ARC EXCESS & SURPLUS, LLC

Cyber Liability Presentation

Disclaimer:

The material presented in this presentation is not intended to provide legal or other expert advice as to any of the subjects mentioned, but rather is presented for general information only. You should consult knowledgeable legal counsel or other knowledgeable experts as to any legal or technical questions you may have. Further, the insurance discussed is a product summary only. For actual terms and conditions of any insurance product, please refer to the policy. Coverage may not be available in all states.

Biographies

Charles P. Bellingrath

Partner & National Practice Leader: Cyber/Tech

Chas Bellingrath is a Partner and National Practice Leader for Cyber, Privacy & Technology E&O at ARC Excess & Surplus, LLC. In his role Chas is responsible for advising agents and clients on issues related to technology, privacy and cyber related risks as well as negotiating with carriers on policy terms and conditions.

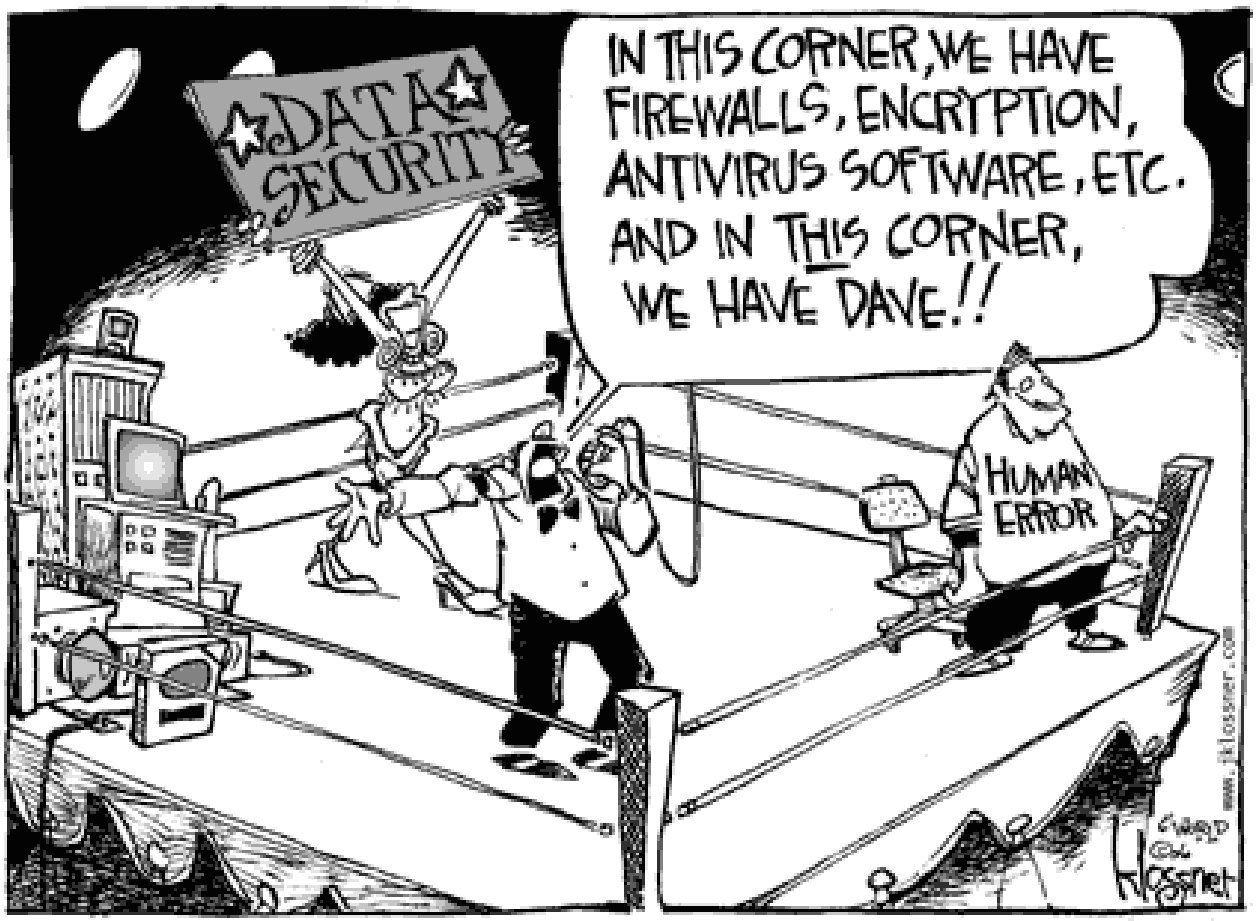
Chas specializes in tailoring tech, cyber, and breach response coverage and advises clients on breach preparedness and incident response planning. In addition, Chas is responsible for product development and production throughout the United States. Prior to joining ARC, Chas was a Senior Broker band head of the Cyber/Tech division at a regional wholesaler where he initially launched the product in 2007.

Chas brings ARC over 12 years of dedicated Cyber, Privacy & Technology risk expertise. Chas is globally recognized and frequently instructs privacy seminars and participates on executive panels for Cyber Risk conferences. Chas also sits on several Producer Advisory Councils for top insurance carriers and the PLUS CyberRisk Task Force.

