CYBER EXPOSURES

THREAT LANDSCAPE | RISKS & EXPOSURES

DATA RISK

PERSONALLY IDENTIFIABLE INFORMATION (PII)
Social security numbers, drivers license numbers, bank account information, online account user names, passwords and health insurance information.

PROTECTED HEALTH INFORMATION (PHI)
Any information about health status, provision of health care, or payment for health care that can be linked to a specific individual.

PAYMENT CARD INFORMATION (PCI)
Debit and credit card information such as the primary account number, cardholder name, expiration date and service code.

CONFIDENTIAL CORPORATE INFORMATION
Confidential information entrusted by third-parties, oftentimes subject to non-disclosure or confidentiality agreements.

OPERATIONAL RISK

Data Loss & Extortion

Computer Forensics Expenses
Cyber Extortion / Ransomware Payments
Data loss and Restoration

SOCIAL ENGINEERING & INVOICE MANIPULATION

Fraudulent instructions inducing employees to wire funds
Disguised communications posing as **YOU** inducing customers

BUSINESS INTERRUPTION / DEPENDENT BI

Malicious attack or system failure affecting **YOUR** network
Malicious attack or system failure affecting a **DEPENDENT PROVIDER**
Oftentimes a result of **RANSOMWARE** attacks

CYBER POLICY

Structure

CYBER POLICY STRUCTURE | GENERAL COVERAGES

BREACH COSTS
Covers forensic costs to identify and confirm the breach, notification costs, credit protection services fees, crisis management and public relations costs.

CYBER BUSINESS INTERRUPTION
Covers financial loss, such as business income when network-dependent revenue is interrupted.
*Coverage variations discussed further

DATA RESTORATION
Covers the costs to recreate or repair damaged or destroyed data, systems or programs.

PRIVACY & NETWORK SECURITY
Covers defense costs, judgements, settlements, and regulatory fines/penalties arising from network security and data breach events.

CYBER EXTORTION
Covers the response costs and financial payments associated with network-based ransom demands.

MULTIMEDIA LIABILITY
Covers the costs to defend and resolve claims related to online content, such as copyright / trademark infringement.

CYBER POLICY STRUCTURE I ADDITIONAL COVERAGES

SYSTEM FAILURE
Non-malicious trigger business interruption coverage.

DEPENDENT SYSTEM FAILURE
Non-malicious trigger business interruption coverage for an event at a dependent IT provider.

DEPENDENT BUSINESS INTERRUPTION
Malicious event triggers a business interruption event at a dependent IT provider (cloud/ hosting, software, etc.).

SOCIAL ENGINEERING
Ensure no call-backs, check for coverage of 'other property' and scope of who's funds are covered.

CLIENT ACCOUNT/INVOICE MANIPULATION COVERAGE
Third-party social engineering coverage triggered by fraudulent invoices being sent from insured's e-mail.

FUNDS HELD IN ESCROW (SOCIAL ENGINEERING / PHISHING)
Some policy forms only cover 'your' funds, not the funds of others in your possession.

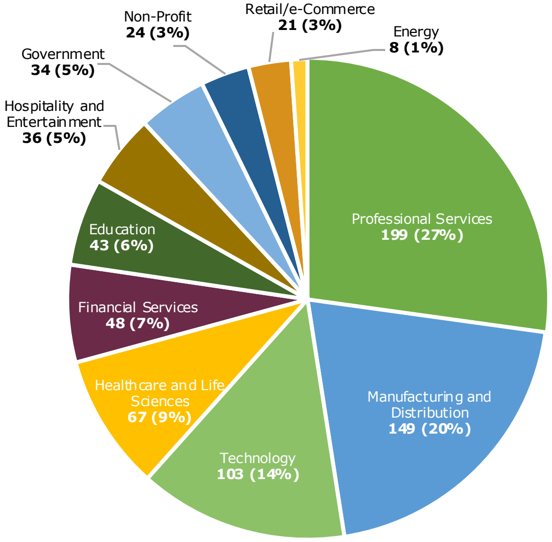
UTILITY FRAUD
Telephone toll fraud, Cryptojacking; Unauthorized use of your systems.

Non-Breach Data Laws
Newer coverage available to cover claims arising from the misuse of data, rather than the breach of data (CCPA).

