PLUS

PROFESSIONAL LIABILITY UNDERWRITING SOCIETY

The Frontier of Cyber Risk and Litigation: How Developing Technologies Will Change Cyber Risk

Presented by PLUS Diamond Sponsors

AXIS beazley CNA We can show you more. SOMPO INTERNATIONAL HISCOX encourage courage TRAVELERS

Meet The Presenters

Peter Cridland
Assistant Vice President
TransRe
https://www.transre.com/
pcridland@transre.com

Richard Sheinis
Hall Booth Smith, P.C.
www.hallboothsmith.com
(980) 859-0381
@SheinisCyberLaw

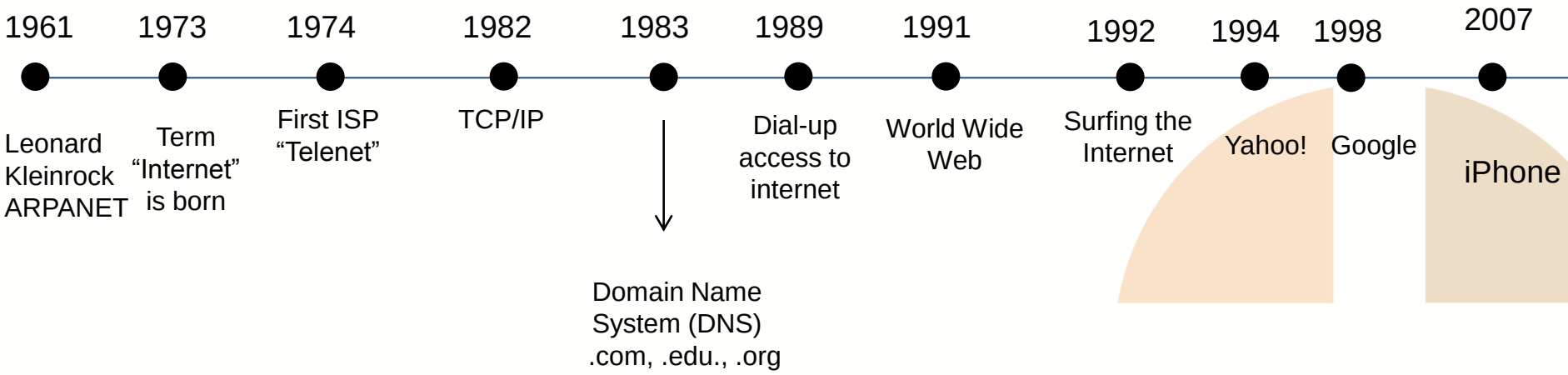
PLUS

The information and opinions expressed by our panelists today are their own, and do not necessarily represent the views of their employers or of PLUS. The contents of these materials may not be relied upon as legal advice.

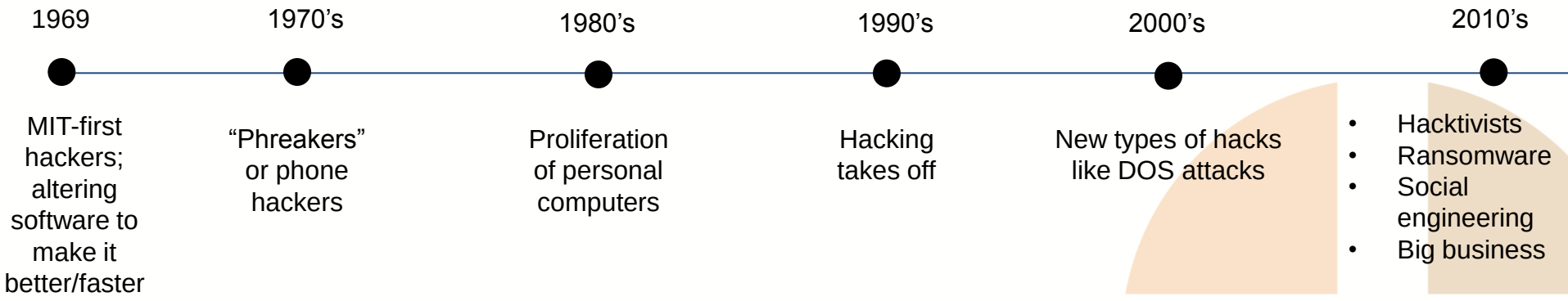
A copy of the presentation slides will be available following this webinar, on the PLUS website at: www.plusweb.org

Where Have We Been?

