McGRIFF, SEIBELS & WILLIAMS, INC.

Prepared for Alabama I-Day, October 14, 2015
By Mary Guzman, SVP, E&O/Cyber Practice Leader
mguzman@mcgriff.com; 404 497-7535

TABLE OF CONTENTS

- Data Breach & Privacy Landscape
- Cyber-Risk Is Not Just Privacy Risk Anymore…
- Cyber-Risk Quantification
- Cyber Market Update
- Cyber-Risk Solutions
- Claims & Breach Response

Data Breach & Privacy Landscape

"There are two types of companies: those who have been hacked, and those who don't yet know they have been hacked."

John Chambers, CEO, Cisco

INDUSTRY FACING SIGNIFICANT CHALLENGES

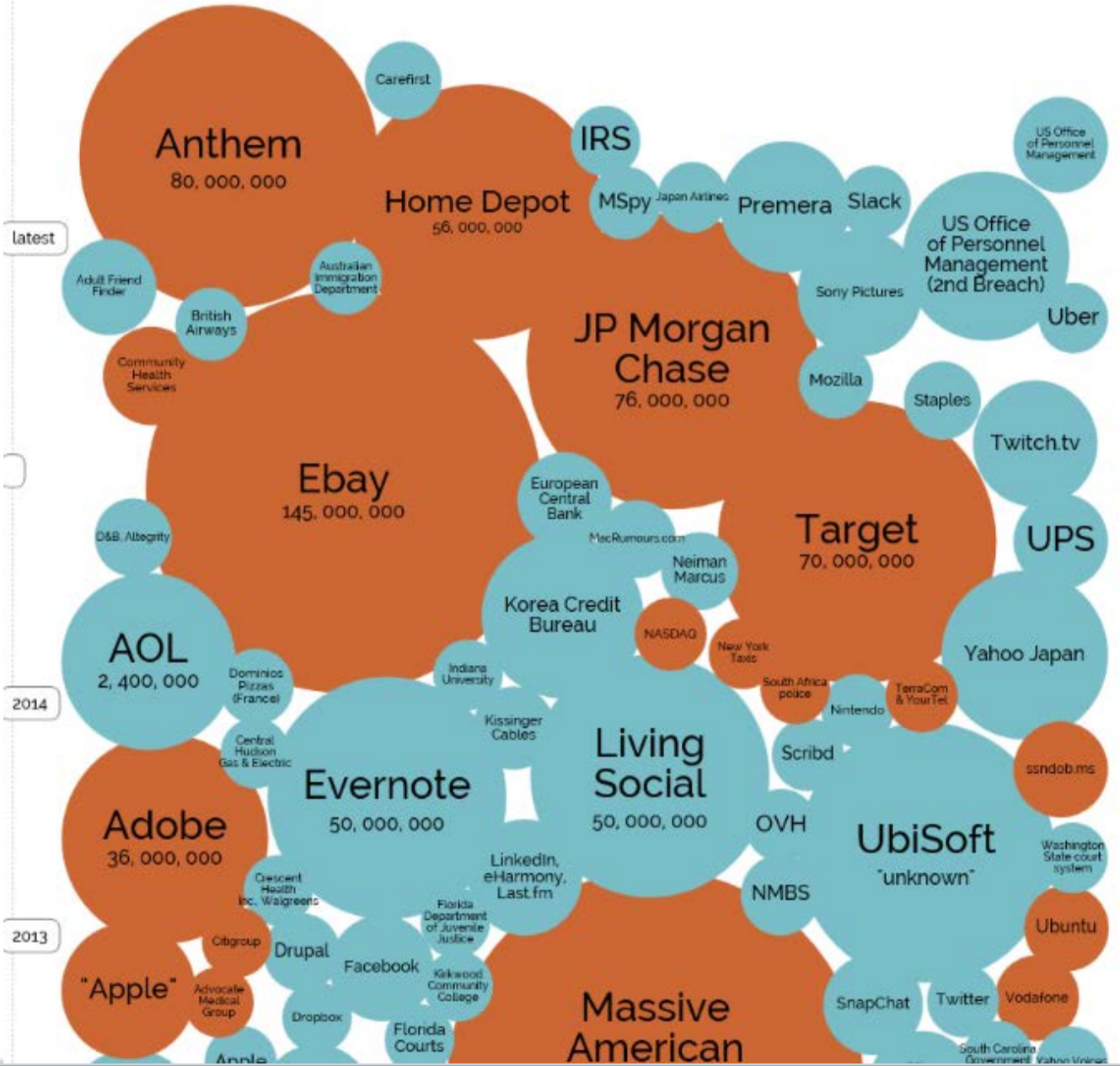
Game changers?

