Breaches, Responses, and Challenges:

Cybersecurity Essentials That Every Lawyer Should Know

Educational Webcast

09 | 15 | 21

HAYSTACK

Ashish Prasad

Vice President & General Counsel for HaystackID

As VP and GC for HaystackID, Ashish is regarded as among the leading experts on discovery in the US. He has served as Litigation Partner, Founder and Chair of the Mayer Brown LLP Electronic Discovery and Records Management Practice, Founder and CEO of Discovery Services LLC, and VP and GC of eTERA Consulting.

Michael Sarlo

Chief Innovation Officer, President of Global Investigations & Cyber Discovery Services for HaystackID

Michael facilitates all operations related to electronic discovery, digital forensics, and litigation strategy both in United States and abroad while working on highly complex forensic and e-Discovery projects. He has full oversight of all facilities and manages workflow and change management to ensure consistent quality and efficiency of all processes for each project entering HaystackID's walls.

Jennifer Hamilton

Deputy General Counsel for Global Discovery & Privacy for HaystackID

Jennifer serves as a resource for corporate clients, support legal and compliance operations, and continue to grow the Enterprise Managed Solutions Group, the company's specialized offerings for corporations and law firms wishing to transform their business of law practices. Jennifer comes from John Deere, where she spent 14 years leading the development of the company's eDiscovery operations and was head of the Global Evidence Team.

Matthew Miller

Sr. Vice President of Information Governance & Data Privacy for HaystackID

Matt is SVP of Information Governance and Data Privacy for HaystackID. With a background in legal, then eDiscovery, Matt formerly co-developed Ernst & Young's IG services practice, and was the Global IG Advisory Services leader at Consilio LLC. He has led highly complex incident response related forensic investigations and multi-national, petabyte-scale, data governance and privacy engagements.

Agenda

1. It's Only a Matter of Time: Security Incident Statistics & Ransomware
2. Advanced Persistent Threat Attack Lifecycle & IT Security Countermeasures
3. The Workflows of Incident Response Between & Within the Participating Companies & Groups
4. The Roles of Key Stakeholders
5. Federal, State, & International Legal Requirements & Strategies for Meeting the Expectations of Different Regulators
6. The Protection of Privilege Considering Recent Case Law
7. Data Breach Notification Reports
8. The Proactive Steps that Companies Should be Taking to be Prepared to Respond to Cybersecurity Incidents

It’s Only a Matter of Time: Security Incident Statistics & Ransomware

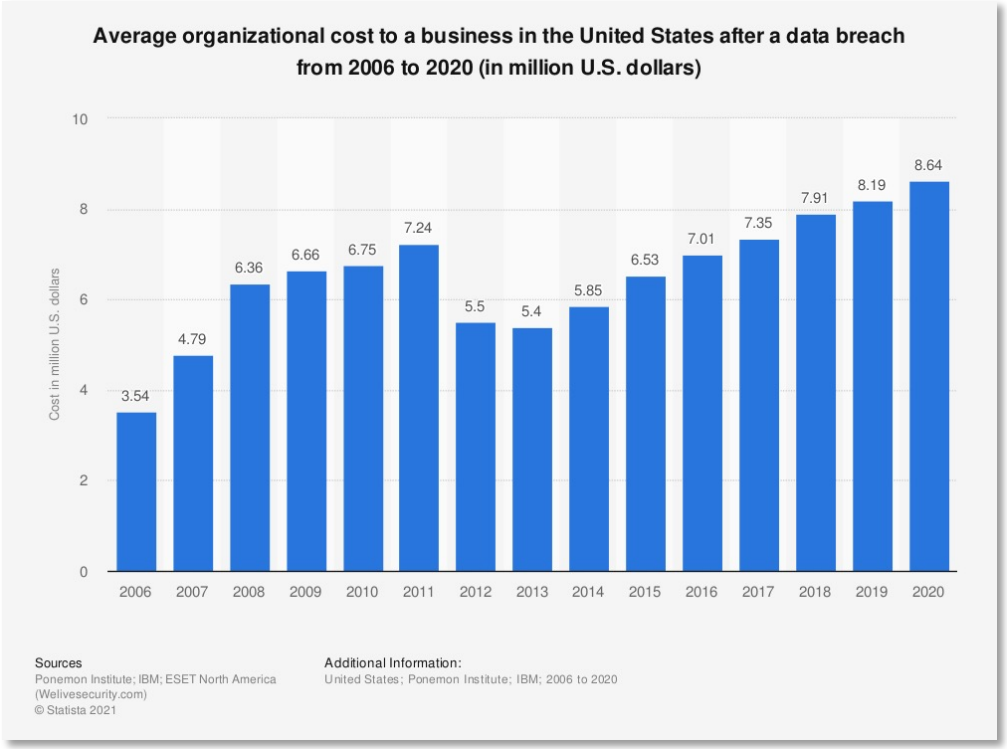
The Average Cost of a Breach

The average cost per data breach:

- United States = **$8.64 million** USD in 2020
  - → **$9.05 million** USD in 2021
- Globally = **$3.86 million** USD in 2020
  - → **$4.24 million** USD in 2021

Total breach costs include:

- **Lost business** resulting from diminished trust or confidence of customers
- Costs related to **detection, escalation, and notification** of the breach
- **Post response activities**, such as credit report monitoring



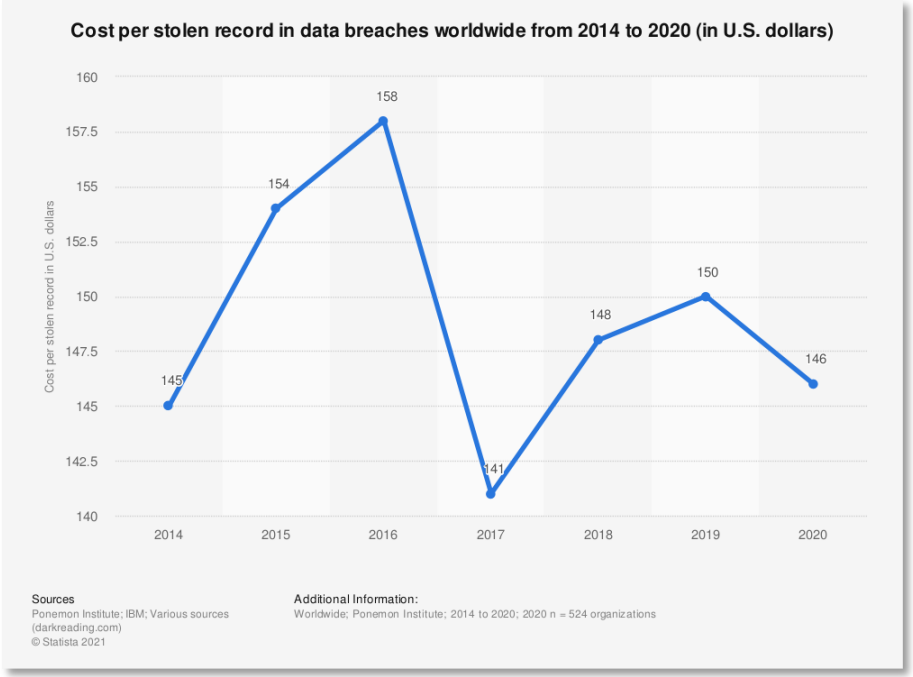
The Average Cost per Record

In 2020, the cost per stolen record in data breaches was amounted to **$146 USD**

