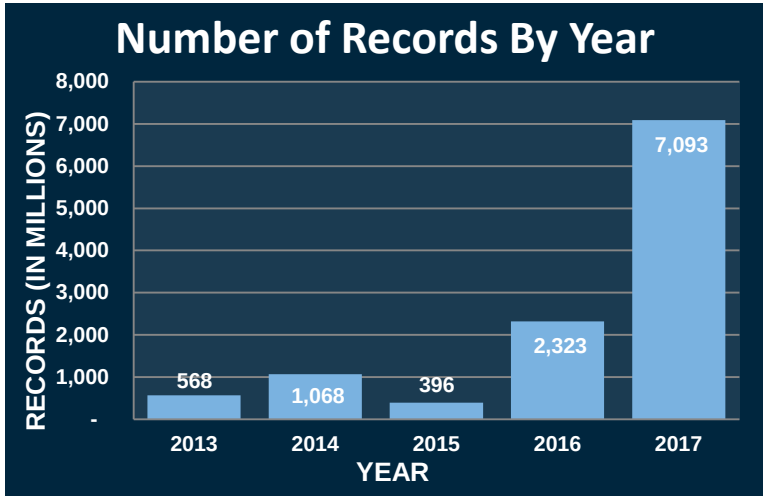
DMI Cyber Liability Coverage

DMI Risk Management Forum – Annual Meeting

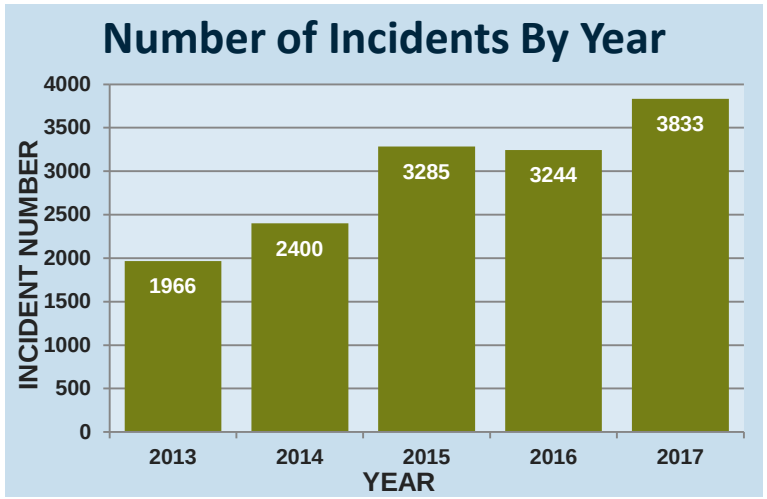
April 11, 2019

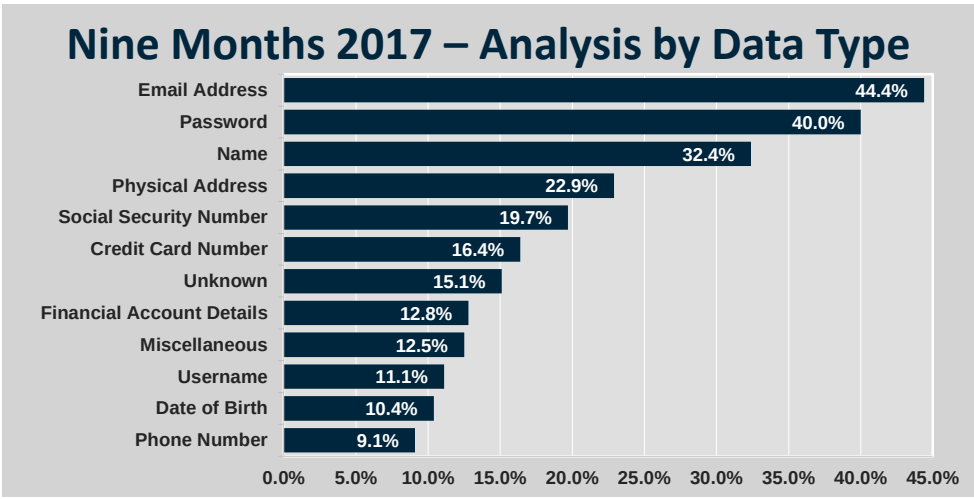
DISTRICTS MUTUAL INSURANCE & RISK MANAGEMENT SERVICES | *Collaborators in Risk Management* |

