Cybersecurity (for information professionals)

DR. LYNNE WILLIAMS, MASTER'S OF SCIENCE IN CYBERSECURITY FACULTY, KAPLAN UNIVERSITY

What is cybersecurity anyway?

According to the U.S. Department of Homeland Security, cybersecurity:

- Concerns preventing unauthorized access or manipulation of:
  - Computers, mobile devices, tablets, networks, “things”, and data (either at rest or in transit)

Security Is Inconvenient

The more robust the security mechanisms, the more inconvenient the process.

What is the balance between security and productivity?

- Based on an acceptable level of risk
- Security/inconvenience ↔ insecurity/ease of use
  - Example: waiting in a security line at the airport

The Current Trend: Share, Not Protect

- Users want:
  - To share data with everyone
  - To access data from anywhere, and quickly
  - To have the same capabilities at home and at work
- Data is shared through web applications, social networking, and online data storage

The Bad Guys Are Very Sophisticated

- Security is a process dependent on **people**
  - Requires time, training, and equipment
- The new hacker profile
  - Profitable businesses: e.g., Anonymous
  - Hierarchical cybercrime organizations
  - State-sponsored hacking
- Creating a secure infrastructure is mandatory in the 21st century, no matter what business you're in

Beware of Common Misconceptions

- What are some common security misconceptions?
  - Our organization is simply not a target for malicious activity
  - Our organization is immune from employee problems
  - IT professionals know everything about computers

What is the “risk landscape” of an organization?

- All organizations have unique cyber security risks in relation to their interaction with public data and the Personally Identifiable Information [PII] of patrons.
- Developing and delivering a risk management program that addresses every cyber security issue with limited IT resources is not only impractical to implement, but impossible to maintain.
- Information professionals must prioritize and focus on high probability cyber risks to guide their cyber defense efforts.

What is the “risk landscape” of an organization?

- Bottom line: even if you aren’t an IT geek, as an information professional, you need to at least be aware of cybersecurity in the current networked environment.

What is the “risk landscape” of a library?

- Libraries, especially public libraries, have an outstanding record of protecting the privacy of their patrons.
- However, some of the traditional tenets of good library administration are directly in opposition to good cybersecurity practice.

What is the “risk landscape” of a library?

- Two important security problems often not addressed in libraries.
  - Privacy offered for data that may be collected or collectable apart from circulation records, such as browsing history.
  - Risk of penetration of library systems from outside parties who may access circulation or other data.

What is the “risk landscape” of a healthcare facility?

- House both personal health and payment - insurance information
- Providers, payers, employees, patients, and other stakeholder information is increasingly intertwined
- Shared data and the increasing use of data analytics provide growing opportunities for loss, error and theft

What is the “risk landscape” of a healthcare facility?

- World Health Organization reports that:
- In healthcare facilities, 46% of all breaches occurred due to theft or loss, with insider abuse causing 15% of incidents, and point-of-sale intrusion causing 9% of incidents.
- Outsiders, such as contractors and suppliers, accounted for 68% of ALL breaches and errors

What are the potential consequences?

- In 2016, hospitals worldwide are getting hit with ransomware attacks:
- One of the most severe cases involves Hollywood Presbyterian Medical Center, based in Los Angeles, which declared an "internal emergency" after staff noticed an apparent ransomware outbreak begin on Feb. 5. The attackers reportedly demanded 9,000 bitcoins, currently worth about $3.6 million. However, in a Feb. 17 statement, the hospital's CEO Allen Stefanek said reports of the ransom being over $3 million were incorrect, and that the hospital paid about $17,000 , or 40 bitcoins, to the attackers to unlock its data. (Schwartz, 2016)

What are the potential consequences?

- Disgruntled employee sending anonymous threatening emails to their employer or colleagues.
- Teenager using stolen credit card to get access to porn or gambling sites.
- Terrorists researching various scenarios or moving money, using public connection to avoid leaving a trail on their own equipment.

What is the “risk landscape” of an organization?

- Consider Web browser software often found on shared computers:
  - History list of sites visited
  - Copies of recently visited Web pages cached on the computer.
- Will this data be analyzed?
- Should steps be taken to erase the cache after a patron uses a system?
- If a violation of organizational policy were suspected, would Web browsing history data be subject to search by law enforcement?

