Welcome to the Cyveillance Weekly Trends Report

Greetings from Cyveillance, the leader in open source threat intelligence. Since threat intelligence is constantly evolving, we publish this newsletter to keep our customers updated on the latest threats to various industries. Each week, we'll send you highlights from our analyst research reports. You can unsubscribe at any time. For the latest security news stories throughout the day, you can also follow us on Twitter, or to view the latest security articles from Cyveillance experts, subscribe to our blog.

In this Issue:

- Top Weekly Incidents
- Energy
- Agribusiness
- Insurance / Healthcare
- Financial Services
- Global Intelligence
- Legal and Regulations
- Pharmaceuticals
- Retail
- Technology
- Telecommunications
- Entertainment
- Defense
- Law Enforcement

Cyber Safety Awareness Training

Protect your Organization with Computer-Based Training

Are your employees the weak link in your security program? We want to help you educate your employees to keep them — and your organization — more secure.

Our computer-based cyber security training can help your employees learn how to protect your organization from the latest threats and reduce the high costs associated with incident remediation.

Click Here To Learn More

Top Incidents

Energy

- Following 20 months of intense, organized community opposition, a major utility company cancelled plans to build a 345 kV transmission line through parts of Arkansas and Missouri.

Agribusiness

- Russia introduced taxes on wheat exports, an effort to reduce food prices after the ruble’s collapse made it attractive for farmers to sell grain abroad.

Insurance/Healthcare
• Federal regulators plan to resume random HIPAA compliance audits in 2015; organizations should prepare by doing their own mock audits. During the mock audits, healthcare providers should ensure that they have all HIPAA-related documentation in one place, so that they can provide proof to government auditors about their security and privacy compliance efforts.

Financial Services

• Hackers released a cache of 13,000 passwords and credit cards associated with two separate gaming stations and one leading ecommerce site on December 27, 2014.

Global Intelligence

• In Vietnam Lao Dong News reported that starting from January 1, 2015 labor regulations required an increase in social insurance taxes but the benefits have been reduced. According to the new regulation, employees who terminate their own employment will not receive unemployment insurance.

Legal and Regulations

• The Federal Communications Commission is expected to introduce and vote on net neutrality rules in February, Brian Fung reports for the Washington Post. Republican lawmakers are preparing to take the net neutrality debate into their own hands if the FCC opts to regulate internet service providers as utility companies, Gautham Nagesh reports for the Wall Street Journal.

Pharmaceuticals

• Activists protested AstraZeneca's plans for a global headquarters and animal testing lab in Cambridge, UK, reported Cambridge News. The group formed towards the end of last year with the aim of opposing the company's planning application to include an animal research lab in the city as part of the new 330-million-pound headquarters on the Biomedical Campus.

Retail

• National Association of Federal Credit Unions (NAFCU) President and CEO Dan Berger renewed the association's push for national data security and breach notification standards for retailers amid news of a possible data breach at Chick-fil-A chain restaurants.

Technology

• The United States imposed fresh sanctions on North Korea on Friday in its first public act of retribution for a crippling cyber-attack against Sony. The stepped-up sanctions, authorized by executive order from President Barack Obama, will affect three North Korean entities, including a government intelligence agency and a North Korean arms dealer. The U.S. is also sanctioning 10 individuals who work for those entities or the North Korean government, the Treasury Department said

Telecommunications

• FairPoint Communications won a small victory in its ongoing fight with its union workers in northern New England as the National Labor Relations Board (NLRB) has rejected the unions' accusations that the service provider is bargaining in "bad faith."

Entertainment

• An FBI bulletin claims that the perpetrators in the Sony breach may extend their efforts to threaten other media companies. The Guardians of Peace posted taunting messages to Pastebin.com that mocked the FBI and an undisclosed media organization's investigation efforts. The targeted media organization has not yet been identified.

Defense

• Despite billions of shekels invested over decades in its defense industrial base, Israel
lacks a coherent plan for safeguarding strategic infrastructure and critical production capacity, according to the nation's top watchdog.

**Law Enforcement**

- The FBI is not backing down on its claim that North Korea was the mastermind behind the disruptive Sony studio hack. The bureau's insistence comes after a growing number of private cyber-security firms are saying there is no evidence to conclude North Korea was the mastermind. FBI agents were briefed earlier this week on a theory that the attack was launched by former disgruntled Sony workers. In a statement, the FBI said North Korea was responsible, citing "intelligence from US intelligence community, DHS [Department of Homeland Security], foreign partners and the private sector."

