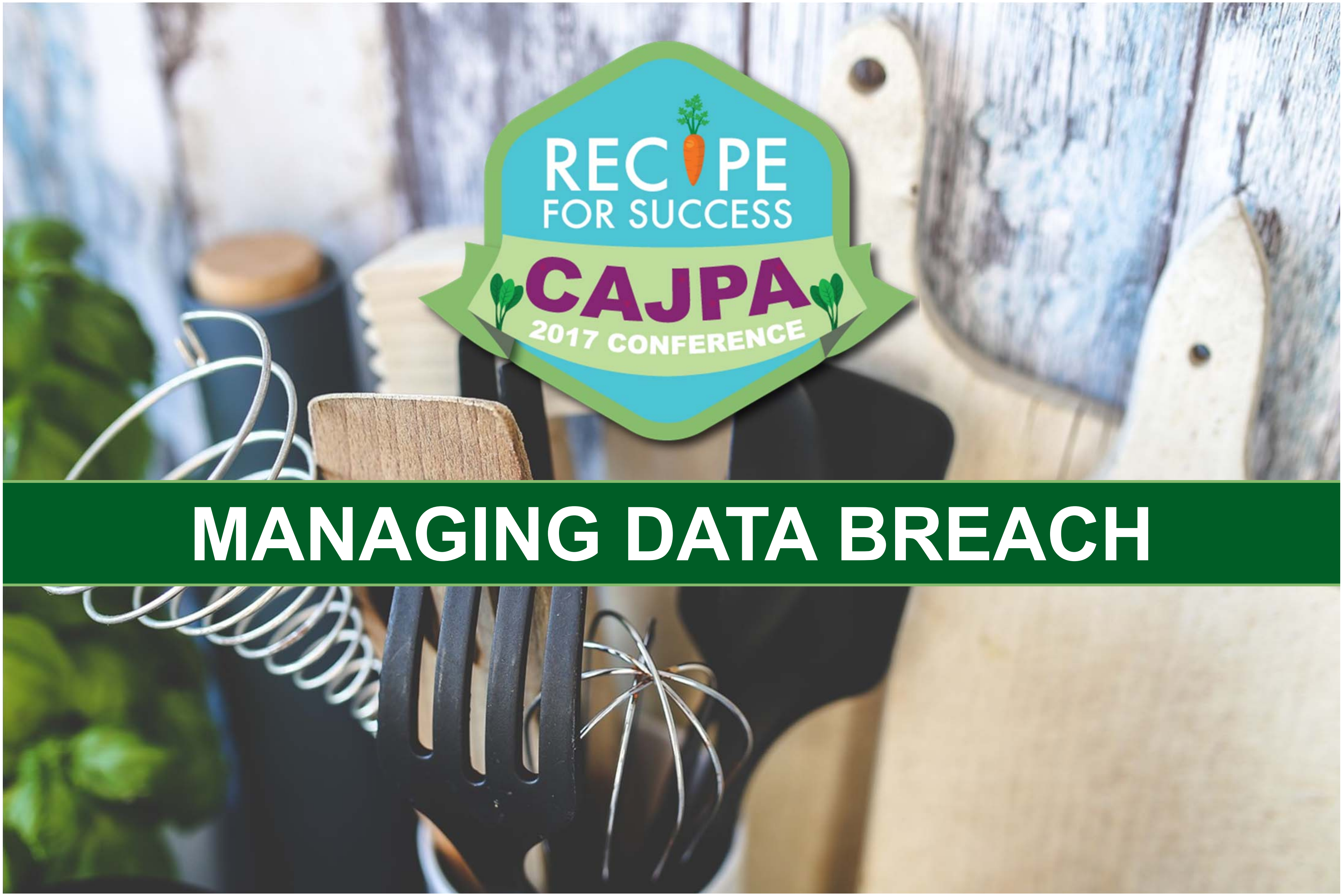


RECIPE FOR SUCCESS

CAJPA

2017 CONFERENCE

MANAGING DATA BREACH

RECIPE FOR SUCCESS

SEPTEMBER 12-15, 2017
SOUTH LAKE TAHOE, CA

Beazley is a specialist insurer and leading provider of cyber insurance.

Michael Phillips is a Claims Manager in the Technology, Media, and Business division of Beazley, and focuses his work on managing incidents related to public entities.

Beazley’s Experience

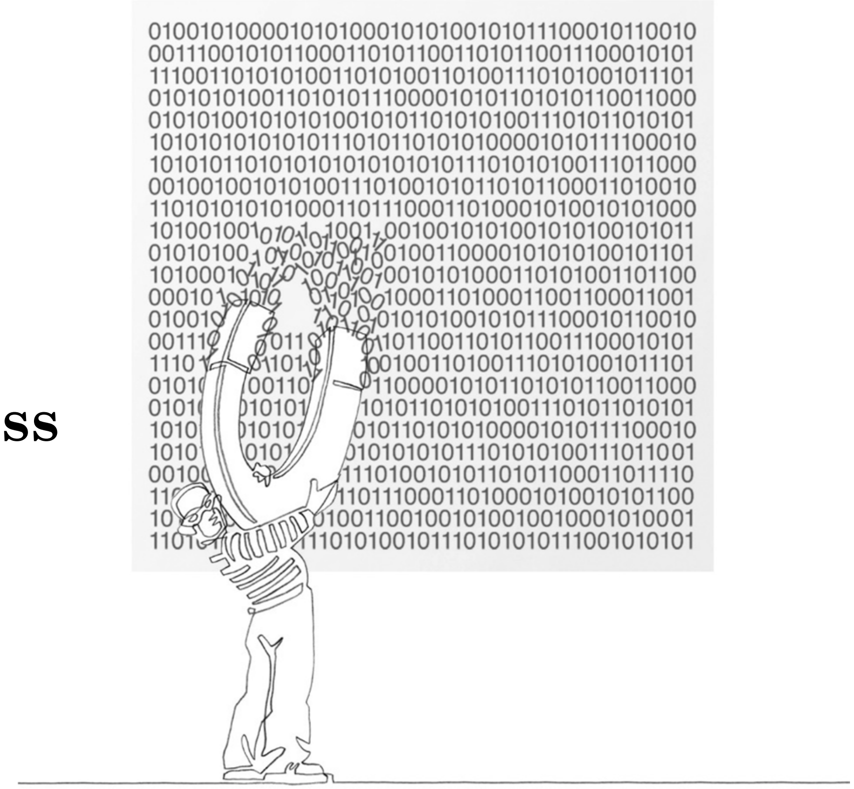
- **Since 2007, we have helped our Insureds manage more than 5,600 incidents, helping them navigate often complex and thorny breach related situations.**