In 2021, the cost per stolen record in data breaches was amounted to **$161 USD**

In 2021, when customer PII was lost or stolen, the cost per record went up 20% to **$180 USD**

Healthcare has the highest cost of **$429 USD** per stolen record



HAYSTACK

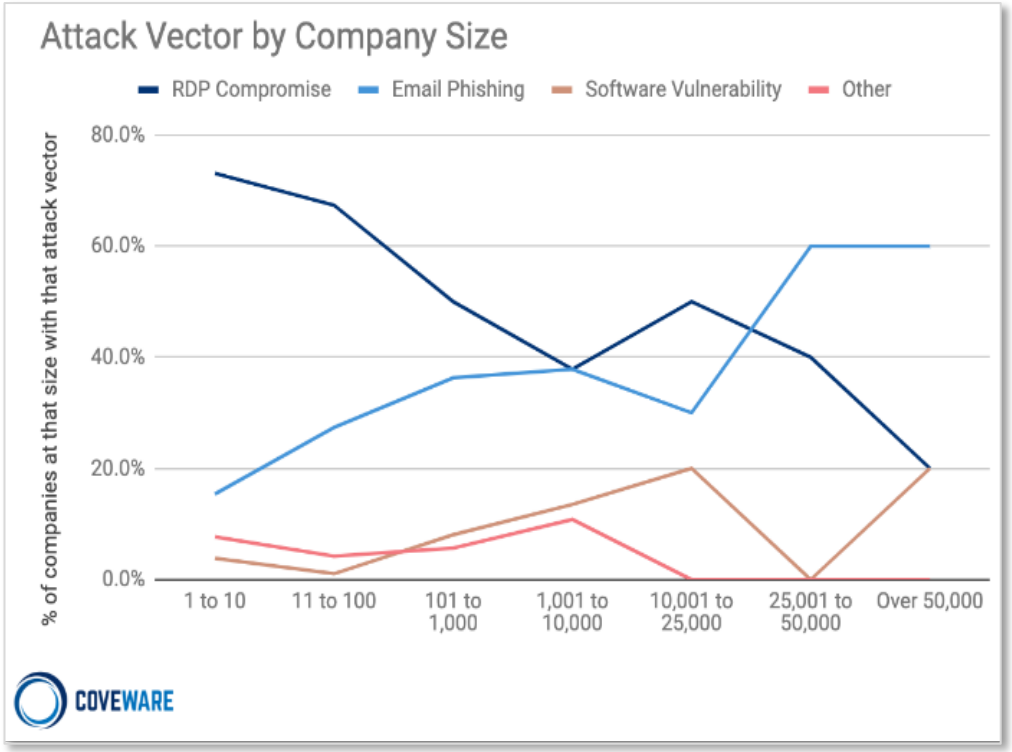
The Anatomy of a Ransomware Attack

Ransomware is like a virus that scans connected drives for files that it encrypts.

The user is also typically locked out of their machine and can only view a screen showing how to make a ransom payment.

Ransomware can reach a user's machine **using a number of vectors**:

- Phishing attack
- Malicious websites or popups
- Unsecured network connections (i.e. if no VPN is used)
- Brute force to hack weak passwords and directly insert the ransomware
- Vulnerabilities in applications during the software development process



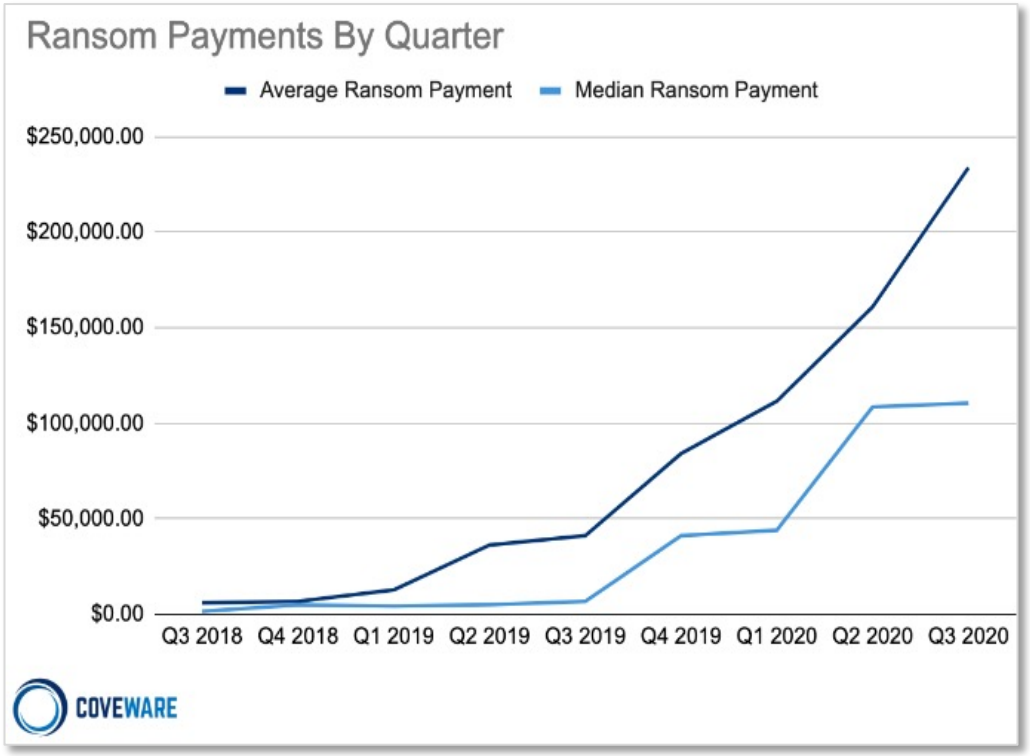
HAYSTACK

Average Ransom Payment Sizing

Cybercriminals continue to be less interested in stealing consumers' personal information.

