgia Division of Public Health
Illinois Dept. of Financial and Professional Regulation
Franklin County Municipal Court
Utah Division of Finance
Foothills Parks and Recreation District
Coos Bay Department of Human Services
Nebraska Workers' Compensation Court
Iowa State Racing and Gaming Commission
St. Louis Metropolitan Police Department

Guttenberg Housing Authority
S. Carolina State Budget and Control Board Employee Insurance Program
Walnut Township School District
Town of Barton
Massachusetts Executive Office of Labor and Workforce Development
Arizona Department of Public Safety
Bay Area Rapid Transit
Texas Police Chief Association
Legislative Data Center
Washington South Supervisory Union
Los Angeles Police Department
North Penn School District
Ridgewood Public Schools
Provo School District
California Statewide Law Enforcement Association
New York State Association of Chiefs of Police
City of Point Pleasant
President's Challenge, Indiana University
Greene County
Syracuse Police Department
Salt Like City Police Department
City of Springfield, Springfieldmo.gov

Los Angeles County Police Canine Association
Town of Plainfield Indiana
National Capital Planning Commission
Utah Department of Health
Berrien County Sheriff's Department
Three Rivers Park District
Lake County Sheriff's Office
California DOJ, High-Tech Response Team
York County, South Carolina
Sierra County, California
www.SD.gov
Glade County Sheriff's Office
New Hampshire Department of Corrections
CIty of Tulsa, Oklahoma
www.naperville.il.us
City of Burlington, Washington
South Carolina Department of Revenue
Administrative Office of the Courts – Washington
City of Akron
Bureau of Automotive Repair
Harris County
Bonneville Power Administration

✓What are they after?

- Money – Ransom-ware
- Your organizations data
  - Personally Identifiable Info (PII)
  - Protected Health Information (PHI)
  - CC Numbers and/or Financial Info
  - Intellectual property – copyrights, trademarks & patents, business plans, customer lists, etc.
- Your customers/partner' data & access to your customers networks…
  - The Target breach happened due to an HVAC vendor (more)

✓Are you prepared?

If you are anything like the typical SMB then “no”

- 86% of SMB’s said they are "satisfied" with the level of security they have in place to defend customer or employee data
- 87% of SMB’s have not written a formal security policy for employees
- 83% lack any security blueprint at all
- 59% have no plan in place to respond to a security incident

--*National Cyber Security Alliance (NCSA) and Symantec “National Small Business” survey*

✓Fact--A breach is going to cost you $

- Attorney Fees
- Plaintiff Demands
- Response Costs
- Reputation Damage

Note Ohio's Data Breach Protection Laws

✓Fact– Your employee is your biggest risk (social engineering)

– The #1 attack vector!

You or one of your employees may receive a fake email or text message with a website created to look like it's from an authentic company.

What it does:

- Trick you into giving them information by asking you to update, validate or confirm your account. It is often presented in a manner than seems official and intimidating, to encourage you to take action.
- Convince you to download Malware

[39 Percent of Employees Admit to Opening Suspicious Emails]

Example:

✓Fact- there are many ways to take you down…

- Pharming
- Cross Site Scripting
- Denial of Service
- SQL Injection
- Dictionary Attack
- Botnets
- Scanning

***see appendix for details*

✓Myth – It has to be expensive..

Security is less about technology and more about business process…

✓What You Must Do – Cyber Liability Insurance

- Ensure you have the appropriate Cyber Insurance coverage for both 1st party liability and 3rd party liability

- Common first-party costs when a security failure or data breach occurs include:
  - Forensic investigation of the breach
  - Legal advice to determine your notification and regulatory obligations
  - Notification costs of communicating the breach
  - Offering credit monitoring to customers as a result
  - Public relations expenses
  - Loss of profits and extra expense during the time that your network is down (business interruption)

- Common third-party costs include:
  - Legal defense
  - Settlements, damages and judgments related to the breach
  - Liability to banks for re-issuing credit cards
  - Cost of responding to regulatory inquiries
  - Regulatory fines and penalties (including Payment Card Industry fines)

- Ensure your coverage covers remediation!