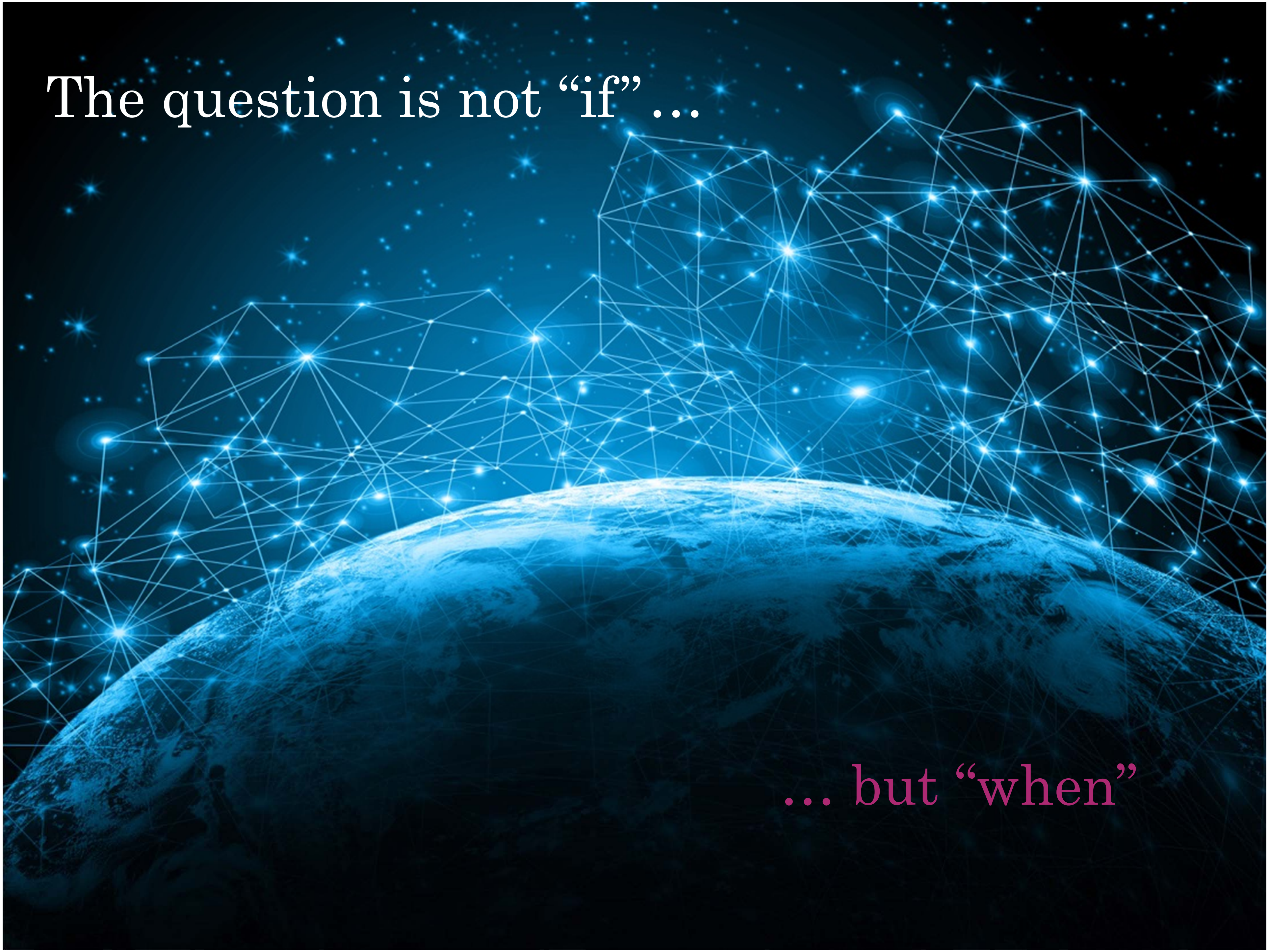
➢ Key sectors:

- Public Entities
- Telecoms
- Utilities
- Healthcare
- Education

Topics

1. Public Sector Cyber Risk Trends
2. Best Practices
3. APIP Coverages
4. The Beazley Claims Process
5. Q&A





The question is not “if” …

… but “when”

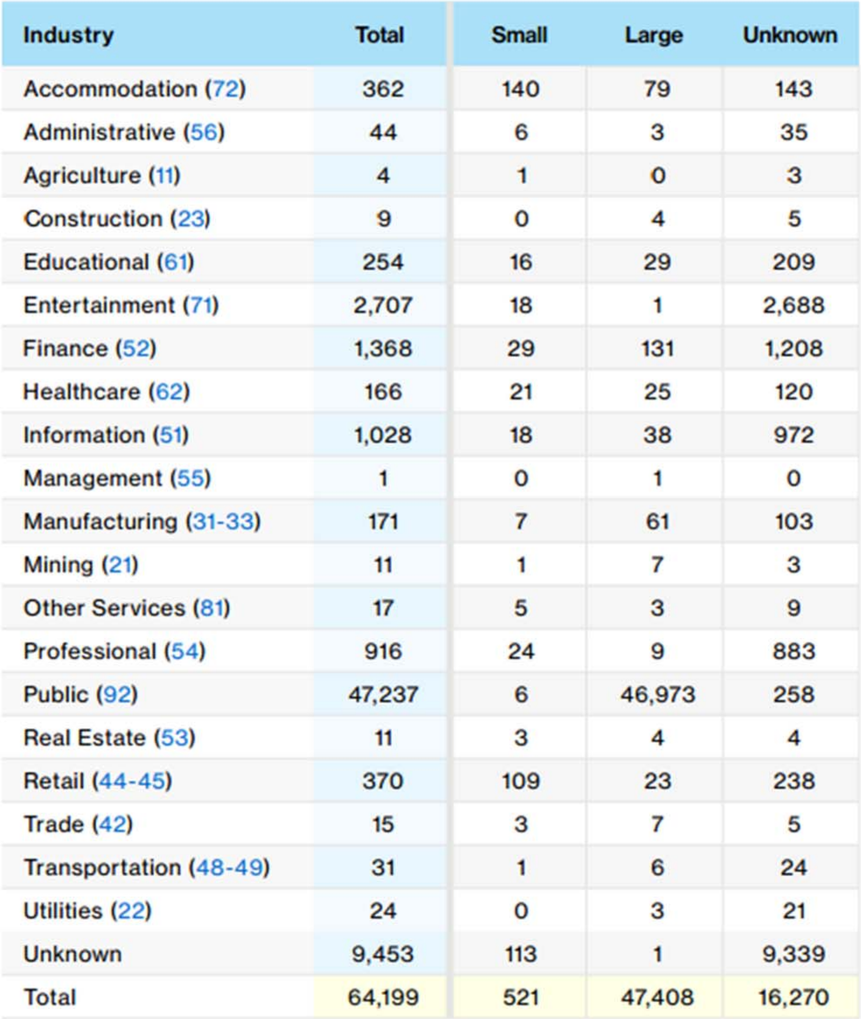
Public Entity Incidents

- San Francisco MUNI (ransomware; approx. 2 days of lost transit revenue)
- Multiple state Dep’ts of Fish & Wildlife (ongoing; Oregon, Washington, Idaho, Kentucky, 6M individuals, hack)
- Utah Department of Health (500K individuals, hack)
- Texas Retirement Systems (3.5M records, inadvertent disclosure)
- U.S. Department of Energy (105K individuals, hack)
- Oregon Employment Department (850K individuals, hack)
- Montana Department of Public Health and Human Services (1.3M individuals, hack)
- South Carolina Department of Revenue (5.7M individuals) (phishing)

Public entities are perceived to be an easier target for cyber criminals.

- **Older, more vulnerable computer systems**
- **Less vigilance**
- **Valuable data**
- **According to the Ponemon Institute’s Annual Study, more than 94 million citizens’ records have been lost or breached since 2009.**

In 2015, Public Entities suffered more security incidents than all other sectors combined.



