Cyber Reporting, Claim Handling, and Incident Response Made Simple

The Hartford

Jennifer Birnbaum, Cyber Underwriting Officer

Daniel Silverman, Underwriting Director, Specialized CyberTech

Keith Tagliaferri, Director, Cyber Claim Practices

Jennifer Droesch, Head of Global Specialty E&O Claims

Laurie Mandell, Director of Claims, Financial Lines , Cyber and Tech

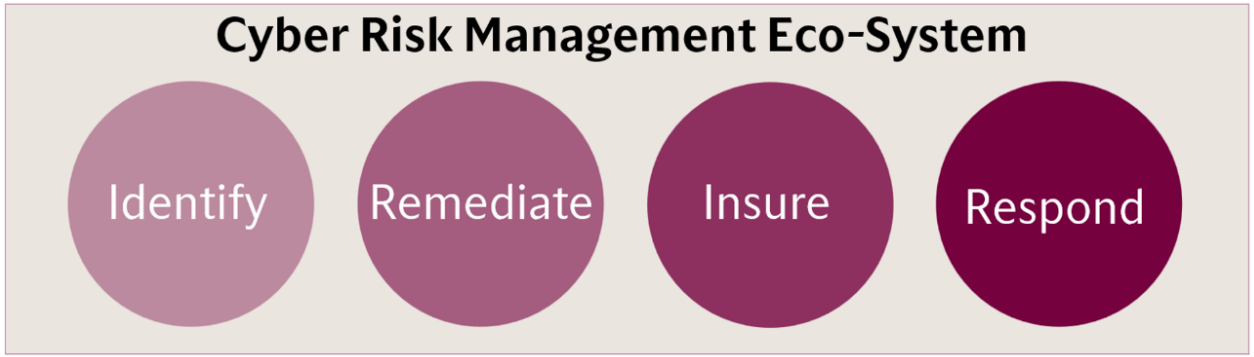
Mullen Coughlin

Jennifer Coughlin, Founding Partner, Mullen Coughlin

February 24, 2026

Our Role – CyberTech Insurance & Risk Management

The Hartford



Agenda

Topic	Discussion Leads
Introduction	Jennifer Birnbaum Dan Silverman Keith Tagliaferri
The Hartford's 24/7 Cyber Claims Hotline and Team	Jennifer Droesch Laurie Mandell
The Hartford's CyberChoice First Responders	Keith Tagliaferri
Incident Response Players & Roadmap	Jennifer Coughlin
Q&A	

Hartford's 24/7 Cyber Claims Hotline

The Hartford's 24/7 Cyber Claims Hotline will guide you through the initial steps to take after a breach, and help you navigate through the incident response and recovery processes, whether or not your claim is compensable.

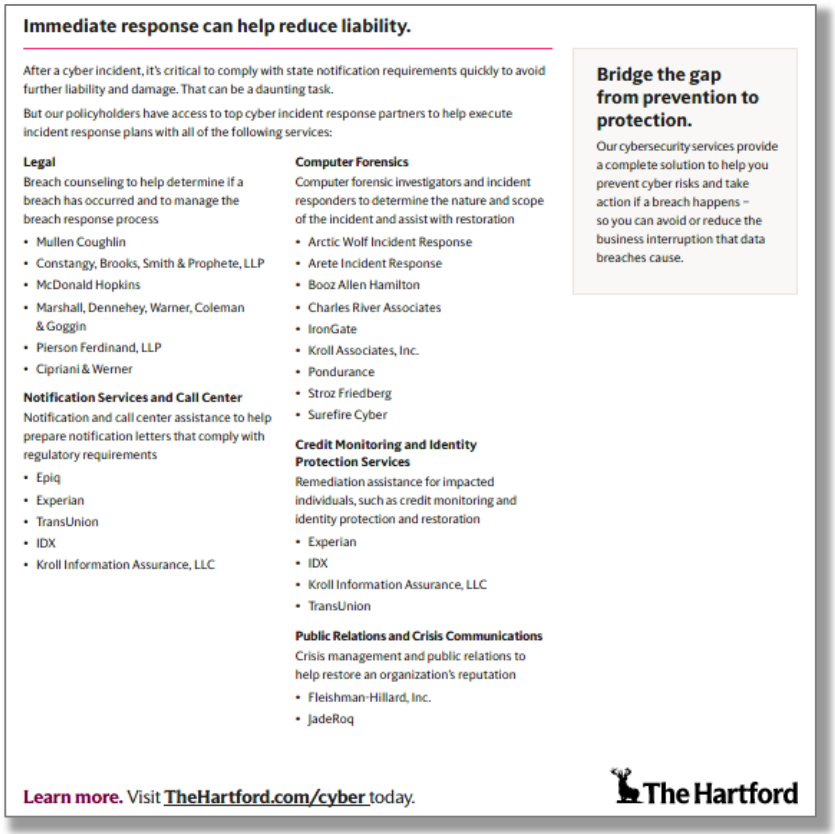
After a breach or other incident, contact these resources immediately:

FirstResponse Hotline: **800-370-0605**

FirstResponse Email:
FirstResponse@thehartford.com

The Hartford's CyberChoice First Responders®

The Hartford provides insureds with a dedicated panel of cyber and breach response professionals to deliver expert support throughout the full incident response lifecycle, referred to as our **CyberChoice First Responders®**.



Immediate response can help reduce liability.

After a cyber incident, it's critical to comply with state notification requirements quickly to avoid further liability and damage. That can be a daunting task.

