Privacy and Security Update

GHA Compliance Officer Retreat 2017

Gina G. Greenwood, JD, CIPP/US
Monarch Plaza, Suite 1600
3414 Peachtree Road, N.E.
Atlanta, GA 30326
Office: 404.589.0009 ext. 1804
Cell: 404.909.0665
ggreenwood@bakerdonelson.com

CYBER ATTACKS

Cyber attacks are in the headlines everyday.

WE are under constant attack by hackers constantly trying to gain access to computer networks!

BAKER DONELSON

Partially Taken from Source: DynaSis

LIVE CYBER ATTACK THREAT MAPS

https://cybermap.kaspersky.com/

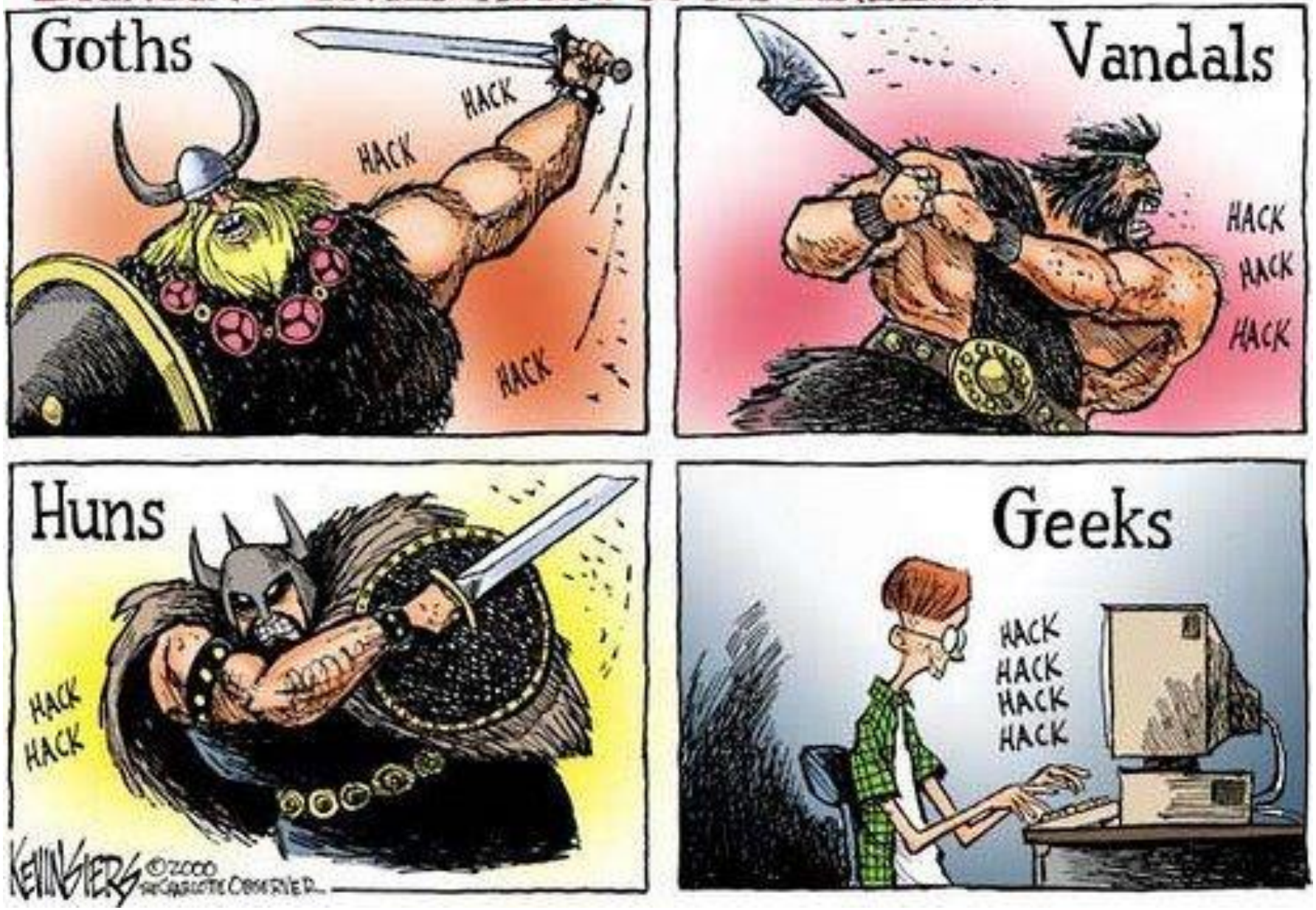
BAKER DONELSON

Incident Trends & Organizational Threats

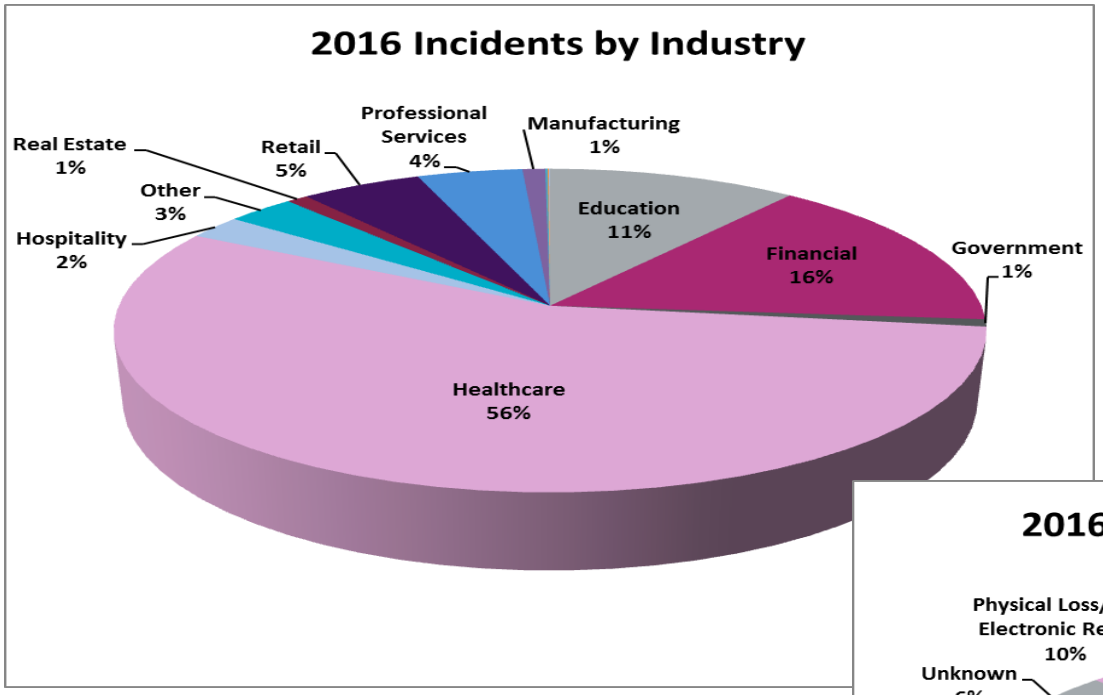
They market on The Dark Web where Everything is For Sale