Industry	Total	Small	Large	Unknown
Accommodation (72)	362	140	79	143
Administrative (56)	44	6	3	35
Agriculture (11)	4	1	0	3
Construction (23)	9	0	4	5
Educational (61)	254	16	29	209
Entertainment (71)	2,707	18	1	2,688
Finance (52)	1,368	29	131	1,208
Healthcare (62)	166	21	25	120
Information (51)	1,028	18	38	972
Management (55)	1	0	1	0
Manufacturing (31-33)	171	7	61	103
Mining (21)	11	1	7	3
Other Services (81)	17	5	3	9
Professional (54)	916	24	9	883
Public (92)	47,237	6	46,973	258
Real Estate (53)	11	3	4	4
Retail (44-45)	370	109	23	238
Trade (42)	15	3	7	5
Transportation (48-49)	31	1	6	24
Utilities (22)	24	0	3	21
Unknown	9,453	113	1	9,339
Total	64,199	521	47,408	16,270

Table 1.

Number of security incidents by victim industry and organization size, 2015 dataset.

Verizon 2016 Data

Breach Report

The Public Sector suffers more incidents caused by human error (misaddressed email, accidentally published data), suggesting improvements in processes and controls can still add value.

2016 Verizon Data Breach Report

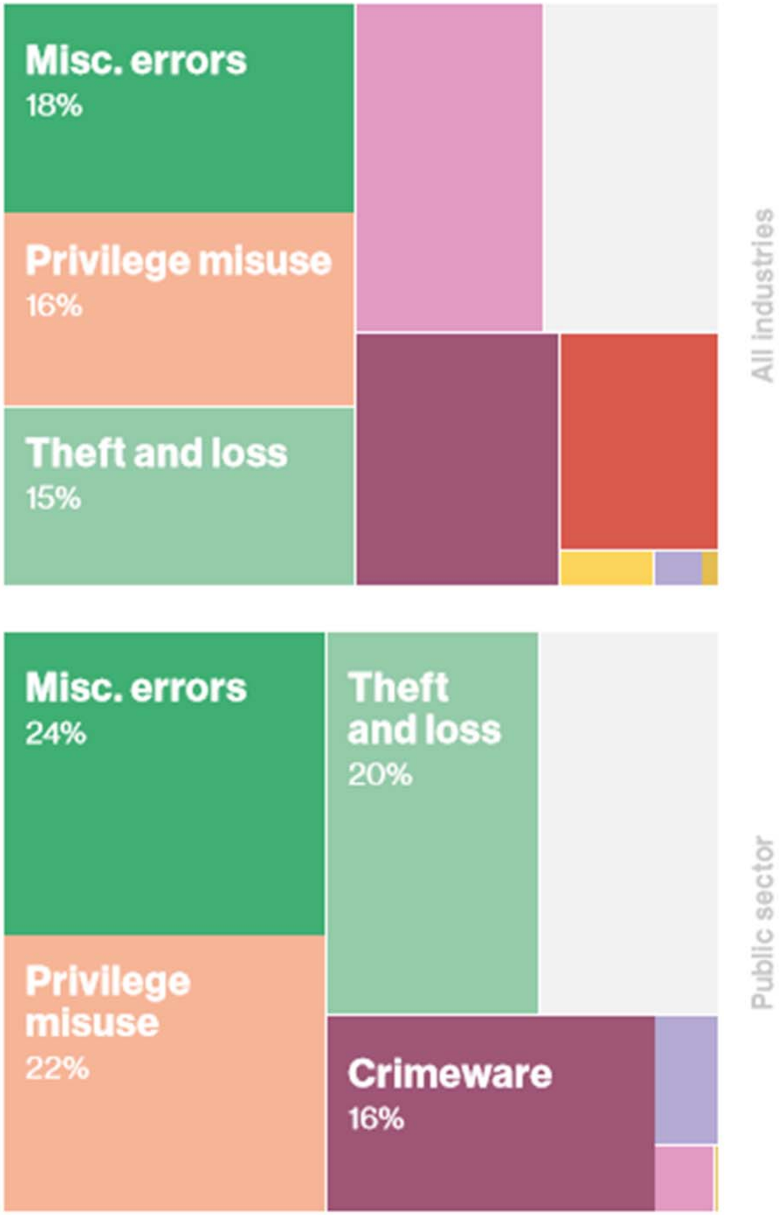
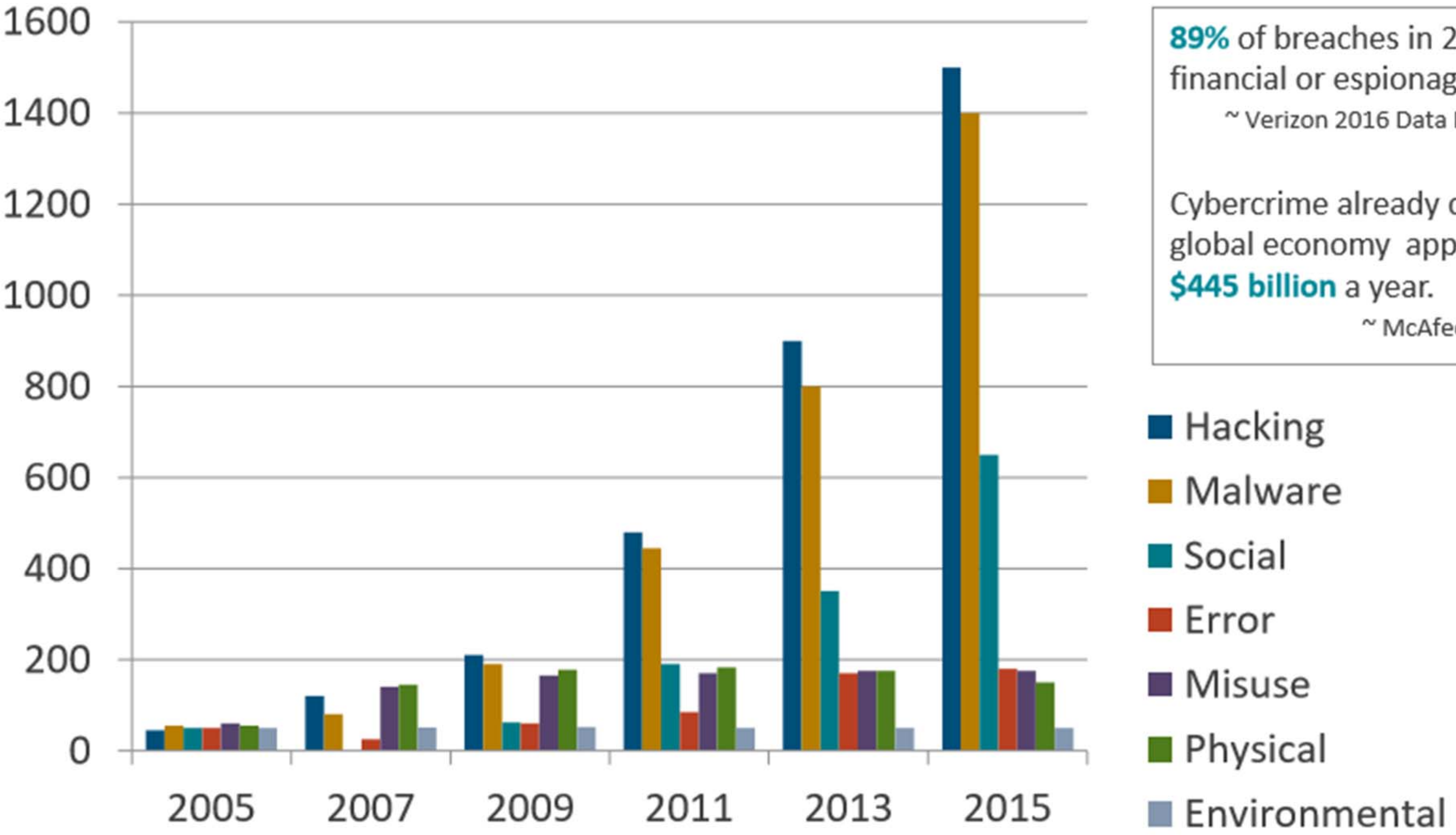


Figure 1: Incidents by pattern: All industries versus public sector

Data Breaches and Cyber Attacks are Increasing in Costs and Frequency.



