
# It Could Happen to You: Surviving a Cyber Attack

*The Crypsis Group & Bryan Cave Leighton Paisner*
*Billy Evans, Director – San Antonio, TX / Kevin Scott, Counsel – Chicago, IL*
*Duane Murray, Moon Baker Insurance Agency / Jason Berry, Berry Family Services*
*October 31, 2019 | Austin, TX*

# Billy M. Evans Jr.

Director

**Over 20 years of industry experience**
Law Enforcement
Incident Response
Forensics

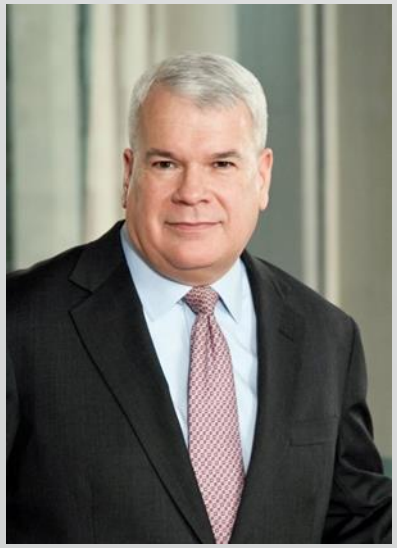
**Previously**
Director Global Cyber Risk Services Alvarez & Marsal
USAA Digital Forensics Laboratory
Special Agent with USAF Office of Special Investigations

billy.evans@crypsisgroup.com

# The Crypsis Group

We create a more secure digital world by providing the highest quality **incident response**, **risk management**, and **digital forensics** for our clients.

We are the firm that gets the call when someone has been the **victim of a cyber crime**. We **respond** quickly, **investigate**, find out **what happened**, and help **prevent** it from happening again.



**Kevin Scott**
Chicago, IL
+1 312 602 5074
Kevin.scott@bclplaw.com

Kevin Scott is a member of the firm’s Commercial Litigation, and Technology, Entrepreneurial and Commercial Practice Groups. He focuses his practice on data security, privacy breach response, payment card industry standards and investigations, and is a member of the firm's Data Breach Hotline. He frequently advises clients on compliance with state, federal and international laws and regulations. He has handled hundreds of breaches for small and large entities, successfully reducing public and regulatory scrutiny and protecting clients’ reputations. He regularly speaks and writes on data privacy and security issues.

