Institute and Faculty of Actuaries

External Scanning for Insurance
Gallagher Re

Michael Georgiou, **Senior Cyber Actuary**
Ed Pocock, **Head of Cyber Security**
James Poynter, **Head of Data Science**

#GiroConf22

Contents

Institute and Faculty of Actuaries

Providers and Use Cases

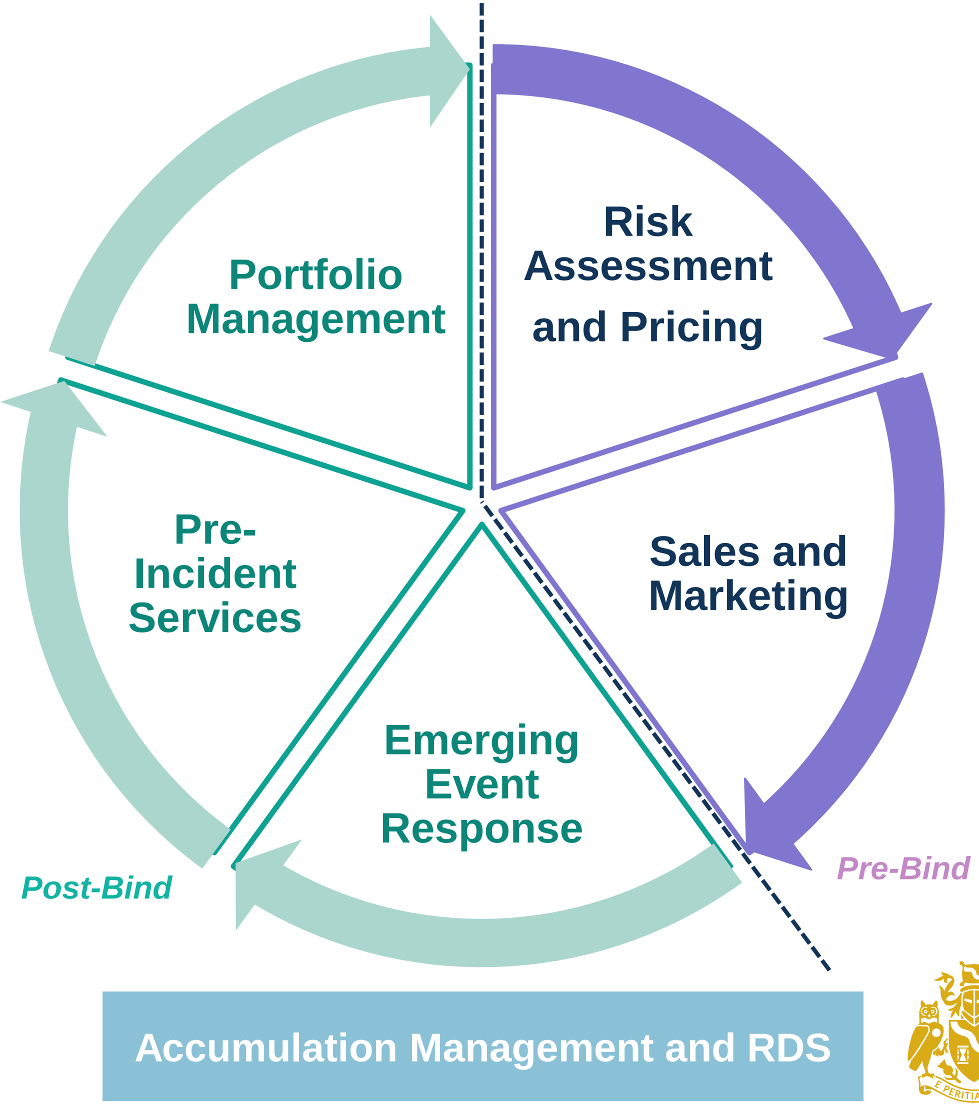
Technology will play a key role in Cyber's future, but traditional underwriting methods won't be replaced

Traditional Underwriting	Outside In	Inside Out
Traditional instruments to manage exposure and reduce risk in UW.	**Externally available technical and firmographic data aiming to indicate a company's security posture**	Data requiring access to an organisation's internal network.
How security controls are designed	**Provides the attackers view**	How security operates in practice
• Can't be entirely replaced by technology (Provides a view on people and process aspects of security) • Enables proactive response to threat landscape changes	• **Difficult to Master** (requiring expertise to translate data into insights) • **Utility across Value Chain** (from UW to portfolio optimisation and event response)	Uptake requires incentivisation Data integration can be automated

Institute and Faculty of Actuaries

How is the insurance market using outside in technology?