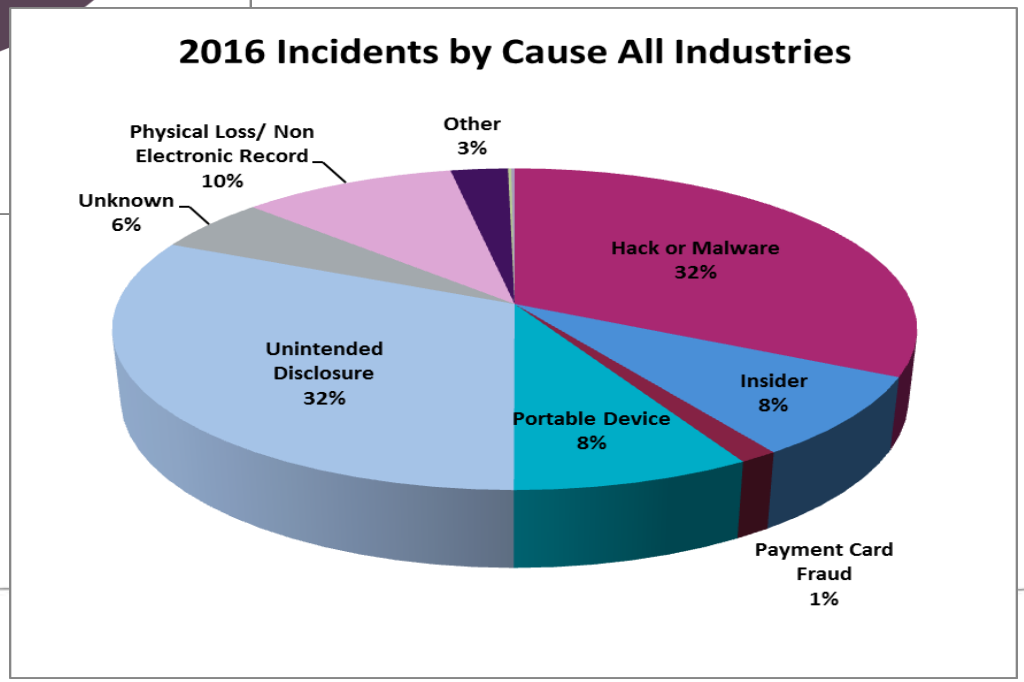
- **DDOS attacks for as low as $5 USD an hour**
- **Banking credentials from 1% to 5% of account balance**
- **300,000 airline points for $90 USD**
- **American Express Cards for $30 USD**
- **ATM skimming devices as low as $400 USD**
- **Crypters from $80 USD**
- **Angler Exploit Kits from $100 USD**
- **Online tutorials from $20 USD**

BRINGING CIVILIZATION TO ITS KNEES...



Incident Trends & Organizational Threats





OCR STATS FROM NIST /OCR 2017 CONFERENCE

September 2009 through July 31, 2017

- Approximately 2,017 reports involving a breach of PHI affecting 500 or more individuals
- Theft and Loss are 48% of large breaches
- Hacking/IT now account for 17% of incidents
- Laptops and other portable storage devices account for 26% of large breaches
- Paper records are 21% of large breaches
- Individuals affected are approximately 174,974,489
- Approximately 293,288 reports of breaches of PHI affecting fewer than 500 individuals

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

OCR Stats . . .

- **Complaints Received and Cases Resolved**
  - Over 158,293 complaints received to date
  - Over 25,312 cases resolved with corrective action and/or technical assistance
  - Expect to receive 17,000 complaints this year

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

BAKER DONELSON

Think

Before You Click!

PLEASE!!!!!

BAKER DONELSON

Cyber Attacks Are Often Triggered By Scam Emails These Range From the More Obvious . . .

- In the past, attacks were much easier to spot.
- One example was the "Arabian Prince" type emails that were full of misspelled words. Fraud was not subtle . . .

From: Armondo Travlio (atavaliow!@#7%@gmail.it)
To: Bob Servant
Subject: Delete This At Your Peril
FROM HIS ROYAL HIGHNEST, PRINCE TAVLIO

Dear Sir,

Permite me to inform you of my desire of going into business. I am Armondo, only son of late King Arawil of tribal land. My father was a very wealthy traditional ruler, poisoned by his rivals. Before his death here in Togol he told me of a trunke containing $75m kept in a security company. I now seek a foreign partner were I will transfer the proceads for investment as you advize. I am willing to offer 20% of the sum as a compensation for your effort/input and 5% for any expenses. If you are willing to help, transfer $1000 to Bank of Tribal Account Number: 3486022200 Routing Number: 12647774 as a show of good faith.

Thanks and God bless,
PRINCE TAVLIO

Source: DynaSis

Today Scams Are Much More Sophisticated:
Emails that appear to be from legitimate companies that you do business with and are designed to entice users to click on links or open attachments.

FedEx Service <details@feedeex.com> August 13, 2012 6:54 AM
To: booking@hopeforthedying.com Details
FedEx delivery problem # Error ID4900

FedEx®
Federal Express

Unfortunately we failed to deliver the postal package you have sent on the 27th of July in time because the recipient's address is erroneous.