But our policyholders have access to top cyber incident response partners to help execute incident response plans with all of the following services:

Legal
Breach counseling to help determine if a breach has occurred and to manage the breach response process

- Mullen Coughlin
- Constangy, Brooks, Smith & Prophete, LLP
- McDonald Hopkins
- Marshall, Dennehey, Warner, Coleman & Goggin
- Pierson Ferdinand, LLP
- Cipriani & Werner

Notification Services and Call Center
Notification and call center assistance to help prepare notification letters that comply with regulatory requirements

- Epiq
- Experian
- TransUnion
- IDX
- Kroll Information Assurance, LLC

Computer Forensics
Computer forensic investigators and incident responders to determine the nature and scope of the incident and assist with restoration

- Arctic Wolf Incident Response
- Arete Incident Response
- Booz Allen Hamilton
- Charles River Associates
- IronGate
- Kroll Associates, Inc.
- Pondurance
- Stroz Friedberg
- Surefire Cyber

Credit Monitoring and Identity Protection Services
Remediation assistance for impacted individuals, such as credit monitoring and identity protection and restoration

- Experian
- IDX
- Kroll Information Assurance, LLC
- TransUnion

Public Relations and Crisis Communications
Crisis management and public relations to help restore an organization's reputation

- Fleishman-Hillard, Inc.
- JadeRoq

Bridge the gap from prevention to protection.

Our cybersecurity services provide a complete solution to help you prevent cyber risks and take action if a breach happens – so you can avoid or reduce the business interruption that data breaches cause.

Learn more. Visit TheHartford.com/cyber today.

The Hartford

Questions?

Disclaimer

The information provided in these materials is intended to be general and advisory in nature. It shall not be considered legal advice. The Hartford does not warrant that the implementation of any view or recommendation contained herein will: (i) result in the elimination of any unsafe conditions at your business locations or with respect to your business operations; or (ii) be an appropriate legal or business practice. The Hartford assumes no responsibility for the control or correction of hazards or legal compliance with respect to your business practices, and the views and recommendations contained herein shall not constitute our undertaking, on your behalf or for the benefit of others, to determine or warrant that your business premises, locations or operations are safe or healthful, or are in compliance with any law, rule or regulation. Readers seeking to resolve specific safety, legal or business issues or concerns related to the information provided in these materials should consult their safety consultant, attorney or business advisors. All information and representations contained herein are as of February 2026.

Incident Response

Presented by:

Jennifer A. Coughlin, *Managing Member* – Mullen Coughlin LLC

February 24, 2026

Mullen Coughlin Incident Statistics
2023-2025

Incident Type

Incident Type	2023		2024		2025	
Business Email Compromise (BEC)	1,343	34%	1,601	38%	1,666	39%
BEC – Other	996		1,224		1,266	
BEC – Wire Fraud	347		377		400	
Ransomware	883	23%	1,011	24%	1,134	26%
Vendor Breach	749	19%	747	18%	59	14%
Other	403	10%	346	8%	36	9%
Network Intrusion	323	8%	322	7%	343	8%
Inadvertent Disclosure	218	6%	228	5%	188	4%
Total	***3,919***	***100%***	***4,255***	***100%***	***4,291***	***100%***

Industry Sector

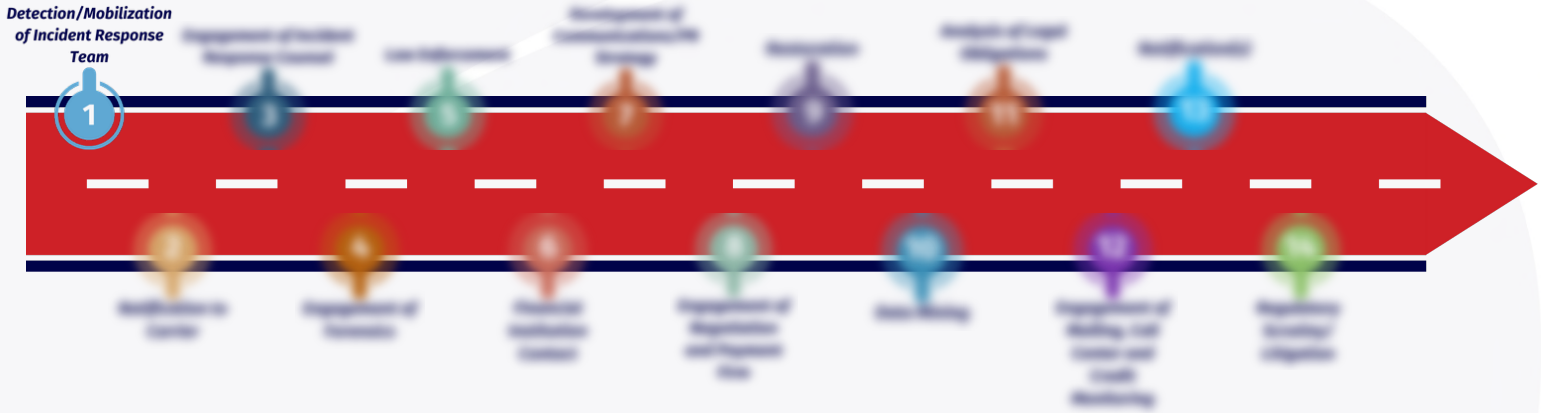
Industry Sector	2023		2024		2025	
Professional Services	928	24%	1,241	29%	1,175	27%
Manufacturing and Distribution	538	14%	563	13%	628	15%
Healthcare and Life Sciences	571	15%	656	15%	496	11%
Financial Services	588	15%	488	11%	500	12%
Technology	372	9%	342	8%	399	9%
Education	245	6%	241	6%	381	9%
Non-Profit	208	5%	212	5%	237	6%
Hospitality and Entertainment	169	4%	194	5%	166	4%
Government	138	4%	155	4%	139	3%
Retail/e-Commerce	130	3%	112	3%	126	3%
Energy	32	1%	51	1%	44	1%
Total	***3,919***	***100%***	***4,255***	***100%***	***4,291***	***100%***

RW & BEC Incidents

Ransomware Incidents	2023	2024	2025
RW Incidents	883 23%	1,011 24%	1,134 26%
RW Incidents Paid	156 18%	161 16%	132 12%
Avg. Ransom Demand	$2,180,723	$1,755,468	$1,131,559
Avg. Ransom Payment	$818,177	$452,530	$469,525
Median Ransom Payment	$192,278	$220,000	$150,000
Ransom Payment Re	D: 50 32%	D: 66 41%	D: 47 36% [illegible]% [illegible]%

