The Current State of Cybersecurity

John Steensen, IT Audit Manager
Safeway Inc.

In-Depth Seminars – D21

Introduction

John Steensen, MBA/TM, CISA®, CRISC™

John Steensen is a Manager of Information Technology (IT) Audit at Safeway Inc., one of the largest food and drug retailers in North America with sales over $36 billion. His primary focus at Safeway is on managing technology-centric audits providing assurance and validation of the control environment and ensuring adherence to corporate and industry standards. His computer security background spans more than three decades and has directed the design, engineering and implementation of highly secure 4-9's multinational infrastructure (data centers and networks) spanning North America and Europe. He has also worked as a computer forensics examiner and as a civilian contractor for the Drug Enforcement Agency's El Paso Intelligence Center (EPIC) as well as at the US Army White Sands Missile Range on secure projects.

Mr. Steensen is a Certified Information Systems Auditor (CISA®) and is Certified in Risk and Information Systems Control (CRISC™). He holds a BS degree in Computer Science from North Carolina State University and an MBA from the University of Phoenix with a specialization in Technology Management. He is recognized as an audit profession thought leader and speaks by invitation at national and local audit profession conferences and forums.

Mr. Steensen invests in the audit profession by volunteering as a member of the Board of Directors for ISACA San Francisco Chapter and by working as a voting member of ASTM's E11 Committee on Statistics and Quality, which sets the world's standards for sampling and quality control.

Session Objectives

Cybersecurity Defined

The United States Department of Homeland Security's (DHS) National Initiative for Cybersecurity Careers and Studies (NICCS) defines cybersecurity as

"The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation."

Cybersecurity Defined

"Protecting stuff in cyberspace."

Cybersecurity Defined

Stuxnet is typically introduced to the target environment by an **infected USB flash drive**. The virus then propagates across the network, scanning for Siemens Step7 software on computers controlling a PLC. In the absence of both criteria, Stuxnet becomes dormant inside the computer. If both the conditions are fulfilled, Stuxnet introduces the infected rootkit onto the PLC and Step7 software, modifying the codes and giving unexpected commands to the PLC while returning a loop of normal operations system values feedback to the users.

Stuxnet reportedly ruined almost one-fifth of Iran's nuclear centrifuges.

A Step Back in Time

- Have the threats and issues surrounding IT changed so much that completely new techniques and technologies must be applied to be able to address the cybersecurity issues?
- The industry “hype” is that the issues today are fundamentally different than they were in the past and that only new techniques and products are capable of addressing the threats.
- Let’s walk through a quick review of some of the issues that IT has faced and is still facing, albeit in an updated form.

What are the Threats?

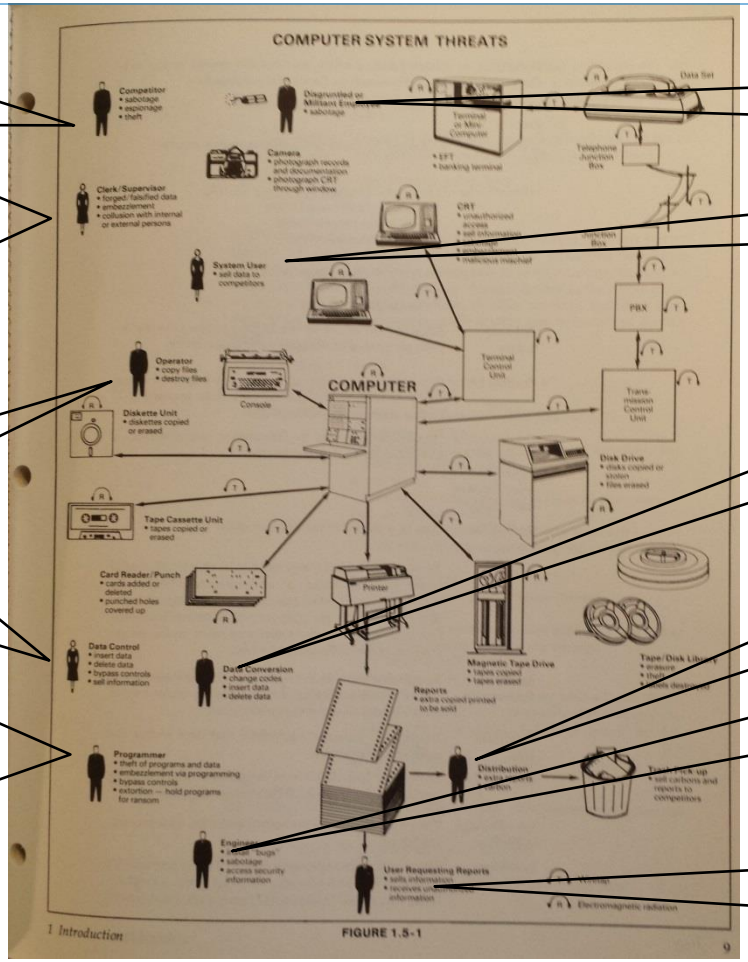
Competitor – Sabotage, espionage, theft

Clerk/Supervisor – Forged or falsified data, embezzlement, collusion with internal or external persons

Operator – Copy files, destroy files

Data Control – insert data, delete data, bypass controls, sell information

Programmer – Theft of programs and data, embezzlement via programming, bypass controls, extortion (hold programs for ransom)



Disgruntled Employee – Sabotage

System User – Sell data to competitors

Data Conversion – Change codes, insert data, delete data

Distribution – Extra reports, carbon copies

Engineer – Install “bugs”, sabotage, access security information

User Requesting Reports – Sells information, receives unauthorized information

Computer Crime Investigation Manual - Copyright © 1980

What are the Threats?

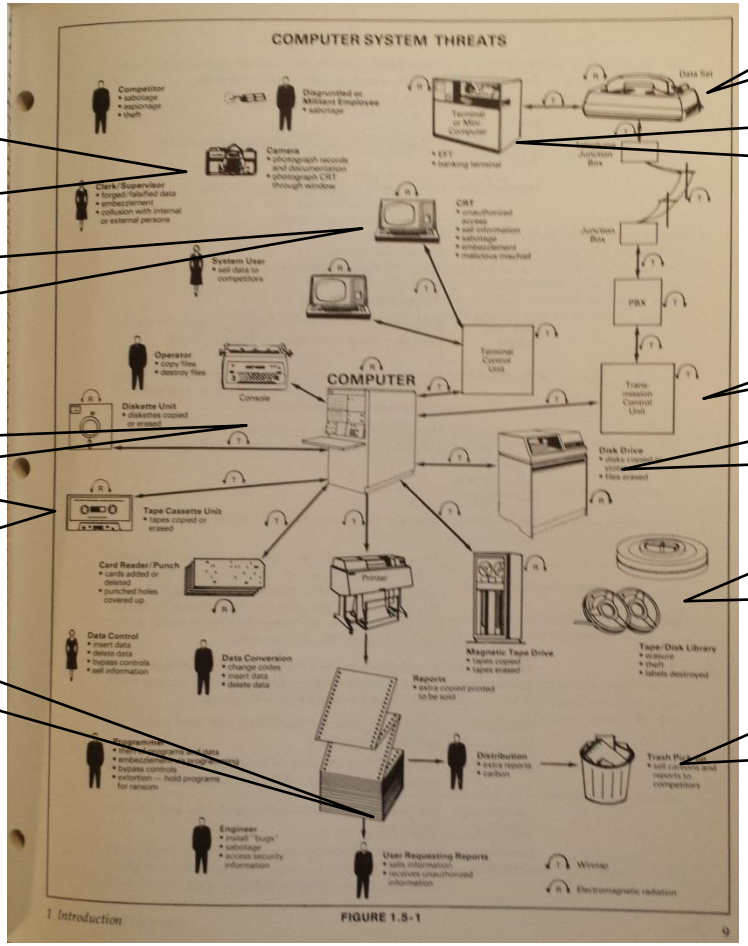
Camera – Photograph records and documentation, CRT screen through window