BRYAN CAVE LEIGHTON PAISNER BCLP

# Agenda

01. Data Breaches

02. Incident Response

03. Legal Considerations

04. Notification

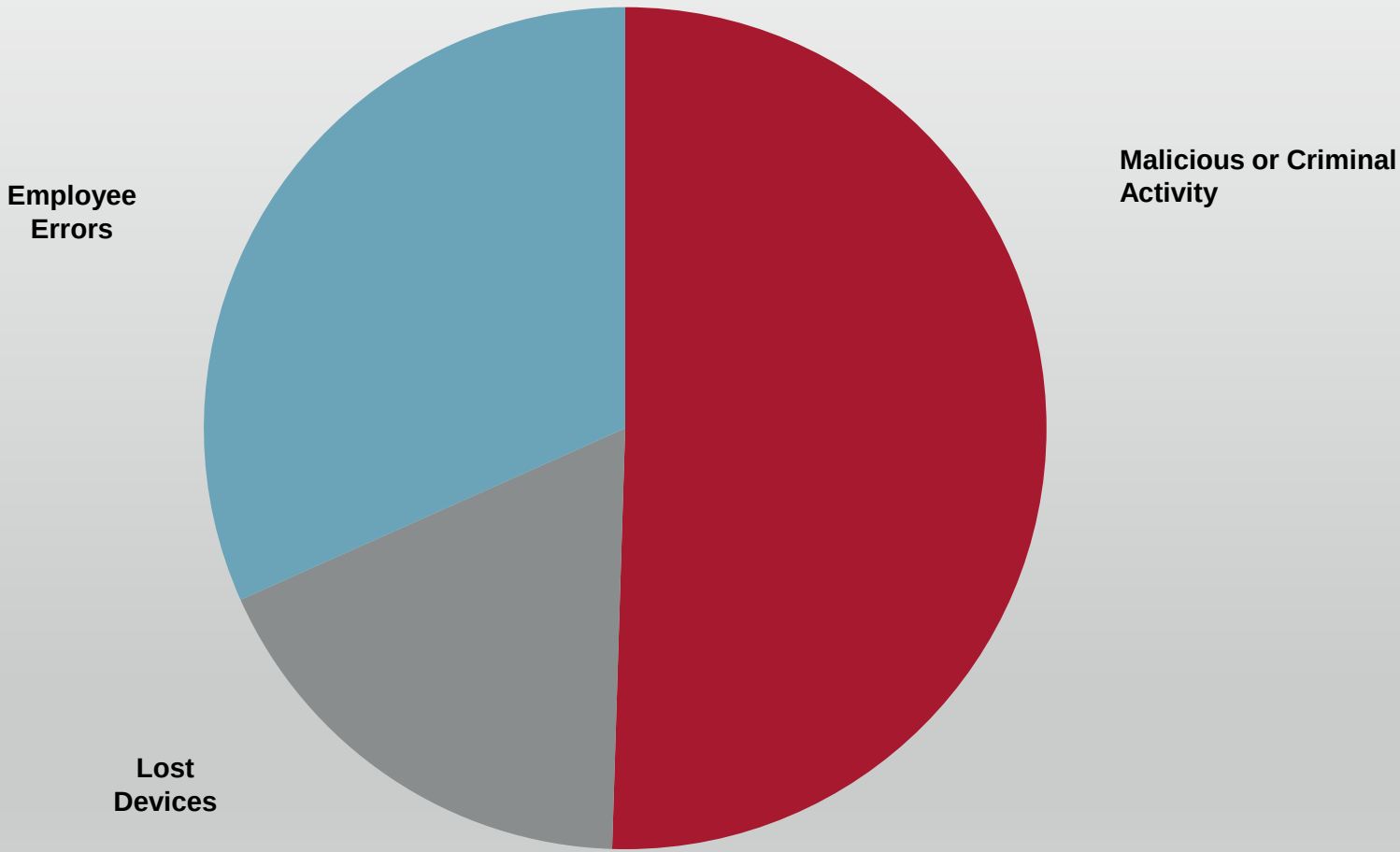
05. Costs of a Data Breach

06. Hindsight is 20/20

# Data Breach: What is it?

- Data breach is the intentional or unintentional access, acquisition, or disclosure of sensitive, protected, or confidential data to an unauthorized individual or individuals.

# Causes of Data Breaches




* Ponemon Institute, 2019 Cost of Data Breach Study (June 2019)