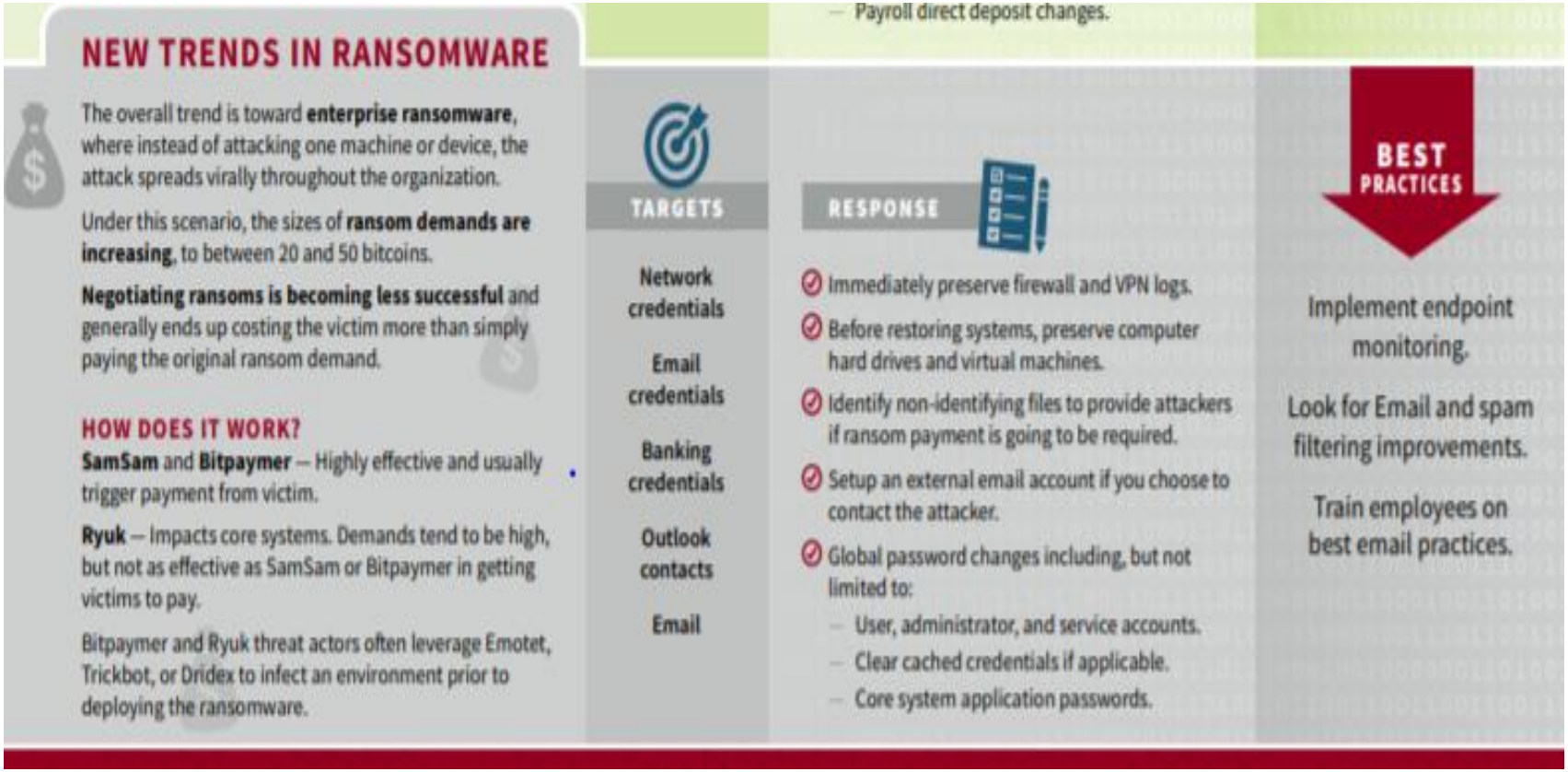
In 2019, Chas received his CCIC (Cyber Cope Insurance Certification) from the Heinz College at Carnegie Mellon University.

Table of Contents

Exposures & Trends


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC.
AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
www.jklossner.com

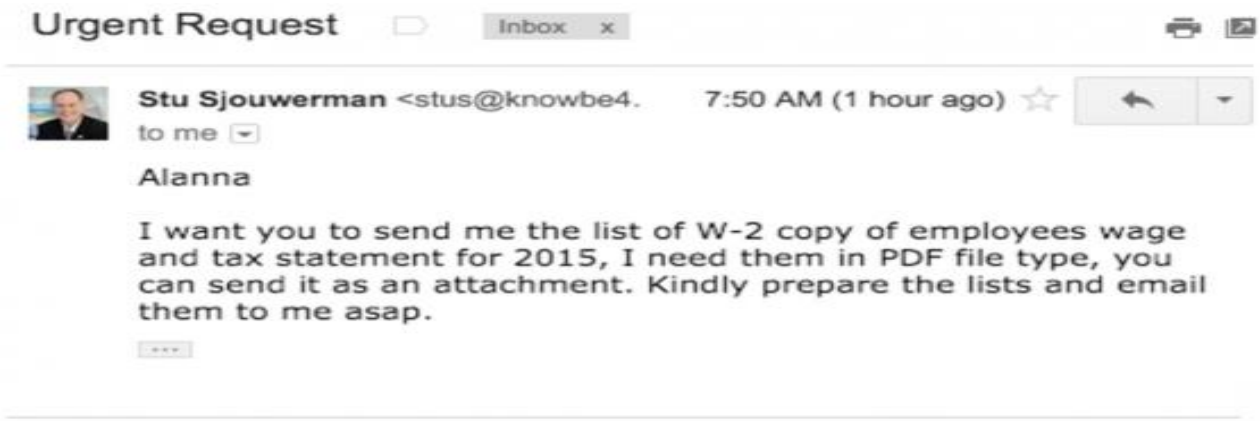
New Trends in Ransomware



Source: Crypsis

W-2, Business Email Compromise & Phishing

- Scammers use emails from a target organization's CEO, asking human resources and accounting departments for employee W-2 information.
- Scammers phish online payroll management account credentials used by corporate HR professionals.
- Scammers send emails pretending to have important Documents, or important new O365 mailbox audit log functionality
- Reverse Social Engineering



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

Source: BakerHostetler Data Security Incident Response Report 2019

Incident Response Trends: Timeline

66
Days
Occurrence to Discovery

8
Days
Discovery to Containment

28
Days
Time to Complete Forensic Investigation

56
Days
Discovery to Notification

Average Forensic Investigation Costs

$63,001
All Incidents

$120,732
Average Network Intrusion

$350,576
Average of 20 Largest Network Intrusions

Source: BakerHostetler Data Security Incident Response Report 2019

Who is being targeted?

