



---

# CAPITOL TECHNOLOGY UNIVERSITY

---

1927

Emerging Challenges to our Privacy and Data Security:  
What's Next You Ask?

Professor William Butler  
Director, Critical Infrastructures and Cyber Protection  
Center (CICPC)

[whbutler@captechu.edu](mailto:whbutler@captechu.edu)

# Data Breaches



eBay has filed a motion to dismiss a class action lawsuit filed against the company in July following a breach earlier this year. Find out why the company says the lawsuit has no merit.

**Shellshock flaws**

**Heartbleed**

A \$500 million class action lawsuit against Home Depot has been filed in Canada following the disclosure by the retailer that 56 million payment cards were exposed in a data breach.

**Backoff point-of-sale malware**



The ice cream and fast food chain Dairy Queen has confirmed that Backoff point-of-sale malware was used in a payment card breach that affected 395 of its 4,500 franchised U.S. locations. Find out how many cards were affected.



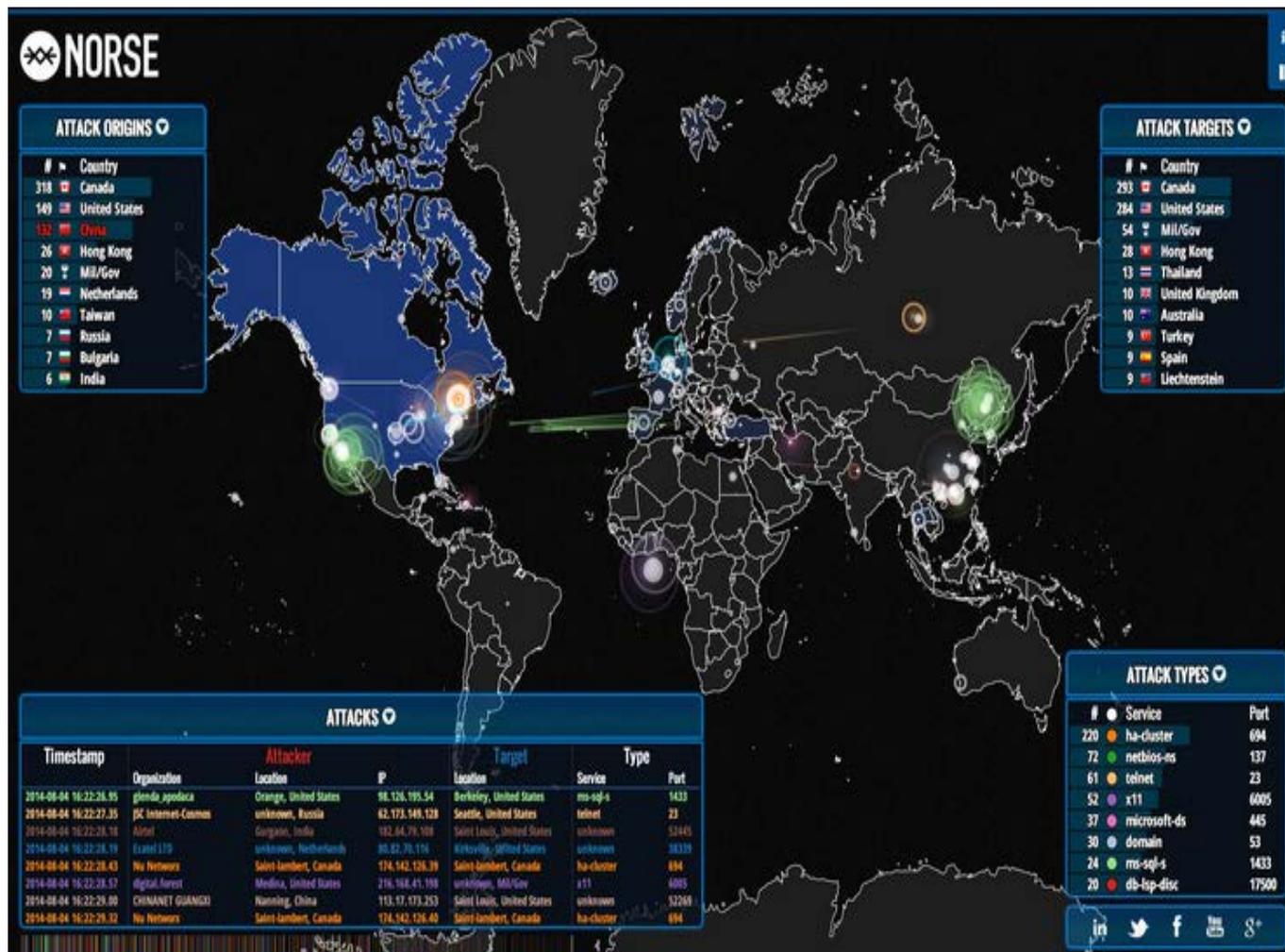
The restaurant chain Jimmy John's has confirmed a payment card data breach affecting about 216 of its locations in 40 states. The breach stems from the compromise of a "point-of-sale vendor."