- Outside in technology has many possible applications for insurance. These applications cover a policy lifecycle, from underwriting to portfolio and exposure management
- Despite hesitations in uptake of the technology, **all use cases outlined below are currently being used** by the insurance industry
- **New ways of using the technology are still emerging**, with warning insureds potentially vulnerable to new and emerging attacks only being fully embraced by forward thinking insurers in recent months.



Institute and Faculty of Actuaries

Rapid update of external scanning data by (re)insurers masks complexity on how data is used in practice

23 of 33
Insurers using external scanning data in risk selection

13 of 33
Insurers using multiple technology vendors

31 of 33
Insurers using external scanning data overall

14 of 33
Insurers using external scanning data for portfolio management

Institute and Faculty of Actuaries

Making sense of the vendor landscape is nearly impossible for (re)insurers… but there is method to the madness!

SecurityScorecard
BITSIGHT
The Standard in SECURITY RATINGS
Censys
SecurityTrails
CyberCube
UpGuard
GUIDEWIRE
ISS ESG
axio
SAFE
BlueVoyant
BLACK KITE
Panorays
PALADIN Cyber
Cyberwrite
KYND
cysmo
POWERED BY ppi

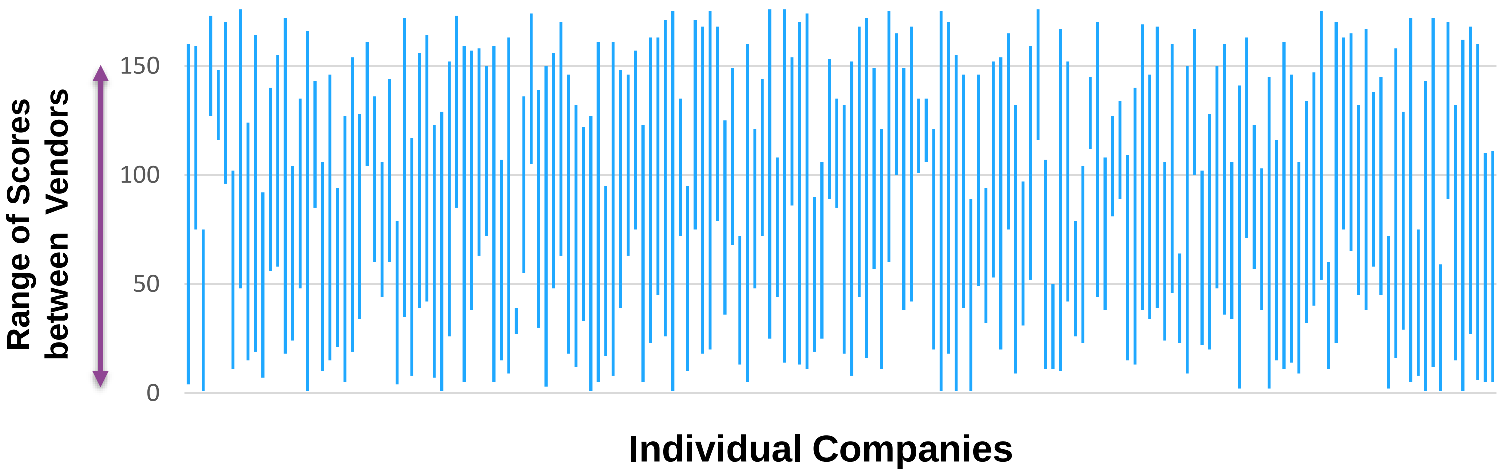
So, what's the problem?

The Problem

Rapid **uptake of technology has been hamstrung by uncertainty** around the ability of technology to predict claims and industry lack of resources.

This **uncertainty makes it hard** to:

- **Evaluate vendors** and data objectively
- **Place reliance on technology** in an appropriate and proportional way
- **Gain trust and better terms from capacity providers** for the effective use of technology



- **Scores are inconsistent** and heavily dependent on scoring methodology
- As a result, **scanning technologies aren't usually 'plug and play'** requiring Cyber Threat and Analytics expertise from the Insurer

Institute and Faculty of Actuaries

Cyber security risk selection

Gallagher RE TIDE, our proprietary Risk Selection model combines claims, firmographic, and "outside in" Cyber Security Rating data to develop an enhanced view of claims frequency risk.

