Today's Cyber Security Weather Forecast: Partly Cloudy with Chance of Rain (But No, The Sky ISN'T Falling...)

Big Sky Information Security Conference

Joe St Sauver, Ph.D. (stsauver@fsi.io)
Scientist, Farsight Security, Inc.

10:00-10:50 AM, April 19th, 2017
North Ballroom in the UC,
University of Montana, Missoula, MT
https://www.stsauver.com/joe/bigsky/

I. Introduction

Thanks

- I'd like to thank **Mr. Adrian Irish** and everyone involved with planning the Big Sky Information Security Conference for the invitation to talk with you today.

- I'd also like to thank **Mr. Nathan Yrizarry** for his patient assistance with meeting/travel logistics.

- Thanks, too, to **Mr. Ben April, Ms. Merike Kaeo** and **Dr. Paul Vixie** at Farsight Security, for letting me take the time to be with you here today.

- And last but not least, thanks to all of **YOU** for making time to attend today.

A Little About Me

- I worked for the **University of Oregon** Computing Center in Eugene for about 28 years. During part of that time, I ran Academic Computing (roughly a third of the Computing Center).
- Around 2006, under a contract UO signed with Internet2, I began working for Internet2 as their **Nationwide Security Programs Manager.** Somewhat later I also assumed responsibility for the InCommon **SSL/TLS Certificate Program** and **Multifactor** Program.
- In 2014, I finally left UO and joined Paul Vixie's company, **Farsight Security, Inc.,** (https://farsightsecurity.com/).
- With Farsight's consent, I remain active in a variety of national and international cyber security activities, including serving as one of half a dozen Senior Technical Advisors for M3AAWG, and participating on the REN-ISAC TAG (Technical Advisory Group).
- You can see some of my previous public talks and blog postings at https://www.stsauver.com/joe/

It's Nice to Be Back In Montana

- In many ways, being here in Missoula feels a lot like "coming home." Every time I've been in the state, I've been struck by its wild beauty and limitless opportunity.

- I also really like Montanans. My wife Bev was born in Helena, and her grandparents used to have a ranch up in the Sweet Grass Hills around Whitlash, outside of Shelby, just south of the Alberta border.

- Anyhow, I think you're lucky to live in a terrific state. Thanks for letting me visit.

Today's Format And Audience

- I've prepared some material to go over with you.
- I was told to expect a mix of regular users and IT folks, so I'm going to interleave my material a bit, with hopefully neither group feeling neglected (or bored or overwhelmed).
- If you've got questions as we go along, you can ask them or save them to the end (I do want to stay on time, so if we get too many questions I may defer some of them to the end).
- I'll be making these slides available, just like most of my talks, so if we don't get through everything, don't worry, you can always check the slides (if you want to).

Speaking of Slides...

- By now you may have noticed my slide style − the exact opposite of the "have three or four brief bullet points per slide" format that's normally recommended for PowerPoint-ware.
- This is intentional, and I do it for a number of reasons, including:
  -- It forces me to **prepare** (semi-)coherent comments. :-)
  -- It helps me **stay on track** and reduces the likelihood that I'll get sidetracked and run out of time
  -- It reduces the likelihood that I'll be **misquoted** by 3rd parties
  -- It eliminates the need for you to try to **take notes** (you can just grab a copy of my slides after the fact)
  -- **Those who couldn't make the session can at least look at the slides if they're curious**
  -- **It's like "captioning"** for the deaf or hearing-impaired.
  -- Google and Bing tend to **index** my slides pretty well, too, FWIW
  -- But relax: I'm NOT going to read my slides to you word-for-word

My Interest in The Perception of Risk and Decision Making

- In many ways, today's talk is all about the **perception of risk**, and how human beings **make security decisions** in light of those risks.
- FWIW, my terminal degree is from what was previously known as the **Decision Sciences Department** (now rechristened "Operations and Business Analytics") at the University of Oregon.
- As part of that program, I was fortunate to be able to take classes from some truly legendary decision theorists, including **Dr. Paul Slovic** of UO's Psych Department & Decision Research, Inc., see (http://www.decisionresearch.org/researcher/paul-slovic-ph-d/)
- That background in Decision Sciences provided a nice foundation for my work in cyber security since the dominant approach to cyber security at the managerial layer has now become firmly rooted in "risk management."

Risk Management?

- When management adopts a risk management approach for cyber security, they think about concepts like...
- "Risk = threat x vulnerability x consequence"
- "Options for responding to a risk: mitigate the risk, avoid the risk, transfer the risk, accept the risk..."
- "Ensure that costs of mitigating risks don't exceed the expected losses that might otherwise have occured."
- Risk management approaches are often lumped within an overall "Governance, Risk and Compliance" framework.
- You can see my take on GRC vs technical security in a dozen slides I put together for "Moving From Security to Governance, Risk and Compliance: Campus Perspective Panel" https://www.stsauver.com/joe/security-to-grc/security-to-grc.pdf

III. Risk, and The Perception of Risk

"[...] people overestimate risks that are being talked about and remain an object of public scrutiny. News, by definition, is about anomalies."

Beyond Fear: Thinking Sensibly about Security in an Uncertain World (2003), Bruce Schneier (https://books.google.com/books?id=btgLBwAAQBAJ&pg=PA27&lpg=PA27)

Believe It Or Not, IMO, Things Are Actually Going Pretty Well In Montana Higher Ed Cyber Security

- To the best of my knowledge, Montana colleges and universities **have NOT and are NOT** experiencing:

  - Major data breaches
  - Widespread malware infections/worms
  - Ongoing distributed denial of service (DDoS) attack
  - Outbound email getting blocked by major service providers
  - Major data center fires or other physical disasters
  - Multi-million-dollar financial loss (e.g., business email compromise, etc)

  THAT'S WONDERFUL!

Specific Examples of Stuff Going Well

- Students took classes and learned new stuff, including online.
- Faculty/staff got their work done (and got paid!), perhaps teaching, perhaps doing research and making some cool new discoveries. Cyber security DIDN'T get in the way.
- Millions of people all over the place used their computers and their smartphones and nothing significant went awry..."
- Americans were able to send and receive mail, buy stuff on the web, spend time on social media, play computer games, etc.
- Some people even recently spent time with their families and friends over Easter dinner with a good bottle of wine and DIDN'T spend the weekend worrying about cyber security or working on fixing compromised computers.
- This is NOT "news." But it really should be. **Stuff is actually working pretty well, at least for the most part, I think.**

I've Said I Think Things Are Going Pretty Well Before

- For example, check out: "Seeing Only Shark Fins and Discarded Plastic Shopping Bags In an Sea of Beauty, Elegance and Plenty," http://www.cybergreen.net/2016/02/01/201621seeing-only-shark-fins-and-discarded-plastic-shopping-bags-in-an-sea-of-beauty-elegance-and-plenty/
- "Today's cyber security culture largely discounts or ignores the Internet's overwhelming success. We've become cable news journalists, continually searching for new tragedies, new disasters. Professional pessimists and paranoids, we search for evidence supporting our persecution complex: yes, the world really is out to get us, see? We take pride in being skeptical, street smart, cynical, and distrustful. Our demeanor is routinely grave, heads shaking back and forth, clearly conveying that the audience should not expect the patient to live, even with our own herculean efforts and the conveyance of much treasure. This is a mistake."