Source: <http://www.databreachtoday.com/news>

<http://www.databreachtoday.com/infographic-2014s-top-breaches-so-far-a-7408>

# Norse DarkMatter Platform

The DarkMatter™ platform is a globally distributed "distant early warning" network of millions of dark sensors, honeypots, crawlers, and agents that deliver unique visibility into the Internet and the darknets, where bad actors operate. Processing hundreds of terabytes daily, Norse DarkMatter computes over 1,500 distinct risk factors for millions of IP addresses every day. The platform continuously analyzes traffic to identify the compromised hosts, malicious botnets, anonymous proxies and sources of attack that other solutions miss



[Click Link for website. Source: http://map.ipviking.com/](http://map.ipviking.com/)

# Cell Phone Interceptors

**Law enforcement and Criminals operate these illegal cell devices**



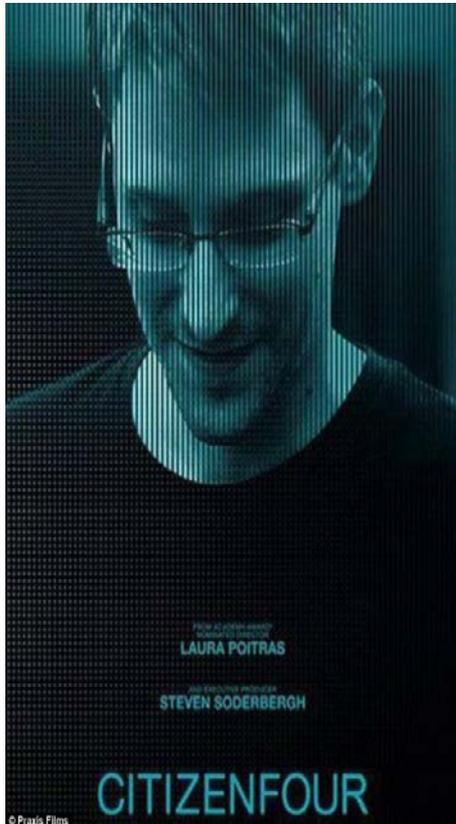
**Click this link for the video**

[Source: http://www.king5.com/story/news/local/2014/09/10/phony-cell-towers-hacking-phones-in-western-wa/15379601/](http://www.king5.com/story/news/local/2014/09/10/phony-cell-towers-hacking-phones-in-western-wa/15379601/)

**ESD Crypto Phone detects illegal cell towers**

# The Snowden Effect

- Consumers seek more protections: iPhone 6 and Android O/S improved encryption
- Two person integrity for data transfers
- Foreign Countries trust in U.S. IT Companies has been impacted (\$\$\$ in lost sales contracts)
- More advanced encryption being developed in general for public use



Forbes Magazine, Huffington Post., and the Economist

# Annual Cyber Crime Studies

- **FBI 2013 Internet Crime Report**

Source: [http://www.ic3.gov/media/annualreport/2013\\_IC3Report.pdf](http://www.ic3.gov/media/annualreport/2013_IC3Report.pdf)

- **Poneman 2014 Cost of Data Breach Study**

Source: <http://www.ponemon.org/blog/ponemon-institute-releases-2014-cost-of-data-breach-global-analysis>

- **Verizon 2014 DATA BREACH INVESTIGATIONS REPORT**

Source: <http://www.verizonenterprise.com/DBIR/2014/>



# Verizon 2014 DATA BREACH INVESTIGATIONS REPORT

Types of data breaches by victim industry: Point of Sales (PoS) intrusions are on the rise in retail and accommodations industries !



