Cyber Attacks: From Notification to Financial Recovery

June 11, 2024 | Confidential

STOUT

Stout At a Glance

Firm Facts

30+ Years of delivering client success

Serving clients in 120+ countries across offices in North America, Asia, and Europe

Consistently recognized as a top U.S. fairness opinion provider since 2012[1]

Committed to building and sustaining a corporate culture that values diversity, equity, and inclusion

Our Clients

99 Advisor to 99 of the top Am Law 100 Law Firms[2]

70% Proportion of Fortune 500 with which we have worked[3]

67% Percentage of the top 100 private equity firms with which we have worked[4]

+90 Net Promoter Score[5] – a measure of our clients' willingness to recommend Stout's services

1 Based on the total number of deals reported by more than 20 companies since 2012 in LSEG's *Global M&A Financial Advisory Review* (formerly known as Refinitiv's *Global Mergers & Acquisitions*): 2 (2023), 1 (2022), 2 (2021), 1 (2020), 2 (2019), 2 (2018), 2 (2017), 3 (2016), 2 (2015), 1 (2014), 3 (2013), 1 (2012).
2 Proprietary analysis based on The American Lawyer's 2022 Top 100 Am Law firms
3 Proprietary analysis based on Fortune's 2022 list of the 500 largest U.S. corporations by total revenue
4 Proprietary analysis representing companies owned by the top 100 private equity firms based on aggregate capital raised in the preceding 10 years according to 2022 data provided by PitchBook
5 On a scale of -100 to +100 since 2016

ABOUT STOUT

Who We Are

Stout is a global advisory firm. Our clients and their advisors rely on our premier expertise, deep industry knowledge, and unparalleled responsiveness on complex matters.

Investment Banking & Restructuring

- M&A Advisory
- Capital Markets
- Corporate Recovery Services
- Special Situations & Distressed M&A
- Strategic Alternative Assessments

Transaction Advisory

- Due Diligence
- Transaction Opinions
- Integration & Separation
- IT M&A Services
- Interim Management
- Business Transformation
- Tax Advisory Services
- Transaction Accounting & Internal Controls

Valuation Advisory

- Corporate Tax Planning & Compliance
- ESOP Valuation & Opinions
- Financial Reporting
- Valuation Disputes
- Trust & Estate

Accounting & Reporting Advisory

- Accounting Advisory
- Accounting & Finance Operations
- Financial Statement Preparation & SEC Filings
- Public Company Readiness
- Risk Advisory

Disputes, Claims, & Investigations

- **Contract Compliance**
- **Expert Testimony & Consulting**
- **Claims**
- **Investigations**
- **Regulatory Compliance & Financial Crimes**

Specialty & Industry Services

- Automotive Component Defect & Recall Consulting
- Construction Services
- Digital & Data Analytics
- Employee Retention Credit Services
- Transformative Change Consulting

The Client Experience

Senior-level Attention

Access to senior-level talent on every project

High-quality, Consistent, On-time Deliverables

Detailed, firm-wide templates, established project processes, rigorous quality control and reviews ensure deliverables are high-quality, consistent, and on-time

Industry Expertise

Industry-specific coverage provides sector-specific knowledge and experience

A Proven Track Record

For over three decades, we have developed and supported opinions that withstand scrutiny – whether that be from the SEC, IRS, DOL, a trier of fact, an auditor review, or a counterparty

Nuanced & Flexible Approach

Approach includes the latest in financial and valuation theory and real-world market information

Responsive

We understand the critical importance of meeting reporting deadlines and do everything we can to ensure timelines, set expectations, and inform you of where we are every step of the way

WHY STOUT?

Claims Practice

$12B Assisted our clients in the recovery of more than $12 billion in policy proceeds, collectively.

40+ Dedicated practice includes more than 40 professionals, some of which average 20+ years of experience in managing complex claims solutions.

Cross-functional expertise in claims consulting and forensic accounting

Decades of experience, knowledge, relationships, and credibility in the insurance claims field

Collaborative approach working between client teams, brokerage teams, and counsel

Proven track record of optimized claim recovery amounts and timeliness of resolution

Value-added benefit of our services covered under professional fees or comparable claim preparation extensions in insurance policies

Claims

Stout offers deep experience working on behalf of policyholders to resolve complex claims with a focus on delivering tangible, measurable, and meaningful results.

Our Team

We have provided claim preparation services to clients across nearly all industry groups and served clients ranging from Fortune 50 multinational corporations to small businesses and government entities. We have helped to resolve some of the largest and most complex claims to hit insurance markets in the last 25 years.

