Legal Considerations for Incident Response

ISSA Phoenix Chapter
Q2/16 Chapter Meeting
April 12, 2016

Patrick Fowler and Tony King
Snell & Wilmer L.L.P.
One Arizona Center ● Phoenix, AZ 85023
Legal Considerations for Incident Response

Context!

- You hold other people’s valuable info. Bad actors want it.
- Threat eco-system is constantly evolving.
  - Internal and external threats, nation-state actors, human error
- Laws/regs/standards are in flux. Yet compliance is expected.

- There’s a report of a possible data breach... Are you ready?
- Many possible breach portals/access points - What happened?
  - Lots of players involved, internally and externally
- People are anxious/unhappy/looking to blame or CYA
- Time, money and reputations are all at stake
Cyber Threat Environment

- Annual global corporate losses to cyber crime and data breaches:
  - 2014: $375 - $575 billion
  - 2019: $2.1 trillion

- Annual global corporate spending on cybersecurity solutions:
  - 2015: $75 billion
  - 2020: $170 billion

Context

This is good cyber security, relatively speaking:
Context

This is bad cybersecurity:
Recipes for Disaster

**Awareness**

- 91% of the high vulnerable board members say they can’t interpret a cybersecurity report.
- Only 10% of the high vulnerable respondents agree that they are regularly updated with information about the types of threats to cybersecurity that are pertinent to their business.
- The low vulnerable respondents are 31% more likely than the high vulnerable respondents to have assessed the likely losses associated with cyberattacks.

**Readiness**

- 98% of the high vulnerable executives are not confident their organization tracks all devices and users on their system at all times.
- 87% of the high vulnerable board members and executives don’t consider their malware, antivirus software, and patches to be always up-to-date.
- Only 9% of the high vulnerable board members said their systems were regularly updated in response to new cyber threats.

Source: Accountability Gap: Cybersecurity and Building a Culture of Responsibility, Tanium, Inc. & NASDAQ (April 2016)
Is this the right time to start thinking about creating a fire drill and escape plan?
A Potentially Violent Collision Between Cyber Security and the Law

• The law always lags behind technology.
• Disputes are often decided by people unfamiliar with technological advances.
• So, disputes are resolved via analog principles, even if they don’t necessarily fit well, because that’s the best we can do.
Standard of Care

- Did your company comply with “the law”?  
  - Statutes, regulations, common law
- Were your company’s efforts “reasonable”?  
  - How did those efforts compare to industry practices?  
  - Did they satisfy applicable standards?  
  - Were they checked and certified by a credible third party?
- Are your company’s efforts well-documented?  
  - *If it’s not written down, it never happened.*
Evaluating “Reasonable” Conduct

• Your pre-Incident policies and practices will be evaluated.
  – Were the board and c-suite leaders engaged and informed?
  – Did you take reasonable steps to protect the information?
  – Were you reasonably prepared for the incident?

• Your post-incident response will be evaluated, too.
  – Did you follow your pre-incident policies and procedures?
  – Did you timely respond?
  – Was your incident response effective?
    • Did you limit the financial and reputational damage to the company?
    • Did you limit the exposure to affected customers/employees, etc.?
Evaluating “Reasonable” Conduct

• Pre-Incident management practices:
  – *Bona fide* corporate board and c-suite involvement
    • Assures appropriate direction and resources
  – Information Governance Plans
    • Record Retention/Destruction Policies, Data Maps
  – Information Security Processes and Procedures
    • Employee Training in InfoSec and Privacy
    • Vendor Management
  – Understand the evolving applicable regulations and laws
    • Multi-jurisdictional (state, federal, international)
      – Neither uniform nor consistent re information protection or breach response rules
    • Industry standards and practices
Legal Considerations for Incident Response

• Pre-Incident (con’t.):
  – Incident Response Plan
    • Response Team: Legal Counsel, Forensics, Communications/P.R., Remediation Provider, Law Enforcement Contacts, Regulator Contacts
    • Practice Makes Better (Perfection is not the goal)
  – Statements made to your customers and employees about data protection and privacy
    • Favorite hunting grounds for regulators, post-breach
  – Cyber liability insurance
  – Review, test, audit and update regularly – at least twice annually
Resources

Best Practices for Victim Response and Reporting of Cyber Incidents
Version 1.0 (April 2015)

Any Internet-connected organization can fall prey to a disruptive network intrusion or costly cyber attack. A quick, effective response to cyber incidents can prove critical to minimizing the resulting harm and expediting recovery. The best time to plan such a response is now, before an incident occurs.