Example

✓What You Must Do - Create IT & Employee Cyber Policies

General

- Acceptable Encryption Policy
- Acceptable Use Policy
- Clean Desk Policy
- Disaster Recovery Plan Policy
- Digital Signature Acceptance Policy
- Email Policy
- Ethics Policy
- Password Construction Guidelines
- Password Protection Policy
- Security Response Plan Policy
- End User Encryption Key Protection Policy

Network Security

- Acquisition Assessment Policy
- Bluetooth Baseline Requirements Policy
- Remote Access Policy
- Remote Access Tools Policy
- Router and Switch Security Policy
- Wireless Communication Policy
- Wireless Communication Standard
- Third Party Access Policy

Infrastructure

- Database Credentials Policy
- Technology Equipment Disposal Policy
- Information Logging Standard
- Lab Security Policy
- Server Security Policy
- Software Installation Policy
- Workstation Security (For FINRA) Policy
- Web application security policy

Examples:

- Sample Policy (here)
- SANS (here)

- What software can I run on the network? Can I run TOR? BitTorrent?
- Can I get my personal mail via my corporate laptop?
- Can I use Facebook on my corp laptop? During work hours?
- Can I plug in a WIFI router on my desk?
- Can I connect my personal phone to the corporate WIFI?
- Can I visit Porn sites on my laptop at home?

✓What You Must Do - Make this a Leadership problem, not an IT problem

- Who is responsible for developing and maintaining our cross-functional approach to cybersecurity? To what extent is leadership (as opposed to IT or risk executives) owning this issue?
- Which information assets are most critical, and what is the “value at stake” in the event of a breach? – Focus limited resources on protecting these assets!
- Understand what promises—implicit or explicit—have you made to our customers and partners to protect their information?
- What roles do cybersecurity and trust play in your customer value proposition—and how do you take steps to keep data secure and support the end-to-end customer experience?
- Compare your approach with your peers.
- Is your approach to security continuing to evolve, and are you changing your business processes accordingly?

✓What You Must Do - Manage your suppliers

- Do your suppliers / partners / contractors have access to your network or Line of Business systems?
- Audit your suppliers / partners / contractors for their cyber liability insurance coverage, their corporate cyber policies and their infrastructure protection
  - Make this a part of their contract!

✓What You Must Do – Audit

Create a process for periodic audits

✓What You Must Do – Have a response plan

Create a cross-organization response plan

✓Practice

✓Train everyone

✓What You Must Do – Understand and leverage “Technology”