Claims Trends: Cyber Liability



- **2017 was a record year for cyberattacks** – Number of breaches increased by 18.2% and number of exposed records increased by 305% (compared with the same period in 2016)
- Cyber events ran the gamut from typical unauthorized disclosure of personal identifiable information to high frequency business email compromises (social engineering) and ransomware attacks
- **Ransomware** – Cyberattacks like NotPetya (which turned out to be destructive malware disguised as ransomware) and WannaCry spread widespread concern over ransomware throughout 2017 first registered in May 2017, after the WannaCry cyberattack.
- **Network Business Interruption** – These losses (exceeding $300M in net income in 2017) have highlighted the extent of damage that may occur





DISTRICTS MUTUAL INSURANCE & RISK MANAGEMENT SERVICES | *Collaborators in Risk Management* |

April 2019 - Risk Mitigation Forum

Cyber Incident Trends

Top 5 Causes

1

37%

Phishing

After phishing occurred, more than 30% of the time a takeover of an Office 365 account occurred

2

30%

Network Intrusion

3

12%

Inadvertent Disclosure

4

10%

Stolen/Lost Device or Records

5

4%

System Misconfiguration

Incident Response Lifecycle

What to Expect & Possible Impact

66
Days
Occurrence to Discovery

8
Days
Discovery to Containment

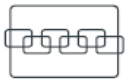
28
Days
Time to Complete Forensic Investigation

56
Days
Discovery to Notification

After gaining access to a device or account, the most common next steps were:

34%
Accessing an Office 365 Account

30%
Roaming Network to Find Available Data



12%
Dropping Ransomware

8%
Obtaining a Wire Transfer to the Attacker's Account

DISTRICTS MUTUAL INSURANCE & RISK MANAGEMENT SERVICES | Collaborators in Risk Management |

Privacy Regulatory Environment

All 50 States

- A vast majority of US states have consumer protection statutes that address the safeguarding on consumer data
- CCPA and Evolution of Other State Laws

Personally Identifiable Information (PII)

- Protected / “Sensitive” information is defined differently in each state but the definition is expanding

Data Owner vs. Data Aggregator

- Transfer of data to a third party does not constitute a shift in responsibility