25%
Healthcare
(including Biotech & Pharma)

17%
Finance & Insurance

17%
Business & Professional Services
(including Engineering & Transportation)

12%
Retail, Restaurant & Hospitality
(including Media & Entertainment)

11%
Education

11%
Other

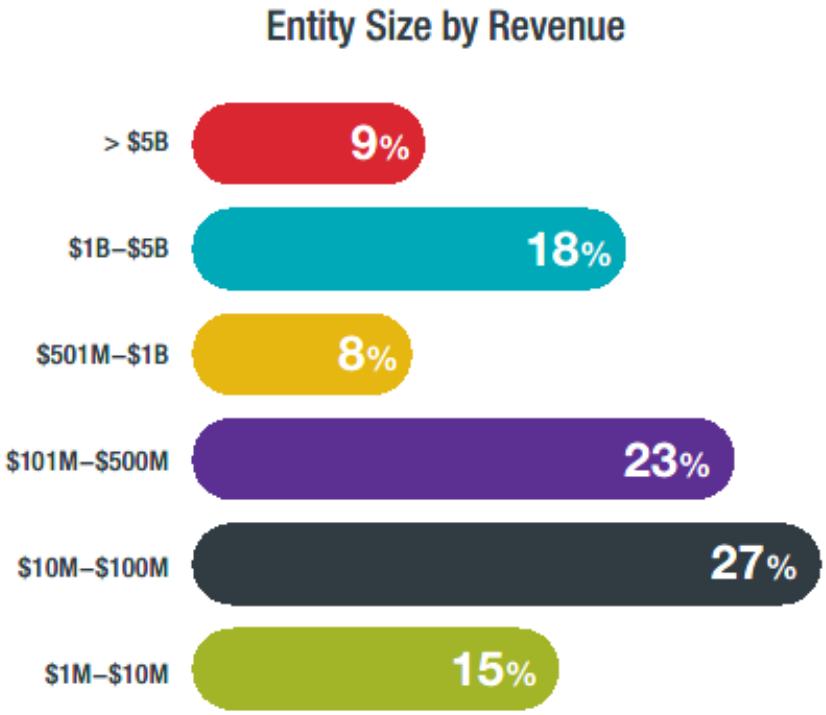
5%
Government

1%
Nonprofit

1%
Energy

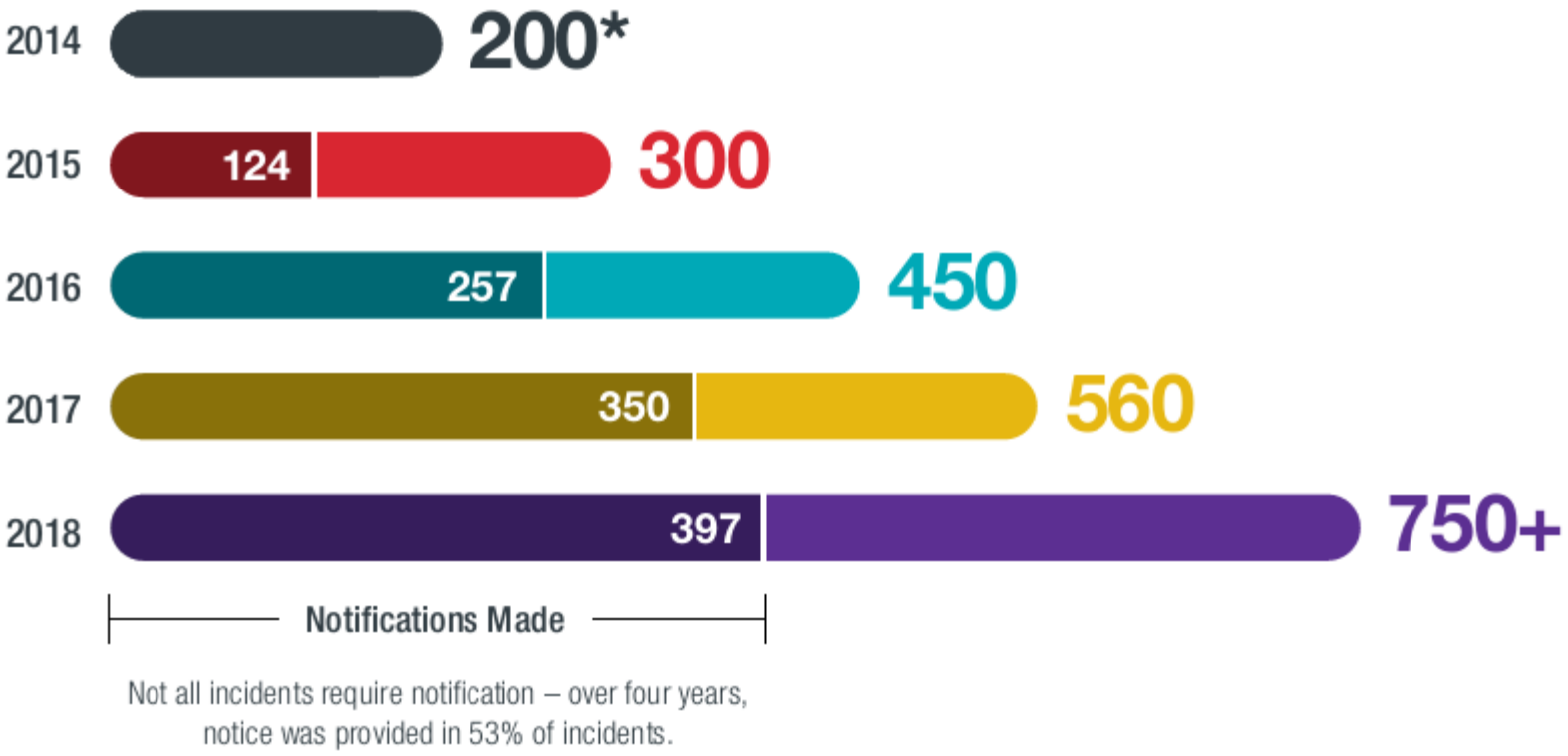
Source: BakerHostetler Data Security Incident Response Report 2019

Who is being targeted?



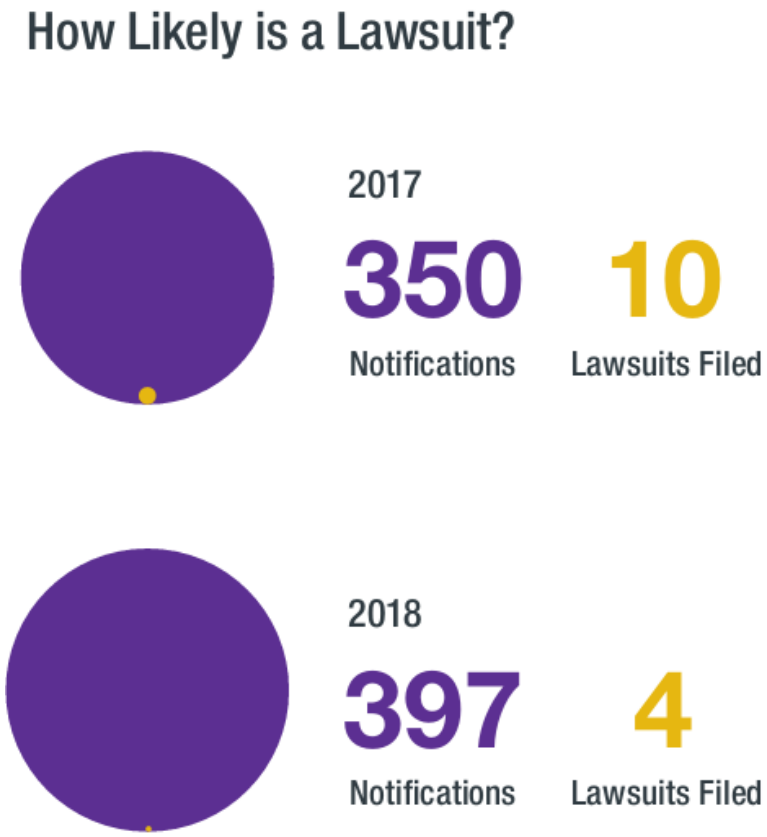
Source: BakerHostetler Data Security Incident Response Report 2019