CRT – Unauthorized access, malicious mischief

Console Access

Diskette Unit – Diskettes copied or erased

Reports – Extra printouts to be sold



Data Set

Terminal – EFT, banking terminal

Transmission Control Unit

Disk Drive – Disks copied or stolen, files erased

Tape/Disk Library – Erasure, theft, labels destroyed

Trash Pickup – Sells carbons and reports to competitors

Computer Crime Investigation Manual - Copyright © 1980

What is the Point?

Key Takeaway

The basics issues of security (actors, information domains, types of threats) haven't changed significantly and, therefore, we already have a lot of experience that is directly applicable

BUT

The technologies and threat manifestations have changed so the detection methods and subsequent responses must continue to evolve to keep up.

The Year of the Breach

What is a Breach?

- According the Identity Theft Resource Center[1]:
- "A **breach** is defined as an event in which an individual's name plus Social Security Number (SSN), driver's license number, medical record, or a financial record/credit/debit card is potentially put at risk – either in electronic or paper format."
- When records are encrypted their loss is not normally considered to be a data exposure. However, password protection alone is not considered adequate, and those records with only password protection are considered to have been exposed.

[1]http://www.idtheftcenter.org/images/breach/ITRC_Breach_Report_2014.pdf

What is a Breach?

- A “security breach” as a compromise of the security, confidentiality, or integrity of, or the loss of, computerized data that results in, or there is a reasonable basis to conclude has resulted in, (1) the unauthorized acquisition of sensitive personally identifiable information (SPII); or (2) access to SPII that is unauthorized or in excess of authorization.
- The section also defines with particularity “sensitive personally identifiable information” and authorizes the Federal Trade Commission to amend this definition as needed through the rulemaking process.

http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/data-breach-notification-section-by-section-analysis.pdf

A Banner Year for Breaches

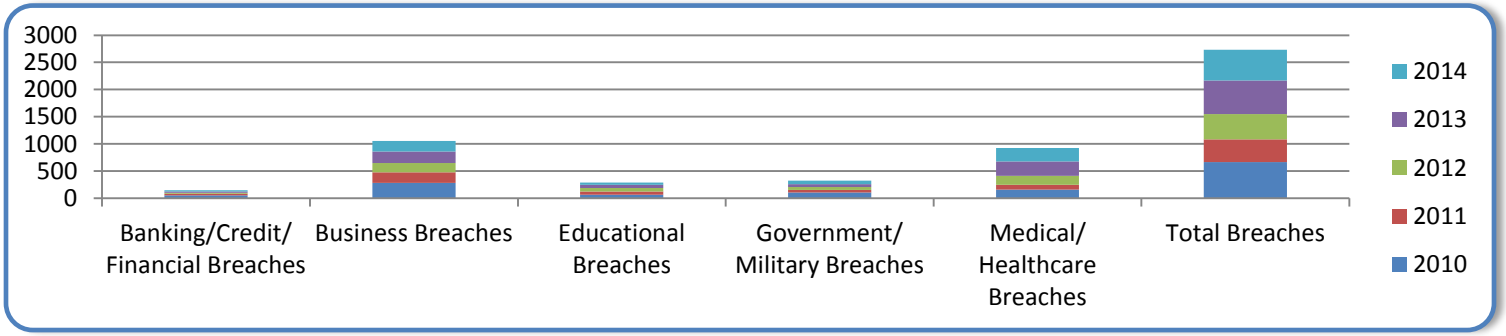
- So far in 2014 there have been 568 data breaches involving more than 75 million records, of which 56 million occurred at Home Depot stores, according to data released by the Identity Theft Resource Center.
- The data breach at Home Depot Inc. was the largest ever in the history of the retail business globally, beating last year's 40 million at Target Corp. in 2013, and 45.6 million at TJX Companies Inc. in 2007.

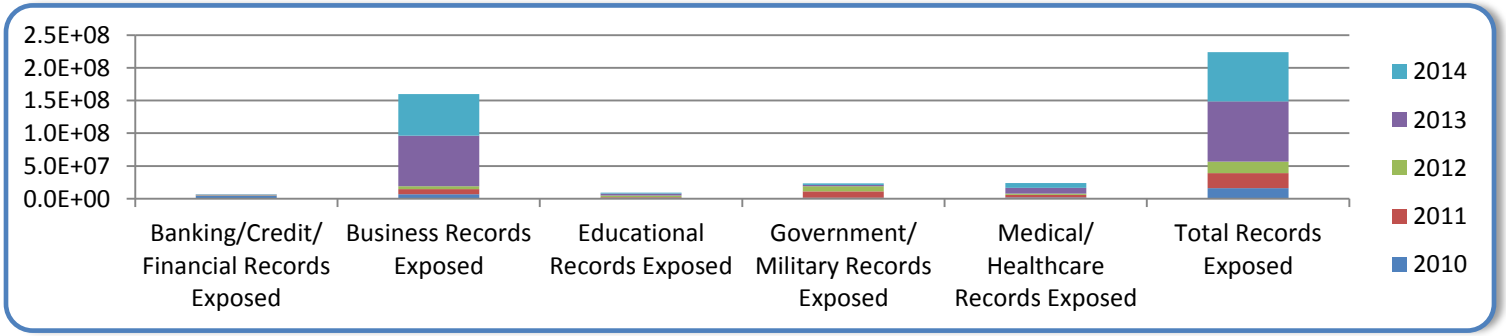
Sector	# of Breaches	% of Breaches	Records Taken (M)	% of Records
Medical & Healthcare	247	43.5	7.14	9.2
Business	195	34.3	63.00	84.0
Banking/Credit/Financial	23	4.0	0.17	0.2
Government/Military	62	10.9	2.75	3.7
Education	41	7.2	1.53	2.0

http://marketbusinessnews.com/data-breaches-reach-record-levels-2014/34045

Breach Trends

The number of breaches are increasing and the magnitudes of the breaches are also increasing.





The Year of the Breach

Key Takeaway

Breachware (and crimeware in general) is a growing business and enables many more "black hat" players to enter the field at a much lower cost and lower skill set.

Keep informed to what's trending.

