WORLD JURIST ASSOCIATION
A WORLD RULED BY LAW, NOT FORCE

WORLD JURIST ASSOCIATION BIENNIAL CONGRESS, BARCELONA, SPAIN

INTERNET: CHALLENGES TO PEACE AND FREEDOM

Panel 1: Justice, Civil Service and the Internet

Hacking Municipal Government: IT Best Practices for the Protection of Confidential, Proprietary and Other Sensitive Local Government Data

May 20, 2016

Benjamin E. Griffith

Introduction: Connect the Dots

There is a growing public awareness that online computer system vulnerabilities in the public and private sector can conceivably lead to a cyber Pearl Harbor attack. As the number and extent of cyberincidents continue to grow at a geometric pace, and as our elected leaders tell us they are focused like a laser on The Next Big Attack, there are still many of us who measure life in terms of pre- and post-9/11. And collectively we have an uneasy feeling that our government may be failing to connect the dots, again.

We are living in the information age where almost every part of our daily lives is in some way inextricably interwoven with the Internet. The problem is that those very networks on which we rely to enable and facilitate many critically important aspects of our increasingly digital lives, governments and systems of commercial activity are vulnerable to cyberattack. Not a day passes when malicious cyber criminals, hacktivists and other highly motivated but misdirected actors are launching attacks that originate beyond our national borders. They are targeting

our businesses, commercial and proprietary trade secrets, critical infrastructure, and sensitive information. The toughest challenges lie in developing effective tools that will enable our national, state and local governments to respond in an appropriate, proportionate and effective manner to malicious cyber attacks and cyber-enabled activities, and to provide a credible deterrence that will make others refrain from engaging in similar activities. Some countries have already begun efforts to confront these growing threats by malicious cyber attackers and cyber actors, but this is a problem that must be predicated on international coordination and development of capabilities beyond those presently existing.

Interrelated Cybersecurity Issues

In this presentation we will explore six interrelated cybersecurity issues that have a direct impact upon local government and the citizens it represents.

1. Vulnerability to attacks
2. Why hackers exploit local government websites and networks
3. Greatest vulnerabilities and need for protection
4. Best cybersecurity practices
5. Hacking vulnerabilities of vehicles and mandatory security standards
6. Feasible means of preventing local governments from becoming gateways to federal and state hacking

Scope of the Problem

Through efforts by government and the private sector in the early 1970s, various forms of cybersecurity were implemented in response to the hacking of telephone systems later expanded to computer systems. One analyst reported in an October 16, 2015 article that the U.S. government had spent over $100 billion on cybersecurity over the past decade and had budgeted $14 billion for cybersecurity in 2016. With cyber-attacks costing businesses $400 to $500 billion a year, these figures to not take into account the thousands of cyberattacks that go unreported because they are small, undetected or do not include the explosive growth in mobile use and the internet. Steve Morgan, *The Business of Cybersecurity: 2016 Market Size, Cyber Crime, Employment, and Industry Statistics*, Forbes, October 16, 2015.

Advances in Technological Innovation vs. New Opportunities for Exploitation

Some have projected that by 2020, the worldwide cost will approach trillions of dollars. This is a game in which cybersecurity will continue to play catchup, with no real prospect of gaining the upper hand over cybercrime for the next two to three decades. As we witness advances in the relentless march of technological

innovation, each step forward is matched by a giant step backward as new opportunities surface for exploitation. *The Changing Face of Cybersecurity & What it Means for Municipalities*, Morris A. Enyeart, Ed.D. Jan. 2016.

A Quick Look at the Numbers

As of 2013, the number of cyberintrusions by various actors was running at a gallop:

BP claimed to have suffered 50,000 attempted cyberintrusions per day.

The Pentagon reported 10 million attempts a day.

The U.S. Energy Department's National Nuclear Security Administration recorded 10 million hacks a day.

The United Kingdom reported 120,000 cyberincidents per day.

The State of Utah claims to have 20 million attempts per day, up from 1 million per day two years before.

Brian Fung, *How Many Cyberattacks Hit the United States Last Year?* National Journal, March 8, 2013.

Stuxnet

When the Stuxnet virus was first reported, its mission had already been accomplished. It is believed that the Stuxnet virus was first introduced into Iranian nuclear facilities by a human intelligence agent seeding those facilities with Stuxnet-infected USB drives that were picked up by engineers and used with their personal laptop computers. The Stuxnet laptops were used to update software that was in turn used in the computerized controllers that directed the centrifuges. Once the laptops were plugged into maintenance ports, they infected the hosts, and the delivery was complete. Stuxnet ran successfully, and the Iranian nuclear program was set back several years. See Chris Inskeep, Managing Attack Vectors to Disrupt Cyber-Attack Delivery (Advances Protection Strategies)('Managing Attack Vectors').

The level of sophistication in cyber attacks and the methodologies behind them has grown significantly since the delivery of the Stuxnet virus gave other state-sponsored actors the incentive to orchestrate multi-stage attacks, spear phishing, DDS (distributed denial of service), encrypted malware, stub-viruses, masquerading through keystroke logging malware and replay of stolen logon credentials. New and

emerging threats are coming from the Stuxnet Family viruses. Managing Attack Vectors.

Spearphishing

One form of direct social engineering attack is spearphishing, delivered by e-mail and designed to exploit human vulnerabilities. Spearphishing exploits a weakness in the e-mail system technology: the sender address is assumed to be correct, hence the addressee routinely opens e-mails that purport to have originated with collegues, business associates, acquaintances and friends. It the attackers can spoof a credible sender's address information, the recipient will be more likely to open the message. The attack delivery would be disrupted and the attack would fail if spurious e-mails were not delivered by the e-mail system, as when the e-mail recipient has an easily available means to verify the origin of the message. Spearphishing is enabled when the recipient is unable to easily verify the message origin or guarantee of origin, and its success reveals serious shortcomings of current e-mail technology. Managing Attack Vectors.

Disruption of Attack Delivery

Many multi-stage cyber attacks begin with spearphishing that uses e-mail as the attack vector, with credible messages that the victim will likely open and respond to positively. Message credibility is a critical factor in such an attack. If the recipient of the message is aware that the message was not from a guaranteed origin, that is, not from whom it purported to be from, message credibility can become a significant hurdle for the attacker.

Multi-Stage Attacks by State-Sponsored Actors

During 2011-12, Coca-Cola Corporation was attacked with what began as a spear phishing targeting of a senior corporate executive with a malicious e-mail purporting to be from the CEO. Contained in the e-mail message was a link to a malicious website that performed a drive by download of keystroke logging malware. The goal of this attack was the theft of data relating to Coca Cola's acquisition of another company, but the attack may have had grander designs. The corporate network was accessed when malware compromised the logon credentials and enabled unauthorized but unrestricted access to the corporate resources on the network. The attackers used stub viruses, a new strain of malware that could be remotely updated with new capabilities. The attack was commenced and the theft of sensitive data was undetected for a lengthy period of time. Managing Attack Vectors.

.

Aramco attack

The Saudi-owned Aramco was subjected to a viral attack in 2012 that killed up to 30,000 desktop computers. The hackers were rumored to be working with or paying off an Aramco insider who was sympathetic to Iran and who helped plant the virus in the Aramco network. The virus was designed to destroy computer hard drives and did so effectively. Aramco was disrupted while the virus was being contained and the network was being disinfected. Managing Attack Vectors.

Zeus Virus and Masquerading

Conventional wisdom tells us that viruses spread through propagation and can be detected by behavior malware detection software. When a virus does not exhibit expected behavior, according to this conventional wisdom, the effectiveness of anti-malware protection controls can be seriously challenged. This brings us to the field of malicious software of a particularly problematic type: The Zeus Trojan Horse Virus.

Stealing Confidential Information from Compromised Systems

The Zeus virus is a keystroke logging software delivered by drive by download, through a Zeus Trojan. It runs on versions of Microsoft Windows and steals information by man-in-the-browser keystroke logging and form grabbing. Zeus is designed to steal confidential information from the computer systems it has compromised and does so by specifically targeting system information, online login credentials and banking information. It has also been used to install the CryptoLocker ransomware and is spread through drive-by-downloads and phishing schemes. The Zeus Trojan can be customized to gather social security and credit card numbers.

Wide Array of Targets In and Outside Government

It was initially identified in July 2007 when it was used to steal information from the U.S. Department of Transportation. By June 2009, it was discovered that over 74,000 FTP accounts on websites at the Bank of America, NASA, Monster.com, ABC, Oracle, Cisco, Amazon and BusinessWeek had been compromised.

Inability to Remove All Versions from Operating Systems

While there are many forms and versions of the Zeus Trojan, it appears that no utility can effectively detect and remove all versions of it from all operating systems. Some estimates indicate that as of 2009, Zeus had infected 3.6 million personal computers in the United States, and security firms proactively advised businesses to continue to offer training to users to implement such practices as not clicking on hostile or suspicious links in e-mails or websites and to keep their

antivirus software current. While some vendors represent that their software protection can prevent some infection attempts, none claim the ability to reliably prevent infection under all circumstances. See *Removing the Zeus Malware Virus*, Cox Tech Solutions, January 21, 2016, at http://www.cox.com/residential/support/internet/article.cox?articleId=9e960f50-c2ae-11e4-52f6-000000000000; Zeus (Malware), at https://en.wikipedia.org/wiki/Zeus_(malware)

Replay Masquerades

Logging user IDs and passwords is performed so the credentials can be used later to gain access to otherwise inaccessible systems. Reusing stolen logon credentials is known as "replay", and the attacker who uses replay "masquerades" as the legitimate owner of the replayed credentials. The highest level of masquerading is compromise and replay of the logon credentials of privileged users, since it opens up the resources of corporate information systems and networks to compromise.

Protection Methodology

The protection methodology against this is two-fold: first, disrupt the implanting of keystroke logging malware, just as one would disrupt drive by downloads and detect malware before it could be implanted. Second, design a one-time credential that cannot be replayed. Options for preventing replay are one-time passwords and adding a second factor to the authentication credential such as a one-time value like the one provided by the RSA SecureID device.

Cat and Mouse

Response to a cyber attack can depend largely the ability, talents and knowledge the attacker has about the human factors and human vulnerabilities of the target. Attack response can become a game of cat and mouse as defensive strategies are rolled out as quickly as attackers modify their attack strategy.

Attack Vectors

A successful cyberattack requires an attack delivery as an essential step. If the cyberattack cannot be delivered, the attack fails, and the danger to the target is averted. The path that a cyber attacker uses to deliver an attack is an attack vector.

Attack vectors are poorly understood and seldom addressed. That may be changing, since the conventional method of attacking was almost always through the wired network, but more and more attention is being given to disruption of attempts at attack delivery. To put it another way, protection from and prevention of attacks

can and should include detecting the attack vector that a cyber attacker plans to use and preventing the attack from being delivered. Managing Attack Vectors.

The Cybersecurity Information Sharing Act (CISA)

The Cybersecurity Information Sharing Act (CISA) was quietly inserted into the $1.1 trillion December 18, 2015 Omnibus Budget Bill that was passed by the United States Senate and signed by the President. CISA was seen by its opponents as a seriously flawed governmental surveillance bill while CISA's proponents said it was a necessary tool to fight cybercrime, their rationale being that the tools and strategies successfully used against a private sector business would also be used against the government and other companies. CISA includes sections about Internet monitoring that modify the Internet surveillance laws, and it broadens the powers of network operators to conduct surveillance for cybersecurity purposes. In so doing, CISA dramatically expands those powers in significant ways, the extent of which is still unknown. See S.754 – Cybersecurity Information Sharing Act of 2015. Congress.gov, https://www.congress.gov/bill/114th- congress/senate-bill/754; Larry Greenemeier, *A Quick Guide to the Senate's Newly Passed Cybersecurity Bill*, Scientific American, October 28, 2015.

Immunity From Consumer Lawsuits

One of CISA's key features is that it enables private entities, non-federal government agencies, state, tribal and local governments who have been victims of cyber threats to share information with any federal entity and with each other. Companies who do share information with federal entities are immune from consumer lawsuits for sharing the data.

Some have expressed concern that such sharing of consumer information to government agencies by private entities or other third parties will create new targets for hackers. Shortly before CISA was voting on by the Senate, the requirement to remove or redact any personal information from data that is shared was deleted, and some critics say this will result in further spreading of personal information. Sharing of information under CISA is voluntary, so one cannot tell how effective or widespread the data sharing program will be when it is fully implemented.

Governmental Cybersecurity Clearing Houses at Federal and State Level

The new clearing house created by CISA focuses on cyber threats. In addition, there are additional clearing houses at the federal and state level that include cyber incidents where hackers have gained access and control of private entity and governmental systems.

Cybersecurity Measures at the State and Local Government Level Level

On May 20, 2015, Governor Chris Christie signed an Executive Order that set up New Jersey's New Jersey Cybersecurity and Communications Integration Cell (NJCCIC) as the State organization responsible for cybersecurity information sharing, cyber threat analysis and hacker incident reporting.

New Jersey League of Municipalities Cybersecurity Awareness Efforts

The New Jersey League of Municipalities is bringing awareness to the municipal level through its Issue Alerts, seminars, webinars, sample proclamations for municipalities and Annual Conference education sessions. See New Jersey State League of Municipalities. www.njslom.org Search cyber security.

Awareness at the Municipal Level

On September 29, 2015, the NJLM alerted it 565 member municipalities about recent attempts to defraud New Jersey municipalities using false emails from the Administrator to the CFO to request wire transfers. These efforts raised awareness about cybersecurity issues and specifically awareness at the municipal level. Marc Pfeiffer, *Keeping your Humans Secure*, November 19, 2014 www.njslom.org/99thconf/conf-presentations/Secured- Humans.pdf ; Minimum Cyber-Security Requirements: What you need to Know, March 7, 2014 www.njslom.org/presentations/League- Webinar-Minimum-Technology-Security-Requirements.pdf ; Managing Technology Risks Through Technological Proficiency, November 2015 http://blousteinlocal.rutgers.edu/wp-content/uploads/2015/11/BLGRC-managing-technology-risk.pdf

Education and Outreach at N.J. Local Government Level

On April 7, 2016, GMIS New Jersey held its 7th Annual Technology Conference in Somerset, N.J. GMIS is an association of New Jersey municipal, Board of Education, county and state governmental members that deal with technology hardware, software and system issues affecting New Jersey governmental entities. Included in the conference will be a review of technology advances and investigation of problems and recommended solutions including cyber threats. Id.

Franklin Township's Fight Against Cyber Threats

Franklin Township in Somerset County, New Jersey is taking the fight against cyber threats a step further by using its website to provide information, videos and hints to raise cybersecurity awareness for residents. This effort is a reflection of the level of electronic interaction that many municipalities have with the public, and it is a feasible means of arming residents with critical cybersecurity information that will make those citizens partners in the fight against cybercrime, while reducing the

risk of accidental malware, phishing and other intrusions. See Cybersecurity resources for Residents. Franklin Township, Somerset, NJ

Japan's Efforts To Prepare Cyberattack Countermeasures

The 2012 London Olympics official website was attacked about 200 million times, and Japan is bracing for even more cyberattacks in 2010. Its concerns are well-founded. In May 2015, the Japan Pension Service, which operates Japan's public pension program, was hit by cyberattacks that led to the leakage of 1.25 million people's personal data.

As Japan's government plans for the 2020 Tokyo Olympics, it is increasing the number and scale of exercises designed to counter cyberattacks. The drills are to be held six times a year and will involve ministry and agency officials, increasing to 10 and then expanded to include local governments trailing in cybersecurity measures. See *Japan to boost drills to counter cyberattacks ahead of 2020 Olympics*, KYODO, JAN 2, 2016.

Japan's central government believes prefectural and municipal governments lack experience in the cybersecurity field and plans to give higher priority to training municipal officials in remote areas, since they cannot rely on specialists in urban areas if their computer systems are attacked. This means that for Tokyo Olympic organizing committee officials, Japan's central government will run drills involving simulated attacks on the ticket sales system of a mock official website, and by having local government officials in charge of computer systems and others join the drills, the number of participants is expected to increase to 2,000 from the present 300 now. Japan will also send officials to Rio de Janeiro, which will host the 2016 Games, to collect cybersecurity information and will seek to bolster security after the May 2015 series of electronic breaches.

Municipal Targets of Cyber Threats

Police and court systems, financial systems, personnel records, payment systems for municipal water and electrical plants are common municipal targets.

As ballot machines become more and more digitally and electronically cyberconnected, they too will become targets for cyber threats.

Recreation registration information can also be valuable targets for hackers to sell.

DDoS: Distributed Denial of Service

DDoS is a form of brute force attack in which the attacker buys access to a botnet system that directs thousands or even millions of computers to access the network, email system or website.

It has been estimated that in 2015 one-third of website outages resulted from DDoS attacks, the result of which was that networks were overwhelmed, shut down, and normal traffic could not get through. This left municipal residents without electronic services to pay taxes and utilities online, interrupted 911 and emergency dispatch functions, and delayed communications with and essential functions of health departments, payroll departments, online facilities for payment of bills, for hours up to several days. Systems that crash due to DDoS attacks may in turn have data corruption problems and require expensive re-building in order to come back online.

Purchase of DDoS Service on the Dark Web

Why would a municipality be subjected to a DDoS attack? This might originate with criminal activity by gangs, political protests, revenge, or disgruntled employees. The cyber attacker need not have sophisticated technical skills to initiate a DDoS attack, but only needs to purchase the service on the dark web.

A few examples illustrate the range of this kind of attack.

►The Maine.gov website was disabled by DDoS attacks three times in March 2015 along with the Bangor, Maine municipal website and other websites. Craig Anderson, *More Maine websites targeted on third day of cyberattacks*, Portland Press Herald, March 25, 2015, www.centralmaine.com/2015/03/25/cyber-attacks-targets-maine-websites-for-a-third-day/

►As a result of a DDoS attack in November 2015, the San Jose Police Department was offline for several days.

►Departments at Rutgers University were shut down by DDoS attacks in 2015. Kelly Heyboer, *Cyber attack shuts down Rutgers online classroom site*, NJ Advance for NJ.com. December 25, 2015 www.nj.com/middlesex/index.ssf/2015/12/ho_ho_hack_rutgers_u_hit_with_another_cyber_attack.html

Approaches to Prevent DDoS Attacks

DDoS attacks are designed to deny electronic access and functioning to a municipality. They shut down the city's doors so no information can get in or out for a prolonged period. While they are not the most damaging of cyber threat to municipalities, they are disruptive and can cost valuable taxpayer dollars in times of limited local resources.

Several approaches have been used by cybersecurity vendors in an effort to prevent DDoS attacks on municipal governments, but these are not the only form of attack.

