Cyber Security in M&A

Joshua Stone, CIA, CFE, CISA

whitleypenn

Agenda

- About Whitley Penn, LLP
- The Threat Landscape Changed
- Cybersecurity Due Diligence
  - Privacy Practices
  - Cybersecurity Practices
- Costs of a Data Breach

Bio

Joshua Stone – CIA, CFE, CISA

- Manager within the Whitley Penn Risk Advisory Services team
- Focuses on:
  - Internal audit outsourcing and co-sourcing,
  - SOX 404 implementations and consulting,
  - Process consulting, and
  - Information technology consulting.
- Primary industries: financial institutions, public sector, managed IT services, oil and gas, and consumer goods.
- Active member of: IIA, ACFE, ISACA, AICPA, and TSCPA.
  - Committee member with the Fort Worth chapter of the TSCPA,
  - Certification Committee Chairman of the FW IIA,
  - Chapter Vice President of the FW ACFE, and
  - Board President of the Tri-Cities Baseball Softball Association.
- Bachelors and Masters Business Administration – Accounting w/ Fraud Emphasis
  - Texas Wesleyan University

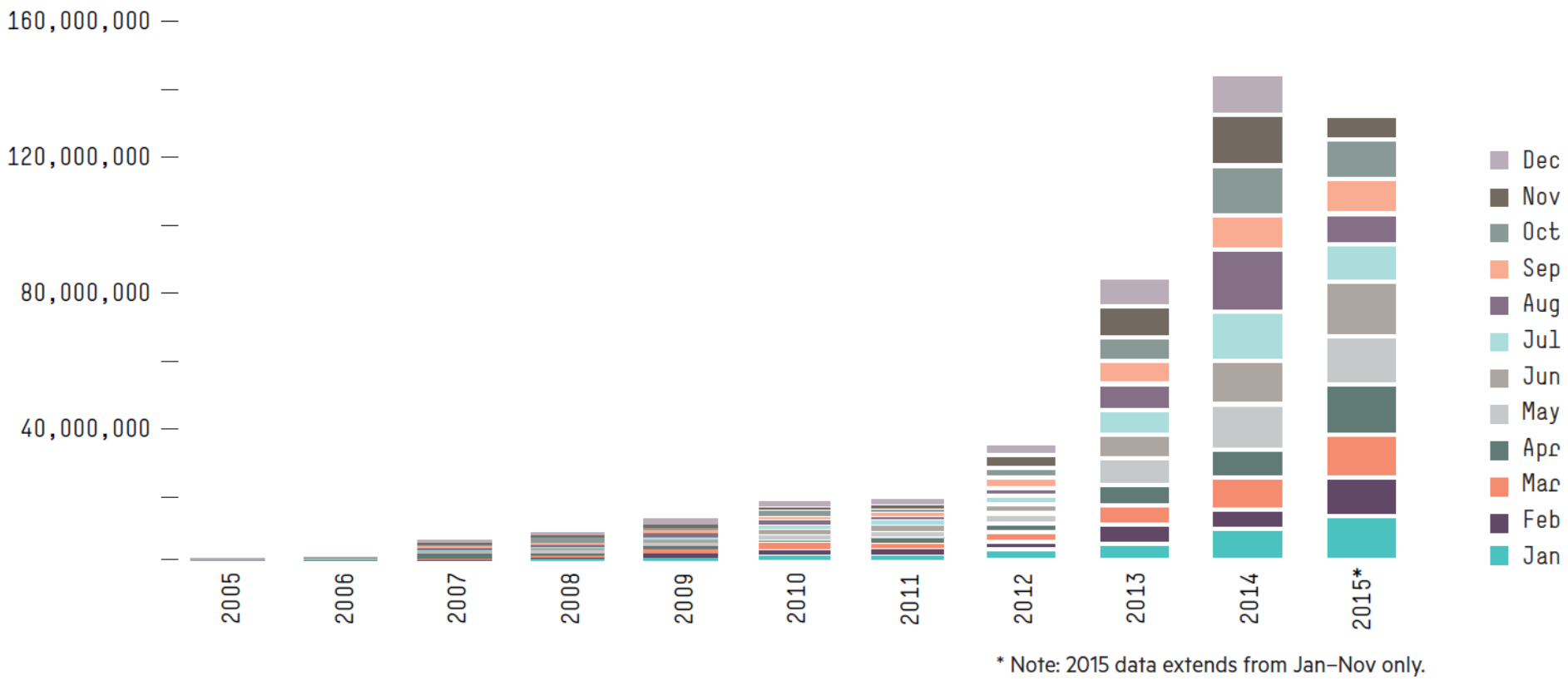
Whitley Penn, LLP – Risk Advisory Services

- Service Areas:
  - IT Audits and Consulting
  - Internal Control Reviews
  - IT and Business Risk Assessments
  - Internal Audit Services
  - Vulnerability Assessments and Network Penetration Testing
  - Service Organization Control (SOC) Reports – 1, 2, & 3
  - Enterprise Risk Management Implementation and Maintenance

whitleypenn
CPAs and Professional Consultants

The Threat Landscape Changed

Growth in Malware



* Note: 2015 data extends from Jan–Nov only.

whitleypenn
CPAs and Professional Consultants

Breaches By Industry

Incident pattern ►	POS intrusions	Web app attacks	Cyber-espionage	Crimeware	Insider and privilege misures	Payment card skimmers
Industry (NAICS #) ▼						
Accommodation (72)	53%	1%			3%	
Administrative (56)		4%	1%		6%	
Educational services (61)		9%	12%	22%	11%	
Entertainment (71)	58%	11%	11%		5%	
Financial services (52)		17%	1%	21%	6%	7%
Healthcare (62)	7%	8%	3%	3%	20%	
Information (51)		26%	9%	46%	1%	
Manufacturing (31-33)		3%	36%	19%	3%	
Mining (21)			11%		67%	6%
Other services (81)	1%	28%	3%	36%	6%	
Professional services (54)	2%	2%	26%	10%	1%	
Public (92)				18%	26%	
Retail (44-45)	20%	2%		25%	1%	4%
Transportation (48-49)			41%	9%	18%	5%
Utilities (22)		17%	50%	17%		
	▼	▼	▼	▼	▼	▼
Most-relevant scenarios – *the scenarios to read first!*	7, 10, 11, 12, 13 , 14, 16, 17, 18	8, 10, 11, 12, 14, 15, 16, 18	1, 6, 13, 14, 16, 18	2, 9, 13, 14, 15, 16, 18	3, 4, 5, 6, 13, 14, 16, 18	5, 7