Focus Practice Areas

- **Claim Preparation & Recovery Solutions**
- **Mass Torts**
- **Exposure Analytics & Liability Estimation**
- **Claims Administration & Advisory**

Experts In

- **Property Damage & Business Interruption**
- **Pollution**
- **Construction**
- **Cyber**
- **Asbestos, Environmental, & Health Hazards**
- **Sexual Abuse & Harassment**
- **Pharmaceutical & Medical Device**
- **Product Liability & Recall**

Cyber Trends

Cyber Attack Trends – Growing Risks

- According to the Identity Theft Resource Center there were 2,365 cyber attacks in 2023

- According to the IBM Cost of a Data Breach Report:
  - The average cost of a data breach in the US was $9.5 million
  - Data breaches impacting the healthcare and financial firms result in the highest average costs

- On average, companies take 204 days to identify and 73 days to contain a breach

- Increase in regulatory response:
  - SEC – New rule (effective Dec.18, 2023) requires public companies to disclose material cybersecurity incidents within four business days of the company's "materiality" determination
  - FDIC, OCC, and the Federal Reserve – The "New Rule" (effective April 1, 2022) requires banks to notify their primary federal regulators within 36 hours of determining a "notification incident" has occurred
  - CISA – Proposed rule (April 4, 2024) requires a covered a covered entity to submit a Covered Cyber Incident Report to CISA no later than 72 hours after the covered entity reasonably believes the covered cyber incident has occurred

Cyber Attack Trends – The Good News

- There are activities that you can undertake now to mitigate potential impacts!