1. Cybersecurity firms can build a firewall that analyzes incoming traffic in real time and blocks incoming traffic when certain characteristics trigger a response. Hosting and network vendors offer cloud and hardware devices that range from $500/month for three million packets per second to $2,500 per month for twelve million packets per second that would protect most municipalities. Larger cities may need the services of companies like Akamai, IBM, Microsoft and Amazon that can run into the hundreds of thousands or millions of dollars depending on the level of DDoS protection needed.
2. Policies, procedures and controlled access methods can be developed and implemented to minimize the risk of such everyday cyber threats as
   (a) Exposure of municipal networks and websites by which hackers gain access to the municipal network, utility systems, or website, and the intrusion cyber threat seeks to gain internal control in order to steal personal/financial information or disrupt the operation while doing maximum damage.
   (b) Theft of personal and financial information on the Internet, through which the hacker's breach may force the municipality to spend hundreds of thousands of dollars to rebuild and harden the network against future intrusions while limiting services to residents, and then hope the system will withstand the next attempted intrusion.
   (c) Despite constant attention to alerts and periodic tests, and even if the municipality's network and systems are hardened and up to date, there will be upgrades and patches to apply constantly over time, and another Trojan or malware could be accidently introduced through a trusted vendor patch, an employee's flash drive or similar network appliance, or human error as when an employee opens an e-mail and clicks on a link or opens an attached file that releases a virus, malware or a Trojan into the network as it is downloaded to the computer attached to the network, or when an employee accesses a non-municipal system that risks introducing viruses, ransomware, or Trojans into the municipal network as he or she checks social media, personal e-mail or conduct personal business using the municipal work station.

Notwithstanding this daunting cat-and-mouse game, there are practices and measures through which municipalities can help ensure the security of their network and systems are secure.

(a) Financial systems and personnel data should be encrypted.
(b) Administrative functions can be tightly controlled.
(c) Strong system passwords can be changed every thirty to sixty days, using password manager software for staff to enter passwords to systems or access the network.

(d) Access via persons using TOR as their website browser should also be blocked since it is a favorite tool used by hackers to hide their origin while hacking a network.
(e) A full time cybersecurity officer may be hired by the largest municipalities, although this is not feasible for most municipalities due to cost. Further, cybersecurity staff are in short supplyvand are paid more than most municipalities can afford.
(f) Municipalities can consider using a shared-service agreement to hire a cybersecurity resource to be shared across multiple municipalities. This resource could create common policies, monitor their implementation, conduct training, work with individual departments where needed and bring best practices to the municipalities at a level they can afford.
(g) Municipalities can establish a comprehensive cybersecurity policy that is reviewed twice a year with staff to ensure they understand all of its elements, including holding separate meetings where policy elements apply only to a single department, and creating a video with a form quiz where the policy applies to volunteers and elected/appointed officials, providing them with a good overview of their responsibilities and restrictions. See Cybersecurity for Municipalities, Colorado Municipal League June 2015 Annual Conference.

Grass Roots Approach to Cyber Security

Cyber-attacks affect more and more organizations in both the public sector and the private sector. While interconnectedness through the internet, the cloud, mobile devices and social media has increased productivity and commerce, these trends also are making businesses, governments and individuals more vulnerable to cyber-attack. The federal government and large corporations constantly seek news ways to fortify their enterprises against attack. However, what is overlooked in cyber-security planning and responses are local governments and small businesses. A "grass-roots" approach to cyber-security is required to compliment the efforts of large enterprises and governments.

Recognizing the Problem

The first step in this grass-roots approach is the recognition of the importance of cyber-security by local leaders to include mayors and town councils, chambers of commerce, school boards and civic groups. Such leadership has the ability to raise awareness of cyber-security among their respective constituencies. They can direct the attention of citizens to the importance of cyber-security. Leaders should use their respective forums to discuss cyber-security at given opportunities.

Coordinated Governance

The next step is for local governments to develop cyber-security committees to bring together stakeholders for the following purpose:

- Raise awareness among citizens;
- Improve cyber-security posture of local government institutions;
- Share best practices with local businesses and organizations;
- Develop a cyber-security curriculum for local schools;
- Coordinate law enforcement response options to reported cyber-crimes.

This cyber-security governance committee would develop, implement and monitor plans to meet these objectives.

Engaging Stakeholders

To meet these objectives, the committee should consist of at a minimum the following individuals:

- Cyber-Security Expert: Municipalities can recruit a volunteer through their local ISACA chapter (www.isaca.org). Service on such a board can count as continuing education credits to maintain good standing as a Certified Information Systems Auditor (CISA).
- Head Law Enforcement Official: This individual will be able to assist in creating mechanisms for reporting cyber-crime.
- Member of Council: This individual assures that planning aligns with local strategic vision and facilitates the approval of resolutions to support the effort.
- Municipal Information Technology Professional: This individual's knowledge of systems, data and access levels are necessary for risk assessments, implementation and monitoring.
- Municipal Manager or Administrator: This individual brings strong knowledge of functional processes in the local government that aid with both risk assessments and implementation and monitoring.
- School Board Representative: This individual assists with improving the school district's cyber-security posture and provides insight into developing a cyber-security curriculum.
- Government Sub-unit Representative(s): These are individuals representing any independent or quasi-independent agencies that have separate information technology systems. Industrial automation in utilities is a focus of these individuals.
- Educational Institutional Representative(s): These individuals represent colleges or community colleges in the municipality to assist with awareness and educational development.
- Business and Labor Representative(s): These individuals represent business groups and labor organizations in the municipality. These individuals can assist with awareness and dissemination of best practices.

Protection of Citizens from Cyberattacks

Ultimately, all governments have a duty to protect its citizens. Cyber-attacks represent a new threat from which citizens require protection. As with any other type of crime, any decrease in cyber-attacks represents an increase in quality of life and a boost to economic development.

Post-Ferguson DDoS Attack

Following the fatal shooting of Michael Brown by a Ferguson, MO police officer on August 9, 2014, the City of Ferguson found itself at the epicenter of worldwide attention, including that of hackers with a sociopolitical agenda. In an excellent article by Colin Wood entitled *Unmasking Hacktivism and Other High-Profile Cyberattacks,* Government Technology, August 28, 2015, accessible at http://www.govtech.com/public-safety/Unmasking-Hacktivism.html

According to Wood, the hactivists at Anonymous engaged in a "shotgun approach to retribution" by mounting a vigilante assault that began with the online release of the home address, phone number and photo of the house of the St. Louis County Police Chief, shortly after which photos of the Chief's daughter and wife began circulating on Twitter. This was only the beginning of their furor as Anonymous expressed its indignation over what its minions perceived as a violation of its moral code. Its online efforts led to others making veiled threats against the safety of the Chief and his family. Anonymous launched DDoS attacks, SQL injection attacks and a phishing campaign against the Missouri state government's digital infrastructure and that of law enforcement agencies and regional governments not directly related to Michael Brown's death. The collateral damage to those targeted by this cyber attack was extensive, and the State of Missouri was not fully prepared.

Similar cyber attacks had been launched by Anonymous as far back as 2008, when it "cut[] its havtivist teeth" in online attacks against Sony, PayPal, Visa, MasterCard, the Motion Picture Association of America, ISIS, Koch Industries, the Westboro Baptist Church, the New York Stock Exchange, and the federal governments of the U.S., Australia, Uganda, Israel, Canada, Tunisia and Egypt. Each target has somehow been selected by Anonymous based on a perceived transgression of its sense of moral propriety.

According to the chief information security officer for the state of Missouri, as Wood explained, the state had not completely implemented its security plan at the time the cyber attacks took place, although overall the state did a good job minimizing their impact. There were several things the state would have done differently when it was subjected to the three forms of attacks in the middle of the night on a weekend. These consisted of DDoS attacks that disabled websites, SQL injections

that infiltrated databases and a phishing campaign that sought to obtain security credentials. Some of the large DDoS partners were hard to reach, and some of the state's vendors wanted an emergency setup fee of $20,000 to $40,000. While the cyber attacks actually helped improve the state's security posture, the state has now contracted with several new vendors to manage security operations, uses a managed DNS provider, and has in place border gateway protocol and application-layer protection to mitigate DDoS attacks.

According to Woods,

> Groups like Anonymous attack their enemies to prove a point. They want to show the government, or whomever, that evil deeds don't go unpunished. It's out of a perceived lack of legitimate recourse that hacktivists disable websites and make personal threats, but of the 10,000 arrows fired, many land on innocent villagers. Roling didn't shoot anyone, but he and the rest of the state's IT team are the ones left picking up the pieces. The more time and money the state spends on its cybersecurity, the less taxpayer funding there is left for citizen services. The people Anonymous wants to advocate for are the same ones footing the $40,000 emergency setup fees and new vendor contracts. Anonymous might mean well, but pestering the state won't stop the next race riot. It's just another thing that poorly funded state and local governments must worry about.

The post-Ferguson cyber attacks on the State of Missouri demonstrate graphically that governments do not have the option of doing nothing, unless they relish the idea of getting pounded repeatedly as "easy, soft targets" and allow citizens' trust in their government to be sacrificed on the alter of cost-control.

Understanding Hactivists' Motivation, Means and Opportunity

There are ways to prepare for hactivist attacks like those spearheaded by grass-roots political movements like Anonymous, and they begin with an understanding of motivation, means and opportunity. As Wood notes,

> Preparing for hacktivism differs little from other forms of cyberdefense. Control frameworks like the one outlined by the National Institute of Standards and Technology are good road maps for governments, Brasso said. Even if organizations aren't ready to implement every piece of the framework, they can know where they stand compared to where they should be. Tools include things like firewalls, advanced malware protection, intrusion prevention tools, vulnerability assessment tools and education to prevent simple mistakes by employees.

Encrypted IPhones and the battle for encrypted data access

Encrypted handhelds, iPhones, cell phones and other products are being rolled out that will allow users alone to access their data. In the wake of the Charlie Hebdo attacks in Paris and the terrorist attacks in San Bernardino, California, the fears of law enforcement officials are being realized. In its pitched battle with Apple over access to encrypted data stored on the county-owned iPhone of one of the San Bernardino attackers, the FBI says its ability to uncover terrorism plots can be hindered by encrypted messaging apps like the one on this iPhone. In that battle, Apple claims a First Amendment right of privacy bars governmental access to the data, and the FBI says it needs immediate access to the contacts made by the terrorist before he himself was killed. See Adam Segal and Alex Grigsby, 3 ways to break the Apple-FBI encryption deadlock, The Washington Post, March 14, 2016, at http://www.syracuse.com/opinion/index.ssf/2016/03/3_ways_to_break_the_apple-fbi_encryption_deadlock_commentary.html

Device management feature lacking

According to a recent investigative report by the Washington Post, the iPhone in question did not have a device management feature that could have been purchased by the county that, if installed on the iPhone, would have given the FBI investigating team easy, immediate access to that data. See Adam Segal and Alex Grigsby, 3 ways to break the Apple-FBI encryption deadlock, The Washington Post, March 14, 2016, at http://www.syracuse.com/opinion/index.ssf/2016/03/3_ways_to_break_the_apple-fbi_encryption_deadlock_commentary.html

Going Dark

According to Segal and Grigsby, U.S. law enforcement has expressed concern over "going dark" since the 1990s, meaning its inability to access encrypted data, even when armed with a court order.

Encryption Backdoors

To prevent future terrorist attacks, tech giants like Apple are being urged to incorporate "backdoors" or "front doors" in their products that will assure the technical ability to decrypt communications pursuant to a warrant. Apple and other tech manufacturers claim that if someone other than the owner of the data is allowed to decrypt communications, such a flaw could be exploited by criminals and state actors, weakening security for everyone. There is a technological workaround,

however, through which the encrypted devices can be broken into, and the government is actively seeking to compel cooperation by the tech companies.

The choice need not come down to an absolutist immediate, on-demand decryption capability or caving in to business interests that favor going dark.
On the contrary, there are existing solutions that would enable law enforcement to gather the evidence it needs without creating encryption backdoors.

1. Congress can empower law enforcement to have the legal ability to hack into a terrorist suspect's handheld or computer with a court order, exploiting existing security flaws in communications software to access the data it needs. As Segal and Grigsby point out,

> It's no secret that software is riddled with security flaws. …[S]ome prominent computer security experts have argued such lawful hacking would allow authorities to use existing vulnerabilities to obtain evidence instead of creating new backdoors. Although this would entail law enforcement adopting the same techniques as criminals, tight judicial oversight would ensure that lawful hacking is employed responsibly, much like the restrictions that already apply to wiretapping. Adam Segal and Alex Grigsby, 3 ways to break the Apple-FBI encryption deadlock, The Washington Post, March 14, 2016, at http://www.syracuse.com/opinion/index.ssf/2016/03/3_ways_to_break_the_apple-fbi_encryption_deadlock_commentary.html

2. A national capacity to decrypt data for low enforcement purposes should be explored by the Executive Branch.

> The challenge of "going dark" affects state and local law enforcement the most: They are the least likely to have the resources and technical capabilities to decrypt data relevant to an investigation. Creating a national decryption capability, housed within the FBI and drawing upon the expertise of the National Security Agency, would provide assistance to state and local law enforcement, similar to what the FBI provides for fingerprint and biometric data. Adam Segal and Alex Grigsby, 3 ways to break the Apple-FBI encryption deadlock, The Washington Post, March 14, 2016, at http://www.syracuse.com/opinion/index.ssf/2016/03/3_ways_to_break_the_apple-fbi_encryption_deadlock_commentary.html

3. Law enforcement needs to ramp up its tech literacy. Just as law enforcement in the 1990s dealt with a problem similar to "going dark" when organized-crime suspects began using disposable phones that hampered wiretaps, it adapted its procedures, and arrests and prosecution of organized-crime suspects continued.

Alternative Avenues to Encryption: Cloud Backup

Encryption of data can occur on a device when data is transmitted and stored in the cloud, but this does not automatically mean the evidence trail will go cold. Encryption in one avenue does not necessarily mean other avenues will be encrypted. It an encrypted iPhone had been backed up to the Apple's cloud storage system known as the iCloud, Apple can still access the content of the encrypted iPhone if it has been backed up to iCloud.

As Segal and Grigsby note,

> Recognizing how and when encryption occurs, and the different security offerings of the more popular service providers, may help law enforcement access data. Better tech literacy might have avoided the current Apple-FBI fight. The FBI could have obtained more information from the San Bernardino attacker's iPhone if it had not hastily ordered the county to reset his iCloud password. Adam Segal and Alex Grigsby, 3 ways to break the Apple-FBI encryption deadlock, The Washington Post, March 14, 2016, at http://www.syracuse.com/opinion/index.ssf/2016/03/3_ways_to_break_the_apple-fbi_encryption_deadlock_commentary.html

While these proposals may not be fully acceptable to law enforcement or the tech sector, and while it is unlikely that a one-size-fits-all solution will be forthcoming, the time is rapidly approaching to consider and develop realistic solutions.

Albuquerque P.D. Going Dark

The City of Albuquerque, New Mexico, is considered a leader in open data and transparency. In August 2014, after members of the Albuquerque, N.M., Police Department fatally shot a mentally ill homeless man who had been camping in the wilderness, the Police Department's website went dark on the heels of cyber attacks from Anonymous. The attacks were seen by some police personnel as tests of how well the city had been maintaining its security program.

The cyber attacks brought down the APD's website for a few hours, but unlike Missouri, the city was able to mitigate the attacks by working with such groups as the Multi-State Information Sharing and Analysis Center (MS-ISAC) and the FBI. While it may be problematic to predict when the threat of hacktivism will surface, whether arising from a police officer's use of force or something that a group sees as social injustice, there are still practical considerations for maintaining a robust social media presence, and promoting city information, but the trick is to "be smart

about what's being publicized." In light of emerging technologies like police body cams, moreover, amidst growing public demands for open data and transparency, the line between good practice and threat to the public servant can become a thin one. "[I]n the online world, everything that has a good motive also can be exploited."

Essential Preparation and Planning

According to the digital services coordinator for Evanston, Ill., one of the best things governments can do when it comes to any disaster is to prepare and plan ahead.

> Make sure you have a robust social media presence up and running, because a lot of these government agencies are slow to adopt and waiting until after that natural disaster hits to start a Twitter account, [but] it's too late….You want to build up those relationships ahead of time."

Basic measures local governments can take

Among the basic measures local governments can take are getting verified status on Twitter and using two-factor authentication. According to an official with the FBI's Cyber Division, state and local governments should expect DDoS attacks and have a mitigation plan and vendor relationships in place. They should monitor how often their networks are being pinged so they can quickly recognize when an attack has begun. Once due diligence has been performed, the most realistic advice may be that offered by Robert Louis Stevenson, author of Treasure Island, who once wrote "Our business in life is not to succeed, but to continue to fail in good spirits."

Developing Nations' Reach for Cyberspying Capabilities

The norms of behavior by nation states in cyberspace like the Peoples Republic of China and the USA may set a lofty standard, but less technologically advanced countries may lack the skill or motivation to follow that lead. Instead, increasing literature indicates a mounting interest among these less sophisticated countries in acquiring cyber espionage capabilities. At a time when governments are trying to curb the volume of hostile activity occurring in cyberspace, the media have revealed instances of suspected U.S. global surveillance and China's rampant commercial cyber espionage. These and similar episodes that unfortunately resemble the old days of Mad Magazine's *Spy vs. Spy* cartoon, have given rise to serious discussions about how and in what manner to establish a baseline for accepted actions for governments to take in cyber space. China, Russia, and the United Nations Governmental Group of Experts on Information Security have developed proposals addressing these concerns.

Cyber Sanctions

Coupled with this trend for nation state cyber responsibility, the President of the United States in an April 1, 2015 Executive Order established "cyber sanctions" that granted authority to the U.S. Department of Treasury to sanction "individuals or entities" that pose a cyber threat to the "national security, foreign policy, or economic health or financial stability of the United States." This was the first sanctions program to allow the Obama administration to impose penalties on individuals overseas who engage in destructive cyber attacks or commercial espionage in cyberspace. *Executive order: Obama establishes sanctions program to combat cyberattacks,* The Washington Post, April 1, 2015, cyberspyinghttp://apps.washingtonpost.com/g/documents/world/executive-order-obama-establishes-sanctions-program-to-combat-cyberattacks-cyberspying/1502/

As the President put it when he signed this EO, "Starting today, we're giving notice to those who pose significant threats to our security or economy by damaging our critical infrastructure, disrupting or hijacking our computer networks, or stealing the trade secrets of American companies or the personal information of American citizens for profit." *Our latest took to combat cyberattacks,* https://www.whitehouse.gov/blog/2015/04/01/our-latest-tool-combat-cyber-attacks-what-you-need-know

The rationale underlying this executive order is that malicious cyber actors often rely on U.S. infrastructure to commit the acts described in the EO, and they often use U.S. financial institutions or partners to transfer their money. By sanctioning these actors, the U.S. can limit their access to the U.S. financial system and U.S. technology supply and infrastructure. Basically, sanctioning them can harm their ability to both commit these malicious acts and to profit from them.

In a landmark agreement in November 2015, governments of the 20 leading global economies – including China – pledged not to engage in cyber-enabled commercial espionage for profit.

FinFisher

FinFisher Gamma Group in Munich has developed and produced a sophisticated, user-friendly spyware that is sold exclusively to government agencies and police forces. It has risen in popularity with government agencies across the world, and over 32 countries – including our host country for this Congress - have been identified as users. FinFisher's software can remotely control any computer it infects, read and copy encrypted files, intercept Skype calls, log keystrokes, and activate webcams. The software has been touted as a way to "help government law

enforcement and intelligence agencies identify, locate and convict serious criminals."

In August 2015, a data breach placed FinFisher's business practices and clients under scrutiny. Stolen files and client information of 33 customers was placed on the web, and some of it suggested that FinFisher was being used for activities beyond tracking criminals. The other activities entailed spying on high-profile Bahraini activists. According to some reports, it was believed that dissidents, law firms, journalists and political opposition in Bahrain and from Ethiopia had been monitored through FinFisher.