Ransomware and phishing attacks directed at organizations are now the preferred method of data theft by cyberthieves:

- Require less effort
- Largely automated
- Generate much higher payouts
  - > **$233,000** per event in Q4 2020



In 2020, ransomware attacks increased

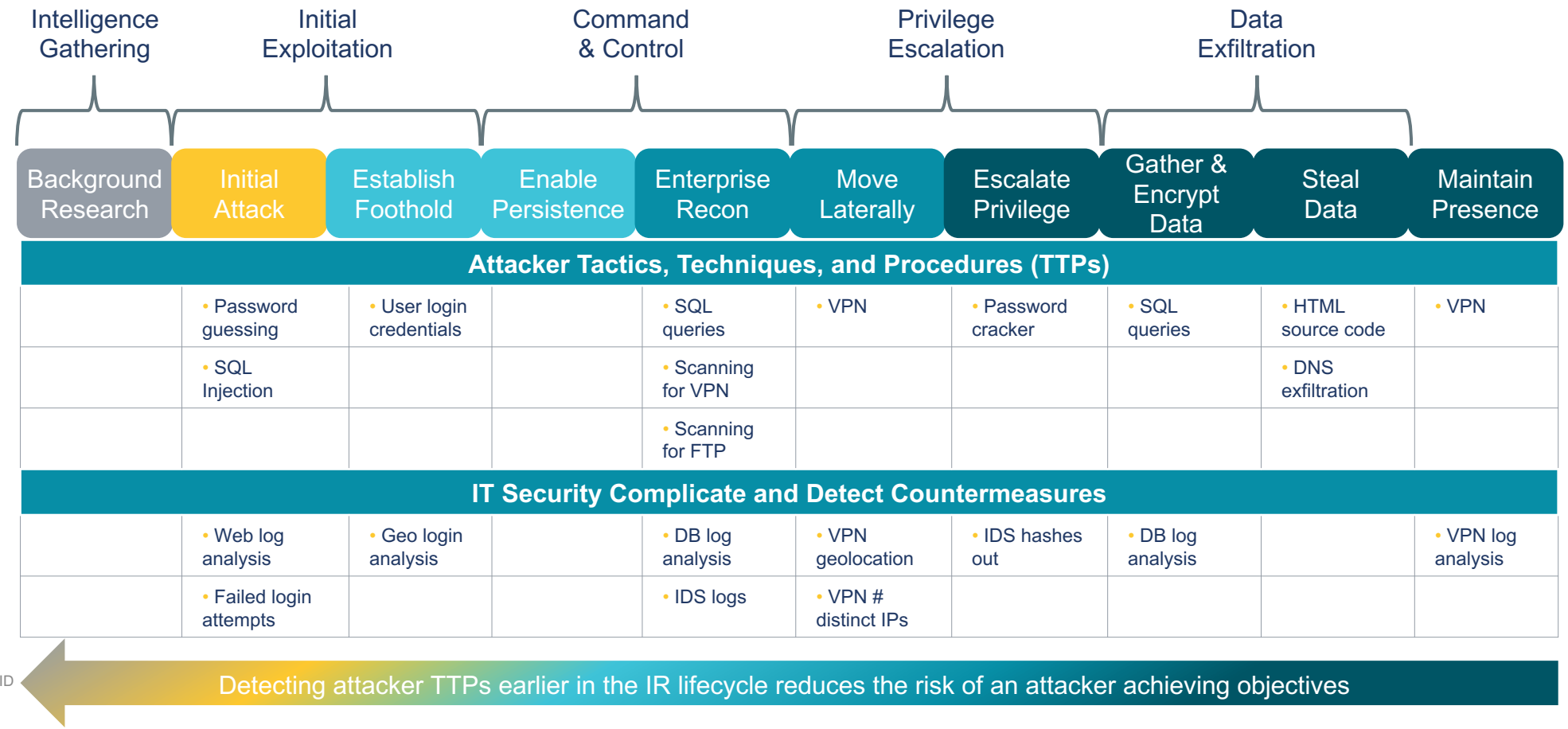
- **471%** in the U.K.
- **150%** in Australia
- **75%** in Singapore
- **70%** in the U.S.

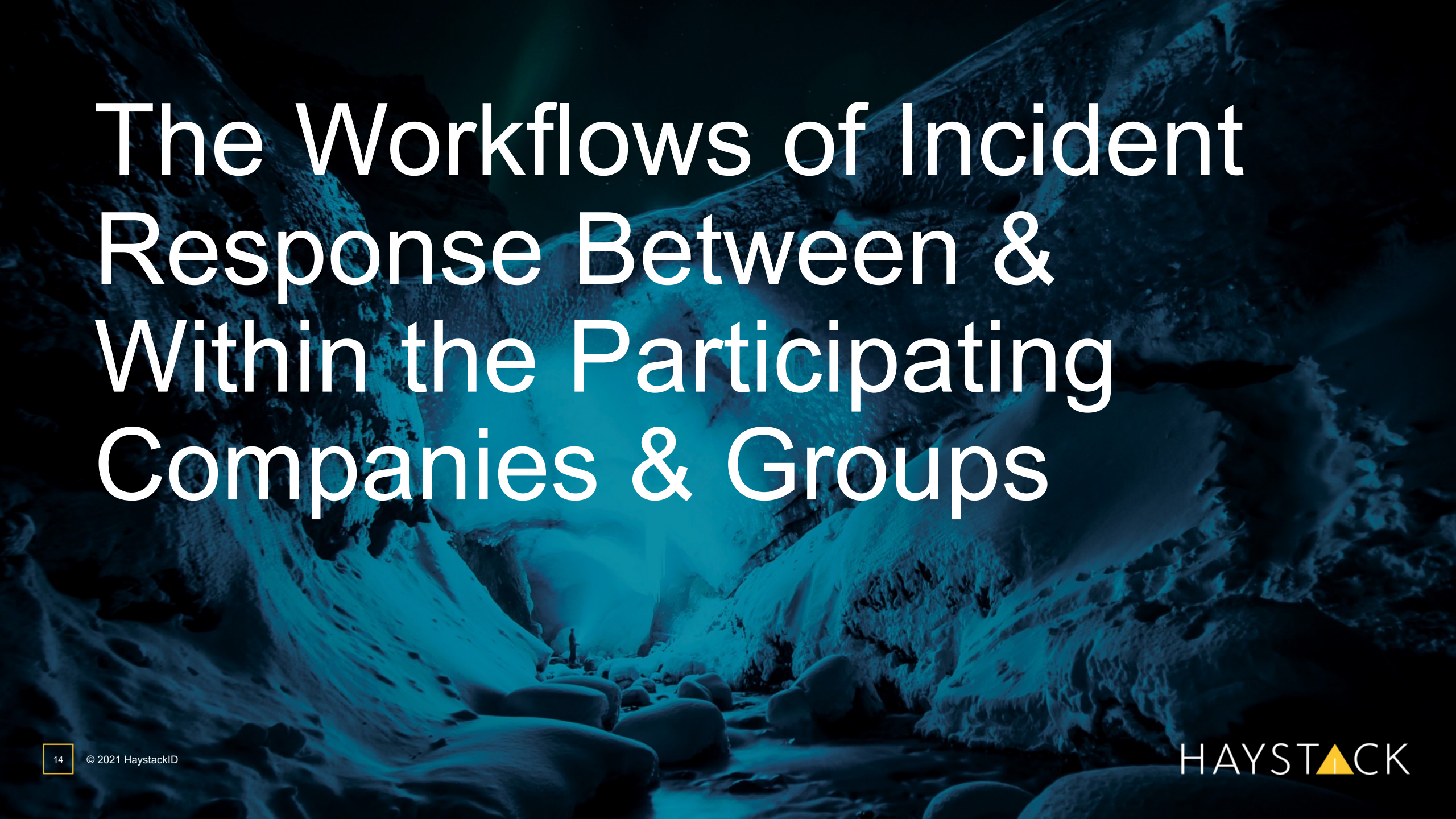
In 2020, phishing was the most favored type of attack globally