Figure 19.  
Frequency of incident classification patterns per victim industry

INDUSTRY	POS INTRUSION	WEB APP ATTACK	INSIDER MISUSE	THEFT/LOSS	MISC. ERROR	CRIMEWARE	PAYMENT CARD SKIMMER	DENIAL OF SERVICE	CYBER ESPIONAGE	EVERYTHING ELSE
Accommodation [72]	75%	1%	8%	1%	1%	1%	<1%	10%		4%
Administrative [56]		8%	27%	12%	43%	1%		1%	1%	7%
Construction [23]	7%		13%	13%	7%	33%			13%	13%
Education [61]	<1%	19%	8%	15%	20%	6%	<1%	6%	2%	22%
Entertainment [71]	7%	22%	10%	7%	12%	2%	2%	32%		5%
Finance [52]	<1%	27%	7%	3%	5%	4%	22%	26%	<1%	6%
Healthcare [62]	9%	3%	15%	46%	12%	3%	<1%	2%	<1%	10%
Information [51]	<1%	41%	1%	1%	1%	31%	<1%	9%	1%	16%
Management [55]		11%	6%	6%	6%		11%	44%	11%	6%
Manufacturing [31,32,33]		14%	8%	4%	2%	9%		24%	30%	9%
Mining [21]			25%	10%	5%	5%	5%	5%	40%	5%
Professional [54]	<1%	9%	6%	4%	3%	3%		37%	29%	8%
Public [92]		<1%	24%	19%	34%	21%		<1%	<1%	2%
Real Estate [53]		10%	37%	13%	20%	7%			3%	10%
Retail [44,45]	31%	10%	4%	2%	2%	2%	6%	33%	<1%	10%
Trade [42]	6%	30%	6%	6%	9%	9%	3%	3%		27%
Transportation [48,49]		15%	16%	7%	6%	15%	5%	3%	24%	8%
Utilities [22]		38%	3%	1%	2%	31%		14%	7%	3%
Other [81]	1%	29%	13%	13%	10%	3%		9%	6%	17%

For more information on the NAICS codes [shown above] visit: <https://www.census.gov/cgi-bin/sssd/naics/naicsrch?chart=2012>

# Poneman 2014 Cost of Data Breach Study

## Root cause of data breaches and costs:

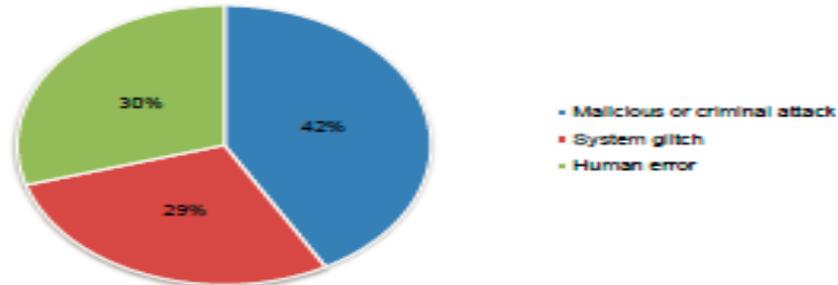
42 % Malicious or Criminal Attack @ \$159.00 per capita cost

30 % Human Error @ \$117.00 per capita cost

29 % System Glitch @ \$126.00 per capita cost

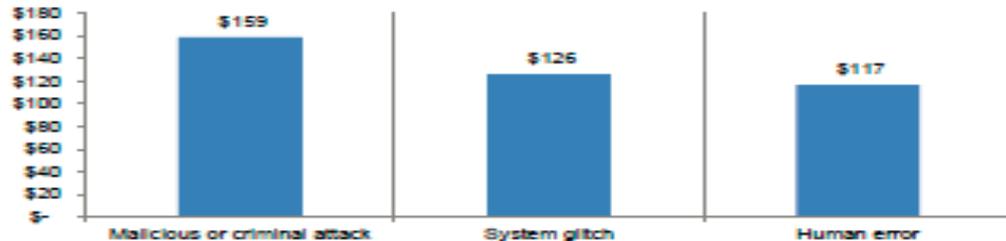


Figure 5. Distribution of the benchmark sample by root cause of the data breach  
Consolidated view (n=314)



