Cybersecurity: Limiting the Harm to Lawyers and Their Clients

SCG Legal
Presented September 8, 2014
If the device can be connected to the Internet, it is susceptible to being hacked.
Key Issues

- PRIVACY
- SECURITY
- PRODUCT SAFETY
- BUSINESS SECRETS
- IP
Hacker Motives

- Criminal intent
- Corporate espionage
- State actors
Relevant Standards

- Federal – no statute, but the NIST standards; federal prosecutors use other statutes to gain convictions, e.g. mail fraud, wire fraud, conspiracy, etc.
- States – 45+ have adopted related privacy and notice laws – and each is different
- Does your industry have a cyber standard?
National Institute of Standards and Technology
Personally identifiable information or PII is "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual‘s identity, such as name, social security number, date and place of birth, mother‘s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information."
By way of example, a user's IP address as used in a communication exchange is classed as PII regardless of whether it may or may not on its own be able to uniquely identify a person.
Commercial Definition – PII

- Individual’s name – along with one of the following -
  - Social Security No.
  - Driver’s License No. or
  - Financial account number in combination with any security code, access code, or password
NIST – PII Defined

- Name, such as full name, maiden name, mother’s maiden name, or alias
- Personal identification number, such as social security number (SSN), passport number, driver’s license number, taxpayer identification number, or financial account or credit card number
NIST – PII

- Address information, such as street address or email address
- Personal characteristics, including photographic image (especially of face or other identifying characteristic), fingerprints, handwriting, or other biometric data (e.g., retina scan, voice signature, facial geometry)
NIST - PII

- Information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, medical information, education information, financial information).

- Partial List
Federal Standard
Background

- *Improving Critical Infrastructure Cybersecurity* – EO 13636 – February 2013
- Cybersecurity Framework – NIST Standards – February 2014
Framework Standards

Provide a unified process by which to evaluate your cybersecurity program:

1) Describe your current cybersecurity posture;
2) Describe your target state for cybersecurity;
3) Assess progress toward your target state;
Framework Standards

4) Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process; and

5) Communicate among internal and external stakeholders about cybersecurity risk.
Framework Core

The Core covers five concurrent and continuous functions — Identify, Protect, Detect, Respond, Recover — designed to provide a 100-foot view of the lifecycle of an organization’s management of cybersecurity risk.
Framework Core

For each of these lifecycle functions, the Core then identifies underlying key categories, and subcategories, and matches them with exemplar references, such as existing standards, guidelines, and practices.
Framework Implementation Tiers

- Provide a numerical representation of how advanced an organization’s risk-mitigation procedures are, given the threat environment, legal and regulatory requirements, business/mission objectives, and organizational constraints. The Tiers range from Partial (Tier 1) to Adaptive (Tier 4).

- “Progression to higher Tiers is encouraged when such a change would reduce cybersecurity risk and be cost effective.”
A Profile enables the organization to establish a road map for reducing cybersecurity risk in a manner aligned with organizational and sector goals, considers legal and regulatory requirements and industry best practices, and reflects appropriate risk-management priorities.
Framework Profile - Results

- Armed with the results or ranking, the Framework allows the organization to evaluate risk vulnerabilities and create a prioritized action plan to address those gaps.

- The question for all companies then becomes how best to adapt to these new recommendations and do so in a cost-effective and meaningful manner.
Legal Fallout

- Federal and state investigations
- Internal investigatory costs
  - Legal, forensic specialist, firings, terminations, process changes, system expenses (hard and soft) reputation and so on
- Shareholder derivative actions
- Class action lawsuits
Supply Chain Security

- C-TPAT – AEO
  - Mutual recognition – Canada, EU, Japan, Jordan, Korea, New Zealand and Taiwan
- Human trafficking
- Lost or damaged cargo
Internal Investigation – Initial Questions

1) Are there government agencies to which we are obliged to give notice about what happened? If so, is there a specific time frame under which we must act?

2) What do we tell our customers and clients and when?

3) What do we tell our staff and when?

4) Who on our staff was involved and what punishment is merited? Is our only choice to fire the people involved?
Investigation – Initial Questions

5) When do we tell our Board? Shareholders? Should we report what happened to law enforcement? If so, to what agency and when?

6) If a vendor was involved, must we change vendors? If so, how quickly? Can we afford to cut off that vendor?
Investigation – Best Practices

- Call your outside lawyer, then jump right in.
- Preserve all available evidence as soon as possible and before meeting with witnesses.
- Chase down all reasonable leads, regardless of where they might take you, ask the tough questions, and be flexible.
Internal Investigation – Best Practices

- Document witness interviews appropriately.
- Do not jump to conclusions.
- Once you have the outcome, take prompt but reasonable action.
- Involve ownership/upper management from the outset.
Vet Your Business Partners

- Do they have the equipment, facilities and staff to work with your company and provide quantity and timeliness?
- Do they comply with local labor and social laws?
- Do they fully understand any special or regulatory requirements?
- Are they willing to promptly inform you when changes are made?
More Factors

- What about other changes that affect compliance?
- Do you regularly check their cyber and other security measures?
- Have you tested if they interface with you in a secure manner?
- Document and keep records.
State Requirements Clearly

- Use your purchase order to clearly state your expectations
- Include penalties for non-compliance with your requirements
- Use whatever commercial leverage you have to insure compliance
Periodic Verification

- Periodically verify the information being given you by your business partners
- Do not simply collect documents – assign someone to verify information and do so regularly and in a timely manner
Deals are no longer just about quality, cost and delivery date
It Really Is All About Due Diligence
MISFORTUNE COOKIES
(MADE IN CHINA)

;) WE'VE HACKED INTO
YOUR GOVERNMENT

;) YOUR BUSINESSES

;) YOUR MEDIA

Star Advertiser  A8 >> MONDAY 2/25/13