Claims over 18 months drawn from different firmographic groups curated and included

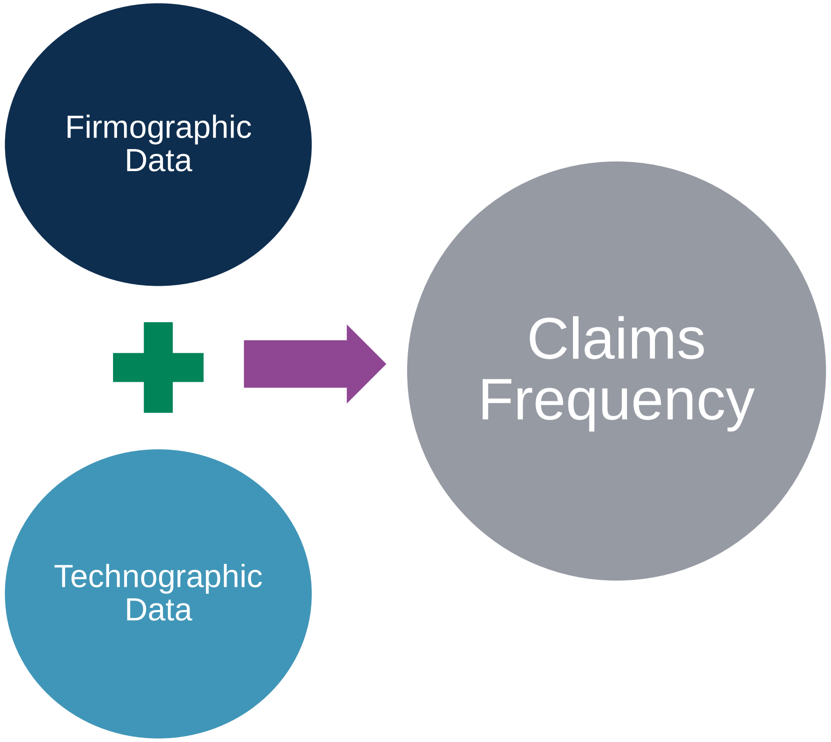
Policy records included complete with firmographic data

Companies technographic data received and analysed

Security Ratings observations considered in analysis

- **Utilising Machine Learning algorithms** to uncover hidden patterns, and predict claim frequency for a given firm

- Leveraging the latest MLOps (Machine Learning Operations) technologies to **automate model development, and data insights**.



Institute and Faculty of Actuaries

Gallagher Re

… and our solution!

Our Solution

We **built a machine learning model powered by technographic data to assess how predictive external scanning data is** of Cyber claims.

Thought Leadership

Revenue is the greatest claims predictor

Only a small % of technographic data added predictive value

Patching Cadence is the strongest technographic predictive indicator

Port Security is still a big driver of claims

Web Security is a material driver of Claims

Mobile Application Security can't be ignored

Institute
and Faculty
of Actuaries

Methodology

#GiroConf22

Core components of an ML build

Data

Target (Claim)

Technographic Features (e.g. Email Security)

Client Features (e.g. Industry)

Model Training

Gradient Boosted Models

LightGBM

Generalised Linear Models

scikit learn

Dummy Models

Gallagher Re

Insights and Validation

Model Validation

Comparing model performance

Model Insights

"Lifting the lid on the Black Box"

Institute and Faculty of Actuaries

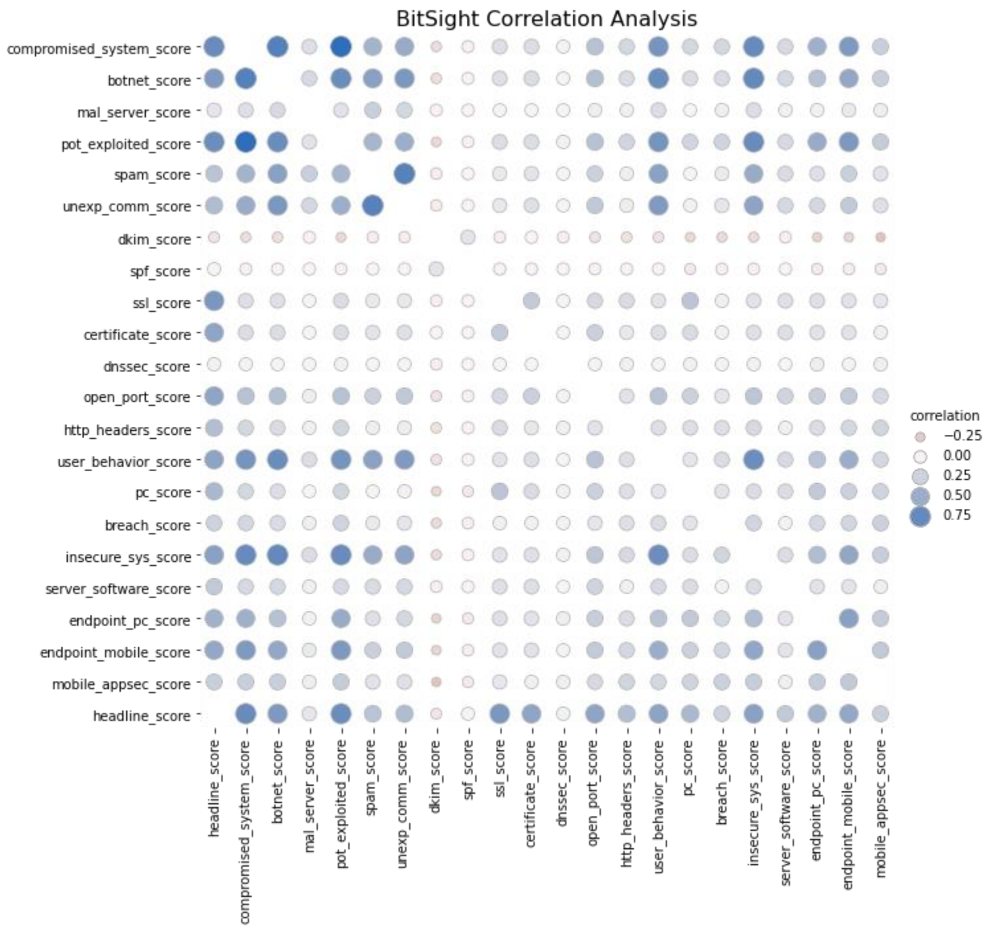
We considered 29 data points for their potential predictive value

