Lawley

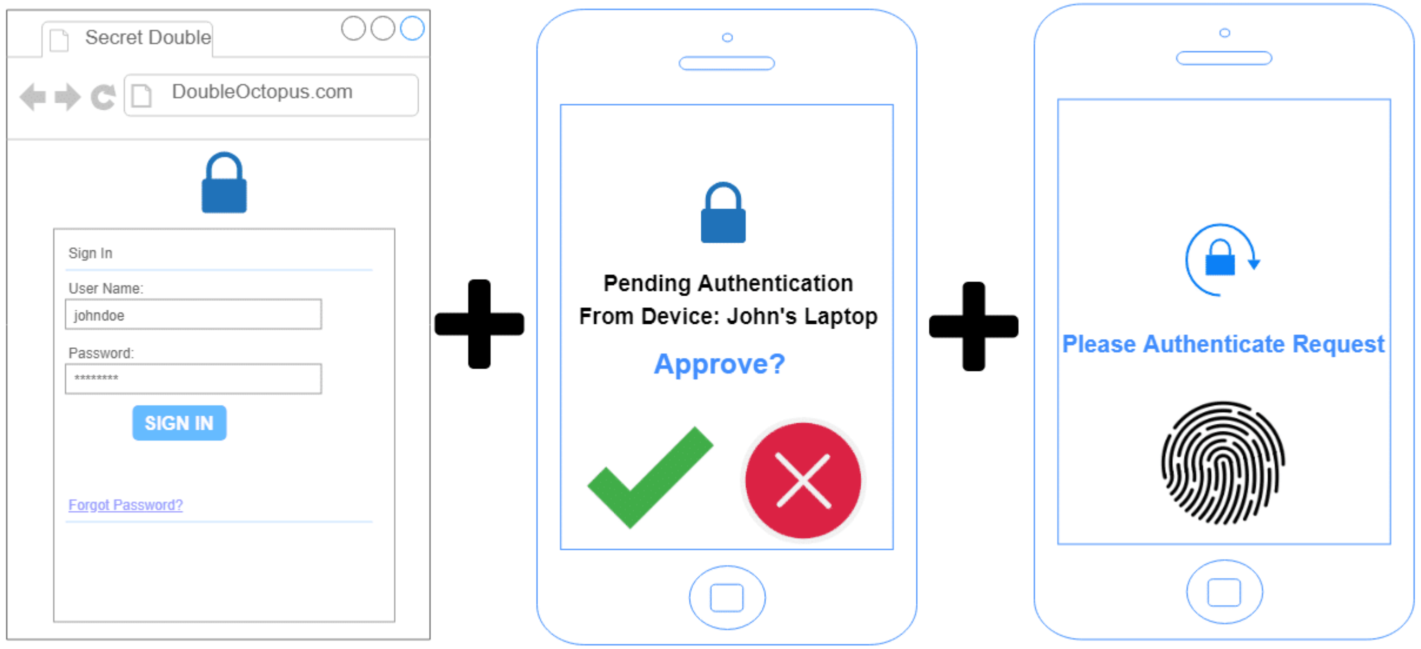
CYBERSECURITY INSURANCE

December 2021

What Would Happen if Your Company was Paralyzed?

Travelers Stat

- Travelers recently reviewed 270 Cyber claims on a countrywide basis
- Of the 270 claims, 269 Insureds did not have Multi-Factor Authentication (MFA) in place



What Would Happen if Your Company was Paralyzed?

What we’ve seen in the last 12 – 24 months

- **Number of claims:** over 55
- *Typical Claims include -*
  - **Legal Costs:** Average $35,000 - $40,000
  - **Forensic Costs:** Average $50,000
  - **Cyber Extortion/Ransomware:** Average $75,000 - $100,000
  - **Business Interruption:** Average $125,000 - $150,000
- **Policies written in 2020** -
  - Premium for cyber in excess of $6,500,000
  - $800,000 in revenue
  - 700 policies
  - Average premium $9,300 per policy

Recent Claim Trends

Ransomware Attacks:

- Contracting company
- Several files on its servers were encrypted
- Ransom of approximately $50,000 initially demanded
- Insurance company promptly notified through their cyber incident response hotline and an incident response coach and a forensic firm were retained
- Client decided to pay the ransom and was able to begin the decryption process
- No personally identifiable information was compromised

As a result of the ransomware attack, the client incurred losses of approximately:

$140,000, which included:

- $15,000 for the incident response coach
- $75,000 for the forensic firm
- $50,000 for the ransom payment

Recent Claim Trends

Phishing Emails:

- Wholesale Construction Material Supply company
- Mass phishing attack - link that enabled the bad actors to obtain system credentials which allowed them to access email accounts
- **Approximately 75 email accounts were compromised**
- Many of the email accounts contained names and bank account numbers of the client's customers
- Several thousand documents needed to be reviewed to determine the nature and scope of the affected files
- Bad actors were able to access the client's other systems to cause several fraudulent wire transfers to take place

It was eventually determined that 40,000 people needed to be notified and provided with two years of credit monitoring

Total first party losses were approximately $650,000, broken down as follows:

- $250,000 for the forensics firm
- $300,000 for the incident response coach (including legal)
- $100,000 credit monitoring and call center fees

Recent Claim Trends

Unauthorized Access:

- Professional organization
- Online portal for its clients to access data experienced a security incident
- Service representatives noticed client registration information was incorrect and there had been a scrambling of data
- Unauthorized access occurred on one of its servers providing external web portal functionality
- No evidence that personally identifiable information (PII) was disclosed during the attack and the data returned from the Insured's database was non-sensitive

Approximately

$100,000

in 1st party costs associated with this matter was covered.

Recent Claim Trends

Fraudulent Instruction:

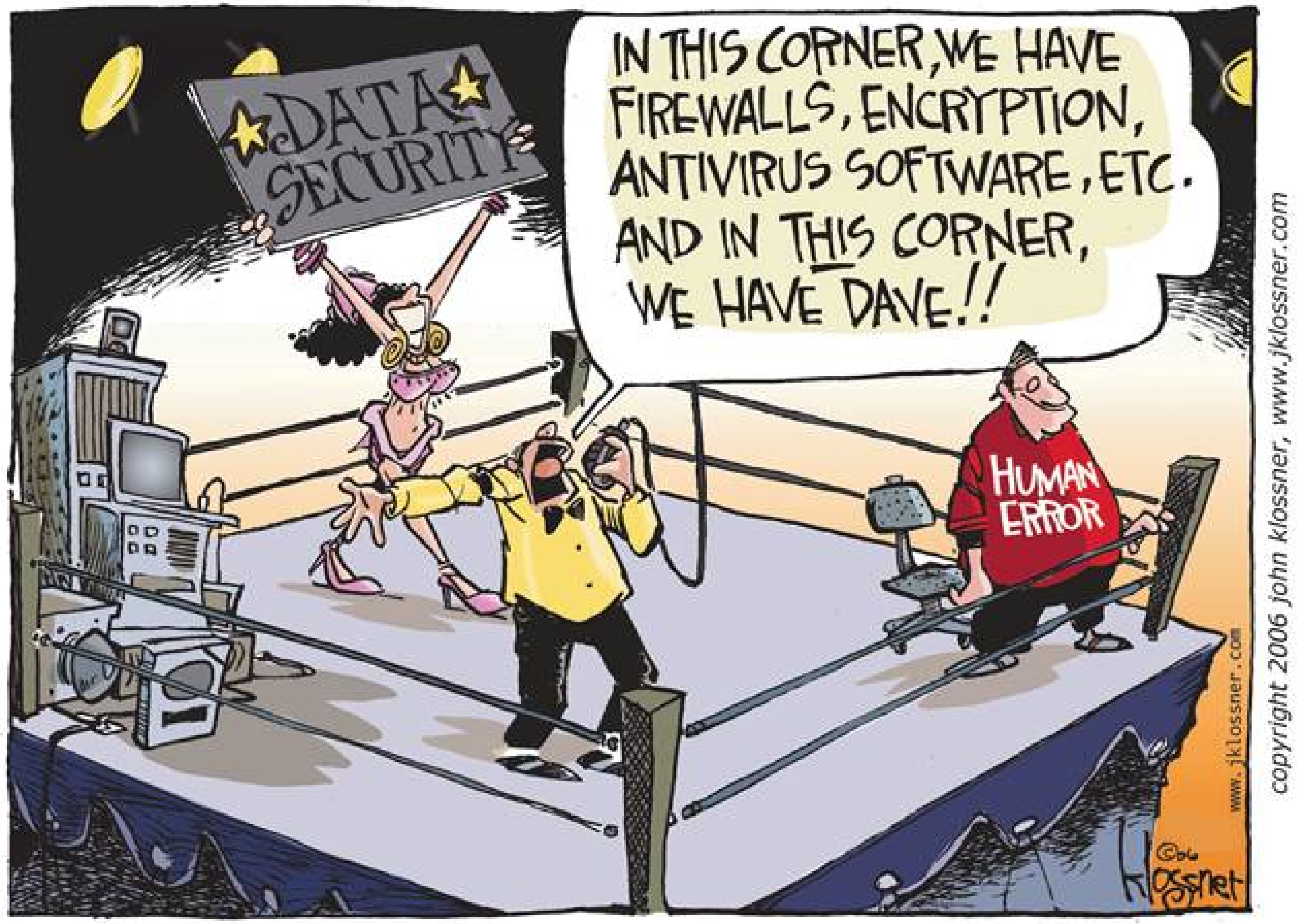
Four Hours on a Friday ….