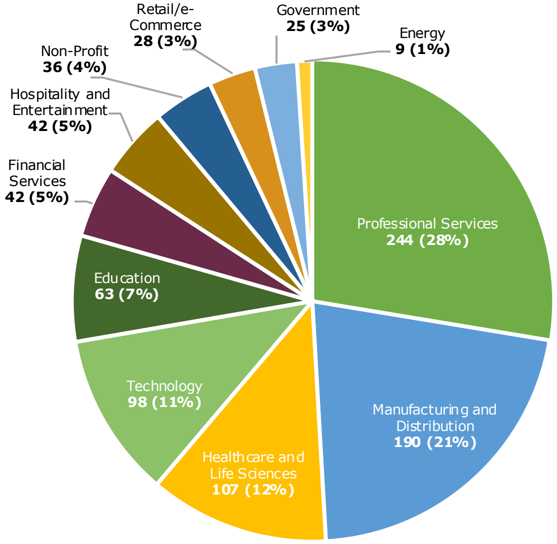
THE COST OF RISK

THE COST OF RISK | RANSOMWARE INCIDENTS

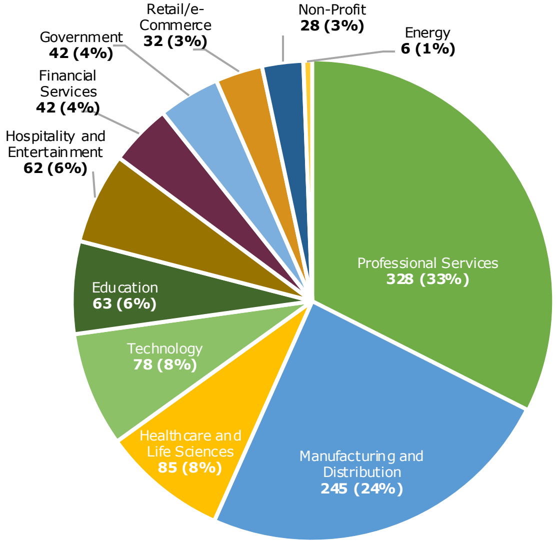
2022	
Number of RW Incidents	732 (25%)
Number of RW Incidents Paid	97 (13%)
Average Ransom Demand	$2,272,682
Average Ransom Payment	$400,791
Median Ransom Payment	$150,000
Ransom Payment Reason	Delete Only – 21 (22%) Key and Delete – 39 (40%) Key Only – 37 (38%)



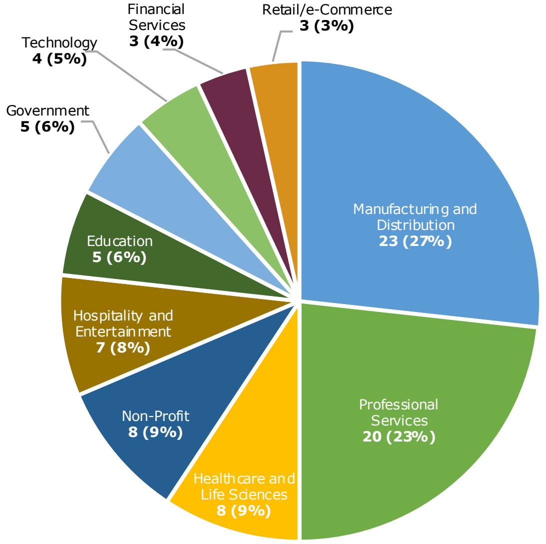
2023	
Number of RW Incidents	884 (23%)
Number of RW Incidents Paid	138 (16%)
Average Ransom Demand	$2,243,227
Average Ransom Payment	$937,751
Median Ransom Payment	$200,000
Ransom Payment Reason	Delete Only – 42 (30%) Key and Delete – 56 (41%) Key Only – 40 (29%)



2024	
Number of RW Incidents	1,011 (24%)
Number of RW Incidents Paid	133 (13%)
Average Ransom Demand	$1,890,232
Average Ransom Payment	$519,395
Median Ransom Payment	$265,065
Ransom Payment Reason	Delete Only – 53 (40%) Key and Delete – 49 (37%) Key Only – 31 (23%)



2025 (through Jan.)	
Number of RW Incidents	86 (18%)
Number of RW Incidents Paid	3 (3%)
Average Ransom Demand	$965,455
Average Ransom Payment	$130,000
Median Ransom Payment	$130,000
Ransom Payment Reason	Delete Only – 0 (0%) Key and Delete – 1 (33%) Key Only – 2 (67%)