Number of Incidents



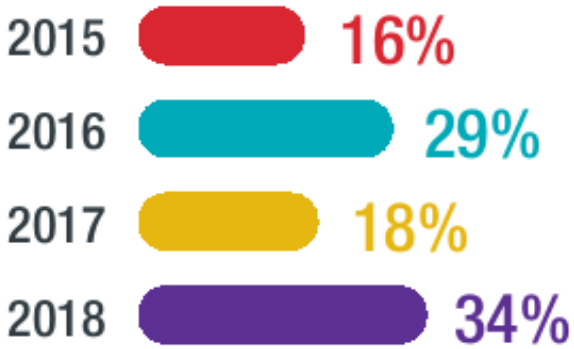
Source: BakerHostetler Data Security Incident Response Report 2019

How Likely is a Lawsuit?



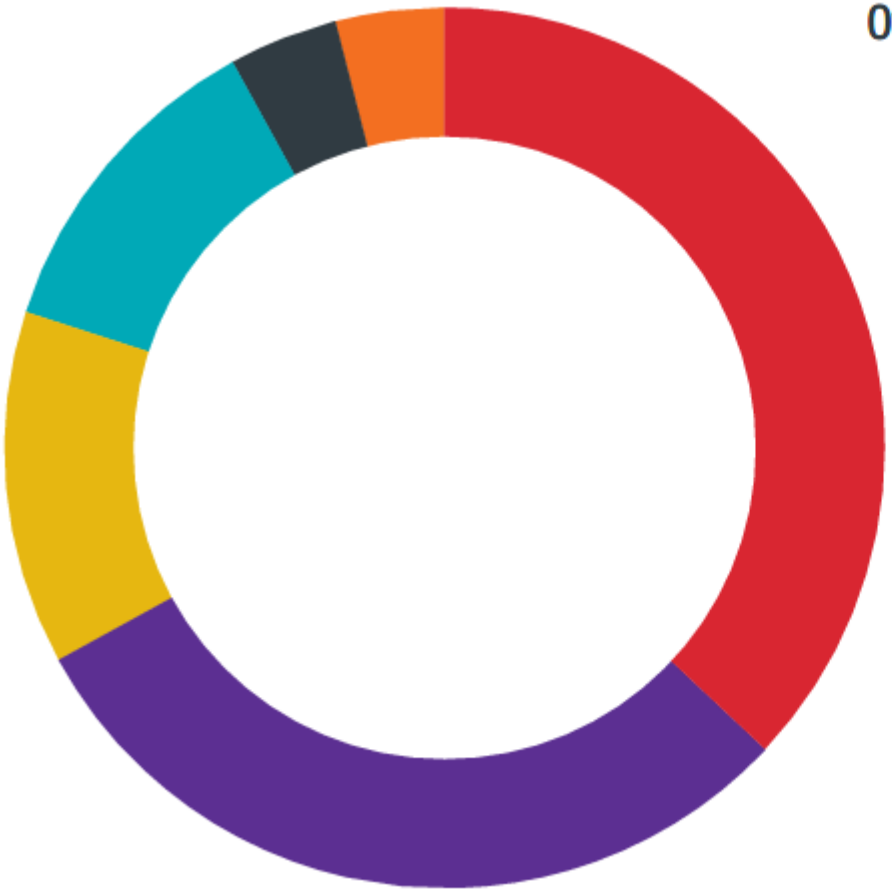
AG Inquiry After Notice

After notification occurs, a regulatory inquiry is the most likely next development (more likely than a lawsuit).



Source: BakerHostetler Data Security Incident Response Report 2019

How are incidents occurring?



Overall

37% Phishing

30% Network Intrusion

13% Stolen/Lost Device or Records

12% Inadvertent Disclosure

4% System Misconfiguration

4% Other

Source: BakerHostetler Data Security Incident Response Report 2019

Responsible Party

55%

Employee

Often there is a combination of an employee mistake exploited by a non-vendor unrelated third party (i.e., a threat actor).