Legend < 10% 11-19% > 20%

whitleypenn
CPAs and Professional Consultants

Vulnerability Marketplace

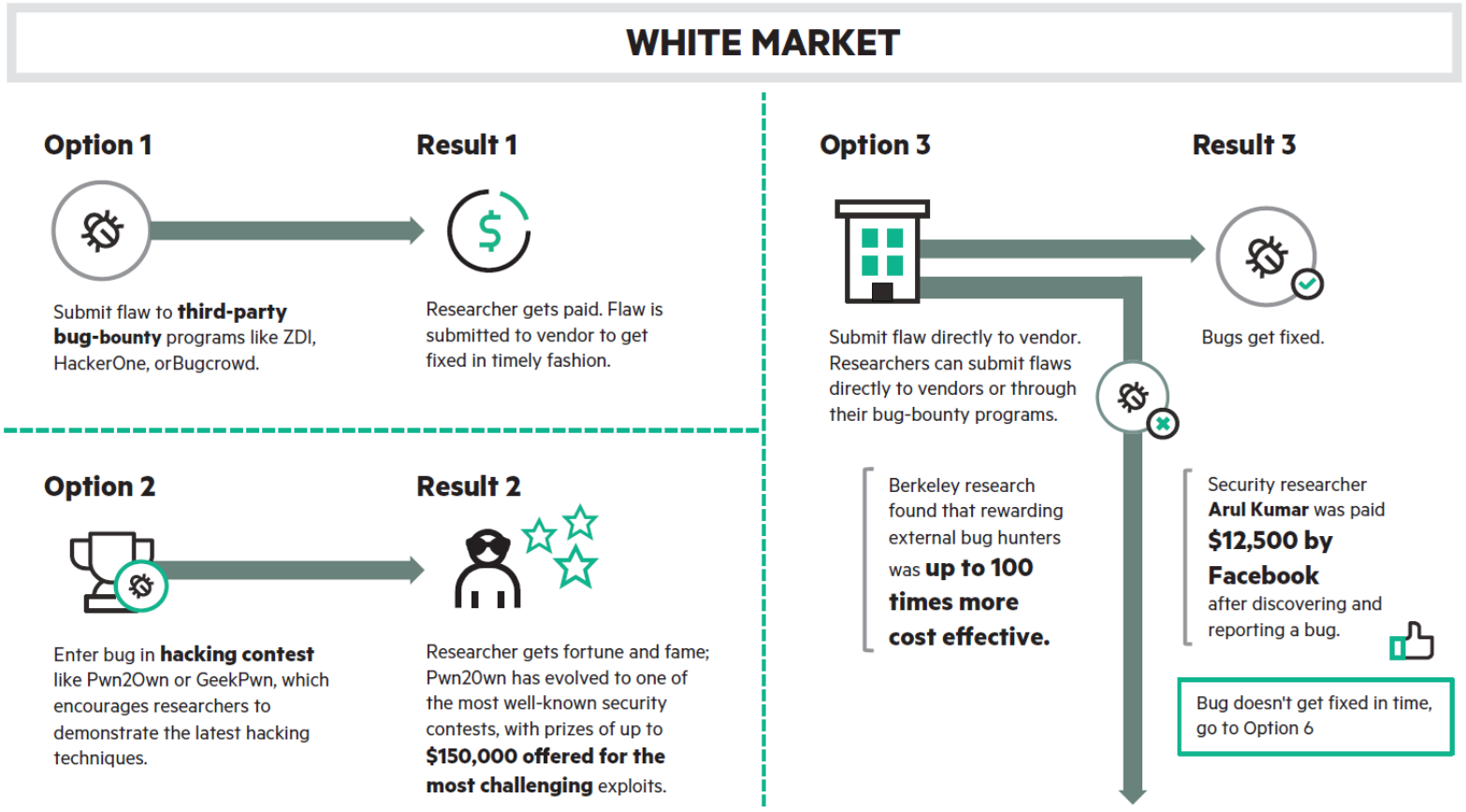


Figure 4. The vulnerability white market

Vulnerability Marketplace

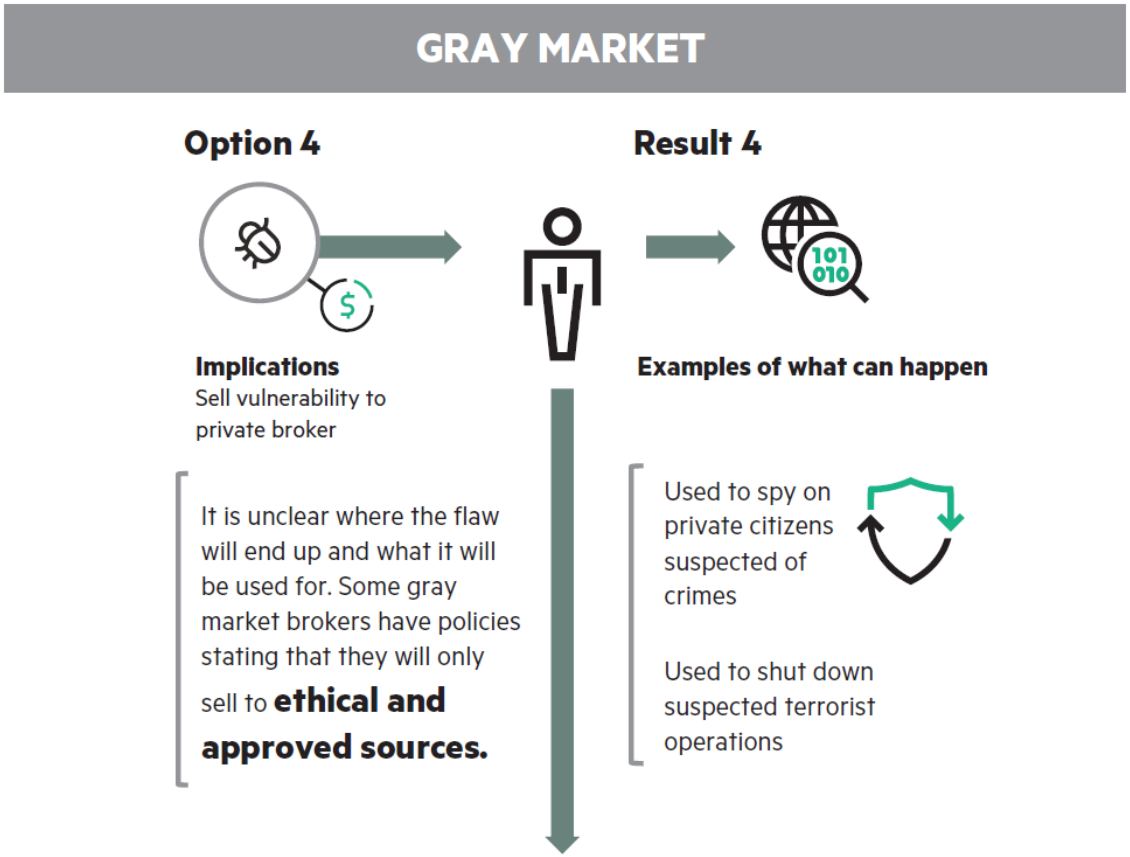


Figure 5. The vulnerability gray market

whitleypenn
CPAs and Professional Consultants

Vulnerability Marketplace

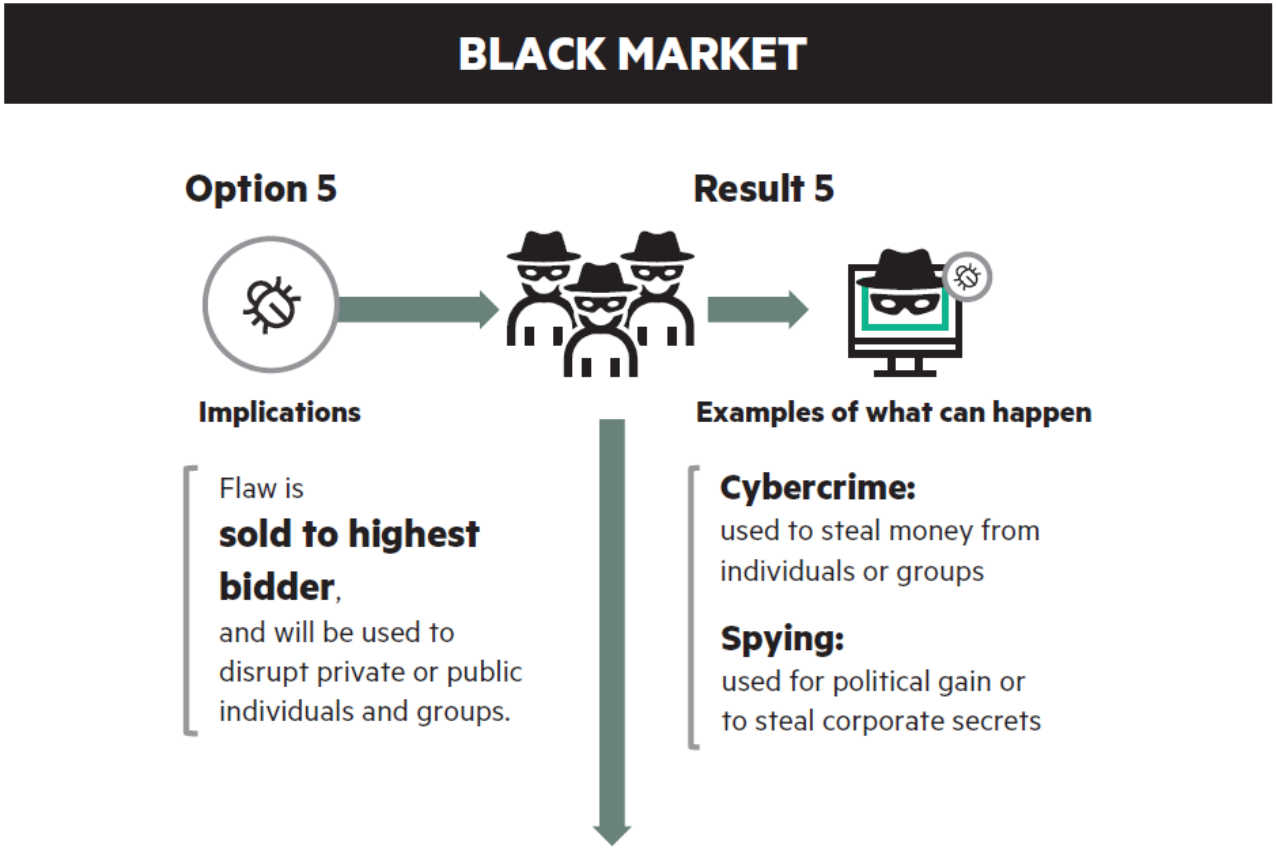


Figure 6. The vulnerability black market

Cybercrime Marketplace

Credit Cards

	Price in 2013	Price in 2014	Recent Prices
Visa and MasterCard (U.S.)	$4	$4	$7
Visa Classic and MasterCard (U.S.) with Track 1 and Track 2 Data	$12	$12	$15
Visa Classic and MasterCard (Canada, Australia, and New Zealand) with Track 1 and Track 2 Data	$19 – $20	$19 – $20	$25
Visa Classic and MasterCard Standard (EU) with Track 1 and 2 Data	$28	$28	$40
Visa Classic and MasterCard Standard (U.K) with Track 1 and Track 2 Data	$19 – $20	$19 – $20	$40
Visa Classic and MasterCard Standard (Japan and Asia) with Track 1 and Track 2 Data	$28	$28	$50
Premium Visa and MasterCard (U.S.) with Track 1 and Track 2 Data		$23 (V); $35 (MC)	$30
Premium Visa and MasterCard (EU and U.K.) with Track 1 and 2 Data		$23 (V); $35 (MC)	$50 – $60
Premium Visa and MasterCard (Canada, Australia and New Zealand) with Track 1 and Track 2 Data		$23 (V); $35 (MC)	$35 for V and MC
Premium Visa and MasterCard (Japan and Asia) with Track 1 and Track 2 Data		$23 (V); $35 (MC)	$80 for V and MC
Premium American Express Card (U.S.) with Track 1 and Track 2 Data		$23 (V); $35 (MC)	$30
Premium Discover Card (U.S.) with Track 1 and Track 2 Data		$23 (V); $35 (MC)	$30
VBV (U.K., Australia, Canada, EU and Asia)	$17 – $25	$28	$25