# Business Email Compromise

Phishing emails provided access to environments


Brute force remote desktop credentials

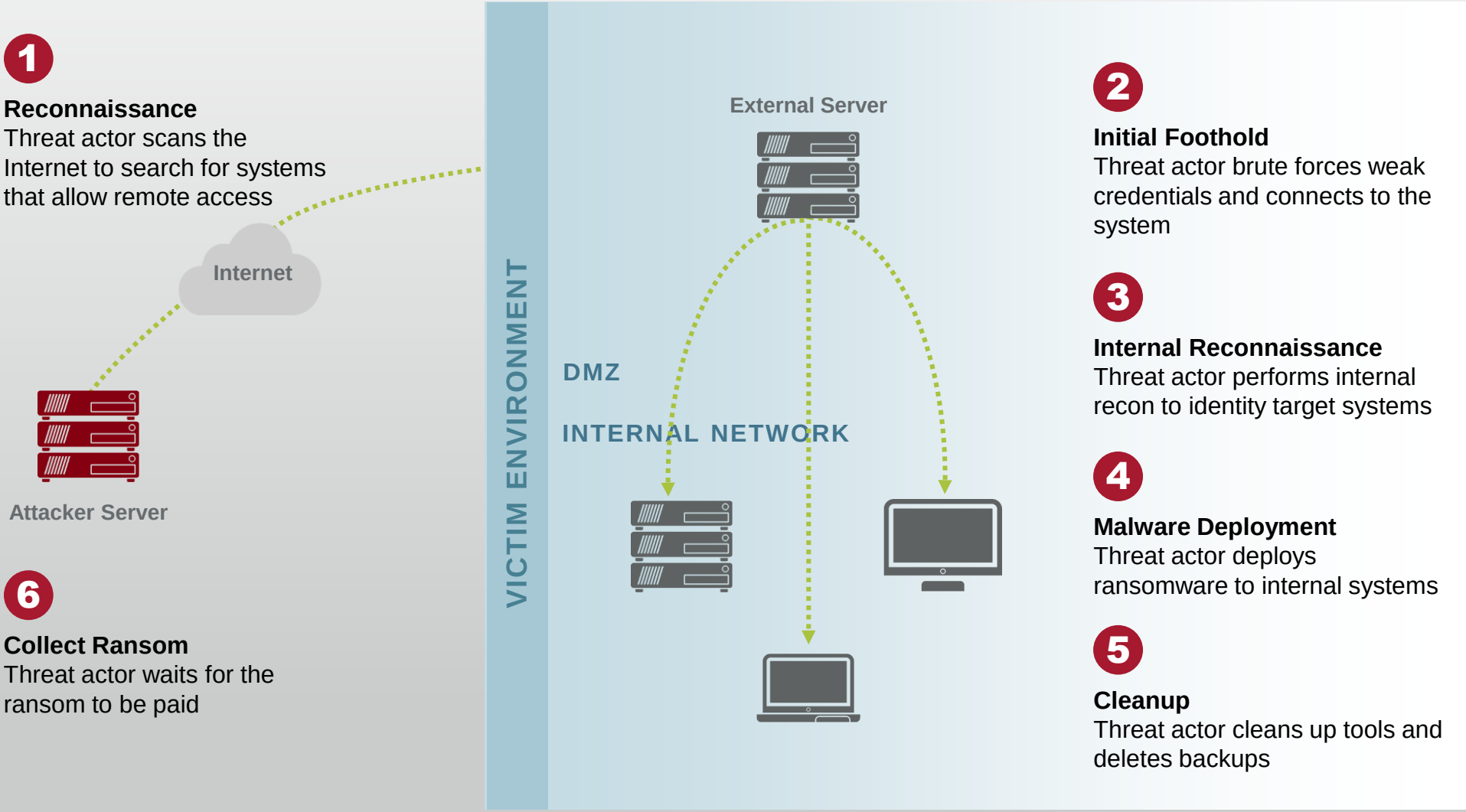
- Lateral movement for persistence
- Intelligence gathering
- Malicious rules/deletions
- Intercept and insertion into comms

- Request for fund transfers
- Mailbox sync
- Spear phishing campaigns
- Access to internal systems


Theft of PII, PHI, PCI

Theft of Intellectual Property

# Anatomy of the Attack – Ransomware



# Ransomware Attack

- Medical practice hit with ransomware attack. Because automated backup running at same time, backup files encrypted as well.
- Primary server and 7 workstations affected.
- Ransom Demand for 1.5 BTC.
- Under HIPAA, the mere encryption of PHI triggers the Breach Notification Rule. In order to avoid notification, Covered Entity must demonstrate a low probability that the PHI has been compromised.
- Crypsis is brought in to negotiate the ransom payment and conduct forensic investigation into the ransomware attack.