**Energy**

- Following 20 months of intense, organized community opposition, a major utility company cancelled plans to build a 345 kV transmission line through parts of Arkansas and Missouri.

- More than 1,600 barrels of crude were ablaze just south of Williston, N.D., on January 1, 2015, after storage tanks caught fire while trucks were delivering oil, but no one was injured.

- Firefighters have managed to extinguish a fire at Libya’s largest oil port, al-Sidra. The blaze began when oil tanks were struck by an insurgent rocket.

- Circuit Judge James C. Kingsley has given activist Chris Wahmhoff a suspended two-month jail sentence and ordered him to serve one year of probation. With the suspended sentence, Wahmhoff will not serve any jail time if he successfully completes probation. Wahmhoff had been convicted of a felony earlier this month for a 2013 protest he staged inside a section of an Enbridge Inc. oil pipeline in Marshall.

- A Shell Oil contractor whose ship ran aground while attempting to drill in the Chukchi Sea in 2012 has pleaded guilty to eight environmental felonies, fined $2.2 million dollars and been put on probation for four years. In addition the parent company of Noble Drilling LLC, which was charged in connection with incidents involving the drill ship Noble Discoverer and the drilling unit Kulluk that it was towing, must create an environmental management system for its mobile offshore drilling units, the U.S. Department of Justice announced on December 9.

- The Guardian reports: Climate change talks next year will be make or break for international efforts to curb global warming, with the credibility of the UN-backed process at stake, the outgoing EU climate chief, Connie Hedegaard, has warned. World leaders are expected to sign an agreement to limit greenhouse gas emissions from 2020 onwards at a Paris conference in December 2015. It could be pivotal in climate negotiations, if China, the US and Europe agree to hold global warming within what scientists say are safe limits. But the risks are great, according to Hedegaard, who recently left the post of European commissioner for climate action and hosted the Copenhagen climate talks in 2009. “Say Paris could not deliver,” she said to the Guardian. “Who would believe the UN process would have credibility after that? That is what [we need] to make leaders understand – it’s now.”

- A federal judge ruled against nine southern New York homeowners who claimed their drinking water was contaminated by a nearby natural gas well. The homeowners had sought $2 billion in damages from Denver-based Anschutz Exploration Corp.

- A third of Britain’s listed oil and gas companies are in danger of running out of working capital and even going bankrupt amid a slump in the value of crude, according to new research. Financial risk management group Company Watch believes that 70pc of the UK’s publicly listed oil exploration and production companies are now unprofitable, racking up significant losses in the region of £1.8bn.
UK oil and gas companies are gearing up for a new era of transparency which will shed light on links between operators and governments around the world, law firm Pinsent Masons says. An overhaul of financial reporting driven by a new European Union directive is due to come into force on New Year’s Day, months ahead of other EU member states. Directors face criminal convictions and unlimited fines if details of any payments made to governments are not disclosed to Companies House.

At the end of 2015, the nations of the world will meet in Paris and attempt to hammer out a global deal to cut greenhouse gas emissions. And Pope Francis hopes that the world’s Catholics, as well as other major religions, will be a big part of serious climate action. This includes a series of steps next year. Francis is expected to tell the planet’s 1.2 billion Catholics why acting on climate change is essential to the faith using an influential church document called an encyclical. This has been long-rumored, but will reportedly be released to the world’s 5,000 bishops and 400,000 priests following a papal visit to the hurricane-damaged city of Tacloban in the Philippines.

Agribusiness

- Russia introduced taxes on wheat exports, an effort to reduce food prices after the ruble’s collapse made it attractive for farmers to sell grain abroad.

- An undisputed claim of analysts and experts is that incomes will grow significantly in big countries like China and India for a while. As a result, there will be more demand for proteins and, consequently, for grains. For U.S. farmers, that means that exports will continue to be steady and will be a bullish factor for grain prices in the coming years.

- Forestry, agriculture, and state assets face increased risk of arson in Chile’s southern Araucanía region.

- A December 31, 2014 fire at Norman Crooks Farms in Stanton, Michigan, damaged all of the potato farm’s storage buildings that housed millions of dollars of farm equipment and millions of potatoes.

Insurance/Healthcare

- Community Health Systems’ data breach affecting 4.5 million people was the largest healthcare data breach of 2014.