- **Target** - Potentially paves the way for Card Issuers to go directly to “merchants” for reissuance expenses
- **Anthem** - Anthem agreed to deal with HIPAA/HHS around breach notice/response issues on behalf of all Insured's; however, may be state regulations that trump HIPAA federal statute for plan sponsor; additional fiduciary responsibilities under ERISA may push companies to want to get in front of Anthem’s response time; as a result hundreds of cyber policies have been put on notice.
- **2008 Turkish Pipeline attack & 2014 German steel mill attack**
  - First and second time where cyber attack was confirmed to have caused physical damage to infrastructure.
- **2014 Sony** - Hack into wide-ranging company data including competitive data and trade secrets. Is this the next evolution of cyber breaches?

REGULATORY ENVIRONMENT

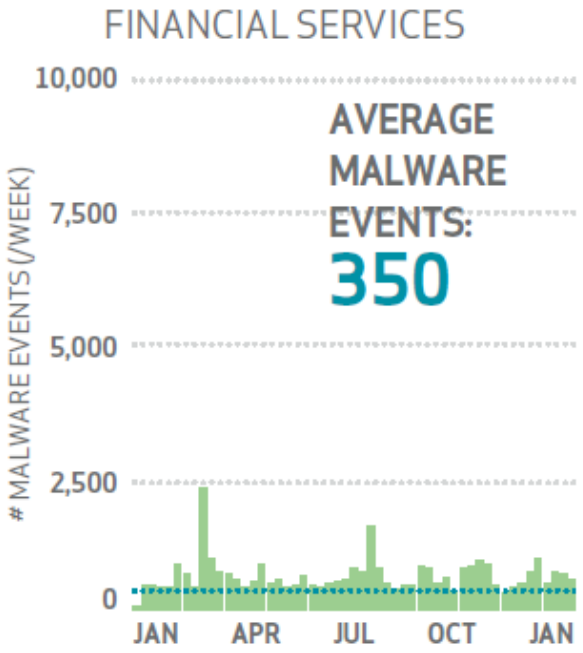
- HIPAA/HITECH
- Card brands
- Various state privacy laws
- FTC
- SEC
- Graham-Leach-Bliley
- NERC CIP
- Various other voluntary assessment tools such as the NIST framework, C2M2, and ISO standards

HISTORICAL BREACHES DATING BACK TO 2013



Source: http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

RECENT MARKET DEVELOPMENTS



Source: Verizon 2015 DBIR

- Total liability capacity nears $800 million with $500 million being largest single program (usually blended with E&O, Bankers Professional or other line); less capacity available for BI/EE and many towers thin out as follow form capacity not available for all insuring agreements or exposures (intellectual property, etc..)
- The cyber market is experiencing an intense hardening, primarily in the retail / hospitality space. The market impact felt as a result of the string of breaches since December 2013, led by Target & Home Depot, has led to more cumbersome underwriting requirements and tightening capacity
- End-to-End encryption is now required for many retailers; some markets insist on a signed warranty affirming that all systems have been tested/scrubbed for BlackPOS *or any similar* malware; some underwriters expecting P2PE plan in addition to EMV implementation.
- Approach from Insurers varies significantly as respects sub-limits on notification, credit monitoring, forensics, fines/penalties and business interruption coverage. Some excess carriers retreating from certain industries or limiting capacity on retail risks.
- Some insurers require that their claims/response team must manage breach response on behalf of the Insured; some provide more flexibility (McGriff clients often prefer to manage their own breach response)

CYBER-RISK IS NOT JUST PRIVACY RISK ANYMORE……..