Malicious attacks are more costly globally. Figure 6 reports the per capita cost of data breach for three root causes of the breach incident on a consolidated basis. These results show data breaches due to malicious or criminal attacks cost companies increased from an average of \$157 in last year's study to \$159. This is significantly above the consolidated mean of \$145 per compromised record and the per capita cost for breaches caused by system glitch and human factors (\$126 and \$117, respectively). Last year, system glitches averaged \$122 and human error stayed the same at \$117.

Figure 6. Per capita cost for three root causes of the data breach  
Consolidated view (n=314)  
Measured in US\$



<sup>1</sup>Negligent insiders are individuals who cause a data breach because of their carelessness, as determined in a post data breach investigation. Malicious attacks can be caused by hackers or criminal insiders (employees, contractors or other third parties).  
The most common types of malicious or criminal attacks include malware infections, criminal insiders, phishing/social engineering and SQL injection.

Source: <http://www.ponemon.org/blog/ponemon-institute-releases-2014-cost-of-data-breach-global-analysis>

# FBI 2013 Internet Crime Report



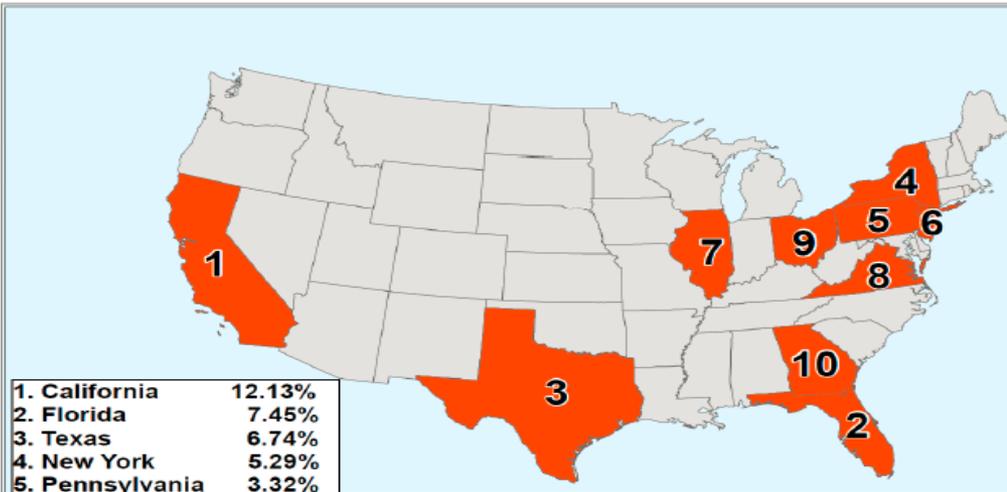
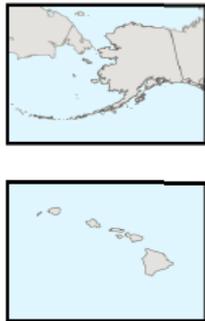
To report an online crime, go to:

**www.IC3.gov**



**DON'T BE A VICTIM OF IDENTITY THEFT!**

Top Ten States Ranked by the Total Number of Complaints Received by IC3 in 2013



1. California	12.13%
2. Florida	7.45%
3. Texas	6.74%
4. New York	5.29%
5. Pennsylvania	3.32%
6. New Jersey	3.21%
7. Illinois	2.95%
8. Virginia	2.84%
9. Ohio	2.75%
10. Georgia	2.58%

Note: 10.09% of the complaints did not include location information

Total Complaints Received In 2013  
262,813

Complaints Reporting a Loss  
119,457

Total Losses Reported  
\$781,841,611

Median Dollar Loss for Only Those Complaints That Reported a Monetary Loss  
\$510

Average Dollar Loss Per Complaint Based Upon the Total Complaints Reported  
\$2,975

Average Dollar Loss for Only Those Complaints That Reported a Monetary Loss  
\$6,245

## Complaint Distribution



Complaints by State:  
Virginia number 8 !