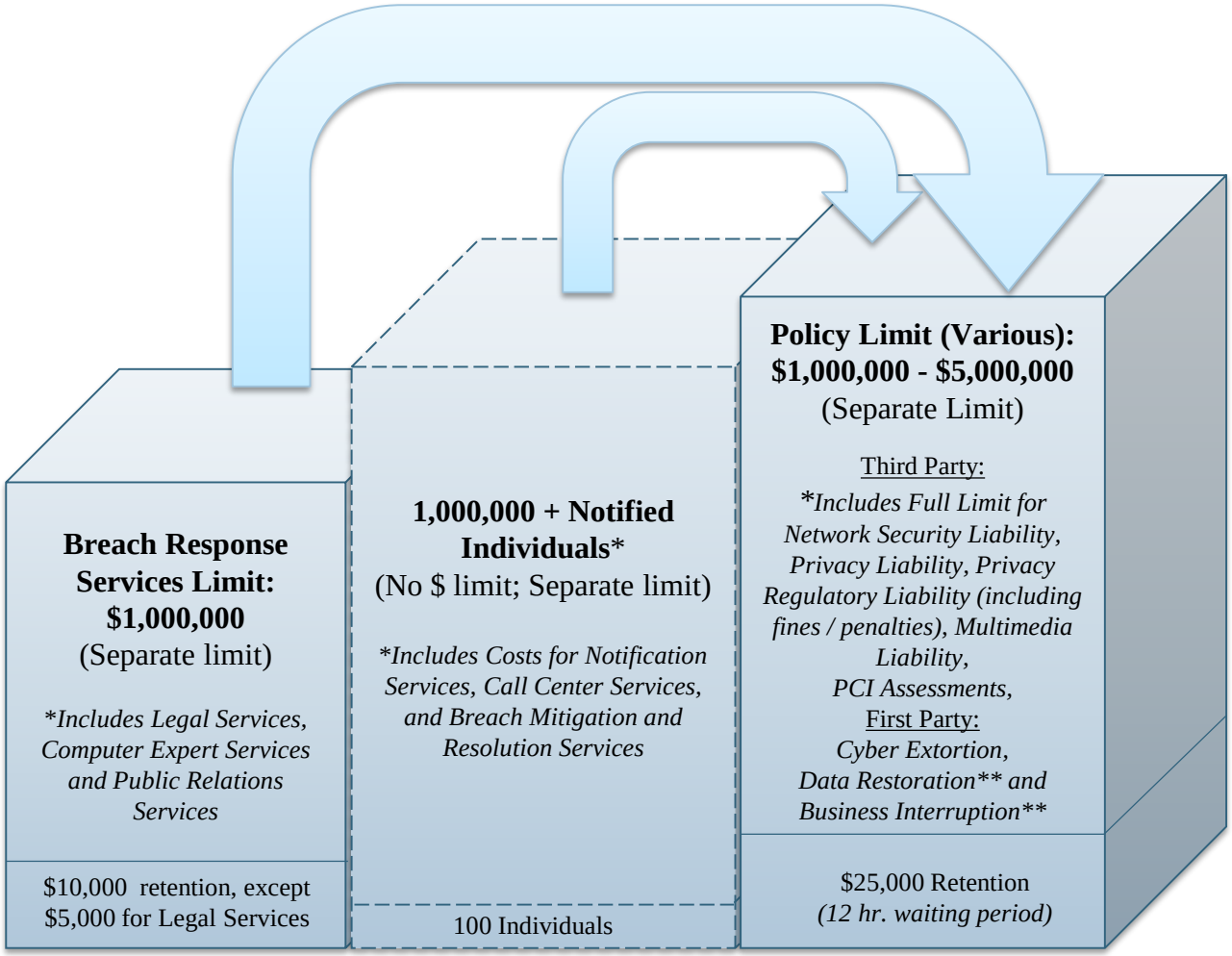
Which Law Applies?

- Affected Individual Residency Governs

Regulatory Testing Grounds

- California, Illinois, Massachusetts, New York

Cyber Liability Coverage



DISTRICTS MUTUAL INSURANCE & RISK MANAGEMENT SERVICES | Collaborators in Risk Management |

3rd Party Liability Coverages

Network Security

- Failures in computer security
- Transmission of malicious software / viruses
- DDoS Attacks

Privacy Liability

- Unauthorized Access or Use
- Failure to protect sensitive information

Media Liability

- Online Content / Multimedia
- Libel / Slander / Defamation
- Copyright infringement

Regulatory Defense, Fines & Penalties

- Regulatory Proceedings & Investigations
- Fines and Penalties where insurable by law