- **25%** of U.S. attacks
- **36%** in Australia
- **75%** increase in Singapore
- Most common data breach type in the U.K. & Germany

HAYSTACK

Advanced Persistent Threat Attack Lifecycle & IT Security Countermeasures





Lifecycle of a Data Breach

React, Repair, Resume

HAYSTACK

The Workflows of Incident Response Between & Within the Participating Companies & Groups

Internal Stakeholders
- Board of Directors
- In-House Counsel
- Compliance
- Finance
- Information Security
- Corporate Security
- Public Relations

Resolution

External Stakeholders
- Law Enforcement
- Regulators
- Insurance Companies
- Outside Counsel
- Incident Response
- Company
- Vendors
- Customers
- Media
- Market Analyst
- Shareholders

A High-Impact Breach
- Theft of personally identifiable information
- Sabotage of industrial control systems
- Highly confidential data theft
- Denial of service
- Industrial property theft
- Broad malware infection
- Ransomware across systems
- Compromise to the integrity of financial reporting systems

Investigation
- How and when the compromise occurred
- What systems and data are impacted
- Who was responsible for the compromise

Forensic Activities
- Identify, collect, and preserve evidence
- Perform forensic analysis and data analysis
- Develop and understand fact patterns

The output may determine more in-depth investigation is needed

Outcome

- Damage assessment and containment
- Remediation
- Eradication
- Crisis management

The Roles of Key Stakeholders

The Roles of Key Stakeholders

Inside the Breached Organization

In-House Counsel

- Interaction with law enforcement & regulators
- Litigation & eDiscovery
- Outside Counsel coordination
- Public Relations oversight

Public Relations

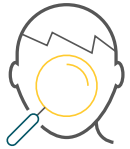
- External communication

Chief Information Officer

- Business continuity
- Disaster recovery

Board of Directors

- Risk oversight
- Overall response strategy



Chief Compliance Officer

- Data privacy & disclosure laws
- Industry-specific regulatory requirements

Chief Financial Officer

- Integrity of financial controls & data
- Financial impact
- Insurance claims

Human Resources

- Policy making
- Internal communication

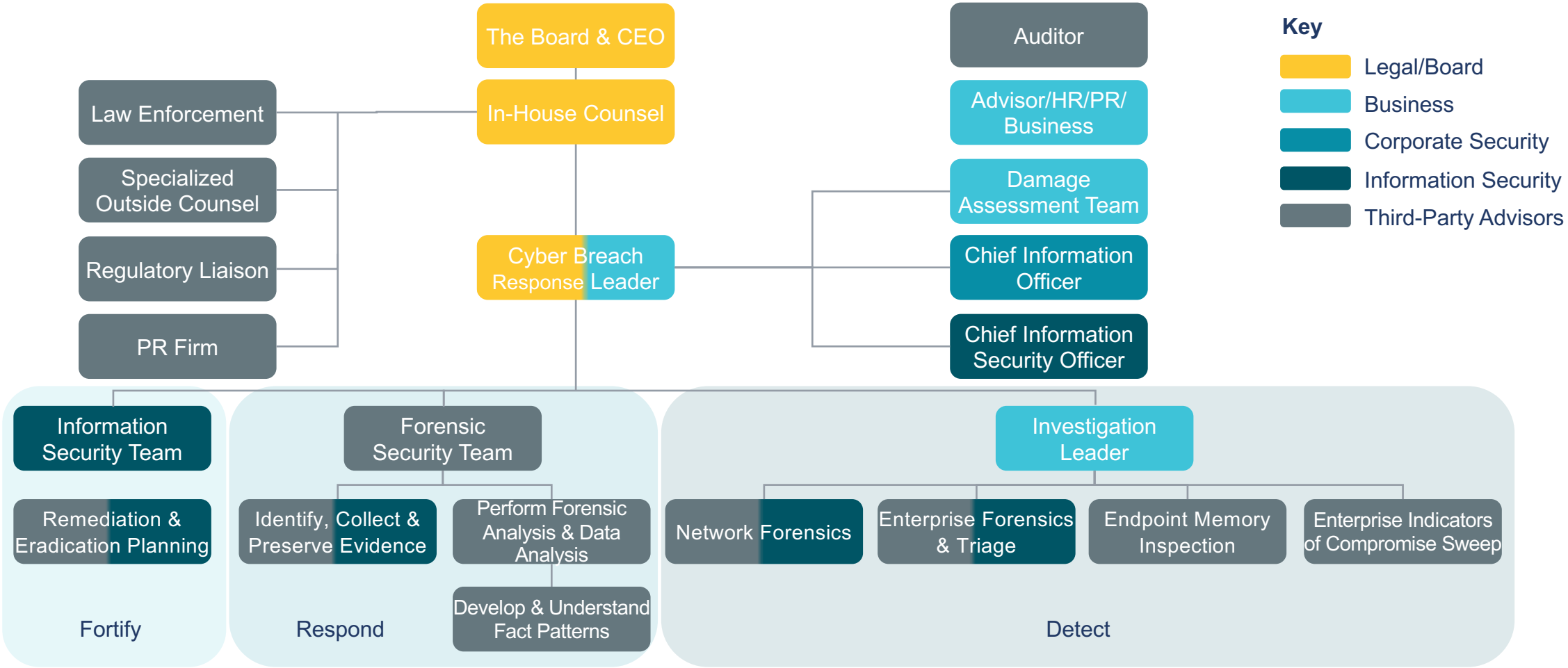
Chief Information Security Officer

- Security of electronic assets
- Evidence gathering, identification & preservation
- Impact assessment & containment
- Remediation
- Eradication