The Weakest Link

The Weakest Link

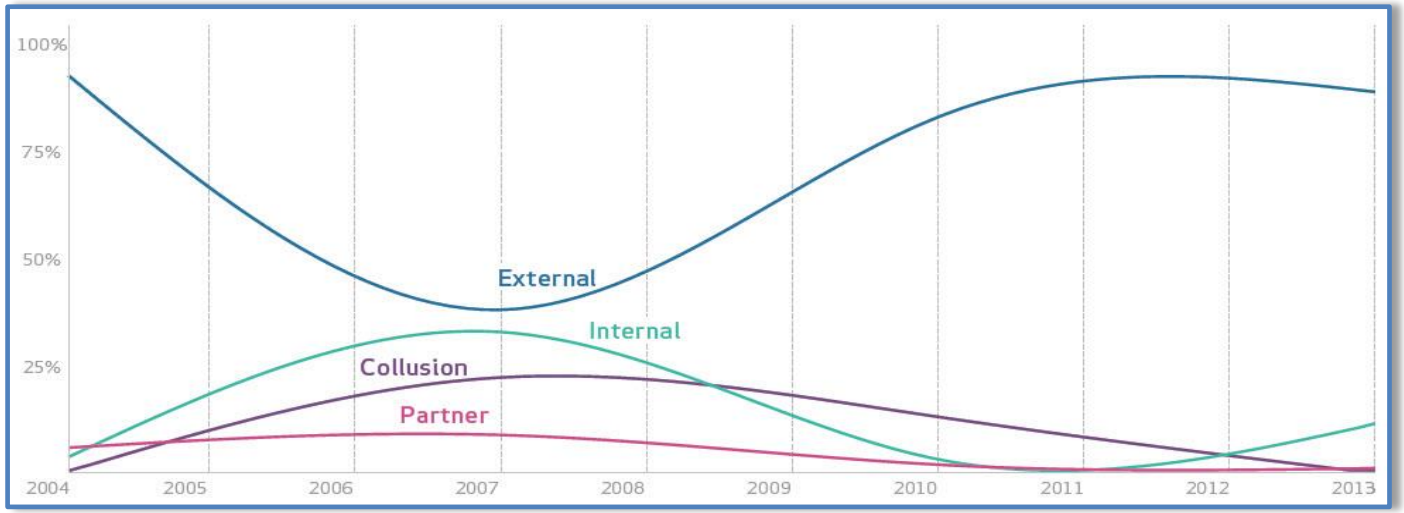
Obvious Steps Make a Difference

When it comes to mitigating the insider threat, the obvious measures can help in preventing data loss and are often the most over-looked. Measures that can stop the little losses from occurring would have stopped Snowden, Winkler says, including access controls and audits.

http://www.govinfosecurity.com/insider-risks-what-have-we-learned-a-7195

Verizon 2014 Data Breach Investigations Report

Figure 5. Percent of breaches per threat actor category over time



My Dirty Dozen Conjectures

1. There are agents of foreign governments working in every major company in the United States.

2. There are agents of competitive businesses working in every major company in the United States.

3. There are criminals working in every major company in the United States.

4. There are agents of foreign governments working in every major governmental organization in the United States.

5. There are agents of the United States government working in every major company in the United States.

6. Every major company has suffered a loss of intellectual property.

My Dirty Dozen Conjectures, cont.

7. Every major company will continue to suffer losses of intellectual property.

8. Every major company has suffered a loss of customer information.

9. Every major company will continue to suffer losses of customer information.

10. Every commercially available information or communications system is subject to unauthorized access.

11. The vast majority of unauthorized accesses will go undetected.

12. The vast majority of unauthorized accesses detected will go unprosecuted.

The Weakest Link

Key Takeaway

A computer system rarely commits an act of aggression without a human participant.

Remain aware of the risks associated with "carbon-based units".

Lessons from the Intel Community

Lessons from the Intel Community

NSA's Prism: Balancing Security, Privacy (6/10/2013)

Over the weekend, the Guardian, the British newspaper that first broke the story, and the Post revealed that they received the classified information about NSA programs from Edward Snowden, a 29-year-old former technical assistant for the CIA and current employee of the business and IT security adviser Booz Allen Hamilton. Snowden has been working at the NSA for the last four years as an employee of various outside contractors, including Booz Allen and Dell, according to the two newspapers.

http://www.govinfosecurity.com/blogs/nsas-prism-balancing-security-privacy-p-1486/op-1

A year later:

Report: New Government Leaker Confirmed (8/5/2014)

U.S. officials have confirmed the existence of a new leaker exposing national security documents, CNN reports. The leak apparently involves documents prepared by the National Counterterrorism Center.

http://www.databreachtoday.com/report-new-government-leaker-confirmed-a-7159

Lessons from the Intel Community

Insider Risks: What Have We Learned?

Organizations Still Not Taking Threat Seriously (8/21/2014)

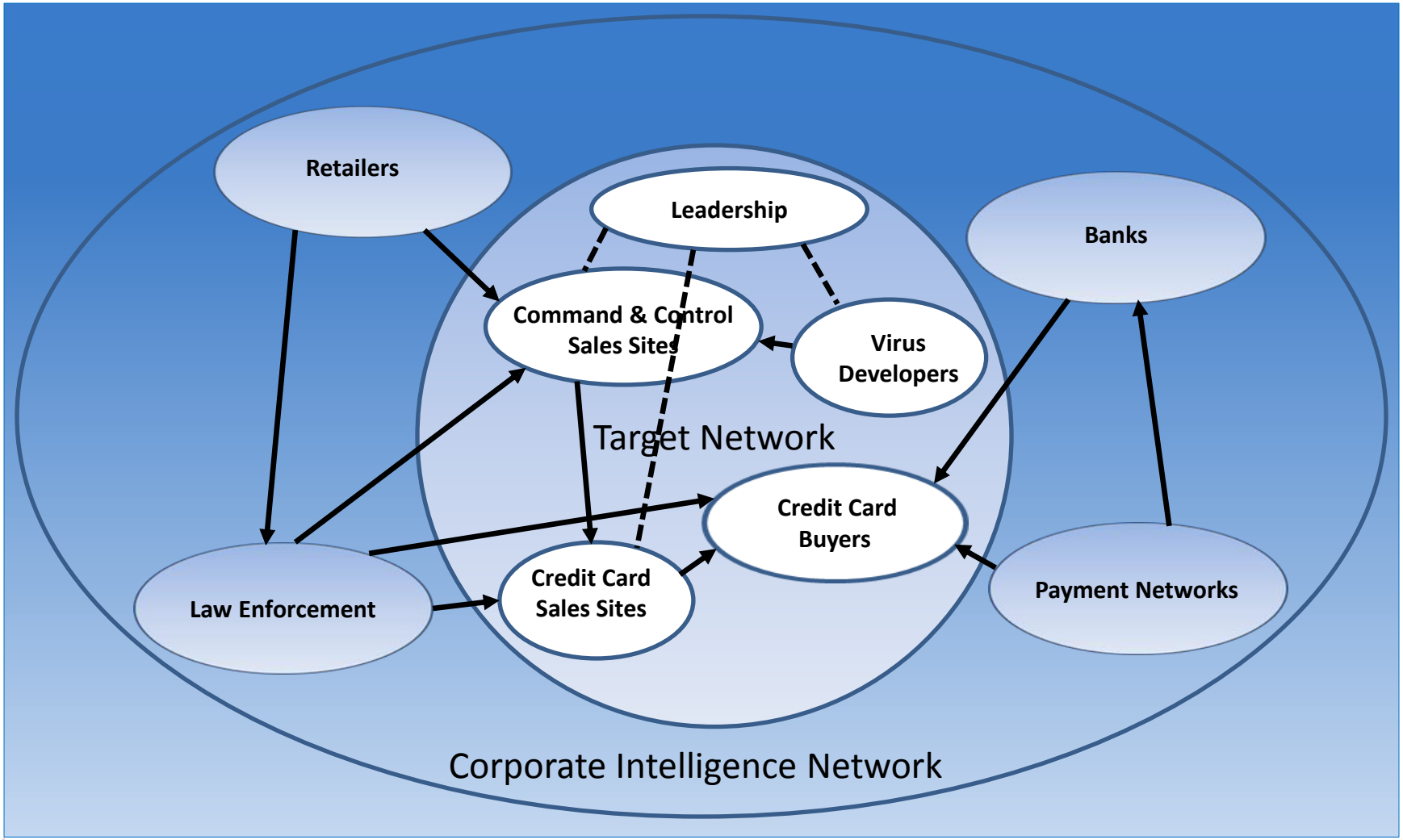
"I think a lot of people unfortunately viewed Edward Snowden as an anomaly," says Eric Cole, a SANS Institute fellow and IT security author. "This was just one person that did harm; this is not a real threat. **Unfortunately, there are a lot of Snowdens out there.** There are a lot of people that are doing this."