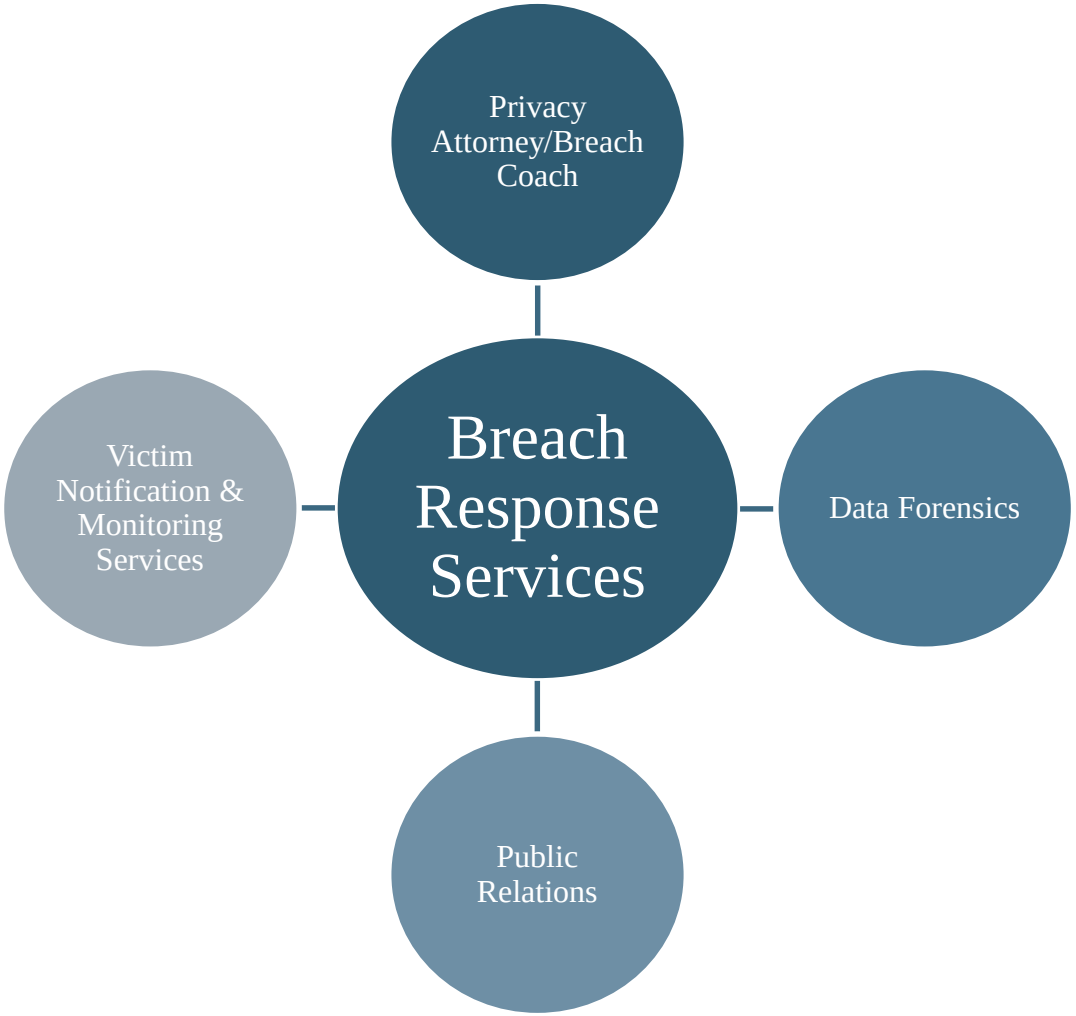
PCI Defense, Fines & Penalties

- Defense Costs
- Fraud Assessments

First Party Coverage

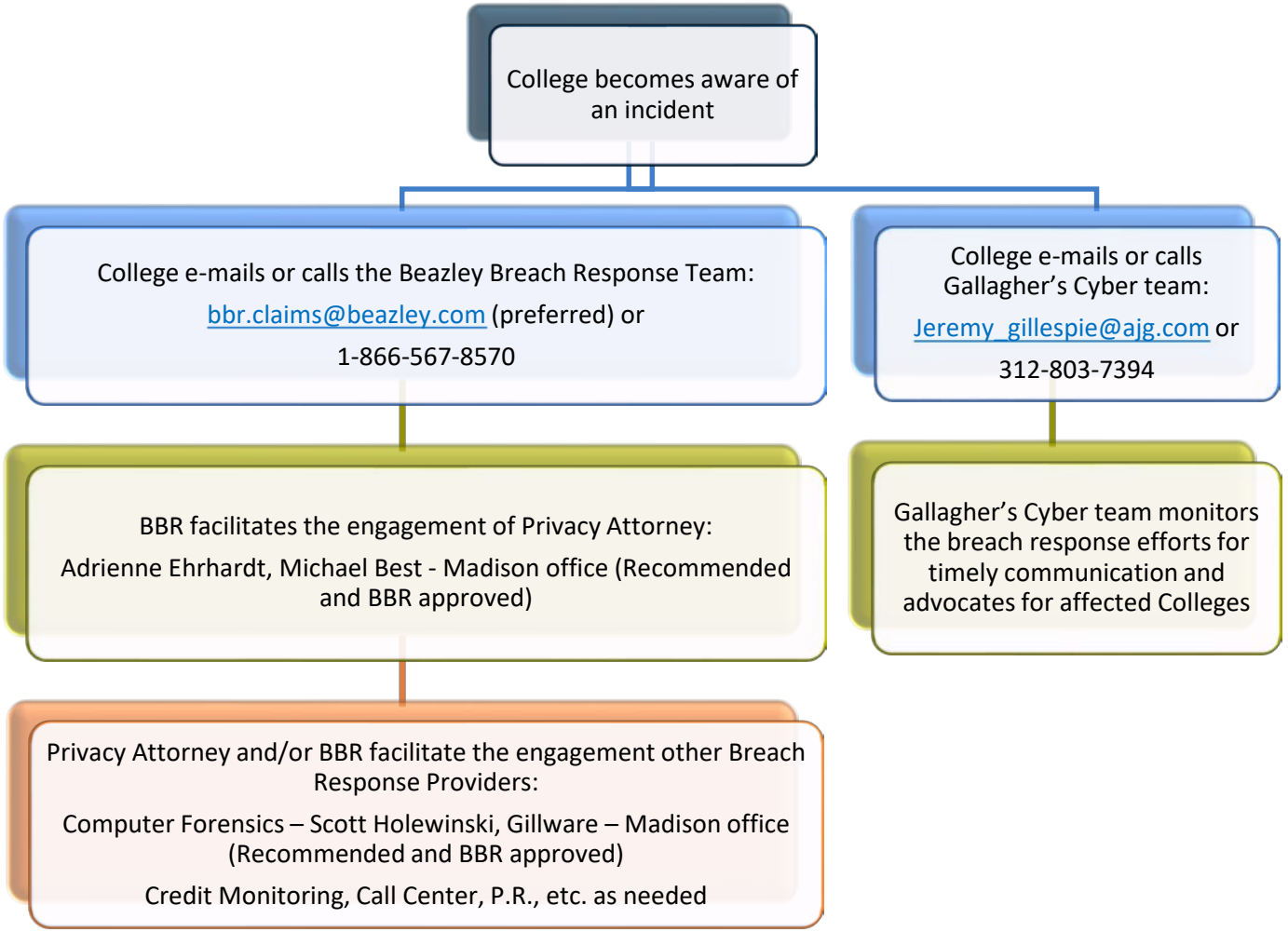
- Cyber Extortion
- Digital Asset Restoration
- Business Interruption & Extra Expense
- Dependent Business Interruption & Extra Expense
- Cyber Crime
- Breach Response Services

Breach Response Services



DISTRICTS MUTUAL INSURANCE & RISK MANAGEMENT SERVICES | Collaborators in Risk Management |

Engaging Breach Response Providers



Cyber Risk Analysis

It is truly difficult to estimate the total cost of a breach. At its very core, the cost of a breach is a function of unique individual records impacted. The results of this benchmark study are our best efforts to predict costs of a breach based on various models and assumptions.

We evaluate cyber risk based on the NetDiligence Data Breach Cost Calculator, which relies on record count (unique individual records categorized by Gallagher as either personally identifiable, personal health or payment card information) and our Gallagher proprietary cyber risk model. This model relies on employee count to predict cyber loss rather than number of records, because employee data is readily available and is highly correlated to enterprise seats. Therefore, our model provides a distinct alternative to the NetDiligence Calculator.

Note:

- *The NetDiligence calculator may underestimate the potential exposure in 3 costs categories:*
  - *First party costs (excluding Data Breaches): Business Income Loss, Data Recovery, and Cyber Extortion are not represented costs of a breach in the NetDiligence calculator*
  - *Litigation expenses (defense and settlement) is generally a function of organizational size and we believe that the actual losses may be substantially higher than indicated by the NetDiligence Calculator.*
  - *The PCI assessment expenses are estimated at the low end of the range that we have seen levied against companies. This range spans from $15 per card breached on the low end to $30 per card on the high end.*

- *The Gallagher Proprietary Model takes a holistic approach to costs of a breach based on several quantifiable data analytics including:*
  - *The average cost of a breach provided by the Ponemon Institute: Cost of a Data Breach Study 2017*
  - *Litigation trends, losses, and legal expenses impacting cyber insurance*
  - *Various datasets indicating developing risk factors and risk trends*