Source: <http://www.ic3.gov/preventiontips.aspx>

# How Bad Is It?:

## More Than “Just” Getting Credit Information



Workers at computers for the California Independent System Operator Corp. in Folsom, California. An attack on the U.S. power grid could cause billions of dollars in damage, and thousands of deaths.

# Malware Proliferation



*Malicious actors have created and used malware targeted to mobile devices since at least 2000.<sup>(1)</sup>*

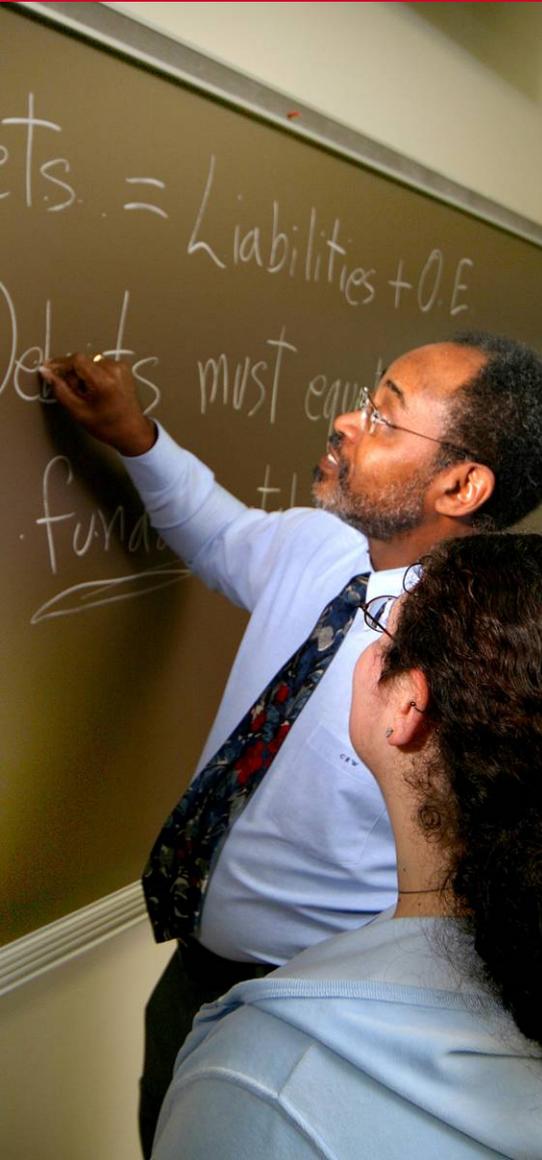
**EXAMPLE:** Ikee B, the first iPhone worm created with distinct financial motivation.

Educational Response:

- Teach the effects of “jaibreaking” a phone
- Teach identification & eradication of botnets
- Stress not using default passwords (e.g. “alpine” for Secure Shell (SSH) operations.

<sup>(1)</sup> U S CERT: Technical Information Paper-TIP-10-105-01. Cyber Threats to Mobile Devices.

# Is It a Business Decision?



Kaspersky Lab's report found that in January the number of malicious Android apps out there topped the **10 million** mark.



Is this a business decision between ROI and the safety of the public?

**YES = Educational Implications:**

**Need to weave into programs of study  
The principles of ethics vs. the bottom  
line**

# Is It Lack of Knowledge?



Apple rushed the release of iOS 7.0.6 on Friday with a patch for a shockingly overlooked SSL encryption issue that leaves iPhone, iPad and Mac computer users open to a man-in-the-middle (MITM) attack.

Is this because of a lack of knowledge in secure coding?