The *News* says...

- If you follow the news, your impression will almost certainly be that the Internet **IS** a **pretty dangerous and scary place.**

- Bad news always seems to makes headlines:

  - **"Horrible new malware..."**
  - **"Huge DDoS!"**
  - **"Inconceivably-boneheaded software flaws"**
  - **"Worse than every before..."**
  - **"Record breaking breach"**

EOTWAWKI?

- The logical conclusion from all this bad cyber security news is that the "End of the World As We Know It" *must* be imminent.
- Surely it MUST be time to disconnect from the Internet, retreat to our homes and passively await the Terminators* and **"Skynet."****
- I mean hey, it's really, **REALLY** bad out there according to the media, right? RIGHT?
- **NO. NOT.**

-----

* "Russia Trains Robot To Shoot Guns: Can Humans Prevent Rise Of Terminator-Like Killing Machines?" (17 April 2017), http://www.techtimes.com/articles/205103/20170417/russia-trains-robot-to-shoot-guns-can-humans-prevent-rise-of-terminator-like-killing-machines.htm

** http://terminator.wikia.com/wiki/Skynet

"But Joe! People Are Really Shelling Out The Bucks!"

- **"Worldwide spending on cybersecurity is predicted to top $1 trillion for the five-year period from 2017 to 2021,** according to the Cybersecurity Market Report, published by Cybersecurity Ventures. [...]

  "In early 2015 Inga Beale, CEO at the British insurer Lloyd's, claimed that cybercrime was costing businesses globally up to $400 billion a year. Several months later Juniper Research released a report which said cybercrime will cost businesses over $2 trillion by 2019. **Microsoft CEO Satya Nadella stated $3 trillion of market value was destroyed in 2015 due to cybercrime."**

  http://www.csoonline.com/article/3083798/security/cybersecurity-spending-outlook-1-trillion-from-2017-to-2021.html

I Don't Care. My Outlook Is Still Optimistic For Cyber

- People may call me "naive" or "simple-minded" or "Pollyannaish"* for believing that things are generally going well online -- optimism has never been very "fashionable" in the cyber security community.
- Gloom and doom is the expected order of the day. **Scare people.** Make things seem as **BAD** as they possibly could be. **Fear SELLS!****
- I admit I've been as prone toward "cyber pessimism" as the next guy, but I'm making a conscious effort to **objectively re-self-assess.**

** "When you put a positive spin on everything, even things that call for sadness or discouragement, you're being pollyannaish. The word comes from a 1913 children's book by Eleanor H. Porter, Pollyanna, about a young girl who tries to find something positive in every situation — a trick she calls "the Glad Game."*
[from vocabulary.com]

*** https://seekingalpha.com/article/4034827-rising-fears-lift-cybersecurity-boats*

I'm Not The Only One "Re-Self-Assessing"

"**Google's** actually a really good example where they've done a lot of user testing in terms of **how do people respond to security warnings.** Having too many of them and having them when they're unclear is really hard to get people to understand what you're trying to communicate to them, and then also motivate them to take the steps and the behavior that you hope that they will do." * * *

"I think one of the **negative consequences of some of this fear-based communication is that when you've sufficiently scared people, they make poor decision[s]** and that's actually how we end up with really poor laws and regulation in this space as well because, you know, we've sufficiently **freaked out society** and they're distracted, they're not focused on the right things." * * *

"[...] **if there's an online account that's compromised today, it's a big headline. It's news everywhere, and I think we need to get people to the point where they're comfortable enough with this new normal, that they don't freak out every time. Because again, that fear is where it makes it really difficult for them to make smart, logical decisions about what to do next."**

"Cybersecurity today: Turning positive with new thinking and innovation" (emphasis added), https://www.helpnetsecurity.com/2017/03/20/cybersecurity-today/

Cyber Security ➔ Weather

- **My new goal is to help people think about cyber security events the way they think about the weather.**

- **We normally don't get too excited about the weather, we just cope with it.**

- It it looks like it's going to rain or snow, we take along rain or snow gear.

- If it's warm and breezy, we enjoy those glorious days..

- But, if there is severe weather coming, we prepare and respond appropriately to that, too. We just don't freak out.

Internet Metaphors Are Not New

- Analogies between the online world and the real world are common and often strained and painful (sorry).
  - "Surfing the Internet wave..."
  - "Riding the information super highway..."
  - "We need a cyber healthcare initiative to cure infected computers..."
  - etc., etc., etc.
- The notion of Internet-as-weather IS yet another cliché, but if it makes everyone calm down and quit reacting hysterically about cyber security, putting up with yet another cliché may be worth it. It's hard to get really hysterical about "cyber drizzle."
- In fact, let's make cyber security really mundane. Let's MEASURE it.

III. Cyber Security Statistics

"To measure is to know."

Lord Kelvin

"Are Things REALLY Going Pretty Well Online?"

- If there's any disagreement over whether things are going well (or going poorly), surely we can just **"check the numbers" and find out what's really true...** This is certainly true in most other fields.
- If someone asserted that the economy is going well (or badly), **economists** could produce studies that document the market is up, or productivity is down, or the balance of trade is unchanged, etc.
- In healthcare, if we wondered how the fight against cancer is going, **doctors** can tell us how many people are newly diagnosed each year, and how many patients are cured or in remission etc.
- Heck, even in **sports** we keep extensive statistics.
- But in **cyber security**, there's often a curious/disconcerting lack of explicit measurements from security researchers or government agencies for something so apparently important, and make no mistake, **cyber security metrics ARE important (if hard to get).**

Some Users of Cybersecurity Metrics

- Metrics tell **the government** whether additional legislation/ regulation (or additional funding) may be needed for cyber security
- Metrics tell **ISPs** how much they might have to spend to clean up botted customers
- **Security software and security hardware vendors** use metrics to help prioritize their R&D for new cybersecurity products
- **Law enforcement agencies** may use cybersecurity metrics to prioritize their limited law enforcement resources ("worst bot?")
- **Users** may even use cyber security metrics to help inform decisions about who or what to trust online.
- See "Bot and Botnet Metrics Guide (Analysis & Recommendations), page 64, Appendix 4, WG7, FCC CSRIC III https://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG7_Report_March_%202013.pdf

Many WANT Hard Numbers About Cyber, But There May Be Few Numbers To Be Had

- **In fact, we actually don't know some pretty basic information about cyber security.**

- For example, consider **malware**. Arguably, malware is one of the biggest cyber security threats.