Yet despite this progress, revelations exposed with the Gamma breach, as well as the one suffered by Italy's Hacking Team in July 2015, continue to demonstrate that states desire to acquire offensive cyber surveillance capabilities, even if they can't develop them indigenously. Some of the customers identified in data were notably states that are neither considered cyber powers, nor considered leading economies. Some of the governments identified in data taken from the breach include Bangladesh, Kenya, Macedonia, and Paraguay. In two of these cases, the intelligence agencies of the governments were linked to FinFisher products.

While these states may not use these capabilities in order to conduct cyber espionage, some of the governments exposed in the data breach are those that Reporters without Borders have identified as "Enemies of the Internet" for their penchant for censorship, information control, surveillance, and enforcing draconian legislation to curb free speech. National security is the reason many of these governments provide in ratcheting up authoritarian practices, particularly against online activities. Indeed, even France, which is typically associated with liberalism, has implemented strict laws fringing on human rights. In December 2013, the Military Programming Law empowered authorities to surveil phone and Internet communications without having to obtain legal permission. After the recent terrorist attacks in Paris, French law enforcement wants to add addendums to a proposed law that blocks the use of the TOR anonymity network, as well as forbids the provision of free Wi-Fi during states of emergency. To put it in context, China, one of the more aggressive state actors monitoring Internet activity, blocks TOR as well for its own security interests.

Cyberspace has been called "the great equalizer" because it is an environment that can be leveraged by smaller, less industrialized nations in order to compete with larger ones. The Snowden document leaks and rampant, unchecked cyber espionage have created an environment in which all governments—regardless of size—want a modern, relatively inexpensive capability indicative of their ability to keep pace with the times.

Despite the lead taken by larger governments to reach consensus on some unacceptable actions in cyberspace, Pandora's box may have reached an aperture too great to close. Whether these poorer nations use the tools they obtain for legitimate national security or law enforcement reasons, or to oppress and keep populations in check will largely rest on perception and interpretation.

What City Officials Need to Know About Cybersecurity

In the wake of highly publicized data breaches and cybersecurity attacks, city officials have begun looking at historically underfunded municipal cyber-defense programs. See Lea Deesing, What City Officials Need to Know About Cybersecurity, June 23, 2015, at http://www.govtech.com/opinion/What-City-Officials-Need-to-Know-About-Cybersecurity.html

Lea Deesing paints an all-too realistic scenario for a municipal government that has been subjected to a well-orchestrated cybersecurity attack. In her hypothetical scenario, the signs of a cyber attack are everywhere:
►city staff unable to log in to their computer network,
►fire and police departments forced to rely solely on radio communications rather than mobile data systems to receive and respond to incidents,
►city staff are limited to communicating through text using the phone numbers in their personal smartphones since the telephone and e-mail systems are down,
►no city employees receive their electronic paycheck via direct deposit the night before payday,
►counter staff do not know how to handle manual transactions and cannot log in to their systems,
►staff who attempt to call the IT department help desk do not even get a dial tone,
►massive lines begin to form in the planning, permitting and cashiering departments, and
►residents and business owners who need to conduct business with the city are getting frustrated.

And all of this has taken place on a Friday.

IT staff finally determine that many city servers have been compromised through a well-organized cybersecurity attack. Weeks later the IT Department discovers the cause of the chaos was a Trojan horse virus that had been transmitted via a city staff member's personal flash drive. Lea Deesing, What City Officials Need to Know About Cybersecurity, June 23, 2015, at http://www.govtech.com/opinion/What-City-Officials-Need-to-Know-About-Cybersecurity.html

Deesing notes that recent cybersecurity breaches in both the private and public sectors have captured the attention of local government agencies. Highly publicized data breaches and cybersecurity attacks raised awareness of these challenges, and

consequently many city officials are looking at historically underfunded municipal cyber-defense programs.

Cybersecurity Awareness Training

Cyber Hackers usually hit the easiest targets first, much like thieves operating in a neighborhood during the holidays. A common breach can occur after a user clicks on a link in a spam or phishing email, and whether such an attack is financially motivated, or an attempt to cause mayhem in the city, or an act of revenge by a terminated city employee, its must be confronted and effectively mitigated.

Cryptolocker

A well-designed trojan horse virus writing like Cryptolocker can generate for its writers millions of dollars in revenue by encrypting the target's data and holding it for ransom until the target pays a fee. According to one cybersecurity expert, top coding talent is being recruited to write these Trojan horse viruses that lie undetected until a future date and contain malicious code that can carry out a specific action when the hacker signals the software. The cyber hacker has the choice of trying to breach a $20,000 security device or convincing someone to insert an infected $5 thumb drive.

Cybersecurity Awareness Programs

Among the simplist ways to mitigate the risk of such cyberattacks is a good security awareness training program. Prevention of internal breaches can be much more effective through utilization of low cost end-user security awareness videos that are available through private-sector security organizations. These preparedness measures can be coupled with good awareness training, and a cybersecurity policy in place that deals with unknown media, suspicious calls or online messages that try to get staff to visit a website, e-mails with suspicious attachments.

End-User Education

It is no longer sufficient for local governments to continue to rely on anti-virus and firewall protections along while ignoring end-user education.

Security Audits, Penetration Tests and Monitoring

Additional security efforts can be implemented by local government in the form of security audits and penetration test. These measures entail getting paid ethical hackers to try to breach the local government's system, then report back their findings so the government officials can take pre-emptive action. There must be an understanding of the long-term cost of a data security breach, and that

understanding must reach the highest level of government management. The cost must be quantified not only in monetary terms but in terms of loss of citizens' and customers' trust. The cost for a full security audit cannot be understood out of context. Further, a decision must be made on whether an annual or biennial security audit is sufficient in the present and future cyber landscape. Attention should be given to such emerging trends as hiring 24/7 managed professional security service providers. These professional can operate from remote security operations centers with fully dedicated certified security teams. The teams watch the local government's network, inside and out, and can identify real time security threats and help develop preventive counter measures. It is not cheap, but its cost in relative terms may make it a bargain.

Security Information and Event Management (SIEM) Tools

Managed security service providers often use special Security Information and Event Management (SIEM) tools. These tools provide a dashboard view into security and server logs that the local government's IT staff likely does not have time or capability to monitor. The IT staff may view these security and server logs after an incident has already occurred, but usually not before.

Continuity of Operations Plan

In the scenario described by Lea Deesing in *What City Officials Need to Know About Cybersecurity*, June 23, 2015, at http://www.govtech.com/opinion/What-City-Officials-Need-to-Know-About-Cybersecurity.html, systems must be prioritized in advance through a continuity of operations plan.

Continuity of operations plans can be vetted through departmental meetings

> where questions are asked, such as, "What would happen if your computer system went down for two hours? A day? A week? A month?" It's surprising what occurs when you have these discussions with departmental staff. They may say, "I never thought it would be possible for systems to be down that long. If we simply take this extra step, in advance, we will be as prepared as possible when the systems fail." For example, a payroll team saves the last successfully run payroll in a PDF format and stores it in a secured location, along with blank check stock. On the day of a disaster, all checks are printed and signed, and required payroll adjustments are made after system recovery.

Questions for Local Government Leaders to Consider

Security measures and security efforts may already be underway in a local government's IT department, but consideration should be given to supporting and implementing the current cybersecurity efforts in a collaborative way. Steps should be taken to require that policies be written and be grounded upon executive sponsorship.

►Questions should be asked of the human resources department on whether it can help support a security awareness training program.
►Consideration should be given to support for new hardware, software or services.
►Given limitations on local government funding, an assessment should be performed at the executive management level regarding the amount of risk the local government is willing to mitigate or simply accept.
►In short, a backup and recovery plan should be a good as the government can afford, since a cyber attacker with the time and desire will gain access one way or another.

State of Cybersecurity in Local, State & Federal Government

In the Ponemon Institute's study of The State of Cybersecurity in Local, State and Federal Government sponsored by Hewlett Packard Enterprise, the report concluded that government is the target of cybercriminals and nation state attackers. See State of Cybersecurity in Local, State & Federal Government at http://www.ponemon.org/library/the-state-of-cybersecurity-in-local-state-and-federal-government

At both the local and state level as well as the federal level, a key challenge is the lack of skilled personnel. This is a major challenge at the state and local level. Lack of budgetary resources is a key issue. State and local governments may not be as involved as they should be in sharing of threat intelligence.

Top security threats for local government can fall in the category of failure to patch known vulnerabilities, negligent insiders and zero-day attacks. State and local governments are not prepared to deal with cybersecurity threats, and often their agencies have achieved a less than optimal level of maturity in their cybersecurity initiatives.

The federal government has also outpaced state and local governments in four areas

1. Ability to recover. Barely over one-fourth of state and local respondents have reported that their ability to recover from a cyber attack is very high.
2. Ability to prevent. Less than 20% of state and local government repondents rate their ability to prevent a cyber attack as very high.

3. Ability to quickly detect. Barely a third of state and local agencies are confident that they would be able to quickly detect a cyber attack.
4. Ability to contain. Under 40% of state and local respondents are very confident in their ability to contain a cyber attack.

Cybersecurity top IT concerns for local government
For the second consecutive year, cybersecurity ranks as the top technology priority for local government technology officials, according to a recent survey conducted by the Public Technology Institute.

The number of cyberattacks has increased at an alarming rate. Target, AT&T, Home Depot, JP Morgan Chase, and even the White House have been among the victims of data breaches just during the past year.

Anyone who has data that needs to be protected should expect to be the target for a cyberattack, according to Sandy Reeser, president of VC3, the Municipal Association's technology partner.

Cities large and small are utilizing tools such as mobile devices and remote access to improve their organizational efficiency and the cost effectiveness of the services they deliver. However, this also increases their security risks, Reeser explained. Because of this, cities and towns cannot afford to ignore that additional efforts are needed to protect the city's information from cyberattacks, he said.

The degree to which a city is affected by a cyberattack will depend upon their ability to protect sensitive information, Reeser said.

"For some, these attacks will take place, they will be defended successfully and perhaps no one in the city will even know they occurred," he said. "For others, however, their defense systems will be breached or bypassed, and they will fall victim to the attack and experience data destruction, data loss or a data breach."

Cyber liability deals with risks associated with the Internet and information technology infrastructure and activities. These risks are typically excluded from traditional commercial general liability policies. While coverage under cyber insurance policies may include first-party coverage against losses such as data destruction, extortion, theft, hacking and denial of service attacks, insurance coverage for such breaches generally is very limited. A breach with far reaching impacts could exceed the limits of available insurance coverage, according to Heather Ricard, director of the Association's Risk Management Services.

Cities need to have a strategy to deal with cyberattacks and to address cyber liability, Reeser said.

First, cities must make sure that they take reasonably prudent steps toward preventing data breaches, he said. This involves leveraging cost-effective tools and technology that will provide a reasonable degree of protection from cyberattacks, educating the city staff on how to behave

in a prudent manner regarding information security, and conducting regular reviews and security audits by an independent party to assess the effectiveness of the measures being taken.

Second, cities must have the tools and technology in place to detect if and when a data breach occurs. They also need to have mechanisms in place to determine the extent of the data breach should the city fall victim to an attack, Reeser continued.

Finally, the city should have an incident response plan that identifies the actions it will take in the event of a breach. Much of the plan will be centered on the type of data that may be at risk, the extent to which the city is responsible for notifications, and the method and manner in which these notifications will be delivered.

Employee education is a key component of cyber liability because, regardless of what other security measures you take, all of these can be bypassed through social engineering or employees who fall victim to things like phishing attacks, Reeser said.

It's important to educate staff on the common techniques used to gain information or to entice employees into clicking on links that will ultimately infect both their information and the entire network. Employees also need to receive training on the many types of social engineering tactics aimed at getting people to reveal information to outside parties who are trying to breach personal data.

"These types of attacks have become more and more sophisticated and so the more you can educate your staff, the better they will be positioned to recognize these attempts and the better everyone will be at protecting your data," Reeser explained.

Employees need to be aware of such scams, should never click on suspicious links in emails, and should never provide username and password information in email or over the phone, Ricard advised.

Additionally, IT professionals can be proactive by using assessment tools to determine if their systems are susceptible to a breach. Members of the SC Municipal Insurance and Risk Financing Fund have access to free tools through a partnership with NetDiligence, a cyber risk management firm. NetDilligence provides prebreach services and education through an online tool called eRisk Hub.

Thus far, the Risk Management Services has only had two cyber liability claims. One involved an employee clicking on a pop-up ad from the Internet. This launched a virus that triggered a breach, according to Ricard.

Incident response and forensics are critical in cyber liability cases, Ricard said. Cities don't want to inadvertently say something to the local media or residents without first understanding the potential liability ramifications. While a breach can occur, it doesn't necessarily mean that it has compromised critical data. Cities should consult with an attorney who specializes in breach responses to formulate a response, she said.

Additionally, cities should notify local law enforcement, the SC Law Enforcement Division and even the FBI when a breach occurs. Forensic specialists can identify the source of the breach and help stop it from reoccurring, Ricard said.

Cities must follow more than just South Carolina's breach notification laws. If the breach impacted individuals outside the state, municipal officials must also adhere to notification laws of all the states involved. Also, penalties may be applicable for each incident, so in addition to the forensics and notification costs, there could be additional costs, she said.

Advanced Cyberthreats in State and Local Governments 2014

Section 1: Executive Overview

In the past, scattershot, broad-based attacks were often more about causing mischief than stealing confidential or financial data. But today, the landscape has changed. Threats are targeted, malicious, persistent and are designed to acquire valuable information. They have the potential to cause millions of dollars worth of damage due to compromised records.

The South Carolina and Utah examples have become legendary — a sort of ghost story CIOs tell each other and hope they never experience personally. South Carolina's incident — a Department of Revenue breach which compromised the data of 6.4 million individuals and businesses — was one of the largest breaches in history. It has already cost the state over $25 million, with lawsuits continuing to unfold. In Utah, a highly respected CTO paid the price — losing his job after cyber criminals pilfered the personal information of over 750,000 Medicaid recipients.

South Carolina and Utah — largely due to the sheer scope of the incidents — have unfortunately become the poster children for cyber crime. But the frightening reality is that, as the saying goes, "It could have happened to anyone." The Washington State Administrative Office of the Courts experienced a breach that may have compromised the Social Security numbers of 160,000 individuals in May 2013. In January 2012, nearly 100,000 students and employees at the City College of San Francisco had their personal information shipped overseas due to malware lurking in the college's computer networks. Also in 2012, the group Anonymous hacked the city of Springfield, Mo. website, obtaining the information of over 2,000 citizens.

Long story short — the threats to government entities are so pervasive and sophisticated that anyone can fall victim, particularly as government agencies are strapped for resources. While the above provides information concerning anecdotal examples, statistical data shows an even more startling scenario of the cyber threats with which state and local governments must contend. Consider:

- The total number of records containing sensitive personal information involved in security breaches in the
United States was over 608 million records among 3,763 data breaches since January 2005.1
- Malicious attacks (defined as a combination of hacking and insider theft) accounted for nearly 47 percent of
the recorded breaches in 2012 in the United States. Hacking attacks were responsible for more than one-
third (33.8 percent) of the data breaches recorded.2
- Government agencies have lost more than 94 million records of citizens since 2009.3
- The average cost per lost or breached record is $194.4

Security was also recently ranked No.1 in NASCIO's annual Top 10 priorities list for CIOs. NASCIO President and Mississippi CIO Craig Orgeron said of the ranking: "It is significant that security has now risen to

the No. 1 priority on our top 10 list. As I presented in congressional testimony before the Committee on Homeland Security last week, cyber attacks against state governments are growing in number and becoming increasingly sophisticated. Security has to be the top priority for all sectors. Clearly, from our top 10 voting results, the state CIOs agree on this."

A recent Center for Digital Government (CDG) survey underwritten by FireEye set out to identify government leaders' understanding of the threats they face, their strategies for combating them and their plans for the future. The survey queried 126 IT and security management individuals in state and local government. The results are interesting — and sometimes surprising.

Overall it appeared leaders may be underestimating the threats they face. Fifty percent of respondents did not think their organizations were being directly targeted by advanced cyber threats. However, when asked if they felt their currently deployed, signature-based anti-malware solutions were effective in blocking advanced and unknown zero-day threats, 56 percent said no or that they did not know. Additionally, while many organizations had cyber security tools in place, many of these tools have proven ineffective when it comes to advanced malware.

This CDG report will further detail respondents' perceptions around cyber threats and their level of preparedness to combat them.

Strapped for resources,

state and local governments are a prime target for the pervasive and sophisticated threats launched by stealthy cyber criminals. These attacks are not just an epidemic, they are a pandemic. Unfortunately, no one is safe and diligent and proactive defense mechanisms are the only cure.

Survey results indicate that government leaders underestimate the cost associated with a cyber security breach. A combined 31 percent believed the financial repercussions of a breach would be $50,000 or less. As evidenced by the situations in South Carolina, Utah and others, this is a gross underestimate of the financial burden a government agency encounters when personally identifiable information (PII) is compromised. According to the Ponemon Institute, the average cost of a data breach is $194 per compromised record.5 For a breach to cost an organization $50,000 or less, it would mean only a small number (250 or less) of records were compromised. In 2011 the Ponemon Institute noted the average number of records lost in a private sector data breach was 28,349.6

What do you think the impact of a serious breach could be to your organization?

Less than $50,000
18%
$50,000
13%
$5 million
18%
$25 million
13%
Don't know
41%

When asked if they understood the difference between malware and advanced malware, 58 percent of respondents indicated they did. However, 50 percent did not feel their organization was being directly targeted by advanced cyber threats. What are the characteristics that separate advanced malware and conventional malware? Conventional malware is typically open (it does not actively hide), known and patchable, broad (attacking indiscriminately) and is a one-time intrusion. Advanced malware is stealthy (actively hiding or cloaking itself), unknown and zero day (exploiting a previously unknown vulnerability), targeted and persistent.

Section 4: The Current Landscape and Strategies for Combating Threats
The survey asked participants about the attacks they had experienced in the recent past, the risks that most concerned them, and the current strategies and technologies they have in place to prevent and respond to cyber threats.
Forty-five percent of respondents rated their organization's ability to detect and block advanced cyber attacks as good, but only 10 percent rated it as excellent. A rather alarming number of participants (39%) rated their ability to detect and block advanced cyber attacks as average, fair or even poor. Part of this could be the solutions most used by organizations to detect malware. Many of these legacy solutions are ineffective against APTs.

What do you feel are the biggest malware threats/risks to state and local government?
Advanced persistent threats
52%
Zero-day target attacks
48%
Bots/stealth bots
43%
Spyware
39%
Dynamic trojans
37%
Worms
30%
Other
6%
Over the past year, in your organization, is the number of cyber incidents associated with malware increasing, decreasing or staying the same?
Increasing Staying the same Don't know

Decreasing
17%
36%
40%
8%
0% 10% 20% 30% 40% 50% 60% 70% 80% 90% 100%

What type of security incident or network breach has your organization experienced in the last year?
Malicious code (virus or worm)
44%
Lost or stolen electronic device or media
37%
Spear phishing
37%
We have not experienced an incident
24%

Intrusion/hacktivism
17%
Insider attack, such as unauthorized access or identity theft
13%
Distributed denial of service
10%
Mobile security (BYOD)
10%
Unauthorized electronic monitoring (sniffers)
9%
Breach as a result of an advanced persistent threat
8%
Other
8%
External financial fraud
4%
Respondents were most concerned about email and Web-based attacks, and were most worried about cyber criminals gaining access to PII and confidential data as well as cyber attacks impacting the business continuity of their organization.