# Incident Response Defined

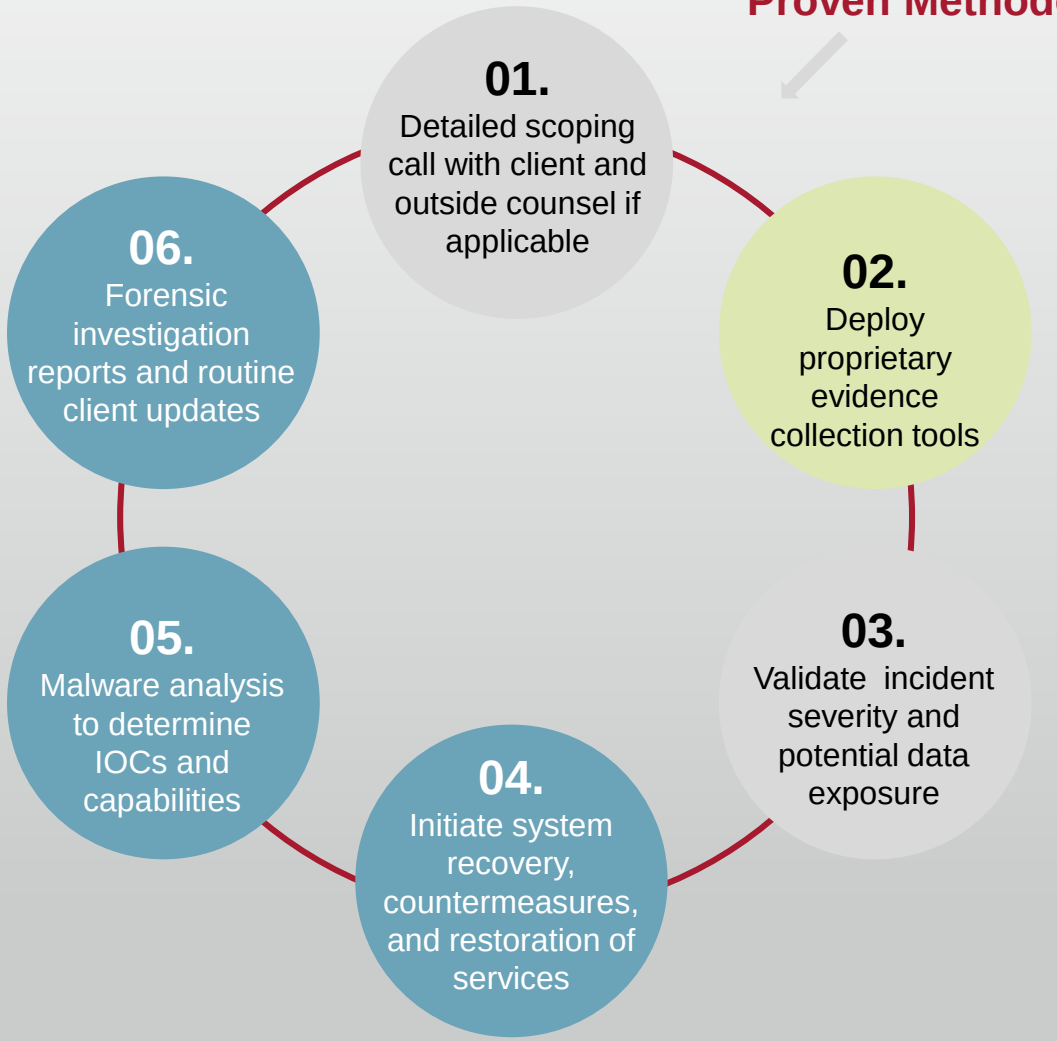
Incident response is a systematic approach to addressing and managing the aftermath of a security incident, computer intrusion, or cyberattack.

The goal is to handle the matter in a way that limits damage, preserves evidence, and reduces recovery time and costs.

# Data Breach Response & Investigations

We are a preferred IR provider for over **35 insurance carriers** and an approved provider for almost every carrier.

## Proven Methodology




- Rapid Onsite Support
- Ransomware Payment Facilitation
- Endpoint Protection Deployment

# Results of Forensic Analysis

- Results were inconclusive.
  - → Actions taken to restore IT network prevented forensic analysis from being able to reach the low probability threshold that any PHI was compromised, resulting in a decision to notify the potentially affected population in an abundance of caution, in compliance with HIPAA.
  - → Under HIPAA, must prove that there was an absence of indicators of access rather than proving that there were indicators of access.

# U.S. Law re Data Breaches

- All 50 states have their own, similar breach notification laws.
- These laws apply if the individual is a resident of that state.
- Focus is not on where the covered entity is located.
- Only apply if certain data elements are exposed – e.g., social security number, driver's license number, financial account number, username/password for online account, and sometimes medical/health, insurance, passport number, and biometrics.
- Certain industries are regulated by federal law (finance - GLBA, healthcare - HIPAA).
- Generally can conduct a risk assessment.
- Notification of living and deceased.
  - → Estates of deceased notified for up to 50 years.