27%

Non-Vendor Unrelated Third Party

11%

Vendor

3%

Non-Vendor Related Third Party

2%

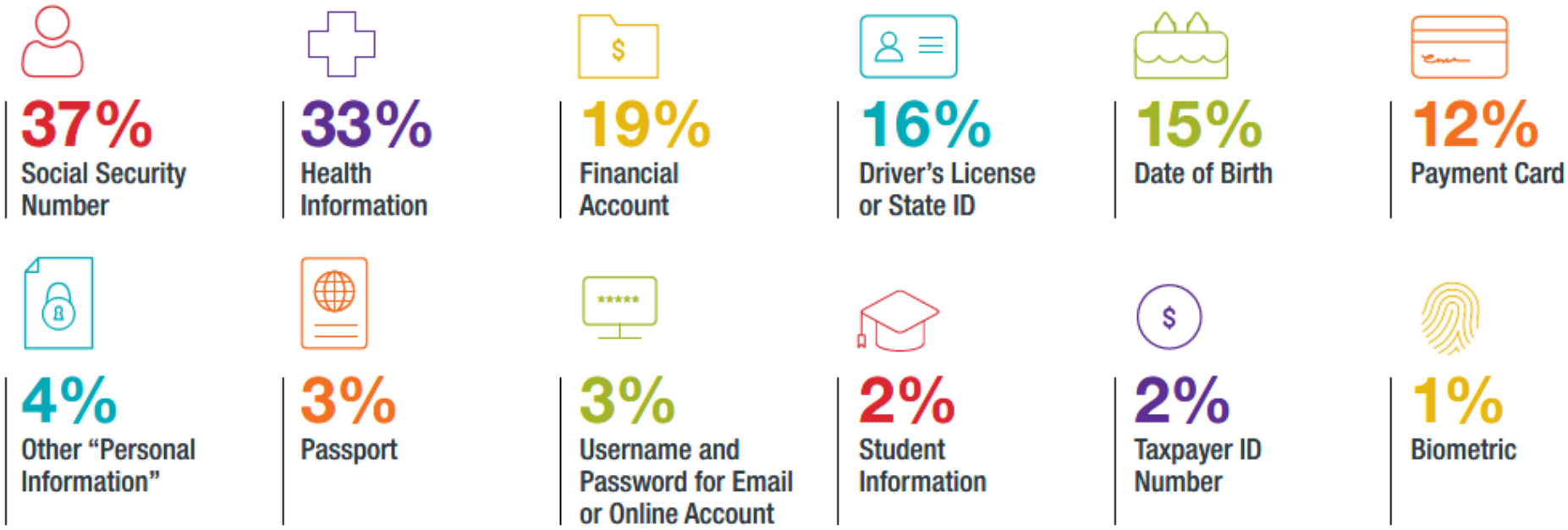
Unrelated Third Party

2%

Not Applicable

Source: BakerHostetler Data Security Incident Response Report 2019

Data at Risk



Source: BakerHostetler Data Security Incident Response Report 2019

Market Conditions

Market Conditions

- Cyber Insurance remains one of the fastest growing lines of business in the insurance industry, with growing coming both domestically (U.S) and internationally.
- This growth is likely driven by a combination of increased risk awareness, as well as increased “outside” scrutiny (boards of directors, regulators, legislatures, etc.)
- As the world continues to become more interconnected , threats continue to evolve beyond data breach / ID theft, Cyber risk has emerged as a significant threat/risk for small and large commercial accounts and individuals alike.
- Insurers have sought to more carefully define the boundaries of property, casualty and cyber policies; property insurers, for example are generally no longer willing to provide coverage for business interruption cause by network intrusion. Those losses are increasingly expected to be covered under cyber policies, which have expanded to response to a wide variety of potential risk while still being competitively priced.
- Capacity is keeping up with the demand for coverage, additional limits are being provided by new entrants in the U.S., London, Bermuda and Asian markets. Notable new entrants in the U.S. Markets include Everest, QBE and Crum and Forster.
- Cyber insurance premiums on renewals are averaging single digit rate increases (primary and excess) despite several high profile breaches, and increase claims frequency.
- Many Carriers are continuing to expand traditional policies to cover gaps in cyber policies when it comes to property, general liability and crime, while others are starting to pull back coverage (NAS, Sompo, Argo)

Source: Dowling and Partners Securities, LLC

Market Conditions (Cont'd)

- Billions of people were affected by data breaches and cyberattacks in 2018 – 765 million in the months of April, May and June alone – with losses surpassing tens of millions of dollars, according to global digital security firm Positive Technologies. (USA Today)

- Cyberattacks increased 32 percent in the first three months of the year and 47 percent during the April-June period, compared to the same periods in 2017 (Positive Technologies)

- The majority of attacks in 2018 were aimed at direct financial profit or obtaining sensitive information. However, attacks aimed at data theft often have financial implications: data can be used for stealing money, blackmailing, and can even be sold on the darkweb. (Positive Technologies)

- Almost a quarter of attacks (23%) hit individuals. As for organizations, government institutions suffered in 19 percent of cases, whereas healthcare and financial institutions were targeted in 11 and 10 percent of cases, respectively. (Positive Technologies)

- Attacks are becoming more and more sophisticated, and often consist of several stages with different methods used. Malware was used in more than half of attacks. (Positive Technologies)

- As recently reported by Protenus, the patient data management company, 2018 saw a 3X increase in breaches of personal health records, exposing over 15 million records.2 The ITRC (Identity Theft Resource Center) reports that in 2018, over 1,200 incidents have exposed 440 million records of personal information, an increase of 126% over 2017 (NAS Report).

- CyberSecurity Ventures reports that ransomware cost businesses $5 billion worldwide in 2017 and upwards of $8 billion in 2018 (NAS Report).

The Legal Landscape

Privacy Class Actions

2018 saw new developments in the evolving law surrounding data privacy class actions. Over the past several years, there has been a shift in the types of cases filed. As entities have taken measures to reduce incidents involving loss or theft of unencrypted devices containing sensitive data, class actions filed over physical theft of data have decreased. Simultaneously, consistent with the increase in phishing and network intrusion incidents, there has been an increase in class actions involving a criminal attack on a network. This includes numerous high-profile attacks where hundreds of millions of individuals were notified.

Source: BakerHostetler Data Security Incident Response Report 2019

Regulators More Involved

The Usual Suspects

Every state now has a breach notification law, and many have made revisions over the years. State attorneys general (AGs) view enforcement of data security incidents as one of their chief consumer protection priorities. Inquiries and investigations are coming from more AGs than just a few of the active state AGs. AGs also are expanding their enforcement regimes, either through new state laws or increased use of existing laws. For example, 2018 saw the first AG multistate lawsuit to enforce HIPAA. Meanwhile, the Office for Civil Rights (OCR) continues as the primary HIPAA enforcer, frequently investigating HIPAA-related incidents involving more than 500 people. And settlement amounts continue to trend upward. Whether initiated by OCR, a state AG, or international regulator, investigations almost invariably go beyond the facts of the incident itself, and a resolution likely will require significant changes to data security practices.