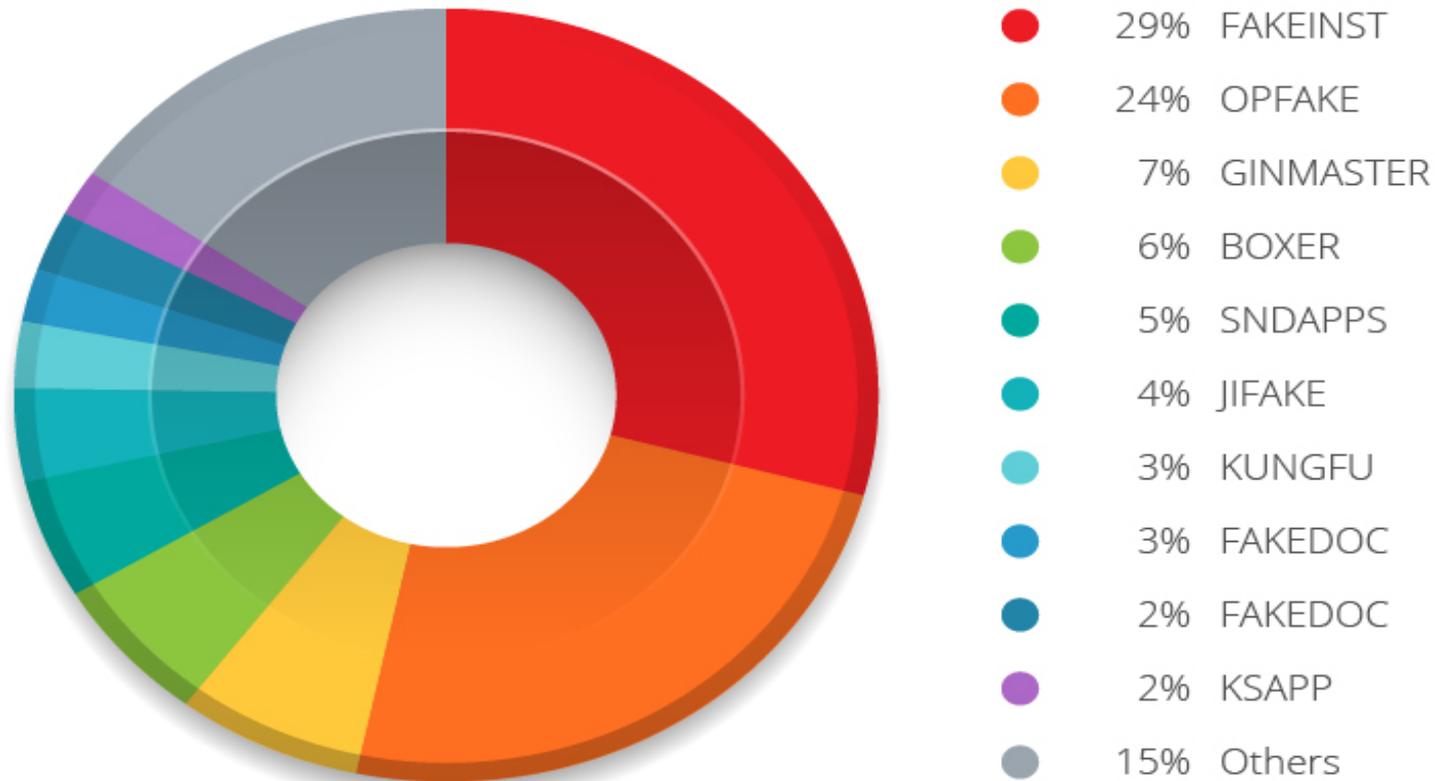
**YES = Educational Implications:**

**Need to weave into programs of study**  
**The principles of secure coding**  
**Carnegie Mellon curriculum**

ZD Net, Feb. 20, 2014

# Educational Response: Study & Research Trends

Around 27% of the detected apps were classified as “high risk apps



The remaining 73% were classified as “malware”.

# It's a Brand New Ball Game



Firms can no longer think in terms of the **react and defend** capabilities developed by on-premise, signature-based technologies. They must instead adopt a more complete “security life cycle” approach with an emphasis on the ability to **predict and prevent**. This requires clearly understanding the threat and potential impact of a security event before it impacts the organization through the use of behavioral, emulation and sandboxing technologies necessary to prevent infection and minimize risk.