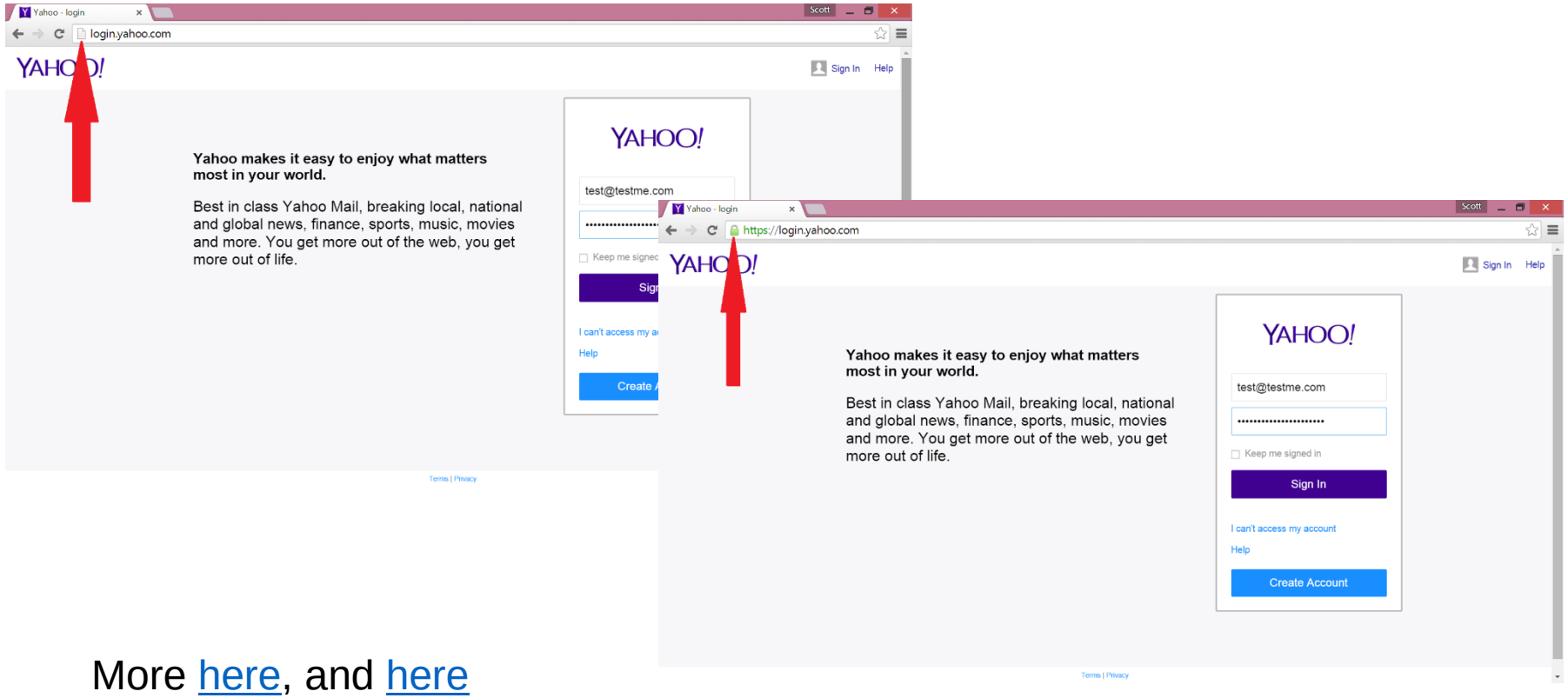
- Systems
  - Ensure your computer systems’ and security software stay up to date
    - Especially Java, Flash and Windows security updates
  - Secure & Encrypt laptops and mobile phones
  - Ensure Backup are scheduled and tested
  - Firewalls, latest routers/switches with up to date software (and no default passwords)
  - Engage a Managed Security Services Provider (MSSP) who offers an end-to-end platform such as http://netwatcher.com versus buying expensive solutions like FireEye…
- Move your Line of Business systems to secure cloud providers
  - Offsite cloud providers will require more stringent firewalls, access credentials and security protocols than onsite stored data.
  - Offsite cloud applications are stored within the walls of a 24/7/365 physically secured data center facility.
  - Cloud application providers build threat assessment models that will work to identify possible leaks within business cloud applications, and constantly work to break those security measures, in an effort to make them stronger and stronger.
- Software you have built
  - Needs to be secure by design (here)

✓What You Must Do – Conduct “Everyone” cyber training

- Training - Continually raise your staff and contractors awareness on cyber security best practices (email, web, phone, text etc…)
- Train employees
  - To recognize an attack
  - On step-by-step instructions about what to do if they’ve witnessed a cyber incident
  - On your corporate cyber policies

✓Train Employee's – Use HTTPS (note the "S")

Unfortunately many websites and services today still offer un-encrypted login. With un-encrypted login, the password is NOT encrypted and considered "cleartext" and can be easily decoded!



More here, and here

✓Train Employee's – Keep software up to date

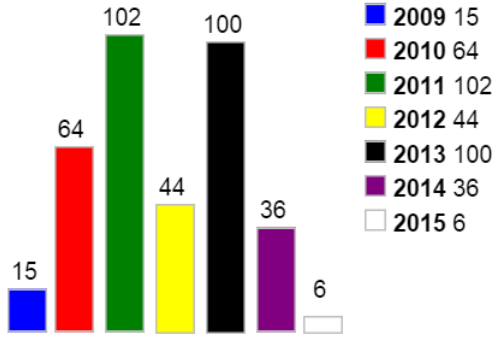
Software vendors such as Adobe, Microsoft, Oracle and others produce frequent security patches that plug holes that can be exploited by bad actors.

If you don't install these patches on a regular basis on your hosts, desktops, laptops and phones your infrastructure will be at risk and will eventually be compromised.

CVE Details is a good place to keep up on the patches. They consolidate vulnerability data from the National Vulnerability Database (NVD) and www.exploit-db.com . Another great site is Mitre's CVE site here .