89% of breaches in 2015 had a financial or espionage motive.

~ Verizon 2016 Data Breach Report

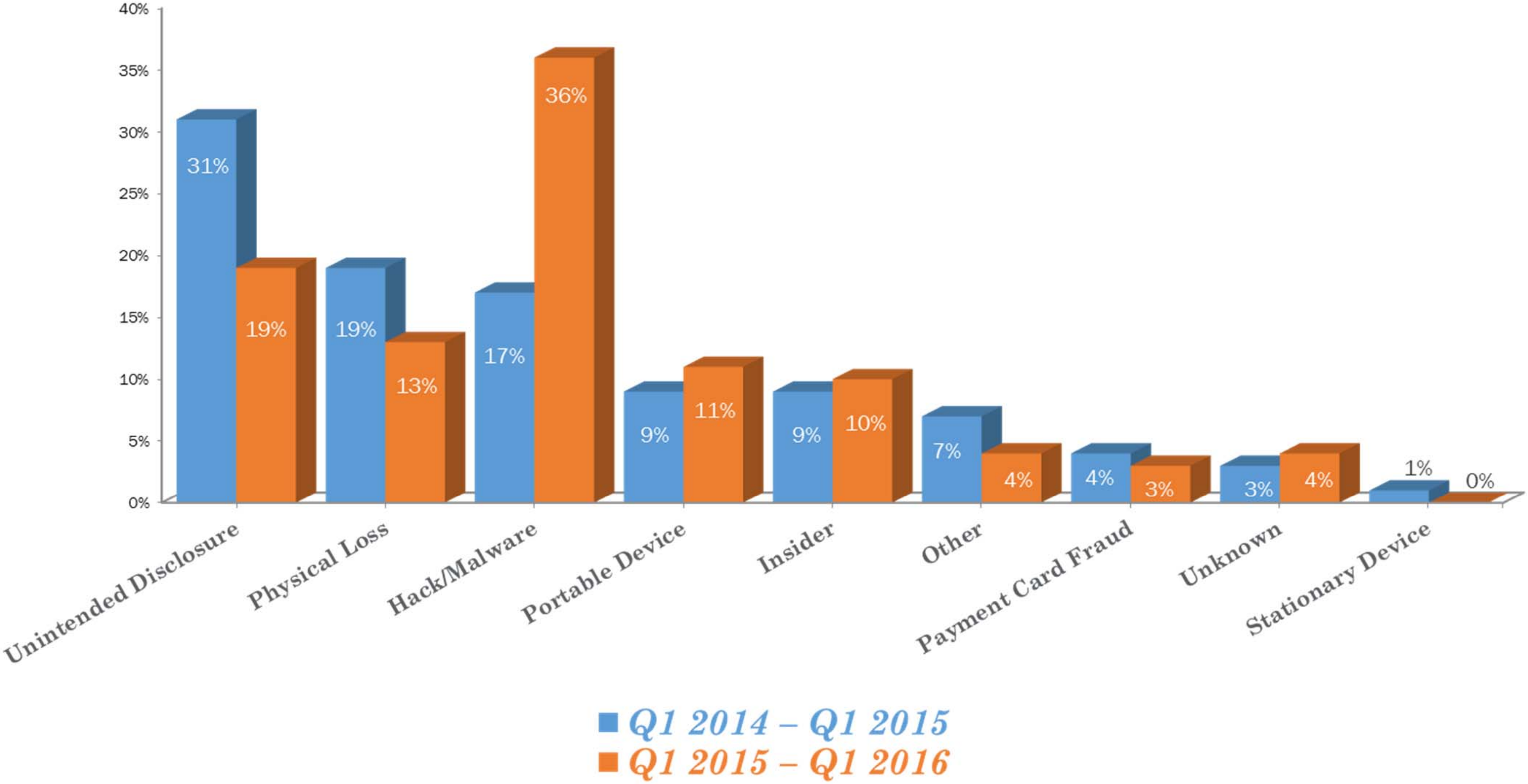
Cybercrime already costs the global economy approximately **$445 billion** a year.

~ McAfee; CSIS (2014)

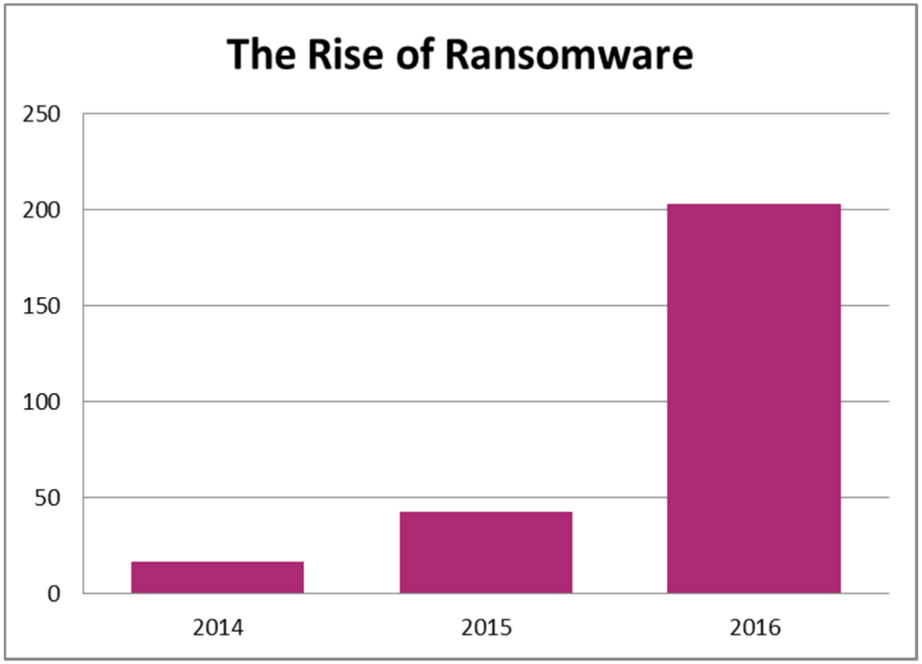
*Source: Verizon 2016 Data Breach Report

