

Kate Morris
Attorney
CIPP/US



Tech Talk: Data Privacy and Security

August 16, 2016

Texas Housing Association
Annual Conference and Trade Show

AUSTIN
COLLIN COUNTY
DALLAS
HOUSTON
MEXICO CITY
NEW YORK
SAN ANTONIO
WASHINGTON D.C.

Strasburger
ATTORNEYS AT LAW

Overview

1. Threat landscape
2. Understanding Data Security and Data Privacy
3. Recognizing Key Legal Issues
4. Strategies for Avoiding Liability and Protecting Data
- 5.



1. Threat Landscape



What is vulnerable?



INFORMATION FLOW



DIGITAL UNIVERSE



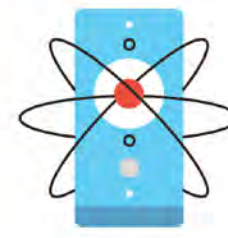
PROCESSING



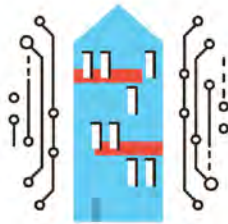
SOCIAL NETWORK



ANALYSIS



SMART TECH



SMART HOUSE



INTERNET OF THINGS



BIG DATA

Kate's Dream House





www.floryday.com

U.S. official blames Russia for power grid attack in Ukraine



By **Evan Perez**, CNN Justice Reporter

Updated 8:27 PM ET, Thu February 11, 2016



Top stories

Water park witness: 'I saw the blood'

Lisa Loeb: '90s were great, but ...

See Our Enterprise Cloud Platform in Action

OPEN DEMO, SEPT. 7 AT 12PM EDT

[RESERVE YOUR SPOT](#)

Advertisement

Story highlights

An Obama official said Russia was behind a December cyber attack on Ukraine's power grid

Elizabeth Sherwood-Randall made the comments to a gathering of electric power grid industry executives

(CNN) — Russia was behind a December cyber attack on Ukraine's power grid that caused widespread power outages, a senior Obama administration official said Thursday.

Elizabeth Sherwood-Randall, deputy Energy Secretary, made the comments to a gathering of electric power grid industry executives, according to an U.S. official familiar with her presentation.

Attack on Electrical Grid Could Collapse Economy

No plan exists to help localities prepare for a lengthy blackout

Posted Jun 1, 2016 3:57 PM

By Rep. Lou Barletta



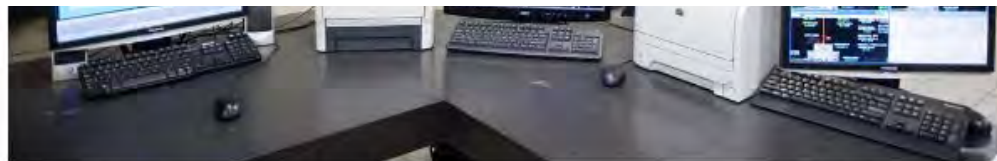
What happened is ominous because it reminded us that we should not believe ourselves immune to such an attack, even in the United States. A cyberattack on the power grid could leave millions of residents and key physical locations without power for an extended period of time. It is a discouraging fact that unlike every other hazard we are likely to face, from hurricanes to earthquakes and chemical attacks to space weather, there is no specific planning scenario to help state and local governments prepare for an extensive blackout.

Buy your tickets today!

Roll Call



#RCNats



The control room at Covanta Energy's resource recovery facility in Alexandria, Va., monitors power generation and pollutants (Bill Clark/CQ Roll Call)

It was like something from a Hollywood movie, but it was real. At about 3:30 p.m. on Dec. 23, a computer in an electricity distribution center in western Ukraine seemed to take on a life of its own. While a helpless worker watched, the cursor on the screen moved by itself and clicked on a box that opened a series of circuit breakers — a move that would take the entire power station offline.

Tech hacking spree: Facebook, Twitter, Google & Oracle breached



Nicholas Monte

August 09, 2016

Stocks (^DJI, ^GSPC, ^IXIC) are up modestly at midday, with consumer staples (XLP) in the green, while energy (XLE) is the only sector in the red. [Stephen Guilfoyle](#), chief market economist at [Stuart Frankel & Co.](#), joins us live from the New York Stock Exchange.

To discuss the other big stories of the day, Alexis Christoforous is joined by Yahoo Finance's Rick Newman and Melody Hahm.

Becoming more and more unproductive

Historically Americans have made more products with fewer materials and labor. But a new trend suggests that workers in the US are increasingly unproductive, making more goods with more materials. What's needed to make the American worker productive again?