WHICH COMPANIES NEED TO CONSIDER AN INFORMATION SECURITY POLICY?

ALL OF THEM!!!

There are many variations on the risks that are not adequately covered by traditional insurance:

1) Energy Companies
   - Utilities- privacy, business interruption/EE, "failure to supply"
   - Pipelines- business interruption/contingent BI, contractual liability
   - Oil & Gas and E&P – business interruption/EE, ***property damage arising out of a cyber event***,
2) Organizations with a lot of PII or PHI (Financial Institutions, Healthcare, Insurance, Retail, Accounting/Legal, Transportation, Grocery/Drug Stores)
   - Privacy breach response, legal liability to consumers, Card Brands, FIs and other
   - Business Interruption/Extra Expense
   - Reputation Harm (potential link to D&O)
3) Telecommunications/Technology
   - Errors and Omissions liability, Intellectual Property (IP) infringement, first party IP loss (theft, destruction of Trade Secrets)
4) Manufacturing/Distribution
   - Business Interruption/Contingent BI, Breach of Contract, first and third party IP risks
5) Maritime/Port Authority
   - Business Interruption from shutdown, third party Bodily Injury and Property damage, contractual liability
6) Pharmaceutical
   - Intellectual Property / Trade Secret

And the list goes on……

ENTERPRISE INFORMATION SECURITY RISKS

Enterprise Operation Risk – IT automation throughout organization (applications and networks, etc.)

- Business Interruption loss
  - Income loss from inability to provide services and/or accurately account for sales
  - Extra expenses to
    - Isolate and contain intrusion and conduct forensic analysis
    - Recover and restore compromised digital assets
    - Relicense critical computer applications
    - Other ongoing expenses during period of recovery
  - Extra Expense to utilize Hot Site and/or other back-up resources
- Dependent Business Interruption Risk – cyber disruption at critical supplier or in supply chain
- Legal Liability – failure to meet contractual obligations

Privacy Liability and Regulatory Response

- Incident response costs – notification, credit monitoring, legal fees, forensics
- Privacy litigation – consumer class actions
- Regulatory investigations and remedies (consumer redress funds)
- Third party beneficiary liability – costs to reimburse banks and card companies for their costs to open new accounts or replace cards of victims of your privacy breach

CYBER / PRIVACY EXPOSURES AND INSURANCE COVERAGE

"Traditional" Privacy Liability & Information Security Risks

- **First Party Risks and Coverage**
  - Business interruption and extra expenses as a result of network or web site outage
  - BI/EE for loss of data, recreation of data, uncollectible accounts receivable, corrupted IP
  - Cyber extortion – threats to post/sell security vulnerabilities and/or confidential data
  - Theft or destruction of Trade Secrets or other IP (Patent and Trade Secret Coverage Excluded under most forms)
  - Reputation harm resulting from unusual business churn immediately following an event

- **Third Party Risks and Coverage**
  - ***Breach notification and mitigation (credit monitoring) expense, Public Relations, Forensics) following the disclosure of Third Party Personally Identifiable Information - most common exposure ; most breaches do not result in 3rd party litigation)***
  - ***A wild card and significant factor driving both cost and limits is the assessment or adjudication process of the Card Brands***
  - Enterprise wide data privacy wrongful acts whether from internal or external "hacker", and whether or not records disclosed in electronic or paper format
    - ***ID theft claims, invasion of privacy claims, damage to reputation/credit***
    - ***Regulatory Defense and investigation, fines and penalties (Red Flags Rule, NERC, HIPAA, others…)***
    - Contractual obligations around security and privacy (particularly with regard to PCI compliance)
    - ***Cost to reissue credit cards (suits from transaction processors or issuing banks)***
  - Use of your Network to launch at attack or "leapfrog" into third party web sites and/or networks (which may or may not be your clients)
  - Media liability, intellectual property infringement (Patent and Trade Secret Excluded under most policy forms)
  - Economic harm to your customers due to "down time" of your own application, network, web site upon which your customers rely (Insurance coverage varies by policy form)