Minimally, effective cybersecurity should include:

- Staff assigned to information security tasks
- Training all personnel in information security issues and procedures
- Specific policies dealing with information privacy, physical security of equipment, and computer security procedures

Minimally, effective cybersecurity should include:

- Physical security plans
- Data integrity measures
- Levels of access to data or equipment, and monitoring for different types of access

The question is, how do you implement these steps at a time when funding is being slashed to the bone and employees are often working more hours for less pay?

Cybersecurity on a shoestring

- Training all personnel in information security issues and procedures
- Specific policies dealing with information privacy, physical security of equipment, and computer security procedures
- Levels of access to data or equipment, and monitoring for different types of access

Cybersecurity on a shoestring

- Wireless cloud is typically the easiest point of unauthorized entry

Example of easy and cheap ways to mitigate criminal activity

"Public" DNS resolvers, such as Comodo Secure DNS

DNS settings on the organization's router (both wired and wireless) are modified to the public DNS addresses

- All network traffic is now resolved using secure DNS servers that will resolve addresses according to organizational policy
- Protects patron privacy, prevents phishing and pharming attacks, can filter traffic to illegal or undesirable sites
- Can also provide malware protection, depending on the vendor

Example of easy and cheap ways to mitigate criminal activity

Keep track of “input ports”, such as USB ports or optical disk drives

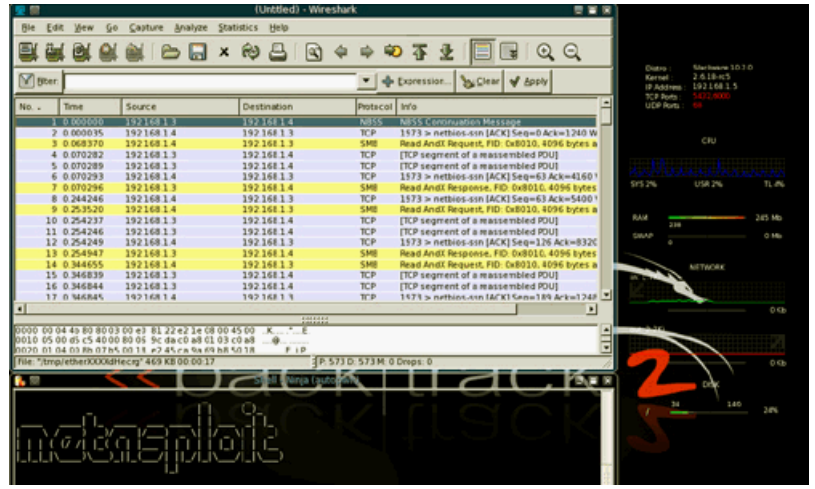
- Example: keylogger

Example of easy and cheap ways to mitigate criminal activity

Keep track of “input ports”, such as USB ports or optical disk drives

- Example: “live CD” (Backtrack)

Allows the user to boot to another operating system without installing anything on the host system. This screenshot is the Backtrack live CD which includes around 300 system tools that can be used to crack passwords, sniff network traffic and other activities.



Example of easy and cheap ways to protect patron privacy

Use the Tor browser on library computers

- Tor is a free, open source software that allows users to surf the web anonymously
- It looks and operates like an ordinary web browser, but leaves no trace of internet activity
- Bonus: drives MI5 crazy because they can't figure out how to track "torrents"

Example of easy and cheap ways to protect patron privacy

Use Bleachbit each evening to clean the library computers

- Bleachbit is a free, open source software that cleans all trace of browsing activity, cached files, temp files and other information detritus
- Not only does it safely clean the flotsam, it can improve performance
- Bonus: drives MI5 crazy because the discarded files are “shredded“ to MoD specifications, very difficult to reclaim data

As if computing systems weren't bad enough: The Internet of Things

- All manner of devices now have embedded operating systems, including your car
- All manner of devices also now have loads of sensors embedded in them
- Sensors collect data related to the use of the device
- Data then gets streamed across the internet… to where? To whom?

(Ndibanie, Hoon-Jae, and Sang-Gon, 2014)

The Internet of Things

- How do you find internet-connected cameras, televisions, refrigerators, and other devices?
- IoT browsers! Shodan is the largest search engine for finding “things”, rather than information.

The Internet of Things

- Shodan searches for anything connected to the internet.
- This includes “nanny-cams”, traffic lights, medical devices and even power plants.
- Shodan isn’t particularly “user friendly”, but can be leveraged by anyone with a few IT skills.
  - IP addressing, some knowledge of how web servers work.