The data points considered are a mixture of technographic and firmographic data

	Feature Name		Feature Name
1	POLICY EFFECTIVE YEAR	16	SSL SCORE
2	CLIENT	17	CERTIFICATE SCORE
3	REVENUE	18	DNSSEC SCORE
4	COUNTRY	19	OPEN PORT SCORE
5	INDUSTRY UPDATED	20	HTTP HEADERS SCORE
6	DEDUCTIBLE	21	USER BEHAVIOR SCORE
7	HEADLINE SCORE	22	PC SCORE
8	COMPROMISED SYSTEM SCORE	23	BREACH SCORE
9	BOTNET SCORE	24	INSECURE SYSTEMS SCORE
10	MALWARE SERVER SCORE	25	SERVER SOFTWARE SCORE
11	POTENTIAL EXPLOITED SCORE	26	ENDPOINT PC SCORE
12	SPAM SCORE	27	ENDPOINT MOBILE SCORE
13	UNEXPECTED COMMS SCORE	28	MOBILE APPLICATION SECURITY SCORE
14	DKIM SCORE	29	HEADLINE DETERIORATION
15	SPF SCORE		

Technographic rating correlation

A number of the 22 different risk rating factors are highly correlated.



Highly correlated features may contain similar information

Highly correlated features often means a smaller number of scores offer additive value

Highly correlated features can be grouped by expert judgement. Although the Gallagher team largely chose to consider factors independently

Institute and Faculty of Actuaries

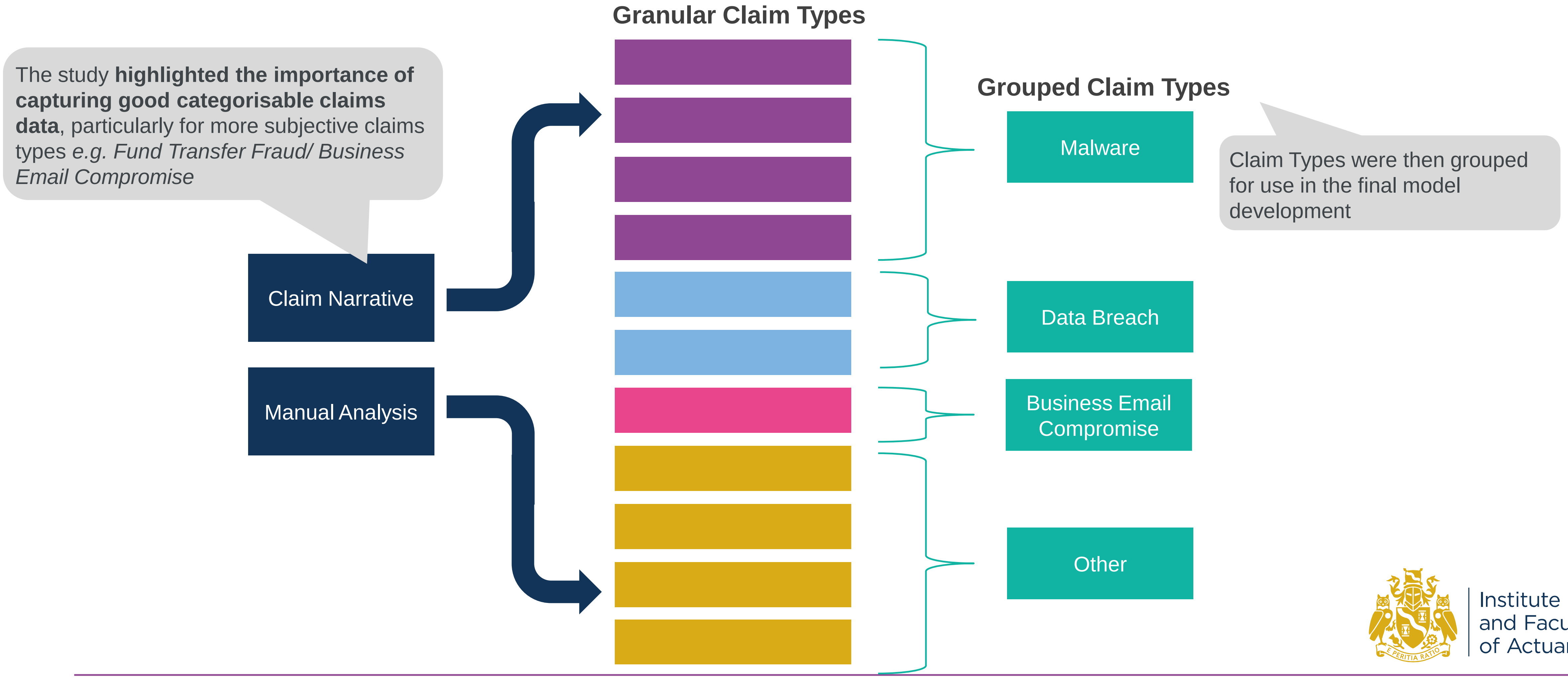
Absence of standardisation for classifying claims limits our ability to spot and respond to trends