Source: BakerHostetler Data Security Incident Response Report 2019

Regulators More Involved

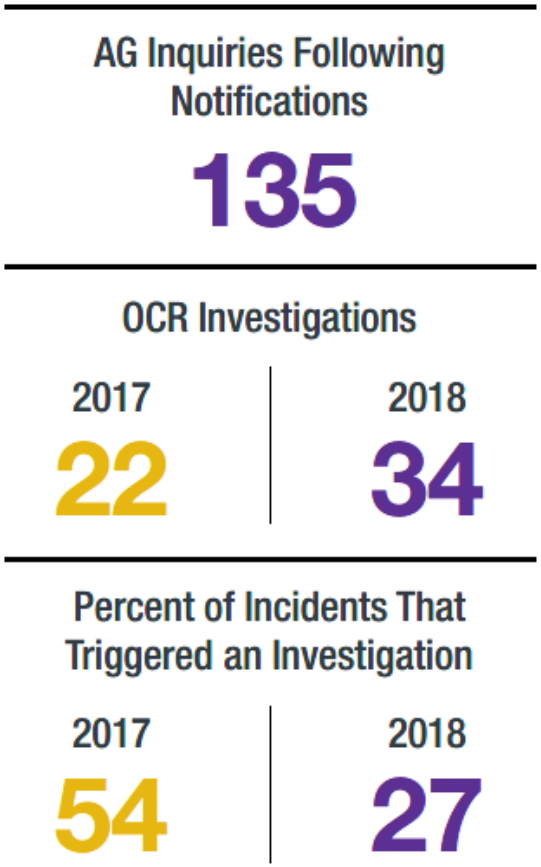
New Kids on the Block

Joining these traditional data privacy regulators are some other entities that have not traditionally been active in the data privacy sphere, including state and federal financial regulators and European Data Protection Authorities (DPAs).

State departments of insurance and financial regulation as well as the U.S. Securities and Exchange Commission are also active. A number of states have adopted or are adopting a model law promoted by the National Association of Insurance Commissioners that requires 72-hour notice of a cybersecurity event.

Source: BakerHostetler Data Security Incident Response Report 2019

Regulators More Involved



Source: BakerHostetler Data Security Incident Response Report 2019

Regulators More Involved

California Alters U.S. Privacy Law

Companies need to start preparing to comply with the forthcoming California Consumer Privacy Act (CCPA), a paradigm-shifting approach to data privacy that borrows heavily from European law. The CCPA will affect all but the smallest businesses with data on California residents. Those with existing compliance programs for the EU's GDPR will have a head start. The CCPA is effective January 1, 2020, but companies will need to have begun detailed data mapping and tracking of data practices as of January 1, 2019 in order to comply in 2020 with notice and consumer request requirements that are subject to a 12-month lookback.

The CCPA gives California residents the right to learn categories of personal information that businesses collect or otherwise receive, sell, or disclose about them; the purposes thereof; and the categories of third parties with whom businesses disclose PI. It also grants California residents the rights to (1) obtain more detailed information about their own personal information; (2) access and obtain transportable copies of their personal information; (3) prevent businesses from selling their personal information; and (4) subject to certain exceptions, to request that a business and its service providers delete their PI.

The CCPA prohibits businesses from discriminating against consumers who exercise these rights, subject to some exceptions. The CCPA will require detailed disclosures as well as multiple methods for exercising data subject rights.

Further, the CCPA requires that contracts with service providers include certain terms, including a requirement to delete personal information.

The California Department of Justice has stated that it will need to secure more than $57.5 million annually in civil penalties to cover its cost, suggesting the potential for robust enforcement. There is also a limited private right of action for security incidents. Plaintiffs' class action attorneys may also attempt to bring claims under California's Unfair Competition Law for CCPA violations, notwithstanding language in the CCPA that should preclude such actions.

Although bringing your company into compliance with the CCPA will require an investment of time and resources, it also provides an opportunity to identify inefficiencies, upgrade outdated processes, and proactively tackle privacy and data security concerns. And with at least 15 other states drafting similar laws, a wait-and-see approach to beginning compliance efforts is likely to leave you scrambling and at risk.

> "The California AG may bring actions for civil penalties of $2,500 per violation, or up to $7,500 per violation if intentional."

Source: BakerHostetler Data Security Incident Response Report 2019

GDPR

EU Update: GDPR a Game-Changer for Data Breach Notification

When the EU GDPR took effect on May 25, 2018, it dramatically changed the way multinationals manage the reporting of personal data breaches. It also substantially raised the stakes: entities found to have violated the GDPR's data security and breach reporting obligations may face much steeper regulatory fines under the new regime, far greater than penalties typically experienced by companies in the U.S.

Among the challenges in responding to a personal data breach in the EU are the scope of what constitutes a notifiable breach and the tight time frame for providing notification. The GDPR defines "personal data" more broadly than the definition of "personally identifiable information" under most U.S. laws. And its definition of a "personal data breach" includes any incident that affects the confidentiality, availability, or integrity of personal data – even incidents caused by accidents or natural events. This departs from some U.S. laws that define breaches more narrowly, with a focus on confidentiality breaches and breaches caused by malicious actors. An entity that experiences a data security incident must investigate and notify regulators within 72 hours of becoming aware that the incident is a personal data breach, unless it is "unlikely to result in a risk to the rights and freedoms of natural persons." In addition, entities must notify affected individuals where the incident is "likely to result in a high risk" to those rights and freedoms. Failure to implement appropriate data protection policies or to properly notify regulators or individuals is punishable by fines of up to 4% of a company's global annual turnover.

In advance of the GDPR's implementation date, our data privacy lawyers guided clients through more than 150 multifaceted GDPR compliance projects. Since late May 2018, we have helped clients investigate and respond to more than 20 incidents where notification was made to a data protection authority in the EU and other international jurisdictions. The incidents ranged from Office 365 account takeovers affecting only a few individuals with relatively low-risk data to complex network intrusions involving notification to individuals and data protection authorities across dozens of countries/territories.

[No Title]

Source: BakerHostetler Data Security Incident Response Report 2019

Take Action: Address the Globalization of Incident Response

- In advance of a breach implicating the GDPR, identify the regulators to whom you will report and the associated reporting requirements. There are substantial challenges to meeting the 72-hour GDPR deadline, beyond just the short time period. Many DPAs have created online reporting portals and allow preliminary reports to be supplemented once affected entities have more information about the incident. However, particularly for English-only speakers, navigating inconsistent, unclear, foreign language-only, or nonexistent reporting portals can consume valuable time while the clock is ticking.
- Entities subject to the GDPR should identify their Lead Supervisory Authority (LSA) before a breach occurs. The benefit of an LSA designation is significant; it permits the entity to report a breach to a single DPA (the so-called "one-stop shop") rather than to authorities in each EU member state.
- Incident response plans should be revised to contemplate GDPR breaches. Consider the timing and complications associated with reporting a personal data breach in multiple countries, including inconsistent or conflicting legal and regulatory requirements, and unique risks that may arise in certain jurisdictions.
- Consider the role of the Data Protection Officer (DPO) or Article 27 Representative. Entities subject to the GDPR's requirement to designate a DPO or a Representative (for businesses not established in the EU) should consider the role of these individuals in the data breach response process, particularly for multinational incidents that might implicate legal privilege in the U.S.
- More than 25 jurisdictions around the world impose some sort of data breach notification obligation. That number is almost certain to grow. The variations in what information must be reported and to whom, as well as the circumstances, format, and language of such reports, are unpredictable. And there is often little guidance as to how authorities will enforce requirements or respond to notification. Multinationals holding personal data for individuals should make privacy and data protection a top priority, with proper planning for cross-border incident response a key component of their data security program.