Please print out the label copy attached and collect the package at our office.

Print a shipping Label

at&t Manage myAT&T Accoun

Voicemail Message

You have received a voicemail at 2013-19-12 35:31:25 CST.

You are receiving this message because we were unable to deliver it, voice message did not go through because the voicemail was unavailable at that moment.

* The reference number for this message is qvfi_cjl09-9107319601-2125579909-62.

The length of transmission was 24 seconds.
The receiving machine's ID: YJH35-TW410-F37JZL.

Thank you,
AT&T Online Services

Contact Us
AT&T Support - quick & easy support is available 24/7.

Receiving ID:
YJH35-TW410-F37JZL

From Number(s):
459-330-7200

Getting To Know AT&T
Watch helpful videos to get you better acquainted with your new AT&T service.
View the videos

We value and appreciate your business!

*Mobile Broadband coverage not available in all areas.
** Based on U.S. carriers.

Attention New Jersey customers and small businesses: FREE e-cycling for electronic devices with video screens more than 4 inches at nearby collection sites. http://www.nj.gov/dep/dshw/ewaste/collectionsites.pdf or 1-866-DEPKNOW

This is a system-generated message from a send only address. Please do not reply to this email.

BAKER DONELSON

Source: DynaSis

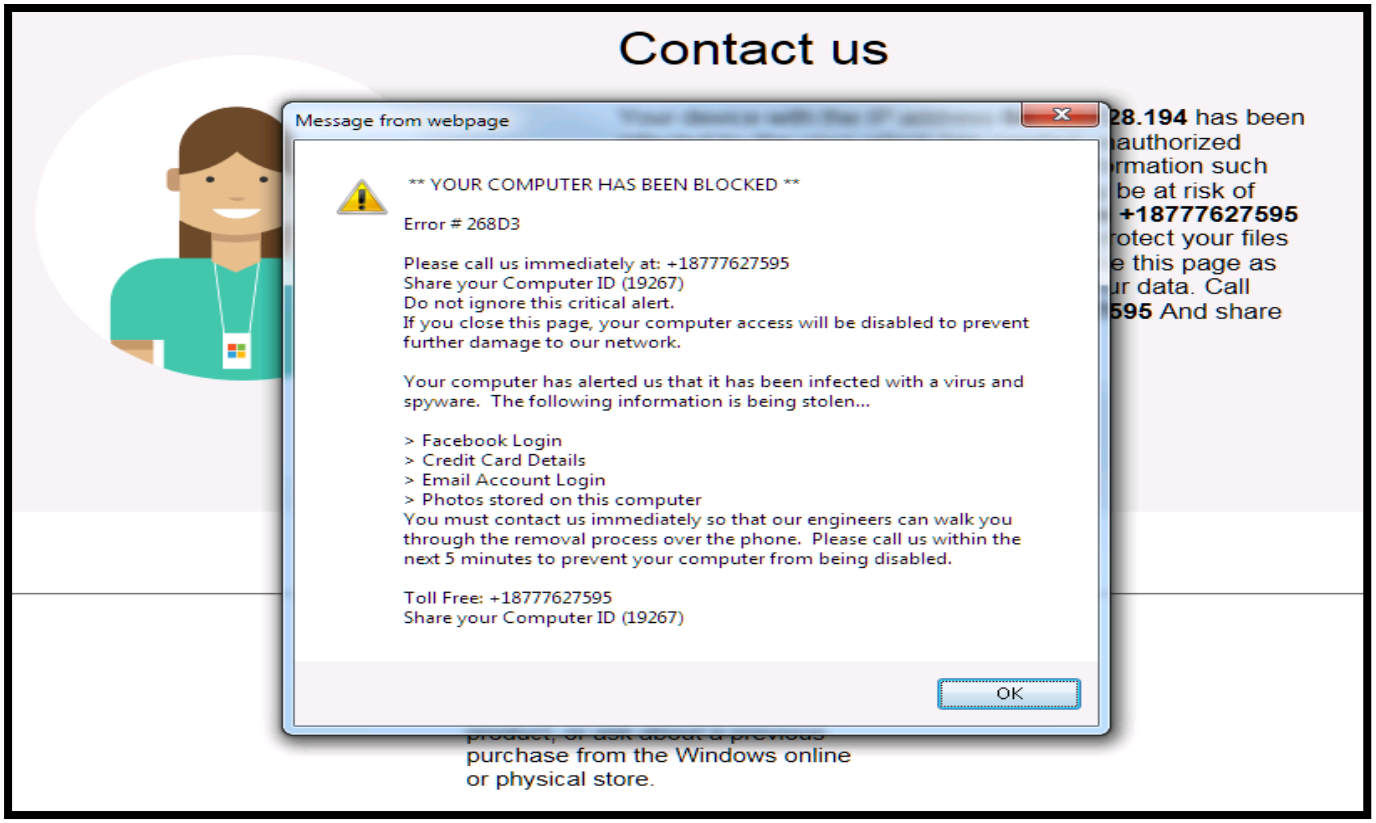
But Look Closely Before Clicking . . .

- Check the sender email address closely before you click. Don't assume an email is legitimate just because the logo looks correct.
- Use common sense. Using the example, if it would be odd for you to get an email about a FedEx delivery failure, that is a red flag.
- Sometimes, you can hover the cursor over the link to see the web address of the link. A FedEx "print shipping label" link should not be to random.net/hotdeal

BAKER DONELSON

Many Attacks Prey On Your Work Ethic And Fears like the "Alert" Pop-up

- Alerts claiming your computer is frozen or data is being stolen, commanding you to call a number or click on a link are scams.
- Shut down your computer or call your IT Department, if you are concerned. Do not click on anything. Do not call the number in the pop-up or share information.



Scam Requests for Payment

Some scams may look like an invoice. Use common sense. References to wire transfer or payment by the same day are red flags. Think before you click.