- **Claims data is littered with inaccurate and misleading terminology** which renders useful analysis almost impossible.
- **Additional standardisation for cyber claims could see huge improvements in the ability to analyse claims data**, and hence, improve the way we can anticipate and respond to changes in the threat landscape.

Insured's website DELETING FILES
HACK Business email compromise
Credit card
UNAUTHORISED ACCESS
Scam cryptomining whale Locked
TROUBLE ACCESSING THEIR SYSTEMS ZERO DAY Fraudulent payment
Revil
Malware #BEC MALW Computer Attack
Dark Web Google cloud downtime Hacking
#ransomware System Compromise phishing BUS Email Compromise
identity theft GDPR breach Malicious Insider
SCAMMER ran Infiltration ransom
STOLEN Email account Ryuk INFECTED #Lockbit
Virus Extortion ransomware Data breach encrypted
Access denied RANSOMW Privacy incident
Wired
Mal malicious email
Demand letter online store suspicious email Social engineering
Office 365 Systematic Event Money Gone

Claim type classification

Gallagher Re utilised claims data compiled from multiple sources. **Claims** data was classified into claim types based on claim description key words, and the expert judgement of our cyber analytics teams.

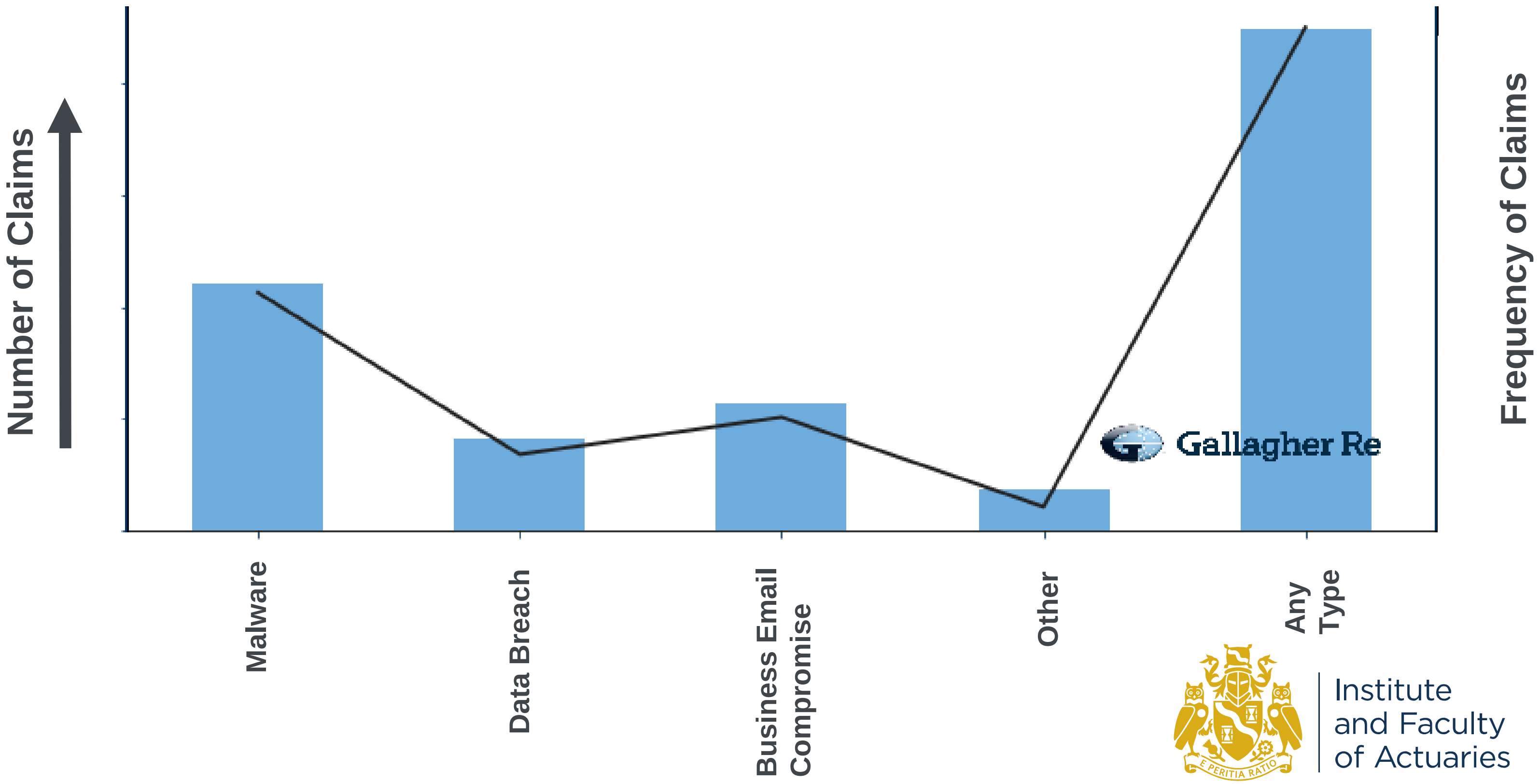


Institute and Faculty of Actuaries

Claim frequency by type

Relatively low claims data volumes, and rare event frequency makes the application of machine learning models challenging. For this reason we also trained traditional GLM based models in parallel to provide a benchmark for model performance.

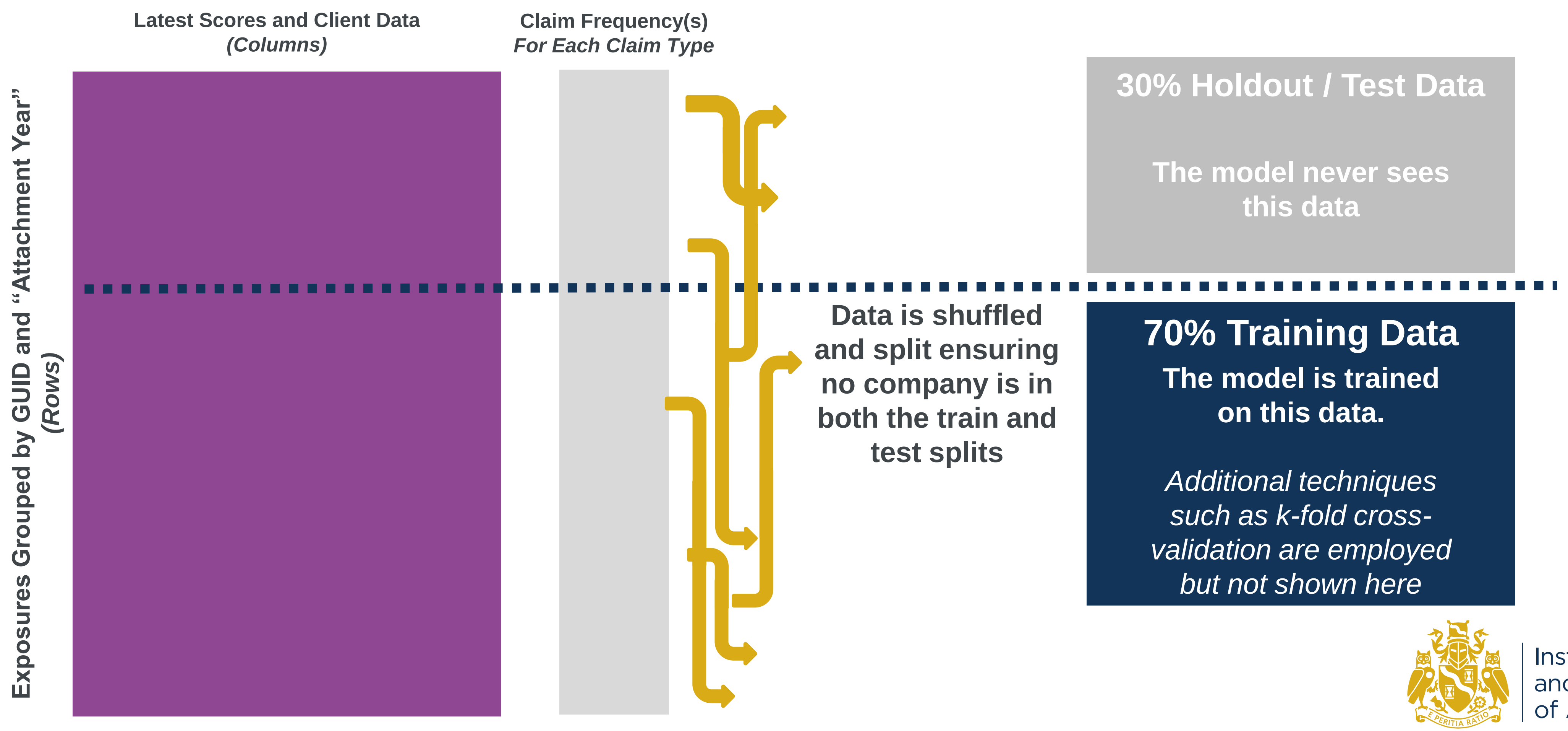
- Around **5% of firms have a loss** in a given underwriting year
- Loss Frequencies in other claims types are lower
- The relatively low frequency and volume of claims can make challenging, in particular achieving a stable model.