Even security leaders that do see the need for an insider threat program often can't get funding for one, says Ira Winkler, information security expert and former intelligence and computer systems analyst at the National Security Agency. **"Security managers are given the budgets they deserve, not the budgets that they need,"** he says. "They only get the budgets that they know how to cost-justify from a business perspective."

http://www.govinfosecurity.com/insider-risks-what-have-we-learned-a-7195

It’s Not Spy vs Spy

It's Network vs Network



Lessons from the Intel Community

Key Takeaway

They hunt in packs – you must defend in packs.

Risk vs Reward

Risk vs Reward

"The purpose of risk management is to improve the future, not to explain the past."

Dan Borge, The Book of Risk

Risk vs Reward

The Risks and Rewards of Mobile Banking Apps

Mobile banking technology may be one of the best retention tools available to banks - a differentiator. Mobile banking customers are 53 percent less likely to leave; and if customers use both mobile banking and bill pay the retention rate increases to 82 percent. The challenge banks face is increasing the security of mobile banking to reduce the number of people who will not use mobile banking **due to security concerns** - 48 percent. Increasing mobile banking app security is attainable, and the retention and operational cost savings should make it a priority.

http://www.govinfosecurity.com/whitepapers/risks-rewards-mobile-banking-apps-w-1126

Risk vs Reward

The Risk of Open Source or The Lie of 'Many Eyes'

For Robert Graham, the CEO of consultancy Errata Security, Shellshock gives lie to a major tenet of open-source software: that open-source code permits "many eyes" to view and then fix bugs more quickly than proprietary software, where the code is kept out of view from most of the world. …the fallacy is the idea that all open-source projects have many eyes. "There's a lot of code that doesn't actually get very many eyes at all," he says. "And a lot of open-source projects don't actually have all that many developers involved, even when they are fairly core."

http://www.wired.com/2014/09/shellshocked-bash/

Risk vs Reward

Key Takeaway

For every initiative you must balance the risk versus reward.

That means:

- **Quantifying the reward from the initiative**
- **Quantifying the risk from the initiative**
- **Understanding your risk appetite**
- **Balance at the start of an initiative and keep measuring and evaluating to ensure the balance remains**

Cybersecurity on the World Stage

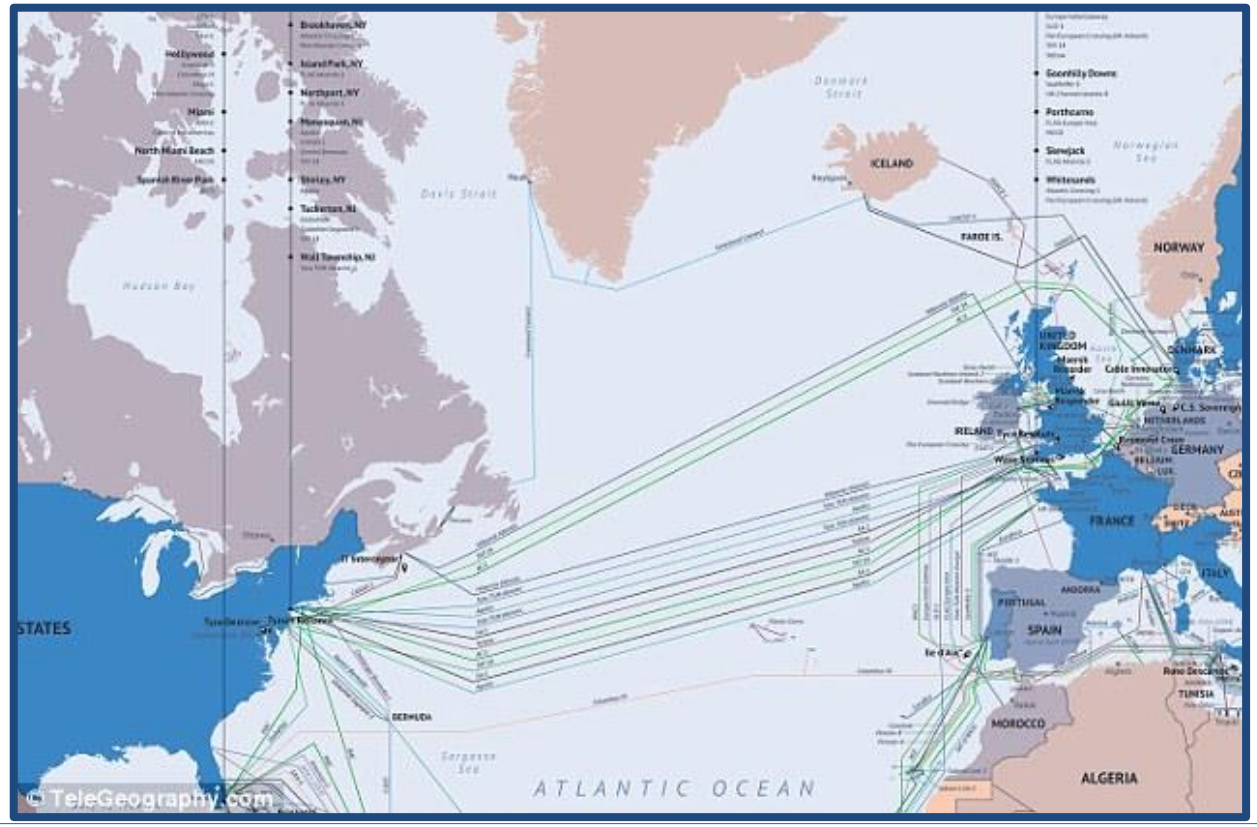
Cybersecurity on the World Stage

- The world's nervous system revealed: Interactive map charts **550,000** mile-long network of underwater cables that carry world's web traffic. The 2014 editions features a total of 285 submarine communication cables. This includes 263 in-service cables and 22 that should be in use by 2015. **Since 2012 this figure has nearly doubled, and is up from 244 in 2013**.