Source: IBM Cost of a Data Breach Report

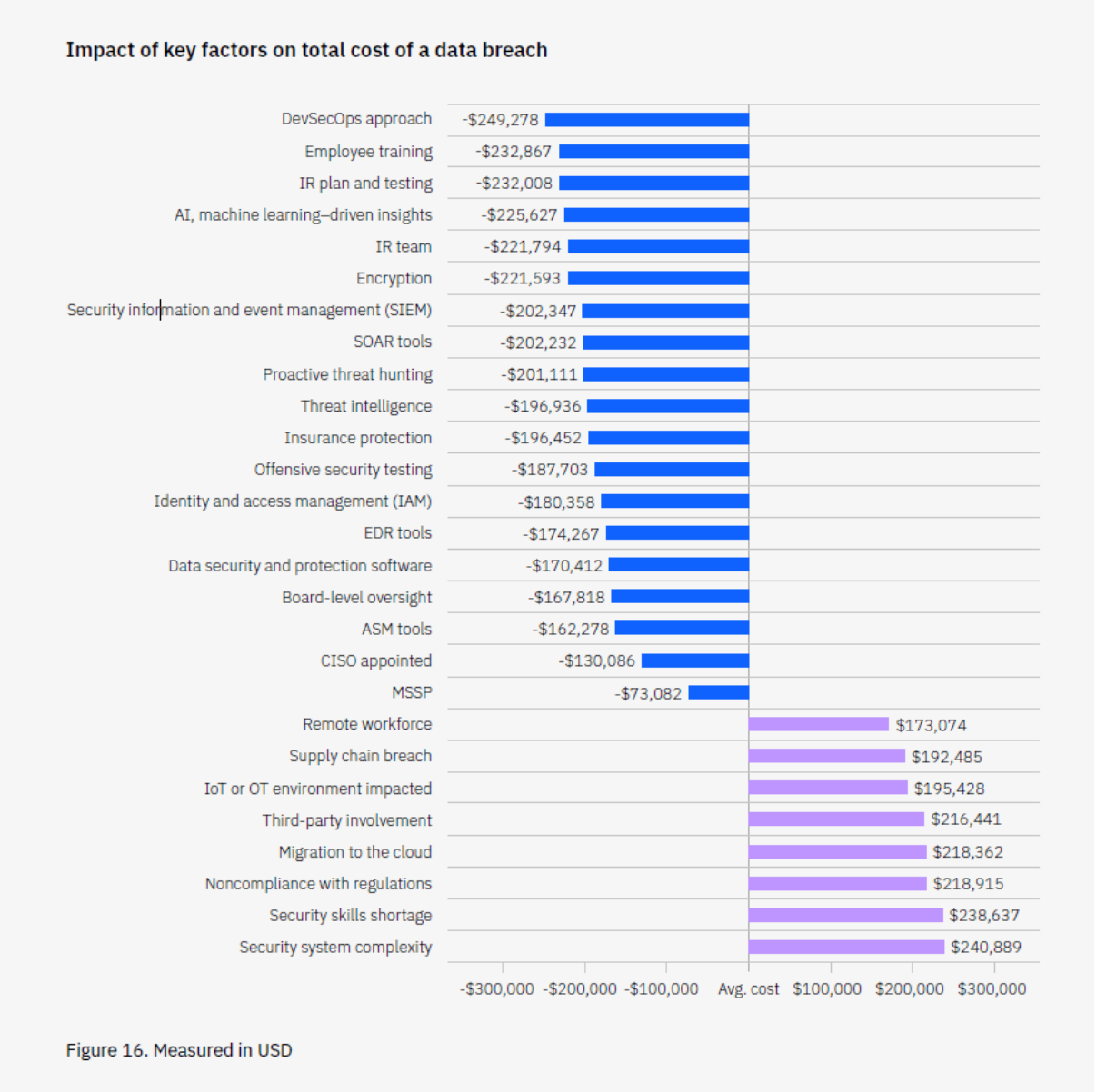


Figure 16. Measured in USD

Business Continuity Planning (BCP)

BCP: What role does it play?

- **Proactive Process** – anticipate potential threats, vulnerabilities & weaknesses
  - Bolster's bank's resilience during crisis
  - Reduce losses
  - Maintain business operations despite disruptions
  - Reduce risk of reputational damage and regulatory non-compliance

- **Core function:**
  - Addresses all banking operations
  - Trains employees to manage disruptions
  - Ensures uninterrupted service to customers / retain market position

- **Four stages:**
  - Mitigation
  - Preparedness
  - Response
  - Recovery

BCP: What is the regulatory environment?

Position and Guidance:

Federal Reserve – Business Continuity Resource Center

- https://www.frbservices.org/resources/resource-centers/business-continuity

FDIC – Financial Institution Letter (Nov. 2019)

- https://www.fdic.gov/sites/default/files/2024-03/fil19071.pdf

FFIEC Business Continuity Management (BCM)

- https://www.ffiec.gov/press/pr111419.htm
- https://ithandbook.ffiec.gov/media/2nifgh2b/ffiec_itbooklet_businesscontinuitymanagement_v3.pdf

BCP: What are the key components?

NOTE: There is no "one size fits all"!

Managerial Protocols – this is the foundation of your BCP, outlining what needs to happen before, during and after disruption (regardless of the type of disaster)

Plan Objectives – every plan is unique and must clearly state its scope

Risk Assessment – to adequately plan for a disaster/disruption, you must understand what the disaster/disruption looks like

Business Impact Analysis – this is a critical component because it uncovers the most urgent threats and enables prioritization

Prevention Strategies – not all disaster/disruption can be prevented, but it is important to identify the steps you are actively taking to prevent disruption

Disaster Response – these are the immediate steps following a disruption in order to assess the situation and determine most appropriate path to recovery

BCP: What are the key components?

NOTE: There is no "one size fits all"!

Recovery Protocols – the immediate response does not always result in full recovery, so it is important to identify additional protocols that will be needed for full recovery

Data Backup and Recovery – financial institutions must be aggressive in deploying technologies that thwart cyber attacks and accelerate recovery

Contingency Planning – it is important to have a "Plan B" for all aspects of operations

Training & Education – it is essential that all staff be trained on BCP/DR (i.e. how to safely use email/internet, identify phishing attempts and what to do in ransomware attack)

Communications – it is critical to maintain clear communications between affected stakeholders

BCP Writing, Testing and Reevaluation – it is a multi-functional effort, written and evaluated by several stakeholders across your organization

**See Appendix for extended version (47-50)*

Case Studies

NetScaler Compromise: Failure to Patch

Background:

On or about July 18th, 2023, Citrix released an advisory and a patch to address a vulnerability in their NetScaler appliances. On July 20th, 2023, CISA released an advisory detailing attacker activity related to the deployment of web shells on NetScaler appliances. The most recent intelligence indicates that the attackers studied the CISA advisory and altered their tactics to circumvent the recommendations. Unfortunately, this change in attacker methodology was used to help the attackers become even more covert in their attacks, thereby making it more difficult to detect their presence (past or present).
It is believed that the number of exploited NetScaler appliances is in the thousands. To be clear, this estimate is not of the number of "vulnerable" appliances, but rather those systems which have been exploited by attackers.

The current recommendations are that if you have not patched your NetScaler prior to July 20th, you should assume you are compromised and act accordingly.
As of this TAC-ALERT there are 8,000 IPs with vulnerable NetScaler's worldwide

Assessment:

This is considered a critical threat against healthcare organizations, and swift action is required. The importance of patching NetScaler appliances cannot be overstated. One of the most recent concerns related to this attack is that a complete proof of concept has been made available on the internet (see image below).