HAYSTACK

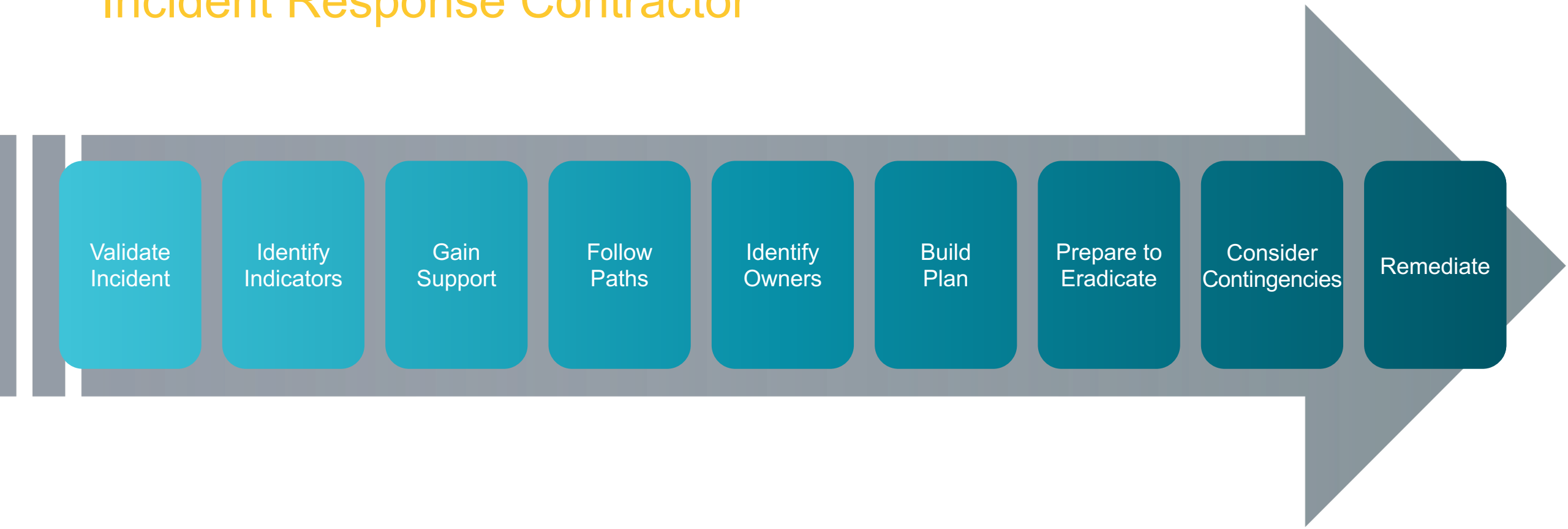
The Roles of Key Stakeholders

In Response to a Large-scale Cyber Breach



The Roles of Key Stakeholders

Incident Response Contractor



HAYSTACK

Example of a Cyber Incident Response Remediation Timeline

Days 1 - 3	Days 4 - 34	Days 35 - 65	Days 66 - 78

Mobilization		Organization		Findings and Deliverables	
Deploy Forensic resources	Deploy Document reviewers	Begin corporate data recovery		Begin production data recovery	Collected computers are cleansed and data is delivered back to end users or IT
Recover decryption server environment	Create analytics framework to identify PII	Conduct PII analytics to identify social security numbers, birthdays, addresses, and phone numbers.		Perform data recovery and cleansing on assets	Recover data from malware affected systems
Create secure private cloud for hosting of infected data		Process data and host unique documents	Identify credit cards, driver's licenses, and passport numbers. Isolate medical history, user credentials, and bank account information		Recover files and deliver to end users on clean media devices
Establish globally consistent project management and reporting		Conduct document review – on/offshore document reviewers	Create privilege categories to expedite attorney review		Resume normal business operations, harden network based on lessons learned

By taking proactive steps to Identify, Classify, Inventory, and Remediate PII before an incident occurs, Legal and Compliance teams can dramatically reduce the response time for PII identification, enabling faster creation of a data breach consolidated entity notification list

Federal, State, & International Legal Requirements & Strategies for Meeting the Expectations of Different Regulators

Federal, State, & International Legal Requirements & Strategies for Meeting the Expectations of Different Regulators

- If the breach involves the disclosure of individuals' personal information, U.S. federal law, state law, and/or international law may require certain notifications of the breach.
- Notification might be required to the affected individuals, consumer credit reporting agencies, and multiple different government regulators.
- Once regulators have been notified, the organization faces the risk of an enforcement proceeding and fines/penalties.
- Once the affected individuals have been notified, the company faces the risk of private lawsuits for damages.

Major Legislation Requiring Data Breach Notification

GDPR

HIPPA

CCPA, CPRA & VA CDPA

State Law

FIPA

NY Shield

HAYSTACK

Breach Notification Requirements

Each major regulation and each state and territory of the US has its own notification requirement and own definition of PII and protected categories of information in the even of unauthorized access to protected information or “breach”.

GDPR

In the case of a personal **data breach**, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, **notify** the personal **data breach** to the supervisory authority competent in accordance with Article 55.

HIPAA

If a **breach** affects 500 or more individuals, covered entities must **notify** the Secretary without unreasonable delay and in no case later than 60 days following a **breach**. If, however, a **breach** affects fewer than 500 individuals, the covered entity may **notify** the Secretary of such **breaches** on an annual basis.

Contract language also often states requirement for notification to client

HAYSTACK

Exception to Notification Requirements

GDPR, HIPPA, and 42 states also allow a “risk of harm analysis” in the determining whether notification is required.

GDPR for instance, states “personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.”

Sample from WI Statute

Notification is not required if the acquisition of personal information does not create a material risk of identity theft or fraud to the subject of the personal information.

Encryption Notification Exclusion

Every State, US Territory, Federal Regulation, and GDPR allows for an exclusion to notification requirements if it can be demonstrated by the data controller that the information was encrypted, and the encryption key was not also compromised in the breach.

Sample PA

Notification is not required when encrypted or redacted information is accessed and acquired. Notice is required, however, if encrypted information is accessed and acquired in an unencrypted form, if the security breach is linked to a breach of the security of the encryption or if the security breach involves a person with access to the encryption key.

Who to Notify?

Depending on type of breach notification may be required to:

- **The Protected Individual**
- **The Entire Household if the Data Pertains to the Household (CA)**
- **Department of Consumer Affairs**
- **State Attorney Generals Office**
- **Foreign Data Authority**

Notices generally cover:

- What happened?
- What information was stolen?
- How can they protect themselves?
- What you've done to correct the harm?

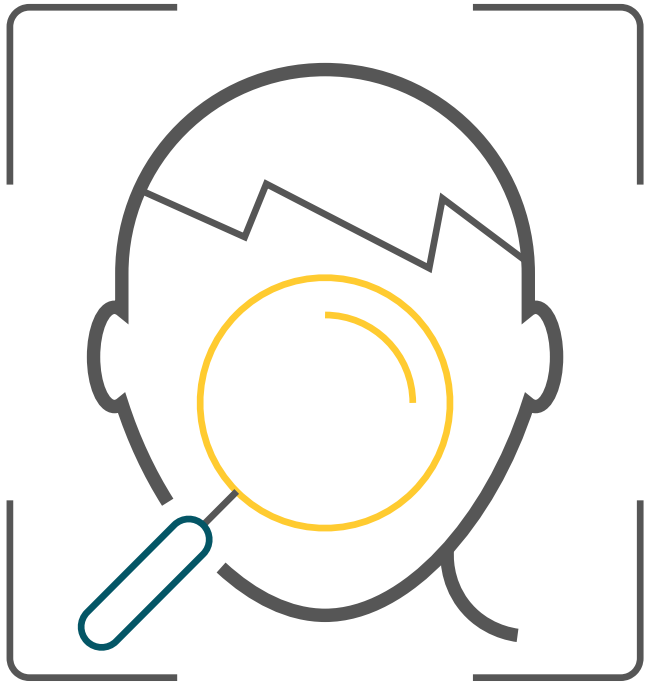
HAYSTACK

Proportionality

Rule 26 (b)(1) does not apply to statutory breach notification, response, or security obligations.