Internet



Hacking


1969
MIT-first hackers; altering software to make it better/faster
1970's
"Phreakers" or phone hackers
1980's
Proliferation of personal computers
1990's
Hacking takes off
2000's
New types of hacks like DOS attacks
2010's
• Hacktivists
• Ransomware
• Social engineering
• Big business

PLUS

Risk & Litigation

- **Litigation…been there, done that**
  - Class action, but few “individual” suits
  - Few privacy lawsuits; privacy has been left up to the federal regulators
- **Plaintiff’s bar coming up with novel theories, i.e., no breach but your poor security put me at risk.**
- **Increased regulatory scrutiny**
  - New York State Cybersecurity Rule, Trump Cyber Executive Order
  - Fines: HHS, AG, etc.
- **Breach Costs**

PLUS

Why Is This All About To Explode?

Fifth Generation Wireless ("5G")

- 2020
- At least 40x (100x) faster than 4G
- 4x more coverage worldwide than 4G
- Opening of high frequency spectrum carries significantly more data

PLUS

We will experience many of the same threat vectors :

- **Ransomware**
- **Phishing/Spear Phishing/Whaling**
- **Pharming**
- **Social Engineering**
- **SQL Injection Hacks**
- **Password brute force attacks**
- **But with greater frequency…**
  more data, more endpoint users,
  more targets, more wireless connections,
  more opportunity

PLUS

IOT Security Risk

IoT is set to become a raging inferno of cyber-attacks…

The crippling DDoS attacks that paralyzed a school and took out Twitter, Spotify, PayPal, Verizon, Comcast, and others, were launched using a **botnet** built from IoT devices. The Mirai malware that made it all possible was estimated to have infected over 500,000 IoT connected devices and brought down more than 80 large websites.

Tony Olzak, “techspective”

PLUS

Artificial or Machine Intelligence

Computer systems that are able to perform tasks that normally require human intelligence.

Hacking devices and obtaining increasing amounts of publicly available information to learn your thoughts, apply AI algorithms, to guide social engineering and phishing.

PLUS

Where Will This Take Us?

- Less need for physical connections
- Wireless World (more openings to be exploited)
- Greater connectivity will lead to faster growth of IoT
- Huge amounts of data being transmitted wirelessly.

PLUS

Want Some Specifics?

- **Internet of things**
  - **2015 ⇨ 10 billion devices connected to the internet**
  - **2020 ⇨ 34 billion devices connected to the internet**

Connected thermostats, refrigerators, security systems, (“smart homes”) wearables, nanny cams, home assistants (Alexa, etc.)

*** Medical devices!**

All of this generates huge amounts of data that includes personal Information, location information, personal preferences

What happens when a hacker takes control of your home or car?

PLUS

- **Where is the insurable risk?**
- **Where is the legal risk?**

Is it on the device manufacturer?

Data Center?

Data Analyzer?

Homeowner or device user?

A combination of the above?

PLUS

Telemedicine and Wearables

Large hospital has 10-15 medical devices per bed and most are internet enabled

- Insulin pumps
- Pacemakers
- CT scanners
- MRI machines
- Dialysis machines

Each internet connected device is a potential opening for a hacker to compromise the device, harm the patient, gain access to the entire hospital network.

PLUS

HYPOTHETICAL

If a hacker compromises an internet connected medical device in a hospital, and interrupts the care to the patient, which causes harm to the patient, how do you determine liability?