NetScaler Compromise: Failure to Patch

- Incident Response (immediate)
  - CISO alert to internal team (IT, Legal, Compliance)
  - Align resources and alert:
    - Cyber carrier
    - Outside counsel
    - Forensic services
  - Communications:
    - Forensics 24/7 and CISO/IT until resolution
    - Daily cadence with incident response team
    - Internal messaging to executive leadership and Board
  - Resolution and post-mortem:
    - Forensic Report
    - Legal/Compliance – privacy impact review
    - IT mitigation – patch process
    - Communicate resolution to internal stakeholders

CISA: Insider Threat Mitigation
https://www.cisa.gov/topics/physical-security/insider-threat-mitigation

Bank of America: Third-Party Breach/Ransomware

Notice received:

Re: Notice of Data Breach

Dear [Participant first and last name]:

We are writing to you about a security incident at Infosys McCamish Systems LLC ("IMS"). IMS provides services for deferred compensation plans, including plans serviced by Bank of America that you were eligible to participate in. Out of an abundance of caution, we are notifying you about this incident and providing tools to help you protect against possible identity theft or fraud.

What Happened: On or around November 3, 2023, IMS was impacted by a cybersecurity event when an unauthorized third party accessed IMS systems, resulting in the non-availability of certain IMS applications. On November 24, 2023, IMS told Bank of America that data concerning deferred compensation plans serviced by Bank of America may have been compromised. Bank of America's systems were not compromised.

In response to the security incident, IMS retained a third-party forensic firm to investigate and assist with IMS's recovery plan, which included containing and remediating malicious activity, rebuilding systems, and enhancing response capabilities. To date, IMS has found no evidence of continued threat actor access, tooling, or persistence in the IMS environment.

What Information Was Involved: It is unlikely that we will be able to determine with certainty what personal information was accessed as a result of this incident at IMS. According to our records, deferred compensation plan information may have included your first and last name, address, business email address, date of birth, Social Security number, and other account information.

What We Are Doing: Although we are not aware of any misuse involving your information, we are notifying you that Bank of America will provide a **complimentary** two-year membership in an identity theft protection service provided by Experian IdentityWorks℠. **You will not be billed for this service, but you must enroll for activation.** This product provides you with daily monitoring of your credit reports from the three national credit reporting companies (Experian, Equifax® and TransUnion®), internet surveillance, and resolution of identity theft. **This service will expire at the conclusion of the complimentary period and will not automatically renew.** Any renewal of service elected by you and paid by you should be done directly through Experian IdentityWorks℠. To enroll, go to https://www.experianidworks.com/bac/ or call Experian IdentityWorks℠ at [enter TFN]. You will need **the activation code and engagement number provided below to complete enrollment.**

Your Activation Code: **Activation Code**
You Must Enroll By: **Expiration Date**
Engagement number: **Engagement Number**

Bank of America: Third-Party Breach/Ransomware

- Financial Software Provider (Nov.3, 2023)
- Impacted 57,028 BOA customers (name, address, SSN, account info)
- Ransomware group – LockBit (2,000 systems encrypted)
- Notification and credit monitoring provided 90 days post-breach (30-day requirement with grace for investigation time)
- Impacted customers – deferred comp plans serviced by BOA
- Liability is a “gray area” – highlighted “gaps” that need to be filled by banks as it relates to 3rd parties (security measures/risk assessment/contract provisions)

Cyber Headlines

"On Feb. 21, Change Healthcare, a subsidiary of UnitedHealth Group, was the victim of the most significant and consequential cyberattack on the U.S. health care system in American history. Change Healthcare is the predominant source of more than 100 critical functions that keep the health care system operating." (*Letter from AMA to US House*)

Cyberattack on Change Healthcare brings turmoil to healthcare operations nationwide

Lawmakers grill UHG CEO at hearings following Change Healthcare cyberattack

Change Healthcare cyberattack was due to a lack of multifactor authentication, UnitedHealth CEO says

Notification

Notification: What is the regulatory environment?

Position and Guidance:

- FDIC, OCC, and the Federal Reserve – The "New Rule" (effective April 1, 2022)
  - The Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers
    - https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20211118a1.pdf
  - Interagency Guidance on Response Programs
    - https://www.fdic.gov/regulations/laws/rules/2000-50.html

- CISA – Proposed "72 Hr Rule": Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) (April 4, 2024 proposed by DHS)
  - A covered entity must submit a Covered Cyber Incident Report to CISA no later than 72 hours after the covered entity reasonably believes the covered cyber incident has occurred
  - https://www.federalregister.gov/documents/2024/04/04/2024-06526/cyber-incident-reporting-for-critical-infrastructure-act-circia-reporting-requirements

Notification: What is the requirement & rationale?