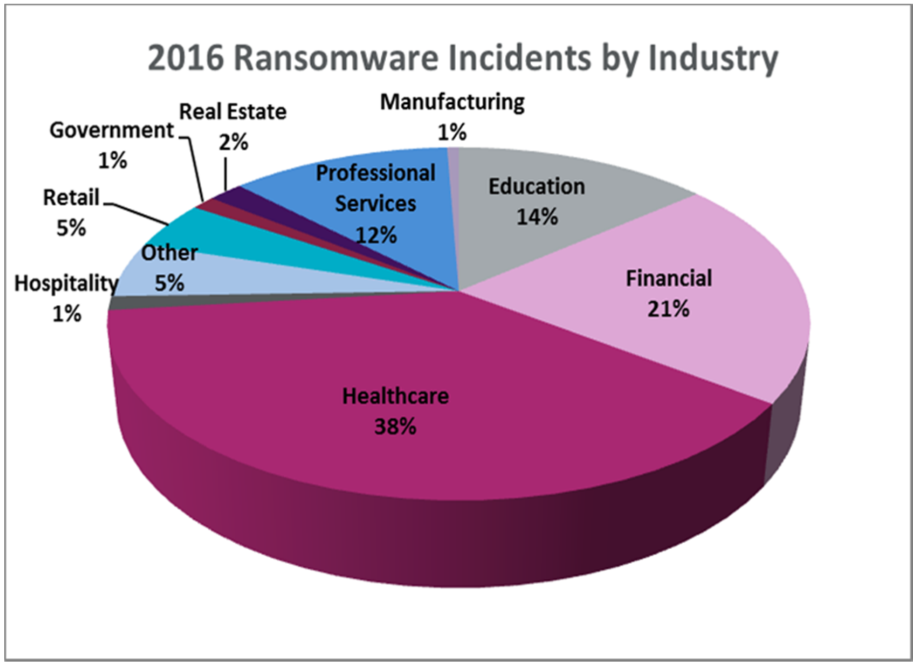
Beazley Breach Response: A Snapshot

Types of Data Breaches



2016 – The Year of Ransomware





Data from Beazley Breach Response Services

Hacking & Malware: *A Costly Trend*

- Cost **4 ½ times** more than "unintended disclosure" breaches
  - Forensics one of the most expensive elements

- ***Common sources***
  - Phishing to exploit credentials
  - Clicking on malicious links
  - Point of purchase infiltrations and skimming devices
  - Exploitation of network vulnerabilities
  - Exploitation of vendor vulnerabilities
  - Re-routing of direct deposit and payroll

A data breach isn’t always a disaster.

Mishandling it is.

Before the Breach

- Beazley's Building Blocks
- Incidence response planning
  - Beazley Offers Template Incident Response Plans
- Manage your relationships with third parties

Best Practices: Breach Preparation

- *7 measures that insureds can do right now:*
  - **Encrypt** your devices
  - **Automate** patch management
  - **Password** protect
  - **Be alert to phishing** – educating employees is key
  - **Double-check** mailing details
  - **Identify** risks, plan, practice and training
  - Make cyber security a **focus of your third-party contracts**

Penetration Testing (“Pen-Testing”)

- Beazley has a number of vetted, trusted, expert computer forensic services as partners, including those with focus on the public sector.
- Types of pen-testing
  - Social Engineering – phishing campaigns and physical tests
  - Network Services and Wireless
  - Web applications
  - Client-side

Develop an Incident Response Plan

- An incident response plan (IRP) is a written roadmap by which organizations intake, evaluate, and respond to a suspected breach of computer systems or theft, loss, or unauthorized disclosure of sensitive information.
- The IRP should be triggered by events that may affect data across the organization.
- Having an IRP is required by a number of laws, regulations, and industry standards.

The Incident Response Team

- Typically, organizations start the IRP drafting process by appointing their incident response team, i.e., the individuals who will actually perform the substantive tasks at hand. While no two organizations are alike, Beazley recommends that its Insureds designate a primary and secondary representative from the following stakeholders:
  - Legal
  - IT/Information Security
  - Risk Management
  - Communications
  - HR
  - Physical Security
  - Business Continuity
  - Privacy Office (HIPAA)

Communicate Thoughtfully

- There is significant danger in communicating prematurely.
- Not every incident is a “breach,” which is a legal term.
- Not all personal data is protected under state and federal law.
- The IRP is not intended to take the place of actual legal analysis or public relations guidance, but it should outline what the organization needs to accomplish once it appears that a data breach may require communication with affected individuals, regulators, or the media.
- Without set guidance in the IRP, organizations struggle on what to say, how to say it, and when to say it. Quite often, even well-meaning intentions not filtered through the IRP result in unnecessary damage to the organization.
- “The Holding Statement.”

Before the Breach – Your 3rd Party Relationships

- Develop your own checklist of contractual requirements based on your privacy and security requirements

- Develop standard contractual clauses that address these privacy requirements and fallback positions

- Develop a checklist to evaluate third-party agreements and to educate third parties about gaps or shortfalls in their ability to meet your requirements

Helping the insured see when this claim . . .

. . . really looks like this.

The Classic APIP Coverages

- Information Security and Privacy Liability (A)
- Privacy Notification Costs (B)
- Regulatory Defense and Penalties (C)
- Website Media Content Liability (Occurrence Based) (D)
- Cyber Extortion Loss (E)
- Data Protection Loss (F) and Business Interruption Loss (G)

Three Components of Cyber Extortion Coverage

- Three basic components of the **Cyber Extortion Loss** coverage:
  - The **Extortion Payment** itself (with Underwriters' prior written consent).
  - Loss of the **Extortion Payment** in transit.
  - Fees and expenses of a security consultant (with Underwriters' prior written consent).
- **Extortion Payment** and security consultant's fees and expenses must be incurred solely to prevent or terminate an **Extortion Threat**.

Ransomware: Cyber Extortion Coverage Considerations

- Cyber Extortion coverage may be triggered by ransomware.
  - Reimbursement for ransom payment itself
  - Reimbursement for costs and expenses to terminate extortion threat
  - *Note that under Beazley's Cyber Extortion coverage, these payment require prior written consent/approval.
- Beazley cannot advise on whether to pay ransom.
  - Most who pay the ransom get their data back, but no guarantee.
  - Law enforcement generally advises not to pay the ransom.
- Beazley cannot advise on where or how to obtain bitcoin.
  - IT generalist (or Google) may be able to help you.
  - For purposes of preparedness, may want to consider establishing a plan for obtaining bitcoin, establishing a bitcoin trading account, and/or buying and holding bitcoin.

Ransomware: Breach Response Considerations

- Most ransomware infections **do not** result in breach notification obligations. That may not be the case in the future.
  - Ransomware that exfiltrates data may become more common.
  - In the future, laws might require notification even if no exfiltration.
- Privacy Breach Response Services – Has any data been exfiltrated from my computer system?
  - Computer forensics to investigate whether any breach has occurred and, if so, scope and extent of information exfiltrated
  - Privacy counsel to advise on breach notification obligations, draft letter
    - 48 state laws
    - HIPAA
    - Different "boxes to check" depending on state, number of individuals affected, and type of information.
  - Notification vendor
  - Call center
  - Credit monitoring
  - Crisis management

Ransomware: Business Interruption Considerations

- A ransomware infection can be limited to a single computer or span an entire computer network.
- While your computers are completely inaccessible…
  - Can you still service customers/students?
  - Can you still bill customers/ students?
  - Can you process payments from customers/ students?
  - Can you record your employees' time?
  - Can you run your employees' payroll?
  - How much extra time will your employees need to work to make up for not having access to their computers?
  - *Note the cascading effect
- Decryption is not instantaneous. Potentially millions of files can be impacted, taking days or weeks to fully decrypt.
- Restoring from backup is not instantaneous, and depending on how periodical your backups are, may result in days or weeks of lost data.