- Chinese authorities have stressed privacy protection for AIDS-affected children and may punish those found leaking private information. No institutions or individuals shall publish information such as the name, address, school, portrait or medical records of children infected with or impacted by HIV without the approval of their guardians, according to a statement jointly issued by the National Health and Family Planning Commission, Ministry of Education and Ministry of Civil Affairs on December 29, 2014.

- HealthcareInfoSecurity’s fourth annual Healthcare Information Security Today Survey is designed to help identify which emerging cyberthreats healthcare organizations are most worried about for 2015. The annual survey, sponsored this year by Caradigm, (ISC)², and ZixCorp, aims to give healthcare information security professionals and other senior executives insights that they can track and measure over time. The deadline to participate is January 5, 2015.

- Federal regulators plan to resume random HIPAA compliance audits in 2015; organizations should prepare by doing their own mock audits. During the mock audits, healthcare providers should ensure that they have all HIPAA-related documentation in one place, so that they can provide proof to government auditors about their security and privacy compliance efforts.

- Innovative Australian online mental health providers could be deserted by clients under
the government's controversial new metadata laws, which may affect the site's ability to provide anonymity and freedom from stigma.

- At least three Greater Toronto Area hospitals do not proactively audit their patient records to detect privacy breaches. A survey of 24 hospitals and health-care centres found that more than half say they check their information systems for inappropriate access at least once a month. In contrast, one hospital — Providence Healthcare — still uses paper-based record keeping and reported that it could not conduct audits until a future electronic system is implemented.

- In an effort to address the cybersecurity challenges of networked medical devices, the National Institute of Standards and Technology, through the National Cybersecurity Center of Excellence, is launching a project to secure those devices from risks such as malware, hacking, and access control.

---

Financial

Financial Services

Activism

- Numerous customers of a leading U.S. financial firm have called on others to boycott and destroy credit and debit cards associated with the organization. This comes after the firm’s leading spokesperson called for celebrities to “call out racist cops.”

Information Security Risk

- A 64-bit version of Havex, a remote access tool (RAT) that has been used in cyber espionage campaigns aimed at industrial control systems, was recently discovered. One of the files observed in the infection is TMPprovider023.dll (BKDR64_HAVEX.A), a component responsible for C&C server instructions for downloading files and executing commands.

- A new step in the evolution of ransomware has been documented by security researchers who discovered a sample that encrypts the files on the storage unit and creates unique instances of itself due to its polymorphic feature. The threat has been named VirRansom and VirLock by researchers in order to relay both its virus and desktop locking and ransomware sides. However, unlike the usual crypto-malware, this one allows decryption of the files, but it won’t stop locking the screen, thus forcing the victim to pay.

- An established hacktivist collective is offering DDoS monthly subscription services. The starting price pays for an attack lasting 100 seconds. A 1,500 second attack costs $28.99. The most expensive package is a 30,000 second attack for $129.99 per month. A “lifetime” subscription is also offered at $500 per month.

- Several U.S. financial institutions discovered a pattern of credit card fraud in accounts used at a particular fast-food restaurant chain across the U.S. between December 2, 2013 and September 30, 2014.

- Nearly 1,300 accounts from a leading U.S. online commerce site were compromised on December 31, 2014.

- Hackers released a cache of 13,000 passwords and credit cards associated with two separate gaming stations and one leading ecommerce site on December 27, 2014.

- A torrent making the rounds in South Korea poses as an Android app to download the controversial movie ‘The Interview’ to mobile devices but instead installs a two-stage banking Trojan onto victims’ devices. The banking Trojan, which was hosted on Amazon Web Services, targets customers of a number of Korean banks, as well as one international bank.

Operational Risk
An activist group based in Seattle, WA will host its first organizing meeting of 2015 on January 6, 2015 to discuss its 2015 objectives from which to conduct "campaigns, events, and actions" in the upcoming year with intent to “hold banks accountable.” The group's objectives include:

- Just-Cause Eviction Protection
- Acceptance of BTA Agreements
- Restitution
- End Bank-Caused Urban Blight
- Push the Government to Uphold Human Rights
- Rent Control
- Transparent Evictions
- Recognize Civil Land Disputes
- King County Moratorium on Bank Evictions
- End Illegal Home Auctions
- Audit All Deeds
- Seattle Must Move its Money
- End Homelessness in King County
- Resist the Commodification of Housing

Multiple open source news outlets report that banks in the United Kingdom are concerned that Apple's attempt to launch its NFC payment solution in the UK will cause privacy and security issues, and, contribute to money laundering and the financing of terrorism.