- Is it a med. mal. case with liability on the doctor?
- Is it the fault of the device manufacturer because the device was not secure?
- The fault of the hospital because it did not maintain or update the security of the device?
- What about the software company that designed the software for the device?

PLUS

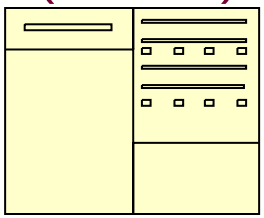
HYPOTHETICAL

A Hospital is subjected to a ransomware attack, during which all EHR are unavailable. Hospital staff resort to handwritten notes, and when Patient X is transferred from the ER to the ICU her pharmacological allergy is not noted. Patient X then is injured by an allergic reaction in the ICU.

- **What policy responds? EHR has changed normal procedures and duties such that basic information like allergies may normally be assumed to have been given to any treating physician – is there a separate liability for the hospital for failure to protect their EHR / IT system?**

PHYSICIAN
(Boston)

Computer Server
(Atlanta)



HOSPITAL
(Idaho)

What happens when a hacker compromises the internet connection mid-surgery? Yikes!

- Proposed Medical Device Cybersecurity Act of 2017 (S. 1656)

PLUS

Real Time Monitoring Of In Home Patients

- Blood sugar
- Blood pressure
- Other vital signs
- Sleep
- Respiration

Ingestible sensors put the doctor in the patient

(See, www.proteus.com)

PLUS

Transportation

Driverless cars, trucks and heavy construction vehicles!

No longer is a traffic accident the fault of one driver or the other.

- **Imagine huge construction equipment operated through the internet by a person miles away. What happens when a hacker takes over the crane with the ability to stop the work, hold the crane for ransom or cause injury?**

Who has the risk?

PLUS

BANKING AND FINANCE

- **Bitcoin (Blockchain Technology)– reputation as the currency of hackers v. growing acceptance in financial markets**
  - Largely anonymous transactions, difficult to trace
    - BTC-e fined $110M, owner arrested
  - Lightning Network innovation: instant micropayments, increasing speed and capacity of the bitcoin network
  - Chicago Board Options Exchange (CBOE) and U.S. Commodity Futures Trading Commission (CFTC) to offer bitcoin futures
  - Market analysts currently predicting bitcoin as the best asset through year end 2017

PLUS

MICROCHIP IMPLANTS

Microchip, using RFID technology, is implanted in a person's hand and is used to open door, gain access to your office, unlock smart phone, and other authorizations. (See, Three Square Market and the Swedish company Biohax International.)

Cannot turn it off, cannot put it away. Potential non-stop tracking device that can be hacked.

PLUS

Privacy v. Security

Increased frequency of privacy related litigation

- **EU General Data Protection Regulation – emphasis on privacy rights with private cause of action for privacy violations**
- **Increased surveillance**
- **Facial recognition**
- **Google Glass Enterprise Edition**
- **Exponential growth in data availability**
- **Data sharing**
- **Opportunity for class actions**

PLUS

MORE TO COME…

- Disney faces privacy complaint over children's apps
- Record level of data privacy complaints made to Data Protection Commissioner (Ireland)
- Chicago Law Firm Accused of Lax Data Security in Lawsuit (“a data breach waiting to happen”)
- Facebook can help detect depression, schizophrenia, study says

Hypothetical

An employer hires a psychology expert to analyze a job applicant’s social media posts, as well as information about the applicant’s driving habits, and purchasing behavior.

- Is this an employment law violation, a privacy violation?

PLUS

Questions

Please submit using the question tool on user dashboard

Thank You Presenters

Peter Cridland
Assistant Vice President
TransRe
https://www.transre.com/
pcridland@transre.com

Richard Sheinis
Hall Booth Smith, P.C.
13024 Ballantyne Corporate Place
Suite 625
Charlotte, NC 28277
www.hallboothsmith.com
(980) 859-0381
@SheinisCyberLaw

PLUS

Presented by PLUS Diamond Sponsors

PLUS

Thank you for your time.

A replay of this webinar will be available to PLUS Members at:
www.plusweb.org