Cybercrime Marketplace

Hacking Email and Social Media Accounts

	Recent Prices
Popular U.S. Email Accounts (Gmail, Hotmail, Yahoo)	$129
Popular Russian Email Accounts (Mail.ru, Yandex.ru, and Rambler.ru)	$65 – $103
Popular Ukranian Email Accounts (Ukr.net)	$129
Popular U.S. Social Media Accounts	$129
Popular Russian Social Media Accounts (VK.ru and Ok.ru)	$194
Corporate Email Accounts	$500 per mailbox
IP address of Computer User	$90

Tools

	Price in 2013	Price in 2014	Recent Prices
Remote Access Trojans (RATs)	$50 – $250	$20 – $50	$5 – $10
Crypters	N/A	$50 – $150	$80 – $440
Angler Exploit Kit			$100 – $135

Cybercrime Marketplace

Identities, Passports, Social Security Cards and Other Documents

	Price in 2013	Price in 2014	Recent Prices
US Fullz	$25	$30	$15 – $65
Fullz (Canada, U.K.)	$30 – $40	$35 – $45	$20 (Canada) $25 (U.K.)
U.K. Passport Scan			$25
Physical Counterfeit Passports (non-U.S.)	N/A	$200 – $500	$1,200 to $3,000 (European)
Physical Counterfeit Passports (U.S.)			$3,000 to $10,000
Templates for U.S. Passports			$100 – $300
New Identity Package, including scans of Social Security Card, Driver's License and, matching utility bill		$250; matching utility bill an additional $100	$90
Physical Counterfeit Social Security Cards		$250 – $400	$140 – $250
Scans of Counterfeit Driver's License			DL Scans $14 – $20 (U.S.) $14 (U.K., CANADA)
Physical Counterfeit Driver's License (France)			$238
Physical Counterfeit Driver's License (U.S., U.K., Germany, Israel, International Driver's Permit)		$100 – $150	$173

Cybercrime Marketplace

Online Accounts	Recent Prices Price based on account balance
Popular U.S. Online "Business" Payment Account Credentials	Ranges from $20 – 149
Transfer Funds from Popular Online Payment Account to Buyer's Account of Choice	$750 cost $226 $1,500 cost $377 $1,520 cost $385 $2,290 cost $573 $2,999 cost $750 $3,799 cost $950
Popular U.S. Online Payment Account Credentials	$330 cost $80 $400 cost $160 $500 cost $240 $600 cost $320 $950 cost $600

Cybercrime Marketplace

Bank Accounts; Airline and Hotel Points	Recent Prices
Bank Account Credentials	Price based on account balance
Bank accounts — ANZ (Australia)	$18,000 cost $4,750
Bank accounts — ANZ (Australia)	$22,000 cost $2,250
Bank accounts — ANZ (Australia)	$62,567 cost $3,800
Bank accounts with no balance listed — Turkey, Sweden, Norway, Romania, Bulgaria, Croatia,	$400 (flat fee)
Bank accounts — (U.K.)	$27,003 cost $2,000
Bank account — (U.S.)	$1,000 cost $40
Bank account — (U.S.)	$2,000 cost $80
Bank account — (U.S.)	$4,000 cost $150
Bank account — (U.S.)	$7,000 cost $300
Bank account — (U.S.)	$15,000 cost $500
High Quality Bank Accounts with Verified, Large Balances of $70,000 – $150,000	6% of the balance of the account
Large U.S. Airline Points Accounts — varies based on amount	Price based on points in account
	1,500,000 points cost $450
	300,000 cost $90
	200,000 cost $60
Large Middle East Airline Points Accounts — varies based on amount	Price based on points in account
	500,000 cost $150
	450,000 cost $90
	250,000 cost $50
Large International Hotel Chain Points Account	Price based on points in account
	1,000,000 points cost $200
	400,000 cost $80
	300,000 cost $60
	200,000 cost $40
	100,000 cost $20
	50,000 cost $10

Cybercrime Marketplace

Hacking Services	Price in 2013	Price in 2014	Recent Prices
Hacking Tutorials	N/A	$1 each to $30 for 10 (depending on the tutorial)	$20 to $40 for multiple tutorials
Hacking Website (stealing data)	$100 – $300	$100 – $200	$350
DDoS Attacks	Per Hour: $3 – $5 Per Day: $90 – $100 Per Week: $400 – $600	Per Hour: $3 – $5 Per Day: $60 – $90 Per Week: $350 – $600	Per hour: $5 – $10 Per Day: $30-$55 Per Week: $200 – $555
Doxing	$25-$100	$25-$100	$19.99

Cybersecurity Due Diligence

Due Diligence on Information

- What information the seller collects?
- What locations is the information collected from?
- How is that information is utilized?
- Where that information is stored, and who has access to it?
- How the information may and may not be utilized during pre-signing and post-signing phases?
- Is the valuation dependent upon personal data? If so, can that data be used for new purposes?
- What policies and procedures govern that information?
- What state, federal, and foreign laws govern that data?
- What responsibilities have been assigned to a third party vendor?
    - What contract terms are in place with those vendors, and are they adequate?

The Target's Privacy Policy

- The privacy policy can impact how PII, PHI, cardholder data, etc. can be used by the acquirer.
  - Can limit the value of data
  - Can pose legal challenges when expanding to new markets
  - Uncertainty in privacy regulations
    - EU Safe Harbor replaced by Privacy Shield
    - Brexit
- Definitions of PII can vary by jurisdiction, so choose the language in warranties and representations carefully.
- Require all versions of the privacy policy that have been in use.