The Internet of Things

ICS-CERT list of more than 300 types of medical device with hard-coded passwords and visible to Shodan, including:

- Glucose meters.
- Surgical and anesthesia devices.
- Fetal heart monitors.
- Ventilators.
- Drug infusion pumps.
- Ventilators.
- External defibrillators.
- Patient monitors.
- Laboratory and analysis equipment.

The Internet of Things

The case of the Trendnet IP surveillance cameras

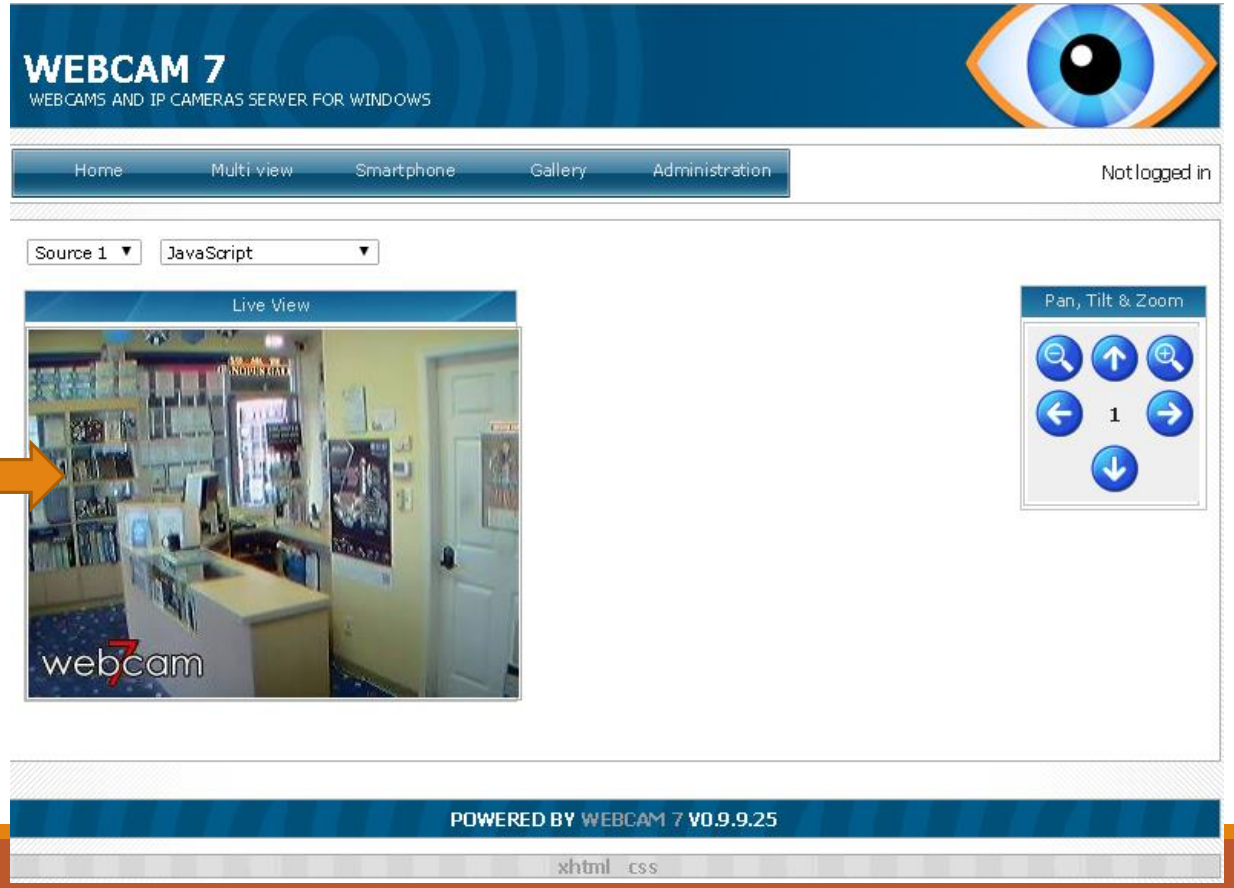
- In 2012, some models of Trendnet IP surveillance cameras were shown to have a security flaw that would allow anyone on the internet to watch what the cameras were watching.

- Any camera owner leaving the cam on default settings allowed anyone who found the cam to view whatever the cam viewed.