- We know that our **vulnerability to malware can be greatly reduced if systems are running the latest operating system (and are fully patched up-to-date).**

- **So what fraction of our systems are running Windows, but not Windows 10?**

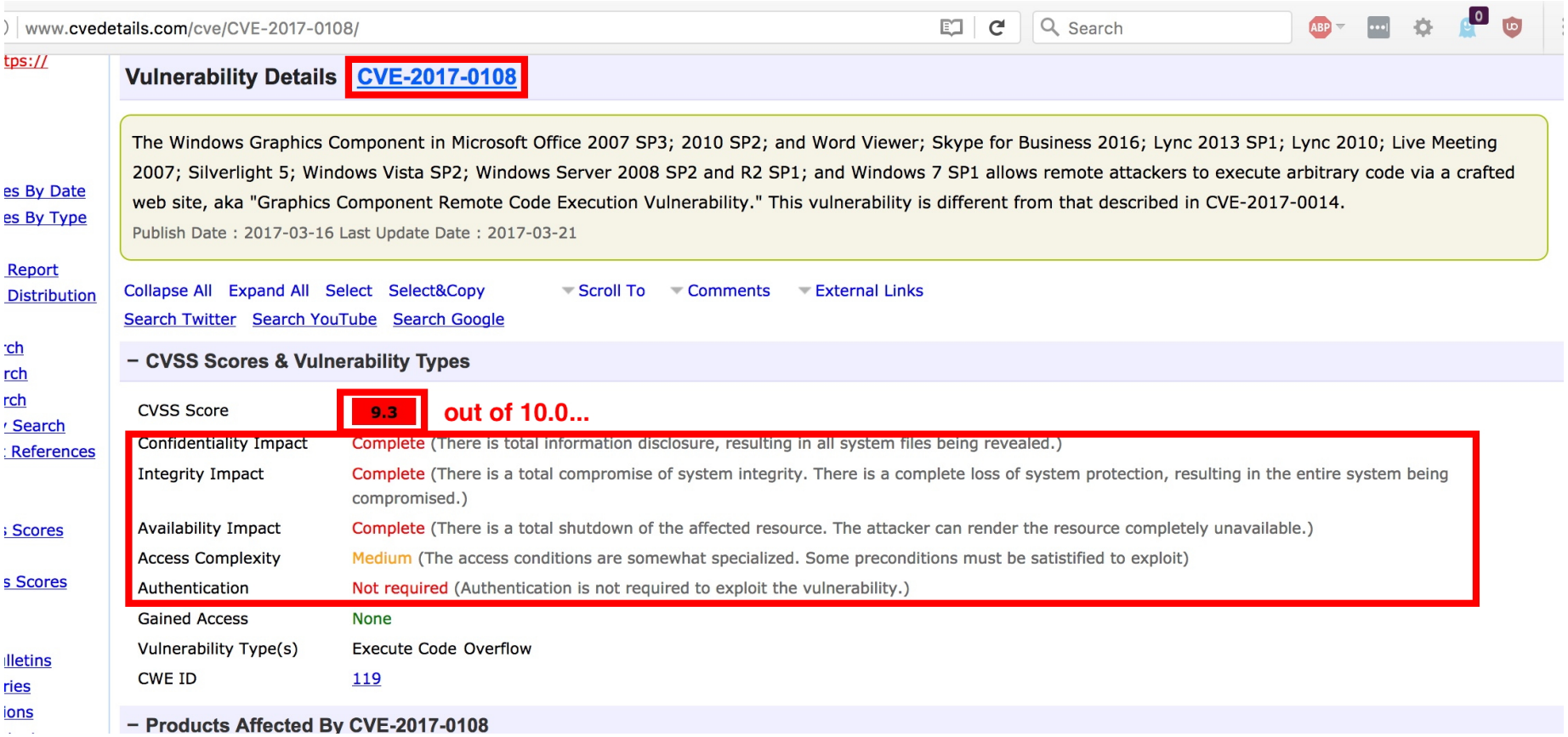
Or Heck, "Tell Me About Windows 7 Usage..."

- Windows 7 was originally **introduced** in **Oct 2009, 7+ years ago.**
- Windows 7 went end of **mainstream support** on **1/13/2015.**
- Windows 7 will go end of **extended support** on **1/14/2020.***
- **Users should really be upgraded by now (but many still have not).**
- **Maybe YOU'RE still running Windows 7? Are you at least carefully patching? Patching is VERY IMPORTANT.**

---

* http://www.pcmag.com/article2/0,2817,2475079,00.asp

Example Of A Recent Vulnerability in Windows 7



This is just **ONE of 700 vulnerabilities, avg. weighted CVSS 7.1** (as of 4/16/2017) found in Windows 7... This vulnerability was patched by Microsoft on March 14th, 2017.

Is Having 700 Vulnerabilities (Over 7 Years) "Bad?"

- Assume you have three choices:

  a) Have **zero vulnerabilities** (that have been reported and fixed)
  b) Have **350 vulnerabilities** that have been found, responsibly disclosed and corrected
  c) Have **700 vulnerabilities** that have been found, responsibly disclosed, and corrected

- Flaws that have been **found and fixed** are flaws that no longer exist, at least IN PATCHED SYSTEMS.
- A large number of flaws may be an indicator that code has been **thoroughly scrutinized,** and **virtually all issues uncovered**
- A large number of flaws may also be a sign that **poor programming practices were employed, and numerous latent flaws still remain.**
- How does this compare to some other operating systems?

What About Windows 10? OS X? iOS? Android?

- **Windows 10: 269 over 3 years, weighted average CVSS: 6.9**
  https://www.cvedetails.com/vulnerability-list/vendor_id-26/product_id-32238/Microsoft-Windows-10.html
- **Mac OS X: 1817 over 18 years, weighted average CVSS: 7.4**
  https://www.cvedetails.com/product/156/Apple-Mac-Os-X.html?vendor_id=49
- **Apple Iphone OS: 1176 over 11 years, weighted average CVSS 6.7**
  https://www.cvedetails.com/product/15556/Apple-Iphone-Os.html?vendor_id=49
- **Android: 880 over 9 years, weighted average CVSS 8.1**
  https://www.cvedetails.com/product/19997/Google-Android.html?vendor_id=1224
- **NO vendor makes a totally flawless operating system.**
- **Should we EXPECT ~100 vulns/product/year on average?**

Could We Scan The Network To Find The %-age of Connected Hosts Still Using Windows 7?

