M3 Cyber Liability Industry Update

What to Watch for in 2016

1. A More Sophisticated Criminal Landscape for Stolen Data Emerges

- In 2015, intentional cyber-attacks overtook employee errors/mishandling as the top source of data breaches.
- 781 data breaches were reported in 2015 (USA reported) which exposed an estimated 170M records. That comes in just shy of the 783 incidents reported in 2014 but with over double the exposed record count.
- Healthcare organizations dominated the large breach landscape in 2015, registering three of the ten largest breaches (Anthem: 80M+; Premera Blue Cross: 11M+; Excellus BlueCross: 10M+).
- The 2015 attack on the Federal Office of Personnel Management marked the first large-scale federal cyber breach; it impacted 22M+ records of federal employees.
- Top industry targets continue to be retail, healthcare, and finance - however, 2015 also saw a rising emergence of cyber threat to industries such as public entities, manufacturing, and critical utility infrastructure.

Takeaway: Attacks in 2015 were more acute in their approach and targeted goals. Despite a relatively flat number of data breaches reported domestically in 2015, the number of impacted records nearly doubled. Information available from cyber insurance carriers suggest that actual claims reported to carriers increased 50% in 2015. 2016 will continue to bring even more activity from a variety of threat sources.

2. Cyber Liability Marketplace is Still Evolving

- Demand for Cyber Liability insurance increased sharply in 2015 across all types of organizations. 74% of organizations currently not purchasing cyber insurance are anticipated to do so in 2016.
- Some carriers will "retreat" from the Cyber Liability marketplace. Carriers hampered by poorly underwritten losses, lack of comfort in qualitative assessments of the insured's security, and a growing underwriting knowledge gap will lead to fewer stand-alone options in 2016.
- Organizations in high-risk industries will experience an increase their Cyber Liability premiums in 2016; increases of up to 50% are estimated in some cases.
- 2015 saw the first litigation stemming from a carrier denying coverage for gross misrepresentation on an application. Carriers can deny claims due to misrepresentation, especially as it relates to regular security procedures like updates, password controls, and software patching.

Takeaway: The Cyber Liability marketplace continues to be one of the most dynamic markets in the insurance industry. Loss data is still not sound enough to generate solid rating platforms and carriers are unable to attract the appropriate IT talent to accurately underwrite risks. Industries facing larger exposures must consider agent representation with specialization in this area to ensure proper protection and policy architecture.

M3 INSURANCE
FREEDOM TO MOVE FORWARD

3. An Incident Response Plan Cannot be Created After an Incident

- Cyber insurance is a funding mechanism; it is not a substitute for an Incident Response Plan. An estimated 75% of US organizations are not prepared to respond to any kind of data breach.
- The most important component of the Incident Response Plan is identification of the post-breach team. Organizations need to establish who will manage clean up in certain areas, including: data forensics, legal advice, notification processing, credit monitoring, crisis management, and public relations. Many law firms and accounting firms are hiring specialists in these areas and Cyber Liability carriers often have established relationships that can be drawn on at discounted rates.
- Incident Response Plans should be a Board-level issue. Plans should be tested annually (at minimum) and updated as operations and IT factors change.

Takeaway: A cyber security incident is like a fire – after it happens, there is no time to formalize a response plan. Vendors who specialize in the area of breach response will continue to grow in 2016. Most Cyber Liability policy carriers offer a panel of professionals who, at little or no cost, will take the time to understand and counsel their clients prior to a breach.

4. Vendor Contracts Won't Always Cover Lost Data

- An increasing number of companies (69% in 2015) are migrating toward "cloud" or "co-location" resources for either primary network infrastructure, backup resources, or through their key software service partners.
- Vendor contracts do not typically contain accountability for data security, offering "reasonable" security requirements in lieu of definitive action or responsibility.
- Vendor contracts often do not require that the vendor even notify the customer of any data breach, leaving the original company unknowingly vulnerable to a breach.
- Oftentimes vendors will not and are not required to share post-breach analysis or critical log data. Understand what your vendor will provide if they are the victim of a breach.
- Vendors in the data business should maintain key information security accreditations and have an active disaster recovery plan in place. It is critical understand how your vendor backs up data in response to any disaster, including a data breach.
- Vendors often refuse to accept any liability associated with potential data breaches and only warranty representations to an "as is" status.

Takeaway: Outsourcing data management and storage is becoming critical to all types of organizations, and will continue to trend upward in 2016. Negotiating terms that are in your best interests will require your diligence in asking the right questions. Data vendor agreements should be negotiated and reviewed with qualified legal counsel, familiar in the area of data management.

5. Ransomware is "User-Friendly" and Phishing Attacks Are Convincing

- A common **Ransomware** called Cryptolocker gained momentum in 2015. Ransomware infiltrates files on a network and encrypts them, leaving only a picture requesting payment to unlock the files. 43% of ransomware attacks in 2015 requested less than $10K USD in ransom payment (just under the threshold where federal regulatory agencies will begin to investigate).
- **Phishing** emails are cleverly designed to fool you and will likely appear to be from companies with which you do business. 23% of individuals currently open phishing messages and 11% click on associated links; on average, those messages are being opened in under two minutes.