- Unknown person obtained corporate email credentials and began impersonating a company executive
- Hacker sent an email to the finance department asking for a wire transfer of approximately $50,000
- Finance department responded with questions to confirm the request
- Hacker used the executive’s email to respond, and in the response referenced another expense (likely obtained from reading the executive’s earlier emails) as an example of how to handle the transfer, which further appeared to legitimize the wire transfer request

The money was wired.

The entire situation happened between 10:30 am and 2:30 pm on a Friday.

How Susceptible are you to a Scam?


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
copyright 2006 john klossner, www.jklossner.com
www.jklossner.com
©06 Klossner

Lawley

Example of a “Fake” Email

Can you tell the difference in these email addresses?

Dave receives an email from John containing an invoice that needs to be paid today. John’s email asks Dave to send payment for an invoice to a new bank account. Dave usually sends payment to John by check, but since they have had a long working relationship and Dave has been looking to find faster/easier ways to make payments on accounts, this request doesn’t seem out of the ordinary.

In addition to that, Dave recognizes John’s email as follows: John.Miles2@emailhack.scam

Can you tell which email below is the correct one?

John.Miles2@emailhack.scam
John.MiIes2@emailhack.scam

So, what’s the difference?

The difference is that the “l” in Miles is a lower case “L” in one, but in the other, the “I” is really a capital “i”

What is a Data Breach?

Actual release or disclosure of information to an unauthorized individual/entity that relates to a person and that:

May cause the **person** inconvenience or harm (financial/reputational)

- Personally Identifiable Information (PII)
- Protected Healthcare Information (PHI)

May cause your **company** inconvenience or harm (financial/reputational)

- Customer Data, Applicant Data
- Current/Former Employee Data, Applicant Data
- Corporate Information/Intellectual Property

Potential Security Threats

- Compromises to the integrity, security or confidentiality of information
- Circumstances where a data breach may have happened or could happen in the future (e.g. lost flash drive with PII/PHI)

Paper or Electronic

Lawley

Information at Risk

Consumer Information

- Credit cards, debit cards, payment info
- Social Security Numbers, ITIN's, taxpayer records
- Protected Healthcare Information (PHI), e.g. medical records, test results
- Personally Identifiable Information (PII), e.g. Drivers License / Passport details
- Non-PII, like email addresses, phone lists, address

Employee Information

- Employers have at least some of the above information on all of their employees

Business Partners

- Sub-contractors and Independent Contractors
- Information received from commercial clients as a part of commercial transactions or services
- B2B exposures like projections, forecasts, M&A activity, trade secrets

PII

(Personal Identifiable Information)

PHI

(Personal Health Information)

Everyone is at risk!

✸Many people think that without credit cards or PHI, they don't have a data breach risk.