- **Sure. In fact, your school may ALREADY be scanning campus systems to find Windows 7 systems that need updating.**
- **That said, we could (in theory) scan the entire global IPv4 Internet in just 3 minutes with *masscan*** (given a 10Gbps network connection), **BUT** because many systems are:
    - behind firewalls and/or
    - using private address space (NAT/PAT),

  it may be impossible to actually assess many of those systems.
- **Firewalls and private address space are an example of a both-good-AND-bad "security technology" -- firewalls and NAT may help tactically, but hurt our "big picture" strategic understanding.**

---

* blog.erratasec.com/2013/09/masscan-entire-internet-in-3-minutes.html

Agent-Based ("Phone Home") Reporting

- Obstacles like firewalls can be overcome via agent-based methods, e.g., small programs running on systems that connect **outbound** through firewalls to periodically "report in" about the current status of the system where they're running.
- *Surprise!* Microsoft 10 (and now even Windows 7 for that matter) includes a telemetry component called "Universal Telemetry Client" (or DiagTrac), see http://www.zdnet.com/article/windows-10-telemetry-secrets/ and https://tweakhound.com/2015/11/02/windows-7-diagnostics-tracking-service/
- Some antivirus products have similar reporting capabilities.
- **If you have stringent privacy concerns,** you may want to consider disabling reporting, or potentially block those connections at the network level − but note that doing so may hamper the security community's understanding of Windows ecosystem, just like people who try to dodge the Federal census taker.

Some 3rd Party Statistics About Windows 7 Use...

- *Duo Security:* "Of all Windows devices analyzed, **65 percent** are running Windows 7..."*
- *NetMarketShare's graph:* Windows 7: **49.42%****
- *StatCounter Desktop Windows Versions Market Share Worldwide March 2017:* **47.06%*****
- *W3Schools OS Platform Statistics, March 2017:* Win7: **33.2%******
- ***Note that range -- from 33% to almost exactly 2X that! WOW...***

---

* https://duo.com/assets/ebooks/2016-Duo-Security-Trusted-Access-Report-Microsoft-Edition.pdf

** https://www.netmarketshare.com/operating-system-market-share.aspx?qprid=10&qpcustomd=0

*** http://gs.statcounter.com/os-version-market-share/windows/desktop/worldwide

**** https://www.w3schools.com/browsers/browsers_os.asp

"How Did Those 3rd Parties Get Their Stats?"

- **Web logs** commonly include operating system information (but note that users can change their user agent string, see for example https://www.howtogeek.com/113439/how-to-change-your-browsers-user-agent-without-installing-any-extensions/)
- **Application installers** may detect operating system information during installation, and then report that data (hopefully after first asking for permission to do so!)
- **Users may select from different versions of products** based on the O/S they're using ("Click here to download Foo for **Windows 7**")
- Researchers may **scan the systems that they *can* reach**
- **Analysts may track aggregate new system sales**
- **Pollsters may ask users to self-report** what they're using
- These and other measures will NOT be unbiased estimators, so take any such estimate as being only a VERY rough approximation.

"Why Don't All The Stats About Windows 7 Agree?"

- People may measure **different things, different ways...**
- Are we looking at stats for just the **United States**, or the **whole world?** (keep in mind that systems located in Indonesia may have the same attack potential as systems located in Idaho)
- Are we looking **at stats JUST for laptop/desktop users**, or stats for **all Internet-connected devices?** (including virtual machines, smart phones, servers, tablets, Internet of Things devices like home security cameras and "smart" light bulbs, etc.?)
  Note that HALF of all Internet-connected devices worldwide may now consist of Android devices...
- If interested, see 'On "Normalizing" or "Scaling" Cybersecurity Metrics and Measuring The Right Thing For The Right Entities,' http://www.cybergreen.net/2016/03/29/2016310on-normalizing-or-scaling-cybersecurity-metrics-and-measuring-the-right-thing-for-the-right-entities/

Practical Information: Upgrading to Windows 10

- **Many colleges or universities may have a Microsoft license plan that covers upgrades for institutional systems. Does yours?**
- Microsoft offered a free upgrade to Windows 10 for the general public until July 29th, 2016. That free upgrade offer is now over, unless you're a customer who uses assistive technologies. If you ARE such a user, see https://www.microsoft.com/en-gb/accessibility/windows10upgrade for a free upgrade path.
- Otherwise you can still buy Windows 10 Home for $120 or Windows 10 Pro for $200 (academic discounts may apply), see https://www.microsoftstore.com/store/msusa/en_US/pdp/Windows-10-Home/productID.319937100
- In still other cases (such as old, slow, or systems that have had hard lives (like some laptops)) it may make more sense to replace your system entirely given that a brand new laptop complete with a license for Windows 10 starts at around $300.

"Didn't I Read Something About US-CERT Telling Users That Windows 7 Was Better Than Win 10?

- You may be thinking of **"Windows 10 Cannot Protect Insecure Applications Like EMET [Enhanced Migration Experience Toolkit] Can,"** see https://insights.sei.cmu.edu/cert/2016/11/windows-10-cannot-protect-insecure-applications-like-emet-can.html
- The comparison in that post is really between **FOUR** options: Win 7 (without EMET), Win 7 (with EMET), Win 10 (without EMET) and Win 10 (with EMET). A table that was added to the article makes it clear that EMET delivers substantial protections to both Win 7 and Win 10, and Win 7 WITH EMET offers more protections than Win 10 WITHOUT EMET. Unfortunately Microsoft is likely still planning to dump EMET on July 31st, 2018. So at least as of July 31st, 2018, Windows 10 will then become the most secure option available (w/o EMET). See also https://blogs.technet.microsoft.com/srd/2016/02/02/enhanced-mitigation-experience-toolkit-emet-version-5-5-is-now-available/

Bottom Line Recommendation

- **If you're still using Windows 7, I think it's time to upgrade to Windows 10 UNLESS you have a specific application that prevents you from doing so, or your local support people tell you not to.**

- Why upgrade? It isn't anything apocalyptic, it's just like trading in your old 200,000 mile Honda or old Ford Pickup when you get the chance... Yeah, that rig may have given you a lot of good miles, but the time comes when it makes sense to get something a little newer and safer and more fuel efficient and more reliablethat you don't have to tinker with or worry about. Don't be too sentimental.