Hackers are getting the last laugh

If your password is 1-2-3-4, it's time to change it. Hackers have taken over the past few months, infiltrating even the highest ranking tech CEO accounts. How much does a password breach hurt social media sites in terms of returning users?

Postal workers vs. dogs

Postal worker might be getting added to the list of most dangerous jobs. Dog attacks on these workers jumped 14%. The Postal Service added "trip hazards" to employees' hand-held devices used to scan packages. Why have dog bites to postal workers jumped so much in the last year?

FBI investigating porn display on electronic billboard in Atlanta

Someone hacked into digital boards Saturday morning and put up several images before owner pulled plug

By Associated Press Thu, May 14, 2015 @ 9:24 am

ATLANTA | The FBI is investigating who possibly hacked an electronic billboard after it displayed a pornographic image in Georgia.

WSB-TV reports an electronic advertisement billboard in Buckhead displayed a graphic picture of a man exposing himself among other images Saturday. A driver who saw the image called 911. The woman said there was not an emergency but the image was disgusting.

Police say the billboard's owner temporarily cut power to the billboard, but not before the image had been posted to social media.

Wednesday, an FBI representative told the station agents are trying to determine all of the servers involved in the apparent hacking and their locations.

The president of Georgia's Outdoor Advertising Association says the industry has established protocols to prevent hacking of digital billboards.

undefined

China is spying on you through your KETTLE: Bugs that scan wi-fi devices found in imported kitchen gadgets

- 20 to 30 appliances 'had hidden chips that send out malware to networks'
- Comes as EU probes claims Russia tried to steal data from G20 leaders

By **SIMON TOMLINSON**

PUBLISHED: 06:55 EST, 31 October 2013 | UPDATED: 10:19 EST, 31 October 2013



259
View comments

Russian investigators claim to have found household appliances imported from China which contain hidden microchips that pump spam data and malware into wi-fi networks.

Authorities in St Petersburg allegedly discovered 20 to 30 kettles and irons with 'spy microchips that send some data to the foreign server', according to Russian media.

The revelation comes just as the EU launches an investigation into claims that Russia itself bugged gifts to delegates at last month's G20 summit in an attempt to retrieve data from computers and telephones.



Kitchen espionage: Kettles imported to Russia from China with hidden microchips which can send spam data and possibly steal information have allegedly been found by authorities in St Petersburg

This has led to speculation that the chips allegedly found in the home appliances may also have the ability to steal data and send it back to Chinese servers.

Strasburger
ATTORNEYS AT LAW

APR 29, 2014 @ 12:13 PM 43,360 VIEWS

The Little Black Book of Billionaire Secrets

Baby Monitor Hacker Still Terrorizing Babies And Their Parents



Kashmir Hill
FORBES STAFF

Welcome to *The Not-So Private Parts* where technology & privacy collide

[FULL BIO >](#)

Last summer, someone hacked into a Houston couple's baby monitor in order to yell at their daughter and tell her to "wake up, you little slut." The Gilbert family was using an Internet-connected Foscam product that had known vulnerabilities that would make it easy for a knowledgeable intruder to get into it and control it. (Think Heartbleed.) Foscam released a firmware update that fixed the problem but people like the Gilberts who bought their camera through a reseller did not get the company's email about the fix, and apparently didn't hear about the 'Babybleed' problem. At the time, I wrote that 40,000 other cams were still vulnerable to hacking, according to security researchers. Well, a hacker found one of those