Dell Inc
5 Polaris Way,
Aliso Viejo, CA 92656,
Tel +1 949 754 8000
Fax +1 949 754 8999
WWW.Dell.com

Customer Name: Wilkins Academy
Account #: 1248447

Dear Customer,
Please be advised, the below overview of invoices is showing as unpaid on your customer account with Dell Software International Limited.

We would like to bring to your attention, we expect your payment to reflect on our account latest by due date, transferred to the respective bank details stated on invoice. In case of payment delays beyond contractual agreements, Dell Software Group is authorized to take further action to ensure timely payment.

Transaction #	Trans Date	Purchase Order	Due Date	Currency	Balance Due
1000223085	**28. 10. 2014**	1-SQH9HT	**31. 1. 2015**	USD	$**1410.10**

Please note that if you are paying by bacs, wire or chaps transfer to Dell software group please ensure that you have the below bank details correct in your system.

Bank name : JPMorgan Chase Bank, N.A. (NY),Account Number: 365839887, Swift Code: CHASUS33XXX,Currency : USD

Kindly include your Dell account number, company name and all invoice numbers when you make the payment so that we can apply the payment into the invoices immediately once we receive the payment. If you have paid any of these amounts, please exclude those from your payment order. Thank you once again for your continued business with Dell.

Sincerely,

Johnathan Griffin
Dell Collections
Email: jgriffin@software.dell.com

BAKER DONELSON

Source: DynaSis

Scam Requests for Payment

The example below includes both a potentially dangerous link and a demand for payment.

Common sense and awareness:

- You should know if you've gotten a parking ticket. A legitimate email would include contact information for questions.
- The sender's email address does not look like an official email address.
- A legitimate email would not be signed "Police Department."

From: Traffic Police Department <gbpftif@ad.maxart.it>
Date: April 19, 2017 at 6:19:01 PM CDT
To: Joe Stewart <jstewart@firm.com>
Subject: Parking Ticket #9856125332

You got a parking fine!
26-143 – Unattended car
Required to appear in trial
Parking ticket number PTD9856125332

Check Parking Ticket

To pay your parking fine, download your ticket and choose one of 2 convenient ways:

1. Online – Pay online by Visa or Mastercard, $2 processing fee.
2. By phone (automated system) - Pay by Visa or Mastercard at 866-562-4828

Best Wishes,
Police Department.

Source: Baker Donelson PC

Scam Requests for Payment

- This email appears to be from a familiar company executive. The executive claims to be unable to talk with you in person but needs you to wire or send funds immediately.
- The sender's email address is a red flag.
- BUT NOTE: A hacker may have ghosted the executive's account such that the email address looks accurate. NEVER send or wire funds without face-to-face confirmation or without otherwise following our procedures.

From: Brenda Director <brendaceo@gmail.com>
Date: April 2, 2017 at 2:12:01 PM EDT
To: John Employee <jemployee@firm.com>
Subject: AT&T Payment – URGENT

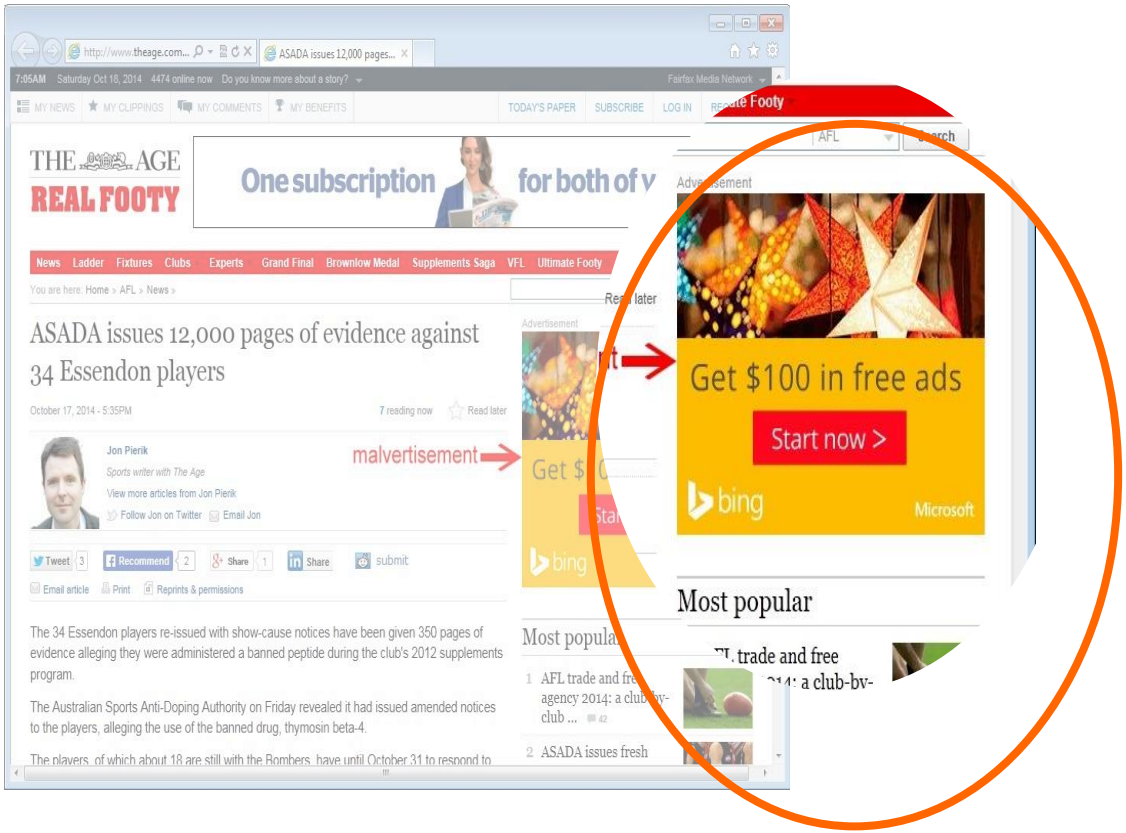
Hi,
I'm out of the office in a meeting with John Smith. The payment to AT&T is overdue. This needs to go out now by wire transfer to avoid interruption of service.

Please immediately wire $5,348.45 to South State Bank, Routing # 351578040, Account # 5831365839887. Let me know when complete. It can't wait.