- BTW, does your site have a specific policy encouraging users to at least stay on a fully Microsoft-supported version of Windows, if you're going to use Windows? If not, maybe that's something to consider?

Don't Forget All Your OTHER Software, Too!

- Once you've got your operating system upgraded and patched, fix all the rest of the software you've got loaded on, too... Your web browser(s), your email client, Microsoft Office, Adobe Reader, Oracle Java, etc., etc., etc.
- The best tool for flagging software in need of an upgrade on the PC is probably Secunia.
- On private systems, see https://www.flexerasoftware.com/enterprise/products/software-vulnerability-management/personal-software-inspector/ (free)
- For institutionally owned and managed systems, consider Secunia CSI, see https://www.flexerasoftware.com/enterprise/products/software-vulnerability-management/corporate-software-inspector/

Alternatives to Windows

- While we're talking about operating systems and apps, let me also remind you that **there are alternatives to Windows.**
- If you spend much time at national or international cyber security meetings, one thing immediately hits you: **there are LOTS of Macs at those meetings.**
- People who do cybersecurity for a living tend to prefer Macs for many reasons, but a major one is that **only a tiny fraction of all malware targets Mac users.** To make that concrete, McAfee says that there are over 600 million different pieces of known malware (see https://www.mcafee.com/us/resources/reports/rp-quarterly-threats-mar-2017.pdf at page 36). But, there are just over 450,000 pieces of Mac malware (see page 39 of the same report). 450,000/600,000,000*100➔0.075%
- Maybe there's a Mac in your future, some day, too?

What About Smart Phone OS's?

- **A large fraction of all mobile malware** (estimates are around 97%, see for example https://www.scmagazineuk.com/updated-97-of-malicious-mobile-malware-targets-android/article/535410/) **targets Android.** Advantage goes to **any** non-Android smart phone.
- Part of the issue is that **only 50% of Android devices are getting updated** (see https://www.wired.com/2017/03/good-news-androids-huge-security-problem-getting-less-huge/), and only 3% of Android phones are running the latest Android O/S ("Nougat") while "nearly 80%" of iOS devices are running iOS 10.
- Now add to that the fact that it is common for many Android users to **jailbreak** their phones, loading "free" apps from "third party sources" where at least some content may routinely be malicious.
- However, even here, there is substantial room for optimism: as noted in the Wired article cited above, Google has made substantial progress in increasing deployment of Android updates.

IV. Data Breaches

"Data breaches often result in CEO firing"

http://www.csoonline.com/article/3040982/security/data-breaches-often-result-in-ceo-firing.html

What's A "Data Breach?"

- In a data breach, an unauthorized person gains access to your personal or financial data.
- For example:
  - An intruder at a college or university gains unauthorized access to **student academic records.**
  - A business that takes credit cards is compromised, and an online criminal **gets customer credit card numbers, plus maybe the credit card owner's name and billing address.**
  - A disgruntled insider downloads a copy of **a proprietary customer list,** perhaps for sale to a direct competitor.
  - A doctor's unencrypted laptop is stolen, potentially exposing **details about her patients and their health care.**
  - Computers are sold as "surplus" with **intact hard drives**
  - These are just a few of **many** possible breach scenarios...

Recent Headlines From The Data Breach Wars

- "**Yahoo says new hack affected 1 billion users, separate from earlier attack**," http://www.cnbc.com/2016/12/14/yahoo-says-new-hack-affected-1-billion-users-separate-from-earlier-attack.html
  But do you know anyone who still uses a Yahoo account for email? I sure don't. So who ARE those "billion users?"

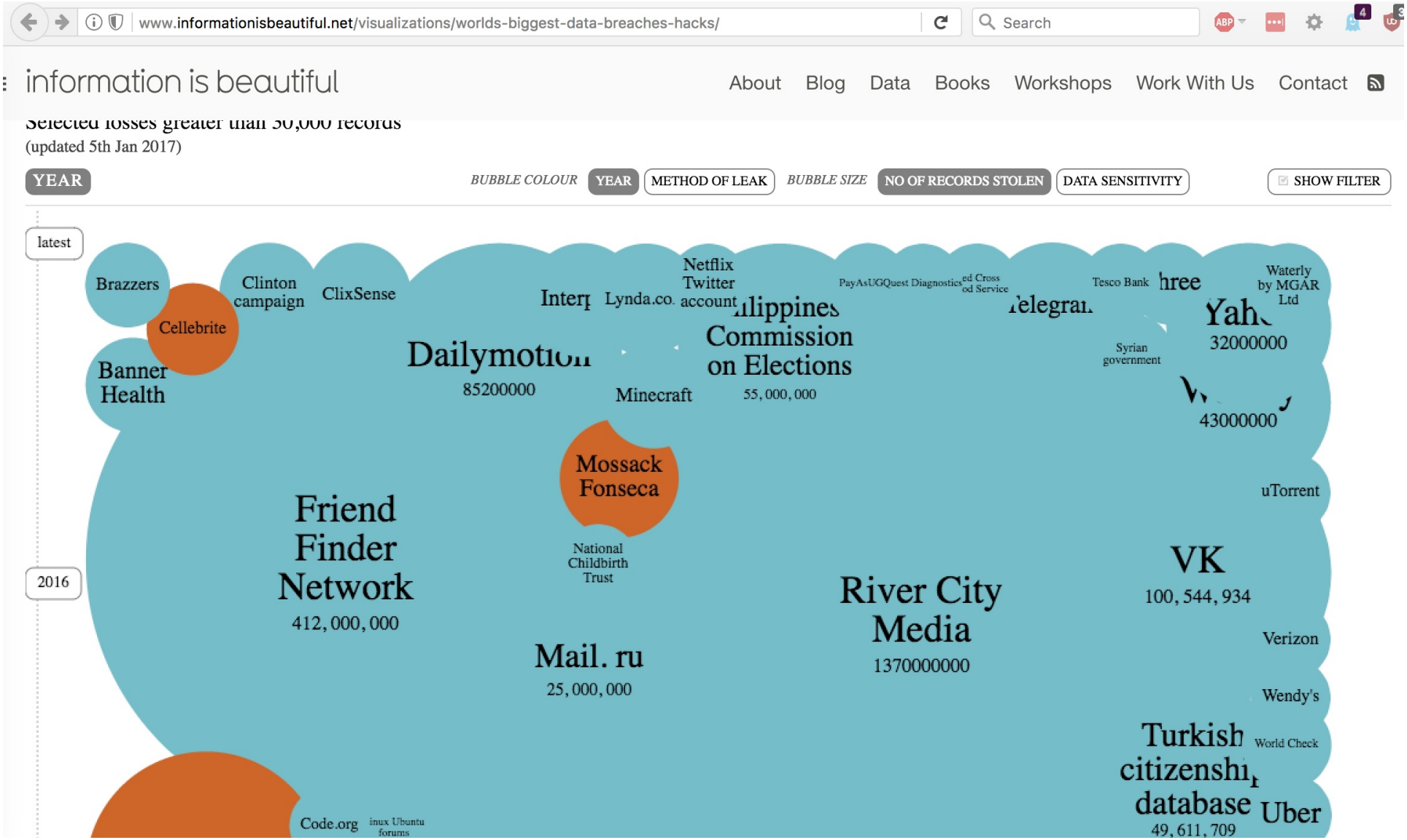
- **"Spammergate: The Fall of an Empire,"** https://mackeeper.com/blog/post/339-spammergate-the-fall-of-an-empire
  "The situation presents a tangible threat to online privacy and security as it involves a **database of 1.4 billion email accounts** combined with real names, user IP addresses, and often physical address."
  But wait, is that even PII? In some states, I suppose yes...