- **Two Primary Elements:**
  - Banks must notify their primary federal regulators within 36 hours of determining a “notification incident” has occurred
  - Bank service providers, subject to the Bank Service Company Act (BSCA), must notify their affected customers as soon as possible when an incident occurs which may cause a disruption for four or more hours
- **Rationale:**
  - Timeliness – provides early awareness of emerging threats and a better position from which to assess the risk of an incident
  - Scope – expands beyond the traditional scope of a data breach and highlights to any type of computer-security incident which could result in “actual harm”
  - Improved Oversight – real-time assessment allowing agencies to implement more effective guidance

Notification: How do you define an incident?

- **Computer Security Incident:**
  "An incident that results in *actual* harm to the confidentiality, integrity, or availability of an information system or the information that the system processes, stores, or transmits." Does not require notification to the agency unless it is a "notification incident"

- **Notification Incident:**
  "A computer-security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, a banking organization's:
  - Ability to carry out banking operations, activities, or processes, or deliver banking products and services to a material portion of its customer base
  - Business line(s), including associated operations, services, functions, and support, that upon failure would result in a material loss of revenue, profit, or franchise value; or
  - Operations, including associated services, functions and support, as applicable, the failure or discontinuance of which would pose a threat to the financial stability of the U.S."

Notification: How do you define an incident?

- **Bank Service Provider Incident:**

  "A computer-security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, covered services provided to such banking organization for four (4) or more hours."

This type of notification allows banks time to determine if the incident experienced by the BSP would also be classified as a "notification incident" for the bank. BSP's must notify their impacted customers "as soon as possible" when they determine they are experiencing this type of incident.

NOTE* Beyond regulatory notification requirements, it is crucial to first alert your internal Incident Response Team as well as all third-parties (cyber insurance carrier, outside counsel, and forensic services). All third-parties should be vetted and engaged as part of your Business Continuity Planning.

Notification: Who should be notified?

The agencies require the bank to notify "the appropriate agency supervisory office or other designated agency contacts”

FDIC:

- FDIC Case Manager
- Any member of an FDIC examination team
- Email: incident@fdic.gov

https://www.fdic.gov/news/financial-institution-letters/2022/fil22012.html

FRB:

- Email: incident@frb.gov
- Phone: (866) 364-0096

https://www.federalreserve.gov/supervisionreg/srletters/SR2204.htm

OCC:

- The bank’s supervisory office
- The BankNet homepage: https://www.banknet.gov/entrance/default.html
- The BankNet Help Desk
  - Email: BankNet@occ.treas.gov
  - Phone: (800) 641-5925

https://www.occ.gov/news-issuances/bulletins/2022/bulletin-2022-8.html

Notification: What must be in the notification?

- **Spirit and intent of notification:**
  - "Early alert"
  - The rule does not describe contents of notification
  - Additional information will likely be requested to determine the impact of the incident and may conduct a review
  - Cybersecurity incidents are chronically underreported (reference)

Cyber Insurance

What risks does cyber insurance cover?

Cyber Insurance Coverage typically includes:

- First-party losses – Losses incurred directly by the business, including:
  - Legal counsel (Breach counsel)
  - Lost or stolen data recovery and replacement
  - Customer notification and call center services
  - Lost income due to business interruption (focus for today)
  - Reputational harm
  - Crisis management and public relations
  - Cyber extortion and fraud potentially including ransom payments
  - Forensic services
  - Restoring personal identities of affected customers
  - Repairing damaged computer systems
- Third-party losses - Losses suffered by other businesses due to a relationship with the affected organization, including:
  - Investigation and defense costs
  - Civil damages
  - Compensation payments to affected parties
  - Settlements
  - Court judgments

What is Business Interruption for Cyber losses?

- Cyber insurance coverage commonly separate from commercial property insurance policies.
  - Cyber business interruption is for loss of income and extra expenses following a Data Breach or Security Breach or System Failure to insured business.

- Measurement of business income loss is tied to a period of time.
  - Period of Restoration (see next slide)

- Basic categories of coverage:
  - Business Interruption (loss of income)
  - Extra Expense (expenses above normal)

What is Business Interruption for Cyber losses?

- "Period of restoration" typically defined to begin on the actual and necessary interruption of the Insured business operations as a result of a Data Breach or Security Breach or System Failure, and typically ends on the earlier of:

  1) the date when the business should be restored, rebuilt or replaced with reasonable speed and similar quality; or

  2) the date when business is actually resumed.