Strasburger
ATTORNEYS AT LAW

IoT

DARPA Wants To Protect Your Refrigerator From Hackers

This system could protect all the IoT devices in your home

f SHARE

t SHARE

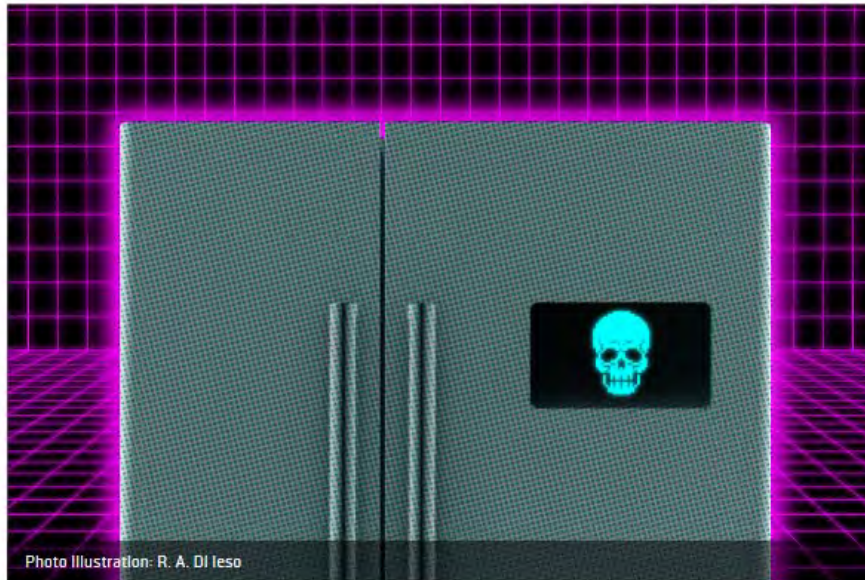


Photo Illustration: R. A. Di Ieso

By Jennings Brown

Aug 09, 2016 at 11:33 AM ET

Medical Devices Vulnerable to Hack Attacks

Security expert and diabetic Jay Radcliffe reveals flaws by hacking into his own insulin pump

By Tammy Leitner and Lisa Capitanini



9/29/2014: We count on medical devices to keep us alive. But not all of those devices are secure -- making it easy for cyber criminals to remotely access them. Tammy Leitner reports for NBC 5 Investigates. (Published Monday, Sept. 29, 2014)

Delivering a lethal dose of insulin, remotely stopping a pacemaker or even administering a deadly shock through a defibrillator are all real possibilities in the world of medical cybercrime, NBC 5 Investigates has found.

