Author and attorney specializing in privacy, computer security, e-mail discovery, records management and BYOD.
SANS Legal 523 Instructor
hack-igations.blogspot.com

Attorney working with clients across industry segments including, electronic goods, software publishing, Internet-based services, shopping centers, and supply-chain management.
Opening Comments

UTD Information Security Office
Nate Howe, CISO
Penn State University Hacked

The College of Engineering's computer network was disconnected from the Internet in response to the breach.

By Jeff Goldman | Posted May 10, 2015

North Dakota University System hacked, roughly 300K impacted

Stanford University hacked, becomes latest data breach victim

University of Maryland hacked; 309,000 Social Security numbers stolen

Butler University Hacked, Universities Becoming Attractive Business for Hackers

Higher Education’s Records Are Key PII and Credential Theft Targets

UCLA Health hacked, 4.5 million victims
Within the education sector, the average cost of a breach is $225 per record. Within the healthcare industry, the average cost is $398 per record.

- 2015 Cost of Data Breach Study, Ponemon Institute\(^1\)

UT Dallas has millions of records on more than 200,000 unique individuals.
Speaker Introductions

UTD Information Security Office
Nate Howe, CISO
A Culture of Security

Minimizing Exposure to Cyber Risks

Information Security Office Presents:
Avoiding Legal Pitfalls by Building a Culture of Security

October 13, 2015

At:

UTDallas
The University of Texas at Dallas

Andrews Kurth
S.T.A.R. TALK IS GOOD BUSINESS®
andrewskurth.com
We now live in a culture of pervasive and continuous data gathering.
DO YOU KNOW WHERE YOUR CHILDREN ARE?

ANDREWS KURTH
STRAIGHT TALK IS GOOD BUSINESS®
andrewskurth.com
They do.
ON THE INTERNET, NOBODY KNOWS YOU'RE A DOG
"Heading off to a two week Caribbean cruise! Bon voyage!"

DO YOU REALLY KNOW WHO’S READING YOUR STATUS UPDATES?

DataSafe
ANDREWS KURTH LLP
Security Awareness Program

© Traveling Coaches

ANDREWS KURTH
STRAIGHT TALK IS GOOD BUSINESS
andrewskurth.com
Police: Burglary Suspects Targeted Fontana Home After Social Media Posts

At 3:30 a.m. on March 25, investigators with the Fontana Police Department were conducting surveillance in the society, following a string of recent thefts in the area, according to police spokesperson Martha Roman Artis. Roman Artis said:

"They had live-in your own, electronic equipment, furniture, all in the U-Haul and they were getting ready to take off with it," Roman Artis said.

One suspect attempted to flee in a U-Haul truck, but was quickly apprehended by police. Two other suspects were also arrested and all of the stolen property was recovered and returned to the victims, police said.

During the investigation, police say officers learned that the suspects had received information..."
Subject: Your Account Password

CHANCE IN 100 THAT HE WORKS FOR YOUR BANK: 0

WOULD YOU CLICK THE LINK?

ANDREWS KURTH LLP
Security Awareness Program

© TrainingCaches

ANDREWS KURTH
STRAIGHT TALK IS GOOD BUSINESS
andrewskurth.com
Would you click this link?
What about these links?
What about these?

**FREE SANS Webcasts: SPOTLIGHT ON --> Master the Game of Who on 10/8**

**To:** ben@setrick.org

**Reply-To:** webcast@sans.org

**SANS Institute <webcast@sans.org>**

**Mon, Oct 5, 2015 at 11:13 AM**

Hello,

Please join us in the upcoming weeks for the following informative, free SANS webcasts. One hour of CPE credit is earned with each webcast.

All SANS webcasts are recorded. If you are unable to attend the live webcast, you can view it at any time after the webcast date: https://www.sans.org/webcastarchive

Simply log into your SANS Portal Account and register for the webcast to view the presentation and download the slides.