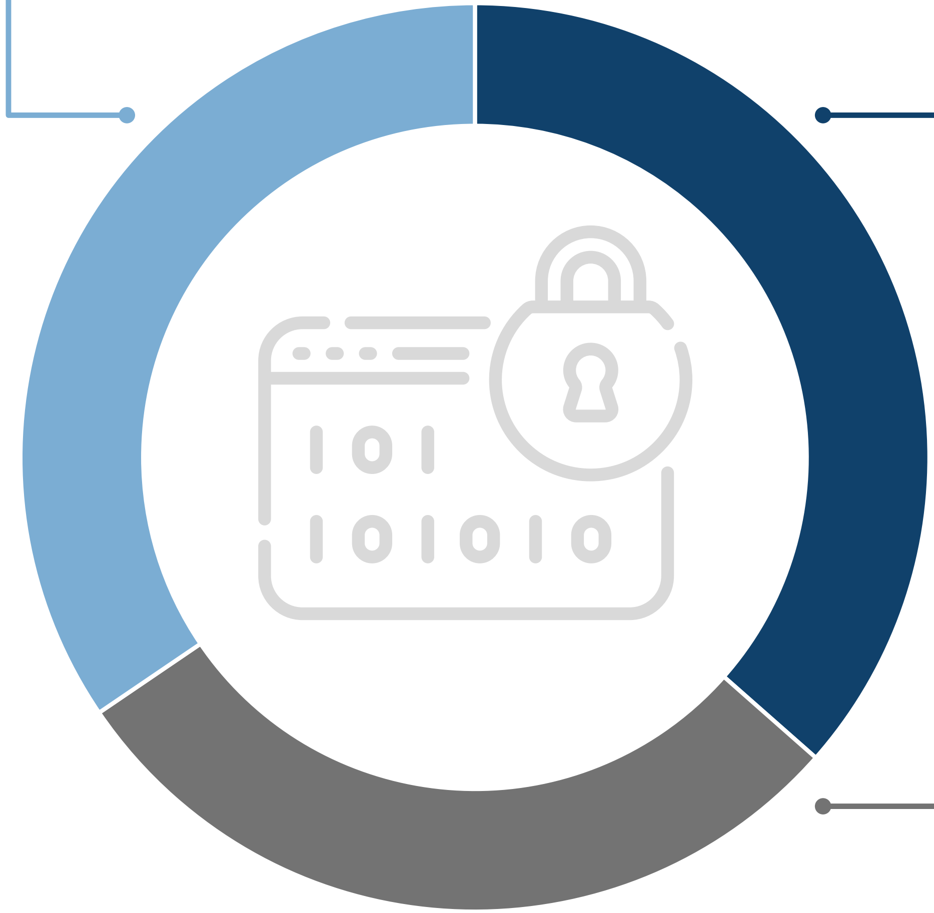
✸But can you think of any business *without* any of the above kinds of information?

Lawley

Causes of Loss

Human Factor
35%

- Lost laptops
- Improper disposal of backup tapes
- Accidental release
- Broken business practices
- Un-shredded documents



Malicious or Criminal Attack
36%

- Hacking
- Virus, Malware
- Phishing
- Spear Phishing
- Network Intrusion

System Glitch
29%

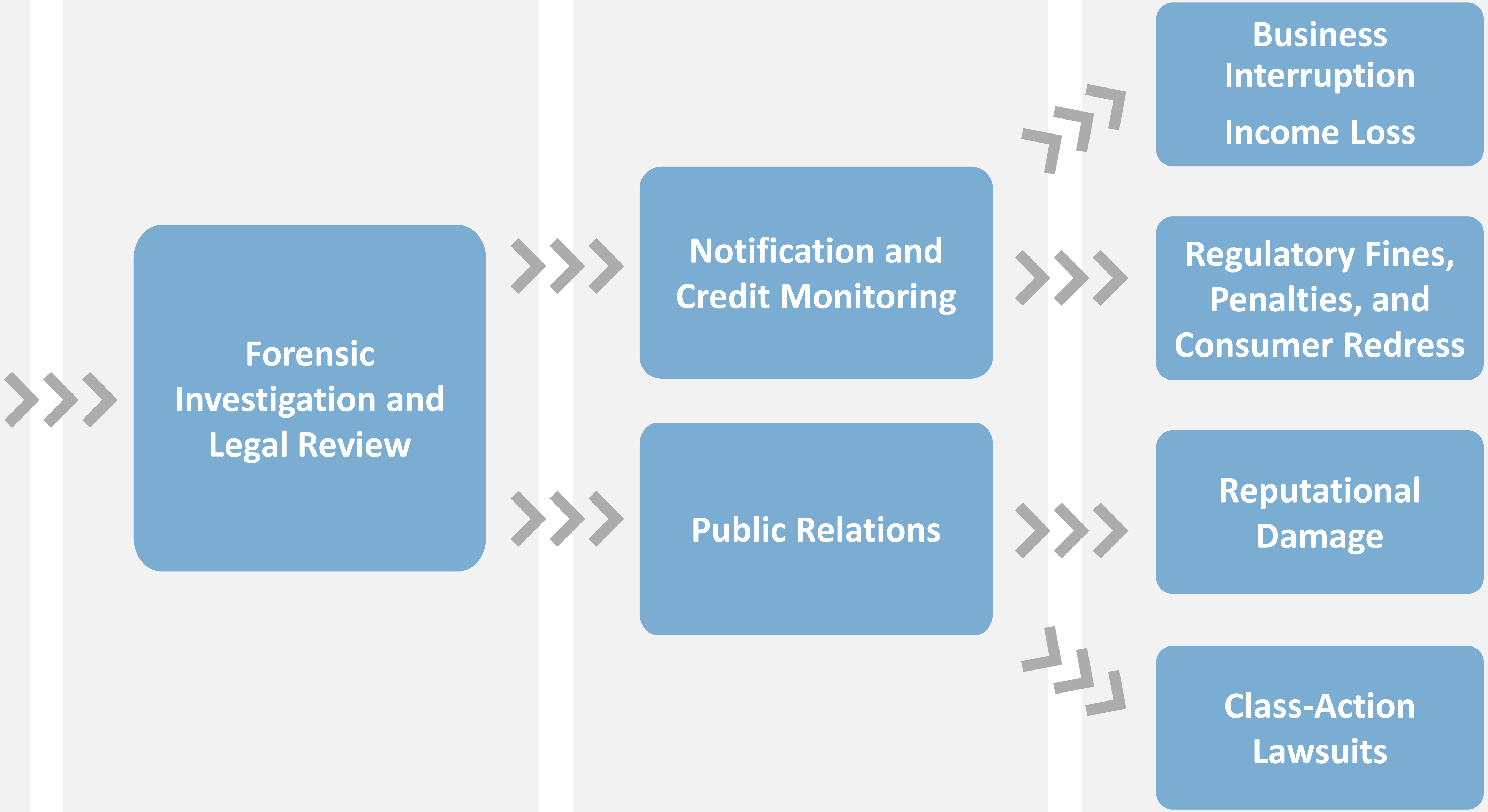
- Software not up-to-date
- Negligent release