Section 5: Conclusion

The overall consensus is that cyber security is important — but, like everything else, it is competing for attention in an age of doing more with less, faster. While a high percentage of those surveyed are in large organizations that serve more than 500,000 constituents (31%), a high percentage of respondents also only had 1 to 3 employees dedicated to security (42%). There may be a misunderstanding as to the different types of malware, as well as a misconception about the likelihood of an APT against their agency. While 59 percent of respondents said they understood the difference between basic malware and advanced malware, most of the technologies being used by organizations — and certainly the most popular — are not effective against advanced malware. And while 50 percent of respondents don't believe they are a target, the stark truth is that nearly every organization and agency is at risk.

The overall takeaway from this survey is that today's advanced cyber threat is likely underestimated, and because of tight budgets and lack of resources, not as high of a priority as it should be in every government agency. There are doubts about the efficacy of solutions deployed and can be misunderstandings about the types of threats that are occurring and the solutions that are effective in combating them.

About FireEye

FireEye has invented a purpose-built, virtual machine-based security platform that provides real-time threat protection against the next generation of cyber attacks to enterprises and governments worldwide. By leveraging the FireEye platform, government agencies can transform reactive cyber operations to proactive cyber operations — protecting invaluable data while saving time and resources.

FireEye enables early and advanced malware visibility. Rather than spending time and resources investigating and remediating breaches after the fact, security professionals can focus on proactively detecting and blocking malware in real time. The longer malware resides in a system, the more damage it can do, and the more costly removal becomes. By detecting attacks quickly, FireEye can help reduce the cost of containing and eradicating malware.

Fine-grained correlation and intelligence also allow security teams to prioritize their response efforts. They can focus on the most critical cyber threats, such as online attacks launched by nation-states, and let automated processes deal with well-known crimeware. With accurate detection and near-zero false positives, FireEye enables security teams to respond quickly to the first indicator of compromise instead of spending hours investigating alert logs from multiple tools.

As the only cyber security solution on the market that can quickly detect, prevent and stop cyber attacks in real time, the FireEye product suite supplements traditional and next-generation firewalls, IPS, anti-virus and gateways, which cannot stop advanced threats. The FireEye suite applies this actionable threat intelligence on both the network and on endpoints and meets many third-party validation requirements for products used in government agencies, including Common Criteria and FIPS validation.

For more information on how the FireEye suite can transform security defenses for your organization, visit the FireEye website at http://www.fireeye.com. Please also download the Thinking Locally, Targeted Globally whitepaper at http://www2.fireeye.com/WP-SLED.html.

Endnotes

1. A Chronology of Data Breaches, Privacy Rights Clearinghouse, June 2013
2. Ibid.
3. Data Breaches in the Government Sector, Rapid7, 2012
4. Cost of Data Breach Study, Ponemon Institute, 2011
5. Ibid.
6. Ibid.

The HPE Cyber Risk Report 2016 provides a broad view of the 2015 threat landscape. It ranges from industry-wide data to a focused look at different technologies, including open source, mobile, and the Internet of Things. The report provides security information leading to a better understanding of the threat landscape, and resources that can aid in minimizing security risk. The report is available online at
https://ssl.www8.hp.com/ww/en/secure/pdf/4aa6-3786enw.pdf

HP gives this frank assessment of the cyber threat landscape in the beginning pages of the report: "In 2015, we saw a continued rise in attackers' success at infiltrating enterprise networks, making it all the more critical for HPE's cybersecurity research team to provide this unique perspective on significant trends in the marketplace. Just as attackers continue to evolve their techniques, defenders must accelerate their approach to detection, protection, response, and recovery. Our research saw an increased sophistication of attacks, even as the security world is encumbered by the same issues that have plagued us for years. The work done by our research team shows that even as regulations become more complex and attack surfaces continue to grow, foundational problems exist that challenge even the best defender. Our more sophisticated customers are responding to these threats, but many small and mid-market customers are not, thus making them an easier target. Security practitioners from enterprises of all sizes must embrace the rapid transformation of IT and ready themselves for both a new wave of regulations and an increased complexity in attacks."

Among the key themes addresses in the HPE Cyber Risk Report:

Theme #1: The year of collateral damage If 2014 was the Year of the Breach, 2015 was the Year of Collateral Damage as certain attacks touched people who never dreamed they might be involved in a security breach. Both the United States Office of Personnel Management (OPM) and the Ashley Madison breaches affected those who never had direct contact with either entity, and whose information resided in their networks only as it related to someone else—or, in the case of the Ashley Madison breach, did not appear at all but could be easily deduced from revealed data. With the OPM breach, the true targets of the breach may be people who never themselves consented to inclusion in the OPM database—and who may be in danger thanks to its compromise. Data compromise is no longer just about getting payment card information. It's about getting the information capable of changing someone's life forever.

Theme #4: Political pressures attempt to decouple privacy and security efforts A difficult and violent year on the global scene, combined with lingering distrust of American tech initiatives in the wake of revelations by Edward Snowden and other whistleblowers, led to a fraught year for data privacy, encryption, and surveillance worldwide. Many lawmakers in the US, UK, and elsewhere claimed that security was only possible if fundamental rights of privacy and due process were abridged—even as, ironically, the US saw the sunset of similar laws passed in the wake of the September 11, 2001, attacks. This is not the first time that legislators have agitated to abridge privacy rights in the name of "security" (more accurately, perceived safety), but in 2015 efforts to do so could easily be compared to the low success of previous efforts made after the attacks of 2001. Those evaluating the security of their enterprises would do well to monitor government efforts such as adding "backdoors" to encryption and other security tools.

Theme #5: The industry didn't learn anything about patching in 2015 The most exploited bug from 2014 happened to be the most exploited bug in 2015 as well—and it's now over five years old. While vendors continue to produce security remediations, it does little good if they are not installed by the end user. However, it's not that simple. Applying patches in an enterprise is not trivial and can be costly—especially when other problems occur as a result. The most common excuse given by those who disable automatic updates or fail to install patches is that patches break things. Software vendors must earn back the trust of users— their direct customers—to help restore faith in automatic updates.

Theme #6: Attackers have shifted their efforts to directly attack applications The perimeter of your network is no longer where you think it is. With today's mobile devices and broad interconnectivity, the actual perimeter of your network is likely in your pocket right now. Attackers realize this as well and have shifted their focus from servers and operating systems directly to applications. They see this as the easiest route to accessing sensitive enterprise data and are doing everything they can to exploit it. Today's security practitioner must understand the risk of convenience and interconnectivity to adequately protect it.

The fragility of privacy

There was perhaps no clearer sign of privacy's fragile situation in 2015 than the notice on the International Association of Privacy Professionals (IAPP) website in November, immediately after the Paris, Kenya, and Beirut bombings.22 The IAPP Europe Data Protection Congress 2015, which was scheduled to be held in Brussels during the first week of December, is not an insignificant conference. The topics on its plate this year were mighty: the then-recent upending of the US-EU Safe Harbor agreement; the continuing fallout from Edward Snowden's surveillance revelations in 2013; the role of encryption; and conversations concerning such rising topics as metadata, data localization, the Internet of Things (IoT), data sharing and breach reporting, and more. And yet it did not happen, and some who had previously cited privacy as their reason for offering certain services used by (among others) the Islamic State/IS terrorists were ceding their ground and changing their services in the face of outrage over their use.23 By the end of 2015, privacy issues seemed dangerously close to decoupling from security issues in the mind of legislators, the industry, and the public. At what would become a prophetic keynote talk during the Cato Institute's second annual Surveillance Conference in October, Senator Patrick Leahy remarked: "There are some in Congress who want to give our national security agencies a blank check. They think any attempt to protect our privacy somehow makes us less safe. I hear members accept a framework of 'balancing' privacy rights and national security. But privacy rights are pre-eminent. Protecting our basic privacy rights and protecting our country are not part of a zero-sum equation. We can do both. But we have to keep in mind: If we don't protect Americans' privacy and Constitutional liberties, what have we given up? Frankly I think far too much. And I think this great nation is hurt if we do."24 Privacy issues gave the security world much to discuss and ponder throughout 2015.

The swamping of Safe Harbor For enterprises, international data-privacy issues years in the making came to a head in October when Europe's highest court struck down the pact that allowed US and European interests to share data that has privacy considerations, specifically data that includes consumers' personally identifiable information (PII).25 The EU has safe-harbor relationships with various nation-states; the agreement in effect with the US had been in place since 2000.26

The US-EU privacy climate has been tepid since well before Edward Snowden's data releases in June 2013, but the case that tipped the EU justices' scales was a result of Snowden revelations about the Planning Tool for Resource Integration,
Synchronization, and Management program, better known as PRISM, a program launched by the National Security Agency (NSA) in 2008.27 Among the data PRISM gathers is "audio, video and image files, email messages and web searches on major U.S. Internet company websites," 28 including the likes of Google and Facebook.

Austrian Facebook user Max Schrems filed a complaint stating that Facebook's Irish subsidiary transferred data to the US and thus passed it through PRISM, in contravention of Europe's rigorous privacy protections. The Irish court agreed to look at the matter, and ultimately asked the European Court of Justice whether privacy watchdogs are bound to accept the original declaration that the US is adherent to the standard set for Safe Harbor relationships. The EU court found that the current Safe Harbor arrangement indeed did not adequately protect user

privacy rights, because it allowed US officials to gain access to user data even when European law would forbid it and allowed for data to move to third party nations with which the Safe Harbor agreement was not in force.29 The Irish data regulator was therefore free to investigate whether the data transfer was properly handled, and Safe Harbor was thus trumped.30 Companies on both sides of the Atlantic were in an uproar, scrambling to put together alternate data-transfer mechanisms (that is, mechanisms that are protected by legal devices, such as contractual data protection clauses, other than the Safe Harbor agreement) even as regulators came knocking.31 Specialized sectors such as healthcare wondered if they would be able to exchange certain kinds of security research data, while Internet titans such as Google and Facebook were warned32 by representatives of the Article 29 Working Party, the entity that oversees privacy matters in the EU, not to get "too creative"33 when plotting end runs around the ruling.

Ironically, among the activities planned for the IAPP conference was a lighthearted "S*fe H*rbor Naming Contest" to pre-christen the new arrangement.34 While this contest drew some creative entries,35 it was later announced that the group was recommending that the new arrangement be called "The Transatlantic Data Protection Framework."36 The US Department of Commerce, with which the original agreement was negotiated and which had been working for two years prior to nail down a stronger agreement, termed itself "deeply disappointed" and vowed to work for a rapid upgrade to the problematic frameworks.37

The US House of Representatives passed the Judicial Redress Act giving certain foreign citizens the right to sue over US privacy violations related to shared law enforcement data, which chief sponsor Jim Sensenbrenner said explicitly could help to mend US-EU fences.38 As this Risk Report went to press, the target date for a new framework was January 31, 2016. If no solution is found by then, "EU data protection authorities are committed to take all necessary and appropriate actions, which may include coordinated enforcement actions."39 According to at least one European official, the likelihood of a solution in that time frame was not good,40 in which case business slowdowns and even very large fines would ensue

Encryption If surveillance manages time and again to seem like a white knight after terrorist incidents, encryption is often the dragon. In the days after the Paris attacks, various simmering encryption-related debates were back on the boil, despite early evidence (still under investigation) that encryption played no role in the terrorists' planning.63 The United Kingdom was already dealing with rushed64 calls by legislators for Internet providers and social-media sites to provide unencrypted access and/or backdoors to encrypted communications to law enforcement and spy agencies.65 By the end of the year some American legislators were making similar calls,66 stating that law enforcement is unable to access necessary data. Those arguments were countered by equally venerable arguments by crypto experts67 about the certainty that backdoors—or, worse, giant stores of unencrypted data—are a recipe for unwanted, sustained, and ultimately catastrophic attention from attackers.68

At the time of this Report's writing, Senator Ron Wyden (D-OR) was brushing off his proposed 2014 Secure Data Act,69 which seeks to ban governmentmandated tech backdoors.70 One hardware manufacturer left an entire market rather than bend to government demands for

unfettered backdoor access, as BlackBerry prepared to leave the Pakistan market at year's end rather than expose its BlackBerry Enterprise Service (BES) traffic to wholesale traffic monitoring.71

Breaches in the news If 2014 was the Year of the Breach, 2015 was the Year of Collateral Damage, as certain attacks touched people who never dreamed they might be present in, or identifiable from, the data involved. It was, as every year for years has been, a year of new records. The January Anthem breach drew headlines for affecting 80 million records.126 By November, a banking breach affecting 100 million accounts passed nearly without a trace in the headlines.127 Anthem was reduced to guest appearances in other healthcare-related breach coverage128 and in background material on the OPM breach, which has been attributed to the same attackers.129

A recounting by someone affected by last year's Sony breach, ironically, seemed to make the rounds far more widely.130 By year's end, a weary observer could see a headline about a potential breach of six million voter records in Georgia and merely think it was odd that the reporter described it as "massive."131

Many consumers are inured these days to breach notifications from credit-card companies and the odd medical clinic, but 2015 brought us attackers who tried to extort crowdfunded artists137 and, more benignly, found ways to turn our teakettles138 and "smart" homes139, 140 against us. And yet these breaches in turn paled when attackers breached V-Tech's customer database,141 which included images of customers and their children.142 Predictably,143 others hijacked a Wi-Fi-enabled incarnation of Barbie.144 Even these breaches were perhaps not the most chilling of the year, even if they did target children and musicians and other relatively harmless folk—because even with all that, the kid possesses the toy, the musician benefits from the crowdfunding account, the homeowner owns the thermostat. There are, however, two 2015 breaches that best demonstrate that personal privacy violations can be perfectly impersonal: the OPM breach and the notorious Ashley Madison hack and data blast. The OPM breach, which hijacked data of over 21 million current and former federal employees, took place in mid-2014 and was revealed last spring.145 Reports indicate that a specific nation-state is believed to have stolen that data,146 though that nation-state denies147 the breach was state-sponsored. The bulk of the action took place in a quiet, intense catand-mouse game, with the affected parties learning details after the fact. In contrast, the Ashley Madison breach148 was deliberately loud and messy—a previously unknown hacker, claiming moral authority over both the site's customers and its business operations,149 unleashed a tidal wave of intensely personal data150—in addition to the startling-to-most fact that an adultery-matchmaking site had 32 million registered accounts, though perhaps not all of them operated by actual humans.151 These breaches don't initially look the same; however, both breaches had terrible effects on people who never had direct contact with the keepers of the data, and whose information appeared in it only as it related to someone else—or, in the case of the Ashley Madison breach, did not appear at all but whose identity could be easily deduced from revealed data (e.g., a spouse's name and address would be

knowable to a nosy neighbor if one spouse was registered on the site under his or her true name152).

Déjà vu again A handful of 2015 incidents seemed to have returned from a previous calendar. Remember when Radio Shack insisted on gathering too much personal information at the register?165 This year it was a clothing retailer doing it instead.166 Remember 2004, when the popular karaoke jam was Outkast's "Hey Ya!"167 and Calyx Internet Access received a National Security Letter it decided to fight in the courts? That's only just been settled.168 In the meantime, a federal court ordered the release of the information requested by an actual NSL.169 How about 2008, when the economy cratered and a recruiter ended up in court for "hacking" a database to which he had a legitimately acquired a password? Still in the courts.170 Remember when we used to worry that we were being tracked for marketing purposes by the mobile phones in our pockets? We were.171 Following the notorious Target breach, the company was back this holiday season with a $39 million settlement to be paid to all the financial institutions that had to scramble on sending new cards to their customers. This also marks the first successful classaction suit by financial institutions against a breached company.172 A Massachusetts jeweler risked the phenomenon known as the Streisand Effect173 when it took Yelp to court to demand the service reveal the name of a user who submitted a particularly angry review.174 This keeps happening175 and petitioners will keep looking for a venue that will throw out the portion of the Communications Decency Act that lets sites off the hook for allegedly libelous statements by users.176 The past isn't dead; it isn't even the past.177

A look ahead
We will be contending with the events of 2015 for some time and 2016 will bring its own excitements. In addition to the Safe Harbor revamp, expect to see activity around the meaning and uses of metadata, the development of the Internet of Things, continued controversy in the worlds of encryption and security, fresh efforts to contain certain kinds of online abuses, and maybe progress in bringing what we've all learned about data privacy to bear in the wider world. Expect to hear from people looking for a more nuanced understanding of metadata and how much it reveals. At Columbia University, a team of researchers led by Steven Bellovin and Stephanie Pell has been examining whether our current concept of metadata takes into proper account how much actual information can be derived from the means and paths of communications, even when the observer is not privy to the specific contents of the communication. For example, if someone were to look at Alice's Internet history and see that she visited one of the Ashley Madison breach data-search sites, followed by web pages such as divorcethat-loser.org, followed three months later by Tinder and Zillow.com, a good guess could be made as to what was going on with Alice lately. As Bruce Schneier noted in his Cato Institute keynote, "nobody here lies to their search engine." In our current system, it's relatively easy for surveilling entities to obtain court permission to track certain kinds of revealing activity because it's classified as "just metadata." The Columbia paper is due out next year. A recently passed digital privacy law in California, traditionally a leader in these matters, also looks to an updated idea of what we mean by, and learn from, data that may not be so "meta" after all. An amicus brief filed with the Ninth Circuit Court in support of an appeal raised by Basaaly Saeed Moalin—the Somali man convicted in the sole successful Section 215 case mentioned above—is also apt to shape our discussion of metadata going forward. Jonathan Meyer, the FTC chief technologist mentioned above, has published on the topic as well. The Internet of Things

experienced significant negative attention for privacy weaknesses this year, and this will undoubtedly continue. Observers predict a great deal of pain as disparate industries attempt to harmonize their approaches to security and privacy, some of them very different from what the traditional tech community might expect or hope for. One potential solution involves minimizing the data sent by individual devices for processing in the cloud. This thought may be anathema to hardline cloud fans, but it would simply represent just another ebb and flow in the great cycle of client-server life. The legislative dam is expected to burst at any moment on drone regulation, though tech companies and would-be flyers are expressing frustration over Federal Aviation Administration (FAA) reluctance to tackle privacy implications of these craft.189

On the ground, expect more discussion on the rights of security researchers to poke at the inner workings of vehicles. Such legislation so far looks somewhat promising, because it would require auto manufacturers to have and publish privacy policies covering data collected by the car or shared by the driver, but many are concerned that other provisions in the legislation drafted so far would criminalize vehicle hacking190— especially after researchers in 2015 made it clear191 that scrutiny is desperately needed.