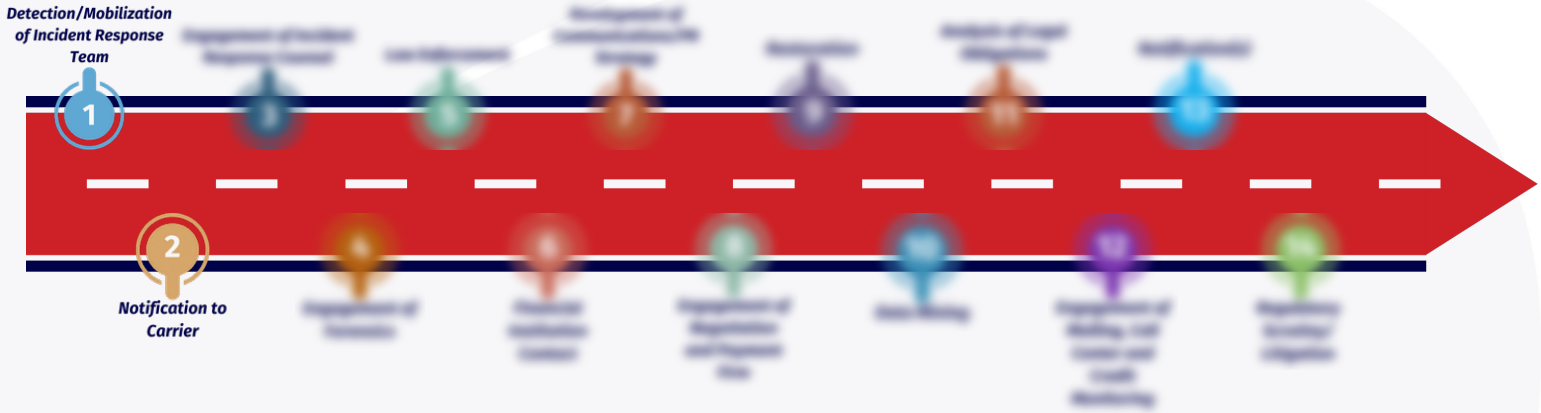
BEC Incidents	2023	2024	2025
BEC / BEC - WF Incidents	1,343 34%	1,601 38%	1,666 39%
BEC – WF Incidents	347 26%	377 24%	400 24%
Avg. Fraudulently Wired	$824,704	$442,961	$796,942
Median Fraudulently Wired	$148,867	$154,622	$114,000

Incident Response Players & Roadmap



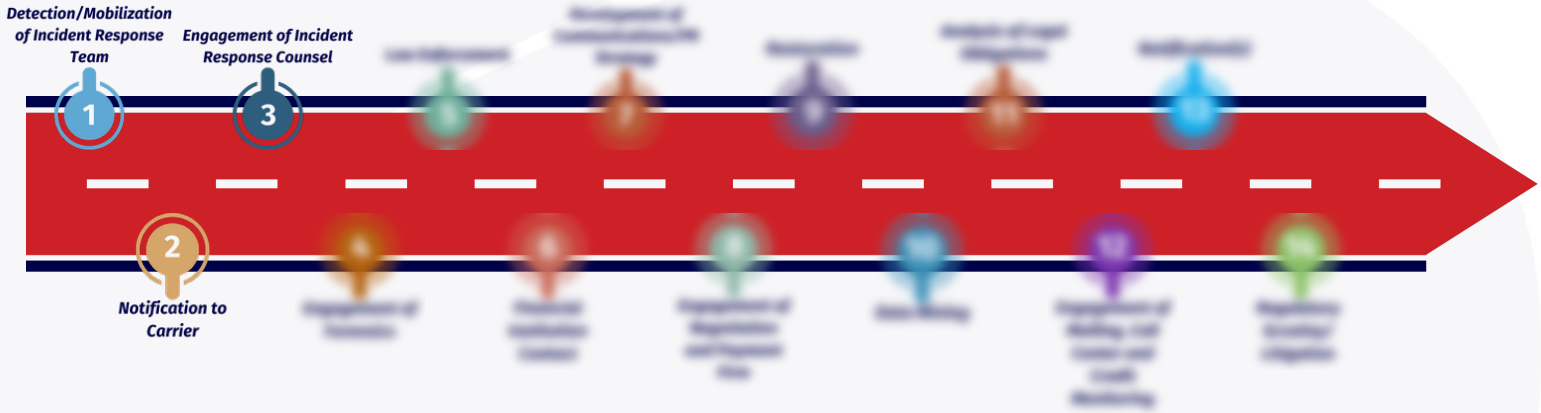
1. Detection/Mobilization of Incident Response Team

- Organizations should develop – and routinely test – an Incident Response Plan, which identifies the internal and certain external stakeholders responsible for investigation and response to incident and responsibilities of each team member. This plan must include the contact information for the organization's cyber insurance carrier.
- Notably, detection of the incident may occur via internal and/or external sources.