HAVE FUN



TREN

1 Gal
Cot

2 vi
Tru

3 We
Tur

Strasburger
ATTORNEYS AT LAW

SHARE



SHARE
1364



TWEET



PIN
7



COMMENT
4



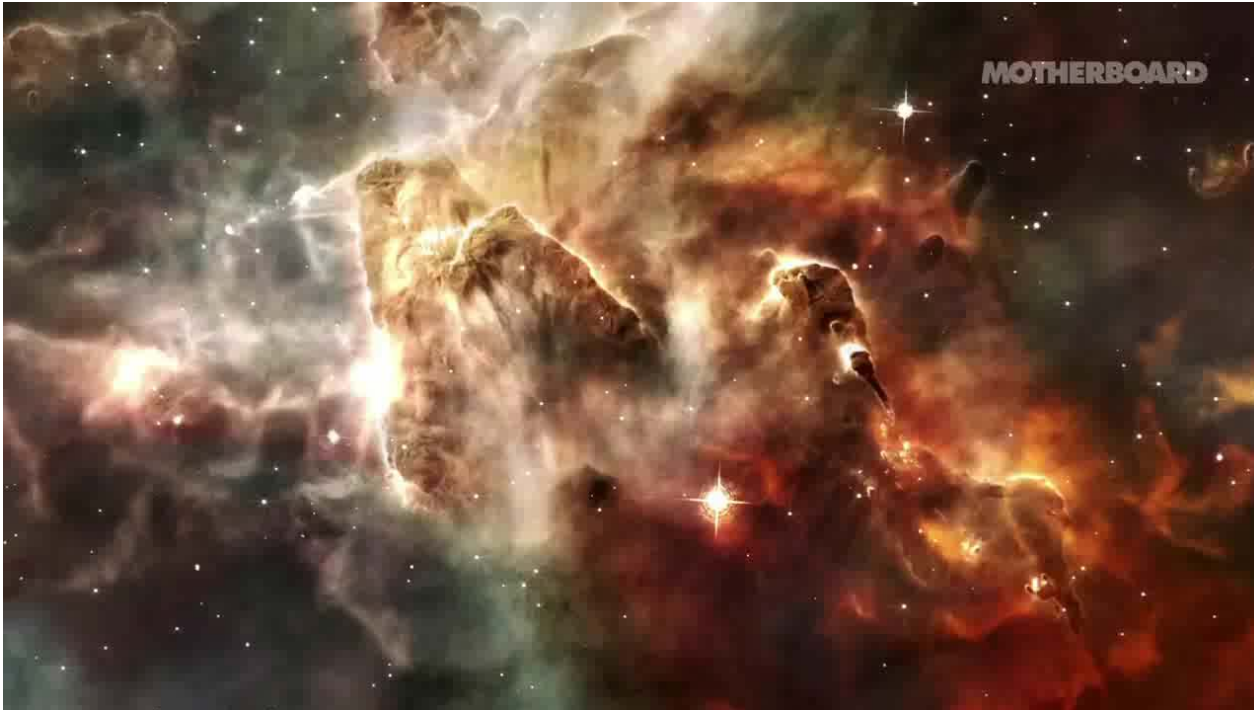
EMAIL

ANDY GREENBERG SECURITY 08.02.16 2:45 PM

HACKERS HIJACK A BIG RIG TRUCK'S ACCELERATOR AND BRAKES



Hackers Remotely Kill a Jeep



MILITARY

SMART RIFLE'S SOFTWARE CAN BE HACKED TO SHOOT OFF-TARGET

THE INTERNET OF THINGS THAT SHOULDN'T BE ONLINE

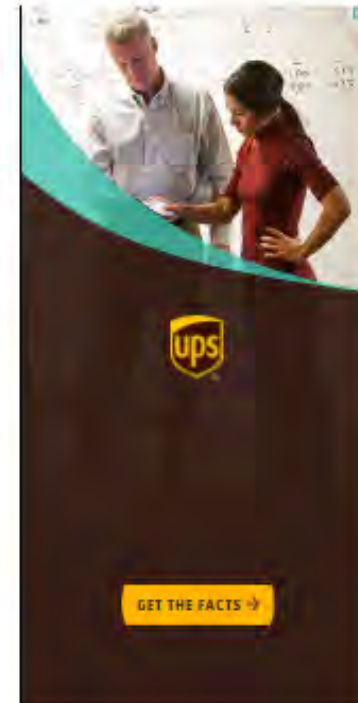
By Kelsey D. Atherton July 29, 2015



Screenshot by author, from YouTube

TrackingPoint Rifle

TrackingPoint's rifles are clever pieces of technology, merging cameras, sensors, and Linux software with a sniper rifle to create a gun very good at hitting targets far away, even when fired by an untrained shooter. Primarily marketed to hunters, last year the U.S. Army was also rumored to be evaluating them. A rifle that relies on software comes with a new risk: it can be hacked. Security researchers and wife-and-husband duo Runa Sandvik and Michael Auger have demonstrated a successful hack, fooling the rifle into software into misdirecting the bullet.



✉ **WANT MORE NEWS LIKE THIS?**

Strasburger
ATTORNEYS AT LAW



Cyber Attack

Cyber Attack

Often times, we may not realize that our actions online might put us, our families, and even our country at risk. Learning about the dangers online and taking action to protect ourselves is the first step in making the Internet a safer place for everyone. Cybersecurity is a shared responsibility and we each have a role to play.



- Individually-owned devices such as computers, tablets, mobile phones, and gaming systems that connect to the Internet are vulnerable to intrusion. Personal information may be at risk without proper security.

> Expand All Sections

> Before A Cyber Attack

> During A Cyber Attack

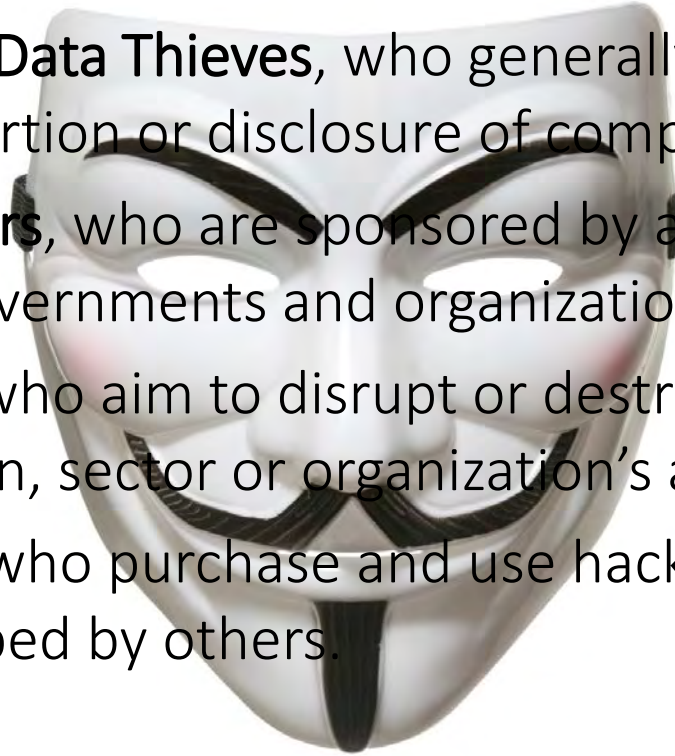
✓ After A Cyber Attack

Who is the Enemy?



HACKER PROFILES

1. **Hacktivists**, who are politically motivated.
2. **Cybercriminals / Data Thieves**, who generally aim to make money through the extortion or disclosure of compromised data;
3. **Nation state actors**, who are sponsored by a nation state to target foreign governments and organizations;
4. **Cyberterrorists**, who aim to disrupt or destroy services that are critical to a nation, sector or organization's activities;
5. **"Script Kiddies"**, who purchase and use hacking tools and malware developed by others.