In other fields, 2015 saw the first instance in which the Federal Drug Administration (FDA) recommended discontinuing use of a medical device because of security concerns, but it is unlikely Hospira's situation will be the last of that kind.192 It is hoped that greater familiarity will lead to better privacy practices for Fitbit Nation193 and thousands of other users of applications transmitting personal medical data.194 Developers of many types of mobile applications will find themselves making finer distinctions between "consumers" and "subscribers" to balance privacy rights and their need to get paid.195

And the US adoption of chip-and-pin technology late in 2015 will provide good hunting for attackers willing to show us just how little we can trust the silicon around us.196

"Swatting"

The world has in the past few years become more aware of the abuse tactic called "swatting," in which anonymous phone calls are made to summon highly armed police units to the homes of unwitting victims.197 The legal situation around swatting has been murky, but it's generally understood that some sort of legal remedy is needed. It may take one or more very bad incident outcomes to raise swatting to the necessary level of public debate, but the odds are excellent that this will come to pass198—and with multiple big wins in 2015 against owners of "revenge porn" sites,199, 200, 201 perhaps there's hope. Fortunately, we can end this section on the brighter note—a hope, even, that the things we've learned in the online world can be made helpful both online and off. Bitcoin, that privacy-centered cryptocurrency, has gained new attention from government authorities in Honduras—not because of its financial prowess, but because Bitcoin architects figured out how to allow people who do not know or trust each other to collaborate on certain kinds of activity.202 Both Honduras and Greece have expressed interest in using the blockchain concept at the heart of Bitcoin as a framework for handling land registries.203

Conclusion

Say what you will about privacy; there's always something interesting afoot. The Year of the Breach was followed by 2015's Year of Collateral Damage, as hacks exposing personal

information of people with no direct relationship to the sites breached caused pain and mayhem for tens of thousands of innocent bystanders. The US federal government struggled with many privacy issues, even as the European Union and other entities pressed the accelerator on efforts to bring US companies in line with norms overseas. With geopolitical tensions worldwide as the year closed, it seems as if privacy issues will struggle in 2016 to keep their rightful footing side by side with security efforts.

Buffer overrun/overflow
A buffer overflow is a type of vulnerability that arises when a program writes an excessive amount of data to the buffer, exceeding the capacity of the buffer and then overwriting adjacent memory. This type of vulnerability may be exploited to crash programs or, with the correct manipulation by a skilled attacker, used to execute arbitrary code on a targeted computer. Buffer vulnerabilities can be avoided by the use of bounds checking, which checks the capacity for inputs before they are written.

Cross-frame scripting
A form of cross-site scripting attack, in which attackers exploit a vulnerability in a web browser in order to load malicious thirdparty content that they control in the frame of a webpage on another site. This attack may allow an attacker to steal sensitive information, such as login details, that may be input into the frame because the targeted user believes the request for login details came from the legitimate site.

Cross-site scripting
An attack that occurs when an attacker exploits a vulnerability in web applications in order to inject malicious code into client-side code that is delivered from a compromised website to an unsuspecting user. The code that is delivered to the user is trusted, and hence executed, as it appears to come from a legitimate source. These types of attack occur due to insufficient checking and validation of user-supplier input. Attackers may use this type of attack in order to bypass access controls or steal sensitive data.

Remote code execution (RCE) vulnerability
A vulnerability that allows attackers to execute their own code on a target system. Depending on the vulnerability used, the RCE may be executed with either user- or systemlevel permissions.

Trojan
Malicious software that, unlike worms or viruses, is unable to spread of its own accord. There are many different types of Trojans that are used in conjunction with other types of malware in order to perpetrate computer crime. One of the most notorious types is a remote access Trojan (RAT) that can be used by a remote attacker to access and control a victim’s computer.

Worm
A self-contained malicious program that is able to spread of its own accord. The classification “worm” is only used to describe the ability to spread without a host file (as may be the case with

computer viruses) and worms contain many different and varied payloads beyond spreading from host system to host system.

Zero day
A previously unknown vulnerability for which no patch from the vendor currently exists. It is referred to as a zero day because the vendor has had zero days to fix the issue.

Waging war in peacetime: Cyber attacks and international norms
20 October 2015 2:17PM
Fergus Hanson is author of Internet Wars: The Struggle for Power in the 21st Century. This post is part of a series that will also examine citizen activism and control of economic chokepoints.

It was only mid-2009 when the US Secretary of Defense ordered the establishment of a dedicated Cyber Command. Now more than 100 countries have military and intelligence cyber warfare units. In the words of then-Chairman of the Joint Chiefs of Staff Martin Dempsey, cyber has become 'one of the most serious threats to national security'.

A key problem is the absence of well-accepted norms of behaviour spanning the use of cyber in conflicts. Even more concerning, there are a broad spectrum of scenarios in which cyber weapons can be used in peacetime.

Russia was first to synchronise cyber attacks with a military offensive when it invaded Georgia in 2008, and there is no doubt cyber will be integrated into future conflicts. Less clear are the appropriate limitations. International law suggests the use of force should be proportionate and limit civilian casualties. However, the internet makes civilian targets the easiest to strike and in many instances causalities are not immediate. For example, disabling an electricity grid during summer might lead to deaths through heat exhaustion.

Also unclear is the appropriate response. If a cyber attack is deadly or enormously destructive, or if the attacked country has only a limited cyber-attack capability, is a conventional military response justified? The ease of launching disruptive cyber attacks also makes them tempting, low-cost ways for a third-party, perhaps an ally, to get involved by launching cyber counter-attacks.

The nature of cyber warfare also means attacks will not always come from states.

A well-organised diaspora population located in a third country could launch a cyber attack during a conflict. If this population was in a friendly state, a law enforcement response would seem likely, but if it was in an unfriendly state a range of other response options might be on the table depending on the severity of the attack. As US Director of National Intelligence James Clapper noted in his statement to the Senate Armed Services Committee in February, it can also be difficult to distinguish between state and non-state actors within the same country, further complicating a decision on the appropriate response.

State-backed efforts to agree to norms of behaviour have begun, but are still in their early stages. One wordily named forum is the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. This formation was established last year 'to study, with a view to promoting common understandings...including norms, rules or principles of responsible behaviour of States'. In June 2015 it offered recommendations. Many were sensible, such as the suggestion that 'A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure'. Unfortunately, the characterisation of some of the recommendations as 'norms' was more aspirational than founded in practice, considering they are being breached on a daily basis.

James Clapper characterised cyber attacks as a 'growing reality' and noted: 'foreign actors are reconnoitring and developing access to US critical infrastructure systems, which might be quickly exploited for disruption if an adversary's intent became hostile'. Key threat actors named were Russia, China, Iran and North Korea, the latter two noted for having 'possibly more disruptive intent'.

Cyber attacks should now be expected during times of war. Of far more concern though is the emerging norm in favour of conducting cyber attacks during peacetime. In 2012, the UK's then-Minister of State for the Armed Forces, Nick Harvey, even made the case to the Shangri-La Dialogue that cyber attacks were 'quite a civilised option.'

Practice would suggest several states agree. In 2012, it was revealed the US had been targeting Iran's nuclear program with cyber attacks. It was the first time a cyber attack had turned hot, doing physical real-world damage. In retaliation, Iran launched a major attack in August 2012 on the world's largest energy company, Saudi Aramco.

North Korea has also been active, attacking South Korean banks and broadcasters in March 2013. In November 2014, it struck again, targeting Sony's spoof movie, The Interview, about the assassination of the North Korean leader. The attackers used the threat of terrorism to persuade theatre chains in the US to pull out of screening the film. As President Obama said at the time: 'We cannot have a society in which some dictator someplace can start imposing censorship here in the United States. Because if somebody is able to intimidate folks out of releasing a satirical movie, imagine what they start doing when they see a documentary that they don't like, or news reports that they don't like.'

These attacks didn't lead to any deaths, but that seems unlikely to last. Major attacks on critical infrastructure could easily result in casualties, making escalation to traditional military options more likely. Cyber attacks may have appeared to be a soft, civilised option when not everyone had them, but with over 100 states now having military and intelligence cyber warfare units and

cyber capabilities increasing, their more benign nature is unlikely to last or to escape the pitfalls of miscalculation and escalation.

As an advanced, open economy, Australia is vulnerable to cyber attack, including on critical infrastructure, as the first unclassified Australian Cyber Security Centre Threat Report made clear. There were 153 attacks reported last year on 'systems of national interest, critical infrastructure and government'. Australia has a strong interest in encouraging a much more robust global discussion that will agree on norms of behaviour and challenge the emerging norm in favour of using cyber weapons in times of peace

Archives: By Topic

In the Pipeline

Coming up for
Wednesday, February 3

EVENT A Conversation on the 2015 Department of Defense Law of War Manual Presented by: Georgetown Law's Center on National Security and the Law Speakers: Marty Lederman, Associate Professor of Law, Georgetown Law and Founding Editor, Just Security; Charles A. Allen, Deputy General Counsel for International Affairs, Department of Defense; and Jamie Baker, Former Chief Judge of the United States Court of Appeals for the Armed Forces Time & Location: 3:30pm; Georgetown Law, Washington, DC Details & Registration: available here… continue »
Coming up for
Wednesday, February 3

EVENT The United States of Jihad Presented by: International Security Program at New America Speakers: Peter Bergen, Vice President & Director of the International Security Program at New America, National Security Analyst at CNN, and Author of United States of Jihad: Investigating America's Homegrown Terrorists; Karen Greenberg, Director of the Center on National Security at Fordham University School of Law and Author, The Least Worst Place: Guantanamo's First 100 Days Time & Location: 6:30pm-8:15pm; New York, NY Details & Registration: available here… continue »
Coming up for
Friday, February 5

EVENT The Frontiers of Cybersecurity Policy and Law Presented by: The Robert S. Strauss Center for International Security and Law, University of Texas at Austin Speakers: Jen Daskal, Assistant Professor of Law, American University Washington College of Law and Executive Editor, Just Security; Kristen Eichensehr, Visiting Assistant Professor, UCLA School of Law and Executive Editor, Just Security; Jennifer Granick, Director of Civil Liberties at the Stanford Center for Internet and Society and Executive Editor, Just Security; and more.… continue »
Featured Posts

News Roundup and Notes: February 3, 2016

By Nadia O'Mara
A Few Keystrokes Could Solve the Crime. Would You Press Enter?
By Jonathan Zittrain
Why Aren't Criminal Defendants Getting Notice of Section 702 Surveillance — Again?
By Patrick C. Toomey
A Legal Map of Airstrikes in Syria (Part 2)
By Jonathan Horowitz
History, Hysteria, and Syrian Refugees
By Jaya Ramji-Nogales
Is the FBI Using Zero-Days in Criminal Investigations?
By Ahmed Ghappour
X HIDE THIS SIDEBAR
International Law and Cyber Attacks: Sony v. North Korea

By Michael Schmitt
Wednesday, December 17, 2014 at 9:29 AM
8Printsubmit to reddit
Sonypicturesentertainmentoffices

It could only happen in the movies. A major Hollywood company produces a film starring well-known comedic actors which involves the tongue-in-cheek assassination of the leader of a remote and rather bizarre dictatorship. The "supreme leader" apparently orders a secret group of cyber warriors calling themselves "The Guardians of Peace" (in actuality, the State-run "Bureau 121") to retaliate by attacking the company's IT system. Data is destroyed, sensitive personal data and highly embarrassing emails are made public and, worst of all, the script for the new James Bond movie is leaked. The international community is outraged, with some pundits calling it "war," while others claim that the operation has crossed the armed attack threshold thereby allowing the United States to respond forcefully. Send in the 7th Fleet….

But truth often proves stranger than fiction. With the exception of the U.S. Navy steaming towards North Korean shores, the description reflects recent events involving an alleged malicious North Korean cyber operation against Sony. This contribution to Just Security analyzes the real world incident from an international law perspective. It draws on the work of the International Group of Experts (IGE) that produced the Tallinn Manual on the International Law Applicable to Cyber Warfare, as well as research underway in the "Tallinn 2.0" follow-up project.

Pursuant to Article 51 of the UN Charter and customary international law, if the malicious cyber operation against Sony had constituted a "use of force" rising to the level of an "armed attack," the United States would have been entitled to respond forcefully, whether by kinetic or cyber means. The IGE unanimously agreed that cyber operations alone may be sufficient to cross the armed attack threshold, particularly when they cause substantial injury or physical damage. Some members of the group went further by focusing not on the nature of the harm caused, but rather its severity. In their view, a sufficiently severe non-injurious or destructive cyber operation, such as that resulting in a State's economic collapse, can qualify as an armed attack.

The cyber operation against Sony involved the release of sensitive information and the destruction of data. In some cases, the loss of the data prevented the affected computers from rebooting properly. Albeit highly disruptive and costly, such effects are not at the level most experts would consider an armed attack. Additionally, some States and scholars reject the view

that the right of self-defense extends to attacks by non-State actors. Even though the attribution of the Sony incident to North Korea has been questioned, this debate is irrelevant because the operation failed to qualify as an armed attack in the first place.

But was the operation nevertheless a violation of Article 2(4) of the UN Charter and customary international law's prohibition on the use of force by States such that it opened the door to responses other than forceful ones? The prevailing view in international law is that "use of force" is a lower threshold than "armed attack;" all armed attacks are uses of force, but the reverse is not true. Unfortunately, after three years of discussion, the IGE could arrive at no black letter definition of a cyber use of force. Its members merely agreed that States would make case-by-case assessments of non-injurious or destructive cyber operations, considering such factors as severity, immediacy of effect, invasiveness, military character, and so forth.

Although the use of force threshold remains ambiguous, it seems highly unlikely that the international community will characterize operations like that against Sony as such. This hesitancy will be driven in part by concern over the U.S. position (a distinctly minority one) that all uses of force are also armed attacks that allow forceful responses. Some States view the premise as potentially destabilizing in that it allows for an earlier use of force than would otherwise be the case. They will accordingly be extremely reticent about characterizing cyber operations as having crossed that threshold.

Another possibility that can be dispensed with quickly is that the operation against Sony constituted an unlawful "intervention" against the United States. Disrupting a private company's activities is not the type of coercive action that intrudes into the domaine réservé of another State, thereby qualifying as intervention. Clear examples of intervention would include the financing of rebel forces examined by the International Court of Justice in its Nicaragua judgment, or even the election return manipulation cited by the IGE in its work—both well-removed from a cyber operation against Sony.

North_Korean_observation_post-public-domain-federal-government

Much more defensible is characterization of the operation as a breach of U.S. sovereignty. To constitute a breach of sovereignty, an action must be attributable to a State. If North Korea's Bureau 21 mounted the cyber operation, there is no question of attribution since its hackers work for the military's General Bureau of Reconnaissance, and therefore are State "organs" whose actions are, as recognized in Article 4 of the ILC's Articles on State Responsibility, attributable to North Korea (even if acting ultra vires). If conducted by a non-State group, attribution for the operation would attach only if North Korea directed and controlled it (Article 8), or later acknowledged and adopted the action as its own (Article 11).

Assuming for the sake of analysis that the targeting of Sony is legally attributable to North Korea, the question remains as to whether it amounted to a breach of U.S. sovereignty. As an aside, it makes no difference that Sony is a private company, for the cyber infrastructure in question is situated in U.S. territory and therefore implicates U.S. sovereignty.

The substantive criteria for breach of sovereignty by cyber means has been the subject of extensive examination in the Tallinn 2.0 process. In the earlier Tallinn Manual, the IGE agreed that at the very least a cyber operation breached sovereignty whenever physical damage (as distinct from harm to data) occurred. While no further consensus could be achieved on the matter, it would seem reasonable to characterize a cyber operation involving a State's

manipulation of cyber infrastructure in another State's territory, or the emplacement of malware within systems located there, as a violation of the latter's sovereignty. This being so, if the cyber operation against Sony is attributable to North Korea, it violated U.S. sovereignty. In the patois of the law of State responsibility, the operation amounted to an "internationally wrongful act".

The commission of an internationally wrongful act entitles an injured State to engage in "countermeasures" under the law of State responsibility, as captured in Article 22 and 49-54 of the Articles on State Responsibility. Countermeasures are actions by an injured State that breach obligations owed to the "responsible" State (the one initially violating its legal obligations) in order to persuade the latter to return to a state of lawfulness. Thus, if the cyber operation against Sony is attributable to North Korea and breached U.S. sovereignty, the United States could have responded with countermeasures, such as a "hack back" against North Korean cyber assets. Indeed, it may still enjoy the right to conduct countermeasures, either because it is reasonable to conclude that the operation is but the first blow in a campaign consisting of multiple cyber operations or based on certain technical rules relating to reparations. It must be cautioned that the right to take countermeasures is subject to strict limitations dealing with such matters as notice, proportionality, and timing. Moreover, they are only available against States and the prevailing view is that a countermeasure may not rise to the level of a use of force.

If the operation is not attributable to North Korea as a matter of law, that State may nevertheless have been in breach of an obligation owed to the United States and other countries to ensure that cyber operations on its territory do not cause foreign States harm. Violation of this obligation of "due diligence" may itself provide a separate basis for countermeasures by injured States. In other words, if a territorial State fails to exercise due diligence in controlling non-State cyber operations launched from its territory, an injured State may resort to countermeasures designed to compel that State to take the remedial measures to put an end to those activities. In the Sony case, even if the harmful cyber operation could not be attributed to North Korea under the law of State responsibility, the United States would have been entitled to conduct cyber operations against North Korea, or engage in other countermeasures, on the basis of North Korea's failure to discharge its due diligence responsibilities. Interestingly, countermeasures in such cases may consist of breaches of the territorial State's sovereignty in the form of hack-backs (below the use of force level) against the non-State actors operating from its territory. So, even though international law does not permit countermeasures against non-State actors on the basis of their own actions, operations against the non-State groups or individuals may be appropriate if styled as countermeasures against the States from which they act.

Countermeasures may only be taken by States. Thus, Sony could not have, on its own accord, responded against North Korea with its own cyber operations. That said, States are entitled to outsource the taking of lawful cyber actions to private entities; when they do so, the States shoulder legal responsibility for the actions.

A very limited, but highly important, basis for a State's response to harmful cyber operations is action pursuant to the plea of necessity, a notion reflected in Article 25 of the Articles of State Responsibility. In the cyber context, the rule applies only when harmful cyber operations affect the State's "essential interest" and the action is the only means to address "a grave and imminent peril" thereto. When this situation occurs, a State may take necessary actions that would otherwise be unlawful so long as the actions do not affect the essential interests of other States. There is no requirement in such situations that there be an initial "internationally wrongful act" or that, as in the case of countermeasures, the internationally wrongful act be attributable to a State. Thus, a plea of necessity is available in situations in which the author of a

harmful cyber operation is either a non-State actor or is unknown. It would appear indisputable that in the case of the operation against Sony, no essential U.S. interest was affected and therefore there was no legal basis to resort to the plea of necessity.

Completing the gamut of possible responses by States to harmful cyber operations mounted against them or entities on their territory is retorsion. Acts of retorsion are those that are unfriendly but lawful. For instance, barring any treaty obligation to the contrary, a State may close its cyber infrastructure to transmissions from another State in response to the latter's harmful cyber operations.

As this analysis illustrates, international law admits of a wide, although rather nuanced, range of possible response options in the face of malicious cyber operations. States and commentators would do well to recognize this reality. And, of course, all of the possibilities explored above are without prejudice to taking lawful measures under domestic law once jurisdiction attaches. Thus, for instance, those involved in the Sony incident risk prosecution under U.S. law in much the same way that five Chinese military hackers were indicted last May for computer hacking, economic espionage and other offenses

IN RE ANTHEM, INC. DATA BREACH LITIGATION.https://scholar.google.com/scholar_case?case=6470222317361935673&q=cyber+attack&hl=en&as_sdt=3,25&as_ylo=2016
https://scholar.google.com/scholar_case?case=6470222317361935673&q=cyber+attack&hl=en&as_sdt=3,25&as_ylo=2016

Case No. 15-MD-02617-LHK.
United States District Court, N.D. California, San Jose Division.