*** SPOTLIGHT Webcast ***

Master the Game of Who: Leveraging Network Intelligence and User Activity to Combat Insider Threats

Thursday, Oct 8, 7:00 AM EDT

Find more details under Webcast #6

Register: http://www.sans.org/u5kO

---

### Here are the upcoming SANS Webcasts:

**WEBCAST 1:**

IC3 Cybersecurity: Models for Success

**WHEN:** Tuesday, October 06 at 1:00 PM EDT (17:00 UTC)

**Featuring:** Michael Assante and Robert M. Lee

http://www.sans.org/u5kG

Cybersecurity is a worthwhile and obtainable goal - but it can be difficult to visualize and understand the keys to success. This requires an understanding of the problem and models on which to guide action. In this presentation, members of the SANS IC3 team will deconstruct the most high profile IC3 cyber attacks and showcase approaches to defense in the form of recommended models. This will also be done with the unveiling of the new SANS IC3 poster and insight into the future of the IC3 curriculum.

**WEBCAST 2:**

Hacked, Or Human Error In Fifteen Minutes Or Less

**WHEN:** Tuesday, October 06 at 5:00 PM EDT (19:00 UTC)

**Featuring:** Elizabeth Netcuit and Chris Crowley

http://www.sans.org/u586f
ONE MAN’S TRASH SHOULDN’T BE ANOTHER MAN’S PROTECTED INFORMATION.
FOR IMMEDIATE RELEASE

June 23, 2014

$800,000 HIPAA settlement in medical records dumping case

Parkview Health System, Inc. has agreed to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule with the U.S. Department of Health and Human Services Office for Civil Rights (OCR). Parkview will pay $800,000 and adopt a corrective action plan to address deficiencies in its HIPAA compliance program. Parkview is a nonprofit health care system that provides community-based health care services to individuals in northeast Indiana and northwest Ohio.

OCR opened an investigation after receiving a complaint from a retiring physician alleging that Parkview had violated the HIPAA Privacy Rule. In September 2008, Parkview took custody of medical records pertaining to approximately 5,000 to 8,000 patients while assisting the retiring physician to transition her patients to new providers, and while considering the possibility of purchasing some of the physician’s practice. On June 4, 2009, Parkview employees, with notice that the physician was not at home, left 21 cardboard boxes of these medical records unattended and accessible to unauthorized persons on the driveway of the physician’s home, within 20 feet of the public road and a short distance away from a heavily trafficked public shopping venue.

As a covered entity under the HIPAA Privacy Rule, Parkview must appropriately and reasonably safeguard all protected health information in its possession, from the time it is acquired through its disposition.

“All too often we receive complaints of records being discarded or transferred in a manner that puts patient information at risk,” said Christina Heide, acting deputy director of health information privacy at OCR. “It is imperative that HIPAA covered entities and their business associates protect patient information during its transfer and disposal.”

Parkview cooperated with OCR throughout its investigation. In addition to the $800,000 resolution amount, the settlement includes a corrective action plan requiring Parkview to revise their policies and procedures, train staff, and provide an implementation report to OCR.

OCR offers helpful FAQs concerning HIPAA and the disposal of protected health information: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/disposalfaqs.pdf

To learn more about non-discrimination and health information privacy laws, your civil rights, and privacy rights in health care and human service settings, and to find information on filing a
Hi!!
I’m here to steal your files!

VERIFY VISITORS LIKE SECURITY DEPENDS ON IT. BECAUSE IT DOES.
No, You Really Can't

By User201515-Oracle on Aug 10, 2015

I have been doing a lot of writing recently. Some of my writing has been with my sister, with whom I write murder mysteries using the nom-de-plume Maddi Davidson. Recently, we’ve been working on short stories, developing a lot of fun new ideas for dispatching people (literally speaking, though I think about practical applications occasionally when someone tailgates me).

Writing mysteries is a lot more fun than the other type of writing I’ve been doing. Recently, I have seen a large tech Inquiry in customers reverse engineering our code to attempt to find security vulnerabilities in it. ‘Insert big sigh here’ This is why I’ve been writing a lot of letters to customers that start with ‘hi, how’s, aloha’ but end with ‘please comply with your license agreement and stop reverse engineering our code, already’.