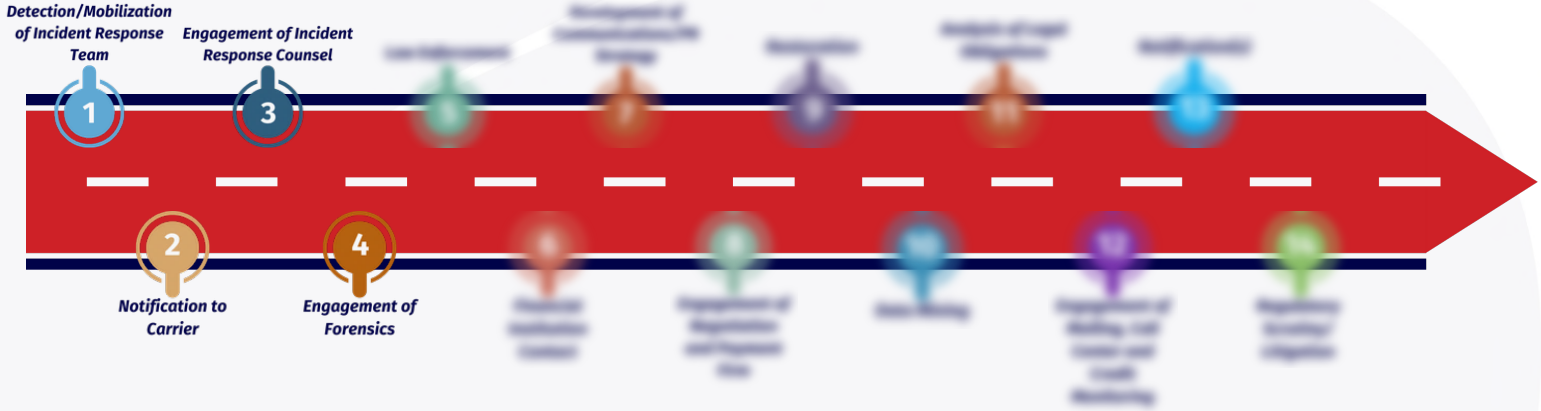
2. Notification to Carrier

- The organization's Incident Response Plan must include the contact information for the organization's cyber insurance carrier.
- The Hartford provides a toll-free hotline and email address for use in reporting cyber claims; however, if there is any concern regarding the security of an organization's email application and to ensure quick response, a call is recommended.



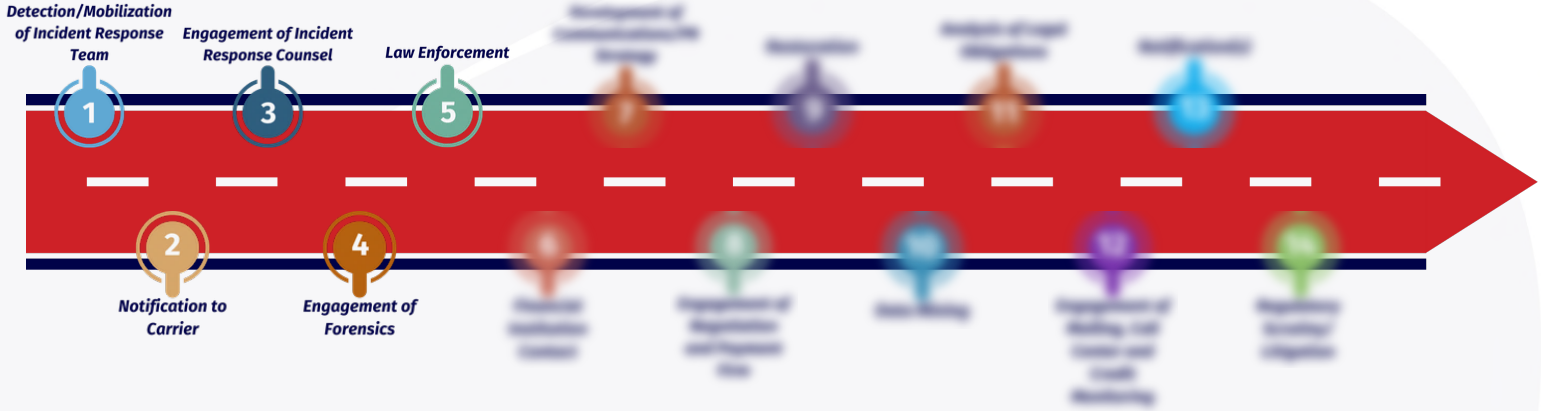
3. Engagement of Incident Response Counsel

- The Hartford has a panel of approved providers, including incident response counsel.
- Engagement of experienced and approved counsel at the outset of a matter is strongly encouraged for several reasons, including but not limited to, the protection of information and communications in attorney/client privilege (where applicable); the development of incident response strategy by an experienced party; and the identification of appropriate vendors to support the incident response process.



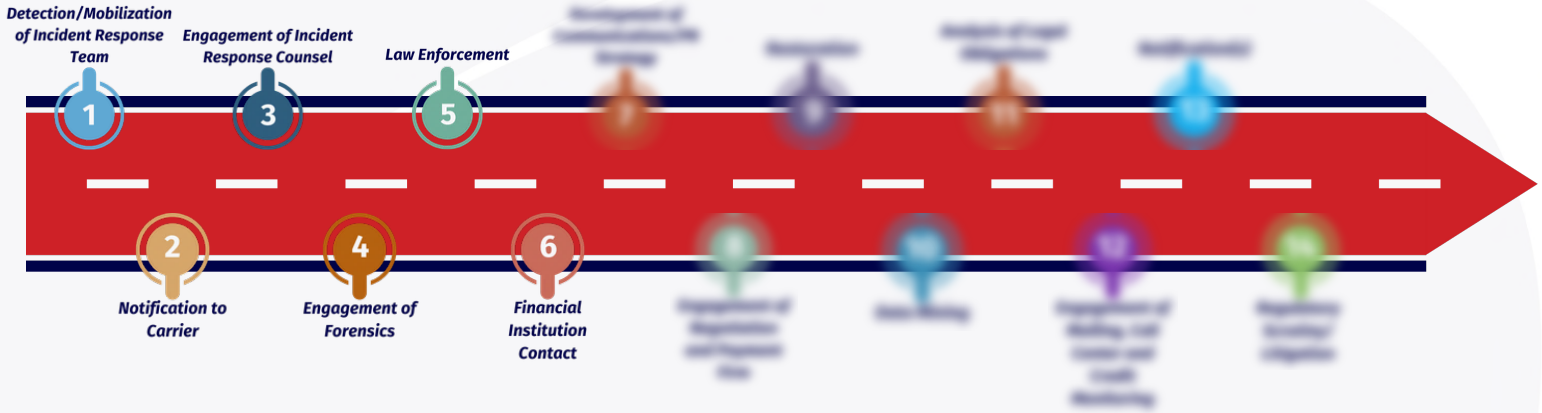
4. Engagement of Forensics

- The Hartford has a panel of approved providers, including forensics.
- Forensics is engaged by counsel and the insured, and works at the direction of counsel.
- Forensics will assist in identifying the nature and scope of the incident, including how the incident happened, whether it is ongoing, and what information may be at risk as a result of the incident.