*Data courtesy of Mullen Coughlin, LLC – www.mullen.law

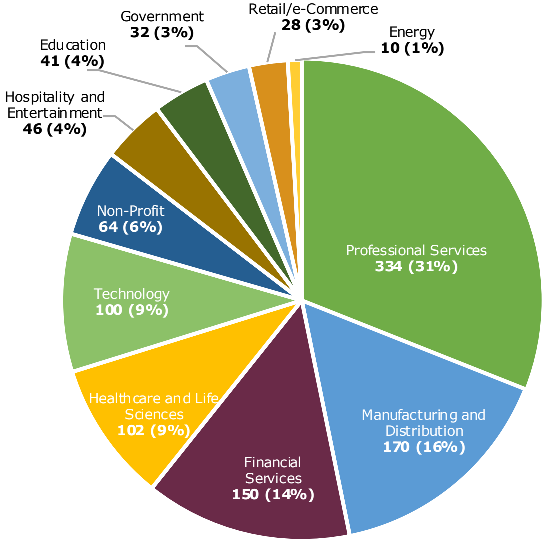
THE COST OF RISK | BUSINESS EMAIL COMPROMISE INCIDENTS

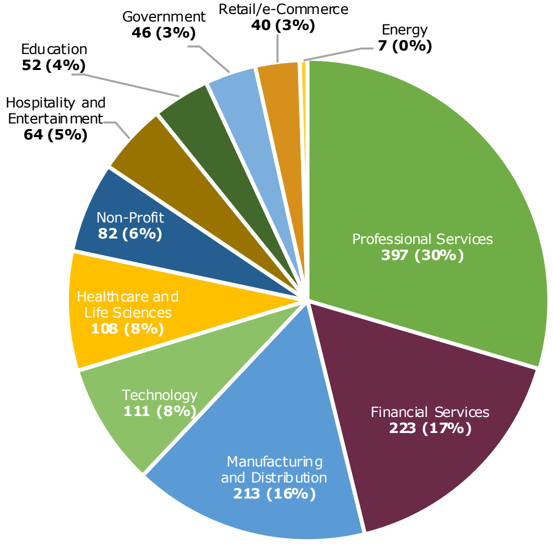
2022	
Number of BEC Incidents	1,077 (36%)
Number of BEC-WF Incidents	344 (32%)
Average Amount Fraudulently Wired	$376,234
Median Amount Fraudulently Wired	$145,000

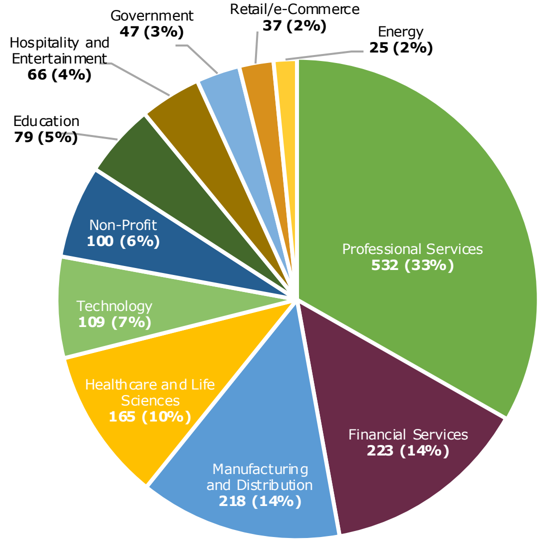
2023	
Number of BEC Incidents	1,343 (34%)
Number of BEC-WF Incidents	347 (26%)
Average Amount Fraudulently Wired	$824,704
Median Amount Fraudulently Wired	$148,867

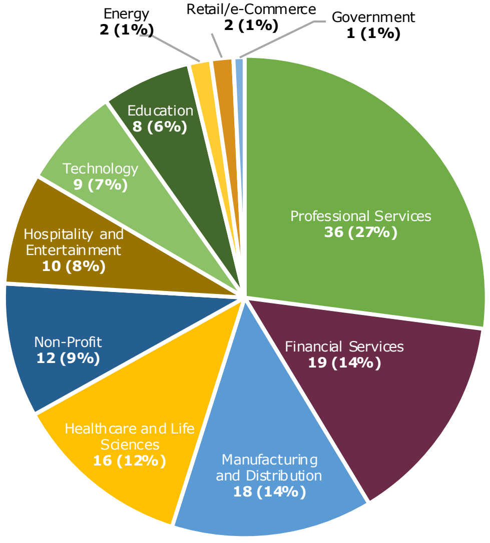
2024	
Number of BEC Incidents	1,601 (38%)
Number of BEC-WF Incidents	377 (24%)
Average Amount Fraudulently Wired	$442,961
Median Amount Fraudulently Wired	$154,622

2025 (through Jan.)	
Number of BEC Incidents	133 (28%)
Number of BEC-WF Incidents	32 (24%)
Average Amount Fraudulently Wired	$312,231
Median Amount Fraudulently Wired	$130,000









*Data courtesy of Mullen Coughlin, LLC – www.mullen.law

Fraud Coverages (Cyber Policies)

