BIG UNIVERSITY 2018

BIG UNIVERSITY 2018

Bonus Session

"Legal Tech Talk for Your 21st Century Business"

Don Geiter, Scott Landis & Joe Falcon (Barley Snyder)

Cyber-risk Oversight

Presented by Don Geiter, Barley Snyder

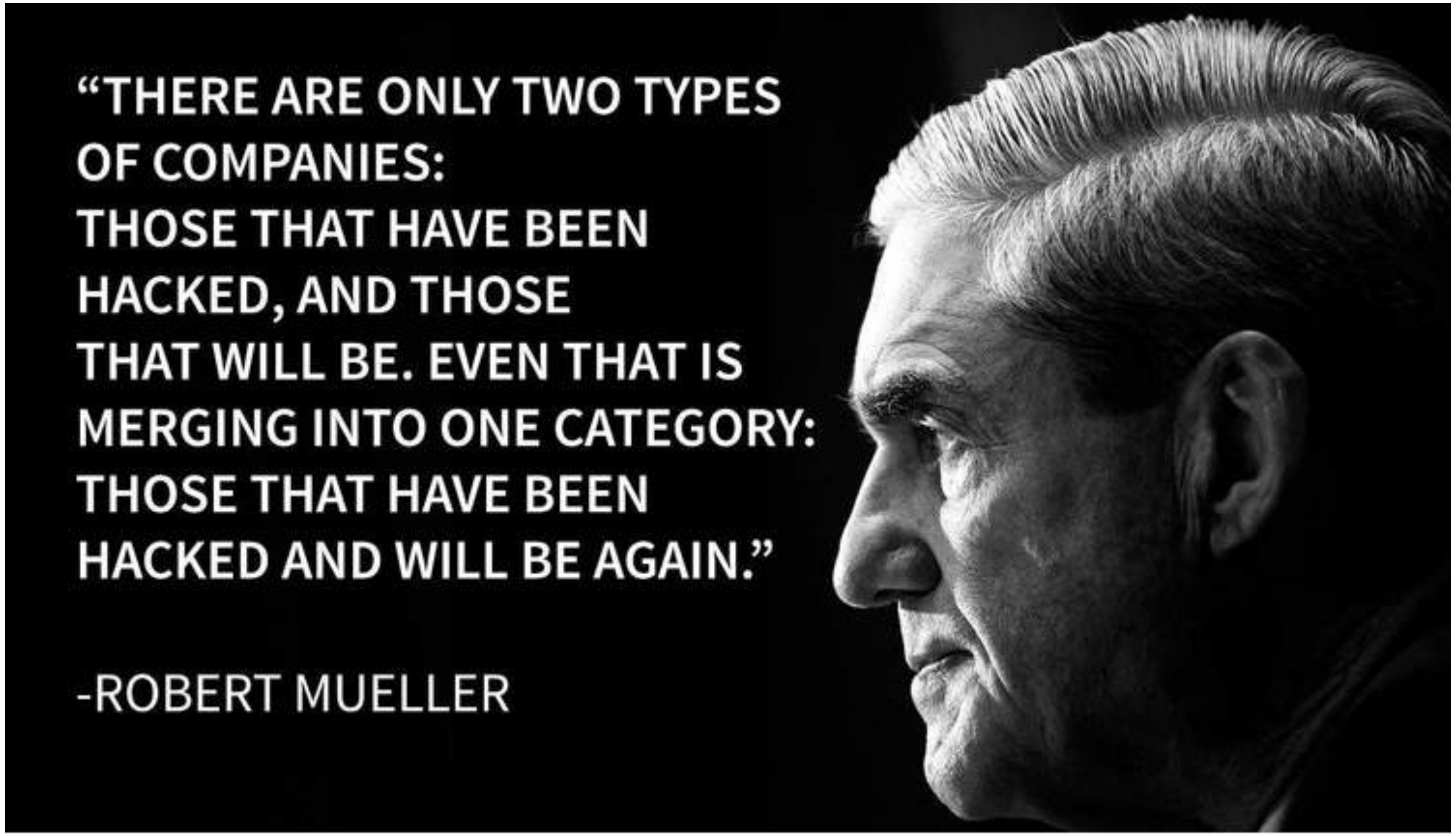
Barley Snyder

ATTORNEYS AT LAW

Cyber-risk oversight

- Do we have a cybersecurity “culture”?
- What are the legal implications?
- Who are my experts and what are my resources?
- How do we balance the risk?