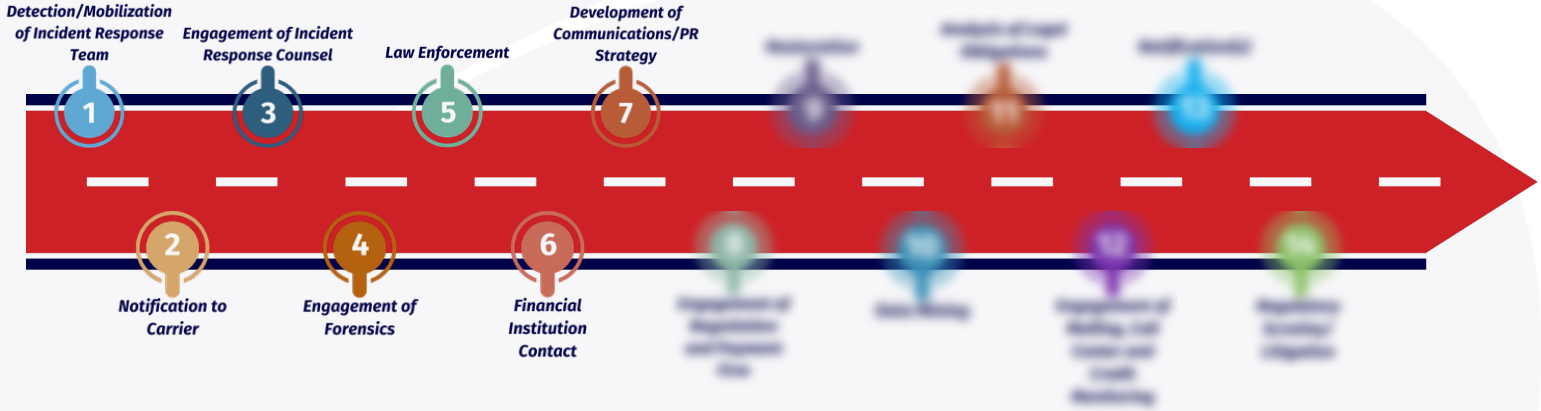
5. Law Enforcement

- Law enforcement is a key stakeholder in the incident response.
- The agency to contact will be determined, in part, by the type of incident, industry sector of the insured, and location of incident/fraudulent activity.



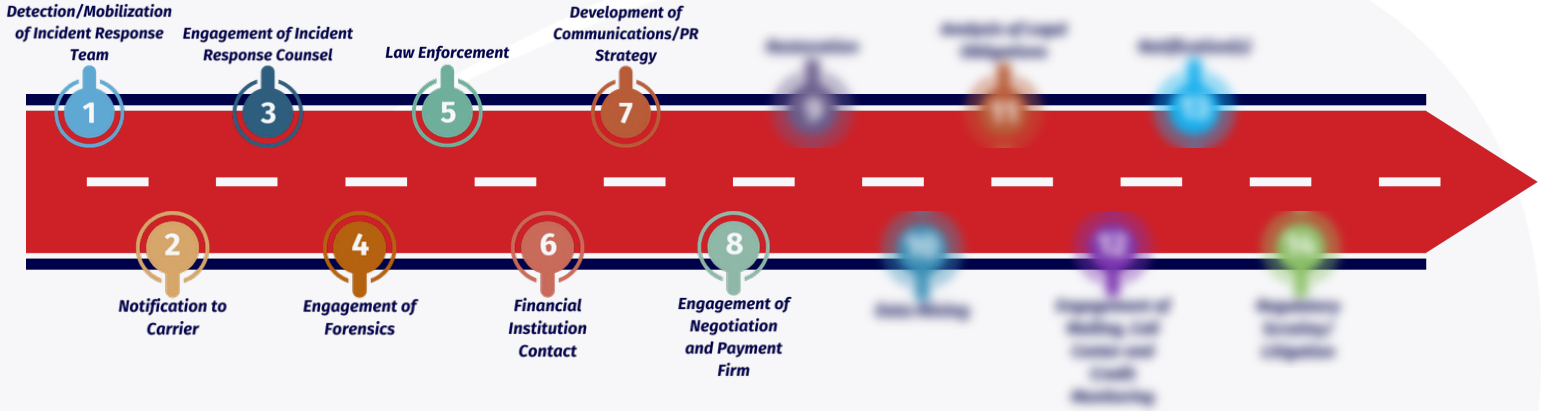
6. Financial Institution Contact

- If dealing with a wire fraud matter, early communication must be made to the wiring financial institution and receiving financial institution in an effort to freeze and recover funds before being released to a fraudster. The wiring and receiving financial institutions may have information helpful to the investigation, as well.



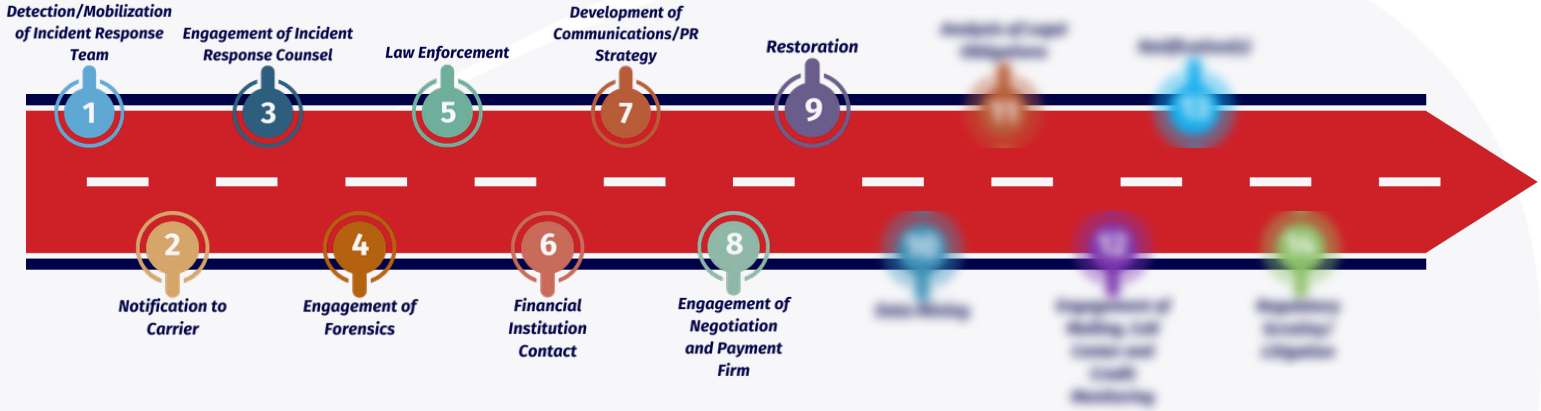
7. Development of Communications/PR Strategy

- When dealing with an incident, an organization must identify and prepare a communications strategy for all potential audiences. This includes, but is not limited to, current and former employees, business partners, customers/clients/patients, the media, regulators, and other third-parties.
- Incident Response Counsel relies upon their experience to develop communications strategy for use in matters; however, in certain circumstances, a public relations firm may be engaged to assist in the communications strategy development and execution.
- The Hartford has a panel of approved providers, including public relations firms. The public relations firm is engaged by counsel and the insured, and works at the direction of counsel.