Regards,
Brenda
CEO

Scam "Malvertising"

Links for "free" services, downloads, or streaming video are also suspicious. The cliché holds: If it sounds too good to be true, it probably is. It could be a link to malware or something that will harm our network.

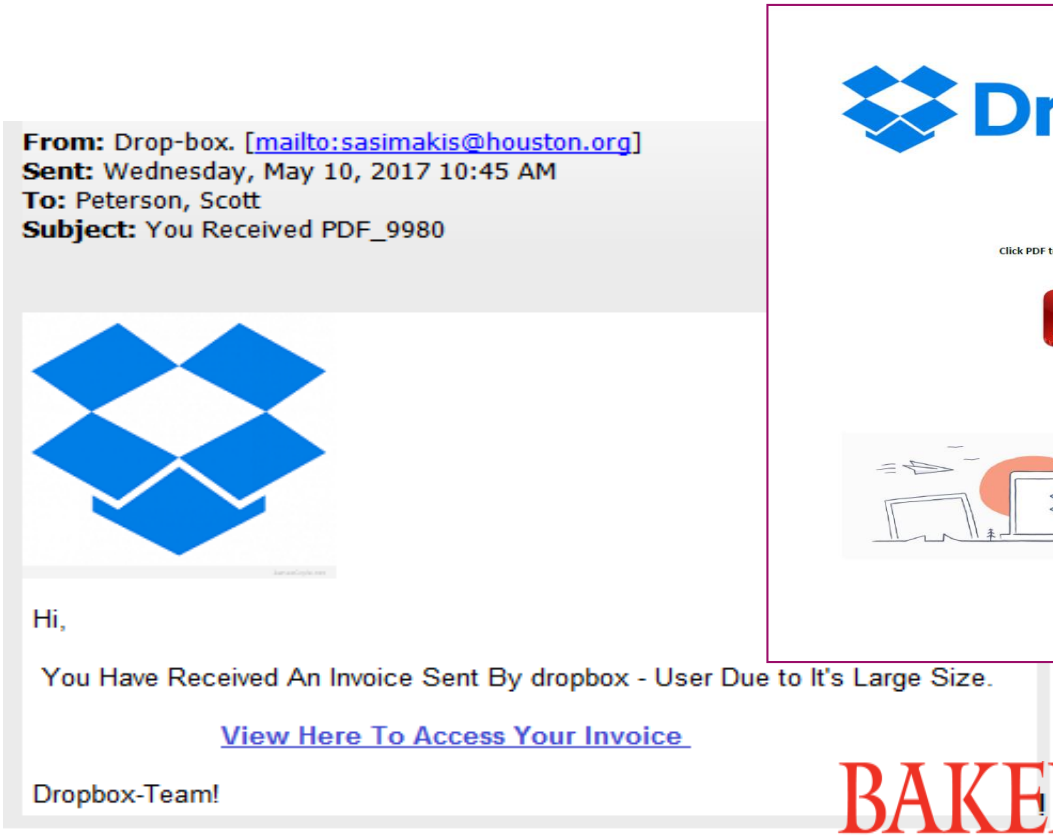


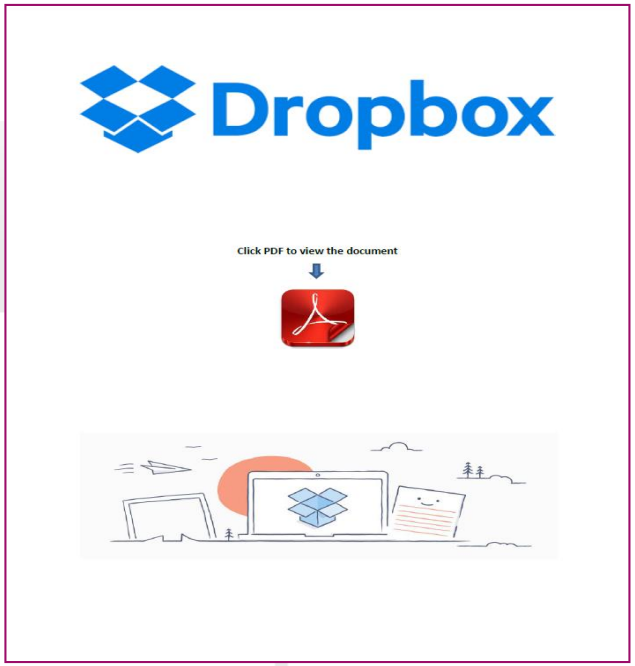
BAKER DONELSON

Source: DynaSis

Scams That Make You Feel You are Missing Out If You Don't Click on the Link!

- Emails that appear to be from a friend linking to pictures or a vendor linking to an invoice or deliverable.
- Be alert: Are you expecting pictures from that friend? Does the sender email make sense or look familiar?
- Hover your cursor over the link. Does the website information fit?
- Unless you are 100% certain, do not click on the link.





BAKER DONELSON

Ransomware: One Wrong Click Can Lead To An Attack

Ransomware launches an attack that lets the hacker hold our computers and network HOSTAGE until we pay a monetary ransom.

If you ever see a screen like the one below or on the following slide, shut down your computer and call the IT Department immediately.

BAKER DONELSON

Ransomware Attacks Come In All Shapes And Sizes And Can Be Very Sophisticated.

Ransomware can launch from one click on a link or email attachment.