Source: BakerHostetler Data Security Incident Response Report 2019

The Privacy "Patchwork"

- Federal & state laws govern the handling of PII/PHI
  - Laws covering SSNs / disposal of PII
  - Other federal and state regulations (e.g. FTC Act, Mass. Regs)

- HIPAA
  - Applies to Covered Entities and Business Associates
  - Preempted except where state law is "more stringent"

- State breach notification laws

- State medical information breach reporting laws

- International data protection regulations

State Laws

- All 50 States have Security Breach Notification Laws
- Laws vary between jurisdictions
- Varying levels of enforcement by state attorneys general
- Limited precedent
  - What does “access” mean?
  - What is a reasonable notice time?

States with Changing Regulations

California

- Clarified breach of encrypted data **with encryption key** requires notice

Illinois

- **Adds data to definition of PI**: medical information, health insurance information, unique biometric, username/email address and password/security question and answer
- Clarified breach of **encryption key** requires notice
- **Added Regulator Notice**:
  - HIPAA Covered Entities must notify IL AG within 5 business days of notifying HHS
  - State agencies must notify AG when 250 or more affected

Massachusetts

- Now **publishing data breach notifications** online list
- Joins other states including: CA, HI, ME, NH, OR, VT, WA

Tennessee

- Clarified **encryption safe harbor** in April: breach of encrypted data (without loss of encryption key) does NOT require notice.

New Mexico

- 48th State to enact
- Notice within 45 days after discovery of breach of computerized data
- Notice Attorney General and consumer reporting agencies if more than 1,000 New Mexico residents are notified.
- Defines PII as name in combination with Social Security Number, Driver's License Number, Government ID Numbers, Financial Account numbers, Biometrics Data

Delaware

- Effective April 14, 2018
- **Expands definition of PI** to include: biometric data, medical information, passport numbers, routing numbers, TINs, and usernames
- Requires one year of **credit monitoring** for breaches involving SSNs
- **Notice to Attorney General** if more than 500 Delaware residents are affected
- Notice within **60 days** after discover of a breach

New York

- **Breach of the security of the system** is unauthorized acquisition or acquisition without valid authorization of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a business.
- In determining whether information has been acquired without authorization, entities may consider the following factors, among others:
  1. indications that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing information;
  2. indications that the information has been downloaded or copied; or
  3. indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.
- **"Personal information"** is any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person. "Private information" is "personal information" in combination with the following, when either the personal information or the data element is not encrypted, or encrypted with an encryption key that has also been acquired: (1) Social Security number; (2) driver's license number or non-driver identification card number; or (3) account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.
- **Notice** should be provided in the **most expedient time possible** and **without unreasonably delay.**
- **Notify Attorney General** (portal), **NY Department of State**, **State Police** (online form)
- If **over 5,000 NY residents** affected, notify **consumer reporting agencies.**
- Attorney General may bring a civil suit for damages or an injunction.

EU General Data Protection Regulation

- Data transfer restrictions are just one of the major issues currently transforming the EU privacy landscape
- Final text of the GDPR was adopted by the EU on April 2016 and became effective May 25, 2018
- Will significantly increase potential liability (including penalties) for U.S. organizations that violate EU data protection laws
- **Expanded Territorial Reach**: Via GDPR, the EU purports to reach even U.S. organizations without boots on the ground or servers in the EU, if "established" in the EU
  - "Established" to be interpreted very broadly, can include online tracking and/or profiling

Data Security Incident Notification (GDPR)

- "**Personal data breach**": incident in security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed

- Data controller must notify the competent Supervising Authority without undue delay and, where feasible, not later than 72 hours after discovery
  - If more than 72 hours later, must give reason for delay
  - Content: (1) Description of incident (number affected, categories of data subjects and data records); (2) DPO contact information; (3) likely consequences of incident, including mitigation efforts

- Individual notification required if there's a high risk (with exceptions)

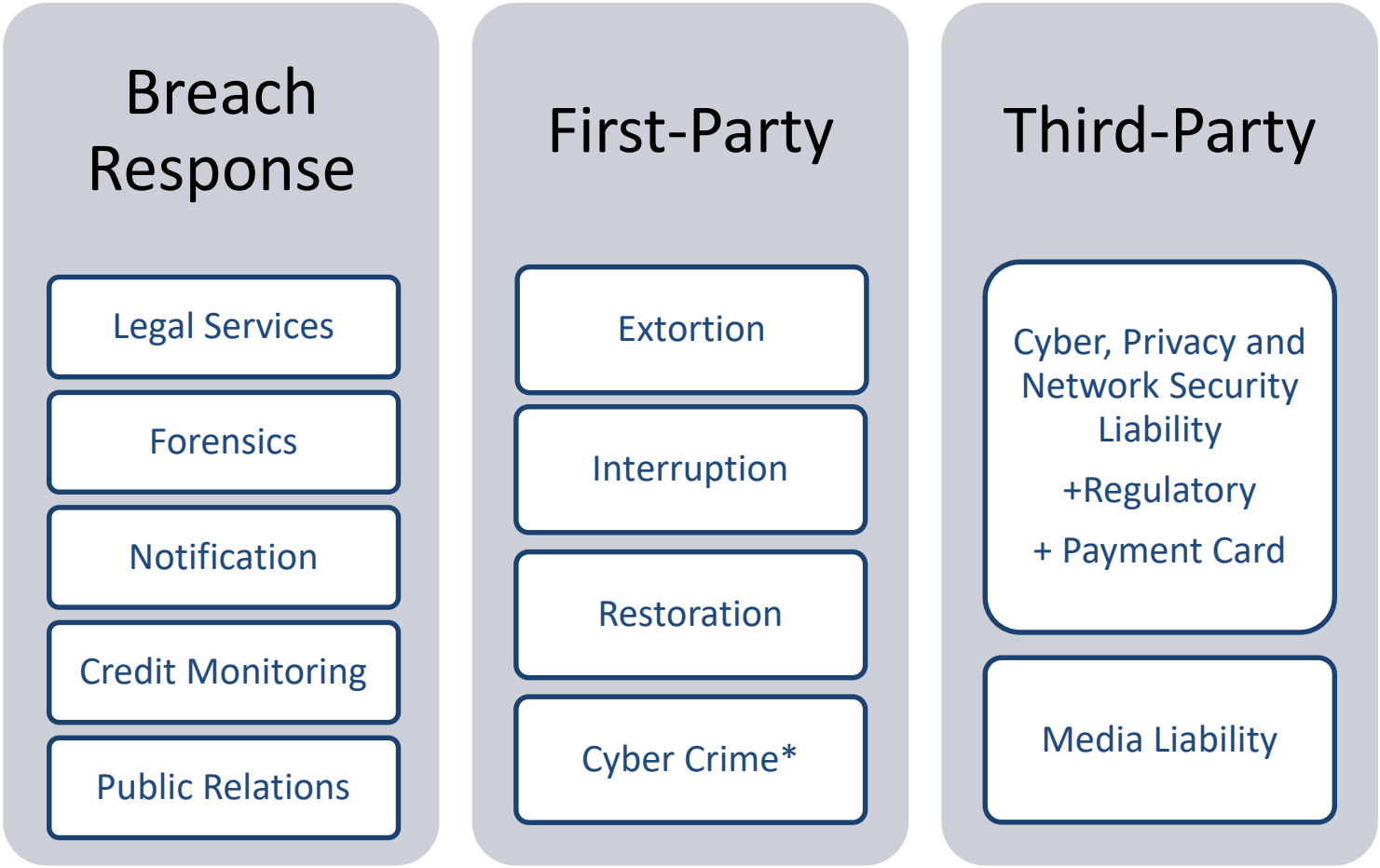
- Data processor must notify data controller "without undue delay" but no strict deadline
  - Entities operating in the EU should prepare a GDPR-compliant data security incident response plan