The Target's Cybersecurity Risks

- How knowledgeable is management and board about the company's cybersecurity risks?
- What types of information does the company manage?
  - Credit card data
  - Protected Health Information ("PHI")
  - Personally Identifiable Information ("PII")
  - Financial Account Information
  - Intellectual Property
  - Controlled Unclassified Information ("CUI")
- Is the seller considered "Critical Infrastructure"
- Does the company host this information, or does a third party?
- Is the company a service provider?
- Who are their customers?
- Is their network connected to any third parties?
- Is they're business model susceptible to Distributed Denial-of-Service ("DDoS") or ransomware attacks?

The Target's Cybersecurity Practices

- Has the company established an information security management program?
  - Risk Assessment
  - Clearly defined responsibility
  - Documented policies and procedures
  - Vulnerability and patch management
  - Security event monitoring and incident response
  - Documented and tested disaster recovery and business continuity plan
  - Is security awareness training provided to all employees?
- Has the program been assessed by a third party?
  - Vulnerability scanning and penetration testing
  - Security assessment or audit
- Has internal or external legal counsel reviewed the company's security compliance?
- Do they have cyber insurance, at what level, and do they comply with any warranties or representations?
- Are there significant gaps that require remediation?

The Target's Vendor Risks

- Does the company have a vendor management program?
  - Have they documented the control objectives that they rely on third parties to perform?
  - How do they monitor vendor performance?
  - Are the contract terms adequate?

Third Party Reporting

- SSAE16 Service Organization Control (“SOC”) 1 – Internal controls over financial reporting
  - Type I – Point-in-Time
  - Type II – Period-in-Time
- SOC2 – Internal controls over security, confidentiality, availability, processing integrity, and privacy.
  - HITRUST
  - NIST
  - Cloud Security Alliance
  - COSO
  - COBIT
- PCI-DSS Attestation of Compliance
  - Point-in-Time
- ISO 27001 – Certification Information Security Management System
  - Point-in-Time

Types of Cybersecurity Due Diligence

- Legal:
  - Review legal obligations, privacy policies, customer contracts, vendor contracts, policies, procedures, and etc.
- Compromise
  - Investigation to identify if the seller is currently compromised.
  - Investigation to identify if the seller's proprietary or confidential information is available for sale on the internet or darknet.
- Audit
  - Evaluate the design and operation of controls to meet security and privacy obligations.
  - Remediation testing.

Disclosures, Warranties, Indemnities and Escrows

Common representations and warranties:

(a) operated its business at all times in compliance with all applicable privacy and data security laws;
(b) complied with its corporate polices applicable to data privacy, data security and “personal information” at all times; and
(c) not experienced any incident in which “personal information” or other sensitive data was or may have been stolen or improperly accessed.

Disclosures, Warranties, Indemnities and Escrows

Warning: I am not a lawyer.

- Breach disclosures may not be an effective means of discovering if a company has been breached. Consider using indemnities or escrows instead, or in addition to.

- Avoid overly broad disclosures and warranties, such as “complies with all relevant data security and privacy laws”.

- For technology service providers, transaction processors or other entities that aggregates large volumes of personal data:
  - Closing conditions tied to the non-occurrence of a breach.
  - Indemnity may cover actual losses associated with a breach.

Integration Plan

- Determine what information can be integrated.
- Develop a process to cleanse information that cannot be integrated, or gain authorization for information that requires opt-in.
- Plan for who will be responsible for complying with information security and privacy requirements during the integration period.
- IT hardware and software maintenance agreements and patch levels can impact insurance coverage in the event of a breach.
- If the buyer is taking on new compliance requirements from the seller, the buyer should consider performing an internal gap assessment.
- Train employees on new or changed responsibilities, policies, and procedures.