Cybersecurity culture



Federal/EU Regulations

- Broad **consumer protection** laws (i.e., Federal Trade Commission Act).
- Laws that apply to **particular sectors** (i.e., Gramm-Leach-Bliley Act and Health Insurance Portability and Accountability Act (HIPAA)).
- Laws that apply to **types of activities** that use personal information (i.e., Telephone Consumer Protection Act (TCPA) and Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act).
- GDPR

State Laws

- Hundreds of privacy and data security laws governing collection, use, protection and disclosure of personal information exist at state level, with inconsistent scope and obligations.
- All states and D.C. have data security laws.
- Congress has been considering multiple proposals for a federal data protection/notification law that may preempt state laws.

Industry Guidelines

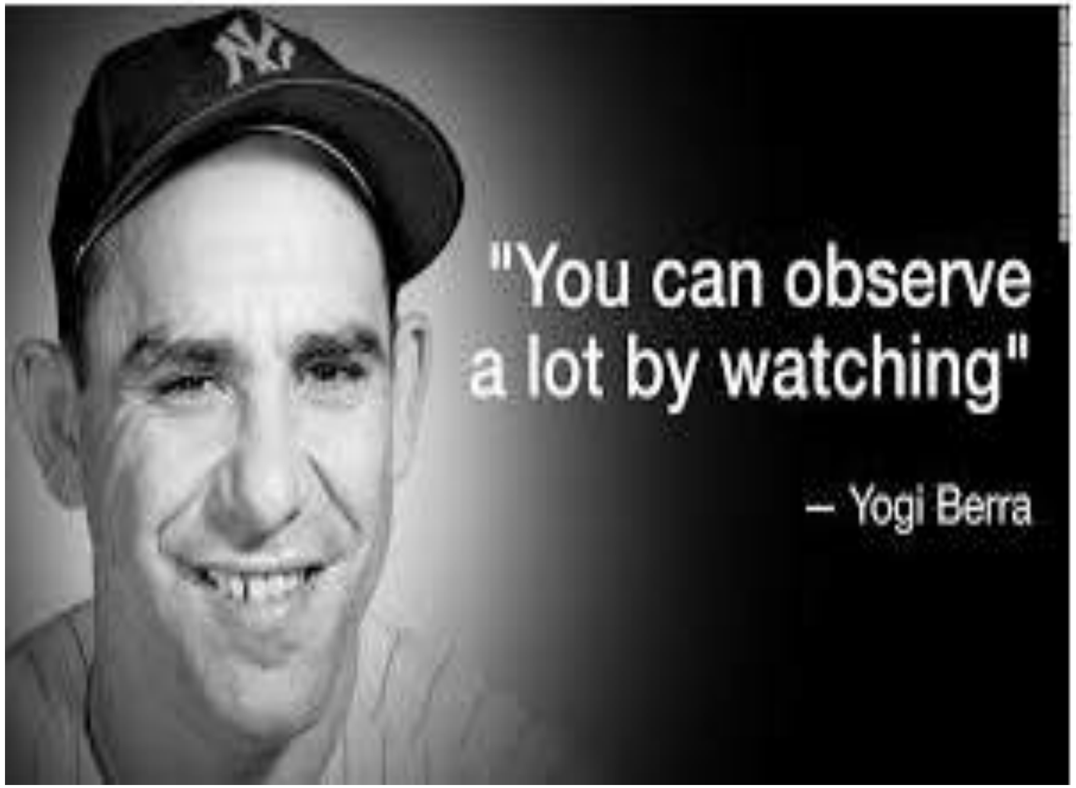
- Guidelines issued by many industry groups are generally considered best practices in those industries (such as the payment card, mobile marketing and online advertising industries), but do not have the force of law.
- The Mobile Marketing Association's Code of Conduct for Mobile Marketers – guidelines for companies advertising on mobile or wireless devices.
- The Payment Card Industry Data Security Standards (PCI DSS) require all entities who process, store or transmit cardholder data to comply with 12 basic security requirements.
- EMV Liability.

Experts and resources

- What is cyber literacy?
- Do we have access to expertise?
- What do management's reports to the board look like?