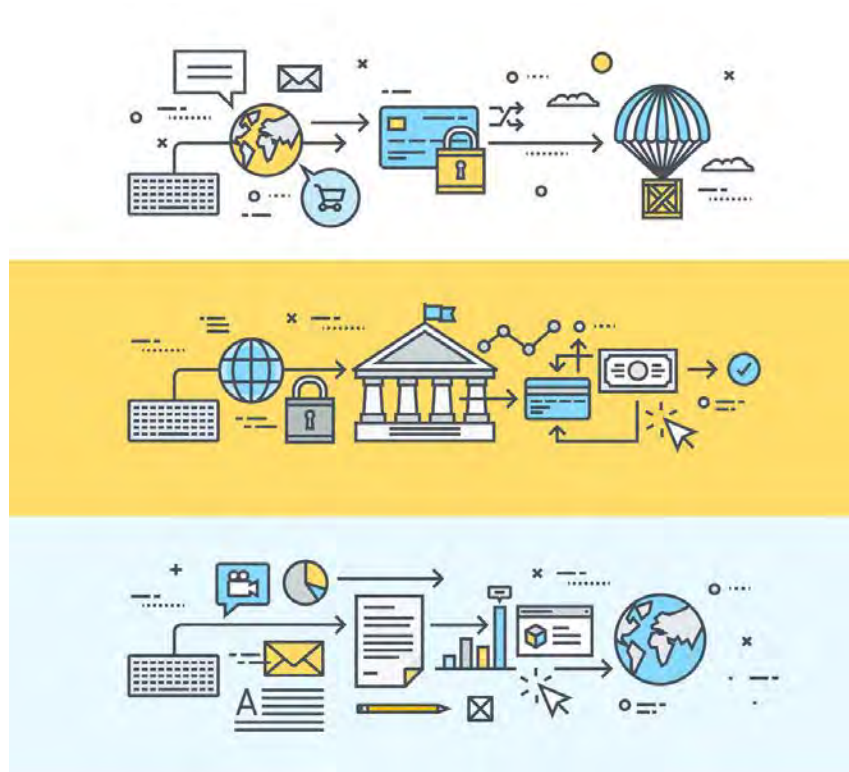


What is at stake?

- Legal risks
- Reputational risks
- Operational risks
- Investment risks



Why is this happening?



Welcome to the Information Economy.

2.

Understanding Data Security and Data Privacy



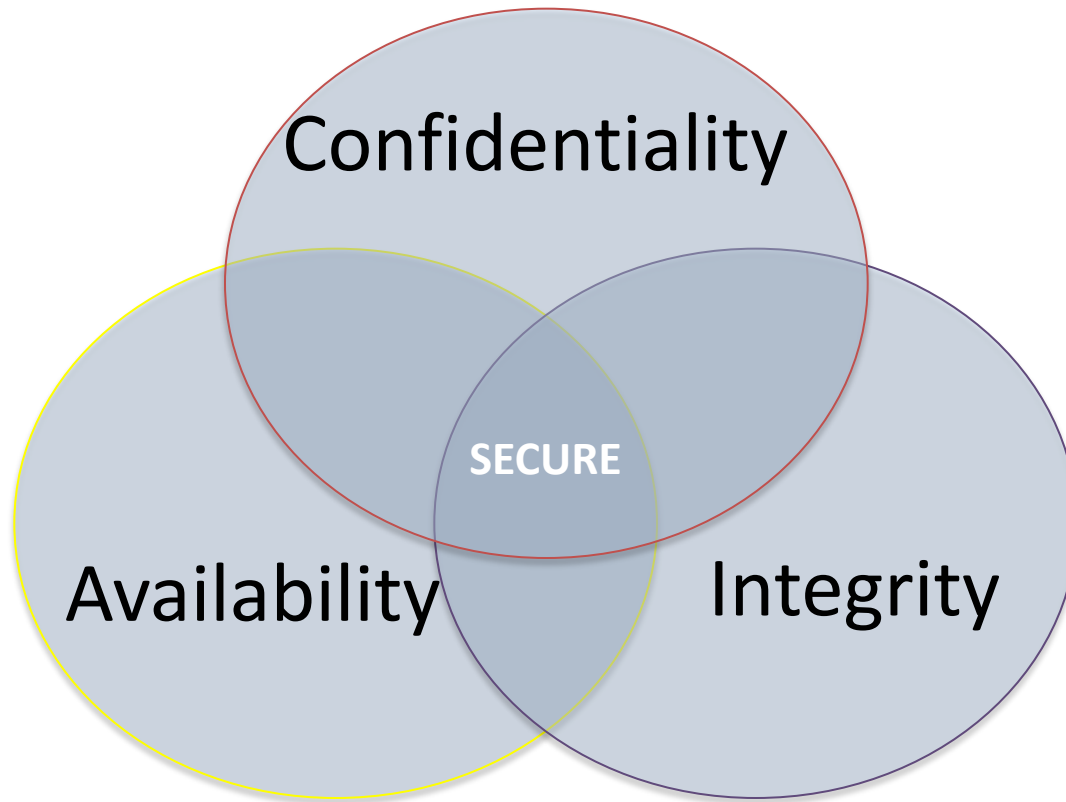
Data Security vs. Data Privacy

Data security =
the confidentiality,
integrity and availability,
of data (CIA Triad)