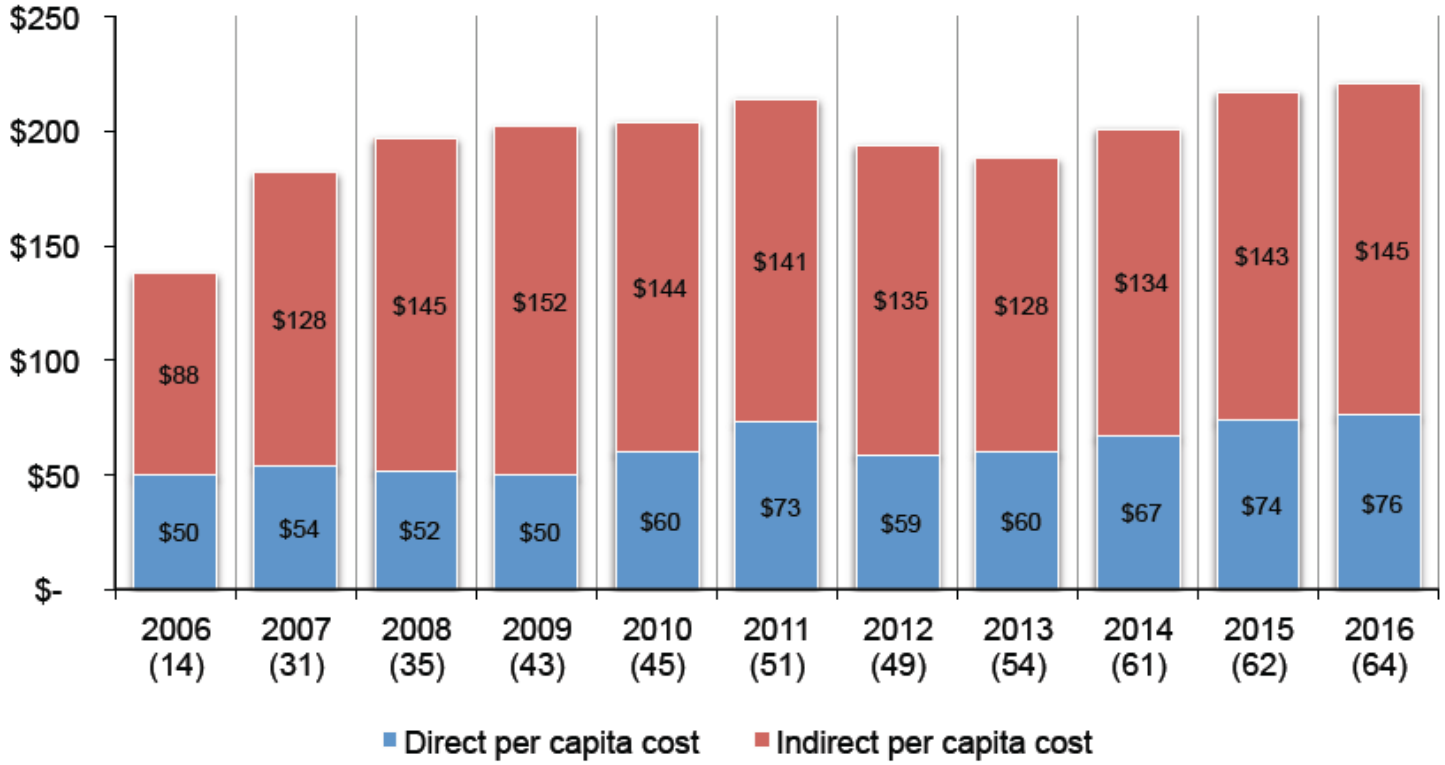
Considerations for Public Companies

- Pressure to disclose board's level of knowledge regarding cybersecurity.
- Under Regulation S-K, the SEC may require cybersecurity disclosures in the following areas:
  - Risk Factors
  - MD&A
  - Description of Business
  - Legal Proceedings
  - Financial Statement Disclosures
  - Disclosure Controls and Procedures

Costs of a Data Breach

Per Capita Cost of a Data Breach

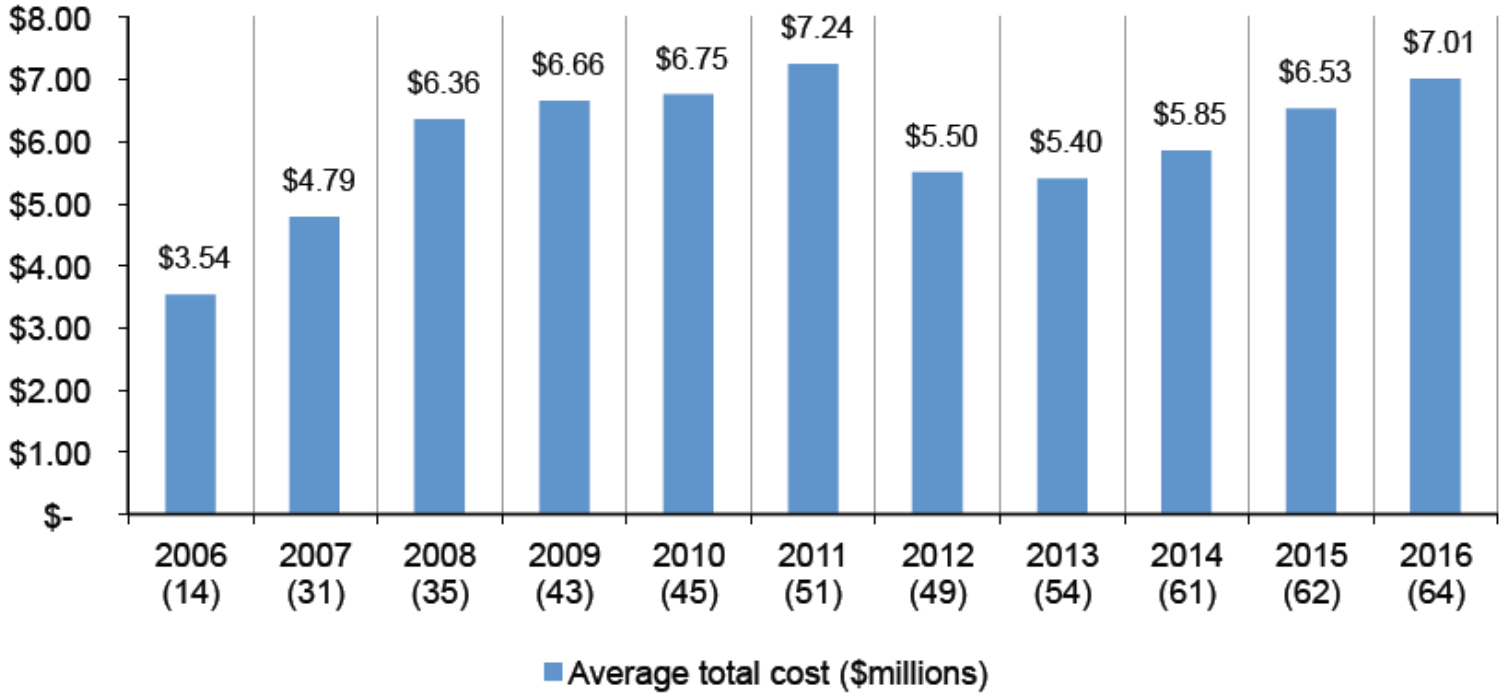
Figure 15. Direct and indirect per capita data breach costs over 11 years