# Notification Requirements

- General Requirements of Individual Notification Letters
  - → What happened and what type of information was compromised?
  - → What can the individuals do to protect themselves and how does the entity plan to assist them?
  - → Credit monitoring and identity theft restoration services.
  - → Explain what has been done and is being done to prevent future events.
- Substitute Notice
- Media Notice

# Regulatory Notification

- As of 01/01/2020, Texas Attorney General Notification > 250 indvls.
- Texas HHS
- Other State Attorneys General
  - → Depending upon current state residency of individual.
- HHS
  - → Less than 500 individuals, March 1st of following calendar year.
  - → 500 or more individuals, within 60 days of discovery.
    - HHS OCR Investigation
      - 500 or more individuals.
      - Investigation can go beyond data breach.
      - Will inquire into HIPAA compliance in both policies and procedures.

# Thinking About Liability

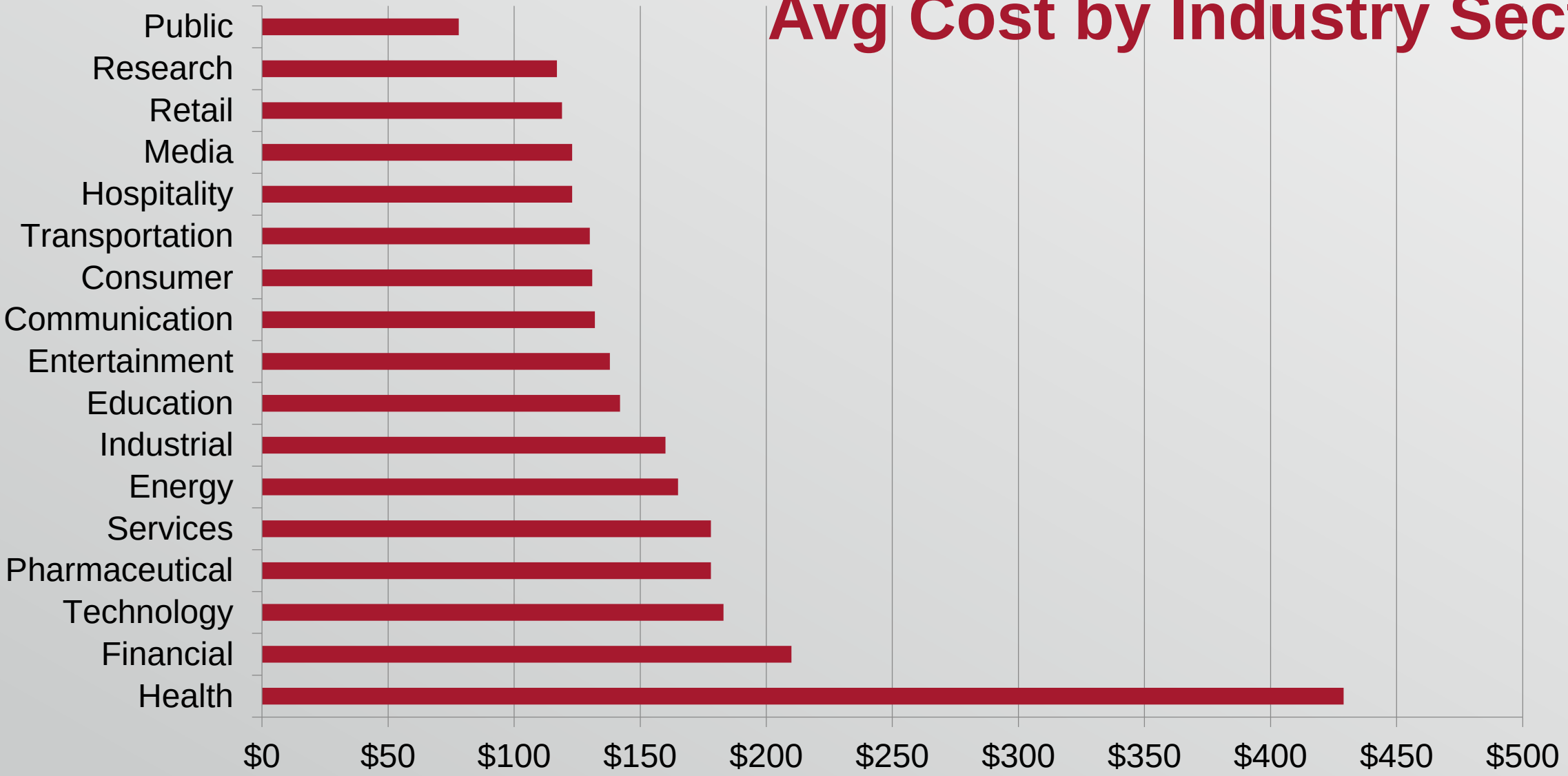
Average Cost of a Data Breach =

**$8.19 million or**

**$242 / Record***

* Ponemon Institute, 2019 Cost of Data Breach Study (June 2019)

# Avg Cost by Industry Sector




* Ponemon Institute, 2019 Cost of Data Breach Study (June 2019)

# Costs of a Data breach

- Breach Coach (legal)
- Ransomware Payment
- Data Recovery/Replacement
- Forensic Investigation
- Notification
  - → Credit Monitoring/Identity Theft Restoration
  - → Call Center
  - → Public Relations
- Regulatory Inquiries
  - → HHS OCR
  - → Texas HHS
  - → State Attorneys General
- Business Interruption Loss

- Evaluate Your Cyber Insurance Policy
- Companies are increasingly purchasing cyber liability insurance
- Many do not understand breach costs, risks, or what the policies cover
- Evaluate policies to ensure appropriate coverage
- Analyze exclusions – do the exceptions swallow the policy?
- Evaluate limits and sub-limits

# Hindsight is 20/20

## If I knew yesterday what I know today, I would have…

- Trained my staff
  - → User awareness training (phishing exercises)
  - → Telephonic wire verification
- Turned on logging or more robust logging
  - → Firewall, SIEM, system\event, unified audit, mailbox
- Implemented two factor authentication (2FA)