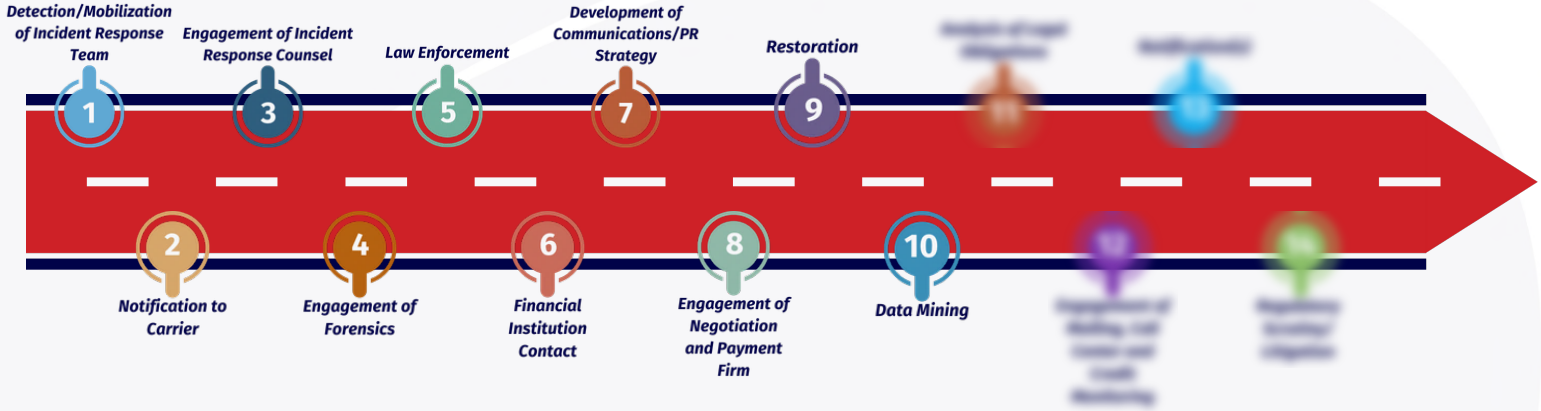
8. Engagement of Negotiation and Payment Firm

- If it is an extortion event, there may be a need to communicate with the threat actor claiming responsibility for the incident. Needs to negotiate and pay the threat actor may arise, as well.
- Many forensic firms provide these services; however, in instances where they do not, another party is engaged by counsel and the insured to provide these services.
- Payment to a threat actor cannot occur unless it is in compliance with OFAC and other laws/regulations/guidances.



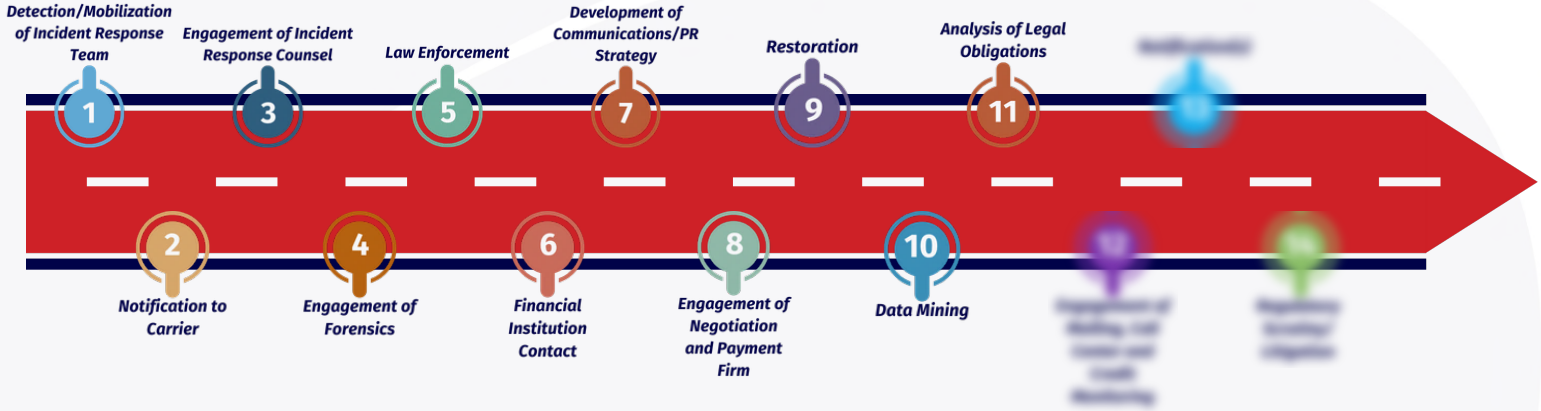
9. Restoration

- In encryption events, part or all of an insured's network may be encrypted and inoperable. Organizations may restore operations via recovery from a back-up or deployment of a decryption tool.
- Insureds may have capacity to utilize internal resources for restoration activity; however, a third-party is sometimes necessary to support or complete the restoration efforts.
- May forensic firms provide these services; however, in instances where they do not, another party is engaged by counsel and the insured to provide these services.