whitleypenn
CPAs and Professional Consultants

Total Organizational Costs of a Data Breach

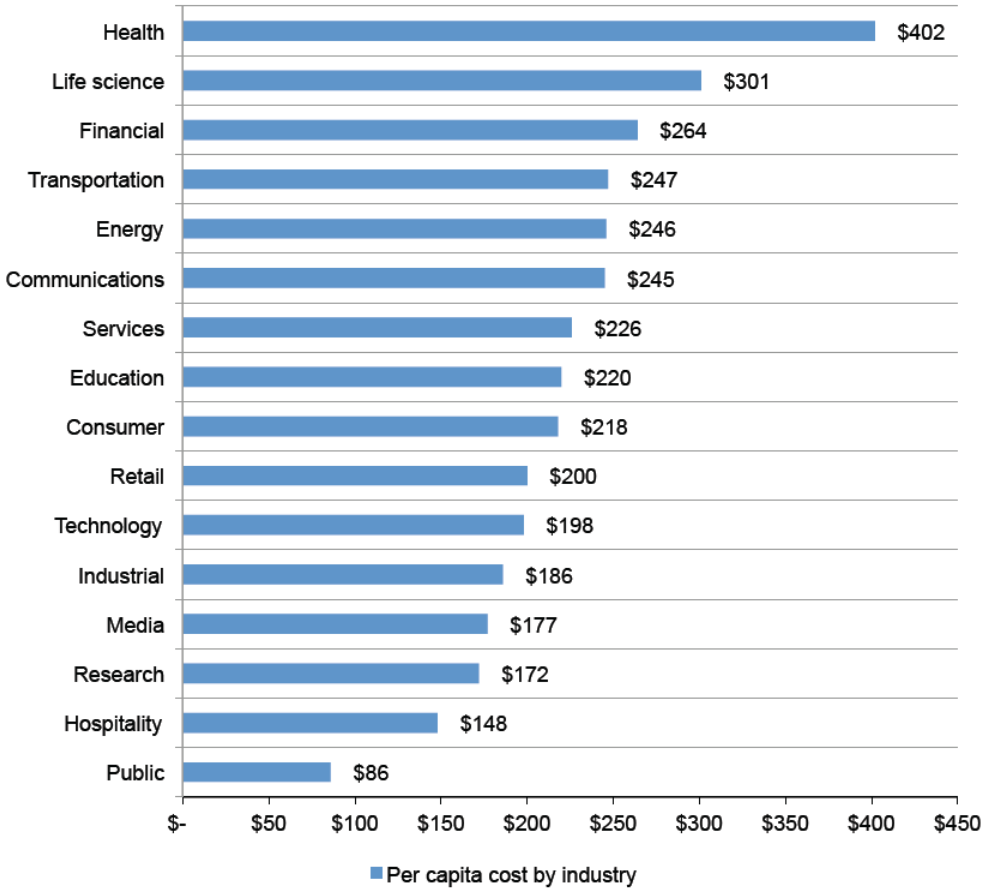
Figure 2. The average total organizational cost of data breach over 11 years
(millions)



whitleypenn
CPAs and Professional Consultants

Per Capita Costs by Industry

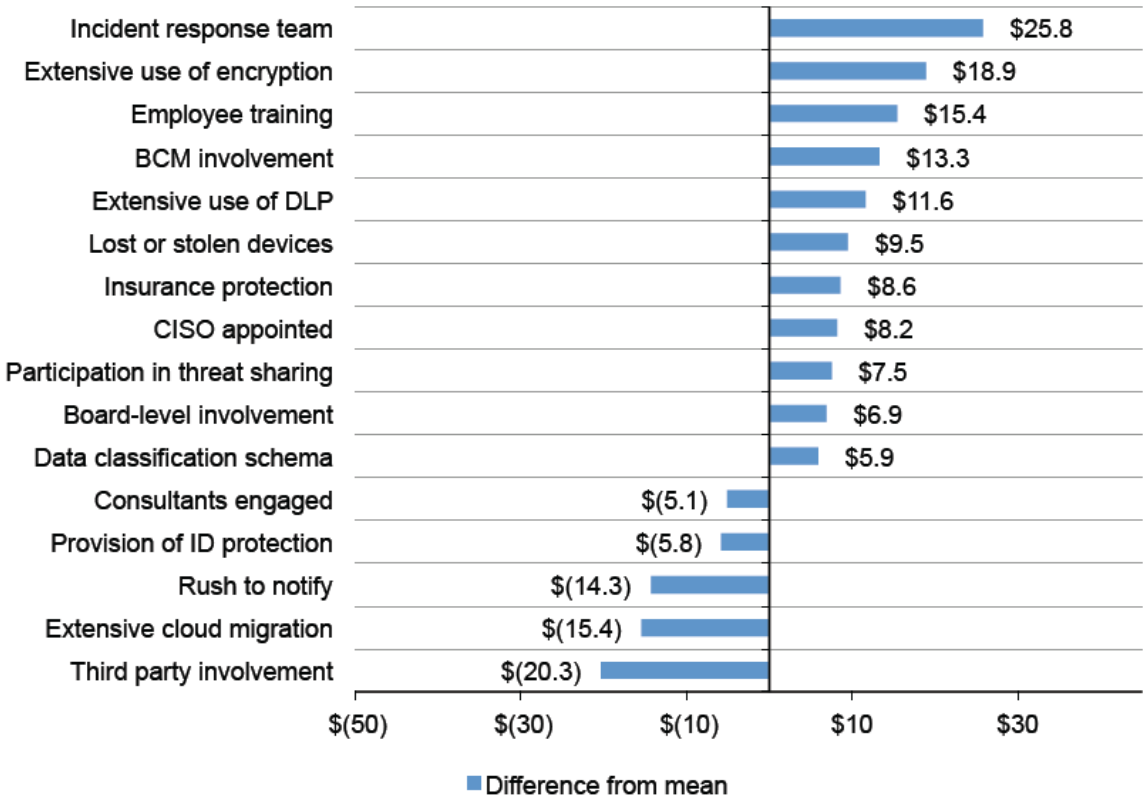
Figure 4. Per capita cost by industry classification of benchmarked companies