Where it could conceivably apply is in breach litigation in providing discovery as the extent of the data breach, collections from custodians likely to yield the same results, expensive forensics on databases and systems possibly affected.

There is very little in the way of legal precedent specifically applying 26(b)(1) proportionality to data breach



The Protection of Privilege Considering Recent Case Law

Privilege Issues

Generally, attorney work product prepared in anticipation of litigation following a breach is covered under the attorney work product privilege doctrine and inadmissible into evidence.

Capital One Consumer Security Data Breach MDL -

Cyber Security Forensics Report not protected by privilege:

- Law firm was hired after the breach and used existing vendor performing existing services.
- Report was shared with outside parties (regulators and accountants).
- Cyber Firm, Mandiant, was paid by Capital One from previously agreed to retainer.

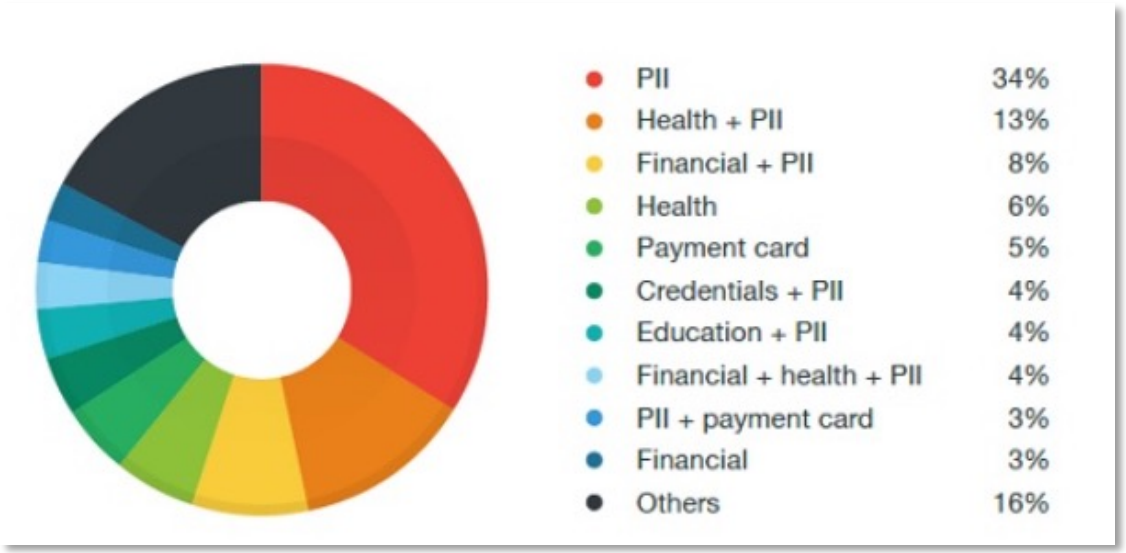
Data Breach Notification Reports

Sensitive Data Breach Assessment Reporting

Automated Customizable Impact Assessment Reporting

AI Engines and Search Workflows Allow for Creation of Customized Reporting that Includes:

- Count of Sensitive Data by Type
- Count of Sensitive Data by Source
- Count of Unique Person Names and Organizations
- Count of Unique Persona Names and Organizations that Overlap with Sensitive Data Types
- Count of Sensitive Data by Range of Confidence Scores
- Count of Document Types within the Above Categories
- Count of Sensitive Data by Type over Custom Date Ranges
- Roll up reporting of Top Folder Locations
- General Dataset Statistics
- Visual Reporting via Customizable Dashboards
- Exception Reporting
- Deduplication Statistics



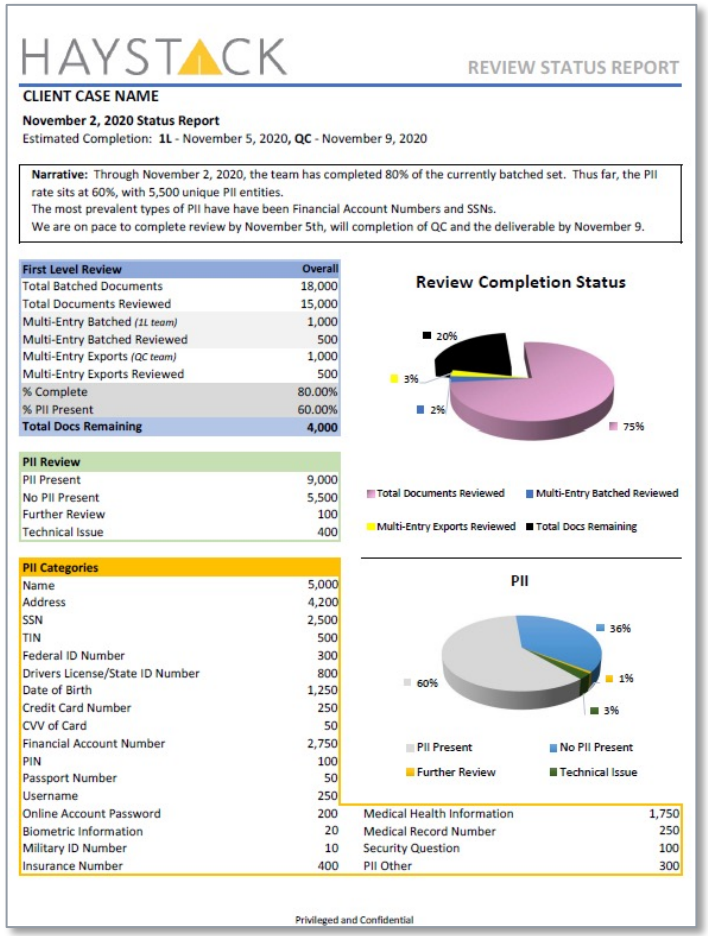
HAYSTACK

Data Breach Notification

PII Review Reporting

Expect customized project review metrics for:

- Up-to-date issue log
- All coding fields and choices
- Unique entity counts
- Estimated completion dates
- QC metrics
- Individual and team pace and overturn rates
- A detailed narrative that provides key information as to the status of the review



HAYSTACK REVIEW STATUS REPORT

CLIENT CASE NAME

November 2, 2020 Status Report

Estimated Completion: **1L** - November 5, 2020, **QC** - November 9, 2020

Narrative: Through November 2, 2020, the team has completed 80% of the currently batched set. Thus far, the PII rate sits at 60%, with 5,500 unique PII entities.
The most prevalent types of PII have have been Financial Account Numbers and SSNs.
We are on pace to complete review by November 5th, will completion of QC and the deliverable by November 9.