The risk balance

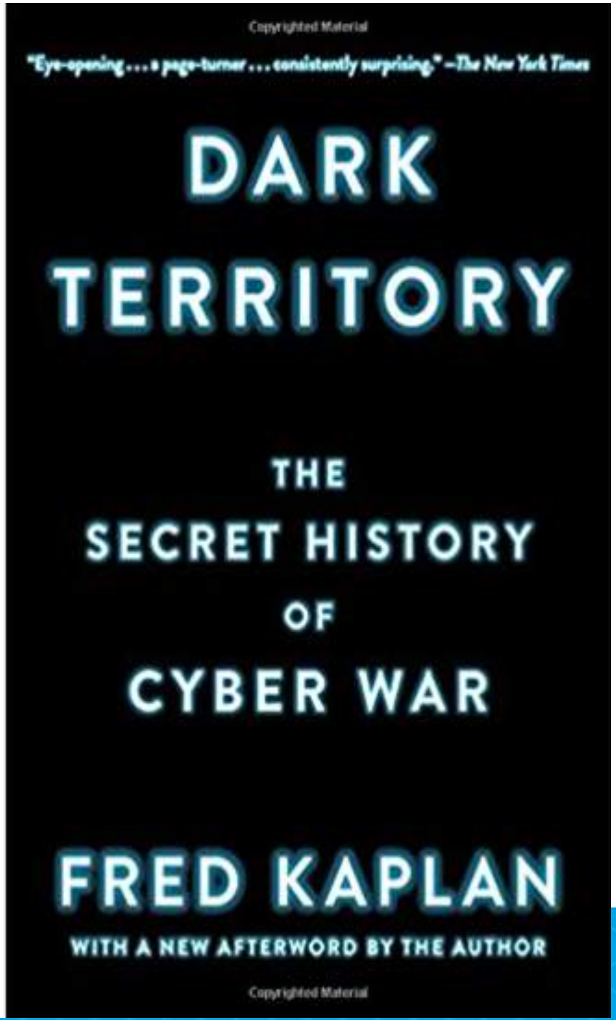
- A word about cyber insurance…

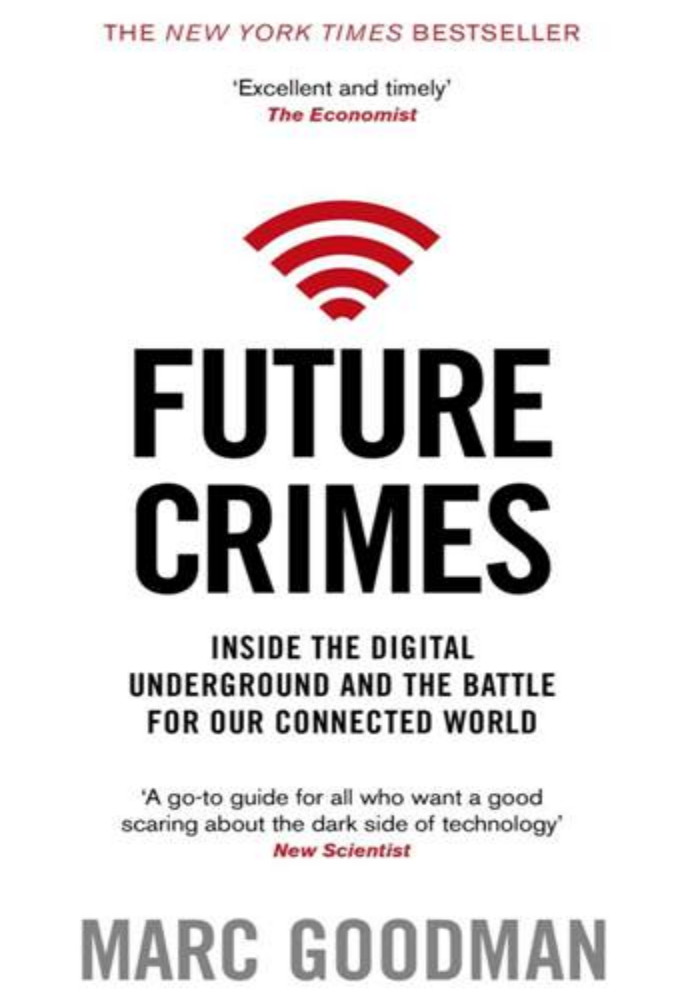


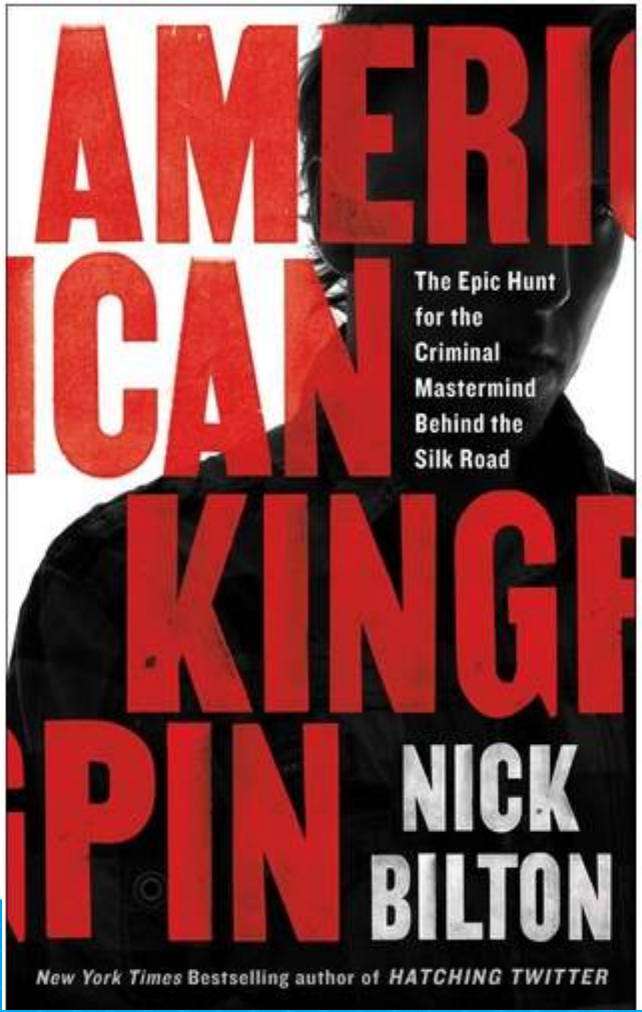
What is cyber insurance, Yogi?

"It's the insurance you really need to have; if you don't have it, that's why you need it."

Bonus material – Summer Reading Plan







Cyber Security: Public Internet Access and the Associated Risks

Presented by Joe Falcon, Barley Snyder

Barley Snyder
ATTORNEYS AT LAW

The Internet Provider

- Among the policies and procedures must often over-looked within businesses who are analyzing their information security risks are those relating to Internet and/or WiFi connectivity provided at a place of business.

Responsibility of Users

- The Internet provider, such as a business owner, may find that he or she is responsible for activity conducted by patrons using that access.
- There are different types of conduct the provider should be concerned with, especially when providing public Internet access to patrons:
  - Illegal activity
  - Infringement
  - Privacy

Illegal Activity

- A patron conducting illegal activity using provided public Internet access is a business owner's primary concern.
- Without restrictions, a patron can easily:
  - access child pornography,
  - purchase controlled substances, or
  - conduct myriad other illegal activities.

Infringement

- Copyright infringement is the use of works protected by copyright law without permission, infringing certain exclusive rights granted to the copyright holder, such as the right to reproduce, distribute, display or perform the protected work, or to make derivative works.
  - Purchase counterfeit goods
  - Access unauthorized copyright content, such as music or films without permission
- It is important for the business owner to identify who is using their Internet access.

Privacy

- Any patron using unprotected public Internet access is open to a range of attacks.
  - personally identifiable information, such as the patron’s address, credit card numbers, or
