Southern Company Gas

Cyber Security in the Utility Industry
Institute for Regulatory Policy Studies
The Environmentally Concerned, Budget Conscious, Technically Savvy Public Utility

Mark Guth
Manager, Information Security Compliance
29Sep16

Agenda

1. Mobile Application Trends
2. Cloud Computing Challenges
3. Utility Industry Cyber Security Challenges - Events
    a. Ukrainian Electric Power Grid Attack
    b. SSL/TLS Vulnerabilities and Extension
    c. SCG Phishing Emails and Malware 2016
    d. Recently Retired IT Platforms
    e. Elevated Rights and Escalated Privileges
4. Lessons Learned
5. Questions

1. Mobile Applications – Utility Industry Trends

Customer Centric Mobility

New Breed of Customers - Generation Y or "Millennials" - Smart Phone Savvy

Mobile Apps Fits in with Utility "Go Green" Strategy

Using Content Marketing to Engage Customers – Blogs, Long-form Content, Infographics, etc.[12]

Company Centric Mobility

Smart Metering/Smart Grid

New Breed of Employees - Generation Y – Mobility is a Perk

1. Mobile Applications – Trends (Continued)

Mobile Application Security Concerns:

Mobile Devices Provide Information to the Application About What Device is Being Used and the Application Adapts to the Characteristics of to the Device – Hackers can use that information.

Limited Quality Assurance on the Security of Apps in the Android App Store (90%+ may contain Malware)

Utilities cannot control the security of a customer's device – Jail Broken Phones.

Mobile Applications have Increasingly More Complex Functionality Offered to Customers.

1. Mobile Applications – Trends (Continued)

Mobile Application Security Mitigation Strategies

1. Employ Rigorous Testing Processes to Ensure Application Functions Properly for all Device Types

2. Code the Mobile Application to Make Multiple Checks on the Security of the Mobile Device Itself – Reject Jailbroken Phone From Connecting

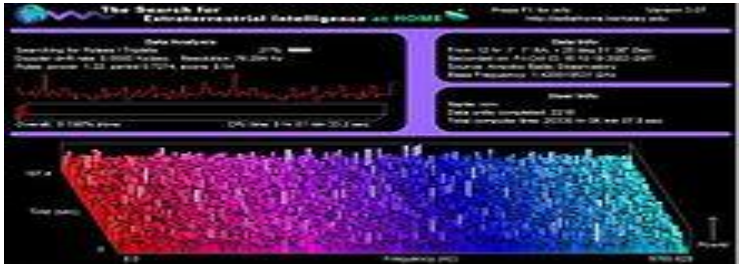
3. Join Open Web Application Security Project (OWASP) – Multiple Resources for Secure Coding and Testing of Web Applications

4. Don't Store PII or PCI on Device or Application

2. Cloud Computing – Rise of the Machines

Cloud Computing[1] – In computer networking, **cloud computing** is computing that involves a large number of computers connected through a communication network such as the Internet, similar to utility computing. In science, cloud computing is a synonym for distributed computing over a network, and means the ability to run a program or application on many connected computers at the same time.

Search for Extra-Terrestrial Intelligence SETI@Home started in 1999[2]