Cyber Risk Analysis

Cyber Limit & Loss Analysis – NetDiligence Data Breach Calculator

NetDiligence requires an assumption of the number of affected individuals to generate the estimated data breach cost. Here are their results based on several hypothetical breach scenarios:

- ❑100K PCI records = $2.79M
- ❑250K PCI records = $5.76M
- ❑250K PII records = $3.22M

This calculator may underestimate the total potential exposure. For example, the per record projection to address all the aspects of a breach seems low based on other industry reports and our experience. Specifically, Computer Forensics, Breach Coach Legal Advice, Notification and Credit / ID Monitoring expenses are lower than other industry report projections and claims that we have monitored for our clients.

Additionally, it does not factor in the exposure to network security and media liability, cyber extortion, data restoration and network interruption. These elements are essential to determine an organization's true cyber risk.

Cyber Risk Analysis

Cyber Limit & Loss Analysis – NetDiligence Data Breach Calculator

HOW MANY PII RECORDS WERE EXPOSED?	250000
HOW MANY UNIQUE PEOPLE WERE AFFECTED?	250000

Data Breach Costs — PRINT | CALCULATE

INCIDENT INVESTIGATION	
FORENSICS INVESTIGATION	$270,000
SECURITY REMEDIATION	$350,000
BREACH COACH® LEGAL GUIDANCE	$108,000
SUBTOTAL	$728,000

CUSTOMER NOTIFICATION / CRISIS MANAGEMENT	
CUSTOMER NOTIFICATION	$250,000
CALL CENTER	$18,750
CREDIT/ID MONITORING	$812,500
PUBLIC RELATIONS	$75,000
SUBTOTAL	$1,156,250

CLASS ACTION LAWSUIT	
DEFENSE	$160,000
eDISCOVERY	$350,000
SETTLEMENT/DAMAGES	$378,750
SUBTOTAL	$888,750

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

REGULATORY FINES & PENALTIES	
STATE AG	$166,625
HHS	$0
OTHER (FTC, SEC, ETC.)	$279,688
SUBTOTAL	$446,313

TOTAL COST	$3,219,313
PER RECORD COST	$13

DISTRICTS MUTUAL INSURANCE & RISK MANAGEMENT SERVICES | *Collaborators in Risk Management* |

Cyber Risk Analysis

Cyber Limit & Loss Analysis – Gallagher Model

Need for the Model – Cyber exposures are new and quickly evolving. With the lack of claims history and common purchasing habits of companies, our clients begged us for assistance in evaluating their specific risk.

Expert for the Job: Phil Norton, Ph.D. in Statistics – Dr. Norton is a veteran insurance broker and has developed numerous risk evaluation models for management liability exposures that are time-tested and industry-recognized.

Basis for the Model – Source, quantity and quality of data are key for the statistical model. With limited claims information, AJG supplements what we do have with Ponemon Institute and The Open Security Foundation data – two organizations that have studied the impact of data breaches for over a decade.

Relevance of the Model – The model looks at industry (24 different listings) and size of an organization, to provide a custom-fit exposure projection.

Cyber Risk Analysis

Cyber Limit & Loss Analysis – Gallagher Cyber Model

Using an average of the DMI Technical Colleges' risk factors as summarized best by size and industry, our modeling process projects the average, 75th and 90th percentile for frequency and severity for your company. This information is incorporated into an overall risk calculation as shown below.

Our cyber model estimates that your exposure to cyber risk as follows:

$5,000,000 – Average

$8,000,000 – Mid-Range / 75%-ile

$12,000,000 – High End / 90%-ile

Cyber Risk Management

1. **PCI-DSS / Regulatory Compliance**
    - Payment Card Industry Data Security Standards
    - Federal Regulations
    - State Laws
2. **Cyber Security Readiness**
    - Network Assessments
    - Remediation of Vulnerabilities
3. **Treatment of Private / Confidential Information**
    - Policies, Access Controls, Security Measures
    - Quantification of Record Count / Transactions
    - Encryption – At Rest, In Transit, On Portable Media Devices
4. **Breach Preparation**
    - Incident Response Plan
    - Business Continuity Plan / Back-up Procedures
5. **Vendor Management**
    - Contract Review
    - Professional E&O / Cyber Insurance and Indemnification Agreement