On The Other Hand...

- **"LeakedSource and its database of hacked accounts is gone,"** https://www.engadget.com/2017/01/27/leakedsource-data-breach-notification-site-down/

- "A website that sold access to a database of more than **3 billion hacked accounts** has suddenly vanished. LeakedSource had built a business on collecting and packaging information exposed through various data breaches. It gathered compromised account details and made it searchable so users could see which of their email addresses, phone numbers and passwords were vulnerable. [...] The circumstances surrounding the site's disappearance are murky. A user going by "LTD" wrote [...]: "LeakedSource is down forever and won't be coming back. Owner raided early this morning. Wasn't arrested, but all SSDs got taken, and LeakedSource servers got subpoena'd and placed under federal investigation [...]"

Recent Breaches, ALL INDUSTRIES, Visualized



Recent Breaches IN ACADEMIA Visualized

There's a Tradition in the Cyber Security Industry of Bashing Higher Ed As Being "Weak" On Cyber...

- For example, CloudMask says "Did you know that since 2005, higher education hacks were responsible for 35 percent of all data breaches and that there is at least one attack on colleges and universities every week?" (https://www.cloudmask.com/videos/higher-education-has-high-risk-of-data-breach-video)
- Or consider "The threat landscape in higher education is more dangerous than ever. In 2016 to-date, the education sector rose to the No. 2 most targeted sector in Symantec's most recent Internet Security Threat Report, moving up from the No. 3 spot last year. [...] colleges have historically lagged behind the corporate sector when it comes to paying attention to data security, embracing the best cyber-security technology available or modernizing their IT environment form a cyber-security defense point of view." (https://www.netswitch.net/education-2-target-for-cyber-attacks-in-2016/)
- **Grr...** Note the fear-based attempt at cyber security selling.
- **Personally, I think higher education takes cyber security VERY seriously. That's reflected in data breach stats for MT higher ed.**

The Breach Problem by The Numbers for Montana

- **Montana's Department of Justice web site lists 472 data breach incidents affecting Montanans, see https://dojmt.gov/consumer/consumers-known-data-breach-incidents/**
- If we use the form on that page, we can see incidents per year:
  - 2017 (through April 9th): 54
  - 2016: 305
  - 2015: 91
  - 2014: 11
  - 2013: 3
- **Searching for "university" the site returns 12 listings, affecting a total of 517 Montanans (none from a university actually located in Montana). Searching for "college", we find another 9 listings affecting 27 Montanans (none from a Montana college). That's pretty good.**

Keeping Your PII Breach-Free Streak Intact

- **Outsource institutional payment card processing if you haven't already.**
- **Categorize and inventory** your data. Know where you have PII, and remember that PII may be on **research** systems as well as **administrative** systems.
- **Manage your PII** -- don't just be a data packrat. Delete any records containing PII consistent with your institution's record retention schedule, and don't collect PII in the first place if you can avoid it!
- **Use full disk encryption on all devices**
- **Require two factor auth** when accessing systems with PII
- Run tools to do **PII discovery**; one list of such products is available at https://cuit.columbia.edu/cuit/it-security-resources/handling-personally-identifying-information/pii-scanning-software
- Use **DBAN** to nuke all hard drives before sale or other disposal

V. Spam, Phishing, DNS and The Web

Outbound Spam and MT Higher Ed Institutions

- **Spam can often be a leading indicator of other latent issues.**

- **SenderBase**

  -- https://www.senderbase.org/lookup/?search_string=university%20of%20montana ***no indication of issues***
  -- https://www.senderbase.org/lookup/org/?search_string=Montana%20State%20University ***also okay***

- **Multirbl.valli.org**

  -- http://multirbl.valli.org/lookup/umt.edu.html – ***looks good.***
  -- http://multirbl.valli.org/lookup/montana.edu.html – ***looks good****.*

SPF, DKIM and DMARC

- Three technologies -- SPF, DKIM and DMARC -- are keystones in the fight against spam and phishing, allowing sites to limit who can send using their domain, while taking responsibility for what they DID send, see http://www.openspf.org/ , http://www.dkim.org/ and https://dmarc.org/ for background.
- SPF, DKIM and DMARC aren't tools that end users can individually use, but those who run your mail servers can use them to protect all users. They aren't completely painless, but the pain of using them is generally worthwhile.
- **umt.edu** isn't using any of these protections (as far as I can tell).
- **montana.edu** is using SPF, albeit rather loosely (e.g. permitting sending from all of 153.90.0.0/16 plus some other sources).
- Maybe consider adding these technologies if you get a chance?
- Helpful tool: https://dmarcguide.globalcyberalliance.org/#/

Phishing

- Phishing schemes typically try to use **social engineering** to connive users into revealing their username and password, or perhaps payment card information.

- In some extreme cases**, malware on a system may automatically intercept and forward credentials as they're being entered.**

- **The best defense against phishing is a skeptical and educated user base.** Never allow yourself to be rushed or panicked into doing something "urgent." Montana and Montana State both have pretty good phishing advice pages, too, in my opinion.

  -- https://www.umt.edu/it/security/phishing/default.php
  -- http://www.montana.edu/uit/malware/phishing.html

Defeating Phishing With Multifactor Auth

- The next anti-phishing step is **multifactor authentication.** If a bad guy/bad gal needs to use a 2nd factor to authenticate as "you," you've just erected a *major* roadblock against phishing.

- I notice that both Montana and Montana State are members of InCommon.org, see https://www.incommon.org/participants/ , **and** they subscribe to the InCommon Cert Service that I used to run (https://www.incommon.org/certificates/subscribers.html).