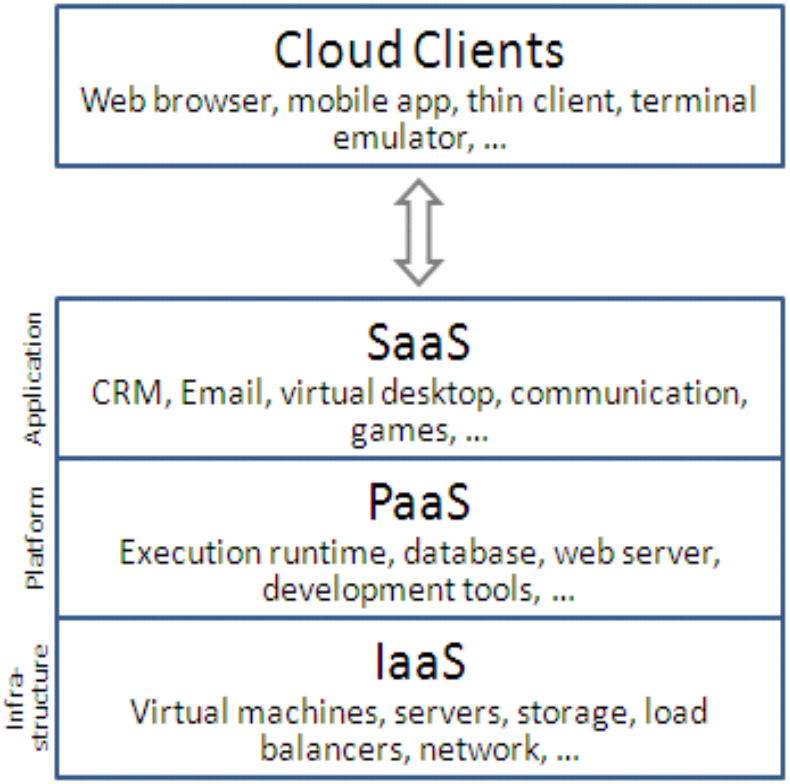


2. Cloud Computing – Platforms

Software As A Service (SAAS) - Salesforce, Gmail, GoogleDocs

Platform As A Service (PAAS) - Amazon Web Services, Openstack, Windows Azure

Infrastructure As A Service (IAAS) - AT&T, Rackspace, Verizon



2. Cloud Computing – Security Challenges

Energy Efficiency Programs – Good Cloud Deployment Candidates

Low Cost to Entry, Quick Deployment Times, Easy to Exit!

Cloud Security Challenges –

Where is your data stored (location may make a legal difference)?

Who has access to your data?

Is your data Co-mingled with other companies' data?

How Long Does Your Cloud Provider Keep Your Data?

2. Cloud Computing – Security Challenges (Continued)

How to Mitigate Cloud Security Risks:

Bring Information Security into the Process Early

Become Member of Cloud Security Alliance[3] –
Great Resources at - https://cloudsecurityalliance.org/

Look for Vendor Certifications - SSAE16, PCI, ISO 27001 to
Pass Some Risk to Vendor

Imbed Strong Security Elements Within Contractual Language to
Extend Your Security Controls to Cloud Providers

Refrain from storing confidential data in Cloud – Less Exposure

As Accountants, Consider TCO when Considering cloud options for
the Business

Recent Developments – ASU 2015-05

Cloud Accounting Notes – GAAP Accounting promotes Tax Advantages to CAPEX.

Cloud has been mainly considered OPEX but recent ruling/guidance have been made.

Local PUC's are asking questions how to use the Cloud to lower costs to rate payers.

Definition of CAPEX Cloud – Must meet both of these criteria:

1. Company has the contractual right to take possession of the code without significant penalty*, and
2. We can feasibly run the software on our own hardware, or hardware we independently host with another third party.

3. Utility Industry Cyber Security Challenges

Recent Cyber Security Events and Trends Affecting Utilities:

A: Ukrainian Power Outage

B: SSL/TLS Vulnerabilities (HTTPS)

C: Phishing Emails and Malware

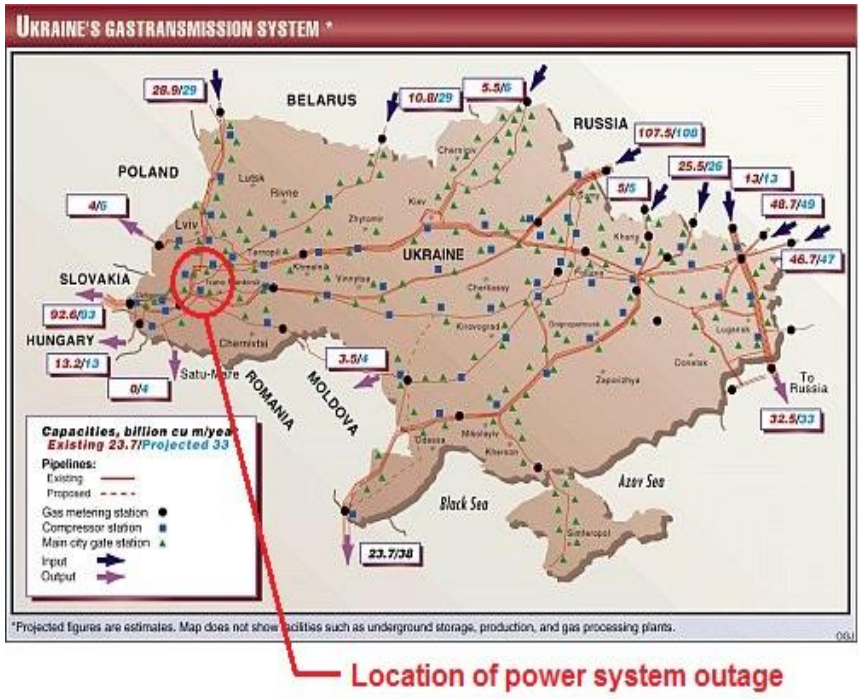
D: Recent IT Platform Retirements

E: Elevated User Access/Privilege Escalation

3A. Utility Industry Cyber Security Challenges – Events
Ukrainian Power Outage

Ukrainian Power Outage December 23rd, 2015:

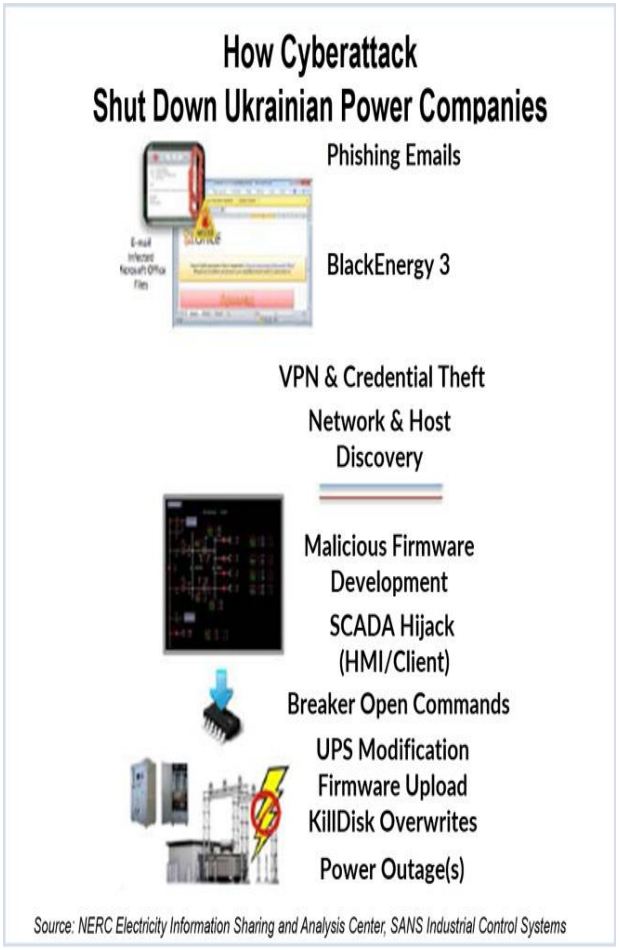
- At 3:55 PM, Technician Witnesses Electric HMI Screens Misbehaving
- 27 Transformers Knocked Offline
- 80,000 Customers in Dark.
- Call Center Overwhelmed with Fake Customer Calls
- Two Other Oblenergos (Electric Utilities) Suffered Similar Events Affecting a Total of 225,000 Customers
- Outages Lasted 6 Hours



3A. Utility Industry Cyber Security Challenges – Events
Ukrainian Power Outage (Continued)

Ukrainian Power Outage Kill Chain Steps 1-5:

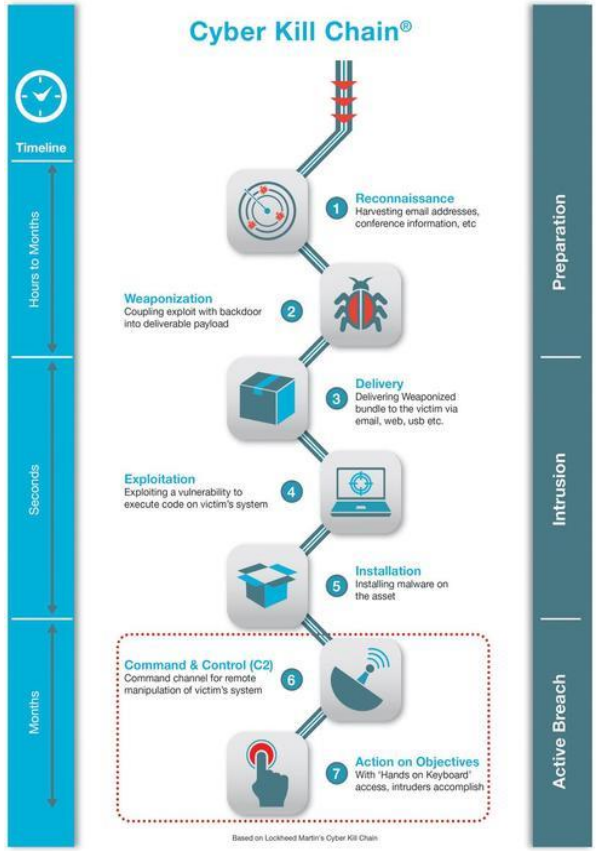
- Phishing emails sent to SCADA Admins (6 months before attack) and use of malicious Microsoft Office attachments.
- Admin clicks allowed for installation of Black Energy Malware that to led to Theft of Legitimate User Credentials.
- Threat Actors Accessed Networks and Mapped Out Network Topology and Connections.
- Threat Actors Installed Remote Access Software for the human-machine interface (HMI).
- Threat Actors Developed Malicious Firmware for SCADA Devices.
- Threat Actors Deployed Kill Disk to ICS and corporate network systems