64%
of breaches are accidental

Source: Cost of Data Breach Study: Global Analysis, Ponemon Institute

A Simplified View of a Data Breach

Theft, loss, or unauthorized disclosure of personally identifiable non-public information or third party corporate information that is in the care, custody or control of the insured organization, or a third party for whom the insured organization is legally liable



Forensic Investigation and Legal Review

Notification and Credit Monitoring

Public Relations

Business Interruption

Income Loss

Regulatory Fines, Penalties, and Consumer Redress

Reputational Damage

Class-Action Lawsuits

Recent Statistics

Cybercrime Loss Numbers

From one of our larger Cybersecurity Companies

2019

- **250,000,000 attacks** targeted at the United States in the fourth quarter of 2019 alone

- 23% of cybercrime claims exceeded $200,000
- The average cybercrime loss amount in 2019 was $116,697

- Most common method of cybercrime remains phishing

- More than 90% of successful hacks and data breaches stem from phishing— emails crafted to lure their recipients to click a link, open a document or forward information to someone they shouldn’t

Overcoming Objections from Clients

Common objections to considering Cybersecurity coverage

- Why would someone target my small company? Only large companies are targeted by cyber criminals.
- My data is in the cloud and my 3rd party vendor takes care of it, so I know it's secure.
- My IT team has me covered, and we already have security measures in place, including multi-factor authentication.
- All of our information is backed up and our company can be up and running in a few days.

Cyber/Privacy Liability Coverage

Insurance Coverage Options - First Party

First-Party Insurance

- **Business Interruption** (including Dependent Businesses)
  - **Ransom demand**
  - **Legal**
  - **Forensic**
- Loss to data from computer system disruption
- Restoration costs
- **Crime:** cyber extortion, computer fraud, funds transfer fraud

First-Party Breach Response Costs

- Pre-claim counsel
- Notification expense
- Crisis management
- Computer forensics
- Credit monitoring
- Call center services

Fines and penalties

- Fees assessed by Payment Card Industry (PCI)
- Fees assessed by HIPAA/HITECH
- Fees assessed by state regulators

Insurance Coverage Options - Third Party

Third-Party Liability

- **Information Security and Privacy Liability**
    - Legal liability, defense costs and expense reimbursement for liability from unauthorized disclosure of PII/PHI or third party corporate information

- **Network Security Liability**
    - Failure of computer security to prevent a security breach

- **Website Media**
    - Liability for online media activities
    - Defamation, copyright infringement, infringement of trademark
    - May include offline media

- **Judgments / Settlements**
- **Defense costs – Litigation & Regulatory**

Cyber Endorsements to Package Policies

Liability limits are low

- $25,000 - $250,000

Narrow in scope

- Expense reimbursement only
- **No** coverage for data restoration
- **No** Business Interruption coverage
- Crisis management services to protect and rebuild the business's damaged reputation
- **No** coverage for regulatory fines and penalties
- **No** coverage for PCI fines and penalties
- **No** coverage for cyber extortion

Should have a stand-alone cyber policy

Ways to Help Minimize Risks

Have an Incident Response Plan in Place

- Know who is on the team (contact information, back-ups, etc.)
- Your cyber policy should be part of the documents shared amongst the team (remember, you may not have access to your documents if your system has been encrypted)

Take Advantage of Loss Mitigation Services:

- Online security courses for employees - New employees, as well as annual refresher courses
- Password defense and monitoring tools

Lawley

THANK YOU!