**Reputational Risk**

- The FBI is investigating whether US financial institutions have started fighting back against hackers by embarking on hacking campaigns of their own, allegedly disabling servers used by Iran in a series of cyberattacks from 2012 into 2013.

- An independent policy think-tank institution based in Oakland, CA that focuses on key social and environmental issues has labeled a leading U.S. brokerage firm as one of the worlds “largest land grabbers right now,” negatively contributing to human rights and agricultural issues.

- An environmental activist group published a year-end 2014 report that details progress in financial firms’ global divestment from fossil fuel and mountaintop removal.

**Global Intelligence**

**China**

- A Chinese cyber security news outlet reported there was a malicious application exploiting the SOP vulnerability on Android to obtain Facebook users’ messages.

- A Chinese technology news outlet reported that Skype Android application contains a high risk security vulnerability that could be exploited to monitor certain Skype user.

- A Chinese news outlet reported a new variant of Trojan.Agent.IXM that is able to released malicious files in specific directory on infected platforms.

- The website 178.com reported the risk of DDoS attacks increased over the past 2 years and paid-DDoS services are appearing in the illegal underground market. The article speculates the online gaming companies will be the main target for DDoS attacks in the future.

- Article on Gmw.com reported Blue Coat Security discovered a new malware targeting Android devices that specialized in attacking high level individuals in government, military, financial, engineering and other industries.

**Germany**
The German state of Bavaria tried in 2014 to bolster its capabilities addressing cybercrime; however, the relative number of identified perpetrators of Internet crimes remained with around 43 per cent about the same level comparable to previous years. This is despite the employment of over 300 computer experts and specially trained police officers and despite the fact that the overall number of Internet crimes is thought to have decreased in 2014. According to the Bavarian minister of the interior, Joachim Herrmann, who presented those numbers, the lack of Internet data retention rules is a main obstacle for investigators.

India

The Nation reported that an angry labor dispute at a Special Economic Zone near Chennai erupted on Monday resulting in scores of arrests. The workers at the Special Economic Zone are frustrated by harsh recent cutbacks at Foxconn. About 250 people tried to enter the gates of the plant to punch the clock to claim wages but police officers blocked them. Union members claimed that 168 were arrested.

Enjoy Share Point reported that India’s largest IT company Tata Consultancy Services may lay off senior employees and the number can come up to 30,000. TCS will do a performance-related restructuring of its workforce, which may also lead to some employees being asked to leave the company. The layoff will happen in both onsite and offsite positions. It will be from middle to senior-level positions and also some employees may be offered positions at vendors working with TCS.

Israeli

Arutz Sheva reported that Treasury and Histadrut labor union officials on Sunday agreed on a framework to raise the minimum wage in Israel to NIS 5,000 per month for full-time workers. The increase will be built into future Histadrut labor contracts, and later advanced for legislation in the Knesset. Officials will discuss a schedule to implement the increases with the Attorney General. According to the plan, the minimum salary for full-time work will increase to NIS 4,650 on April 1, 2016, and to NIS 4,825 on August 1 of that year. Salaries will again increase to NIS 5,000 on January 1, 2017.

Malaysia

A Malaysian news outlet reported that a flood is under control in the State of Kedah and Perlis. The article mentioned that an evacuation center is still open in Kulim.

A Malaysian news outlet reported that MTUC urged private sector employers in the flood-affected states to consider granting paid leave to their employee until floodwater’s recede.

A Malaysian news outlet illustrated the harsh working condition of a Nepalese worker in a Japanese-owned electronic manufacturing plant located in Kuala Lumpur.

MTUC shared a news article dated to November 24, 2014 regarding the revision of minimum wage is expected to be completed in early 2015. MTUC speculates whether the minimum wage will be remaining at RM900 or if there will be an increase.

Vietnam

Ping West reported that the base salary in Hanoi, Vietnam is $145/month compared to Guangzhou and Shenzen of $395/month and $295/month, respectively. As such, Microsoft is laying off workers in China and move its phone production mainly Hanoi, Vietnam.

Lao Dong News reported that starting from January 1, 2015 labor regulations required an increase in social insurance taxes but the benefits have been reduced. According to the new regulation, employees who terminate their own employment will not receive unemployment insurance.