whitleypenn
CPAs and Professional Consultants

Factors that impact the per capita cost

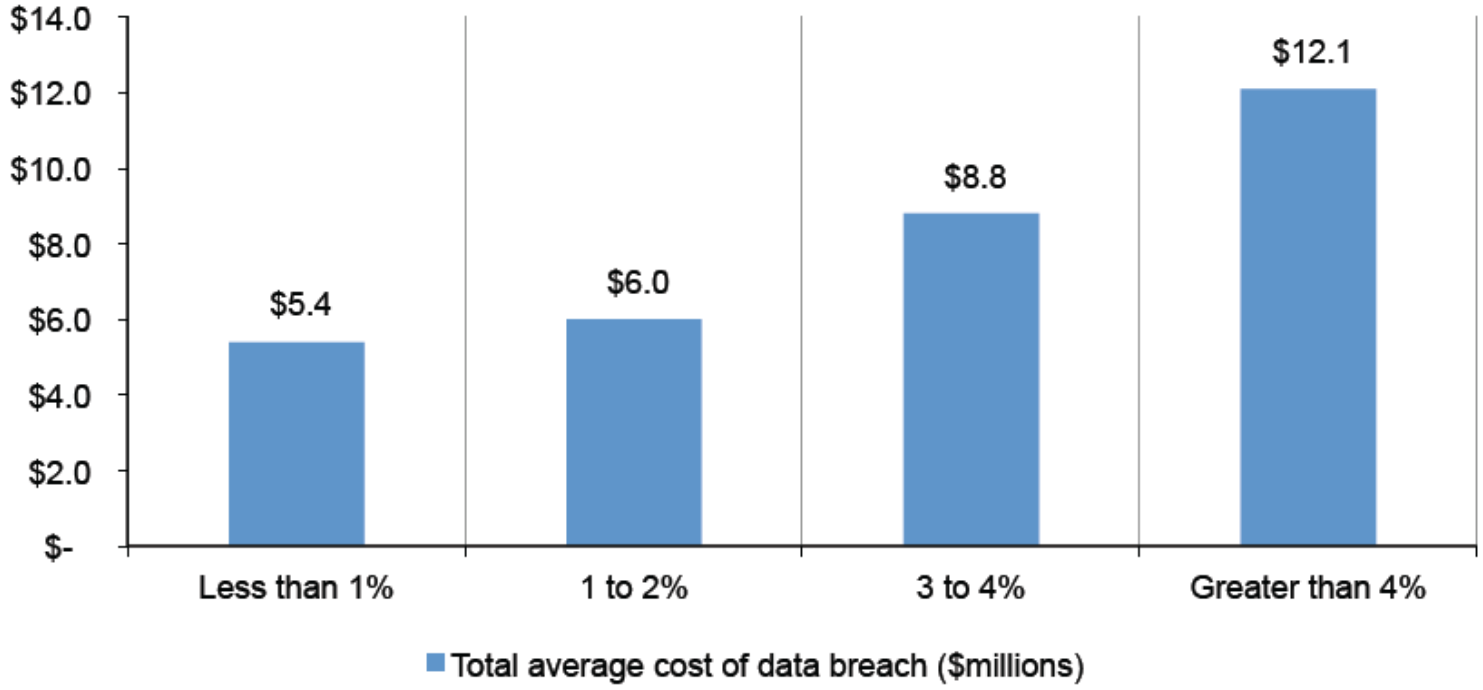
Figure 7. Impact of 16 factors on the per capita cost of data breach



whitleypenn
CPAs and Professional Consultants

Impact of Abnormal Churn Rates

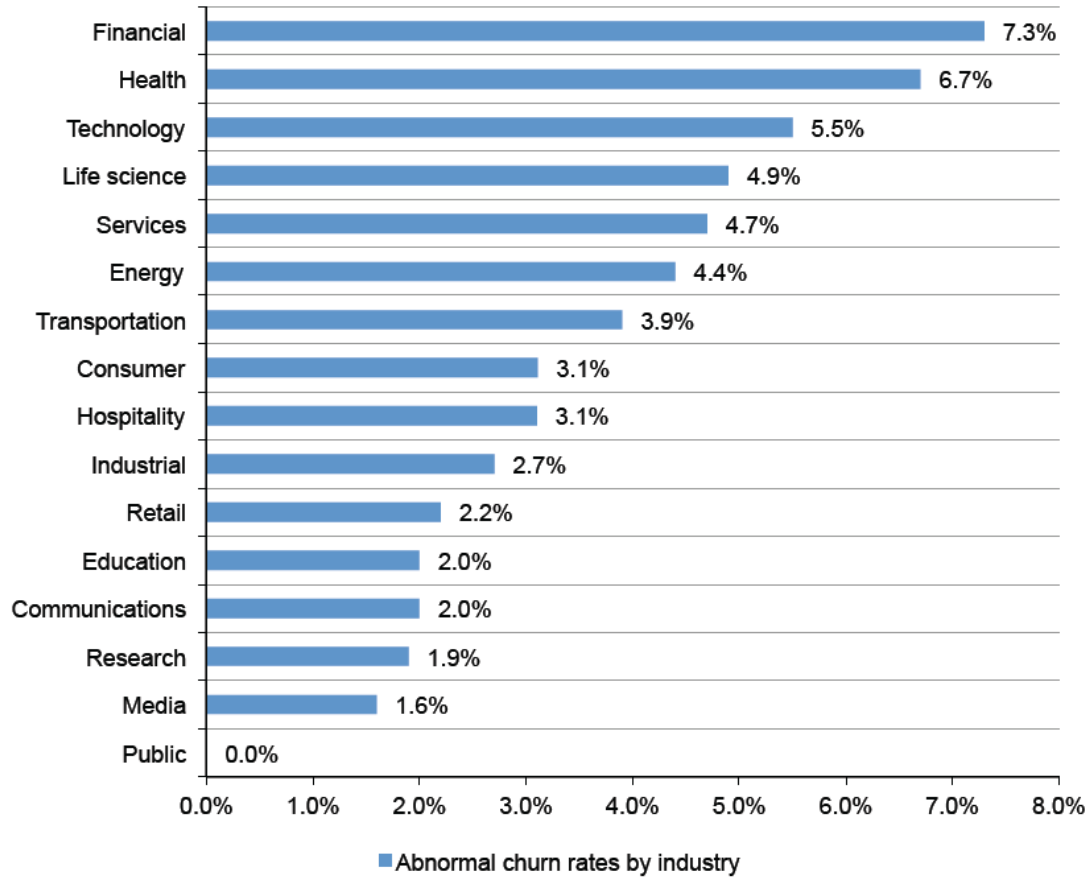
Figure 9. Total cost of data breach by abnormal churn rate



whitleypenn
CPAs and Professional Consultants

Abnormal Churn Rates by Industry

Figure 10. Abnormal churn rates by industry classification of benchmarked companies



whitleypenn
CPAs and Professional Consultants

Questions

References

- HP Enterprise – 2016 Cyber Risk Report
- Verizon 2016 Data Breach Digest
- IBM 2016 Cost of Data Breach: United States
- Dell SecureWorks – 2016 Underground Hacker Markets