The Internet of Things

It’s not just Trendnet cameras, it’s any device set to the default settings

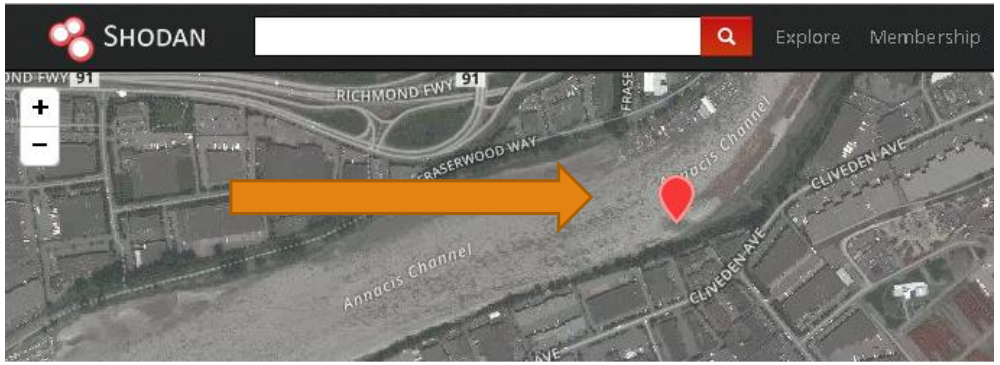
Someone’s store in Canada,
Camera is streaming live.



The Internet of Things

Even worse, it's easy to figure out the store's location

Someone's store in Canada,
Camera is streaming live.



96.49.21.161 S0106001346facf25.vc.shawcable.net

City	Richmond
Country	Canada
Organization	Shaw Communications
ISP	Shaw Communications
Last Update	2014-10-07T02:08:41.152326
Hostnames	S0106001346facf25.vc.shawcable.net
ASN	AS6327

The Internet of Things

It’s easy to figure out a residential address too…

Someone’s living room in
Seattle, WA
Camera is streaming live.

The Internet of Things

Here's someone's wifi router

Note that the router hasn't been updated in years.
Owner probably thinks it's secure because users have to enter a network key to get connected, but the management software is wide open and available on the internet.

The Internet of Things

- **The defaults…**

It’s easy to find lists of default usernames and passwords for just about any vendor…

TrendNET Router Password List

TrendNET		
Model	Default Username	Default Password
TEW-435BRM 1	admin	password
TEW-311BRP	admin	admin
TEW-231BRP	blank	blank
TEW-411BRP+	blank	admin
TW100-S4W1CA	blank	blank
TEW-431BRP	blank	blank
TW100-S4W1CAvF	blank	blank
TW100-BRF1141	blank	blank
TEW-611BRP	UNKNOWN	UNKNOWN
TEW-432BRP	admin	admin
TEW-432BRPv2	admin	admin
TEW-211BRP	admin	1234
TEW-452BRP	admin	admin
TDM-C400	admin	admin
TEW-632BRP	admin	admin
TEW-633GR	unknown	unknown
TEW-511BRP	blank	admin
TW100-S4W1CAv2	admin	blank

Searching The Internet of Things

Don’t assume that none of your devices are connected to the internet, particularly if something has been purchased in the last five or six years. Research your devices using the manufacturer’s web site.

The Internet of Things

MAKE SURE THAT NONE OF YOUR DEVICES, IF THEY HAVE AN ADMINISTRATIVE WEB PAGE, ARE STILL USING THE DEFAULT LOGIN.

Searching The Internet of Things

Be paranoid! Never assume that you can’t be seen on the internet! Research your devices and know for certain what your devices are capable of exposing.

Your webcam could be watching you… even if you think it’s not…

A couple of screen captures

- Sniffing wifi traffic: https://vimeo.com/160891582
- Getting into other people's open webcams: https://vimeo.com/139251506

References

Ashton, K. (2009, June 22). That 'Internet of Things' Thing. *RFID Journal*.

Ndibanje, B., Hoon-Jae, L., & Sang-Gon, L. (2014). Security Analysis and Improvements of Authentication and Access Control in the Internet of Things. Sensors (14248220), 11(8), 14786-14805. doi:10.3390/s140814786

Schwartz, M. J. (2016, February 16). Ransomware Hits Hospitals. Retrieved April 01, 2016, from http://www.bankinfosecurity.com/ransomware-hits-hospitals-a-8872/op-1

Contact:

lwilliams4@kaplan.edu