Lao Dong News reported that over 2,500 workers from Hyundai Vinashin company went on strike after announcements that the company will only increase salary by 5%, less than 50% of the salary increase in 2014. On December 27, 2014 company leader
informed workers that the salary increase will be 10% instead of 5%, the workers got back on the bus and returned home. A majority of the workers requested that salary be increase to 15% and retain company subsidy at 50,000 VND/person/month, and increase Lunar New Year bonus from 1,000,000 VND/person to 1,300,000 VND/person. Hyundai

Legal and Regulations

- The Federal Trade Commission’s Endorsement Guides apply not only to bloggers who receive promotional merchandise, but also to contest promotions and corporate social media advertising. A recent FTC action confirms that advertising agency staffers cannot casually tweet nice things about their clients without disclosing their relationship. In this action, the FTC asserted that by asking its employees to tweet about the product in this fashion, Deutsch LA had “represented, directly or indirectly, expressly or by implication, that these comments about the PS Vita were independent comments reflecting the views of ordinary consumers who had used the PS Vita.” Under a settlement order, Deutsch LA (advertising agency hired by Sony) is barred from such conduct in the future. Companies and their advertising agencies must be cautious about engaging social media in the promotion of products or services without disclosing their employment or other pertinent relationship. This concern is likely to become an even larger issue with the growing prominence of anonymous social media services such as Yik Yak, Secret and Whisper.

- The Indiana attorney general proposed legislation December 22, 2014 to impose strict requirements for the storage of sensitive data, reduce harm to consumers in the case of a data breach, and increase transparency of online privacy policies. The proposed legislation also includes an amendment to Indiana’s Disclosure of Security Breach Act. Indiana is just the latest state seeking to expand privacy and data security requirements. In the last few months, New Jersey, New York, and Oregon have announced plans to amend existing regulations. Last month, the New Jersey Assembly unanimously approved a bill designed to expand the state’s data breach laws to include disclosure of a breach of security of online accounts. In September, the New York Assembly introduced legislation that would require entities that conduct business in New York and deal with computerized private information to develop, implement, and maintain a comprehensive information security program. Finally, Oregon’s attorney general also recently announced plans to introduce legislation to enhance data privacy standards and increase enforcement of civil penalties against non-compliance. States are trending toward tougher and tighter privacy and data protection regulations.

- The Federal Communications Commission is expected to introduce and vote on net neutrality rules in February, Brian Fung reports for the Washington Post. Republican lawmakers are preparing to take the net neutrality debate into their own hands if the FCC opts to regulate internet service providers as utility companies, Gautham Nagesh reports for the Wall Street Journal.

Pharmaceuticals

- Drug makers that sell prescription painkillers may face yet another government lawsuit. Maura Healey, the attorney general-elect in Massachusetts, is considering legal action against pharmaceutical makers in hopes of thwarting the abuse and misuse of opioid painkillers. The medicines have increasingly been blamed for fueling addiction and crime, and serving as a bridge to a growing heroin trade.

- Antibiotics producers in China are suspected of dumping waste water and polluting the country’s drinking water source.

- Business Standard reported that US drugmakers with significant operations in India are said to be seeking easier rules for doing business in the country, especially with
regard to pricing controls. According to the news source, which cited unnamed sources, several US-based firms are lobbying with regulatory authorities over the price-control framework.

- Activists protested AstraZeneca's plans for a global headquarters and animal testing lab in Cambridge, UK, reported Cambridge News. The group formed towards the end of last year with the aim of opposing the company's planning application to include an animal research lab in the city as part of the new 330-million-pound headquarters on the Biomedical Campus.

Retail

- The CEO of Revlon is a bigoted bully who hates “dirty” Americans, thinks Jews “stick together” and believes he can “smell” black people when they walk into a room, according to a new lawsuit. The beauty company's boss, Lorenzo Delpani, made the ugly comments after taking over in 2013, according to a discrimination suit filed by Revlon's former top scientist, Alan Meyers, who says he was ostracized because of his Jewish heritage.

- Parking services have taken a beating this year at the hands of hackers bent on stealing credit and debit card data. This week's victim — onestoparking.com — comes compliments of the same organized crime gang thought to be responsible for stealing tens of millions of card numbers from shoppers at Target and Home Depot.

- National Association of Federal Credit Unions (NAFCU) President and CEO Dan Berger renewed the association's push for national data security and breach notification standards for retailers amid news of a possible data breach at Chick-fil-A chain restaurants.