Data privacy =
the appropriate use of
data



Data Security



THE CIA TRIAD

Data Privacy

- Laws, regulations, guidelines
- Technology-related contracts with third parties
- Privacy policies, Privacy notices and Terms of Use



Laws, Regulations and Guidelines

- International
 - EU Privacy Shield
 - APEC Framework
- Federal Laws (enforced by DOJ, FTC, FCC, SEC, EEOC, NLRB)
 - Children's Privacy (COPPA, CIPA)
 - Consumer Privacy (FTC Act, FCRA, ECPA, CAN-SPAM, VPPA, TCPA, JFPA)
 - Health Privacy (HIPAA, HITECH)
 - Educational Privacy (FERPA)
 - Financial Privacy (GLBA, Red-Flags Rule)
 - Law Enforcement (USA-Patriot Act, CALEA)
- State Law
 - Breach Notification Laws - 47 States (Ala, NM, SD),
 - Marketing laws
 - Data Security Laws (SSN, Data destruction)
 - California SB-1
- Guidelines
 - PCI-DSS
 - ISO 27001



Technology-Related Contracts with Third-Parties

- IT outsourcing agreements.
- Cloud Contracts.
- Enterprise resource planning (ERP) agreements, including infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and software-as-a-service (SaaS) systems.
- Service level agreements Service Level Agreements (SLA) and end-user agreements (EULA) for SaaS applications.
- Master Service Agreements.



Privacy Policies, Privacy Notices & Terms of Use 29

Privacy Policies govern the manner in which Organizations collect, use, maintain and disclose information collected from users of websites or applications.

Privacy Notices are how Organizations communicate their policies to their users.

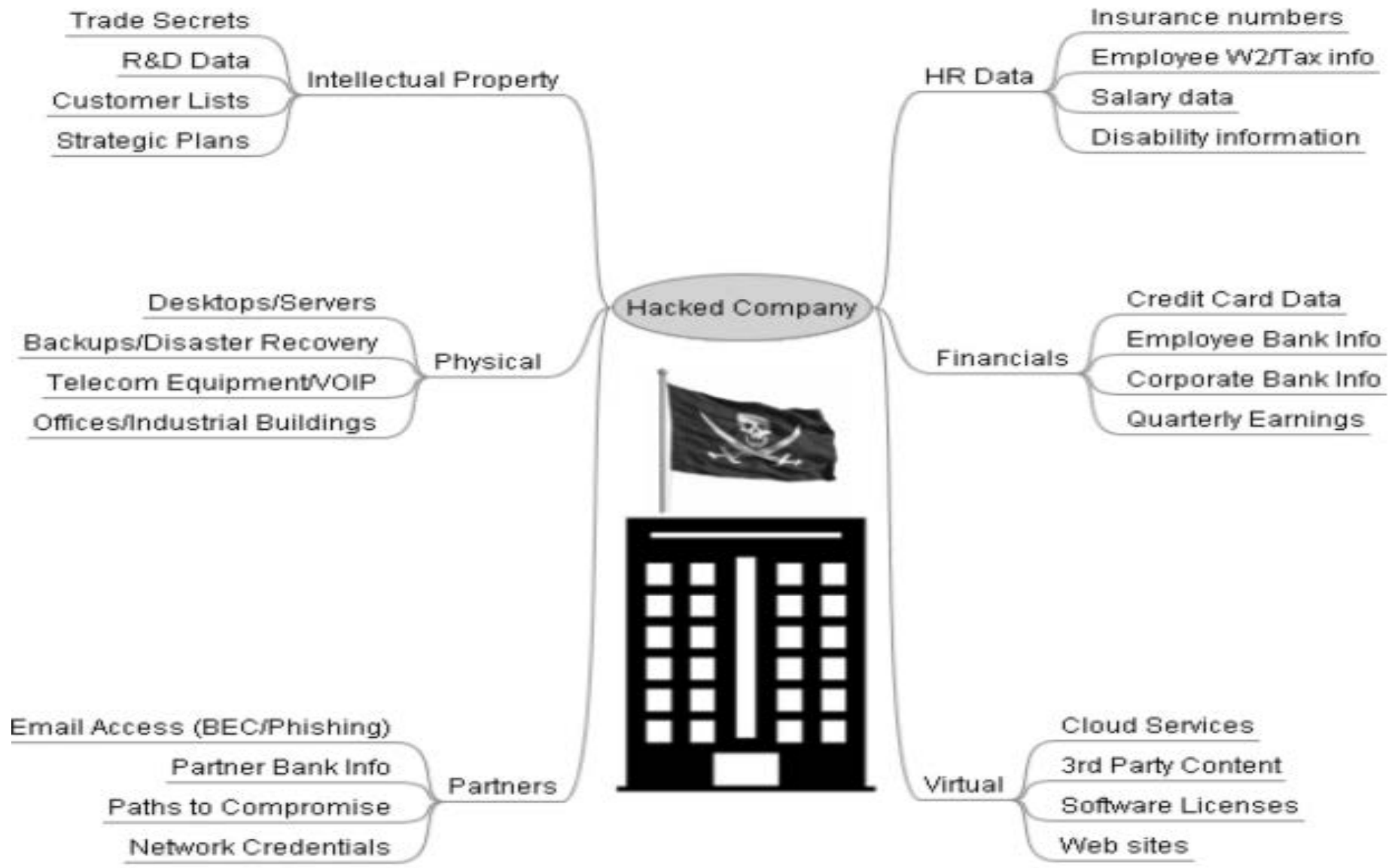
Terms of Use (a/k/a Terms of Service) prescribe the rules users must abide by when using a particular website or application.