Incident Trends & Organizational Threats

Increasingly Common: Dropper

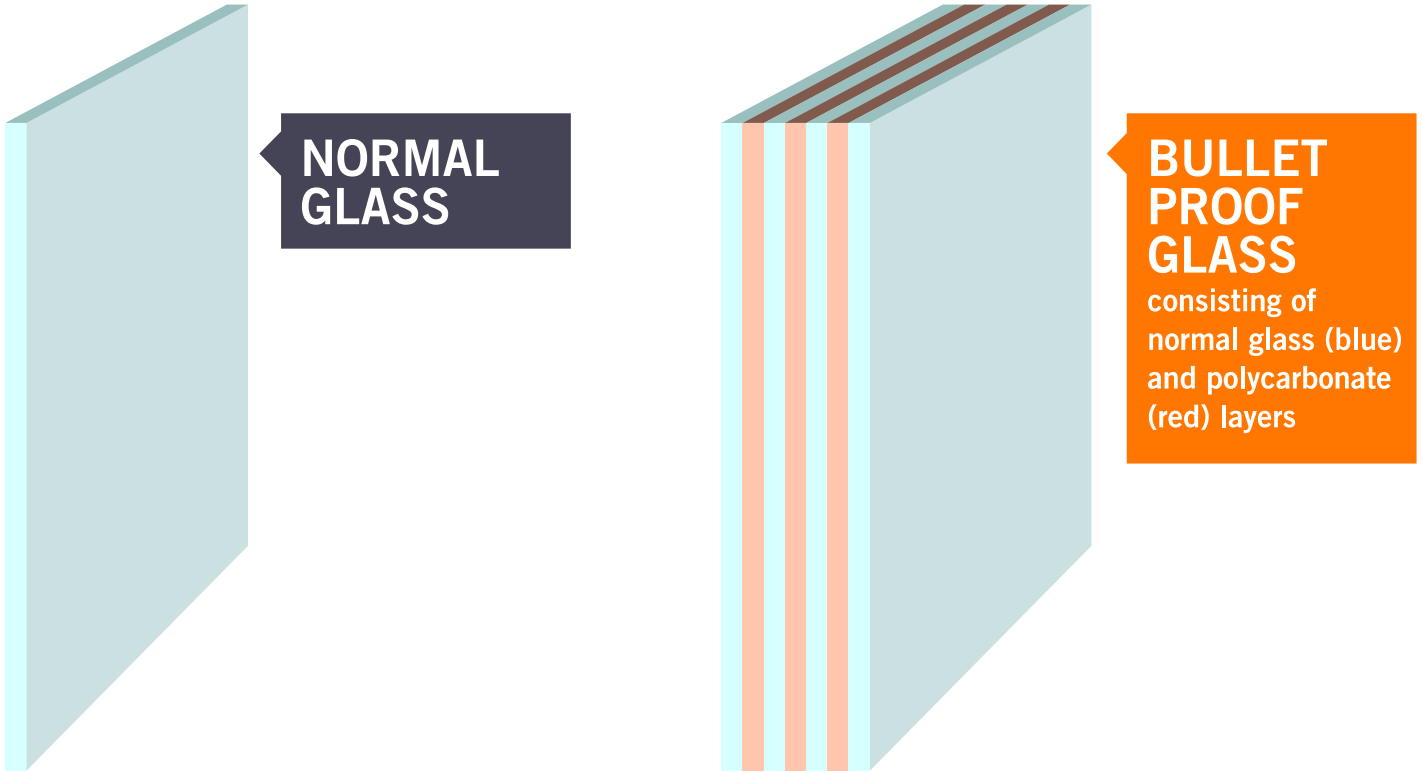
TACTIC

Malware that installs other malware

1. Bad actor gets a piece of malware on computer
2. Malware sits quietly and just phones home; not the old fashion flashy/noisy malware of yesterday
3. Bad actor sells or rents ability to infect computer
   - Malware phones home
   - Installs main payload: Ransomware, etc.
4. If contract ends or need more capacity, just install more Malware

DynaSis

Preventing An Attack Takes Layers of Protection and Prevention



BAKER DONELSON

DynaSis

Security And Risk Management Is About Managing Risk Through A Layered Approach

USER TRAINING: Establishing Safe Habits

INCIDENT RESPONSE EMERGENCY PREPAREDNESS PLAN

PRIVACY AND SECURITY POLICIES / PROCEDURES factoring in applicable law

TESTING SYSTEMS / TABLE TOPS

Cyber Liability Insurance

BACK–UP FILES / CONTAINMENT / BLOCKING

MANAGING ADMIN AND ACCESS RIGHTS – Multifactor Authentication

FILTERING: Email Content Filtering

ANTI–MALWARE / ANTI-VIRUS SOFTWARE

WEEKLY PATCH UPDATES: Workstation & Server

FIREWALLS / ENCRYPTION

DATA MAPPING / DEVICE MANAGEMENT

BAKER DONELSON

Security Risk Analysis & Management

"[a] flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy."

Vulnerabilities can be technical or non-technical.

"[t]he potential for a person or thing to exercise (accidentally trigger or intentionally exploit) a specific vulnerability."

Threats can be natural, human, or environmental.

"the net mission impact considering (1) the probability that a particular [threat] will exercise (accidentally trigger or intentionally exploit) a particular [vulnerability] and (2) the resulting impact if this should occur."

A Vulnerability triggered or exploited by a Threat equals a Risk.

Source: NIST SP 800-30, Risk Management Guide for Information Technology Systems.

http://www.healthit.gov/providers-professionals/security-risk-assessment

Security Risk Assessment | ...

File Edit View Favorites Tools Help

Google Free Hotmail

Page Safety Tools

Blog | Federal Advisory Committees (FACAs) | Contact | Get Email Updates

HealthIT.gov

in Partnership with the National Learning Consortium

Newsroom FAQs Multimedia Implementation Resources

Providers & Professionals | Patients & Families | Policy Researchers & Implementers

Benefits of EHRs | How to Implement EHRs | Privacy & Security | EHR Incentives & Certification | Success Stories & Case Studies | Resource Center

HealthIT.gov > For Providers & Professionals > Privacy & Security > Security Risk Assessment

Print | Share

Security Risk Assessment

What is Risk Assessment?

The Health Insurance Portability and Accountability Act (HIPAA) Security Rule requires that covered entities conduct a risk assessment of their healthcare organization. A risk assessment helps your organization ensure it is compliant with HIPAA's administrative, physical, and technical safeguards. A risk assessment also helps reveal areas where your organization's protected health information (PHI) could be at risk. Watch the Security Risk Analysis video to learn more about the assessment process and how it benefits your organization or visit the Office for Civil Rights' official guidance.