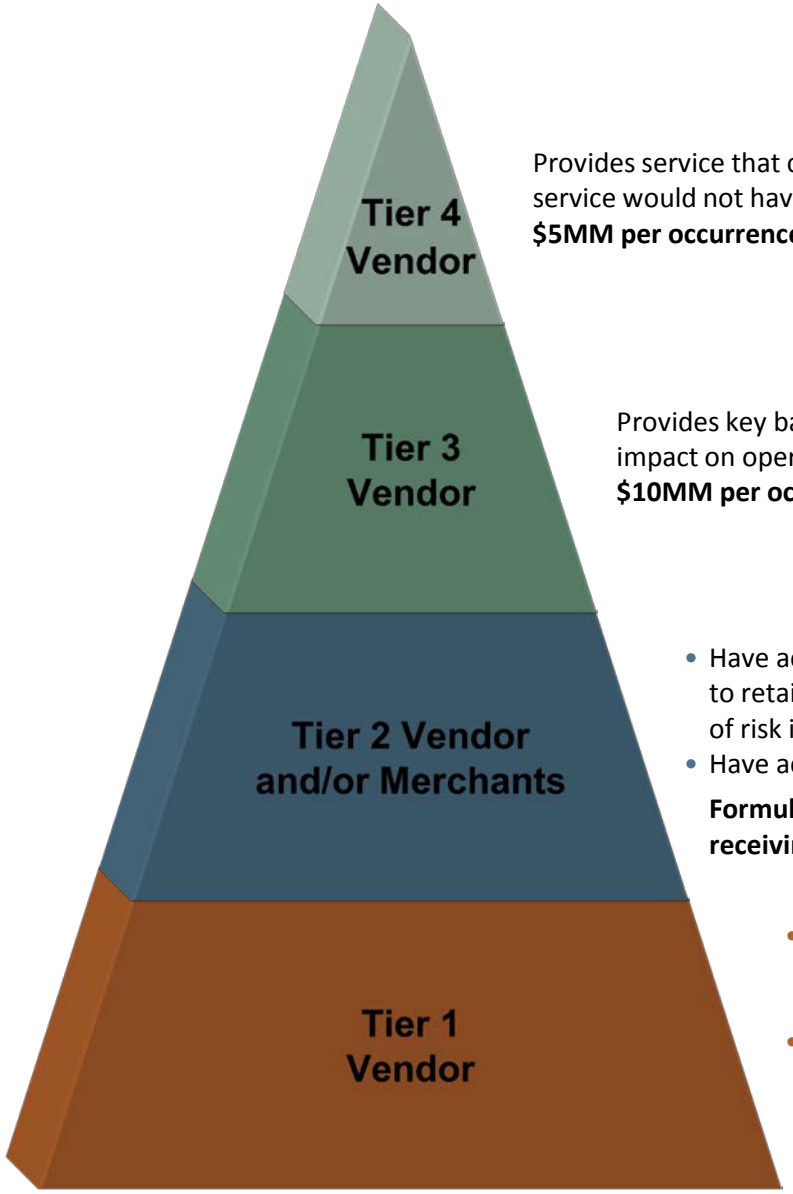
THE HIDDEN RISKS OF OUTSOURCING…

- Virtually every company today outsources some component of their IT system to third parties, but most companies have not measured the risks associated therewith. Companies use third parties for everything from web hosting to payroll outsourcing to credit card processing.
- Outsourcing function = Loss of Control, but does NOT release the "data owner" from liability for privacy violations
- FTC Act, Dodd-Frank, Red Flags Rule, PCI Compliance, NERC CIP, HIPAA, and many other state and federal regulations extend to not only you but the vendors you use as well, putting the responsibility for compliance (and the reputation risk) squarely on your shoulders
  - FTC Act gives broad ranging authority around "unfair or deceptive trade practices" regarding use of vendors, enforcement of appropriate privacy and security policies
- Outsourcing can greatly increase your "contingent" business interruption risk

MSW's Information Security risk subject matter experts can:

- Assist in the categorization of vendors and redevelopment of contract protocols
- Review insurance for cyber and/or E&O provided by those vendors for adequacy
- Design custom insurance solutions for you and your vendors

VENDOR CLASSIFICATION– NOT BY SIZE



Provides service that can be easily replaced and for which the loss of their service would not have significant short-term impact
$5MM per occurrence and in the aggregate

Provides key back office service that could have significant impact on operations
$10MM per occurrence and in the aggregate

- Have access to Customer Confidential Information (this guidance applies more to retail operations; private business customer data can have much higher cost of risk if data is compromised)
- Have access to Personal Health Information

Formula: Total *rounded* Product of Projected # of employees using or receiving service *multiplied* by $25 per person breach response expense

- Have access to corporate confidential information, or provides services affecting "mission critical" systems, a loss of which would cause substantial income loss and/or negative brand impact
- Information Security Contractors that are provided access to network architecture and/or the totality of your confidential data (SOX audit, Managed Security)

$20MM per occurrence and in the aggregate

- Vendors should be categorized as low, medium, or high risk according to what service they are actually providing (per their Statement of Work in their contract with you) or the level of access they have to confidential information
- Contracts with vendors can be tailored so that the indemnification, information security standards, and insurance requirements ***actually*** protect your company's interests

CYBER-RISK QUANTIFICATION/TRANSFER

Data Breach Cost Calculator

HOW MANY RECORDS WERE EXPOSED?	100000
WHAT TYPE OF DATA WAS EXPOSED?	PHI
IS THIS THE ORGANIZATION'S FIRST BREACH?	Yes / No
WAS THE DATA STORED IN A CENTRALIZED SYSTEM/LOCATION?	Yes / No
IS FRAUD EXPECTED?	Yes / No
IS A CLASS ACTION LAWSUIT EXPECTED?	Yes / No
DOES YOUR ORGANIZATION CURRENTLY HAVE DATA BREACH COVERAGE?	Yes / No

Data Breach Costs

CALCULATE

INCIDENT INVESTIGATION

FORENSICS INVESTIGATION	$40,000
SECURITY REMEDIATION	$120,000
BREACH COACH ® LEGAL GUIDANCE	$38,000
SUBTOTAL	$198,000

PCI

FINES & PENALTIES	$0
FRAUD ASSESSMENTS	$0
CARD REISSUANCE	$0
SUBTOTAL	$0

CUSTOMER NOTIFICATION / CRISIS MANAGEMENT

CUSTOMER NOTIFICATION	$100,000
CALL CENTER	$7,500
CREDIT/ID MONITORING	$29,000
PUBLIC RELATIONS	$20,000
SUBTOTAL	$156,500

REGULATORY FINES & PENALTIES

STATE AG	$989,500
HHS	$1,092,500
OTHER (FTC, SEC, ETC.)	$0
SUBTOTAL	$2,082,000

CLASS ACTION LAWSUIT

DEFENSE	$283,000
eDISCOVERY	$200,000
PUBLIC RELATIONS	$150,000
SUBTOTAL	$633,000

TOTAL COST	$3,069,500
PER RECORD COST	$31

CYBER POLICY COVERAGE COMPONENTS

	Coverage	Description
1st Party Costs	Business Income / Extra Expense	Reimbursement for loss of income and/or extra expense resulting from an interruption or suspension of computer systems due to a network security breach.
	Data Asset Protection	Recovery of costs and expenses you incur to restore, recreate, or recollect your data and other intangible assets that are corrupted or destroyed by a computer attack
	Cyber Extortion	The costs of consultants and extortion monies for threats related to interrupting systems and releasing private information
	Breach Response	The costs of complying with the various breach notification laws and regulations, legal expenses, call centers, credit monitoring, forensic services, identity /fraud monitoring, and public relations
3rd Party Costs	Privacy Liability	Defense and liability for the failure to prevent unauthorized access, disclosure or collection of confidential information, or for the failure of others to whom you have entrusted such information. Coverage can also include liability for not properly notifying of a privacy breach and includes corporate proprietary information
	Network Security Liability	Defense and liability for the failure of system security to prevent or mitigate a computer attack. This could include a malicious virus or a denial or service attack. This coverage also includes the failure of written policies and procedures addressing technology use
	Privacy Regulatory Defense	Costs to defend an action or investigation by regulator due to a privacy breach, including indemnification for any fines or penalties assessed
	Media Liability	Defense and liability for online libel, slander, misappropriation of name or likeness, plagiarism, copyright infringement, disparagement, negligence in content to those that relied on content