3.

Recognizing Key Legal Issues





Standard Definitions for State Breach Laws









Breach of Security: The unlawful and unauthorized acquisition of personal information that compromises the security, confidentiality, or integrity of personal information.

Personal Information: An individual's first name or first initial and last name plus one or more of the following data elements: (i) Social Security number, (ii) driver's license number or state issued ID card number, (iii) account number, credit card number or debit card number combined with any security code, access code, PIN or password needed to access an account and generally applies to computerized data that includes personal information. Personal Information shall not include publicly available information that is lawfully made available to the general public from federal, state or local government records, or widely distributed media. In addition, Personal Information shall not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

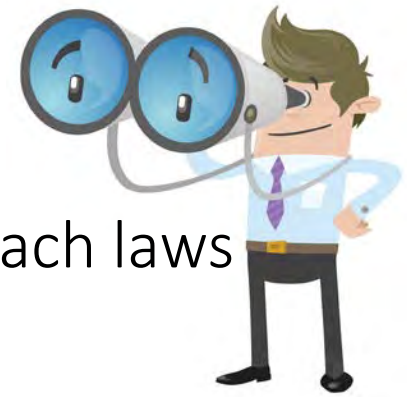
State Breach Laws are not Uniform

TEXAS

Some state breach notification law have the following:

- A broader definition for “personal information” 
- Triggers upon “access” to PI, rather than “acquisition” of PI 
- Requirements for:
 - A risk of harm analysis; 
 - Notice to the Attorney General or State Agency; 
 - Notification within a certain time frame; 
- Authorization of a private cause of action; 
- Encryption safe-harbors; 
- Triggers by breach of security in Electronic and/or Paper Records. 

Issue Spotting



- Legal compliance with data protection/ data breach laws
- Protecting intellectual property
- Cybercrime and tort law issues
- Risk analysis and incident response procedures
- Ensuring adequate security, indemnity and insurance in technology-related contracts
- Security policy, implementation and auditing issues
- Complying with information governance requirements within the Organization

Knowing when you need a Privacy Lawyer

- Breach response
- Information security plan
- Document retention schedules and policies
- Permissible use policies
- “Bring your own device” policies
- Cloud-computing policies
- Social media guidelines
- Privacy Policies, Privacy Notices & Terms of Use
- Cyber-Insurance
- Technology contracts & IT Outsourcing Agreements

4.

Strategies for Avoiding Liability and Protecting Data



Avoiding Liability

- Identify and protect your critical data (i.e. customer data and financial information)
- Work with privacy counsel to ensure compliance with required privacy laws and regulations, both internal and external to the organization.
- Develop, adopt, implement, and periodically update clear and effective:
 - privacy policies, procedures, training, communications and awareness materials;
 - privacy remediation and corrective action initiatives,
 - protocols and controls to ensure proper and timely privacy compliance;
- Conduct due diligence and highly negotiate vendor and third-party technology-related contracts.

12 Questions Your Cloud Contract Should Answer

1. Who owns the data?
2. Does the vendor do anything with the data for its own purposes?
3. Does the vendor have strict policies on who can access data, including staff or other cloud tenants?
4. What does the vendor do with access logs and other statistics?
5. Where is the data stored?
6. Does the vendor separate your data from other client's data?
7. Who owns and has access to backups?
8. What regulations can the vendor verify that they adhere to?
9. If the data needs to be transferred back to you, what form will it be delivered in and at what cost?
10. What happens when you need to transfer the data?
11. Does the vendor carry adequate insurance for its storage activities?
12. Does the vendor provide indemnity for its negligence and that of its sub-contractors?