I can understand that in a world where it seems almost every day someone also had a data breach and lost a million gazillion records to unnamed intruders who may have been working at the behest of a hostile nation-state, people want to go the extra mile to secure their systems. That said, you would think that before gearing up to run that extra mile, customers would already have ensured they’ve identified their critical systems, encrypted sensitive data, applied all relevant patches, be on a supported product release, use tools to ensure configurations are locked down - in short, the usual security hygiene - before they attempt to find zero day vulnerabilities in the products they are using. And in fact, there are a lot of data breaches that would be prevented by doing all that stuff, as unsexy as it is, instead of hyperbolizing that the Big Bad Advanced Persistent Threat using a zero-day is out to get me! Whether you are running your own IT show or a cloud provider is running it for you, there are a host of good security practices.
What’s the Point?

Incident response plan

Using strong encryption

Employee training

Rapid detection
Copyright © 2014 Andrews Kurth LLP. No lawyer-client relationship exists until the appropriate engagement letter has been executed. The enclosed information has been compiled to establish potential interest in the services of Andrews Kurth LLP. It is agreed and understood that Andrews Kurth LLP has neither given nor received confidential information and none of our discussions will preclude Andrews Kurth LLP or any other Andrews Kurth entities or lawyers from future representation of others with interests adverse to you if no lawyer-client relationship results from our discussions. Andrews Kurth LLP is a Texas limited liability partnership.
Don’t Prejudge An Investigation

Attorney Benjamin Wright
Benjaminwright.us
This is education, not legal advice. If you need legal advice, you should consult your organization’s lawyer.
Information Security Law and Politics Are Dangerous

- Plaintiff lawyers want to make money
- Politicians and regulators want to attract attention
- The media want to attract viewers
Arguable We Give Too Many Breach Notices

• State of Ohio loses unencrypted backup tape containing social security numbers
• Spends $3 million on breach notice and credit monitoring service
• But risk of harm to “victims” was virtually zero
• Similar: University of Utah 2008
Legal Standards Are Subjective and Open to Interpretation

• HIPAA Omnibus Rule 2013
• Incident presumed to be a breach UNLESS a risk assessment shows low risk of harm, recognizing
  – Was risk mitigated?
  – Was data actually viewed or downloaded?
  – Nature of the data and likelihood of identification
Legal Adversaries Can Disagree with University’s Interpretation of the Facts

- Reasonable minds can look at same facts and reach different conclusions.
- But adversaries may not be entitled to know about university’s interpretation.
Breach at Lucile Packard Hospital at Stanford University

- Hospital saw it had an “incident.”
- After investigation, it gave notice.
- Notice required within 5 days.
- California Department of Public Health said notice from hospital was late.
- CDPH claimed hospital owed $250,000.
- They settled for $1100 on a technicality; both parties claimed victory!
Lessons from Packard Hospital

• Legal adversaries want to punish and shame the institution.

• Adversaries would love to get institution’s internal investigation records . . . so the adversaries can second-guess whether there was a breach or whether it was handled properly.
When You Have an Incident ...

• You don’t know whether you had a “breach” until you complete an investigation.
• Investigation can take time and sweat.
• Investigation might conclude no breach because (for example) no significant risk of harm.
• Or investigation might reach other conclusions that adversaries disagree with.
University Has Incentive to Keep Investigation Confidential

• First, limit who has knowledge of the investigation.
• Second, cloak investigation in “attorney work product”
• “Attorney work product” prevents details of investigation from being disclosed under subpoena or lawsuit.
What is “Attorney Work Product” Doctrine?

• Similar to attorney-client privilege
• Protects details of investigation conducted under auspices of attorney.
So, When “Incident” Arises

• Don’t jump to conclusion you have “breach”
• Don’t write email saying you have “breach”
• Involve legal counsel early
• Label reports, risk assessment and emails “attorney work product”
• Keep legal counsel engaged in the investigation
Conclusion

- Staff should avoid jumping to conclusions. Staff are not qualified to reach legal conclusions before investigation is complete.
- IT Department and legal staff should plan in advance for how handle incidents.
Closing Comments & Questions

UTD Information Security Office
Nate Howe CISO
Thank You For Attending

UTD’s Information Security Office
Distinguished Speaker Series

Benjamin Wright  Ben Setnick

Special thanks to our presenters

securityawareness@utdallas.edu