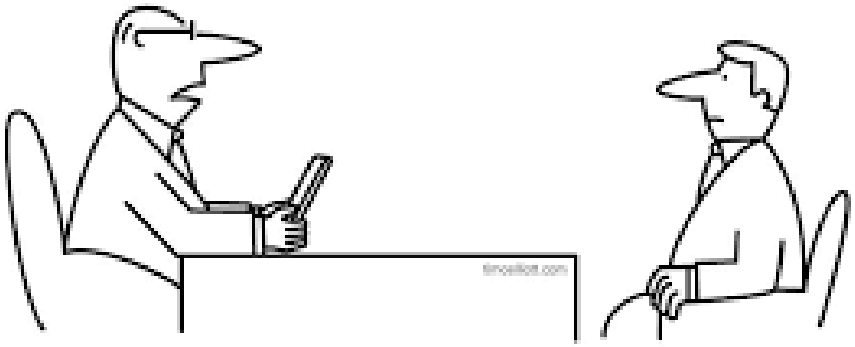
- Date when the business "should be restored" is typically measured by an objective test and is not dependent on when the insured actually completed the restoration.

Extra Expense and Expenses to Reduce Loss

- Sample policy language
  - Extra Expense means reasonable and necessary expenses incurred by the Insured Organization during the Period of Restoration to minimize, reduce or avoid Income Loss, over and above those expenses the Insured Organization would have incurred had no Security Breach, System Failure, Dependent Security Breach or Dependent System Failure occurred.
- Clear intent of language is to encourage the client to mitigate the BI loss
- Expense to Reduce Loss has financial test to overcome

Business Interruption

- Measuring business interruption losses is complicated…
  - Many variables to consider in establishing a realistic measure of how the business would have performed if no loss had occurred
    - Historical performance and trends, peer performance, forecasts, seasonality, weather, data anomalies etc…
- Certain variable expenses may necessarily continue during the interruption of business
  - Franchise, management, national adverting and various other fees may be owed on business interruption insurance proceeds



"No, I'm afraid we can't 'just make the data up' —this is business, not politics..."

Case Study – Payment Card Processor

- American payment card processing company.
- Company processes approximately 3.5 billion transactions for ~$200 billion annually.
- Customers include 200,000 businesses in the retail, hospitality, leisure and restaurant industries.
- On a Saturday night in August 2021, suffered a significant multi-hour outage of its payment system, which merchants (customers) were unable to process credit and debit card transactions.
- Months after the event company still suffered the impact to its business and the resulting losses and reputational damages from this outage.

Case Study – Payment Card Processor

- Cyber outage affected customers at the busiest point in the week when the most transactions are processed: Saturday evenings are the peak time for their businesses.
- Impact was felt by some of its largest merchants hosting live events.
  - Most venues are now “completely cashless”
  - Attendees unable to use credit cards to purchase food and beverages and merchandise during outage
- Impacted third parties included MLB, WWE, NFL and many other merchants large and small.

Case Study – Payment Card Processor

- Calls from merchants big and small unable to process credit cards rose exponentially during this period resulting in hold times in excess of one hour.
- Throughout the outage and after the outage, merchants demanded compensation, threatened to sue, threatened to post on social media, and threatened to terminate their contracts.
- Client faced monumental and increasing losses not only from lost revenue due to the outage, but also the significant impact arising from lost customers and reputational damage if merchants cancelled contracts or posted negatively on social media.

Case Study – Payment Card Processor

- Client communicated with its merchants regarding potential mitigation payments attributable to the impact from the outage.
  - We helped client utilize a modeling process to determine the relative impacts to each merchant. Many merchants accepted payment of the amount identified.
- Other merchants disputed the amounts through a vetting process client established, which required more analysis of the claimed impact to validate and determine the appropriate payment.
  - Client eventually reached agreements with these merchants.
- Had client not immediately taken mitigation action with its merchants, the demands from merchants would have been exponentially higher and the damage to the business more significant.
- All payments to merchants were recorded as contra revenue, which is reflected as a reduction of client “Gross revenue.”

Adjustment Process

How can you be prepared?

- Work with team and advisors to make sure the cyber policy aligns with your business interests and risk transfer objectives
- Confirm that limits and reported values are current and accurate
- Ensure that team understands sublimits, deductibles and exclusions that may apply for different types of losses

Claims – Tips & Takeaways

- Read your policy to determine how coverage may apply to the losses your organization is experiencing
  - Be relentless about documenting your loss
  - Establish dedicated G/L codes to track all claim related costs and expenses
  - Communicate protocols and procedures to documenting losses and incremental expenditures
  - Audit claim G/L to ensure that relevant costs are being captured

- Ask for help
  - Assemble a cross-functional team of experts to support the organization through the claims process
  - Internal: Risk management, finance, operations, legal
  - External: Broker advocate, forensic accountant, technical consultants, coverage counsel

- Take a proactive approach to managing your claim
  - Be responsive to all “reasonable” carrier/adjuster/forensic accountant requests
  - Prepare and periodically submit claim submission and support packages
  - Demand interim payment for the undisputed elements of the claim

*See Appendix for First Party Claims Checklist (51)

Concluding Thoughts

Concluding Thoughts

Banking trends:

- AI revolution in banking and financial services – redefining how banks interact with customers and secure transactions
- Embedded finance and open banking – making banking more accessible, personalized and efficient
- Cloud-based banking – makes banks quicker and more creative
- Blockchain and cryptocurrencies – new perspectives on traditional banking and will play a pivotal role in the future

Cybersecurity:

- The push to digital is unceasing. Customers are demanding not just services, but the digital experience.
- Cybersecurity is foundational both in current state and in the future in order to protect customer data and financial systems.
- As digital banking and AI evolve, the volume and sophistication of cyber threats will increase.