Institute and Faculty of Actuaries

Training and testing strategy

Splitting data into a training and holdout set enables us to better understand the real world predictive performance of the model.

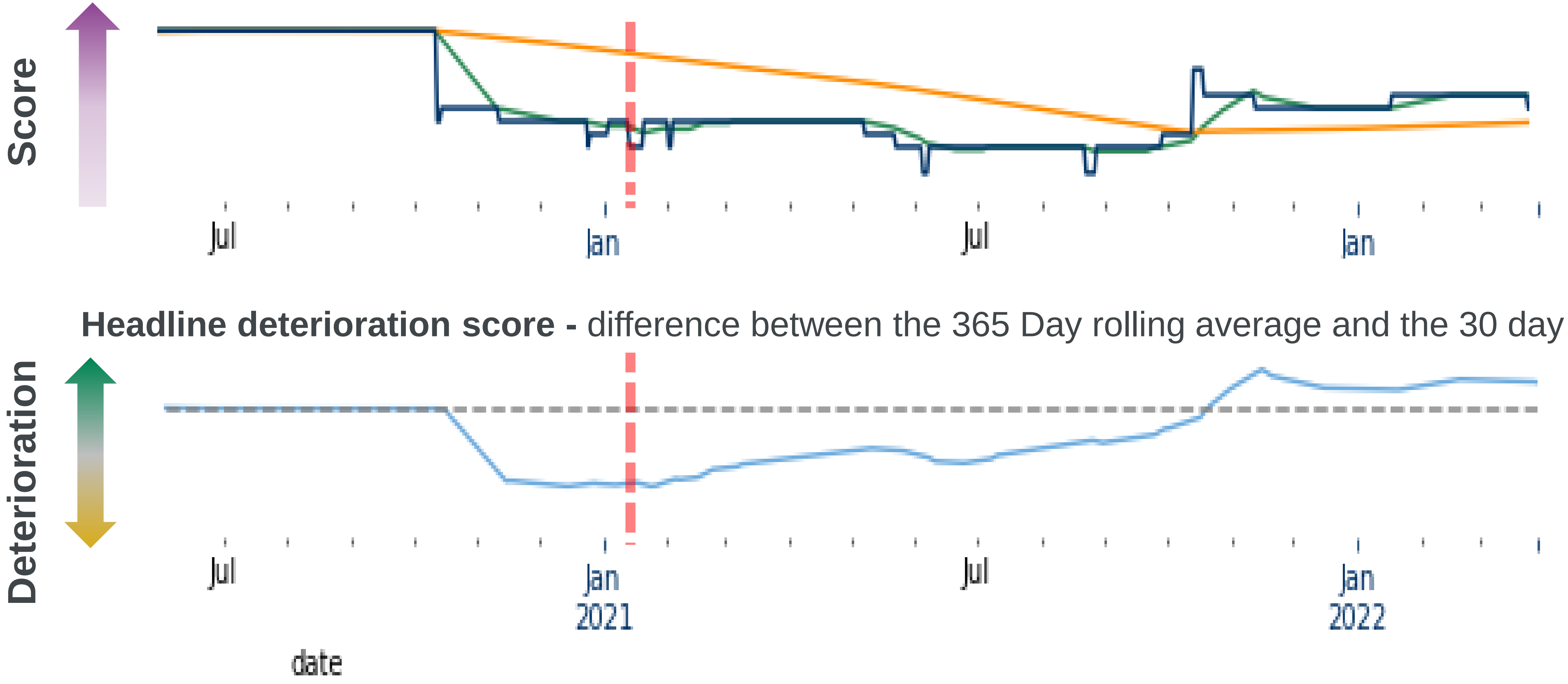


Feature engineering case study – Headline score deterioration

Feature engineering is the process of creating new features to help ML models make better predictions