Read the HHS Press Release

Download the SRAT event files from the April 29 Webinar [ZIP - 4 MB]

Security Risk Assessment Tool

ONC, in collaboration with the HHS Office for Civil Rights (OCR) and the HHS Office of the General Counsel (OGC), developed a downloadable Security Risk Assessment Tool (SRA

SRA Tool Videos

Watch videos on what a risk assessment may involve, and learn how to use the SRA Tool by watching the SRA Tool Tutorial video.

We want to hear from you!

Share with us your thoughts and submit your comments on the SRA Tool by Monday, June 2nd.

100%

9:31 AM
3/10/2015

http://www.healthit.gov/providers-professionals/your-mobile-device-and-health-inform

Mobile Health Security: Mo...

File Edit View Favorites Tools Help

Suggested Sites Web Slice Gallery Free Hotmail

Page Safety Tools

Blog | Federal Advisory Committees (FACAs) | Contact | Get Email Updates

HealthIT.gov

in Partnership with the National Learning Consortium

Newsroom Help Center Multimedia

Providers & Professionals | Patients & Families | Policy Researchers & Implementers

Benefits of EHRs | How to Implement EHRs | Privacy & Security | EHR Incentives & Certification | Health Information Exchange (HIE) | Success Stories & Case Studies

HealthIT.gov > For Providers & Professionals > Privacy & Security > Your Mobile Device and Health Information Privacy and Security

Print | Share

Privacy & Security

Your Mobile Device and Health Information Privacy and Security

Physicians, health care providers and other health care professionals are using smartphones, laptops and tablets in their work. The U.S. Department of Health and Human Services has gathered these tips and information to help you protect and secure health information patients entrust to you when using mobile devices.

Read and Learn

- How Can You Protect and Secure Health Information When Using a Mobile Device?
- You, Your Organization and Your Mobile Device
- Five Steps Organizations Can Take To Manage Mobile Devices

Watch and Learn

- Worried About Using a Mobile Device for Work? Here's What To Do!
- Securing Your Mobile Device is Important!
- Dr. Anderson's Office Identifies a Risk

100%

2:16 PM
10/22/2013

Biggest Areas of Risk

- No Risk Assessment
- No or Unfollowed Risk Management Plan
- No BA Agreement
- BAs allow overseas storage / access
- Unsecured Devices / Drives
  - Mobile Devices
  - Laptops
- No Plan for Attacks
- Disposal Issues
- Ransomware due to failure to train workforce / patch
  - Sign up for the FBI watch lists
- Internet of Things
  - Patient Devices

BAKER DONELSON

Incident Trends & Organizational Threats:

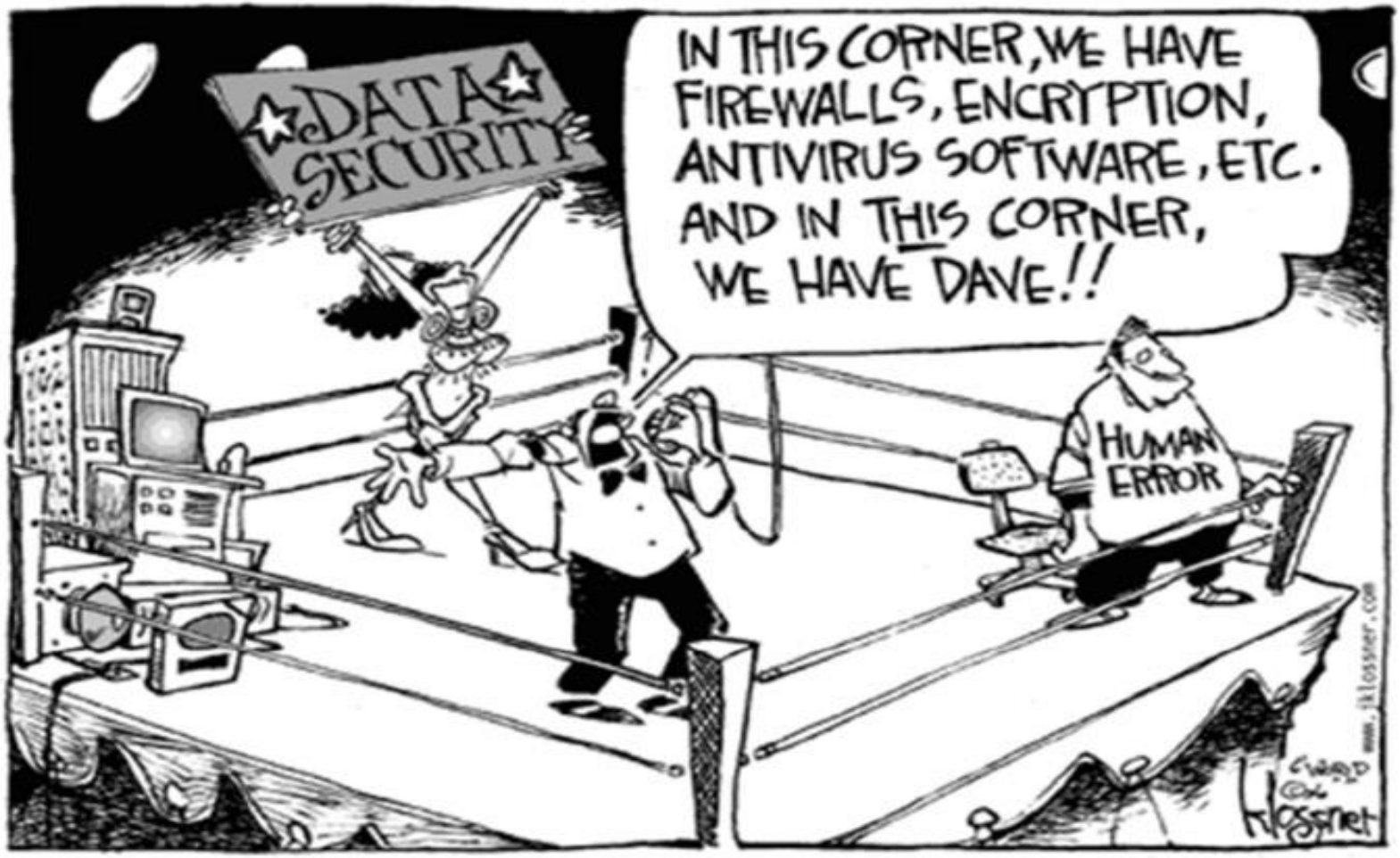
Attackers are targeting the weakest links in the supply chain

DUE DILIGENCE VENDORS!!!