# Then There are the Niche Areas - I



## TRANSPORTATION



### RAIL

Poland (2008): A teenage boy hacked into the City of Lodz tram system and used it like a giant train set. The boy studies the trams and tracks for a long time and then built a device that looked like a TV remote control and used it to maneuver the trams and the tracks. He had converted the television control into a device capable of controlling all the junctions on the line .(1)

### AUTO

Demonstrating their Pentagon-funded work at the global "DefCon" hackers conference in Las Vegas in August, Charlie Miller and Chris Valasek showed global security experts in attendance how they could take control of a 2010 Toyota Prius and Ford Escape model using just a laptop. They were able to remotely take control of the cars' electronic smart steering, braking, displays, acceleration, engines, horns and lights. They could even make the fuel tanks show a full tank of gas when there wasn't. To top it all, they did all this using an old Nintendo handset. (2)

(1) Keeping railways safe and secure in the digital era. Smart Rail World Feb. 18, 2014

(2) CNBC. <http://www.cnbc.com/id/101123279>

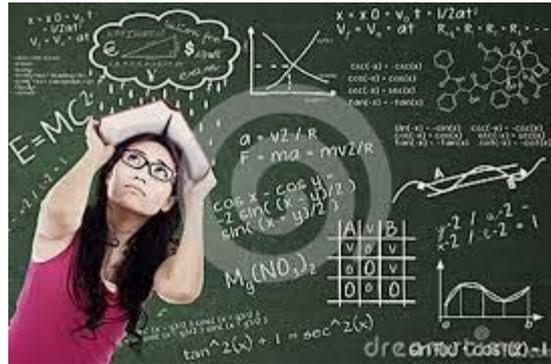
# Niche Areas II

## MEDICAL



Flaws were found with the programming of the wireless transmitters inside the pacemakers and ICDs. Those transmitters monitor for irregularities in heartbeats and deliver life-saving corrective jolts of electricity on a regular basis to correct poor heart function. Unfortunately, the devices are easily tricked by a special command to give up their serial numbers and other info needed to authenticate into them and control those transmitters; and, worse, they often have backdoors that allow the wireless signals to be hijacked even without the credentials. So, either way, a hacker with a commanding laptop can take control and deliver a deadly shock, from up to 50 feet away – the range of many of these vulnerable devices.

# Your Not In Kansas any More



- Current equipment in the labs is **critical**.
- Internships and COOPs working with latest technology is **critical**
- Subject Matter Experts “On Campus” are **critical**
- Participation on advisory boards is **critical**.

# Cybersecurity is a “Hands On” Learning Experience:

**Not just theory – if the system is broken  
– fix it & harden it-**



Capitol College: CYBER BATTLE LAB  
<https://www.capitol-college.edu/node/1206>

# Beyond Mobile Computing



## What will the cybersecurity workforce of the future look like?

- Globally, the cyber security workforce will grow by 2.0 million new workers between now and 2017
- A diverse set of skills beyond technical skills in information security are needed to be successful:
  - Business acumen
  - Communication Skills
  - Legal Knowledge
- Able to handle asymmetrical threat environment.
- The age of The Security analyst

Booz, Allen, Hamilton. Critical Times Demand Critical Skills. A Whitepaper derived from ISC2 Global Information Security Workforce Study. 2013

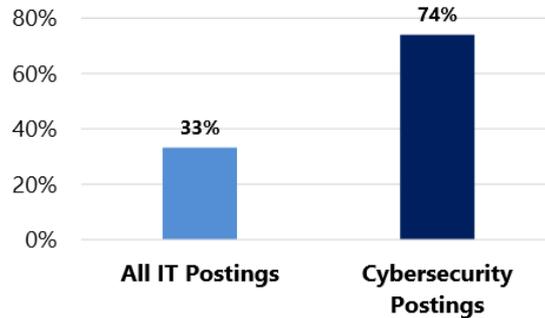
# Job Market Intelligence: Report on the Growth of Cybersecurity Jobs: Burning Glass