Ransomware: Other Coverage Considerations

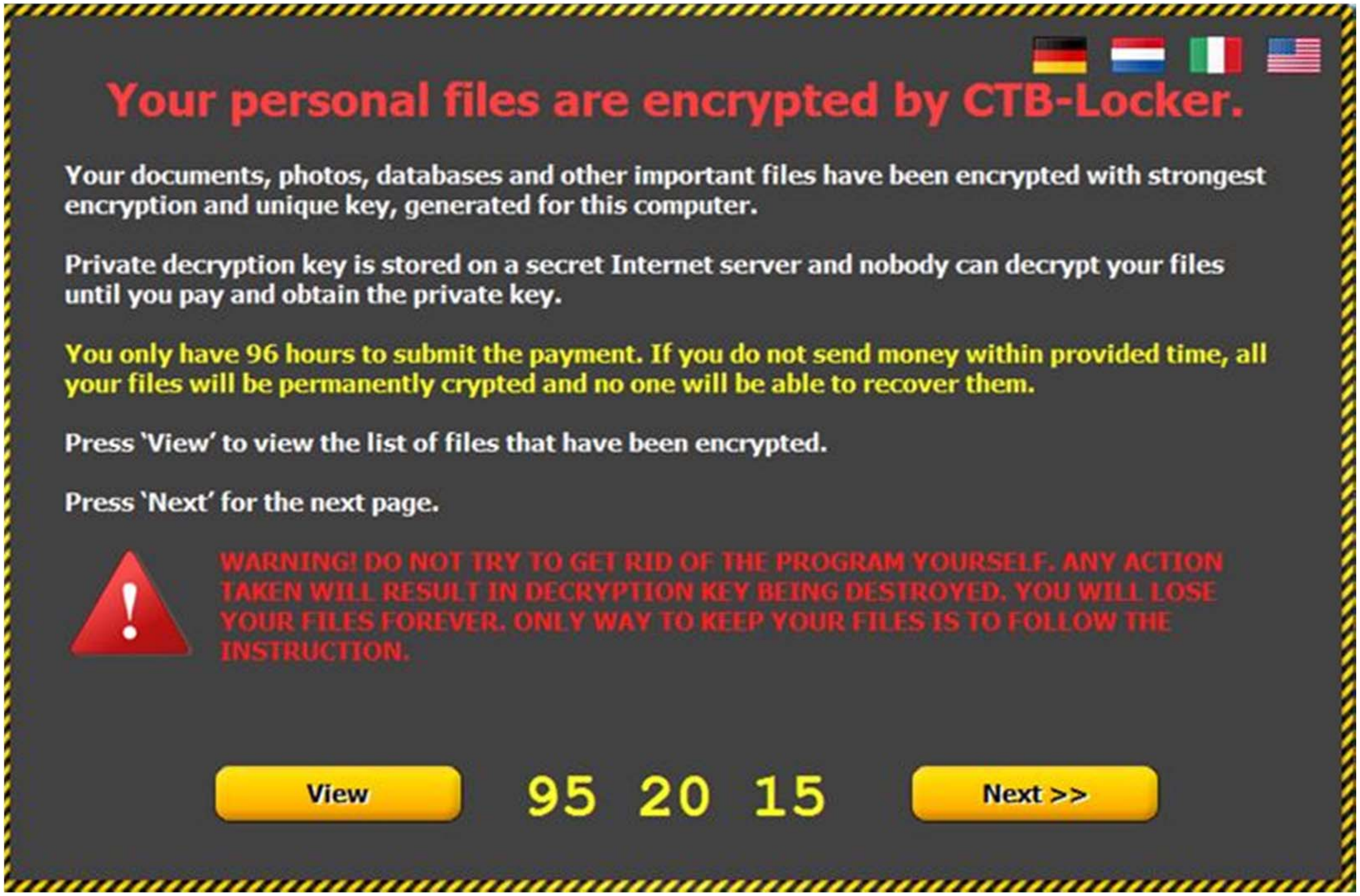
- Since ransomware is so destructive in nature, coverage may be triggered across several different policies.
  - Cyber policy
  - Property policy
  - Crime policy
  - Malpractice/professional liability policy
- Coordinate with your insurance broker to discuss what coverage would need in the event of a ransomware attack.
- Broker may be able to help you notify your insurers and coordinate your reimbursements to maximize coverage under your policies.

Key Points

- **Extortion Payment** “means cash, marketable goods or services demanded to prevent or terminate an **Extortion Threat**.” At present, we consider Bitcoin a “marketable good.”
- Coverage for **Cyber Extortion Loss** is subject to a retention and sublimit of liability.
- Coverage for **Cyber Extortion Loss** is excluded when a threat to physically harm or kidnap any person is involved; and where there is a threat to harm, take, or transfer property other than a **Data Asset**.
- Cyber extortion may be just the beginning. Potential data breach, business interruption, and data protection coverage issues.

Ransomware: Some Coverage Considerations

- Since ransomware is so destructive in nature, coverage may be triggered across several different policies.
  - Cyber policy
  - Property policy
  - Crime policy
  - Malpractice/professional liability policy
- Coordinate with your insurance broker to discuss what coverage would need in the event of a ransomware attack.
- Broker may be able to help you notify your insurers and coordinate your reimbursements to maximize coverage under your policies.



Your personal files are encrypted by CTB-Locker.

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer.

Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.

You only have 96 hours to submit the payment. If you do not send money within provided time, all your files will be permanently crypted and no one will be able to recover them.

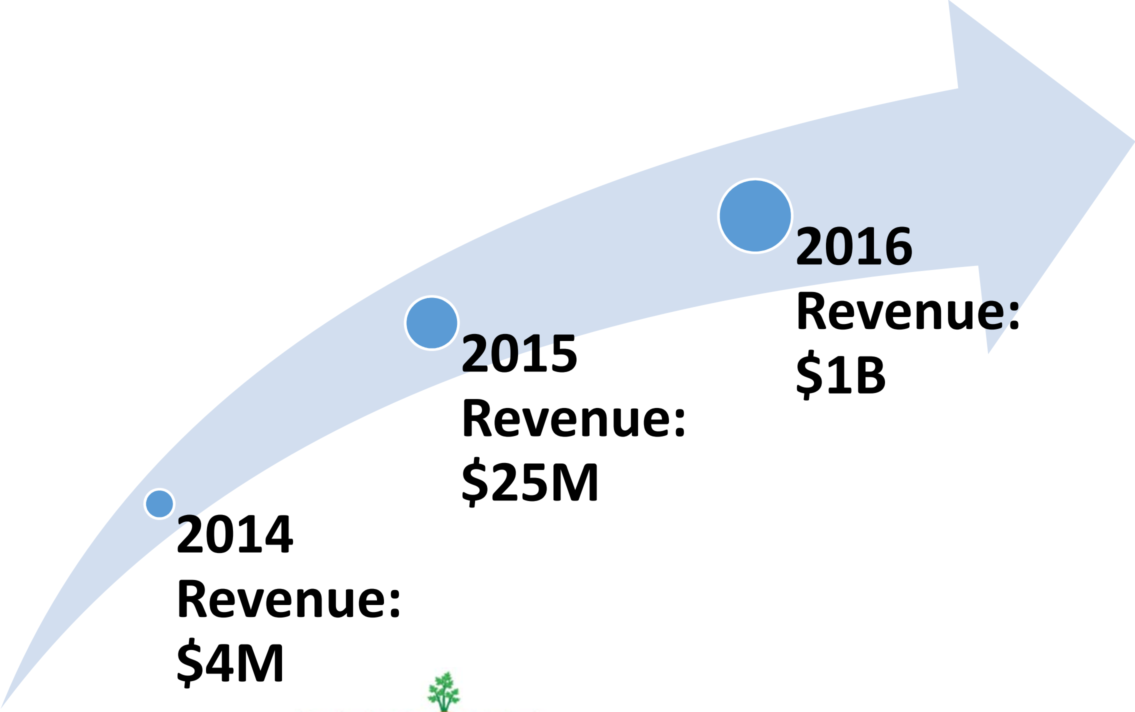
Press 'View' to view the list of files that have been encrypted.