Here are 2 examples to give you some perspective on how many vulnerabilities a software can contain:

- Here is a list of Adobe Flash vulnerabilities.
- Here is a list of Oracle Java vulnerabilities.
- Here is a simple chart that shows how many vulnerabilities have been published over the years in the Windows 7 OS



✓Train Employee's – Don't use risky software

Examples:

- BitTorrent - you have no control over what the BitTorrent user is downloading and you don't want to end up like this guy . (or these people)
- TOR – You don't know who is sniffing on the exit nodes (example)
- TFTP – It's all in clear text (more)
- Misc Android Apps – 97% of mobile malware is on Android (more) (example)

✓Train Employee's – Passwords

- Use Secure Passwords (more)
- Use throw away passwords on non-mission critical sites
- Understand Password Managers may not be that secure (example)
- Change Default Passwords! (more)
- If available enable two factor authentication (example)

✓Train Employee's – Your Phone

Here are 7 Tips to Prevent Mobile Malware

- Understand the mobile risks - A mobile device is a computer and should be protected like one. If you access the corporate network with their mobile device you should understand the risk imposed by downloading applications and accessing website that are not from trusted sources. You need to also know the value of keeping your operating system on the device up to date with the latest security patches from the manufacturer/mobile provider and operating system vendor.
- Only access corporate data via Wi-Fi over a secure tunnel as over the air networks are exposed to malicious capturing of wireless traffic. There are several mobile Virtual Private Networking technologies (VPN) that can be deployed that can allow users to connect through these secure tunnels.
- Understand your group's Bring Your Own Device to work (BYOD) policies
- Ask your organization if they have a Mobile Device Management (MDM) platform and Mobile Application Management Platforms from companies like Good and others.
- Encrypt your devices - It is very difficult for someone to break in a steal data on an encrypted device (this goes for the SIM card as well).
- If you use Android then use anti-malware software

✓Train Employee's – Home network and public WIFI's

- Change the default password and keep the firmware up to date on your home internet router
- Don't connect to random WIFI's (example)
- Don't allow others to download programs to computers or phones that will connect to your companies network. Here is a Minecraft example.
- Use a Virtual Private Network (VPN) (example, example)

✓Train Employee's – Explicit sites

Pornography and Malware… They go together. (more)

Visitors to Pornhub.com, the 63rd most popular website in the world (and 41st in the US) have a 53% chance of coming into contact with malware

Great advice from SecurityMetrics (here)

- **Disconnect** from the Internet by pulling the network cable from the router to stop the bleeding of data. Do not turn off your computer/phone/tablet
- **Follow** your groups cyber security policy step by step plan. Your group will usually:
  - **Document** all network changes, notification/detection dates, and people/agencies involved in the breach
  - **Segregate** all hardware devices in the payment process, or devices suspected of being compromised (if possible) from other business critical devices.
  - **Quarantine** instead of deleting.
  - **Preserve** firewall settings and firewall logs
  - **Restrict** Internet traffic to only business critical servers and ports outside of the credit card processing environment.
  - **Disable** (do not delete) remote access capability and wireless access points.
  - **Call a PFI.** Once the breach is contained by steps 1-7, consult with a forensic PFI to plan a compromise analysis.

Appendix

✓Pharming

You or one of your employees may be pointed to a malicious and illegitimate website by redirecting the legitimate URL. Even if the URL is entered correctly, it can still be redirected to a fake website.

What it can do:

- Convince you that the site is real and legitimate by looking almost identical to the actual site down to the smallest details. You may even enter your personal information and unknowingly give it to someone with malicious intent.
- Convince you to download Malware.

✓Cross Site Scripting

You or one of your employees opens a website that has embed hidden scripts, mainly in the web content, to steal information such as cookies and the information within the cookie (eg passwords, billing info).

✓Denial of Service (DOS)

A bad actor will attempt to make one of your network resources unavailable to its intended users by saturating the target with external communications requests, so much so that it cannot respond to legitimate traffic, or responds so slowly as to be rendered essentially unavailable.

✓SQL Injection

A bad actor may try to get valuable information from your website by exploiting vulnerabilities in the sites databases.

✓Dictionary Attack

A brute force attempt to guess your network assets passwords, by using common words and letter combinations, such as “Password” or “abc123”.

✓Botnet

A collection of software robots, or 'bots', that creates an army of infected computers (known as ‘zombies') that are remotely controlled by the originator. Yours may be one of them and you may not even know it.

What they can do:

- Send emails on your behalf
- Spread all types of malware
- Can use your computer as part of a denial of service attack against other systems

✓Scanning

Your hosts are being scanned daily by server farms all over the world looking for current vulnerabilities (example: Heartbleed) that you may not have patched yet…

What they can do:

- Take control of your organization….