- **However it looks like neither school has yet elected to take advantage of InCommon's Duo Security Multifactor offering** (which I also used to run) (You can see the 128 colleges or universities that ARE doing so at http://www.incommon.org/duo/subscribers.html).This might be something worth considering...

Another Very Cool Anti-Phishing Technique

- Another anti-phishing/anti-malware technology option to know about: consider creating a DNS "firewall" via your recursive resolvers by using **DNS RPZ (Response Policy Zones).**
- In a nutshell, RPZ teaches your recursive resolver (such as BIND) to "lie" about evil domains (such as those known to be involved with malware or phishing). You can use RPZ to make those domains not resolve, or you could redirect users to an educational website instead of the real one. See **https://dnsrpz.info/** for more info.
- Full disclosure: Paul Vixie and Vernon Schryver of Farsight Security wrote the IETF draft for the DNS RPZ protocol, see https://tools.ietf.org/html/draft-vixie-dns-rpz-04 however you can use anyone's RPZ feed you want, or even create your own if you feel so inclined (this is NOT a "Farsight only" solution). You can use RPZ and we'd not necessarily ever see a dime from anyone.

Web Crypto Configurations?

- One of the other things I like to check when I talk with folks is their web crypto configuration. The cryptographic configuration of web servers can be quite complex, and easy to get wrong, so it's always worthwhile to double check out how things have been set up.
- My favorite tool for this is: https://www.ssllabs.com/ssltest/
- Checking **www.umt.edu, it earns an "A" rating,** good job!
- Checking **www.montana.edu, it only gets a "B" rating** due to using weak (1024 bit) Diffie Hellman Ephemeral (DHE) key exchange. (BTW, see https://weakdh.org/sysadmin.html for information on how to fix that issue)
- Note: most universities have LOTS of https web servers, not just www.[domainname]. Staff should test EACH such system to ensure that all systems have their SSL/TLS settings appropriately configured.

DNS Configuration

- At the same time I check web crypto configuration, I also normally check a site's DNS configuration. My favorite tool for that is the free site http://dnscheck.iis.se/

- Checking umt.edu, I see "All tests are OK" (good!) although I'm not seeing IPv6 or DNS support at this point.

- Checking montana.edu, I see "All tests are OK" (good!) although I'm not seeing IPv6 or DNSSEC at this point.

- Adding IPv6 and DNSSEC would be two more great projects to consider tackling when you have the chance. In the mean time, good job on the rest of your DNS infrastructure!

Contribute Data To SIE?

- While we're talking about DNS, I should mention that Farsight is always seeking additional DNS data contributions for the Security Information Exchange (see https://www.farsightsecurity.com/solutions/security-information-exchange/). SIE feeds many projects, including Farsight's own passive DNS database, DNSDB (see https://dnsdb.info/)
- Because of how we collect that data (e.g., above large shared DNS recursive resolvers), no PII gets collected and user privacy is carefully preserved. Contributing data ensures that if a security incident does arise at your site, there's an excellent chance that the passive DNS data needed to work it will be available in DNSDB. Contributing data also helps the anti-abuse community fight cyber crime, and supports academic research.
- For more information, drop me a note at stsauver@fsi.io

VI. Backups

"If you've got two, you've got one."

Aphorism reportedly from the military special operations community, recommending backups for everything

Backups

- **Backups are the MOST BORING THING IN THE WORLD,** UNTIL you need them, whether we're talking about a 2nd motor on your old fishing boat or a backup copy of your hard drive.
- Historically, **hardware failures** used to be the prime reason why we'd encourage people to backup their systems: drives would routinely fail *then*, and they still fail *today* (although not as often).
- Nowadays, however, backups also make a huge difference if your system is **lost or stolen**.
- And backups these days can be an absolute lifesaver if you get hit with **"ransomware"** (encrypting malware such as Cryptolocker).
- WITH clean backups, ransomware can be just a nuisance.
- WITHOUT clean backups, your pain will be a lot greater although sometimes you may be lucky and have the ability to use a free decryptor, see for example https://noransom.kaspersky.com/

RAID Mirror, Plus Local Backup, Plus Cloud Backup

- If you're a **belt and suspenders** sort of person consider having multiple approaches to backing up your system.
- For example, if you have room for a pair of drives, consider **mirroring** them. This is the most painless sort of protection against hard drive failure.
- Mirroring will NOT protect you against loss of data if your system is lost, stolen, destroyed or subject to data corruption − both drives will probably suffer the same fate.
- That's why you ALSO want to ensure that you have additional backups. Maybe you'll decide to buy a multi-terabyte external hard drive for a hundred bucks or so, and do backups to that − just don't leave it hooked right next to your system − it might burn down right along with the system it's backing up!
- As insurance against that sort of failure, you might want to have yet another backup online, "in the cloud."

Encryption; Multiple Generations; Do A Test Restore

- Backups can contain highly sensitive information. You need to protect them from unauthorized disclosure UNLESS they've been protected with strong encryption. **We strongly encourage you to encrypt your backups**, just be sure to safeguard the key you'll need to decrypt them!
- When taking backups, keep **multiple generations.** Why? Well, imagine that you only keep one generation, and you find that your system has become infested with something nasty. You go to roll back to your most recent backup, but you find that IT TOO has the same problem. Wouldn't it be nice to be able to go FURTHER BACK? Do your best to keep multiple generations of your backups!
- TEST your backups! Try restoring some files, and make sure that they checksum identically to your originals.
- Spread the backup "gospel" to your friends and family, too. I predict they'll thank you for it some day.

V. OTHER Personal Steps

Everything is perfect and
there is always room for improvement.

Shunryu Suzuki

Antivirus

- We all know that antivirus is struggling (and often failing) to keep up with the tide of malware that's in circulation.

- Nonetheless, it WILL catch some malware, and that's better than nothing, so you SHOULD still typically run an antivirus product. This is particularly true for Windows and Android mobile devices, but all systems can ootentially benefit.