Phishing Best Practices

Take Action: Stop Phishing

Phishing remains the most common method used by all attackers – from the most to the least sophisticated – to gain access to a target. And as more assets are moved to the cloud, where they can be accessed with just a username and password, the importance of using a multi-pronged approach to address this risk is critical. The key elements of phishing prevention include:

- **Employee awareness and training.**
- **Enabling MFA (if you cannot do this everywhere immediately, start by prioritizing accounts with access to sensitive data).**
- **Disable or set alerts to identify suspicious activity, such as authentication from IP addresses in high-risk regions, mail forwarding, and legacy connection protocols.**
- **Information governance – pay attention to what data is in the cloud and how long it is kept there, especially email.**
- **Separate administrative accounts from user accounts, and segment sensitive data.**
- **Enforce an account lockout after a specific number of failed attempts.**

Ransomware Awareness

Take Action: Address Ransomware Risk

Ransomware and its often-devastating impact on business operations will not go away on its own. When an infection occurs, an entity has three choices:

1. **Restore from an available backup,**
2. **Pay the ransom, or**
3. **Suffer the impact of downtime while rebuilding the affected device(s)/systems.**

Entities continue to overestimate the ability to restore and the time to restore. Consider your entity's approach to paying a ransom before a ransom scenario occurs, including under which scenarios you would pay and how you would pay.

91%
Percent of time when ransom was paid that a decryption key was received

$28,920
Average ransom paid

94%
Percent of time entity used a third party to pay ransom

$250,000
Largest ransom paid*

*In 2019 our clients have already paid three ransoms of $1 million or more

DISTRICTS MUTUAL INSURANCE & RISK MANAGEMENT SERVICES | Collaborators in Risk Management |

Vendor Management

Contract Review & Professional E&O / Cyber Insurance Requirements

- ✓ Proper indemnification from your vendors will help to mitigate your vicarious liability should your chosen partner make an error that is out of your control

- ✓ Vendor Acceptance Process is vital
  - ❑ Develop Errors & Omissions, Cyber, and Crime Insurance Contract Language designed to be made part of your existing insurance contract requirements
  - ❑ *Develop reasonable requirements* that are relevant to the current cyber risk environment
  - ❑ Prepare a vendor evaluation worksheet!!!

Vendor Management

SAMPLE CONTRACT WORDING – CYBER, E&O AND CRIME

Vendor) shall obtain at its own expense and evidence via Certificate(s) of Insurance the following insurance requirements before commencement of any awarded work and throughout the duration of the Agreement:

A) Errors and Omissions (E&O), Technology E&O / Technology Products E&O: minimum of $5 million limit and in the annual aggregate, inclusive of defense costs

B) Network Security / Privacy Liability; including
(1) computer or network systems attacks
(2) denial or loss of service
(3) introduction, implantation, or spread of malicious software code
(4) unauthorized Access and Use of computer systems
(5) privacy liability
(6) breach response coverage

- Liability coverages should have a minimum of $5 million limit and in the annual aggregate
- Breach response sublimits of at least 50% of the liability limit

C) Crime Insurance: Vendor, at its sole cost and expense, shall obtain and maintain in full force and effect, Third Party Crime/Employee Dishonesty Insurance in an amount not less than $1,000,000. The insurance shall name _____ as a loss payee.

If policy or policies are written on a claims-made basis, coverage must be in place for a period of at least 12 months after the completion or termination of the Agreement. "INSURED" and subsidiaries must be named as an additional insured under E&O, Technology E&O / Technology Products E&O and Network Security / Privacy Liability coverage sections. Further, an appropriate endorsement deleting the Insured vs. Insured exclusion must be evidenced, so as not to impede a claim by "INSURED" and subsidiaries for a wrongful act of (Vendor). All insurance carrier(s) must carry an A.M. Best rating of at least A-, Class VIII.

Gallagher

Insurance | Risk Management | Consulting

Thank you!

DISTRICTS MUTUAL INSURANCE & RISK MANAGEMENT SERVICES | *Collaborators in Risk Management* |

April 2019 - Risk Mitigation Forum