Cyber Insurance Trends:

- Coverage forms are not consistent across insurers and are evolving over time.
- Insurers are raising numerous coverage defenses including exclusions, betterment and unrealistic hypotheticals
- Success requires common sense and flexibility

Joe Tess

Managing Director, Claims

Joe is a Managing Director in Stout's Dispute, Claims and Investigations practice. Joe has over 20 years of experience specializing in forensic accounting, expert testimony, litigation support and complex claims consulting.

Joe has extensive experience analyzing complex financial and economic issues related to commercial disputes and transactions. Joe has assisted clients and their counsel with business interruption calculations, cyber insurance claims, forensic accounting, damages quantification, insurance allocation modeling, mass tort claim estimations, decision modeling, and developing negotiation/settlement strategies.

Joe's clients include leading public and private corporations and many Fortune 500 companies in a wide range of industries, including ecommerce, oil and gas, energy generation and distribution, healthcare, chemical production, hospitability, renewable energy, paints and coatings and manufacturing working directly with executive level employees, internal and external counsel, auditors, brokers and outside stakeholders.

Prior to joining Stout, Joe was a Managing Director and founding member at The Claro Group. Prior to Claro Joe worked in Insurance Claims Consulting practice at LECG

Practice Areas

First Party Claim Preparation & Recovery Solutions | Legacy Long-Tail Liability Claims | Mass Torts | Exposure Analytics & Liability Estimation | Complex Business Litigation | Risk Management Consulting |

Industry Focus

Manufacturing | Energy & Power Generation | Consumer/Ecommerce | Healthcare | Industrials | Hospitality/Leisure | Food Processing | Defense Contracting | Technology | Technology | Chemicals |

Education

M.B.A., Accounting, Economics Finance and Organizational Behavior
University of Chicago

B. S., Finance and Operations Management, Indiana University

Contact
Office: +1.312.546.3416
Mobile: +1.708.574.7861
jtess@stout.com
Chicago

Hillary Harlan

Managing Director, Disputes, Claims, & Investigations

Hillary Harlan is a Managing Director in the Disputes, Claims, & Investigations group. Her specialties include regulatory compliance, complex claims and reimbursement, analysis, litigation support, investigations, and monitorships. Her clients include healthcare entities, providers, payors, and law firms.

Ms. Harlan has served at the executive level as VP Chief Compliance Officer, with oversight for regulatory compliance with an emphasis on HIPAA Privacy and Security, False Claims, Stark, Anti-kickback / Anti-referral, and fraud, waste, and abuse. Additionally, she has had executive oversight for risk management, governance, and legal services.

Ms. Harlan has experience in acute care, long-term care, ambulatory care, home health and hospice, pharmacy (inpatient and retail), healthcare technology, and healthcare merger and acquisition.

Prior to joining Stout, Ms. Harlan served an executive role for the third largest health system in Western Pennsylvania, where she facilitated the merger of two community health systems (five hospitals and over 1,000 employed providers). Ms. Harlan has also served an executive compliance role with McKesson, Inc. (Business Performance Services), which provided third-party revenue cycle management, claims adjudication, third-party administration services, proprietary technology, and physician management services (MSO).

Education

B.A. English
Southern Methodist University

B. S. Nursing
Texas Tech University

J.D. Law
Texas Tech University School of Law

Contact
Office: +1.267.571.5411
Mobile: +1.214.908.1158
hharlan@stout.com
Philadelphia, PA

Appendix

Business Continuity Planning

- **Managerial Protocols** – this is the foundation of your BCP, outlining what needs to happen before, during and after disruption (regardless of the type of disaster)
  - Who does the decision making in emergency situation?
  - What are the "mission critical" responsibilities of each executive and manager?
  - What are the protocols for personnel in each department?
  - Who needs to do what to restore operations?
- **Plan Objectives** – every plan is unique and must clearly state its scope
  - What does the plan aim to achieve?
  - Is the plan relevant to all banking operations or a specific department?
  - What is the core purpose of the plan?
  - What are the limitations of the plan?
  - Are additional documents needed?
- **Risk Assessment** – to adequately plan for a disaster/disruption, you must understand what the disaster/disruption looks like
  - What operational risks does the organization face?
  - Which threats have greatest likelihood?
  - What are the causes of each threat?
  - What does each disaster/disruption scenario look like?