Press 'Next' for the next page.

WARNING! DO NOT TRY TO GET RID OF THE PROGRAM YOURSELF. ANY ACTION TAKEN WILL RESULT IN DECRYPTION KEY BEING DESTROYED. YOU WILL LOSE YOUR FILES FOREVER. ONLY WAY TO KEEP YOUR FILES IS TO FOLLOW THE INSTRUCTION.

Ransomware on the Rise

- On April 29, 2016, the FBI issued a warning that ransomware attacks were on the rise, and there are few indications (other than awareness/prevention) that 2017 will be much different.



2014 Revenue: $4M

2015 Revenue: $25M

2016 Revenue: $1B

Common Types of Extortion Threats

- Most common types of **Extortion Threat**s:
  - Denial of service attacks (*i.e.*, flooding the insured's computer systems with so many bogus data requests that the computer systems cannot respond to legitimate data requests).
  - Crypto-ransomware (*i.e.*, CryptoWall, CryptoLocker, Locky; where insured's data becomes encrypted and a ransom is demanded in order to obtain decryption key).
  - Theft or misuse of data through external access (*i.e.*, threatening to cause a data breach).
- The term **Extortion Threat** is defined more specifically in the endorsement. See the endorsement for details.

Cyber Extortion

- Cyber Extortion can be conducted by:
  - Ransomware
  - Distributed denial of service (DDoS) attacks

- Cybercriminals use the ransomware to encrypt target data so that the criminal can extort money from the target institution or person, or use DDoS to shut down the website and deny service from the institution/person until ransom is fulfilled.

- Notable Healthcare Ransomware Incident:
  - Hollywood Presbyterian Medical Center

- CryptoWall Ransomware Gang nets almost $330,000 in bitcoin from ransomware infections on ~670 victims – *Imperva Hacker Intelligence Initiative: The Secret Behind CryptoWall's Success* (2016)

- Ransomware attacks increased by 58% in the second quarter of 2015 – *McAfee Labs Threats Report* (August 2015)

Cyber Extortion in the News

- Ransomware. On February 17, Hollywood Presbyterian Hospital paid the equivalent of $17,000 in Bitcoin to obtain keys to decrypt files that had been encrypted by ransomware.
- DDoS Attacks. In 2015, groups calling themselves “The Armada Collective” and “DD4BC” threatened hundreds companies with denial of service attacks if they did not pay a ransom demand in Bitcoin.
- The Future. Cyber extortion is a booming and rapidly evolving criminal industry.
  - New ransomware variants are popping up all the time – some threatening to leak user data.
  - Hackers are holding data for ransom.
  - Criminals are targeting a range of industries and business sizes, including small and medium-sized municipalities and government agencies. If you do business through your website, you are a potential target.

Preventing a Ransomware Infection

- Update anti-virus
- Train employees on phishing
- Use phishing campaigns
- Block problematic file types at e-mail gateway
- Disable dangerous plug-ins
- Harden web servers

- Evaluate application whitelisting
- Enable automated patching
- Segment network
- Enable strong identity and access management (IAM), implement “least privilege”
- Invest in intrusion detection systems (IDS)
- Implement and test data backup and recovery plan

Responding to a Ransomware Incident

- Disconnect, but don't unplug, infected machines
- Evaluate extent
- Identify ransomware variant
- Identify connections to other resources
- Clean infected machines
- Restore from reliable backup

Hypothetical Claim Timeline

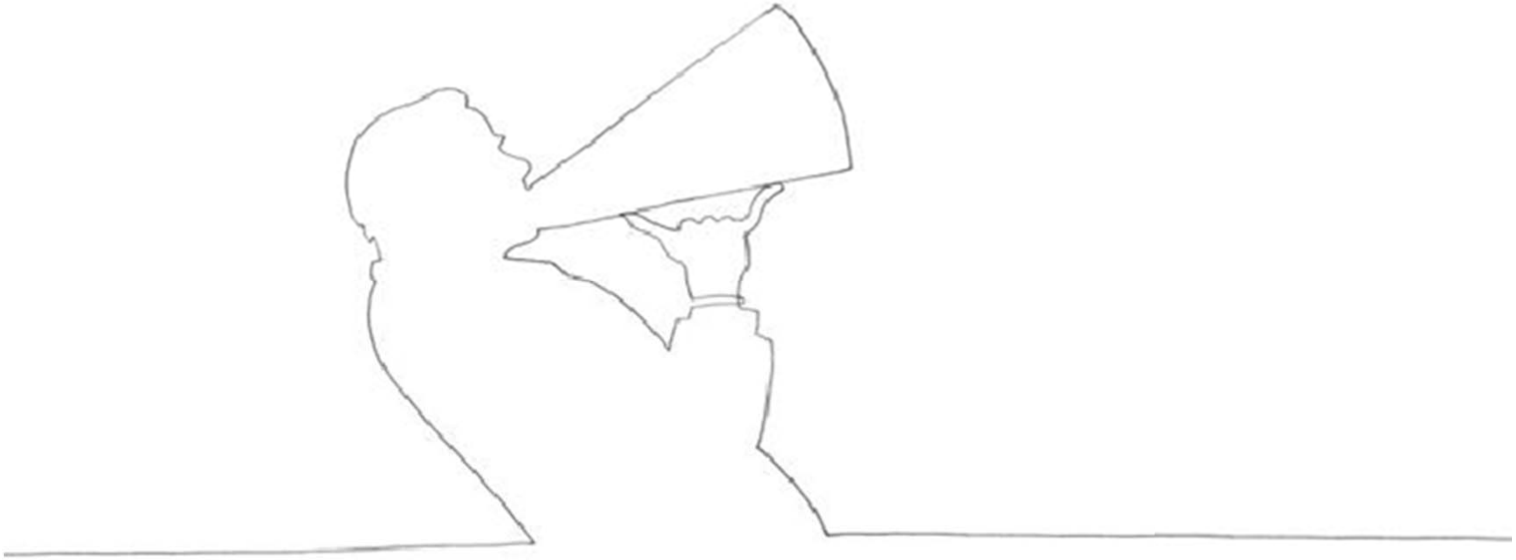
- Insured receives an extortion threat from a third party.
- Insured notifies Beazley of an Extortion Threat.
- Insured requests Beazley's consent to payment of Extortion Payment and/or retention of security consultant.
- If payment is demanded in Bitcoins, insured purchases Bitcoins with U.S. dollars using Bitcoin exchange site. (Beazley will not advise on or facilitate this transaction.)
- Insured pays Extortion Payment and/or security consultant. If payment is in Bitcoins, insured will provide details of transaction so Beazley can confirm that payment was made.
- Insured seeks reimbursement for Extortion Payment and/or security consultant's fees.
- Beazley reimburses insured for Extortion Payment and/or security consultant's fees. Bitcoins will be reimbursed in U.S. Dollars.