- That’s roughly 22 times around the world!!

http://www.dailymail.co.uk/sciencetech/article-2549329/Interactive-map-reveals-550-000-mile-long-network-UNDERWATER-cables-carry-worlds-web-traffic.html#ixzz3G6EhNgep

Cybersecurity on the World Stage



http://www.dailymail.co.uk/sciencetech/article-2549329/Interactive-map-reveals-550-000-mile-long-network-UNDERWATER-cables-carry-worlds-web-traffic.html#ixzz3G6EhNgep

Cybersecurity on the World Stage

What Cyberthreat Does ISIS Pose?

"ISIS has over $500 million and has talked about cyber-attacks," Kobza, executive director of the National Health Information Sharing and Analysis Center, said this week at a government-sponsored symposium on safeguarding healthcare information. "It's more critical than ever to come together ... in a trusted public/private partnership to protect the healthcare sector."

Should Kobza be worried? Does ISIS pose a threat to the critical digital assets of the United States and other nations? When asked, a spokesman for the Department of Homeland Security responded: "No comment."

http://www.inforisktoday.com/blogs/what-cyberthreat-does-isis-pose-p-1747

Cybersecurity on the World Stage

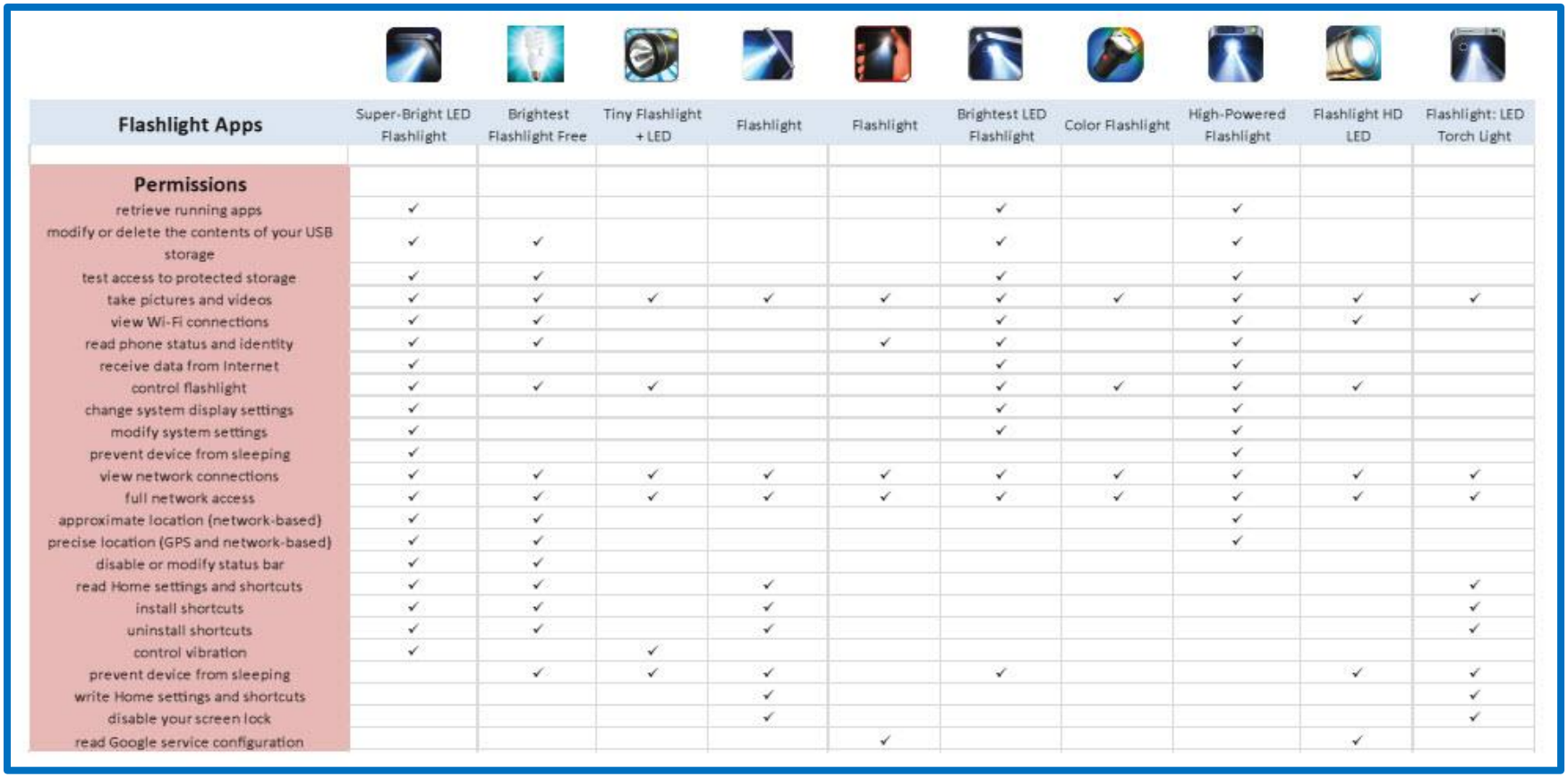
Skilled, Cheap Russian Hackers Power American Cybercrime

"When it comes to finding original ways of virtually stealing real money, Russian criminals are in a class of their own. **With an estimated annual turnover of more than $2 billion a year, the Russian cybercrime industry is the source of at least a third of all viruses, Trojans and other malicious software, or malware, sent around the world.**

Take, for example, the recent data breach at Target. Investigators have traced the software that was used to steal millions of shoppers' credit-card details back to a 17-year-old hacker from St. Petersburg named Sergey Taraspov. He allegedly wrote the program and then sold it for $2,000 on a Russian-language website. At least 40 different criminals, most from the former Soviet Union, used the code to attack American retailers. **So far, at least 110 million American shoppers had their credit card numbers stolen with his software."**

http://www.nbcnews.com/news/world/skilled-cheap-russian-hackers-power-american-cybercrime-n22371

Shedding Light on Cybersecurity



Flashlight Apps	Super-Bright LED Flashlight	Brightest Flashlight Free	Tiny Flashlight + LED	Flashlight	Flashlight	Brightest LED Flashlight	Color Flashlight	High-Powered Flashlight	Flashlight HD LED	Flashlight: LED Torch Light
Permissions										
retrieve running apps	✓					✓		✓		
modify or delete the contents of your USB storage	✓	✓				✓		✓		
test access to protected storage	✓	✓				✓		✓		
take pictures and videos	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
view Wi-Fi connections	✓	✓				✓		✓	✓	
read phone status and identity	✓	✓			✓	✓		✓		
receive data from Internet	✓					✓		✓		
control flashlight	✓	✓	✓			✓	✓	✓	✓	
change system display settings	✓					✓		✓		
modify system settings	✓					✓		✓		
prevent device from sleeping	✓							✓		
view network connections	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
full network access	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
approximate location (network-based)	✓	✓						✓		
precise location (GPS and network-based)	✓	✓						✓		
disable or modify status bar	✓	✓								
read Home settings and shortcuts	✓	✓		✓						✓
install shortcuts	✓	✓		✓						✓
uninstall shortcuts	✓	✓		✓						✓
control vibration	✓		✓							
prevent device from sleeping		✓	✓	✓		✓			✓	✓
write Home settings and shortcuts				✓						✓
disable your screen lock				✓						✓
read Google service configuration					✓				✓	

http://www.snoopwall.com/wp-content/uploads/2014/10/Flashlight-Spyware-Appendix-2014.pdf