3A. Utility Industry Cyber Security Challenges – Events
Ukrainian Power Outage (Continued)

Ukrainian Power Outage
Kill Chain Steps 6-7 :

- Threat Actors Leveraged Legitimate Remote Access Pathways (VPNs), using Legitimate User Credentials to Log Into the HMI Machines.
- Executed Disconnect Commands for Electric Substations Cutting Off Electricity to Thousands of Customer.
- Executed Firmware Overwrites that Disabled or Destroy field equipment
- Executed Kill Disk Software on Workstations
- Executed Unauthorized Disconnects of Data Center Uninterruptable Power Supplies (UPS) to Take Data Center Devices Offline.
- Use of Telephone Denial of Service (TDoS) to disrupt customer restoration.

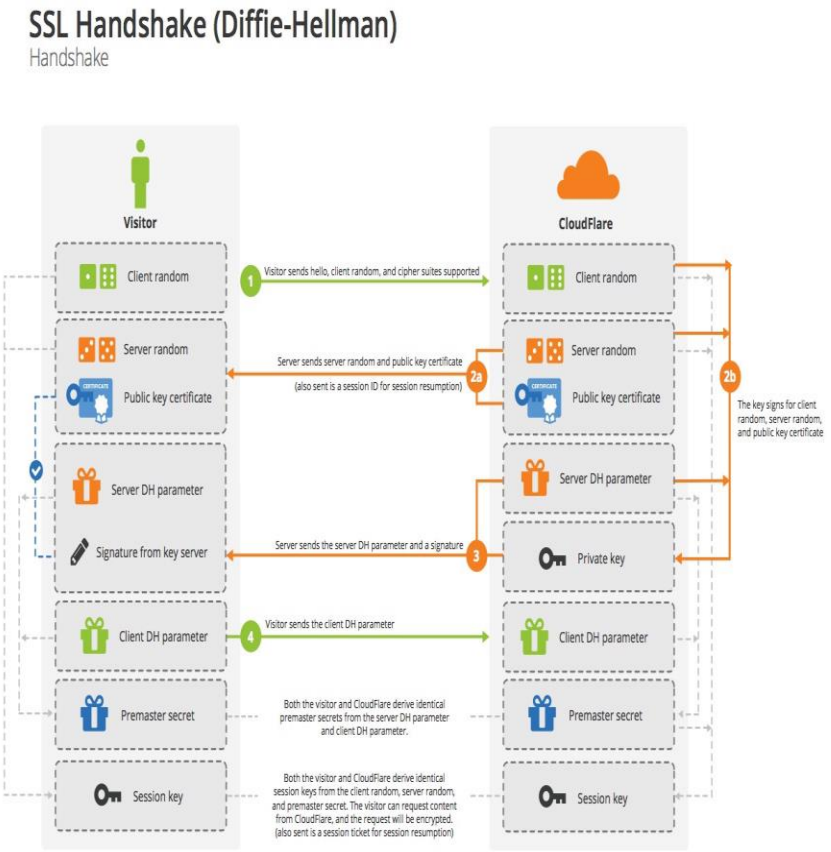


3B. Utility Industry Cyber Security Challenges – Events
SSL/TLS Vulnerabilities

SSL (Secure Sockets Layer)/TLS (Transport Layer) Vulnerabilities:

CVE-2015-0204

- During the late 1990's, early 2000's, more secure methods of encryption were developed. But US export laws allowed older and less secure keys to be included.
- As those less secure keys were compromised, hackers figured out how to exploit their use.
- Hundreds of thousands of web Sites still rely on SSL or TLS For HTTPS encryption



3C. Utility Industry Cyber Security Challenges – Events
SCG Phishing Emails and Malware 2016

1. SCG Blocks more than 20 Executive Phishing Emails Daily

2. Domain Typo Squatting – Registering a Domain Name Close to AGLResources.com to Trick Employees to Click on email links:

Glresources.com	Aglressources.com
Alresources.com	Algresources.com
Agresources.com	Aglresuorces.com
Aglresoures.com	Aglresoruces.com
Aglresource.com	Atlresources.com
Agllresources.com	Ag1resources.com

3. Cyber Triage Team Responded to over 1100 Workstation Infection Attempts in the first 6 months of 2016 – only one Actual Infection

4. Internet Content Filtering Tools Blocked More Than 1300 Malicious Web Site Access Attempts in the first half of 2016

3C. Utility Industry Cyber Security Challenges – Events
Phishing Emails – Actual Examples Targeting Executives

Mark Guth

From: John Somerhalder <ceocommpany@gmail.com>
Sent: Monday, December 07, 2015 10:04 AM
To: Beth Reese

Hello Beth,Are you in the office now?

Thanks,
John W. Somerhalder II
Chief Executive Officer

External Email - Click here to report this email as spam.

1

3C. Utility Industry Cyber Security Challenges – Events
Phishing Emails – Actual Examples Targeting Executives

Mark Guth

From: Andrew W. Evans <aevans.aglresources@yahoo.com>
Sent: Sunday, January 10, 2016 7:10 PM
To: Beth Reese
Subject: Follow Request

Beth,

Are you available ?

Andrew W. Evans
President and
Chief Executive Officer
aevans@aglresources.com

External Email - Click here to report this email as spam.

1

3D. Utility Industry Cyber Security Challenges – Events Recently Retired IT Platforms

Impact of Retired Vendor Platforms:

No more security updates for known issues.

Vulnerabilities identified in the future will not be fixed.

Significant Number of Machines still need to be upgraded or replaced.

MS:Windows Server 2003 Support Ended 7/14/15
MS:Windows XP Support Ended 4/08/14
MS: Internet Explorer 8.0 Support Ended 1/14/16
MS: SQL 2005 Support Ends 4/12/16
MS: .Net 4.5.1 Support Ended 1/12/16
SSL 1.0, 2.0, 3.0 Compromised 2014
Adobe X - 11/18/2015

Users – Prepare for Change!
Pressure Vendors to Stay Current!

3E. Utility Industry Cyber Security Challenges – Events Elevated Rights and Escalated Privileges

Escalated Privilege Risk:

- The #2 VERIS Threat Actions for confirmed data breaches over the previous three years is the use of stolen credentials. [10]
- 60% of all attacks in 2015 were by an insider, whether malicious or inadvertent.[11]

- Inadvertent – Make a Mistake
- Intentional – Plan to Act Inappropriately
- Misappropriated – Credentials Stolen

Lessons Learned

Improve Training and Incident Response Processes – Technology Not Enough – People Remain Still The Weakest Link (Phishing, poor decisions, make mistakes, etc.).

Know who are your Elevated Rights users and Monitor their usage. Consider Implementing an Insider Threat Program.

Provide More Detailed Security Awareness Training for all Security and SCADA Operators – “Learn to Connect the Dots”

Must Have an asset lifecycle process defined. All electronic assets come to an end of life, that pace appears to be accelerating for computer related assets.

Subscribe to the Microsoft Support Lifecycle newsletter highlighting the retirement dates for products and service packs.

4. Utility Industry Cyber Security Challenges
Events Lessons Learned (Continued)

Lessons Learned

Validate and Monitor all “trusted” third party network connections. Eliminate or firewall off “untrusted” third party networks.

For remote access, validate and monitor two factor authentication for all remote access users. Look for usage patterns outside of “normal” – afterhours, extra long sessions, etc.

Employ network segmentation to hamper the threat actors from easily moving laterally within the network.

Employ security tools to look for existing or attempted Indicators of Compromise (file hashes, IP addresses, etc.)

4. Utility Industry Cyber Security Challenges Events Lessons Learned (Continued)

Lessons Learned

Having a formal vulnerability management program and incident response plan is critical to assess the risk, impact, and response to emerging vulnerabilities.