Legal Considerations

• Incident Response – the first 24 hours:
  – Record the moment of discovery
  – Call your legal counsel to get legal advice/privilege
  – Alert the incident response team & cyber insurer
  – Secure the premises/preserve evidence
  – Stop additional data loss
  – Document everything
  – Interview involved parties
  – Review notification protocols
  – Assess priorities and risks
  – Bring in forensics firm
  – Contact law enforcement

Source: Experian 2015-2016 Data Breach Response Guide
Legal Considerations

• Breach notification to affected persons
  – Different states have different requirements
    • Some states require an investigation to confirm breach before affected persons are notified;
    • Other states require breach notification as expeditiously as possible, without initial investigation;
    • Most allow for a reasonable delay at the request of law enforcement;
    • Some require notification of state government agencies as well as affected residents;
    • There is no uniform national breach reporting rule;
    • Generally speaking, sooner is better than later.
• Breach notification to affected persons
  – Some federal agencies have reporting requirements
    • HIPAA – HHS OCR – Health records
    • Gramm-Leach Bliley Act (GLBA) – Financial institutions
Legally speaking, hope is not a plan.

• Remarkably, many companies still have no:
  – information security program,
  – incident response plan or
  – cyber liability coverage
An Evolving Regulatory Landscape
The issue of cyber security is a high priority for the Obama Administration, the White House said today, asserting that it would not tolerate any cyber espionage and other attacks that badly hit the American national security and economic interests.

"The issue of cyber security is a high priority for the Obama Administration, the White House said today, asserting that it would not tolerate any cyber espionage and other attacks that badly hit the American national security and economic interests."
Executive Order -- "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities"

EXECUTIVE ORDER

BLOCKING THE PROPERTY OF CERTAIN PERSONS ENGAGING IN

SIGNIFICANT MALICIOUS CYBER-ENABLED ACTIVITIES

By the authority vested in me as President by the Constitution and the laws of the United States of America, including the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.) (IEEPA), the National Emergencies Act (50 U.S.C. 1801 et seq.) (NEA), section 212(f) of the Immigration and Nationality Act of 1952 (8 U.S.C. 1182(f)), and section 301 of title 3, United States Code,

I, BARACK OBAMA, President of the United States of America, find that the increasing prevalence and severity of malicious cyber-enabled activities originating from, or directed by persons located, in whole or in substantial part, outside the United States constitute an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States. I hereby declare a national emergency to deal with this threat.
Cyber Security – a “National Emergency” in 2015

- the increasing prevalence and severity of malicious cyber-enabled activities
- originating from, or directed by persons located, in whole or in substantial part, outside the United States
- constitute an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States.

- I hereby declare a national emergency to deal with this threat.
• When the government assigns a **high priority** to something, it commits **massive resources** to it.
  – Department of Commerce
  – Securities & Exchange Commission
  – Federal Financial Institutions Examination Council
  – Federal Trade Commission
  – Federal Communications Commission
  – Food & Drug Administration
  – Department of Homeland Security
  – Department of Justice
  – Department of Defense
  – National Security Agency
  – Congressional legislation
Federal Cyber Guidance/Regs – Accelerating

- **February:** FINRA releases Report on Cybersecurity Practices
- **February:** SEC OCIE’s Cybersecurity Examination Sweep Summary
- **February:** EO issued encouraging “Information Sharing & Analysis Organizations” (ISAO”) for private industry and with DHS
- **April:** EO announces offensive steps against external malicious cyber threats (“national emergency”)
- **April:** SEC issues new “Cybersecurity Guidance” to investment funds and advisers
- **April:** DOJ issues “Best Practices” for Victim Response and Reporting of Cyber Incidents
Federal Cyber Guidance/Regs – Accelerating

- **May:** DOJ and FTC urge companies to cooperate with post-breach investigations by law enforcement
- **June:** FTC issues “Start With Security: A Guide for Business”
- **August:** DOD releases draft “rapid reporting” requirements for defense contractors that experience a possible data breach.
- **August:** OMB issues draft guidance for improving cyber security in the federal acquisitions process
- **September:** DHS awards grant to University of Texas San Antonio for ISAO Standards Organization
- **December:** Congress passes cyber security legislation (CISA)
  - To encourage sharing of cyber threat information by business
  - Includes liability protections for information sharing
Trending in Privacy and Cybersecurity

• New government enforcement actions:
  • Federal agencies now investigate some big breaches:
    • FTC, SEC, FCC, HHS, DOJ, FDA, CFPB
    • Monetary penalties can be significant
    • “Settlements” may include decades of enhanced self-reporting
  • The FTC’s power to regulate cybersecurity practices was affirmed in August by a federal appeals court.
    • FTC v. Wyndham Worldwide Corp.
  • FCC and FTC now in a simmering turf war over consumer data protection enforcement. Who’s the boss?
Several states have recently added new laws on privacy protection and data breach notification: CA, FL, MT, NV, OR, MT

- 48 states have data breach notification laws. Neither uniform nor consistent.
- Still no uniform federal data breach notification law

State Attorneys General are investigating higher-profile data breach events upon breach disclosure

- Threats of government investigations complicate the data breach victim’s ability to focus on breach response
  - See: Anthem, JP Morgan
Trending in Privacy and Cybersecurity: Europe