Technology

- The United States imposed fresh sanctions on North Korea on Friday in its first public act of retribution for a crippling cyber-attack against Sony. The stepped-up sanctions, authorized by executive order from President Barack Obama, will affect three North Korean entities, including a government intelligence agency and a North Korean arms dealer. The U.S. is also sanctioning 10 individuals who work for those entities or the North Korean government, the Treasury Department said.

- Apple is facing a lawsuit accusing the company of falsely advertising the storage capacity available in its iPhones, iPads and iPods.

Telecommunications

- Newly fortified Republicans in Congress are considering a number of ways to stymie the Obama administration's planned regulations on broadband Internet providers in 2015, making Capitol Hill a new front in the fight over "net neutrality."

- FairPoint Communications won a small victory in its ongoing fight with its union workers in northern New England as the National Labor Relations Board (NLRB) has rejected the unions’ accusations that the service provider is bargaining in "bad faith."

Entertainment
An FBI bulletin claims that the perpetrators in the Sony breach may extend their efforts to threaten other media companies. The Guardians of Peace posted taunting messages to Pastebin.com that mocked the FBI and an undisclosed media organization's investigation efforts. The targeted media organization has not yet been identified.

Defense

Despite billions of shekels invested over decades in its defense industrial base, Israel lacks a coherent plan for safeguarding strategic infrastructure and critical production capacity, according to the nation's top watchdog.

Accenture LLP, a consulting giant that was tapped in January to help fix the embattled HealthCare.gov, on Monday said it won a five year, $563 million contract to continue its work on the federal insurance site.

Law Enforcement

The FBI is not backing down on its claim that North Korea was the mastermind behind the disruptive Sony studio hack. The bureau's insistence comes after a growing number of private cyber-security firms are saying there is no evidence to conclude North Korea was the mastermind. FBI agents were briefed earlier this week on a theory that the attack was launched by former disgruntled Sony workers. In a statement, the FBI said North Korea was responsible, citing "intelligence from US intelligence community, DHS [Department of Homeland Security], foreign partners and the private sector."

A St. Louis man was charged Thursday with making threats against police and the St. Louis City Justice Center on Twitter. Jason Valentine, 35, faces 10 felony counts of making a terrorist threat, the St. Louis Circuit Attorney's office said. Valentine allegedly tweeted about "Kill a pig Night" throughout December, the probable cause statement said, and that he threatened an explosion at the Justice Center on Wednesday. "St. Louis City Justice Center Mysteriously Exploded December 31, 2014," one tweet read, according to the statement. Another said, "New Years Eve Massacre Kill A Pig Night."

Leaders of the U.S. Senate Judiciary Committee said Wednesday they were seeking answers from the Obama administration about federal law enforcement's use of surveillance technology that sweeps up basic cellphone data. In a bipartisan letter to the departments of Justice and Homeland Security, Sens. Patrick Leahy, a Democrat, and Chuck Grassley, a Republican, described a recent policy change by the FBI that they said had left them with additional questions about how the equipment was used and about what privacy protections were in place. Among the tools singled out in the letter is Stingray, a device that pretends it is a cellphone tower and tricks cellphones into identifying some of their owners' account information. Law enforcement authorities have said the technology, which allows police to obtain cellphone information without having to ask for help from service providers, is useful for catching criminals, though civil liberties advocates have raised privacy concerns.

The FBI said last week that it's seeking technology experts — including those with experience in "ethical hacking" — to become "cyber special agents." In its job post, which is open until January 20, 2015 the agency said it has "many vacancies" for cyber special agents. Such agents, the FBI said, should have the skills to "conduct multifaceted investigations of high-tech crimes, including cyber-based terrorism, computer intrusions, online exploitation and major cyber fraud schemes."

Homeland Security has failed on all five of its main missions, according to a scathing oversight report by U.S. Sen. Tom Coburn. "Ten years of oversight of the Department
of Homeland Security finds that the Department still has a lot of work to do to strengthen our nation’s security,” Coburn said. “Congress needs to review the Department’s mission and programs and refocus DHS on national priorities where DHS has a lead responsibility.” One unanswered question, according to the report, is whether the $50 billion that Homeland Security spent in the past 11 years on counterterrorism made the country any safer. The report also criticizes Homeland Security for failing to properly protect the borders and combat cyber-attacks.