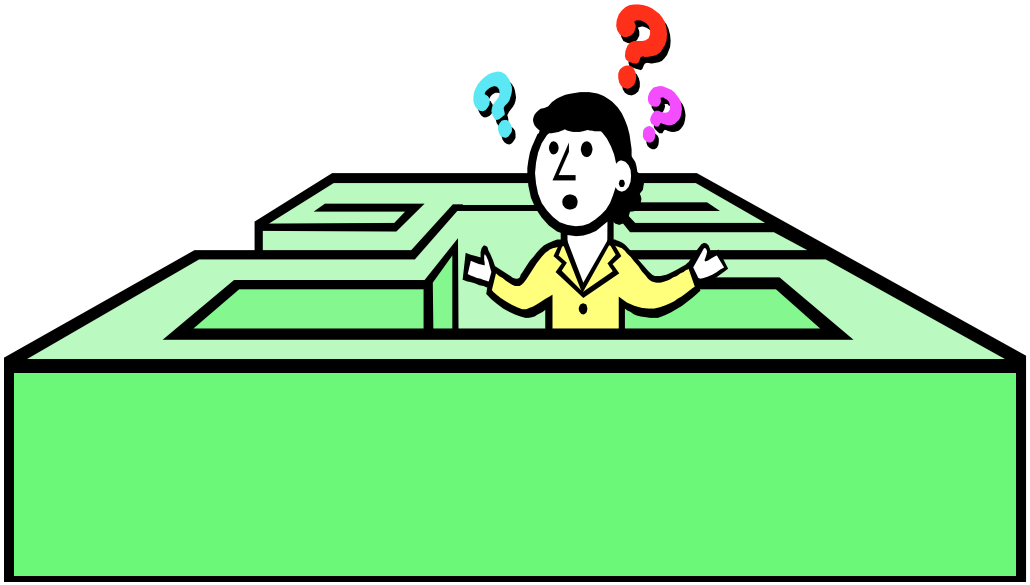
At home, change all your passwords if use the same one on multiple sites and one of the those sites had a vulnerability or breach.

Consider “freezing” your credit with the credit bureaus.

Don't do your home banking from an XP PC or Laptop. Replace your old Hardware and vulnerable Operating System Software.

Configure your web browser to not use insecure SSL/TLS versions. Test your most common web sites you access for compatibility.

Questions?



Email me at: mguth@southernco.com

Appendix: How to Stay Vigilant at Home

@ Home You Can:

- Replace your XP PC or Laptop with Windows 10
- Turn Your Home Computer off When Not in Use
- Embrace Password Complexity Rules – Develop a System to Make Complexity Easier – Picture, Calendar, etc.
- Use Encrypted Portable Storage for Confidential Data – DVD's or USB Stick – Always Back Up Your Data
- Don't Click on an Email Attachment You Are Not Expecting
- Learn how to recognize mismatched email headers – sender is not from the domain indicated in the header.
- If the Victim of a Data Breach, Use the Credit Monitoring Service Provided to You. Freeze Your Credit!

PG&E Metcalf Substation Attack[5]

Disorganized Event on April 16th 2013 where Attackers Shot Up a San Jose Electric Substation

Included Physical and Cyber Security Attack Vectors

No One has ever been Identified or Claimed Responsibility

Prompted Utilities to Examine Their Own Facility and Asset Security Measures.