Other Key GDPR Changes

- **Mandatory Data Protection Officer Appointment**
- **Data Protection Impact Assessments**
- **Stricter requirements to obtain valid consent**
- **New obligations of processors:** GDPR introduces direct compliance obligations for data processors and requires detailed provisions in third-party processing contracts
- **Data portability rights**: GDPR requires organizations to provide personal data in a "portable" format
- **Potential for huge sanctions:** Max fine for serious infringements of the GDPR = the greater of €20 million or 4% of worldwide turnover for the preceding financial year

The Coverage

Coverage Sections



First Party Coverage

Incident / Breach Response

- Legal/Breach Coach fees, forensics, notification costs, credit/identity monitoring, public relations, crisis communications, call center services etc.
  - Cyber Incident Response Expenses
  - Cyber Incident Response Coach / Legal Counsel

Data Restoration / Digital Asset

- Costs to restore or replace lost or damaged data or software
  - Digital Data
    - Does not include tangible property, or does it??
- Digital Data Recovery Costs
  - Network Security Failure/Malicious Computer Act

First Party Coverage

Cyber Business Interruption

- **Loss of profits and expenses from interruptions of insured's systems; and with Contingent Business Interruption, adds losses from interruptions of others' systems**
  - Business Interruption Loss and Extra Expenses
  - Interruption in Service
  - Period or Restoration
  - Waiting Period
- **Dependent Business Interruption Loss and Extra Expenses**
- **System Failure – Business Interruption (Non-Malicious Computer Act)**
  - Human Error
  - Programming Error
  - Power failure of an electrical system controlled by and Insured, and not arising from Property Damage
- **Dependent System Failure**

First Party Coverage

Cyber / Network Extortion

- **Payments to prevent digital destruction/impairment**
  - Network Extortion Threat
  - Extortion Expenses
  - Coverage includes Ransomware

  also includes bitcoin and cryptocurrency

Cyber Crime

- **Computer Fraud:** Third party accessing insured's computers to take money
- **Funds Transfer Fraud:** Third party tricking a bank into transferring funds from insured's account
- **Social Engineering Fraud:** Third party tricking an employee into transferring money

Telecommunications Fraud

- **Costs incurred as phone bill charges due to fraudulent calling**
  - Telephone Fraud Financial Loss
  - Telephone System

Third Party Coverages

- **Cyber, Privacy and Network Security Liability**
  - **Failure to protect private or confidential information of others, and failure to prevent a cyber incident from impacting others' systems**
    - Network Security Failure
    - Protected Information
    - Privacy or Cyber Law

- **Payment Card Loss (PCI)**
  - **Contractual liabilities owed as a result of a cyber incident**
    - PCI Data Security Standards
    - Payment Card Loss

Third Party Coverages

- **Regulatory Defense, Fines and Penalties**
  - **Defense for regulatory actions and coverage for fines and penalties**
    - Privacy or cyber laws – includes state, federal and foreign
    - Consumer Redress Fund
    - Regulatory Fines

- **Media Liability**
  - **Copyright and trademark infringement within scope of defined media content**
    - Electronic, Social and Printed Media Liability
    - Media Incident
    - Media Content

Important Provisions & Reminders

- Know your responsibilities as an Insured
  - Reporting Security Incidents in a timely fashion
    - Engaging with your broker and carrier (s)
    - Reporting via email
    - Breach Hotlines

- Breach Response Vendors
  - Can we use our own counsel, forensics??
  - Panel list review
    - Scheduling Preferred Counsel

Risk Management Services

- Beazley Breach Solutions – www.beazleybreachsolutions.com

Resources on Security Breach Information

- Privacy Rights Clearinghouse- www.PrivacyRights.Org
- Ponemon Institute, LLC- www.ponemon.org
- Privacy Law Blog- https://www.bakerlaw.com/PrivacyDataProtection
- NetDiligence – Junto by eRiskHub - http://juntoblog.net/
- Advisen Cyber FPN – https://www.advisenltd.com/front-page-news/cyber-fpn-30-day-trial/

Contact Information

Charles P. Bellingrath, CCIC
Partner & National Practice Leader: Cyber/Tech
ARC Excess & Surplus of MA LLC
495 Old Connecticut Path, Suite 110
Framingham, MA 01701
Direct: 857.239.5051
Cell: 860.819.4395
Email: cbellingrath@arcne.com
www.arcbrokers.com

Questions?

As a specialty insurance brokerage firm, ARC Excess & Surplus provides innovative specialty solutions, offering superior client service nationwide.