February 14, 2016.
ORDER GRANTING IN PART AND DENYING IN PART ANTHEM DEFENDANTS' MOTION TO DISMISS AND ORDER GRANTING IN PART AND DENYING IN PART NON-ANTHEM DEFENDANTS' MOTION TO DISMISS

Re: Dkt. No. 410, 413

LUCY H. KOH, District Judge.

Plaintiffs[1] bring this putative class action against Anthem, Inc., 28 Anthem affiliates,[2] Blue Cross Blue Shield Association, and 17 non-Anthem Blue Cross Blue Shield Companies.[3] The Court shall refer to Anthem, Inc. and the Anthem affiliates as the "Anthem Defendants," and shall refer to Blue Cross Blue Shield Association and the non-Anthem Blue Cross Blue Shield Companies as the "Non-Anthem Defendants." The Court shall refer to the Anthem and Non-Anthem Defendants collectively as "Defendants."

Before the Court are separate motions to dismiss Plaintiffs' consolidated amended complaint ("CAC") filed by the Anthem and Non-Anthem Defendants. See ECF No. 334-6 ("CAC"); ECF No. 410 ("Anthem Mot."); ECF No. 413 ("Non-Anthem Mot."). Having considered the parties' submissions, the relevant law, and the record in this case, the Court hereby GRANTS in part

and DENIES in part the Anthem Defendants' motion to dismiss and GRANTS in part and DENIES in part the Non-Anthem Defendants' motion to dismiss.

I. BACKGROUND

A. Factual Background

Defendant Anthem, Inc. ("Anthem") is one of the largest health benefits and health insurance companies in the United States. CAC ¶ 109. Anthem serves its members through various Blue Cross Blue Shield ("BCBS") licensee affiliates and other non-BCBS affiliates. Id. ¶ 155. Anthem also cooperates with the Blue Cross Blue Shield Association ("BCBSA") and several independent BCBS licensees via the BlueCard program. Id. ¶ 156. "Under the BlueCard program, members of one BCBS licensee may access another BCBS licensee's provider networks and discounts when the members are out of state." Id.

In order to provide certain member services, the Anthem and Non-Anthem Defendants "collect, receive, and access their customers' and members' extensive individually identifiable health record information." Id. ¶ 157. "These records include personal information (such as names, dates of birth, Social Security numbers, health care ID numbers, home addresses, email addresses, and employment information, including income data) and individually-identifiable health information (pertaining to the individual claims process, medical history, diagnosis codes, payment and billing records, test records, dates of service, and all other health information that an insurance company has or needs to have to process claims)." Id. The Court shall refer to members' personal and health information as Personal Identification Information, or "PII."

Anthem maintains a common computer database which contains the PII of current and former members of Anthem, Anthem's affiliates, BCBSA, and independent BCBS licensees. Id. ¶ 158. In total, Anthem's database contains the PII of approximately 80 million individuals. Id. ¶ 204. According to Plaintiffs, both the Anthem and Non-Anthem Defendants promised their members that their PII would be protected. Blue Cross of California, for instance, mailed the following privacy notice to its members:

> We keep your oral, written and electronic [PII] safe using physical, electronic, and procedural means. These safeguards follow federal and state laws. Some of the ways we keep your [PII] safe include securing offices that hold [PII], password-protecting computers, and locking storage areas and filing cabinets. We require our employees to protect [PII] through written policies and procedures. . .. Also, where required by law, our affiliates and nonaffiliates must protect the privacy of data we share in the normal course of business. They are not allowed to give [PII] to others without your written OK, except as allowed by law and outlined in this notice.

Id. ¶ 163 (emphasis removed). In February 2015, Anthem announced to the public that "cyberattackers had breached the Anthem Database, and [had] accessed [the PII of] individuals in the Anthem Database." Id. ¶ 203. This was not the first time that Anthem had experienced problems with data security. In late 2009, approximately 600,000 customers of Wellpoint (Anthem's former trade name) "had their personal information and protected healthcare information compromised due to a data breach." Id. ¶ 194. In addition, in 2013, the U.S. Department of Health and Human Services fined Anthem $1.7 million for various HIPAA violations related to data security. Id. ¶ 195. Finally, in 2014, the federal government informed Anthem and other healthcare companies of the possibility of future cyberattacks, and advised these companies to take appropriate measures, such as data encryption and enhanced password protection. Id. ¶¶ 200-01.

Plaintiffs allege that Defendants did not sufficiently heed these warnings, which allowed cyberattackers to extract massive amounts of data from Anthem's database between December 2014 and January 2015. Id. ¶ 226. After Anthem discovered the extent of this data breach, it proceeded to implement various containment measures. Id. ¶ 232. The cyberattacks ceased by January 31, 2015. Id. In addition, after learning of the cyberattacks, Anthem proceeded to retain Mandiant, a cybersecurity company, "to assist in assessing and responding to the Anthem Data Breach and to assist in developing security protocols for Anthem." Id. ¶ 207. Mandiant's work culminated in the production of an Intrusion Investigation Report ("Mandiant Report"), which Mandiant provided to Anthem in July 2015. Id.

According to Plaintiffs, the Mandiant Report found that "Anthem and [its] Affiliates [had] failed to take reasonable measures to secure the [PII] in their possession." Id. ¶ 236. Likewise, Plaintiffs allege that "Anthem and Anthem Affiliates [] lacked reasonable encryption policies." Id. ¶ 237. Additionally, "BCBSA and non-Anthem BCBS allowed the [PII] that their current and former customers and members had entrusted with them to be placed into the Anthem Database even though there were multiple public indications and warnings that the Anthem and Anthem Affiliates' computer systems and data security practices were inadequate." Id. ¶ 243. Plaintiffs further aver that although Anthem publicly disclosed the data breach in February 2015, many affected customers were not personally informed until March 2015, if at all. Id. ¶ 250. Finally, Plaintiffs contend that Anthem still has not disclosed whether it has made any changes to its security practices to prevent a future cyberattack.

B. Indiana Negligence (against Anthem and Non-Anthem Defendants)

"The elements of a negligence claim under Indiana law are: (1) a duty owed to plaintiff by defendant, (2) breach of duty by allowing conduct to fall below the applicable standard of care, and (3) a compensable injury proximately caused by defendant's breach of duty." Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 635 (7th Cir. 2007) (internal quotation marks omitted). Here, Plaintiffs allege that the Anthem and Non-Anthem Defendants "violated the duty of care owed Indiana Plaintiffs and Class Members by collecting and storing their [PII] without adequate data security." Anthem Opp'n at 3.

As to whether Indiana law provides Plaintiffs a private cause of action, the parties acknowledge that no Indiana court has yet ruled on this question. The Court therefore looks to the law of the Seventh Circuit, of which Indiana is a part. On this point, the Court finds instructive the Seventh Circuit's decision in Pisciotta v. Old National Bancorp. In Pisciotta, Old National Bancorp ("ONB") maintained a website containing the personal information of potential customers. In 2005, ONB learned that its website had been hacked, and ONB subsequently informed affected potential customers of this breach. Upon receiving this information, Luciano Pisciotta ("Pisciotta") and Daniel Mills ("Mills") proceeded to file a putative class action complaint against ONB. As in the instant case, the Pisciotta complaint asserted a negligence claim under Indiana law. The District Court for the Southern District of Indiana determined that Pisciotta and Mills could not bring such a claim as a matter of law, and granted ONB's motion for judgment on the pleadings. 499 F.3d at 632-33 (reciting procedural history). The Seventh Circuit upheld the district court's decision on appeal.

In reaching this conclusion, the Seventh Circuit first observed that "[n]either the parties' efforts nor our own have identified any Indiana precedent addressing" whether "Indiana would consider

that the harm caused by identity information exposure, coupled with the attendant costs to guard against identity theft, constitutes an existing compensable injury and consequent damages required to state a claim for negligence." Id. at 635. Accordingly, "[w]ithout state authority to guide us, `[w]hen given a choice between an interpretation of [state] law which reasonably restricts liability, and one which greatly expands liability, we should"—as a general matter— "choose the narrower and more reasonable path (at least until the [state] Supreme Court tells us differently).'" Id. at 635-36 (quoting Todd v. Societe Bic, S.A. 21 F.3d 1402, 1412 (7th Cir. 1994) (en banc)) (alterations in original).

With this general canon of interpretation in mind, the Seventh Circuit further observed that "the Indiana authority most closely addressed to the issue"—a series of statutes enacted by the Indiana legislature in 2006—weighed against finding that Pisciotta and Mills could assert a private right of action against ONB. Id. at 636-37. The statutory provisions "applicable to private entities storing personal information require only that a database owner disclose a security breach to potentially affected consumers; they do not require the database owner to take any other affirmative act in the wake of a breach." Id. at 637. Moreover, "[i]f the database owner fails to comply with the only affirmative duty imposed by the statute—the duty to disclose—the statute provides for enforcement only by the Attorney General of Indiana. It creates no private right of action against the database owner." Id. Thus, disclosure to those affected is the only duty imposed upon the database owners by Indiana's data breach statutes, and these statutes only allow for enforcement by the Indiana Attorney General.

The Seventh Circuit went on to reject the view "that the statute is evidence that the Indiana legislature believes that an individual has suffered a compensable injury at the moment his personal information is exposed because of a security breach." Id. Indeed, "given the novelty of the legal questions posed by information exposure and theft, it is unlikely that the legislature intended to sanction the development of common law tort remedies that would apply to the same factual circumstances addressed by the statute." Id.

The Court finds Pisciotta persuasive for the following reasons. First, this Court, as an MDL court, "must apply the law of the transferor forum, that is, the law of the state in which the action was filed." In re Vioxx Prods. Liab. Litig., 478 F. Supp. 2d 897, 903 (E.D. La. 2007); see also In re Korean Air, 642 F.3d at 699 ("[T]he MDL transferee court is generally bound by the same substantive legal standards . . . as would have applied in the transferor court."). This legal principle means that, for a negligence claim brought under the laws of Indiana, the MDL court should—as a general matter—follow the lead of the Seventh Circuit.

Second, although Pisciotta was decided in 2007, the parties have identified no subsequent cases—state or federal—that have discussed Indiana's data breach statutes. The Court has found none in its own research. Thus, Pisciotta continues to serve as the final word on how courts should interpret Indiana's data breach statutes and, critically, whether individuals may maintain a private cause of action for negligence. 499 F.3d at 637 ("Had the Indiana legislature intended that a cause of action should be available against a database owner for failing to protect adequately personal information, we believe that it would have made some more definite statement of that intent.").

Third, the Pisciotta decision is consistent with the negligence law of other jurisdictions. In Amburgy v. Express Scripts, Inc., 671 F. Supp. 2d 1046, 1054 (E.D. Mo. 2009), for instance, plaintiff alleged "that defendant was negligent in its failure to properly secure its computerized database system[,] thereby rendering the system vulnerable to a security breach and, further,

was negligent in its failure to timely disclose the alleged breach." In rejecting plaintiff's claim, the Amburgy court "note[d] that the Missouri legislature [had] recently enacted a data breach notification law." Id. at 1055. That law, like Indiana's statutes, holds that the state "Attorney General [is] to have exclusive authority in bringing claims against data handlers for a violation of the notice requirements." Id. The Missouri statute did not provide a private cause of action, and the Amburgy court declined to create a cause of action "where one does not exist." Id.

Similarly, in Willingham v. Global Payments, Inc., 2013 WL 440702, *17 n.19 (N.D. Ga. Feb. 5, 2013), plaintiffs sought to assert a common law negligence claim against defendant. In arguing that defendant owed plaintiffs such a duty, plaintiffs cited data breach statutes from Kansas and California. Id. After carefully reviewing these statutes, the Willingham court concluded that the statutes "do not give [p]laintiffs a [private] cause of action for negligence." Id. As the district court explained, these statutes contain a notice provision which requires companies to provide notice to affected customers of a data breach. Like the statutes at issue in Pisciotta and Amburgy, however, these statutes do not contain a private enforcement mechanism.

Third, and finally, Plaintiffs' attempts to distinguish Pisciotta are unavailing. Plaintiffs, for instance, point to the fact that the Indiana legislature amended Indiana's data breach statutes in 2009. The statutes now require database owners to "maintain reasonable procedures . . . to protect and safeguard from unlawful use or disclosure any personal information," a provision that did not exist at the time Pisciotta was decided. Anthem Opp'n at 4. The amendments also exempt some "database owners with security policies under HIPAA from some . . . [statutory] requirements." Anthem Mot. at 2 n.3. None of these amendments, however, address whether individual plaintiffs may maintain a private cause of action in negligence. Indiana's data breach statutes continue to provide a single enforcement mechanism: an action brought by the state Attorney General. Ind. Code. Ann. § 24-4.9-4-2. The Court thus fails to see how the 2009 amendments give support to Plaintiffs' attempts to maintain a private cause of action. Pisciotta was decided in 2007. The Indiana legislature, presumably aware of the Pisciotta decision, declined to provide plaintiffs a private cause of action when given the opportunity to amend the state's data breach statutes in 2009.

Plaintiffs also contend that Indiana courts "frequently borrow from statutes that do not contain a private right of action to impose common law duties." Anthem Opp'n at 4. Plaintiffs cite Kho v. Pennington, 875 N.E.2d 208, 212 (Ind. 2007), where the Indiana Supreme Court recognized a private right of action for statutory negligence "arising from the violation of the identity confidentiality provision in Indiana Code § 34-18-8-7(a)(1)."

WebImagesMore…vralitigator@gmail.com
Pisciotta v. Old Nat. Bancorp, 499 F. 3d 629 - Court of Appeals, 7th Circuit 2007
ReadHow citedSearch
Highlighting cyber attack
499 F.3d 629 (2007)
Luciano PISCIOTTA and Daniel Mills, on behalf of themselves and others similarly situated, Plaintiffs-Appellants,
v.
OLD NATIONAL BANCORP, Defendant-Appellee.

No. 06-3817.
United States Court of Appeals, Seventh Circuit.

Argued May 21, 2007.
Decided August 23, 2007.
631*631 William N. Riley (argued), Price Waicukauski Riley & Debrota, Indianapolis, IN, for Plaintiffs-Appellants.

Mark J.R. Merkle (argued), Greg A. Small, Krieg Devault, Indianapolis, IN, for Defendant-Appellee.

Before RIPPLE, WOOD and EVANS, Circuit Judges.

RIPPLE, Circuit Judge.

Plaintiffs Luciano Pisciotta and Daniel Mills brought this action on behalf of a putative class of customers and potential customers of Old National Bancorp ("ONB"). They alleged that, through its website, ONB had solicited personal information from applicants for banking services, but had failed to secure it adequately. As a result, a third-party computer "hacker" was able to obtain access to the confidential information of tens of thousands of ONB site users. The plaintiffs sought damages for the harm that they claim to have suffered because of the security breach; specifically, they requested compensation for past and future credit monitoring services that they have obtained in response to the compromise of their personal data through ONB's website. ONB answered the allegations and then moved for judgment on the pleadings under Rule 12(c). The district court granted ONB's motion and dismissed the case. The plaintiffs timely appeal. For the reasons set forth in this opinion, we affirm the judgment of the district court.

I

BACKGROUND

A. Facts

ONB operates a marketing website on which individuals seeking banking services can complete online applications for accounts, loans and other ONB banking services. The applications differ depending on the service requested, but some forms require the customer or potential customer's name, address, social security number, driver's license number, date of birth, mother's maiden name and credit card or other financial account numbers. In 2002 and 2004, respectively, Mr. Pisciotta and Mr. Mills accessed this website and entered personal information in connection 632*632 with their applications for ONB banking services.

In 2005, NCR, a hosting facility that maintains ONB's website, notified ONB of a security breach. ONB then sent written notice to its customers. The results of the investigation that followed have been filed under seal in this court; for present purposes, it will suffice to note that the scope and manner of access suggests that the intrusion was sophisticated, intentional and malicious.

B. District Court Proceedings

Mr. Pisciotta and Mr. Mills, on behalf of a putative class of other ONB website users, brought this action in the United States District Court for the Southern District of Indiana. They named

ONB and NCR as defendants and asserted negligence claims against both defendants as well as breach of implied contract claims by ONB and breach of contract by NCR. The plaintiffs alleged that:

[b]y failing to adequately protect [their] personal confidential information, [ONB and NCR] caused Plaintiffs and other similarly situated past and present customers to suffer substantial potential economic damages and emotional distress and worry that third parties will use [the plaintiffs'] confidential personal information to cause them economic harm, or sell their confidential information to others who will in turn cause them economic harm.
R.37 at 2.

In pleading their damages, the plaintiffs stated that they and others in the putative class "have incurred expenses in order to prevent their confidential personal information from being used and will continue to incur expenses in the future." Id. at 4. Significantly, the plaintiffs did not allege any completed direct financial loss to their accounts as a result of the breach. Nor did they claim that they or any other member of the putative class already had been the victim of identity theft as a result of the breach. The plaintiffs requested "[c]ompensation for all economic and emotional damages suffered as a result of the Defendants' acts which were negligent, in breach of implied contract or in breach of contract," and "[a]ny and all other legal and/or equitable relief to which Plaintiffs... are entitled, including establishing an economic monitoring procedure to insure [sic] prompt notice to Plaintiffs ... of any attempt to use their confidential personal information stolen from the Defendants." Id. at 5-6.

NCR moved to dismiss for failure to state a claim; its motion was granted. This ruling has not been appealed. ONB, the remaining defendant, answered the second amended complaint. The plaintiffs moved for class certification. ONB then filed a motion for judgment on the pleadings under Federal Rule of Civil Procedure 12(c) and a memorandum in opposition to class certification.

The district court granted ONB's motion for judgment on the pleadings and denied the plaintiffs' motion for class certification as moot. Specifically, the district court concluded that the plaintiffs' claims failed as a matter of law because "they have not alleged that ONB's conduct caused them cognizable injury." R.78 at 3. In support of its conclusion, the court noted that, under Indiana law, damages must be more than speculative; therefore, the plaintiffs' allegations that they had suffered "substantial potential economic damages" did not state a claim. Id. (emphasis in original).

The district court looked to five cases from other district courts across the Country that had rejected claims for "the cost of credit monitoring as an alternative 633*633 award for what would otherwise be speculative and unrecoverable damages." Id. Finding their reasoning persuasive, the district court concluded that "[t]he expenditure of money to monitor one's credit is not the result of any present injury, but rather the anticipation of future injury that has not yet materialized." Id. at 4 (citing Forbes v. Wells Fargo Bank, N.A., 420 F.Supp.2d 1018, 1021 (D.Minn.2006)). The court also concluded that, although not enumerated as a separate cause of action in the complaint, the plaintiffs had made allegations that could relate to a claim for negligent infliction of emotional distress; the court dismissed this claim as well. It noted that, as a matter of Indiana law, any such action was dependent on an underlying negligence claim. Id. at 5. Finally, the court concluded that there could be no action for breach of contract under Indiana law in the absence of an allegation of cognizable damages.

The plaintiffs then timely appealed the entry of judgment for ONB on the claims for negligence and breach of implied contract[1] and further asked that this court vacate the order denying class certification as moot.