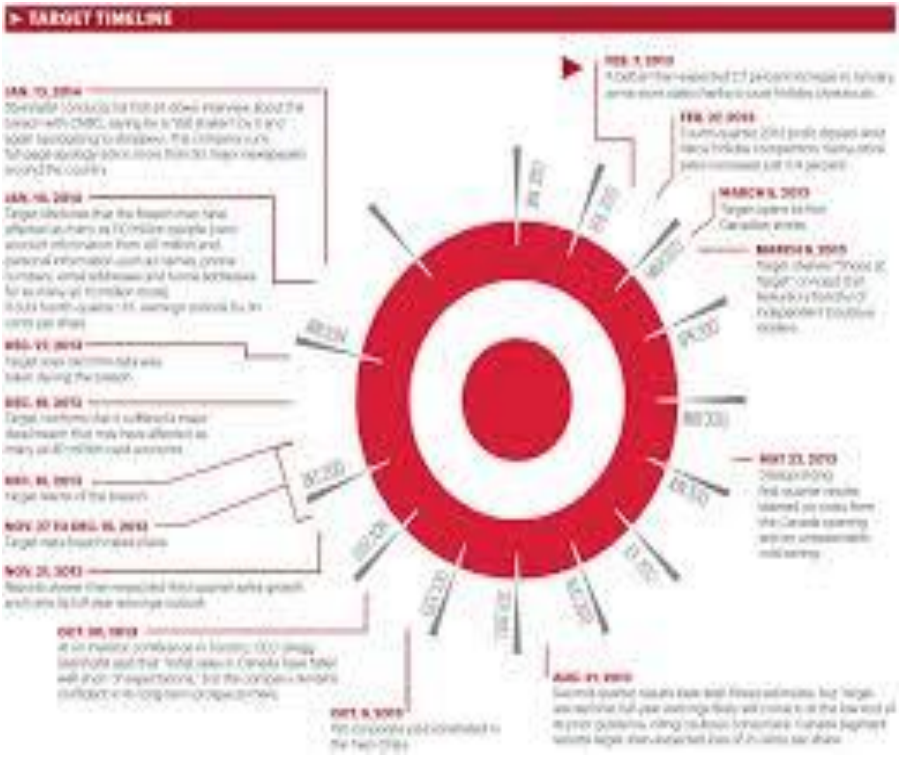
Target Data Breach:

Malware Deployed to Target POS Systems – 11/28/13[4]

Target Acknowledges Breach - 12/18/13

Target Confirms Malware Components

Target SOC Received Security Alerts from their Tools and Dismissed Them Without any Action



Heartbleed Vulnerability:

Issue with specific versions of OpenSSL which is used to encrypt data transmissions, especially on the internet.

This Vulnerability was known by NSA for at least two years before its existence was made public. Who else knew?

Utilities had to check their own systems and inquire about those of their business partners.

Employ fix - patch system if needed, replace certificate, and force users to change passwords.

Poodle Vulnerability:

"Padding Oracle On Downgraded Legacy Encryption" - Man in the Middle Exploit that takes advantage of flaws in SSL and TLS Security.

This Vulnerability Identified by Google in October, 2014.

Though not as bad as Heartbleed (see Appendix), this still affects about 50% of the World's Users.

Communicate to users that your Company is going to Disable TLS 1.0 before 6/30/2016 (the PCI DSS Certification cut off date)

Anthem Data Breach:

Discovered 1/27/15 by DBA who Saw a database job running Under his ID.

Breach Disclosed 2/04/15

80,000,000 Records Disclosed – Names, DOB, SSN, street addresses, email addresses and employment information, including income.

No Additional Details of Hack Available – Though it Involved use of WE11POINT.COM and has been Attributed to China

Works Cited

- [1] *http://Wikipedia.com/* 14 April 2014
- [2] http://www.seti.org/ started in 1971, public cloud computing in 1999
- [3] https://cloudsecurityalliance.org/
- [4] *Inside A Targeted Point-of-Sale Data Breach* Dell Secureworks
- http://krebsonsecurity.com/wp-content/uploads/2014/01/Inside-a-Targeted-Point-of-Sale-Data-Breach.pdf
- [5] *Assault on California Power Station Raises Alarm on Potential for Terrorism* Wall Street Journal *February 5, 2014*
- http://online.wsj.com/news/articles/SB10001424052702304851104579359141941621778
- [6] *Sandworm* , iSIGHT Partners Inc. 2014
- [7] http://www.darkreading.com/attacks-breaches/deconstructing-the-cyber-kill-chain/a/d-id/1317542?image_number=1

Works Cited

- [7] *Defending Against the Dragonfly Cyber Security Attacks,*
- Joel T. Langill, written for Belden, 10 December 2014
- [8] http://krebsonsecurity.com/2015/06/how-i-learned-to-stop-worrying-and-embrace-the-security-freeze/ Brian Krebs 08 June 2015
- [9] *Analysis of the Cyber Attack on the Ukrainian Power Grid,*
- SANS Industrial Control Systems with the Electricity Information Sharing and Analysis Center, March 18, 2016.
- [10] http://veriscommunity.net/enums.html#section-actions
- [11] Securion – www.Securion.io
- [12] *Meet The Millennials* American Gas Magazine, June 2016.

See The History of Data Breaches At:

http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/