  - other potentially damaging private data, including employer trade secretes and client confidential information.

Recommendations

- Draft and adopt a public Internet access policy.
- Prepare and use an agreement and disclaimer for conditions of use, including prohibitions and authorizations of use.
- Consider using a controlled sign-in or password access system.
- Consider using filtering programs which block access to sites known to promote illegal activity.

Considerations in Cloud Computing Agreements

Presented by Scott Landis, Barley Snyder

Barley Snyder

ATTORNEYS AT LAW

SAAS (Cloud Computing) v. Traditional Software Licensing

- Traditional Software – Licensor provides one or more copies of software for customer's on-site use.
- SAAS – Many customers share access to the software through the provider's remotely located server.

Potential Benefits of SAAS

- Reduced cost
- Increased efficiency
- Increased data security
- Data back-up / business continuity
- Software always up to date

Typically Standard Terms and Conditions

- Negotiability of terms will depend on:
  - Customer's bargaining power
  - Type of service
  - How critical the service is to the customer's infrastructure
  - The sensitivity of the data
  - The size of the transaction

SAAS Agreement Considerations

- Pre-agreement Due Diligence
- Uptime Service Levels
- Response Time Service Levels
- Remedies for Service Level Failures
- Data Security
- Notification of Security Issues

SAAS Agreement Considerations

- Disaster Recovery and Business Continuity
- Use of Customer Data
- Data Conversion and Transition
- Insurance
- Indemnification
- Limitation of Liability

SAAS Agreement Considerations

- License / Access Rights
- Term
- Warranties
- Training / Support

Questions/Discussion

Thank you to our sponsors

Barley Snyder
ATTORNEYS AT LAW

Barracuda

CISCO

D&H

DUO

KnowBe4
Human error. Conquered.

Maryland Construction Network

McCONKEY & CO.
INSURANCE & BENEFITS
Innovative Solutions. Traditional Values.

VIEWPOINT

RADWIN

ydop
Near-user Marketing®