- Disabled Remote Desktop Protocol (RDP)
- Mandated the use of complex passwords
  - → 15 characters, upper/lower case, numbers and special characters
  - → Controls in place
- Data Mapping (flow and where data lives)
  - → Who has/stores sensitive data
- Risk Assessments/Management
  - → Independent
    - Internal
    - Third Parties

# BCLP's Data Privacy and Cyber Security Team

- Our team is located across the United States and Europe and advise clients in a variety of sectors including manufacturing, software, travel, financial services and retail.
- We focus on one thing – helping our clients utilize data to increase opportunities and enhance user experience, all while decreasing corporate risk.
- Our team has experience handling the full scope of privacy and security issues. In the context of data privacy we advise clients on:
  - privacy and data protection programs
  - data sharing and international mobilization of data
  - Policies and procedures
  - complex transactions involving monetization and licensing of data
- Additionally, we conduct gap assessments to align compliance with international privacy standards, respond to regulatory investigations and inquiries, and defend companies in courts and before government agencies in enforcement actions.
- In the context of data security, we have a world class data breach response practice which has responded to two thousand significant breaches or incidents. We leverage that experience to help companies identify gaps in their readiness to respond to a breach, and to train companies on how to respond to breaches effectively. Should an incident occur, BCLP's 24 hour hotline connects clients directly with experienced attorneys who will guide our clients through all aspects of breach response, from investigation to notification to regulatory investigation or litigation. Our experience and practical approach to data breach response uniquely equips us to assist organizations by understanding both the law and the business implications of data breaches.
- We regularly coordinate advice across multiple jurisdictions for clients looking to achieve as streamlined an international data strategy as possible.

# Questions

billy.evans@crypsisgroup.com
www.crypsisgroup.com

kevin.scott@bclplaw.com
www.bcplaw.com