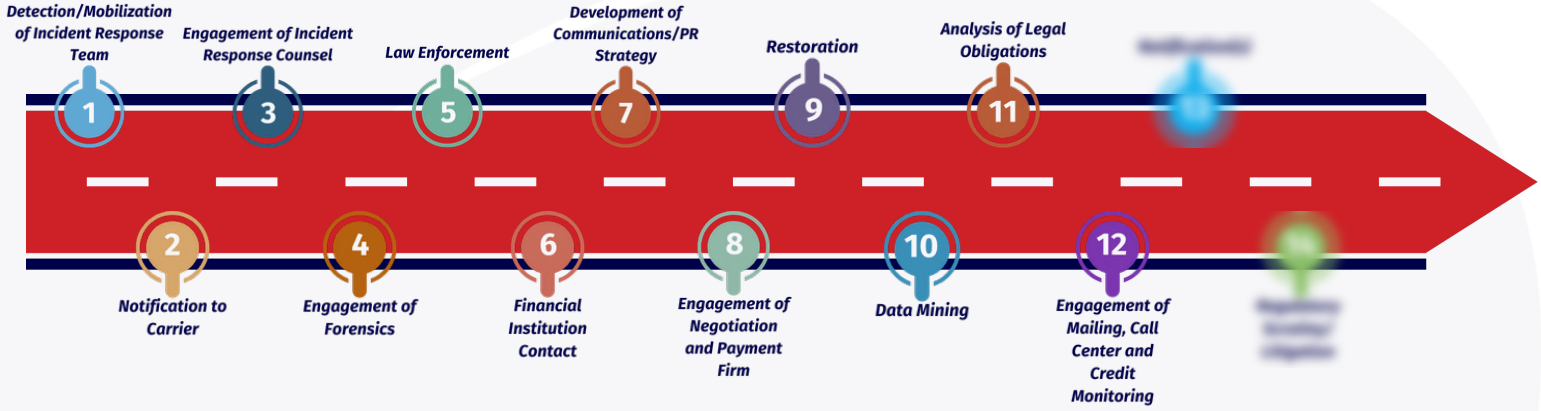
10. Data Mining

- In matters where data is or may have been subject to unauthorized access or acquisition, the victim organization must identify precisely what data may be at risk as a result of the incident.
- In instances where the impacted data set is voluminous or the client is unable to identify the data via internal resources, a third-party is engaged to provide these services via programmatic and manual review.
- Many forensic firms provide these services; however, in instances where they do not, another party is engaged by counsel and the insured to provide these services.



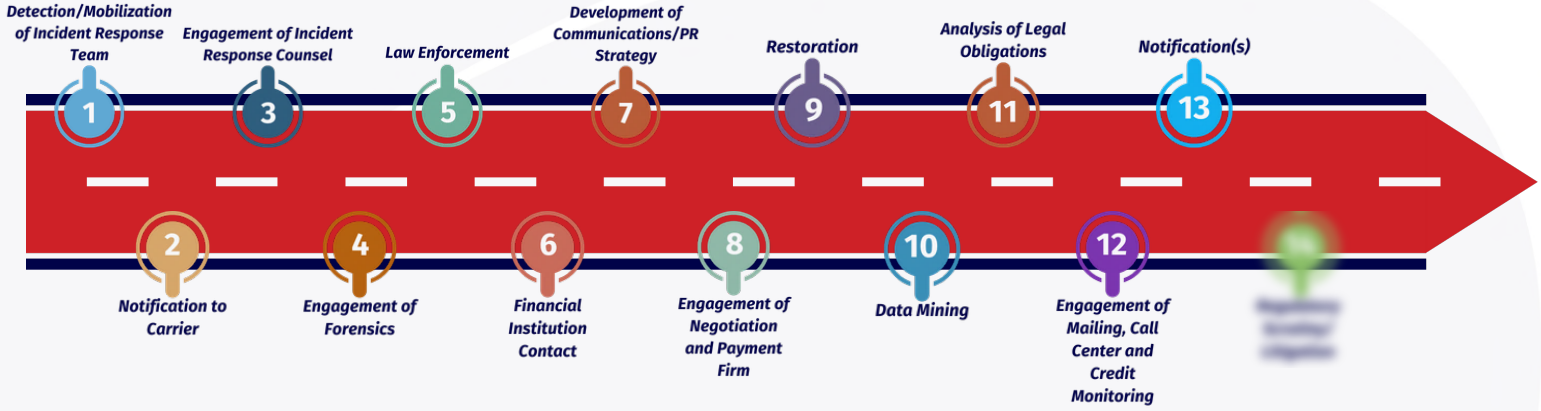
11. Analysis of Legal Obligations

- Incident Response Counsel will provide advice on legal obligations arising from the incident, including but not limited to, obligations to disclose or document the incident and the organization's investigation and response.
- The laws, guidances, and considerations will be specific to the incident, the industry sector of the impacted organization, and the data at risk as a result of the incident.



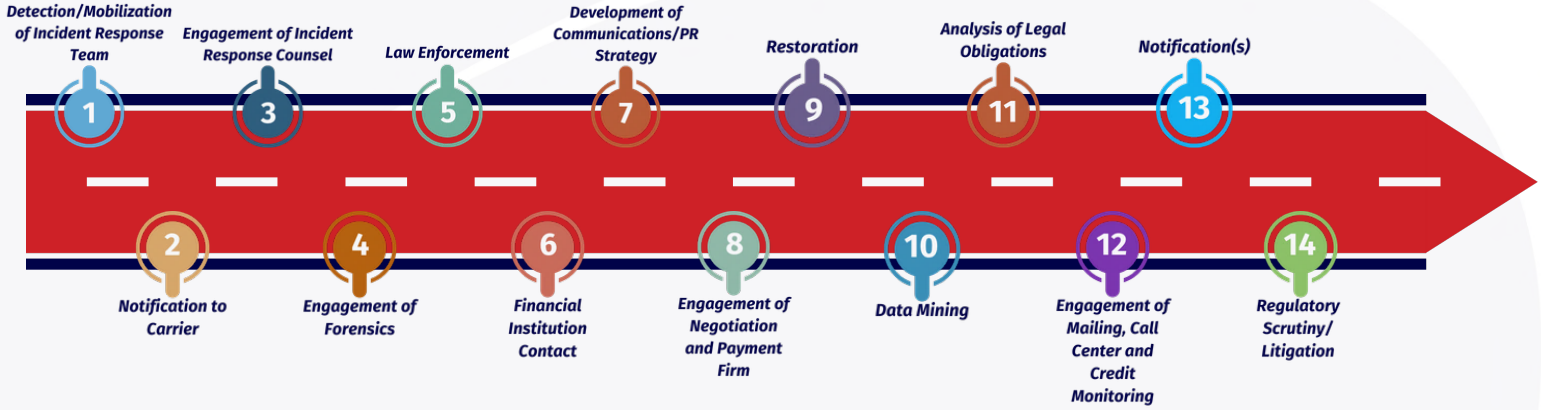
12. Engagement of Mailing, Call Center and Credit Monitoring