FBI's Cyber's Most Wanted

Cybersecurity on the World Stage

But Beware the Hype:

"This **terrible news** [referring to the JP Morgan breach] only further underscores the urgent need for Congress to pass comprehensive cyber security legislation," Senator King said. "The longer we wait to take action, the more vulnerable we become, and as we've seen today, Americans will pay the price. We simply cannot afford to wait any longer. Congress must work to pass legislation that will improve our capabilities and protect us against more attacks like these. **The next Pearl Harbor will be cyber, and shame on us if we're not prepared for it.** We have a bi-partisan bill teed up in the Senate and I'd like to see it move before the end of the year."

http://www.king.senate.gov/newsroom/press-releases/in-response-to-jpmorgan-chase-attack-king-calls-on-congress-to-pass-cyber-security-legislation

Cybersecurity on the World Stage

Key Takeaway

What happens in Vegas DOES NOT STAY in Vegas!

Unless you "air-gap" your systems you are connected to the world so you must pay attention to what is going on across the globe.

The Future of Cybersecurity

The Future of Cybersecurity

The future of cybersecurity is industry, government, professional associations and educational institutions working together. Not getting involved is no longer an option:

The Council on Cybersecurity (www.counciloncybersecurity.org)

Retail Industry Leader's Association Cybersecurity and Data Privacy Initiative (www.rila.org)

ISACA Cybersecurity Framework (www.isaca.org)

NIST Cybersecurity Framework Version 1.0 (www.nist.gov)

NSA National IA Education and Training Program (NIETP) (https://www.nsa.gov/ia/academic_outreach/)

Federal Bureau of Investigation (http://www.fbi.gov/about-us/investigate/cyber)

The Future of Cybersecurity

The Council on Cybersecurity

Critical Security Controls

The Council actively promotes the development and adoption of the Critical Security Controls - the measures widely acknowledged as representing the most critical steps an enterprise can take to markedly strengthen its ability to thwart attacks. An underlying theme of the Controls is support for large-scale, standards-based security automation for the management of cyber defenses.

Professionalizing the Workforce

The Council is committed to the development of the cybersecurity workforce. Through the work of its expert panels, the Council seeks to develop consistency in job profiles, competency models, skills assessment and workforce management to contribute to the development of this essential workforce and support its evolution as a profession.

http://www.counciloncybersecurity.org/#critical-security-controls

The Future of Cybersecurity

Talent Development

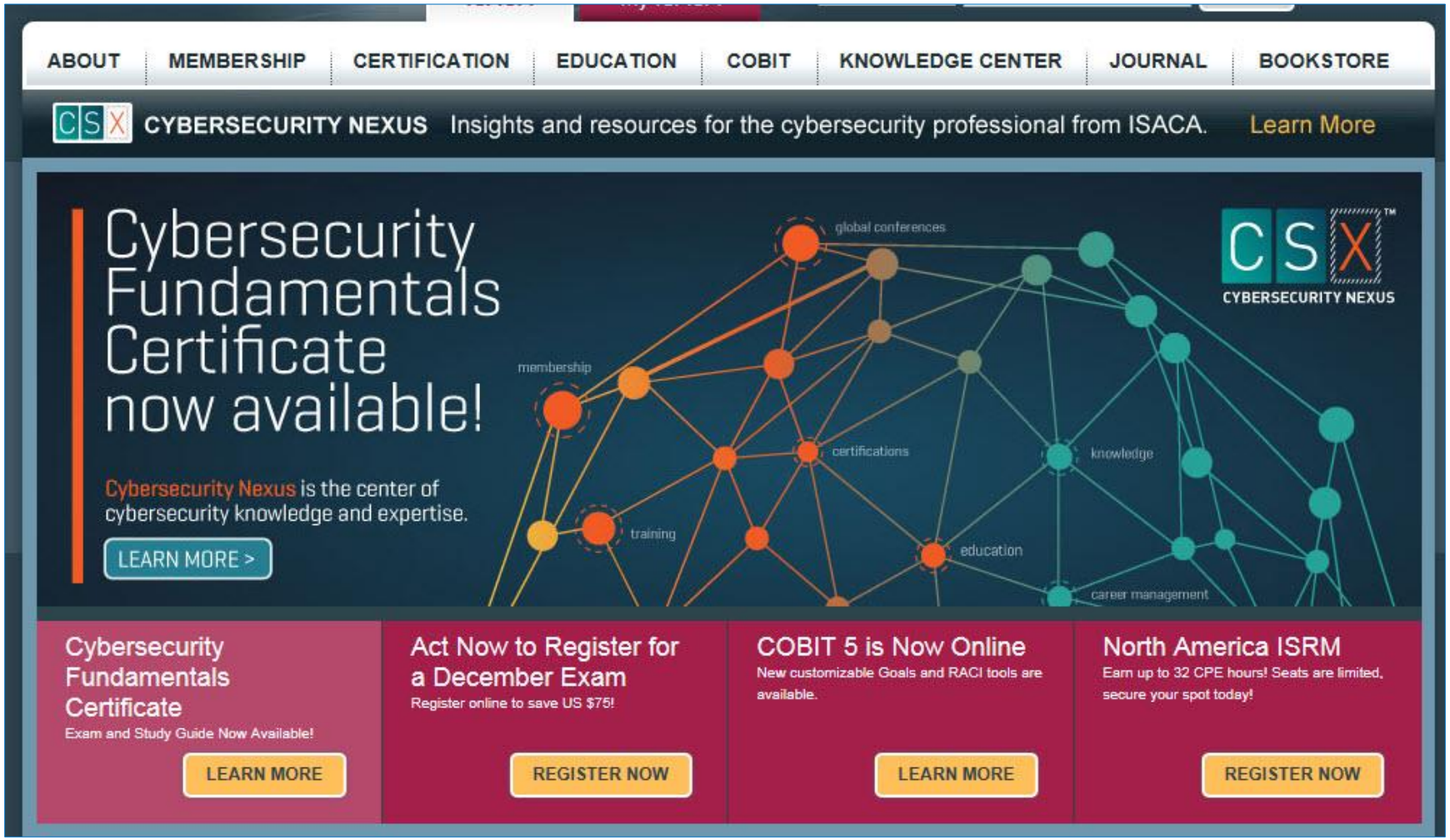
The Council is home to U.S. Cyber Challenge, which works with the cybersecurity community to bring accessible, compelling programs that motivate students and professionals to pursue education, development, and career opportunities in cybersecurity.