This isn’t the time to learn on the job.

The smallest breach can become a big problem
if not handled correctly.

An Incident Happens: *What Next?*

Notice Beazley EARLY AND OFTEN



Beazley's Approach

Collaborative discussions with forensics to drive conclusions

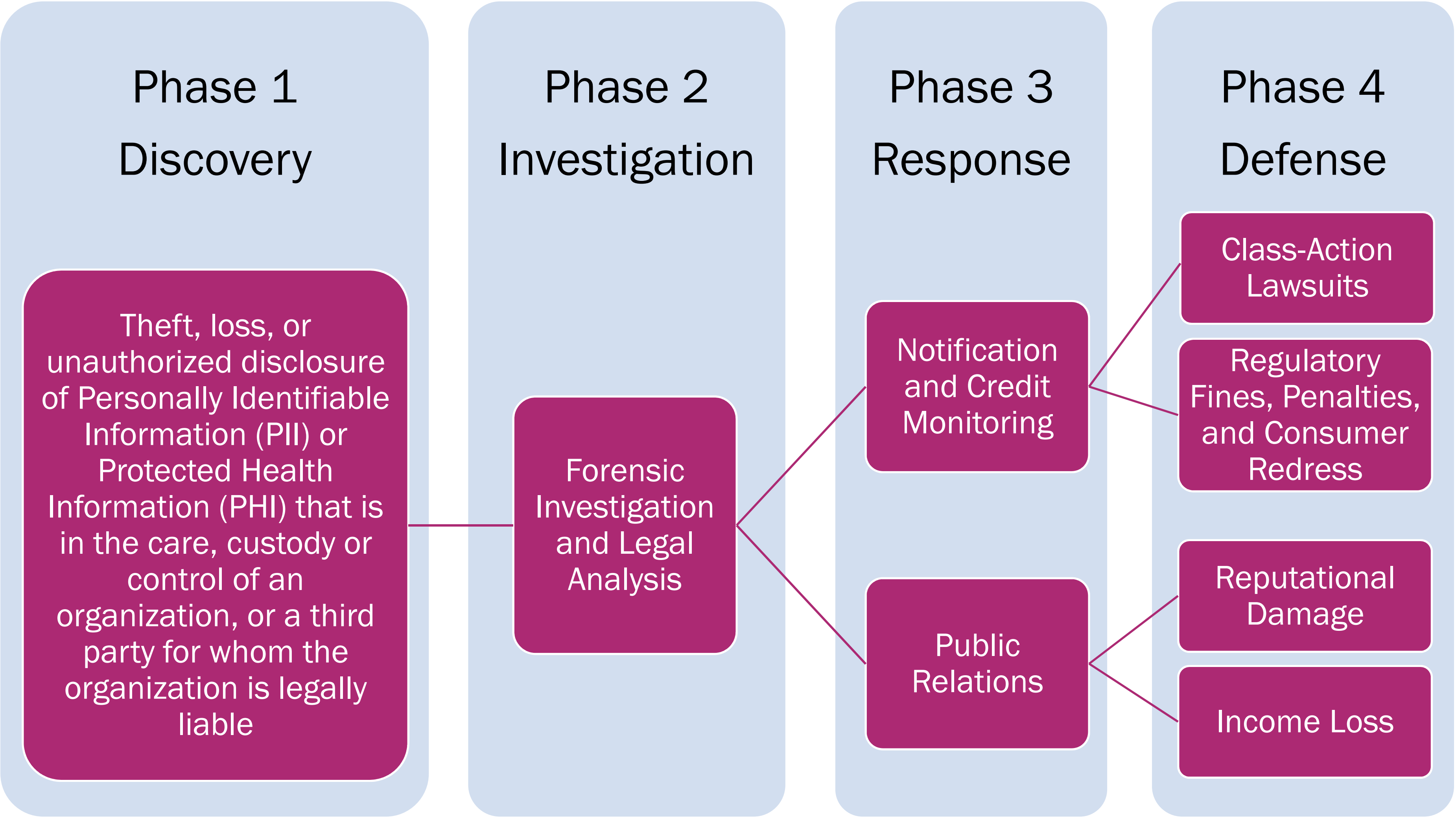
Assisting Insureds in understanding fully the legal landscape in complex situations

Enabling identity/credit monitoring for individuals whose data has been breached

Facilitating strategic dialogue with Insureds and counsel about media communications and escalation issues

Driving notification through the printing and mailing process even when tight statutory deadlines provide no more than a few days to comply

The Lifecycle of a Breach



Phase 1

Discovery

Theft, loss, or unauthorized disclosure of Personally Identifiable Information (PII) or Protected Health Information (PHI) that is in the care, custody or control of an organization, or a third party for whom the organization is legally liable

Phase 2

Investigation

Forensic Investigation and Legal Analysis

Phase 3

Response

Notification and Credit Monitoring

Public Relations

Phase 4

Defense

Class-Action Lawsuits

Regulatory Fines, Penalties, and Consumer Redress

Reputational Damage

Income Loss

A Typical Breach Case Study

- State Community College: A USB drive and a personal handheld device were stolen from an employee's car when he took information home to do after-hours work.
  - The names and Social Security numbers of 9,747 current or former students were on the handheld device, along with 1,194 current or former employees.
  - Potential need for forensics, privacy counsel, notification and call center vendors.
- Breakdown potential costs depends on factual details, but from our experience: tens of thousands for forensics, ten thousand plus for legal, about a dollar per individual for notification, thousands for call center and tens of thousands for credit monitoring.

Lessons Learned

“We’ve already had your first breach for you.”

- **Focus on solving the customer’s problems**, not just selling risk transfer
- **Hand-picked vendors**, because expertise makes a big difference for claim outcome, but most companies don’t have the in-house expertise to respond to a breach

- **Encourage clients** to notice even the smallest breaches, since little breaches can be big problems if they aren’t handled well
- **One e-mail or one phone call** to access experienced claims managers, because many companies want help with the dirty work

Beazley's Cyber Experience

- We have seen thousands of breaches and can provide insureds insight on successful breach response:
  - Insureds see a **large drop in breach costs** after their second breach.
  - Entities that provide **timely and accurate notification** see less reputational damage and attract less regulatory scrutiny.
  - Good breach response requires **experience and specialized expertise**, so most companies struggle when handling their data breaches independently.
  - **Mitigating reputational damage** by avoiding unnecessary breach notifications is critical.

We always encourage insureds to notify
Beazley of incidents ***as soon as possible***

Official Note

The descriptions contained in this presentation are for preliminary informational purposes only. The exact coverage afforded by the products described herein is subject to and governed by the terms and conditions of each policy issued. The publication and delivery of the information contained herein is not intended as a solicitation for the purchase of insurance on any US risk.