- Organizations impacting the security of information may result in disclosure obligations to, among other parties, impacted individuals whose protected information is at risk as a result of the incident.
- The laws provide for the permissible methods of notification, including written notice via U.S. mail, as well as requirements regarding an offering of credit/identity monitoring and restoration services and access to additional information regarding the incident.
- The Hartford has a panel of approved notification providers. The notification provider is engaged by incident response counsel and the insured, and works at the direction of incident response counsel.



13. Notification(s)

- The data breach notification laws speak to the method, content, and timing of notification to individuals, regulators, consumer reporting agencies, and other third-parties.



14. Regulatory Scrutiny/Litigation

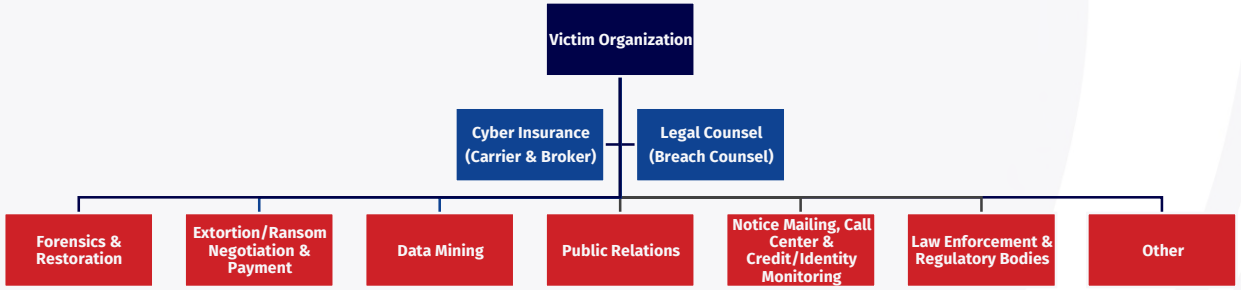
- Many data breach notification laws require an entity to self-report an incident to a state regulatory agency.
- State regulatory agencies are active in investigating incidents reported to their respective offices; however, the timing, method, and outcome of the investigations vary.
- In addition, the plaintiffs' bar is active in monitoring the dark web for information regarding organizations experiencing incidents and regulatory websites for information on self-reported events. Settlements reached in class action litigation over the past few years motivates the plaintiffs' bar to continue in their aggressive pursuit of claims against organizations; however, successful defense strategy is resulting in more instances of dismissal via motion practice, motivating organizations to take a more active approach to defending against these claims.

Key Stakeholders in the Incident Response Process

Internal Stakeholders

- CISO/Information Technology
  - General Counsel
    - Risk Manager
  - Human Resources
  - Communications
- Executive Leadership
  - Other

External Stakeholders



Case Studies

Case Study 1

A **property management company** experienced an **encryption** event, wherein the entirety of their systems were encrypted by a well-known **ransomware threat actor**. The organization engaged Mullen Coughlin as legal counsel, and we in turn engaged a forensic firm to assist with the investigation and response to the event.

Early in the forensic investigation, a ransom note was found on the system, requesting contact be made with the threat actor to obtain the ransom demand. Contact was made with the threat actor, who demanded **2,000,000 in BTC** be paid in exchange for production of the **decryption tool** and **deletion of exfiltrated data**. However, the organization had viable backups from which it could restore, and did not need the decryption tool.

Initially, the organization was not interested in negotiation with the threat actor; however, the forensic investigation revealed - and the threat actor provided - proof of **exfiltration of sensitive data from the organization's system**.

Over a several week period of time, negotiations with the threat actor occurred, and the organization made a **$500,000 ransom payment**. A programmatic and manual review of the exfiltration data was necessary, and the **names and Social Security numbers of 1,700 individuals** (investors and employees) were contained therein. Notice was **required** to be provided to these 1,700 individuals and **10 state regulatory agencies**. A state attorney general launched a **12-month investigation** into the event, but ultimately **closed the matter with the issuance of a warning letter**.

Costs incurred:

- **Ransom Payment: $500,000**
- **Forensic Investigation: $50,000**
- **Notification and Monitoring: $8,000**
- **Legal Fees: $48,000**
- **Total Costs**: **$606,000 + 12-Month State AG investigation**

Case Study 2

A **sales company** employee identified suspicious activity on his computer system and within his email account, and reported it to the company's IT department. The IT department investigated, and determined the employee had **clicked on a link that allowed an unauthorized user to access his computer system**. The organization engaged Mullen Coughlin, who engaged forensics, to launch an investigation into the incident.

Logging was **not** configured to collect all artifacts that would have been helpful for the investigation, but it was determined the threat actor **accessed 18 GB of data over a several week period of time**. The data was reviewed, and **protected information of 52 people** was confirmed to be at risk as a result of the incident.

The organization provided **notice to all 52 individuals**, as well as **3 state regulatory agencies**.

Costs incurred:

- **Forensic Investigation: $17,000**
- **Data Mining: $10,000**
- **Notification: $2,700**.
- **Legal Fees: $21,000**
- **Total Costs**: **$50,700**

Contact / Q&A

Contact

Jennifer A. Coughlin, *Managing Member*
Mullen Coughlin LLC
(267) 930-4774
jcoughlin@mullen.law

If you suspect your organization is currently experiencing a data privacy and security incident, contact the 24/7/365 Mullen Coughlin U.S. Incident Response Hotline at (844) 885-1574 or via email at breachhotline@mullen.law.