- If your school doesn't provide an antivirus product for you at no charge, you may want to see the review that's at

  -- "The Best Antivirus Protection of 2017" (April 11, 2017)
  http://www.pcmag.com/article2/0,2817,2372364,00.asp **or**
  -- "The Best *Free* Antivirus Protection of 2017" (April 17, 2017)
  http://www.pcmag.com/article2/0,2817,2388652,00.asp

Personal Firewalls

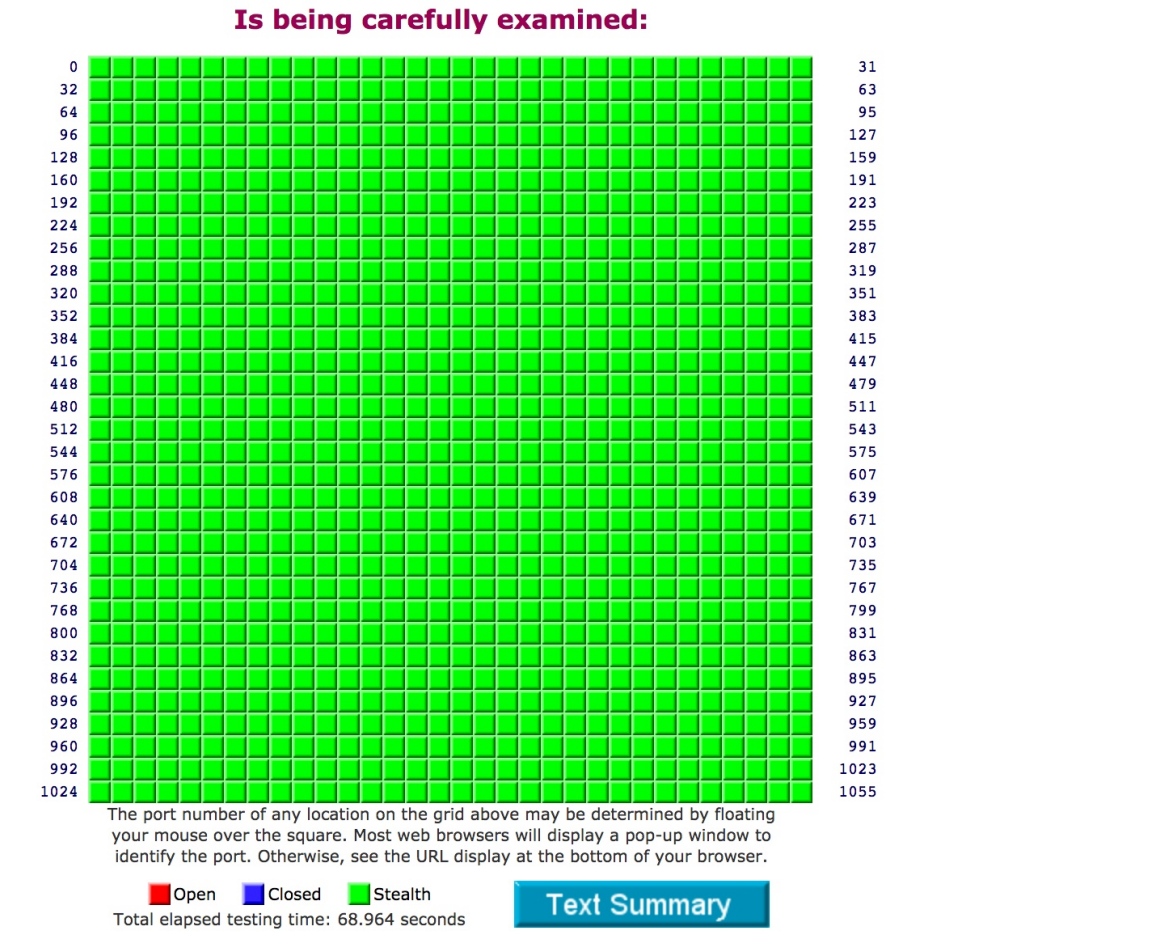
- My attitude toward personal firewalls has evolved over time.

- At this point in time, it DOES probably makes sense for you to have some sort of software packet filter that blocks incoming connections by default. The integrated Windows 10 firewall, and the integrated Mac OS Sierra firewalls are fine, but if you don't like them, pick an alternative, just run SOME sort of software firewall.

- Hardware firewall devices have also come a long way. While you should NOT stand up your own wireless access point without coordinating with/receiving permission from your local networking staff, you SHOULD consider installing a hardware firewall in front of your hardwired systems if this is allowed at your school (and certainly deploy one if you're living in a house or off-campus apartment) with commercial ISP connectivity.

Firewall Testing With ShieldsUP! (All Green==Good)

https://www.grc.com/x/ne.dll?bh0bkyd2



Passwords and Password Managers

- One of the other best things you can do to improve your security is to use a **password manager. M3AAWG** agrees, see https://www.m3aawg.org/sites/default/files/m3aawg-password-managers-bps-2017-03.pdf). Password managers help you to use long-and-strong passwords without going crazy, even if you have dozens and dozens of different accounts. If you don't already use one, I strongly encourage you to consider doing so.
- Normally this is the point when someone asks, "So which ONE do you recommend I use?" I encourage you to read some of the reviews that are available from popular computer and networking magazines − most of them should work fine, but do your own due diligence. One starting point:

  "The Best Password Managers of 2017," April 17, 2017
  http://www.pcmag.com/article2/0,2817,2407168,00.asp

Ad Blocking/Blocking Online Trackers

- Many of the Internet's must popular free sites are supported by online ads. Unfortunately, online ads can also serve as an "express lane" for dropping malware on your system. Taking ads on your PC is generally totally discretionary.
- Therefore I'd encourage you to routinely **block them** with an ad blocking tool. It will help your security, and reduce distractions, too.
- It is perhaps noteworthy that **Adblock Plus** is the **#1 add-on for Firefox**, used by nearly 17 million users, see https://addons.mozilla.org/en-US/firefox/extensions/?sort=users
- While you're sanitizing your browsing experience, you may also want to consider running **Ghostery**. It blocks many of the trackers and other tools advertisers deploy in an effort to track you. Again, those trackers are not needed, so block 'em!

Use Whole Disk Encryption

- Whole disk encryption has become a staple recommendation at many sites.

- Does Montana or Montana State encourage or require use of whole disk encryption?

- If not, I'd encourage y'all to consider doing so...

- Some starting points:

  "The Best Encryption Software of 2017"
  http://www.pcmag.com/article/347066/the-best-encryption-software-of-2016

VII. Conclusion

Cyber Security Has Gotten A LOT Better

- No matter how many fear-inducing spiels you may hear, don't let the pessimists scare you.
- If you pay attention to basic cyber security chores, your chances of staying safe online are really quite good (although obviously I can't guarantee you won't get hit by a bolt out of the blue, even if you've done everything a reasonable and prudent person might)
- If things DO go awry for you, some basic steps (like backing up your system, and using whole disk encryption) can make the consequences a lot less dire than they otherwise might be.
- At the same time that end users need to do their bit, central IT staff need to do their part, too. In my opinion the UMT and Montana State teams have done a pretty good job to date, although there are always new options to explore.
- **Thanks for the chance to talk today! Are there any questions?**