**Education**

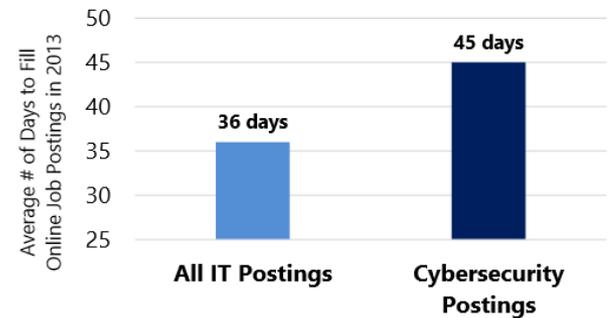
**Certifications**

**Experience**

**Growth in Job Postings (2007-2013)**



**Posting Duration (2013)**

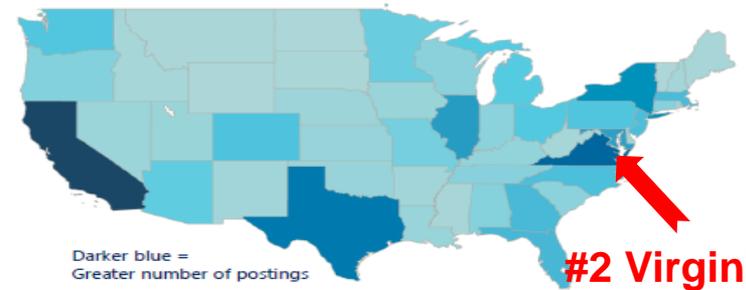


## Cybersecurity Job Postings by State

**Top States by Total Postings\***

	State	Total Postings	Postings/10,000 Residents	% Growth (2007-2013)
1	California	27,084	7.1	64%
2	<b>Virginia</b>	20,507	25.1	53%
3	Texas	16,376	6.3	97%
4	New York	12,405	6.3	59%
5	Illinois	11,136	8.6	116%
6	<b>Maryland</b>	10,627	18.1	94%
7	Florida	7,923	4.1	46%
8	Georgia	7,539	7.6	214%
9	Massachusetts	7,107	10.7	76%
10	New Jersey	6,814	7.7	12%
11	North Carolina	6,676	6.8	129%
12	Colorado	6,039	11.6	158%
13	Pennsylvania	5,630	4.4	22%
14	Washington	5,444	7.9	76%
15	Ohio	5,086	4.4	34%

**Cybersecurity Job Postings in 2013 By State**



*The greater Washington D.C. area has thousands of unfilled cyber security jobs !*

**#2 Virginia**

**#6 Maryland**

# Cyber Security must be multidisciplinary

## *Post survey student comments:*

*“I never included security into my mission planning”*

*“Satellite data should be protected from acquisition to storage”*

*“I am now looking for phishing emails at work because of the threat”*

*“Using the STK software opened my eyes to how much fun and complicated these missions can be to plan”*

## *More Questions to answer:*

*“How do sensors work with drones?”*

*“How do we secure the video feed?”*

*“What Big data analysis tools are available?”*

- **Last spring semester Capitol ran a hybrid course matching 6 Astronautical Engineering (AE) with 6 Computer Science (CS) and Information Assurance (IA) students.**
- **Students were taught by AE and IA Professors.**
- **Students learned to use STK, the systems engineering approach, system lifecycle and network modeling tools and cyber security principles.**
- **Students formed 2 teams to plan a secure satellite mission (AE lead).**
- **The CS/IA student designed the ground segment and networks; AE student designed the space segment. They switched roles during the presentation (surprise).**
- **Next Spring semester hybrid courses will again pair AE/IA students to study integrating sensors with drones and protecting that data. EE/IA students will study integrating sensors with Raspberry pies and Adreno boards as payloads for satellites and drone missions.**

# What Makes Capitol Unique?



## Full Spectrum Study:

- BS, MS, DSc

## National Recognition

- DHS/NSA Designated Nat'l Center of Academic Excellence in Information Assurance Education
  - Mapped to six national IA training standards at advanced levels - 1 of 3 academic institutions in U.S. with this distinction
  - The government & government-related companies are the #1 employer of Capitol alumni

[www.captechu.edu](http://www.captechu.edu)

# Contact info

**Professor William Butler**  
**Director, Critical Infrastructures and**  
**Cyber Protection Center (CICPC)**

**[whbutler@captechu.edu](mailto:whbutler@captechu.edu)**

**240-965-2458**