First Level Review	Overall
Total Batched Documents	18,000
Total Documents Reviewed	15,000
Multi-Entry Batched *(1L team)*	1,000
Multi-Entry Batched Reviewed	500
Multi-Entry Exports *(QC team)*	1,000
Multi-Entry Exports Reviewed	500
% Complete	80.00%
% PII Present	60.00%
Total Docs Remaining	**4,000**

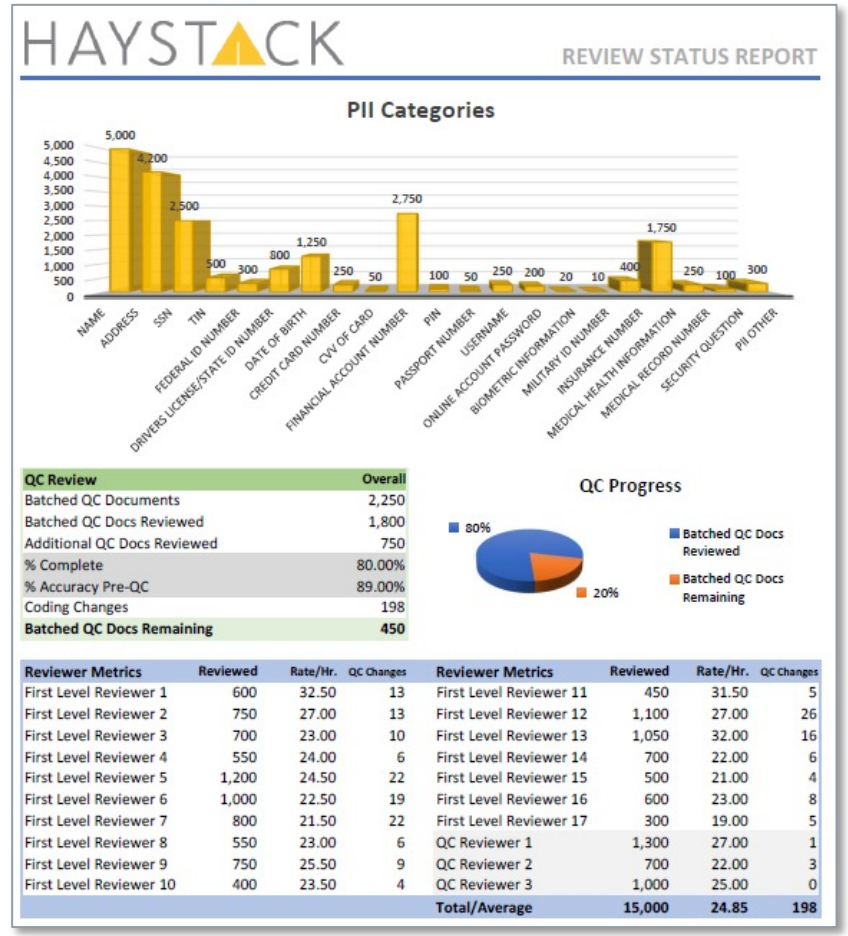
PII Review	
PII Present	9,000
No PII Present	5,500
Further Review	100
Technical Issue	400

PII Categories	
Name	5,000
Address	4,200
SSN	2,500
TIN	500
Federal ID Number	300
Drivers License/State ID Number	800
Date of Birth	1,250
Credit Card Number	250
CVV of Card	50
Financial Account Number	2,750
PIN	100
Passport Number	50
Username	250
Online Account Password	200
Biometric Information	20
Military ID Number	10
Insurance Number	400
Medical Health Information	1,750
Medical Record Number	250
Security Question	100
PII Other	300

Review Completion Status

PII

Privileged and Confidential



HAYSTACK REVIEW STATUS REPORT

PII Categories

QC Review	Overall
Batched QC Documents	2,250
Batched QC Docs Reviewed	1,800
Additional QC Docs Reviewed	750
% Complete	80.00%
% Accuracy Pre-QC	89.00%
Coding Changes	198
Batched QC Docs Remaining	**450**

QC Progress

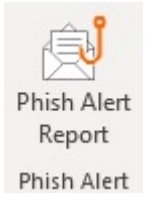
Reviewer Metrics	Reviewed	Rate/Hr.	QC Changes
First Level Reviewer 1	600	32.50	13
First Level Reviewer 2	750	27.00	13
First Level Reviewer 3	700	23.00	10
First Level Reviewer 4	550	24.00	6
First Level Reviewer 5	1,200	24.50	22
First Level Reviewer 6	1,000	22.50	19
First Level Reviewer 7	800	21.50	22
First Level Reviewer 8	550	23.00	6
First Level Reviewer 9	750	25.50	9
First Level Reviewer 10	400	23.50	4

Reviewer Metrics	Reviewed	Rate/Hr.	QC Changes
First Level Reviewer 11	450	31.50	5
First Level Reviewer 12	1,100	27.00	26
First Level Reviewer 13	1,050	32.00	16
First Level Reviewer 14	700	22.00	6
First Level Reviewer 15	500	21.00	4
First Level Reviewer 16	600	23.00	8
First Level Reviewer 17	300	19.00	5
QC Reviewer 1	1,300	27.00	1
QC Reviewer 2	700	22.00	3
QC Reviewer 3	1,000	25.00	0
Total/Average	**15,000**	**24.85**	**198**

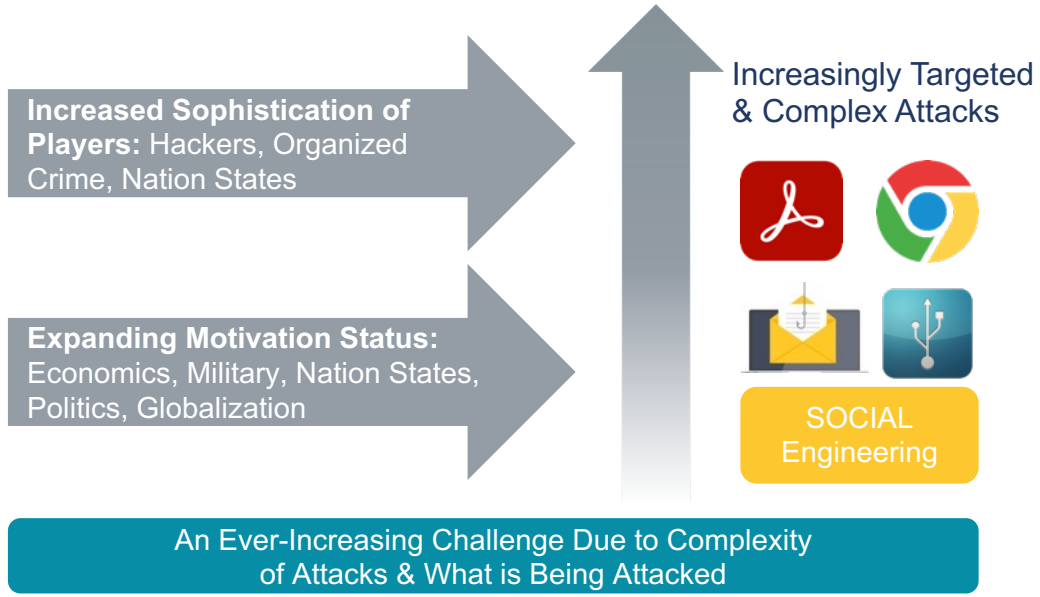
Post COVID-19 Impact on Cybersecurity

Proactive, Defensive Technology Measures

- Back-up, Disaster Recovery, Resiliency Planning
- Identify and classify sensitive data (PII/PHI/PCI) to enforce data protection and remediation
- Updates and patches
- Only use licensed software
- Only use WiFi networks that are password protected
- 2FA, MFA, VPN
- Employee Training – Please Don't Click
- Add the Phish Alert Report plug-in to M365



In 2020, Cybercriminals preyed on consumers with false information about the COVID-19 pandemic, stimulus payments, and lockdowns via sophisticated spear phishing attacks.



