AGENDA

• ARE WE AT WAR?
• REGULATIONS IN THE DOMESTIC BATTLEFIELD.
• HOW CAN YOU ARM YOURSELF?
THE CYBER WAR IS REAL

• 87% of infosec specialists believe in midst of cyber war (RSA 2019)

• Quote from Head of US Cyber Command – “in the cyber domain...our adversaries...continue to increase in sophistication, magnitude, intensity, volume and velocity, and remain a threat to our national security”
PRIVATE ORGANIZATIONS ON THE OFFENSIVE?

• 72% believe nation-states have a right to “hack back”
• 58% believe private organizations should have right to “hack back”
• Currently, no legal right to do so
  – Prohibited by Computer Fraud & Abuse Act
  – May Change – proposed Active Cyber Defense Certainty Act (ACDC)
ISSUES WITH “HACK BACK”

• Lack of oversight
• Issue of determining attribution
  – More challenging with use of IoT
• Interference with law enforcement
• Dangerous escalation?
  – Foreign nation-state
WE ARE AT WAR, TIME TO DEFEND

- Better to strengthen defenses
- Develop / implement a plan to mitigate risk
IS ANYONE IMMUNE?

• 58% of malware attacks are against SMBs
  – Easy targets
  – More vulnerable than large corporations
• 92.4% of malware delivered via e-mail
  – All companies rely on e-mail
• Jupiter estimates that 33 billion records will be stolen in 2023
  – 50% of these will be from the U.S.
• Between 2015-2017, U.S. accounted for 38% of targeted attacks, world-wide
NATION-STATE ATTACKS

- Nation-States targeting U.S. and others
  - WannaCry – North Korea
  - NotPetya – Russia
  - Turla – Russia
  - Skulls – North Korea
  - OPM Attack – China
  - Sony – North Korea
  - Triton malware (Saudi Arabia) – Iran
  - Stuxnet – U.S. / Israel target Iran
• IRP companies, e.g. Black Carbon
  – Reporting China now leading source of cyber attacks
  – Stealing U.S. IP – fastest, easiest way to compete with U.S., commercially
Companies also must battle with domestic concerns, mainly regulators

- GDPR
- CCPA
- CA IoT regulation
GDPR

• GDPR
  – Arrived May 25, 2018
  – Significantly more individual data protection rights
    • General Data Protection Regulation (GDPR) the European Commission has strengthened and unified data protection for individuals within the European Union (EU), while addressing the export of personal data outside the EU
    • Potentially more significant penalties
    • Avoid being the first example
    • Consider matching compliance to get ahead of US law changes, states & federal
• Background of CCPA:
  • Passed in July of 2018 due to data privacy concerns (mini-GDPR).
  • Goes into effect on January 1, 2020.
  • Applies to all personal information (PI) collected by an organization, whether or not collected electronically.
  • PI defined broadly. Information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, to a particular consumer or household.
How will the CCPA apply to you? Consumers granted 5 rights:

1. The right to know what information is being collected;
2. The right to have access to that information;
3. The right to deletion of their PI;
4. The right to opt out of an organization selling their PI; and
5. The right to equal service (non-discrimination in services provided), if they opt out of the selling of their data.
CALIFORNIA CONSUMER ACT (CCPA)

Must update privacy policies to comply with the law.

• Must understand your data. What PI is being collected, where it is sourced from, what it is being used for, whether it is being sold or shared, and to whom, etc.

• Must be able to respond within 45 days to verified consumer requests for information about what PI was collected in the past 12 months, free of charge.

• Must be able to delete consumers’ PI, upon a verified request (with exceptions).

• Must provide consumers with the ability to “opt out” of the sale of their PI and ensure their data is not sold after opting out.

• Must update privacy policies and websites to include a link to an “opt out” web page.

• Must obtain opt-in consent from a child’s parent or guardian before selling their PI.
What happens if you are not in compliance on 1/1/20?

- 30-day window to cure violations.
- The AG may bring an enforcement action with statutory penalties ($2,500 fine per violation not cured within 30 days and $7,500 fine per violation for intentional violations).
- Private right of action if data breach occurs exposing PI that results from failure to implement “reasonable security procedures and practices.” (PI here defined less broadly in Civil Code Section 1798.81.5(d)(1)(A)). Damages of $100-$700 per consumer or actual damages, whichever is higher.
IoT, or “Internet of Things,” is the integration of sensors and devices into everyday objects that are connected directly or indirectly to the internet.

These devices collect and transmit massive amounts of personal information and often have security vulnerabilities that increase the risk of cyberattacks and exposure of PI.

Examples are Amazon Echo, Google Home, Hue Lights, Nest doorbells, smart televisions, cameras, sprinklers and thermostats.
• Law goes into effect on January 1, 2020.
• Requires manufacturers of IoT devices sold in California that connect directly or indirectly to the internet and that have a Blue Tooth or IP addresses to equip them with “reasonable security features.”
• Impetus behind the law is to decrease security vulnerabilities, prevent cyberattacks and prevent the exposure of data/PI collected and transmitted by the devices.
Manufacturers of IoT devices, including Smart Home devices, that are sold in California will need to comply. Builders will need to ensure that Smart Home devices installed in homes built in California comply.

Compliance is left up to the device manufacturers as “reasonable” security measures lacks specifics in the law. Security measures must be: (i) appropriate to the nature and function of the device; (ii) appropriate to the information collected, contained or transmitted; and (iii) designed to protect the device, and any information contained in the device, from unauthorized access, destruction, use, modification or disclosure.

In reality, all IoT devices will have to comply due to the CA market.

No private right of action; only enforceable by the Attorney General.
SPECIFIC STANDARDS

• UL 2900
  – Series of standards created to provide manufacturers with testable and measurable criteria to assess software vulnerabilities, weaknesses and the presence of applicable security controls in the design, development and maintenance of network-connectable products
SPECIFIC STANDARDS

• UL 2900 a widely recognized standard
  – White House Cybersecurity National Action Plan (CNAP)
  – FDA – for testing medical devices
  – ANSI (American National Standards Institute) standard
SPECIFIC STANDARDS

• ISO / IEC 27001
  – Standards to bring information security under explicit management control
  – 3-year certification
  – Widely viewed at high level standard
STANDARDS – WHAT SHOULD YOU DO?

• Key - must do something
• Following either standard (or others) creates defensible cybersecurity strategy
  – Strong evidence of being “reasonable”
• UL 2900 – More specifically geared towards IoT
• ISO / IEC 27001 – More overarching, systematic approach to information security
HOW TO DEFEND YOURSELF

• Focus on medical industry
  – Array of risks
  – Attack vectors
  – Reaction
WIDE ARRAY OF RISKS

• Massive amounts of PII
  – Don’t forget about employee information
• Medical devices
  – External
  – Internal
• Importance of availability
• Integrity of information
• IP assets
• Reputation
VARIOUS ATTACK VECTORS

• Physical Intrusion
• Exploitation of vulnerable software
• Attack mobile devices
• Disrupt / hijack internal devices
• Phishing / malicious e-mail
METHODS TO DEFEND

• Culture of security / awareness – leadership
• Strengthen IT, security infrastructure
  – Implement strong security controls
• Physical security
  – Hospitals, work stations, mobile devices, IoT
• Training employees
• Prepare / practice an IRP
• Vendor compliance program
• Insurance
KEY TAKEAWAYS

• Protect assets by protecting organization
• Need for complete, global holistic approach
• Do something, don’t wait!!
CONTACT US

Jeff Dennis
Jeff.dennis@ndlf.com
949-271-7316