IT Vendor Management

Vendor selection and due diligence

- Reputation
- Financial condition & insurance
- Information security controls
- Point of transfer
- Disposal of information
- Employee training
- Vendor incident response

Vendor Contract Negotiation

- Ownership of Data
- Confidentiality
- Indemnity
- No further use of shared information
- Use of subcontractors
- Notification and disclosure of breach
- Information security provisions

Protecting Data – 3 Basic Rules for Online Safety

1. *“If you didn’t go looking for it, don’t install it!”*
2. *“If you installed it, update it.”*
3. *“If you no longer need it, remove it.”*



3 Easy Ways to Protect your Data

1. Don't email personal information, and if you violate this rule, at least use encryption (i.e. Rpost - <http://www.rpost.com/>)

2. Avoid using public Wi-Fi (use your own hotspot!)

3. Protect all of your accounts, devices and apps with strong passwords – least 10 to 15 upper- and lowercase letters, numbers and special characters to create strong passwords.



Protect your Data – Super-Secret Tips





Protect your Privacy - iPhone Edition



- **Stop your iPhone from Tracking You:**
Settings -> Privacy -> Location Services -> System Services -> [Switch off Frequent Locations]
- **Prevent Siri & Passbook Access from your lock screen:**
Settings -> Touch ID & Passcode -> [Enter your passcode] -> [Switch off all under Allow Access When Locked]

Protect your Privacy - iPhone Edition continued!



- **Disable Apps from Accessing Your Mic:**
Settings -> Privacy -> Microphone -> [choose wisely (not Shazam)]
- **Disable Passwords & Credit Card AutoFill:**
Settings -> Safari -> Passwords & Autofill -> [disable Names and Passwords, and Credit Cards]
- **Disable Ad-Tracking:**
Settings -> Safari -> [select Do Not Track]

Protect your Privacy - Android Edition



46

- **Fine Tune or Stop your Android from Tracking You:**
 - Settings ->Location->[Consider switching off]
 - Google Settings ->Location ->[Switch off or Delete Location History]
- **Disable Cloud-Based Backup:** Settings-> Backup & Reset-> [Switch off Back up my data]
- **Prevent unauthorized apps from installing:** Settings ->Security ->[Switch off Unknown sources]
- **Opt out of interest-based ads:** Google Settings ->Ads->[Opt out of interest-based adds]

Kate Morris, Esq., CIPP/US

Associate

PRIVACY, INTERNET & TECHNOLOGY LAW

901 Main Street, Suite 4400

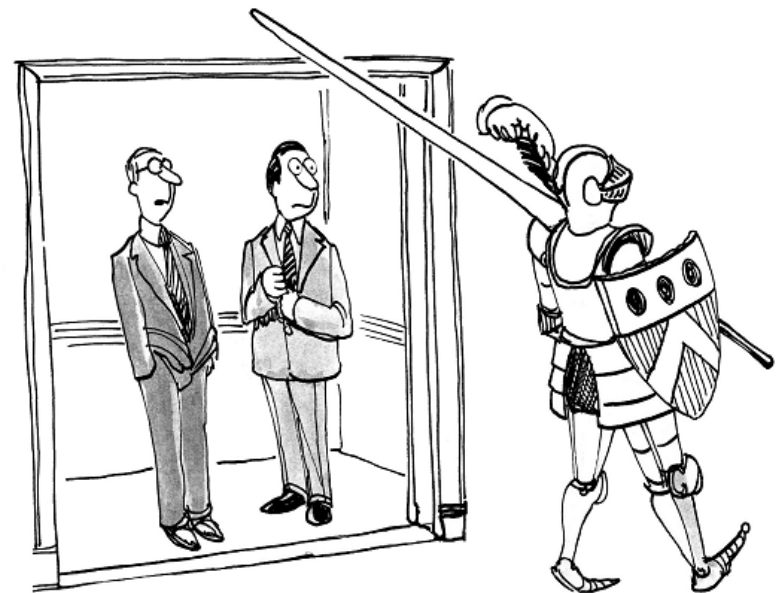
Dallas, TX 75202

kate.morris@strasburger.com

Tel: 214.651.2043

<https://www.linkedin.com/in/kathrynemorris/>

<http://www.strasburger.com/blogs/intellectual-property-law/>



“He really takes IT Security seriously.”

Strasburger
ATTORNEYS AT LAW