BAKER DONELSON

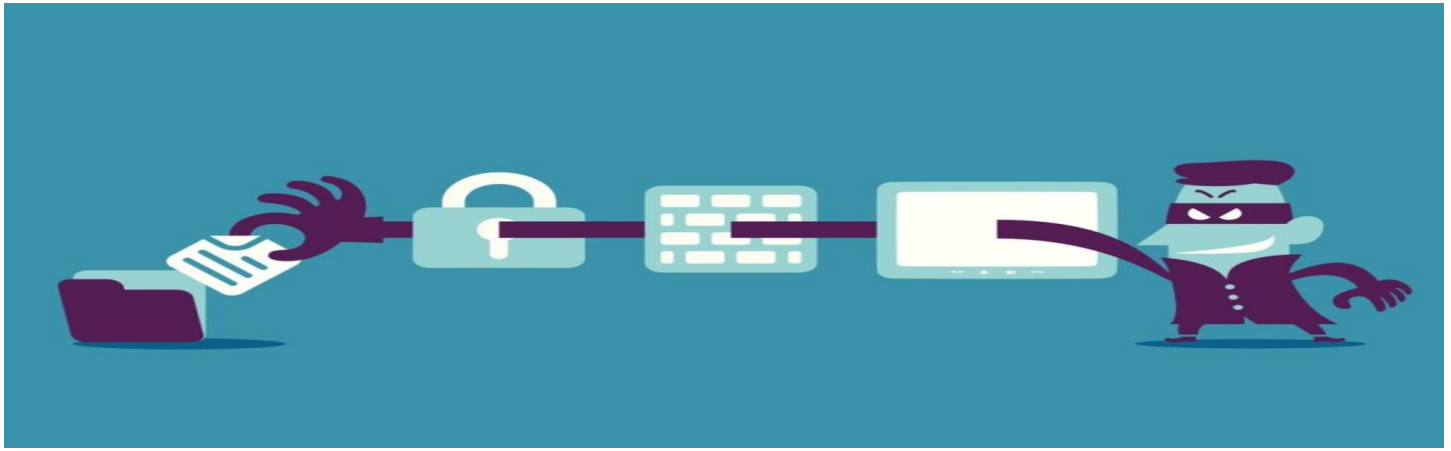
Source: DynaSis

User Error Remains the Biggest Risk . . .
Don't cause that error!!



BAKER DONELSON

Your Role Is Critical: Educate Yourself and Your Organization



U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

OFFICE FOR CIVIL RIGHTS

- **Cyber Security Guidance Material Webpage**

https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/index.html

  - Includes a Cyber Security Checklist and Infographic, which explain the steps for a HIPAA covered entity or its business associate to take in response to a cyber-related security incident.

- **Additional Cybersecurity Guidance: Ransomware and Cloud Computing**

  - Ransomware: http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html
  - NIST Cybersecurity Crosswalk with HIPAA Mapping:
  - https://www.hhs.gov/sites/default/files/nist-csf-to-hipaa-security-rule-crosswalk-02-22-2016-final.pdf?language=es

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

OFFICE FOR CIVIL RIGHTS

Monthly Guidance: Cybersecurity Newsletters

Feb. 2016	Ransomware, "Tech Support" Scam, New BBB Scam Tracker
March 2016	Keeping PHI safe, Malware and Medical Devices
April 2016	New Cyber Threats and Attacks on the Healthcare Sector
May 2016	Is Your Business Associate Prepared for a Security Incident
June 2016	What's in Your Third-Party Application Software
Sept. 2016	Cyber Threat Information Sharing
Oct. 2016	Mining More than Gold (FTP)
Nov. 2016	What Type of Authentication is Right for you?
Dec. 2016	Understanding DoS and DDoS Attacks
Jan. 2017	Audit Controls
Feb. 2017	Reporting and Monitoring Cyber Threats
March 2017	Reporting and Monitoring Cyber Threats
April 2017	Man-in-the-Middle Attacks and "HTTPS Inspection Products"
May 2017	Cybersecurity Incidents will happen…Remember to Plan, Respond, and Report!
June 2017	File Sharing and Cloud Computing: What to Consider?
July 2017	Train Your Workforce, so They Don't Get Caught by a Phish!
August 2017	Protecting yourself from potential scammers while being charitable

http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html

https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/index.html

Gina Ginn Greenwood, JD, CIPP/US

Monarch Plaza
3414 Peachtree Road, N.E.
Suite 1600
Atlanta, Georgia 30326

Direct: 404.589.0009 ext. 1804
Cell: 404.909.0665
ggreenwood@bakerdonelson.com

BAKER DONELSON

Gina Greenwood is a healthcare attorney and IAPP Certified Information Privacy Professional (US) who assists clients across the country with data and other compliance needs, data breaches and internal and external compliance investigations.

- Gina concentrates her practice on a wide range of health care and privacy/security matters, including cyber liability, risk management, data breaches and response, HIPAA Privacy and Security Rule compliance and HIPAA / HITECH breaches; PCI, COPPA, CAN-SPAM, TCPA Act, FTC Act, GLBA, GINA, Part 2, etc. compliance, meaningful use audits, fraud and abuse compliance and EMTALA/COP investigations, corporate health care transactions and day to day compliance advice to hospitals and other licensed health care entities.
- Gina has authored numerous materials including privacy and security policy manuals, licensure policy manuals, and Internet-based employee training modules.
- Gina has been recognized as one of the Best Lawyers in US (Healthcare) and by Chambers USA as a leading health care lawyer in America. She has been voted *Georgia Trend Magazine* Legal Elite. She served as 2014 expert legal witness on EMTALA and mental health issues during the USCCR hearings in Washington, DC. – which provided testimony to US Congress and President of the United States.