Takeaway: Critical files must be backed up frequently (hourly if possible). Ransomware is typically deployed through phishing attacks and can be activated by any employee of an organization. Deploy specialized training to employees on how to spot a phishing email and use credible security technology to check the authenticity of all emails, including any embedded files or links.

M3 INSURANCE
FREEDOM TO MOVE FORWARD

6. International Data Security Requirements to Surpass Domestic

- The General Data Protection Regulation (GDPR) received overwhelming support in 2015 and European Union (EU) legislation is likely to go into effect in 2016. The GDPR will be guiding EU law on data breaches, not only within the EU but also within multinational organizations, which may collect EU data stored in the US.
- Highlights of the legislation include strict corporate governance surrounding security prevention, fines of up to 1M euros or 2% of revenues, requirement for EU authorities to be notified of any data breaches within 72 hours of incident, and security vetting of end users prior to EU data being ex-filtrated stateside.

Takeaway: The GDPR will be enforced on organizations that fail to abide by its rules and do not perform "good faith" efforts to secure data. Understand the type and origin of data being held by your organization and the potential international regulation. Typical Cyber Liability policies contain worldwide coverage territories, but terms and conditions of policies including Duty to Defend and regulatory coverage may be limited by non-domestic regulatory bodies.

7. Cyber Security Remains a Directors & Officers Issue

- Target, Home Depot, Heartland Financial and Whydham Worldwide topped the list of Directors & Officers litigation stemming from data breaches in 2015. So far, the list is isolated to large publicly-traded companies with large shareholder bases. Expect this trend to continue in 2016, eventually trickling down to private entities.
- Directors, officers, and board members must understand and oversee the cyber security of their organizations.
- Claim sources will include shareholder lawsuits for loss of value and class action litigation from affected parties for corporate oversight and complacency.

Takeaway: Regulatory bodies and organizational stakeholders will continue to hold leadership accountable for breaches of privacy due to negligence. Not all Directors & Officers policies will automatically provide cover for claims alleging breach of duty related to a data security. Coverage should be reviewed with a knowledgeable professional for coverage limitations and potential carve back for cyber security claims.

8. Third Party Cyber Breach Class Action Suits

- A plaintiff must be able to demonstrate direct financial loss in order to have a right to damages. Many class action lawsuits from "headline-worthy" cyber breaches are dismissed in the early stages for lack of material or provable damages on behalf of the plaintiffs.
- Courts continue to determine that a loss of data does not constitute financial damages, as seen by relatively low settlements in the Target and Home Depot cases.
- Defense costs continue to lead post-breach costs when litigation is involved.

Takeaway: When assessing your cyber security risk, do not completely discount the cost to defend and settle a potential third party lawsuit. Understand your absolute exposure in this area and adequately budget for defense expenses. Understand that companies that have a public brand face increased potential for litigation as the allure of class action litigation by plaintiff attorney's increases.

M3 INSURANCE
FREEDOM TO MOVE FORWARD

9. Federal Cyber Security Regulation is Coming… Just Not Any Time Soon

- With a lack of federal regulation, cyber security jurisdiction will remain somewhat uncertain in 2016.
- The Federal Trade Commission (FTC) took the lead in 2015 in terms of jurisdictional authority over federal cyber security incidents with supportive legal positions as well as vague interpretation of Section 5 of their federal charter. All in, the FTC has fined over 50 organizations since 2005 for a total of $75M.
- The Department of Justice was new to the cyber legal landscape in 2015, they join the following regulatory bodies with the authority to fine: SEC, FINRA, Gramm-Leach Bliley, PCI, HIPAA, HITECH, Consumer Protection Bureau, DOL, Department of Commerce, DHS, FCC, FERPA, and COPPA.
- The upswing of state agencies' involvement in the investigation and penalization of cyber breaches will continue in 2016. With a lack of federal framework, each state responds differently to data breaches. Some states investigate and fine through authority granted to the Attorney General's office, while other states take a passive approach. (To date, Wisconsin has not identified a specific agency or organization that is tasked with investigating data breaches)

Takeaway: Clear-cut regulation providing preventative security measures and post-breach notification guidelines will not arrive in 2016. Until this legislation is passed and jurisdiction is appointed, uncertainty surrounding breach response will continue. Proactive cyber security awareness and planning continues to be the best defense to potential regulatory action and penalization. Companies implementing best practices can avoid costly litigation and penalties

10. Social Engineering and Computer Fraud on the Rise

- **Social engineering** scams use internet data mining of company personnel records coupled with disguised or counterfeit email addresses (i.e., @rn3ins.com vs. @m3ins.com) to mislead organizations into sending phony ACH payments and wire transfers. Examples are emails pretending to be the CFO to Controller or CEO to CFO which may include supporting documentation such as fake invoices or W-9's for subcontractors.
- **Computer fraud** is the process of securing the personal credentials of key internal individuals used for online banking. With this information, the criminals can generate fraudulent wire frauds without the knowledge of the organization.
- Sophistication and frequency of social engineering and computer fraud scams rose nearly 40% in 2015.

Takeaway: Social engineering and fraud tactics mirror more traditional theft of funds but do so using tools that all professionals use on daily basis. The success of these schemes in 2015 indicate they'll be on the rise in 2016. Implement and train on internal procedures, such as dual authorization to release funds, to ensure payments are only made to authentic sources. Understand your bank's protocol for identifying and stopping unusual activity, such as callback procedures.