II

DISCUSSION

We review a district court's decision on a 12(c) motion de novo. Moss v. Martin, 473 F.3d 694, 698 (7th Cir.2007). We take the facts alleged in the complaint as true, drawing all reasonable inferences in favor of the plaintiff. Thomas v. Guardsmark, Inc., 381 F.3d 701, 704 (7th Cir.2004). We review the judgment for the defendants by employing the same standard that we apply when reviewing a motion to dismiss under Rule 12(b)(6). Guise v. BWM Mortgage, LLC, 377 F.3d 795, 798 (7th Cir.2004). The complaint must contain only "a short and plain statement of the claim showing that the pleader is entitled to relief." Fed.R.Civ.P. 8(a)(2); see also Conley v. Gibson, 355 U.S. 41, 47, 78 S.Ct. 99, 2 L.Ed.2d 80 (1957). There is no need for detailed factual allegations. Conley, 355 U.S. at 47, 78 S.Ct. 99. However, the statement must "give the defendant fair notice of what the ... claim is and the grounds upon which it rests." Id. "Factual allegations must be enough to raise a right to relief above the speculative level." Bell Atl. Corp. v. Twombly, ___ U.S. ___, 127 S.Ct. 1955, 1965, 167 L.Ed.2d 929 (2007); see also Jennings v. Auto Meter Prods., Inc., 495 F.3d 466, 472 (7th Cir.2007).

A. Jurisdiction

The plaintiffs filed this action in the district court under the Class Action Fairness Act of 2005, Pub.L. 109-2, § 4, 119 Stat. 4, 9 (codified at 28 U.S.C. § 1332(d)) ("CAFA"), on behalf of a putative class that includes residents of Indiana, Illinois, Kentucky, Missouri, Ohio and Tennessee. Under CAFA, the district court had jurisdiction over this action because "the matter in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs," 28 U.S.C. § 1332(d)(2), and because at least one member of the proposed class is a citizen of a State different from ONB. Id. § 1332(d)(2)(A). In short, subject to limitations not relevant here, CAFA allows for incomplete diversity. Id.; cf. Strawbridge v. Curtiss, 3 Cranch 267, 7 U.S. 267, 2 L.Ed. 435 (1806) (interpreting the language of the general federal diversity statute to require complete diversity). In calculating the requisite amount in controversy, CAFA requires that the claims of 634*634 all the plaintiffs be aggregated. 28 U.S.C. § 1332(d)(6); cf. In re Brand Name Prescription Drugs Antitrust Litig., 123 F.3d 599, 607 (7th Cir.1997) (noting the otherwise applicable rule that aggregation is not permitted and, therefore, at least one plaintiff in a particular class must satisfy the jurisdictional minimum).

We have, of course, an independent responsibility to examine our subject matter jurisdiction. See Steel Co. v. Citizens for a Better Env't, 523 U.S. 83, 95, 118 S.Ct. 1003, 140 L.Ed.2d 210 (1998). As we have noted, in reaching the conclusion that dismissal was appropriate, the district court in this case relied on several cases from other district courts throughout the Country. Many of those cases have concluded that the federal courts lack jurisdiction because plaintiffs whose data has been compromised, but not yet misused, have not suffered an injury-in-fact sufficient to confer Article III standing.[2] We are not persuaded by the reasoning of these cases. As many of our sister circuits have noted, the injury-in-fact requirement can be satisfied by a threat of future harm or by an act which harms the plaintiff only by increasing the risk of future harm that the plaintiff would have otherwise faced, absent the defendant's actions.[3] We concur in this view.[4] Once the plaintiffs' allegations establish at least this level of injury, the fact that the

plaintiffs anticipate that some greater potential harm might follow the defendant's act does not affect the standing inquiry.

B. Availability of Credit Monitoring Damages Under Indiana Law

With the issue of jurisdiction resolved, we now turn to the merits of the plaintiffs' claim for damages. This case, invoking CAFA's special rules for diversity jurisdiction, alleges causes of action under Indiana law. Our duty, therefore, as in every diversity case, is to apply state substantive law, as we believe the highest court of the state would apply it. State Farm Mut. Auto. Ins. Co. v. Pate, 275 F.3d 666, 669 (7th Cir.2001).

635*635 The principal claims in this case are based on a negligence theory. The elements of a negligence claim under Indiana law are: "(1) a duty owed to plaintiff by defendant, (2) breach of duty by allowing conduct to fall below the applicable standard of care, and (3) a compensable injury proximately caused by defendant's breach of duty." Bader v. Johnson, 732 N.E.2d 1212, 1216-17 (Ind.2000) (emphasis added). The plaintiffs' complaint also alleges that ONB has breached an implied contract. Compensable damages are an element of a breach of contract cause of action as well. See McCalment v. Eli Lilly & Co., 860 N.E.2d 884, 894 (Ind. Ct.App.2007).

As this case comes to us, both the negligence and the contractual issues can be resolved, and the judgment of the district court affirmed, if the district court was correct in its determination that Indiana law would not permit recovery for credit monitoring costs incurred by the plaintiffs. We review de novo the district court's determination of the content of state law. Hinc v. Lime-O-Sol Co., 382 F.3d 716, 720 (7th Cir.2004); see also Salve Regina Coll. v. Russell, 499 U.S. 225, 231-32, 111 S.Ct. 1217, 113 L.Ed.2d 190 (1991) (rejecting a rule of deference to district court determinations of state law). We must determine whether Indiana would consider that the harm caused by identity information exposure, coupled with the attendant costs to guard against identity theft, constitutes an existing compensable injury and consequent damages required to state a claim for negligence or for breach of contract. Neither the parties' efforts nor our own have identified any Indiana precedent addressing this issue. Nor have we located the decision of any court (other than the district court in this case) that examines Indiana law in this context. We are charged with predicting, nevertheless, how we think the Supreme Court of Indiana would decide this issue. See Dumas v. Infinity Broad. Corp., 416 F.3d 671, 680 n. 11 (7th Cir.2005).

When faced with a novel question of state law, federal courts sitting in diversity have a range of tools at their disposal. First, when the intermediate appellate courts of the state have spoken to the issue, we shall give great weight to their determination about the content of state law, absent some indication that the highest court of the state is likely to deviate from those rulings. See Woidtke v. St. Clair County, Illinois, 335 F.3d 558, 562 (7th Cir.2003). We also shall consult a variety of other sources, including other "relevant state precedents, analogous decisions, considered dicta, scholarly works, and any other reliable data tending convincingly to show how the highest court in the state would decide the issue at hand." McKenna v. Ortho Pharm. Corp., 622 F.2d 657, 663 (3d Cir.1980); see generally Dolores K. Sloviter, A Federal Judge Looks at Diversity Jurisdiction, 78 Va. L.Rev. 1671 (1992) (discussing the challenges facing federal courts in applying uncharted areas of state law). In the absence of any authority from the relevant state courts, we also shall examine the reasoning of courts in other jurisdictions addressing the same issue and applying their own law for whatever guidance about the

probable direction of state law they may provide. See Allstate Ins. Co. v. Tozer, 392 F.3d 950, 952 (7th Cir.2004).

In the end, however, the plaintiffs must come forward with some authority to support their view that they have a right to the relief they seek because, as we have stated, we have "limited discretion... with respect to untested legal theories brought under the rubric of state law." A.W. Huss Co. v. Cont'l Cas. Co., 735 F.2d 246, 253 (7th Cir.1984). Without state authority 636*636 to guide us, "[w]hen given a choice between an interpretation of [state] law which reasonably restricts liability, and one which greatly expands liability, we should choose the narrower and more reasonable path (at least until the [state] Supreme Court tells us differently).". Todd v. Societe Bic, S.A., 21 F.3d 1402, 1412 (7th Cir.1994) (en banc); see also Insolia v. Philip Morris Inc., 216 F.3d 596, 607 (7th Cir.2000) ("Federal courts are loathe to fiddle around with state law. Though district courts may try to determine how the state courts would rule on an unclear area of state law, district courts are encouraged to dismiss actions based on novel state law claims."); Home Valu, Inc. v. Pep Boys, 213 F.3d 960, 965 (7th Cir.2000) (adopting an interpretation of state law which, between two possible options, "take[s] the approach that is restrictive of liability").[5] With these principles in mind, we turn to our consideration of whether Indiana would recognize a cause of action for a data exposure injury. Specifically, we shall examine whether Indiana would compensate victims who undertake credit monitoring to guard against identity theft that might follow.

1.

We begin our inquiry with the Indiana authority most closely addressed to the issue before us. On March 21, 2006, the Indiana legislature enacted a statute that applies to certain database security breaches. Specifically, the statute creates certain duties when a database in which personal data, electronically stored by private entities or state agencies, potentially has been accessed by unauthorized third parties. I.C. § 24-4.9 et seq.[6] The statute took effect on July 1, 2006, see Ind. Pub.L. 125-2006, § 6 (Mar. 21, 2006), after the particular incident involved in this case; neither party contends that the statute is directly applicable to the present dispute.[7] 637*637 We nevertheless find this enactment by the Indiana legislature instructive in our evaluation of the probable approach of the Supreme Court of Indiana to the allegations in the present case.

The provisions of the statute applicable to private entities storing personal information require only that a database owner disclose a security breach to potentially affected consumers; they do not require the database owner to take any other affirmative act in the wake of a breach. If the database owner fails to comply with the only affirmative duty imposed by the statute — the duty to disclose — the statute provides for enforcement only by the Attorney General of Indiana. It creates no private right of action against the database owner by an affected customer. It imposes no duty to compensate affected individuals for inconvenience or potential harm to credit that may follow.[8]

The plaintiffs maintain that the statute is evidence that the Indiana legislature believes that an individual has suffered a compensable injury at the moment his personal information is exposed because of a security breach. We cannot accept this view. Had the Indiana legislature intended that a cause of action should be available against a database owner for failing to protect adequately personal information, we believe that it would have made some more definite statement of that intent. Moreover, given the novelty of the legal questions posed by information exposure and theft, it is unlikely that the legislature intended to sanction the development of

common law tort remedies that would apply to the same factual circumstances addressed by the statute. The narrowness of the defined duties imposed, combined with state-enforced penalties as the exclusive remedy, strongly suggest that Indiana law would not recognize the costs of credit monitoring that the plaintiffs seek to recover in this case as compensable damages.

2.

The plaintiffs further submit that cases decided by the Indiana courts in analogous areas of the law instruct that they suffered an immediate injury when their information was accessed by unauthorized third parties. Specifically, the plaintiffs claim that Indiana law acknowledges special duties on the part of banks to prevent the disclosure of the personal information of their customers; they further claim that Indiana courts have recognized explicitly 638*638 the significant harm that may result from a failure to prevent such a loss. See Indiana Nat'l Bank v. Chapman, 482 N.E.2d 474 (Ind.Ct.App.1985); American Fletcher Nat'l Bank & Trust Co. v. Flick, 146 Ind.App. 122, 252 N.E.2d 839 (1969). In Indiana National Bank v. Chapman, 482 N.E.2d 474 (Ind.Ct.App.1985), the Court of Appeals of Indiana considered a claim that, in the course of an investigation into possible financial motives for an arson, the bank, intentionally and without authorization, had disclosed to law enforcement that an account of one of its customers had been marked for repossession. The court held that the bank had contracted impliedly with its customers not to reveal financial information to law enforcement, absent a public duty. Id. at 482. In American Fletcher National Bank & Trust Co. v. Flick, 146 Ind.App. 122, 252 N.E.2d 839 (1969), the Court of Appeals considered liability based on a bank's erroneous dishonor of a customer's check when a third-party attempted to cash it. The appellate court concluded that the plaintiff, whose creditors had been told that the plaintiff's business account had insufficient funds to cover the checks the plaintiff had written, had suffered a presumptive present harm to his business reputation and credit. Id. at 846.

Whatever these cases say about the relationship of banks and customers in Indiana, they are of marginal assistance to us in determining whether the present plaintiffs are entitled to the remedy they seek as a matter of Indiana law. The reputational injuries suffered by the plaintiffs in American Fletcher and Indiana National Bank were direct and immediate; the plaintiffs sought to be compensated for that harm, rather than to be reimbursed for their efforts to guard against some future, anticipated harm. We therefore do not believe that the factual circumstances of the cases relied on by the plaintiffs are sufficiently analogous to the circumstances that we confront in the present case to instruct us on the probable course that the Supreme Court of Indiana would take if faced with the present question.[9]

Although not raised by the parties, we separately note that in the somewhat analogous context of toxic tort liability,[10] the 639*639 Supreme Court of Indiana has suggested that compensable damage requires more than an exposure to a future potential harm. Specifically, in AlliedSignal, Inc. v. Ott, 785 N.E.2d 1068 (Ind.2003), the Supreme Court of Indiana held that no cause of action accrues, despite incremental physical changes following asbestos exposure, until a plaintiff reasonably could have been diagnosed with an actual exposure-related illness or disease. Id. at 1075. In its decision that no compensable injury occurs at the time of exposure, the court relied on precedent from both state and federal courts in general agreement with the principle that exposure alone does not give rise to a legally cognizable injury. Id. at 1075 n. 8.

Although some courts have allowed medical monitoring damages to be recovered or have created a special cause of action for medical monitoring under similar circumstances, see

Badillo v. American Brands, Inc., 117 Nev. 34, 16 P.3d 435, 438-39 & nn. 1-2 (2001) (citing cases interpreting the law of seventeen states to allow medical monitoring in some form), no authority from Indiana is among them. Indeed, its recent holding in AlliedSignal indicates a contrary approach. To the extent the decision of the Supreme Court of Indiana in that matter provides us with guidance on the likely approach that court would adopt with respect to the information exposure injury in this case, we think it supports the view that no cause of action for credit monitoring is available.[11]

3.

Finally, without Indiana guidance directly on point, we next examine the reasoning of other courts applying the law of other jurisdictions to the question posed by this case. Allstate Ins. Co., 392 F.3d at 952. In this respect, several district courts, applying the laws of other jurisdictions, have rejected similar claims on their merits. In addition to those cases in which the district court held that the plaintiff lacked standing,[12] a series of cases has rejected information security claims on their merits. Most have concluded that the plaintiffs have not been injured in a manner the governing substantive law will recognize. See, e.g., Kahle v. Litton Loan Servicing, LP, 486 F.Supp.2d 705, 712-13 (S.D.Ohio 2007) (entering summary judgment for the defendant because the plaintiff had failed to demonstrate an injury); Guin v. Brazos Higher Educ. Serv. Corp., Inc., 2006 WL 288483 (D.Minn. Feb.7, 2006) (unpublished) (same); Stollenwerk v. Tri-West Healthcare Alliance, 2005 WL 2465906, at *5 (D.Ariz. Sept.6, 2005) (unpublished) (granting summary judgment for defendants because the plaintiffs had failed to provide evidence of injury); see also Hendricks v. DSW Shoe Warehouse, 444 F.Supp.2d 775, 783 (W.D.Mich.2006) (dismissing an action where "[t]here is no existing Michigan statutory or case law authority to support plaintiff's position that the purchase of credit monitoring constitutes either actual damages or a cognizable loss").

Although some of these cases involve different types of information losses, all of the cases rely on the same basic premise: Without more than allegations of increased risk of future identity theft, the plaintiffs have not suffered a harm that the law is prepared to remedy. Plaintiffs have not come forward with a single case or statute, 640*640 from any jurisdiction, authorizing the kind of action they now ask this federal court, sitting in diversity, to recognize as a valid theory of recovery under Indiana law. We decline to adopt a "substantive innovation" in state law, Combs v. Int'l Ins. Co., 354 F.3d 568, 578 (6th Cir.2004), or "to invent what would be a truly novel tort claim" on behalf of the state, Insolia, 216 F.3d at 607, absent some authority to suggest that the approval of the Supreme Court of Indiana is forthcoming. See Todd, 21 F.3d at 1412 (noting that federal courts should be wary of broadening untested theories of liability under state law); see also Insolia, 216 F.3d at 607 (noting that we would neither recognize independently nor certify a question to the state regarding "every creative but unlikely state cause of action that litigants devise from a blank slate"); Birchler v. Gehl Co., 88 F.3d 518, 521 (7th Cir.1996) (favoring narrow interpretation of undecided issues of liability under state law); Ry. Express Agency, Inc. v. Super Scale Models, Ltd., 934 F.2d 135, 138 (7th Cir.1991) (noting that "recent opinions of this court have strongly encouraged district courts to dismiss actions based on novel state law claims").

In sum, all of the interpretive tools of which we routinely make use in our attempt to determine the content of state law point us to the conclusion that the Supreme Court of Indiana would not allow the plaintiffs' claim to proceed.

Conclusion

Because we conclude that the damages that the plaintiffs seek are not compensable as a matter of Indiana law, we affirm the judgment of the district court.

AFFIRMED

[1] The plaintiffs have waived review of the district court's order on their claims for negligent infliction of emotional distress. See Appellants' Br. at 9 n. 4.

[2] See Randolph v. ING Life Ins. & Annuity Co., 486 F.Supp.2d 1, 10 (D.D.C.2007); Bell v. Acxiom Corp., 2006 WL 2850042, at *2 (E.D.Ark. Oct.3, 2006) (unpublished); Key v. DSW, Inc., 454 F.Supp.2d 684, 690 (S.D.Ohio 2006); Giordano v. Wachovia Sec., LLC., 2006 WL 2177036, at *5 (D.N.J. July 31, 2006) (unpublished).

[3] See, e.g., Denney v. Deutsche Bank AG, 443 F.3d 253, 264-65 (2d Cir.2006) (stating, in dicta, that exposure to toxic substances creates a cognizable injury for standing purposes, "even though exposure alone may not provide sufficient ground for a claim under state tort law"); Sutton v. St. Jude Med. S.C., Inc., 419 F.3d 568, 574-75 (6th Cir.2005) (holding that standing was present where a defective medical implement presented an increased risk of future health problems); Cent. Delta Water Agency v. United States, 306 F.3d 938, 947-48 (9th Cir.2002) (holding that "the possibility of future injury may be sufficient to confer standing on plaintiffs" and concluding that the suit could proceed when the plaintiffs demonstrated a factual issue about "whether they suffer a substantial risk of harm"); Friends of the Earth, Inc. v. Gaston Copper Recycling Corp., 204 F.3d 149, 160 (4th Cir. 2000) (en banc) ("Threats or increased risk thus constitutes cognizable harm.").

[4] See Lac Du Flambeau Band of Lake Superior Chippewa Indians v. Norton, 422 F.3d 490, 498 (7th Cir.2005) ("[T]he present impact of a future though uncertain harm may establish injury in fact for standing purposes."); Johnson v. Allsteel, Inc., 259 F.3d 885, 888 (7th Cir.2001) (holding that an ERISA plan administrator's increased discretion increased risk that the participant would be denied benefits and that "[t]he increased risk the participant faces as a result is an injury-in-fact" for standing purposes); Vill. of Elk Grove Vill. v. Evans, 997 F.2d 328, 329 (7th Cir.1993) ("[E]ven a small probability of injury is sufficient to create a case or controversy — to take a suit out of the category of the hypothetical — provided of course that the relief sought would, if granted, reduce the probability.").

[5] We have applied this restrictive approach to a plaintiff's novel theory of liability under state law even where the plaintiff had no choice but to litigate his claim in federal court. Insolia v. Philip Morris Inc., 216 F.3d 596, 607 (7th Cir.2000) (noting that even where "state law ... is stunted by the ability of [defendants] to remove cases under diversity jurisdiction .... that does not justify the federal courts imposing a new tort claim" on a state).