Sensible Policies

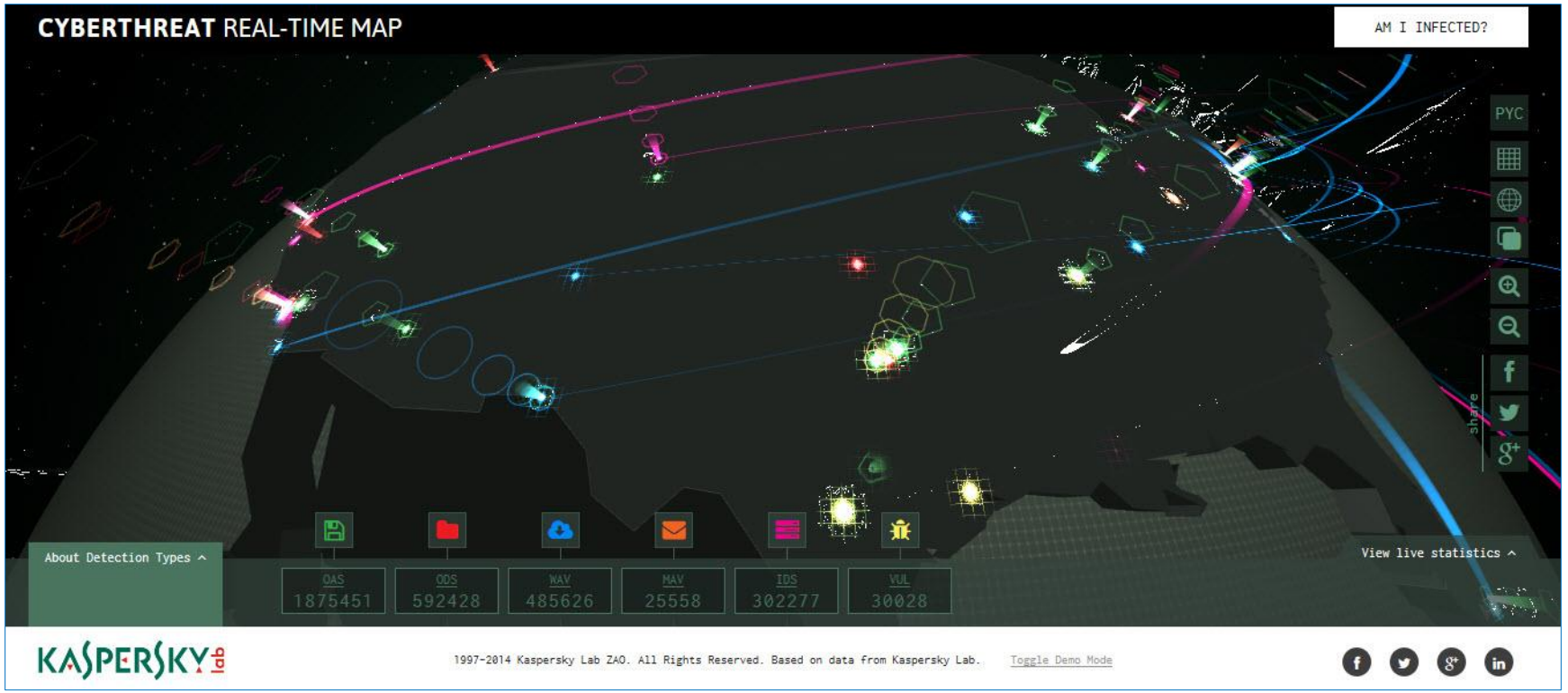
Sensible policy is required to provide well-informed guidance, constraints and incentives to drive adoption of best practices in cybersecurity and protect the interest of the broader community. The Council makes specific policy recommendations based on the collective insight of our experts.

http://www.counciloncybersecurity.org/#critical-security-controls

ISACA Offers Certificate



Seeing Cyber Threats in Real Time



http://cybermap.kaspersky.com/

DHS Sponsors 11th Annual

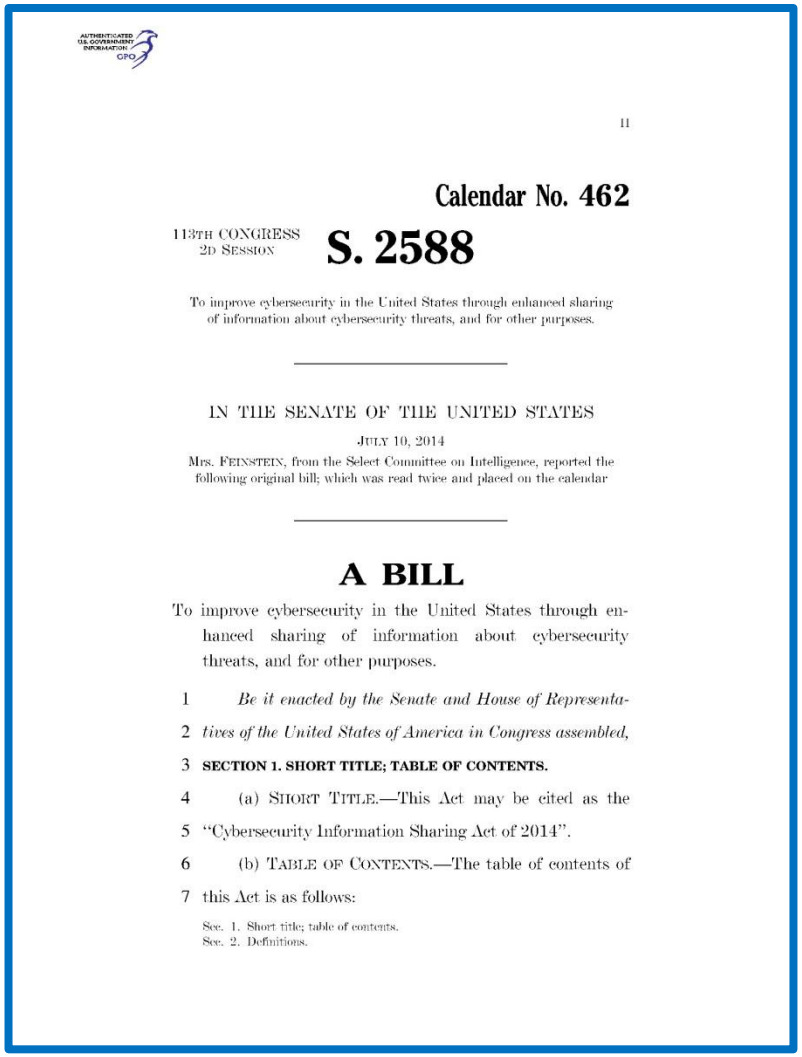
Looking Forward to 2015

President Obama's fiscal year 2015 budget outlines a set of priorities - a wish list - of programs the administration hopes to pursue, including **a federal cyber campus** where civilian agencies can collaborate on cyber-incident response.

The budget proposes $35 million for the design of a federal cyber campus **to co-locate key civilian agencies in the Washington area** to promote a "whole-of-government" approach to cybersecurity incident response. At a press briefing, GSA Administrator Dan Tangherlini says the initiative - to shift about 600,000 square feet of leased space to a federally owned building - is in the early planning stages. "We're spending substantial amounts of resources on rent to maintain multiple, separate activities that we think could provide value if they were consolidated and co-located in single state-of-the-art campus, recognizing that this is the type of work that we're going to need to do in a collaborative way going forward," he says.