Social Engineering, Invoice Manipulation Fraud, Funds Transfer Fraud

Insured's 'voluntary parting of title'

Insured's computer system utilized to deceive a vendor or client into paying a fraudulent invoice

Threat actor utilizes insured's system to issue a funds transfer instruction to a financial institution

*No Employee Theft

Expanded Coverages

Customer Funds

Physical Property

Control Group or Employee Funds

Frequent Exclusions

- No coverage will be available for loss in-excess of $50,000, unless the transferring, payment or delivery of Money or Securities is made
  - By a Control Group Member
  - By an Employee, agent, or independent contractor or other representative of the Insured after receiving Official Authorization from:
    - A Control Group Member
    - An Employee acting in a supervisory capacity
- Computer Fraud Costs means the amount fraudulently obtained from the insured. Computer fraud costs include the direct financial loss only.
  - Computer fraud costs do not include any portion of such amount that can reasonably be expected to be reimbursed by a third party
- Fraudulent Instruction means the transfer, payment or delivery of Money or Securities by an Insured as a result of fraudulent written, electronic, telegraphic, cable, teletype or telephone instructions provided by a third party, that is intended to mislead an Insured through the misrepresentation of a material fact which is relied upon in good faith by such Insured.

- Fraudulent Instruction will not include loss arising out of fraudulent instructions received by the Insured which are not first authenticated via a method other than the original means of request to verify the authenticity or validity of the request
- Any Claim based upon, arising from or in any way involving the giving or surrendering of Money, Securities or Other Property in any exchange for or purchase of goods or services that are not yet delivered, whether fraudulent or not.

Definitions:

- Computer Crimes (definition in lieu of Invoice Manipulation) means the intentional, fraudulent, or unauthorized input, destruction, or modification of electronic data or computer instructions into Computer Systems by an entity which is not an Insured Organization or person who is not an Insured Person.
- Invoice Costs means the direct net cost incurred by the Insured Organization to provide or transfer goods, products or services to a third party.

Mutually Repugnant Exclusions

Crime & Cyber will both have some version of an "Other Insurance" exclusion

"this Policy will be excess over and will not contribute with any other valid and collectible insurance providing any other coverage afforded under this Policy, unless such other insurance is specifically written as excess over this policy"

COMMON MISCONCEPTIONS | SAMPLE CLOUD CONTRACT TERMS

16. DISCLAIMERS.

(A) all goods and services are provided “as-is”. Except as expressly required by law without the possibility of contractual waiver, we and our service suppliers and licensors disclaim all warranties, express and implied, including the warranties of merchantability, fitness for a particular purpose, non-infringement, title, and any warranties arising from a course of dealing, usage or trade practice. You are solely responsible for the suitability of all goods and services chosen and for determining whether they meet your capacity, performance and scalability needs.

(B) we and our service suppliers and licensors do not warrant that the cloud services will be uninterrupted, error-free, completely secure, or that all defects will be corrected. You acknowledge that we do not control or monitor the transfer of data over the internet, and that internet accessibility carries with it the risk that your privacy, confidential information and property may be lost or compromised.

17. LIMITATION OF DAMAGES.

Except as expressly required by law without the possibility of contractual waiver (a) neither we nor any of our employees, agents, representatives, service suppliers, or licensors, will be liable for any punitive, indirect, consequential or special damages, or for any lost profits, lost data, lost business, lost revenues, damage to goodwill, lost opportunities or loss of anticipated savings, even if advised of the possibility of same, and regardless of whether the claims are based in contract, tort, strict liability, infringement, or any other legal or equitable theory; and (b) the aggregate liability of us and our employees, agents and representatives to you under any theory of **liability, whether in contract, tort, strict liability or otherwise, will not exceed the total amount you actually paid to us for the cloud services.**

CYBER SECURITY| INCIDENT RESPONSE STAKEHOLDERS

The Victim Organization

Cyber Insurance Carrier/Broker

Incident Response Counsel ("Breach Coach")

Other Insurance Policy Carriers/Brokers
(*e.g.*, K&R, Property, Crime, Etc.)

Law Enforcement

Financial Institution(s)

Forensic Investigation and System Restoration Firm(s)

Extortion, Negotiation and Payment Firm(s)

Data Mining Firm(s)

Other Legal Counsel
(Depending on Specific Data Impacted and Applicable Regulatory Framework)

Public Relations Firm(s)

Notice Mailing and Call Center Provider(s)

Credit/Identity Monitoring Services

Insured Business Partners

CYBER SECURITY| POTENTIAL INCIDENT RESPONSE ROADMAP