[6] For present purposes, it will suffice to note the relevant substantive provisions added to the Indiana Code by § 6 of Public Law 125-2006 (Mar. 21, 2006), codified at I.C. § 24-4.9 et seq.:

(a) Except as provided in section 4(c), 4(d), and 4(e) of this chapter, after discovering or being notified of a breach of the security of a system, the data base owner shall disclose the breach to an Indiana resident whose:

(1) unencrypted personal information was or may have been acquired by an unauthorized person; or

(2) encrypted personal information was or may have been acquired by an unauthorized person with access to the encryption key;

if the data base owner knows, should know, or should have known that the unauthorized acquisition constituting the breach has resulted in or could result in identity deception (as defined in IC XX-XX-X-X.5), identity theft, or fraud affecting the Indiana resident.

(b) A data base owner required to make a disclosure under subsection (a) to more than one thousand (1,000) consumers shall also disclose to each consumer reporting agency (as defined in 15 U.S.C. 1681a(p)) information necessary to assist the consumer reporting agency in preventing fraud, including personal information of an Indiana resident affected by the breach of the security of a system.

I.C. § 24-4.9-3-1 (eff. July 1, 2006).

[7] "As a general rule, the law in place at the time an action is commenced governs. Unless a contrary intention is expressed, statutes are treated as intended to operate prospectively, and not retrospectively." Indiana Dep't of Envtl. Mgmt. v. Med. Disposal Servs., Inc., 729 N.E.2d 577, 581 (Ind.2000) (internal quotation marks and citation omitted).

[8] The Act provides as the exclusive remedy an action by the Attorney General against the database owner:

A person that is required to make a disclosure or notification in accordance with IC 24-4.9-3 and that fails to comply with any provision of this article commits a deceptive act that is actionable only by the attorney general under this chapter.

I.C. § 24-4.9-4-1(a) (emphasis added).

In such an action, the statute provides that the Attorney General may obtain an injunction against future violations, a civil penalty of not more than $150,000 per deceptive act and the Attorney General's reasonable costs in investigating the act and maintaining the action. Id. § 24-4.9-4-2; see also Joanna L. Grama & Scott L. Ksander, Recent Indiana legislation hopes to stem release of personally identifying information, Res Gestae, Nov. 2006, 35 at 39 ("[B]oth new Ind.Code § 24-4.9 (private entities) and Ind.Code § 4-1-11 (state agencies) offer no remedy to those persons whose information was obtained by an unauthorized person as a result of a security breach, other than that those persons be informed of the breach." (emphasis added)); id. at 42 n. 65 ("Of course, in a subsequent criminal action against the unauthorized person who acquired the personal information, a trial court could order restitution for victims. See Ind.Code § 35-50-2-2.3(a)(5)." (emphasis added)).

[9] The plaintiffs also contend that Article I, Section 12 of the Indiana Constitution requires courts to fashion common law remedies in all circumstances, for any harm alleged. That section provides, in pertinent part, that "every person, for injury done to him in his person, property, or reputation, shall have remedy by due course of law." Indiana Const. Art. I, § 12. We are aware of no precedent from Indiana in which this provision was held to mandate a damages remedy in a suit by one citizen against another whenever the plaintiff claims that he has been "injured."

Indeed, as the Supreme Court of Indiana recently has observed, "Article I, Section 12 does not specify any particular remedy for any particular wrong. Rather, it leaves the definition of wrongs and the specification of remedies to the legislature and the common law." Cantrell v. Morris, 849 N.E.2d 488, 499 (Ind.2006) (emphasis added). As we read this provision in light of Indiana precedent, it does not appear to command that the plaintiffs in this case have a present, viable right of action.

[10] See generally Vincent R. Johnson, Cybersecurity, Identity Theft, and the Limits of Tort Liability, 57 S.C. L.Rev. 255, 305-11 (2005) (noting the propriety of the analogy between toxic torts and cybersecurity breaches). We need not endorse this analogy for present purposes. We merely note that, to the extent the analogy is apt, it does not support the view that Indiana tort law recognizes costs of monitoring as a compensable damage. Even in jurisdictions where medical monitoring has been acknowledged as a compensable damage, courts still have expressed doubt that credit monitoring also should be compensable. See Kahle v. Litton Loan Servicing, LP, 486 F.Supp.2d 705, 712 (S.D.Ohio 2007); Key, 454 F.Supp.2d at 691.

[11] See also Hendricks v. DSW Shoe Warehouse, Inc., 444 F.Supp.2d 775, 783 (W.D.Mich.2006) (dismissing a case where no Michigan authority supported an action for credit monitoring and where Michigan had considered and rejected a cause of action for medical monitoring).

[12] See note 2, supra.

Electronic Privacy Info. Ctr. v. National Security Agency, 678 F. 3d 926, 930-33 (D.C. Cir. 2012)

Following a January 2010 cyber attack on Google that primarily targeted the Gmail accounts of Chinese human rights activists, Google changed Gmail's privacy settings to automatically encrypt all traffic to and from its servers. Gmail is a "cloud-based" email program through which the data and applications of the user reside on remote computer servers operated by Google. Prior to this cyber attack, Google had allowed Gmail users to encrypt the mail that passed through Google servers using Hypertext Transfer Protocol Secure (HTPS), but did not provide encryption by default.

According to the Wall Street Journal and Washington Post, Google contacted the National Security Agency immediately after the cyber attack. Such collaboration between the NSA and private companies like Google was “inevitable,” according to the former director of the NSA. EPIC claimed that collaboration between Google and NSA was widely reported in the national media and acknowledged by the former director of the NSA was similarly unavailing. NSA never never officially acknowledged a collaborative relationship with Google.

Electronic Privacy Information Center ("EPIC") filed a FOIA request with the National Security Agency ("NSA") seeking disclosure of any communications between NSA and Google, Inc. regarding encryption and cyber security, including records in these categories:

1. All records concerning an agreement or similar basis for collaboration, final or draft, between the NSA and Google regarding cyber security;
2. All records of communication between NSA and Google concerning Gmail, including but not limited to Google's decision to fail to routinely encrypt Gmail messages prior to the cyber attack;

3. All records of communications regarding NSA's role in Google's decision regarding the failure to routinely deploy encryption for cloud-based computing service, such as Google Docs.

NSA responded to EPIC's request by issuing a Glomar response, in which the agency neither confirmed nor denied the existence of any responsive records. NSA's response was upheld on summary judgment. A Glomar response is named after Hughes Glomar Explorer, "a ship built to recover a sunken Soviet submarine, but disguised as a private vessel for mining manganese nodules from the ocean floor." Bassiouni v. CIA, 392 F.3d 244, 246 (7th Cir.2004). NSA issued a Glomar response to EPIC's request for records pertaining to the agency's contact with Google, claiming that any responsive records would be exempt from disclosure under applicable exemptions of the National Security Agency Act, and that acknowledgement of the existence of such records would cause harm cognizable under the exemption.

EPIC filed suit in the district court challenging NSA's Glomar response, specifically challenging NSA's claim that the protected information sought by EPIC pertained to NSA's organization, functions, or activities. Elec. Privacy Info. Ctr. v. NSA, 798 F.Supp.2d 26, 31-32 (D.D.C. 2011).

In its de novo review of the district court's grant of summary judgment, the D.C. Circuit found that under FOIA, an agency in addition to withholding records that are exempt may issue a Glomar response, in which it refuses to confirm or deny the existence or nonexistence of responsive records if the particular FOIA exemption at issue would itself preclude the acknowledgement of such documents. NSA issued the Glomar response since to answer the FOIA inquiry would cause harm cognizable under an applicable statutory exemption, and even acknowledging the mere existence of responsive records would disclose exempt information.

EPIC argued that it was seeking nonexempt unsolicited communications from Google to NSA, but the court reasoned that that "if NSA disclosed whether there are (or are not) records of a partnership or communications between Google and NSA regarding Google's security, that disclosure might reveal whether NSA investigated the threat, deemed the threat a concern to the security of U.S. Government information systems, or took any measures in response to the threat." On this basis, the court found that information pertaining to the relationship between Google and NSA would reveal protected information about NSA's implementation of its Information Assurance mission and that even if EPIC was correct that NSA possessed records revealing information only about Google, "those records, if maintained by the agency, are evidence of some type of interaction between the two entities, and thus still constitute an NSA "activity" undertaken as part of its Information Assurance mission, a primary "function" of the NSA." Further, according to the court, "if private entities knew that any of their attempts to reach out to NSA could be made public through a FOIA request, they might hesitate or decline to contact the agency, thereby hindering its Information Assurance mission."

EPIC also argued that any insistence on secrecy in intelligence gathering did not apply to the NSA's Information Assurance mission "because it is public knowledge that the U.S. government uses Google applications and that NSA is investigating security vulnerabilities in Google's commercial products." The court rejected this argument, reasoning the NSA's determination that certain security vulnerabilities in Google technologies pose (or do not pose) a risk to the government's information systems constituted an "activity" of the agency, as did a relationship between the agency and Google.

Agility Public Warehousing Company KSV v. NSA, Civil Action No. (BAH) 14-0946 (D. D.C. July 10, 2015), concerned a FOIA request by Agility, a Kuwaiti logistics company that provided food to U.S. troops stationed in Iraq, Kuwait, Qatar, and Jordan from 2003 through 2010, as part of a series of contracts with the Defense Logistics Agency. This case presented multiple competing interests all of significant public concern, including personal privacy, national security, and transparency in government, along with the related concern of ensuring agency accountability.

After Agility was indicted for conspiracy to defraud the U.S. and wire fraud stemming from its provision of goods under these contracts, and after it was also sued under the False Claims Act for violations stemming from its provision of goods to U.S. soldiers, Agility filed its FOIA request. In its request, Agility sought from the NSA "all [of the] email, letter, telephonic, or other communications" of Agility in the NSA's possession, arguing that NSA had indiscriminately collected millions of telephone and e-mail communications from U.S. citizens and maintained records of Agility's historical communications. The NSA issued a "Glomar" response, neither confirming nor denying the existence of records responsive to Agility's request.

Agility's FOIA request to the NSA sought several categories of documents, including (1) all e-mail, letter, telephonic, or other communications by Agility; (2) the name of any U.S. or foreign communications provider that intercepted Agility's communications; (3) documents relating to two contracts between the plaintiff and the Defense Supply Center; (4) documents relating to the two lawsuits brought against Agility; (5) all communications between the NSA and any other investigative or law enforcement agency regarding Agility; (6) documents pertaining to meetings among employees or contractors of any of the Department of Justice, the Office of the Director of National Intelligence, and the NSA regarding Agility; and (7) documents pertaining to meetings between employees or contractors of the NSA and employees or contractors of the Federal Bureau of Investigation, the Central Intelligence Agency, the Department of Defense, and the Department of Homeland Security, relating to Agility.

Granting the NSA's motion for summary judgment, the court found that in defending against these charges, Agility had made extensive use of e-mail and telephone communications to communicate from Kuwait with its U.S.-based attorneys. It further found that while Agility and the NSA exchanged communications clarifying the scope of Agility's FOIA request, the NSA never provided a response to Agility prior to this litigation. This appeal to the district court resulted from the NSA's constructive denial of Agility's FOIA request.

The court found that the NSA had officially acknowledged the collection of certain telephony metadata from Verizon Business Network Services but had not otherwise officially acknowledged its possession of any other records sought by Agility, and that "[t]o require the NSA to acknowledge the existence or non-existence of materials beyond that limited period would require the NSA to acknowledge information that has not otherwise been publically disclosed."

The court also found that Agility had made no showing of public disclosures of any of the other electronic communications programs, including the PR/TT program, the PRISM program, and the upstream collection program. On the contrary, Agility had conceded that the NSA has not acknowledged a service provider with respect to the bulk collection of electronic communications and thus failed in its burden to overcome the NSA's Glomar response with respect to all other electronic communications programs.

In Remijas v. The Neiman Marcus Group, No. 14 C 1735 (N.D. Ill. 2014), cyber hackers breached several Neiman Marcus servers, resulting in the potential disclosure of 350,000 customers' payment card data and personally identifiable information. Following the breach, at least 9200 of the affected payment cards were used fraudulently elsewhere. Among the 350,000 customers were plaintiffs, who brought this action against Neiman Marcus for failing to adequately protect against such a security breach, and for failing to provide timely notice of the breach once it happened. Their suit included claims of negligence, breach of implied contract, unjust enrichment, unfair and deceptive business practices, invasion of privacy, and violation of several state data breach acts.

Neiman Marcus argued that none of the asserted injuries sufficed to confer Article III standing on the plaintiffs, including exposure to an increased risk of future fraudulent credit card charges, an increased risk of identity theft, loss of time and money associated with resolving fraudulent charges, the loss of time and money associated with protecting against the risk of future identity theft, the financial loss from having purchased products that the plaintiffs would not have otherwise purchased had they known of the alleged misconduct, and the loss of control over and value of their private information.

In addressing the standing issue, the district court found that “the overwhelming majority of the plaintiffs allege only that their data may have been stolen,” in contrast to about 2.5 % of the customers who actually had fraudulent charges appear on their credit cards and whose date were actually stolen and actually misused. It was unclear to the court that such "fraudulent charge" injury alleged to have been incurred by the 9,200 customers was an injury sufficient to confer standing, in the sense that the present and future injuries must be concrete. There were no unauthorized credit card charges for which any of the plaintiffs were financially responsible and hence none could qualify as "concrete" injuries. The court concluded that without a more detailed description of some fairly substantial attendant hardship, it could not agree with Plaintiffs that such "injuries" confer Article III standing.

Further, the court was not persuaded that the 350,000 customers at issue were at a certainly impending risk of identity theft. First, the plaintiffs did not allege that data belonging to all of the customers at issue were in fact stolen, but that approximately 2.5% of the customers at issue saw fraudulent charges on their credit cards, supporting a strong inference that those customers' data were stolen as a result of the Neiman Marcus data breach. Second, while accepting the inference from this that additional customers were at a "certainly impending" risk of future fraudulent charges on their credit cards, it was “a leap too far” to assert on this basis that either set of customers was also at a certainly impending risk of identity theft. Accordingly, the court concluded that the complaint did not adequately allege standing on the basis of increased risk of future identity theft.

Data Breaches, Identity Theft and Article III Standing: Will the Supreme Court Resolve the Split in the Circuits?
Bradford C. Mank, (Copyright 2015)1; Draft Do Not Quote or Cite Without Express Permission
Accepted for Publication in 92 NOTRE DAME L. REV. (forthcoming 2016)
Abstract
In data breach cases, the plaintiff typically alleges that the defendant used inadequate computer security to protect the plaintiff's personal data. In most, but not all cases, the plaintiff cannot prove that a hacker or thief has actually used or sold the data to the plaintiff's detriment. In most cases, a plaintiff alleges that the defendant's failure to protect their personal data has caused them damages by increasing their risk of suffering actual identity theft in the future and therefore imposed costs on the plaintiff when he reasonably takes measures to prevent future unauthorized third-party data access by purchasing credit monitoring services.
In data breach cases, the lower federal courts have split on the question of whether the plaintiffs meet Article III standing requirements for injury and causation. In its 2013 decision Clapper v. Amnesty International USA, the Supreme Court, in a case involving alleged electronic surveillance by the U.S. government's National Security Agency, declared that a plaintiff alleging that it will suffer future injuries from a defendant's allegedly improper conduct must show that such injuries are "certainly impending." Since the Clapper decision, a majority of the lower federal courts addressing "lost data" or potential identity theft cases in which there is no proof of actual misuse or fraud have held that plaintiffs lack standing to sue the party who failed to protect their data. But a significant minority of lower court decisions have disagreed that the Clapper decision requires denial of standing in data breach cases in which there is no proof of present harm because a footnote in Clapper acknowledged that the Court had sometimes used a less strict "substantial risk" test when plaintiffs allege that a defendant's actions increase their risk of future harm.

Currently, there is no comprehensive federal statute addressing data breach issues so plaintiffs have invoked a variety of state and federal laws to sue defendant companies that have failed to protect the plaintiffs' data.11 For example, some of the cases are brought under state common law negligence or breach of contract theories, and others pursuant to federal statutes such as the Fair Credit Reporting Act.12 A related issue is where a defendant has allegedly falsely reported information about a plaintiff to third parties in violation of various federal statutes, but it is difficult to measure the actual harm to the plaintiff.13

Protecting water and wastewater infrastructure from cyber attacks
Srinivas Panguluri , William Phillips, John Cusimano

Abstract
Multiple organizations over the years have collected and analyzed data on cyber attacks and they all agree on one conclusion: cyber attacks are real and can cause significant damages. This paper presents some recent statistics on cyber attacks and resulting damages. Water and wastewater utilities must adopt countermeasures to prevent or minimize the damage in case of such attacks.
Many unique challenges are faced by the water and wastewater industry while selecting and implementing security countermeasures; the key challenges are: 1) the increasing interconnection of their business and control system networks, 2) large variation of proprietary industrial control equipment utilized, 3) multitude of cross-sector cyber-security standards, and 4) the differences in the equipment vendor's approaches to meet these security standards. The

utilities can meet these challenges by voluntarily selecting and adopting security standards, conducting a gap analysis, performing vulnerability/risk analysis, and undertaking countermeasures that best meets their security and organizational requirements.
Utilities should optimally utilize their limited resources to prepare and implement necessary programs that are designed to increase cyber-security over the years. Implementing cyber security does not necessarily have to be expensive, substantial improvements can be accomplished through policy, procedure, training and awareness. Utilities can also get creative and allocate more funding through annual budgets and reduce dependence upon capital improvement programs to achieve improvements in cyber-security.

Government Information Quarterly
2004, Vol.21(4):406–419, doi:10.1016/j.giq.2004.08.002

Electronic government: Government capability and terrorist resource ☆

L. Elaine Halchin

Abstract
The federal government's war on terrorism has heightened understanding and appreciation of the many facets of electronic government. Electronic government is used as a resource in the war on terrorism, helping to prevent and prepare for attacks. It might also prove useful in recovering from attacks. Unfortunately, e-government itself is a likely target for terrorists. Cyber intrusions into government Web sites and damage to, or destruction of, infrastructure, whether a computer system or an electrical grid that supplies power, could impair e-government. E-government is also attractive as a potential target for the information it provides, information that enemies of the United States could use in identifying weaknesses and planning attacks. While the Bush Administration has developed a comprehensive policy, based on a market model, for facilitating the use and effectiveness of e-government, its approach to e-government security, particularly in the area of Web content, has been ad hoc. Soon after the September 11, 2001, attacks, federal agencies began scrubbing their Web sites, an effort that has implications for the notion, and practice, of having a well-informed citizenry.

A Model for the Impact of Cybersecurity Infrastructure on Economic Development in Emerging Economies: Evaluating the Contrasting Cases of India and Pakistan

Abstract
The possibilities and risks inherent in the dissemination of ICT necessitate implementation of cybersecurity initiatives. Yet, we know very little about the specific relationships between national information infrastructure (NII), cybersecurity capability, and economic development in emerging economies. This paper proposes a model based on national nuclear threat security through which a developing nation could develop an effective cybersecurity infrastructure while simultaneously positively impacting economic development. Our model extends the cybersecurity triad of internal governance, private sector partners and an active cybercitizenry to add a fourth influence – foreign government relations – that significantly impacts socioeconomic development. The model will be elaborated through the lens of two case study nation-states: India and Pakistan

Information, Innovation and the Boogeyman: Contextual Factors that Influence the Canadian Government's Response to Cyberspace Risk

Trevor Fowler (Dalhousie University, Halifax, Nova Scotia, Canada & City of London, Ontario, Canada) and Kevin Quigley (School of Public Administration, Dalhousie University, Halifax, Nova Scotia, Canada)

Volume 1, Issue 2. 19 pages.