CLAIMS & BREACH RESPONSE

IDENTIFYING KEY BREACH RESPONSE PARTNERS

- Legal
- Forensic (2 may be necessary…)
- Business Continuity
- Notification
- Credit Monitoring
- Call Center
- Public Relations

APPENDIX

NOTABLE BREACHES

Target 2013 Breach

- Records Disclosed: 110,000,000
- Customer Class Actions: $10,000,000 settlement
- Card Brand Litigation: $19 million settlement with MasterCard (rejected); $67 million settlement pending approval by participating Banks
- Bank Litigation: Target bid to dismiss rejected by judge; case ongoing.
- Expenses paid to date: $256m (1Q2015)

Anthem 2015 Breach

- Records Disclosed: 80,000,000
- Cyber attackers (suspected Chinese) gained access to Anthem customer and employee PII/PHI
- Names, birthdays, social security numbers, street addresses, email addresses, employment information, income data
- FBI , State's Attorney's investigations
- 50+ class action lawsuits filed to date, no settlements yet

NOTABLE BREACHES

OPM (US Government) 2015 Breach

- Records Disclosed: 40,000,000 (and counting...)
- Systems breached in December 2014, but OPM became aware April 2015
- SS#s, full names, fingerprints, birth dates, home addresses , background investigation records current, former and prospective Federal employees and contractors, contain information about mental health and financial history
- Information of non-applicants, primarily references, spouses or co-habitants of applicants
- $133m paid for Breach Notification & Identity Theft Protection Services

Sony Pictures 2014 (Breach #2)

- Perpetrators hacked into wide-ranging company data held including:
  - Unreleased movie scripts
  - Trade Secrets
  - Compensation of Executives & Actors
  - Personal emails
  - Employee SS#, compensation, address, health check records
- Suspected nation-state perpetrator or possible disgruntled employee?
- Forensics, IT Repairs, Loss of Data, Loss of Movie Profits, PR expenses, Employee Litigation, Loss of Competitive Advantage, Lost jobs

TIPS IN ASSESSING INFORMATION SECURITY EXPOSURE

- What sensitive information do you handle, manage, store, destroy or otherwise control – consider your own information, third party information and employee, dependent/beneficiary information
- Identify significant third party vendors providing data and systems management services; review contracts for controls/remedies and retained risk
- Does your organization have a person responsible for privacy compliance, information security officer and/or other executive level oversight of IT/OT security?
- Do you have a formal Incident Response Plan and is the plan been regularly tested and amended?
- Have you pre-negotiated contracts with qualified vendors to assist you in your breach response?
- What kind of indemnities do you provide to clients whose non-public information you transmit, store, process, etc?

TIPS IN ASSESSING INFORMATION SECURITY EXPOSURE

- Have you identified your “critical” systems/applications/data/networks and conducted an information security threat analysis?
- Have you conducted a business impact analysis (e.g. MFL or MPL as a result of an extended period of interruption?
- What vendors or suppliers are you reliant upon to provision your own products and services?
- What kind of impact would result from a competitor or other third party gaining access to your IP and/or R&D information?
- Are you a party to a Merchant Services Agreement and have you evaluated the financial obligations stipulated therein as respects a breach to credit/debit card data?
- Do you have a PCI DSS compliance obligation (merchant level) and have you been assessed by a QSA for compliance? Have you implemented PCI 3.1?
- Does your organization encrypt sensitive information at rest and in transit? Do you use tokenization, data masking and other techniques/technologies to protect PII?
- How would you rate your company’s security maturity? Have you had an external assessment conducted? Has your organization implemented a national standards framework such as NIST, ISO, SANS, E2-C2M2 or industry specific standard and been independently audited for same?