Reaction to President's Plan Franklin Reeder, who chairs the Council on Cybersecurity, a not-for-profit that promotes a secure Internet, says co-locating situational awareness and response operations makes sense. "**They need to collaborate but they have very different roles, and I would be concerned about promoting group-think**," says Reeder, a former senior manager at the Office of Management and Budget.

Cybersecurity Information Sharing Act of 2014 (the other CISA)



II

Calendar No. 462

113TH CONGRESS
2D SESSION

S. 2588

To improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes.

IN THE SENATE OF THE UNITED STATES

JULY 10, 2014

Mrs. FEINSTEIN, from the Select Committee on Intelligence, reported the following original bill; which was read twice and placed on the calendar

---

A BILL

To improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the "Cybersecurity Information Sharing Act of 2014".

(b) TABLE OF CONTENTS.—The table of contents of this Act is as follows:

The Future of Cybersecurity

Solving one problems often creates another problem –

Security Leaders Must Address Threats From Rising SSL Traffic

"The inspection of network traffic is a core component of a network security policy strategy and often involves more than one technology. In the interests of enterprise security, communications to internal and external servers are encrypted. Paradoxically, this **Secure Sockets Layer (SSL) traffic "blinds" other network security mechanisms from inspecting this traffic**….

…In response to attacks and compromises, many major public Web services have already switched to HTTPS by default (Google, Yahoo, Twitter and Facebook) or will soon (Wikipedia). Mobile application toolkits and HTML5 frameworks remove most of the complexity of enabling SSL communication by default. As a consequence, the amount of encrypted traffic represents an increasing share of enterprise network traffic, with steady growth every year. Web traffic encrypted using SSL (HTTPS) accounts for 15% to 25% of total outbound Web traffic and **often carries sensitive or personal data**."

http://www.gartner.com/technology/reprints.do?id=1-1T7QE3B&ct=140421&st=sg

Estimating Losses

What are the costs of a cyber attack?

- Cost estimates – rarely explain key assumptions.
- Physical losses – the immediate direct losses are often very low.
- Remedial costs – what do you include particularly if part of those go to the installation of detective, preventative and mitigating technologies that should have been there in the first place?
- Consequential losses – what are the criteria for inclusion? For example, an insurer might be prepared to pay out for provable loss of revenue (based on a previous year‘s business records), but not for a lost business opportunity.
- Reputational losses – how do you measure the impact on future business?
- Ongoing costs – how do you classify your increased insurance premiums?

Source: OECD (Organisation for Economic Cooperation and Development) - “Reducing Systemic Cybersecurity Risk”

Who Pays for Losses

- If you have a valid insurance policy and incur a covered loss – you will be compensated for most of that loss.
- Is the insurer's payout on claims a cost of the cyber attack or a normal part of an insurer's business?
- Estimates of annual global losses attributable to cyber events or cybercrime are even more problematic as there is no guarantee that all possible victims have been polled, or that they have provided detailed responses. One study[1] estimates worldwide losses at between $375 and $525 billion US.

[1]Net Losses: Estimating the Global Cost of Cybercrime, Economic impact of cybercrime II, Center for Strategic and International Studies, June 2014

Creative Attacks

Fake Cell Towers: Understanding the Risks and Trends

https://www.iansresearch.com/_actions/downloaddocument.aspx?id=11521

"Over the course of the last few weeks, I have reviewed ESD America's findings and also participated in real-time discovery of some unauthorized base stations both in the Las Vegas, Nev., area and around Washington, D.C. We also noted at least three separate attacks emanating from those rogue towers."

"Although few actual incidents have been reported by victimized companies, the fact that we were able to discover several of these "fake cell towers" operating in major metropolitan areas should put companies on notice."

Hacker Spoofs Cell Phone Tower to Intercept Calls

http://www.wired.com/2010/07/intercepting-cell-phone-calls/

Doing this kind of interception "used to be a million dollars, now you can do it with a thousand times less cost," Paget said during a press conference after his attack. "If it's $1,500, it's just beyond the range that people can start buying them for themselves and listening in on their neighbors."

A Smorgasbord of Trends

Blue Coat - Cybersecurity Trends for 2014
https://www.bluecoat.com/blogs/2014-02-21/cybersecurity-trends-2014

1. **Botclouds, not Botnets**
2. **CryptoCurrency Surprise**
3. **Wearable Malware**
4. **Deep Web Starts to Surface**
5. **3rd Part Security Requirements Increase**
6. **Big Data Becomes Huge Data**

paloalto Networks - 2014 Predictions: Cybersecurity Trends
http://researchcenter.paloaltonetworks.com/2013/12/2014-predictions-cybersecurity-trends/

1. **Cybersecurity will be more than ever a business topic**
2. **A heightened need for better intelligence and sharing on cyber threats**
3. **Security will meet reliability as attacks target control systems**

A Smorgasbord of Trends

Recorded Future - 5 Cyber Security Trends That Will Affect Your Business
https://www.recordedfuture.com/cyber-security-trends/

1. **Data Breaches**
2. **The Rise in Malware**
3. **Social Media Hacking**
4. **Web Server Mistakes**
5. **Data Breaches for Government Agencies**

A Smorgasbord of Trends

Cherry Bekaert - Cybersecurity Trends for 2014
http://www.cbh.com/cybersecurity-trends-for-2014/

1. **Enhanced use of encryption**
2. **Increased scrutiny of internal data use**
3. **Resistance to cloud technology**
4. **Risk assessment and software analysis**
5. **More destructive attacks**
6. **Rising levels of smartphone malware**
7. **Old fashioned phishing and hacking of individual users**
8. **More sophisticated malware**
9. **Active defense**
10. **Following up on network threats**
11. **The end of the internet as we know it**

A Smorgasbord of Trends

Information Age - 8 cybersecurity predictions for 2014
http://www.information-age.com/technology/security/123457447/8-cyber-security-predictions-for-2014

1. **Advanced malware volume will decrease.**
2. **A major data-destruction attack will happen.**
3. **Attackers will be more interested in cloud data than your network.**
4. **Redkit, Neutrino and other exploit kits will struggle for power in the wake of the Blackhole author arrest.**
5. **Java will remain highly exploitable and highly exploited — with expanded repercussions.**
6. **Attackers will increasingly lure executives and compromise organisations via professional social networks**
7. **Cybercriminals will target the weakest links in the "data-exchange chain"**
8. **Mistakes will be made in "offensive" security due to misattribution of an attack's source.**

Trends Watching

Key Takeaway

Trends are the aftermath of events and relatively useless in defending against new cyber attacks. Predicting trends, while useful as a marketing tool, rarely provides insight into the future.

What Should You Pay Attention To?

- Your network of professionals
- Your technology suppliers and partners
- Law enforcement agencies
- Industry newsfeeds
- New laws and regulations – both domestically and internationally
- Developing your talent base
- Most of all - your customers

Stay Focused

Key Takeaway

The most important thing, is to keep the most important thing, the most important thing.

Stephen Covey, 8th Habit

Questions

We Are Hiring!

http://www.careersatsafeway.com/

Email

John.Steensen@Safeway.com

LinkedIn

http://www.linkedin.com/in/jsteensen

Thank you!


ISACA
Trust in, and value from, information systems
San Francisco Chapter
2014 Fall Conference - "Think Big"
CRISC
CGEIT
CISM
CISA