HAYSTACK

Does your Organization…

Know all data it retains and processes?

Know where all data is located and stored?

Have visibility into all metadata and content?

Control who can and should have access to which data?

Know how to retrieve data rapidly when needed?

Only retain data as long as necessary?

Dispose, deidentify, or encrypt data regularly?

***Processing PII** = creation, collection, use, processing, storage, maintenance, dissemination, disclosure, or disposal (NIST.SP.800-53r5, PT-3, Sept. 2020)*

HAYSTACK

Implement Defensible Data Disposition

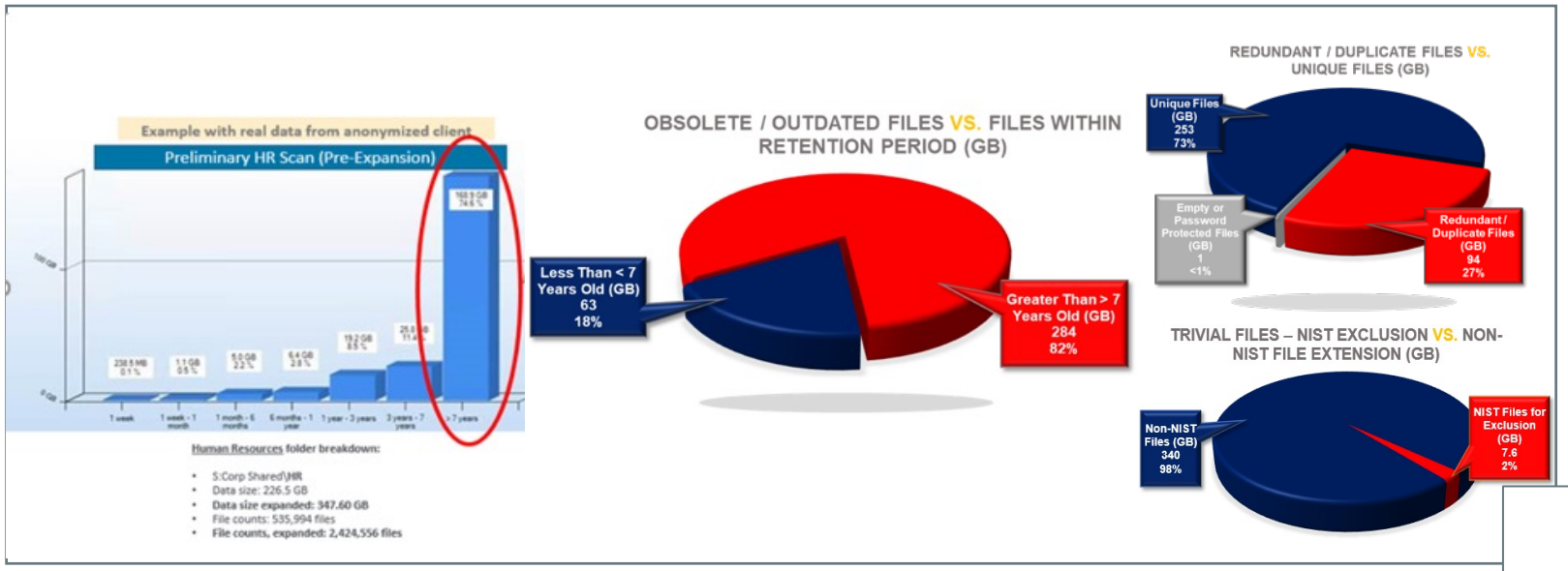
The Sedona Conference, Commentary on Defensible Disposition (April 2019), provides guidance on disposition of **information that is no longer subject to a legal hold and has exceeded** the applicable legal, regulatory, and business **retention requirements**.

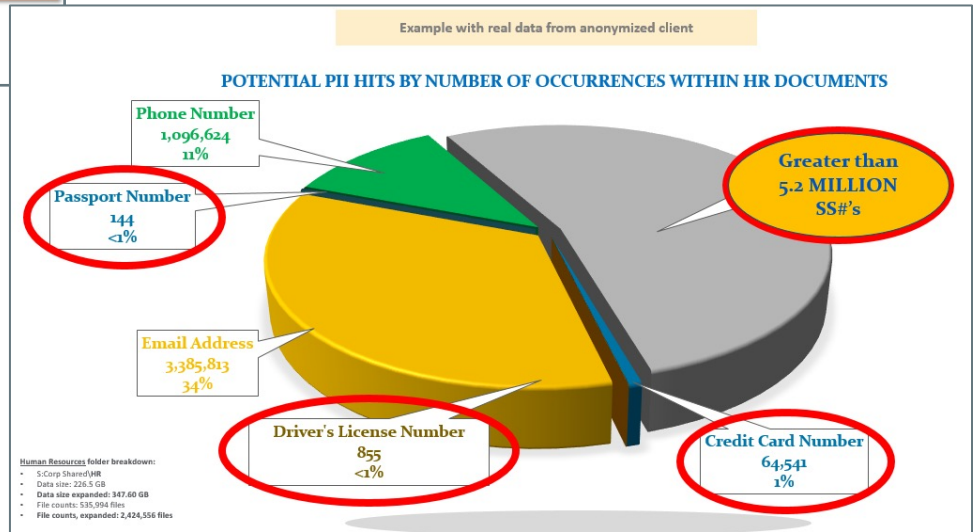
- **Principle 1: Absent a legal retention or preservation obligation, organizations may dispose of their information**.
- **Principle 2:** When designing and implementing an information disposition program, organizations should identify and manage the risks of over-retention.
- **Principle 3:** Disposition should be based on Information Governance policies that reflect and harmonize with an organization's information, technological capabilities, and objectives.

HAYSTACK

Operationalize Policies

Implement Defensible Disposition & Remediation – Use Case





HaystackID's Information Governance Methodology

Step 1

Solidify Foundational Elements
Maturity Level, Program, Data Map

Step 2

Identify, Classify & Inventory Data
Critical, Sensitive, and ROT

Step 3

Operationalize Policies
Implement Defensible Disposition and Remediation

Step 4

Enable Automated Continuous Data Supervision

Step 5

Ensure Cyber Incident Preparedness
Proactive and Post-Breach Approaches

Step 6

Exceed Reasonable Security Measures

How can we help you?

Learn how our infinite capabilities can help you at HaystackID.com
or reach out to us at Info@HaystackID.com / 877.942.9782

HAYSTACK