Business Continuity Planning

- **Business Impact Analysis –** this is a critical component because it uncovers the most urgent threats and enables prioritization
  - How does each threat actually disrupt the bank's operations?
  - What is the immediate and long-term impact?
  - What is the anticipated length of time for each disruption?
  - What is the cost?
- **Prevention Strategies –** not all disaster/disruption can be prevented, but it is important to identify the steps you are actively taking to prevent disruption
  - What technologies are in place to prevent cyber attacks?
  - What systems are implemented to block malicious files from entering the network?
  - How adequate are your data backup and recovery systems?
  - Are your bank branches built to withstand various natural disasters?

Business Continuity Planning

- **Disaster Response –** these are the immediate steps following a disruption in order to assess the situation and determine most appropriate path to recovery
  - How should disruptions be evaluated to determine what actually happened and what happens next?
  - Which banking services are highest priority if limitations are in place?
  - What protocols are in place if technological roadblocks prevent access to systems?
  - If staffing has been affected, what are the minimum staffing requirements required to maintain operations?
- **Recovery Protocols –** the immediate response does not always result in full recovery, so it is important to identify additional protocols that will be needed for full recovery
  - What steps should be followed to fully restore operations?
  - Which aspects of the business take priority if several operations are disrupted?
  - Who will oversee the recovery for each type of disaster/disruption? To whom will they provide updates/
  - What are the recovery objectives and expectations?
  - How long is each type of recovery expected to take?

Business Continuity Planning

- **Data Backup and Recovery –** financial institutions must be aggressive in deploying technologies that thwart cyber attacks and accelerate recovery
  - What is the bank's primary business continuity and disaster recovery system?
  - Which data recovery methods should be used (i.e. ransomware, accidental deletion, hardware failure, etc.)?
  - What is the bank's recovery time objective (RTO)?
  - How long should it take to recover lost data or systems?
- **Contingency Planning –** it is important to have a "Plan B" for all aspects of operations
  - What if sensitive data was stolen in a cyber attack and held at ransom?
  - What happens if the physical bank location was destroyed in a disaster?
  - What if a third-party service provider is unavailable and are disrupting your operations (i.e. technology provider, utilities, ATM access providers, etc.)
  - What if additional hardware is suddenly needed for a branch location?
- **Training & Education –** it is essential that all staff be trained on BCP/DR (i.e. how to safely use email/internet, identify phishing attempts and what to do in ransomware attack)
  - What types of training are needed to achieve continuity objectives?
  - How often does the training occur and how is it deployed?
  - Who receives the training?
  - Who develops and tracks the training?

Business Continuity Planning

- **Communications –** it is critical to maintain clear communications between affected stakeholders
  - Which methods will be used to maintain communications after a disaster?
  - Which personnel will need emergency devices (i.e. cell phones) and how will that process work?
  - Will the public need to be provided updates (i.e. press release, PR, etc)
- **BCP Writing, Testing and Reevaluation –** it is a multi-functional effort, written and evaluated by several stakeholders across your organization
  - Who is in charge of maintaining your BCP?
  - How often should it be reviewed?
  - Who has access to the BCP documentation and/or management software?
  - How will the plan be tested?
  - How will you know that the protocols are effective?

First Party Claims Checklist

- ✓ Work with broker to tender notice of loss to all potentially impacted carriers pursuant to the requirements of your policy
- ✓ Assemble claims team to support the organization through the claims process, which may include internal personnel (risk management, finance, operations, legal) as well as external resources (broker advocate, forensic accountant, technical consultants, coverage counsel)
- ✓ Establish dedicated accounting codes to track all claim related costs and expenses
- ✓ Review and understand all duties and deadlines under your policy
- ✓ Track all time your employees spend on claim-related activities (i.e., billing backlog claims, reconciling advance payments, etc.)
- ✓ Collect information necessary to prepare a preliminary proof of loss
- ✓ Maintain copies of communications from customers and suppliers regarding issues that may impact your bottom line
- ✓ Document all operational and financial impacts on timeline, include supporting documentation as appropriate
- ✓ Prepare and submit a business interruption claim that conforms to the valuation provisions of your policy
- ✓ Develop a claim narrative that explains how the loss event has impacted your ability to conduct business
- ✓ Request advance payments as necessary
- ✓ Continually update claim estimates; distinguish incurred costs and realized losses from estimated future costs/losses
- ✓ Respond to all reasonable requests made by the carrier(s), adjuster, and forensic accountants to avoid delays in the adjustment process