• The “Safe Harbor” treaty between the U.S. and EU was voided by the European Court of Justice last October
  • Facilitated transfer of personal information from the EU to the U.S.
  • “Privacy Shield” is in negotiations, but not yet in place

• The new EU General Data Protection Regulation becomes effective in early 2018, replacing Directive 95/46/EC.
  • Will carry significant penalties and fines for non-compliant data controllers and processors (i.e., up to 4% of global revenues)
  • Very short breach notification (i.e., 72 hours) to inform gov’t regulators
  • Clarifies the so-called “right to be forgotten”
HELLO
I AM...
SUING YOU
Litigation Considerations Following a Data Breach

• Whether you are the plaintiff or the defendant in the lawsuit, preservation of evidence is critical
  – Especially electronic records
Litigants Have An Affirmative Obligation to Preserve ESI

  – “The obligation to preserve evidence arises when the party has notice that the evidence is relevant to litigation or when a party should have known that the evidence may be relevant to future litigation.”

• Examples:
  – Date lawsuit filed in court
  – Date claim filed with administrative agency
  – Date company receives demand letter from attorney
  – Date complaint filed with company
  – Date that company employees believe litigation is possible
What Must Be Preserved?

• Federal Rule of Civil Procedure 26(b) provides the scope of discovery:
  – “Parties may obtain discovery regarding any nonprivileged matter that is relevant to any party’s claim or defense and proportional to the needs of the case, considering the importance of the issues at stake in the action, the amount in controversy, the parties’ relative access to relevant information, the parties’ resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit. Information within this scope of discovery need not be admissible in evidence to be discoverable.”
  – Relevant evidence includes—and today is dominated by—ESI
Amended Rule Specifically Addresses ESI

• Effective December 1, 2015, new Federal Rule of Civil Procedure 37(e):

  • “If electronically stored information that should have been preserved in the anticipation or conduct of litigation is lost because a party failed to take reasonable steps to preserve it, and it cannot be restored or replaced through additional discovery, the court:

    • (1) upon finding prejudice to another party from loss of the information, may order measures no greater than necessary to cure the prejudice; or
    • (2) only upon finding that the party acted with the intent to deprive another party of the information’s use in the litigation may:
      – (A) presume that the lost information was unfavorable to the party;
      – (B) instruct the jury that it may or must presume the information was unfavorable to the party; or
      – (C) dismiss the action or enter a default judgment.”
Potential Court Sanctions for Loss of ESI

• Refusal to use evidence
• Adverse inference or presumption that lost ESI was harmful to company
• Adverse jury instruction requiring jury to conclude that lost ESI was harmful
• Default judgment or dismissal of lawsuit
• Payment of attorneys’ fees
Preservation, Collection, and Production

• Preservation:
  – Written record retention policies
    • No universal or magic policy, but if you have a written policy, follow them!
    • Ensure the policy is comprehensive
      – Cover various sources of data or documents, such as emails, data logs, server logs, metadata, internal files, etc.
      – Cover transitioning or departing employees
  – Investigation process itself
    • Response to data breach
    • Communications with third party vendors
    • Communications to those affected by data breach
  – Litigation holds
    • Typically comes from in-house counsel or outside lawyer
    • Triggers an obligation to preserve relevant documents and ESI
Preservation, Collection, and Production

• Collection:
  – Searching for information can be critical
    • Having 1-2 employees who are familiar with your company’s systems and capabilities in order to search for the materials you are looking for can be invaluable in this process
  – Review and export ESI
    • Know your sources/types of ESI
    • Examples: emails and attachments, metadata, email servers, shared networks, personal workstations, unique applications, software programs, electronic databases, cellular telephones, text messages, external hard drives or flash drives, social media
  – Non-ESI still must be preserved and collected too
    • Handwritten notes, paper files, memorandums, summaries, investigations, notebooks, post it notes
  – Perform in house or retain outside vendor?
Preservation, Collection, and Production

• Production
  – Once exported, attorneys will perform their review to determine relevance, privilege, and other issues
  – Different production formats: TIFF, PDF, native
  – Avoid data dumps
  – Just because a document is preserved doesn’t mean it will be produced, but the duty to preserve is not dependent on whether the document will be produced
The Courts Continue to Lag Behind Technology

Even as technology evolves and advances, the legal system will inevitably be addressing older or obsolete systems or versions of applications.

Keep this in mind when looking at your systems and processes after the fact!
Wrap-up and Questions
Thank you!

Anthony T. King  
Snell & Wilmer L.L.P.  
One Arizona Center  
Phoenix, AZ 85023  
602.382.6513  
aking@swlaw.com

Patrick X. Fowler  
Snell & Wilmer L.L.P.  
One Arizona Center  
Phoenix, AZ 85023  
602.382.6213  
pfowler@swlaw.com  
@eDataBreachLaw  
http://www.swlaw.com/blog/data-security/