Original data + rolling 365 and 30 day averages

Headline deterioration score - difference between the 365 Day rolling average and the 30 day rolling average



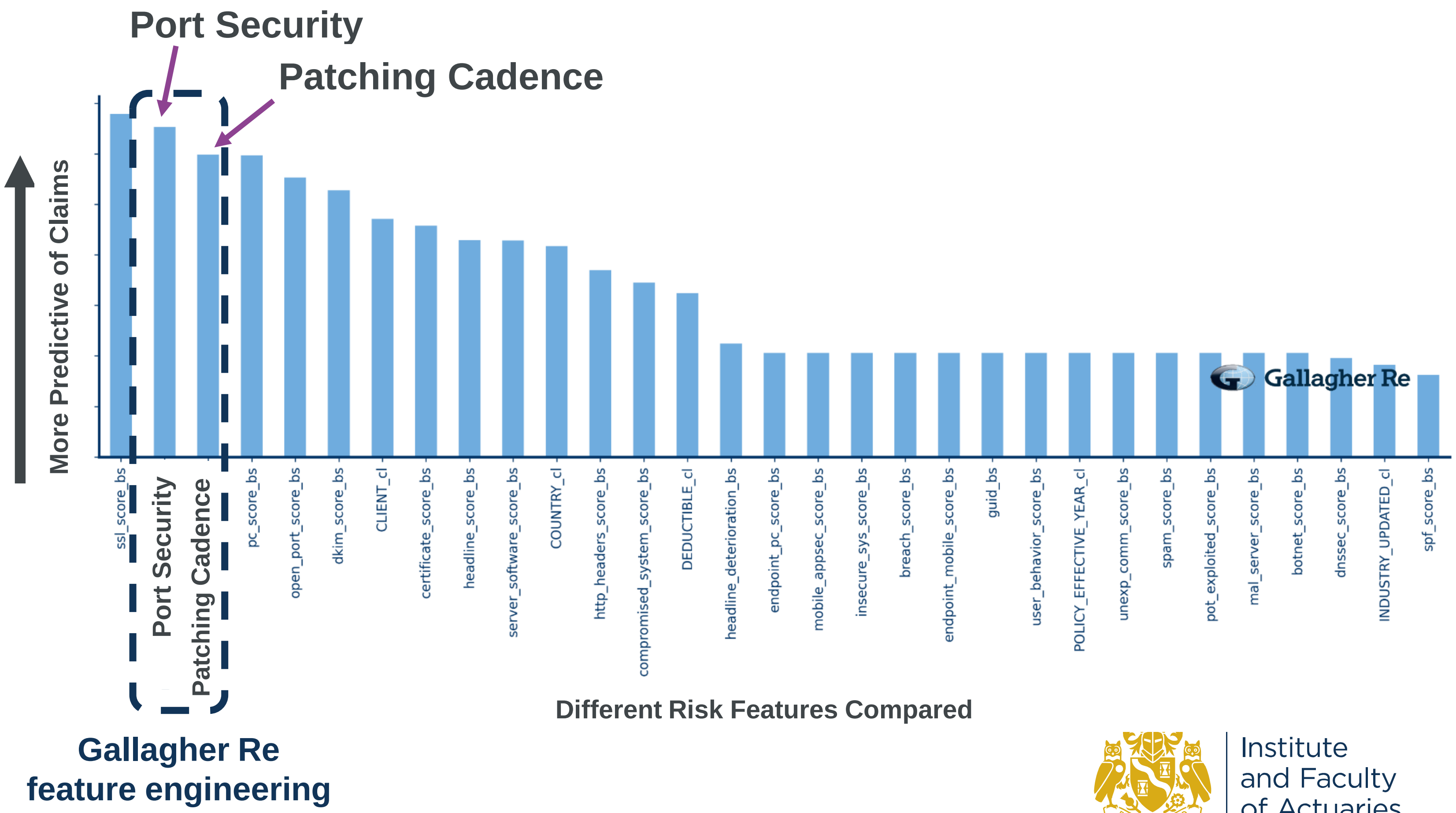
Institute and Faculty of Actuaries

Results

All claim type univariate GLMs

Open Port, Patching Cadence, and SSL Scores were deemed the most important risk features when compared independently.

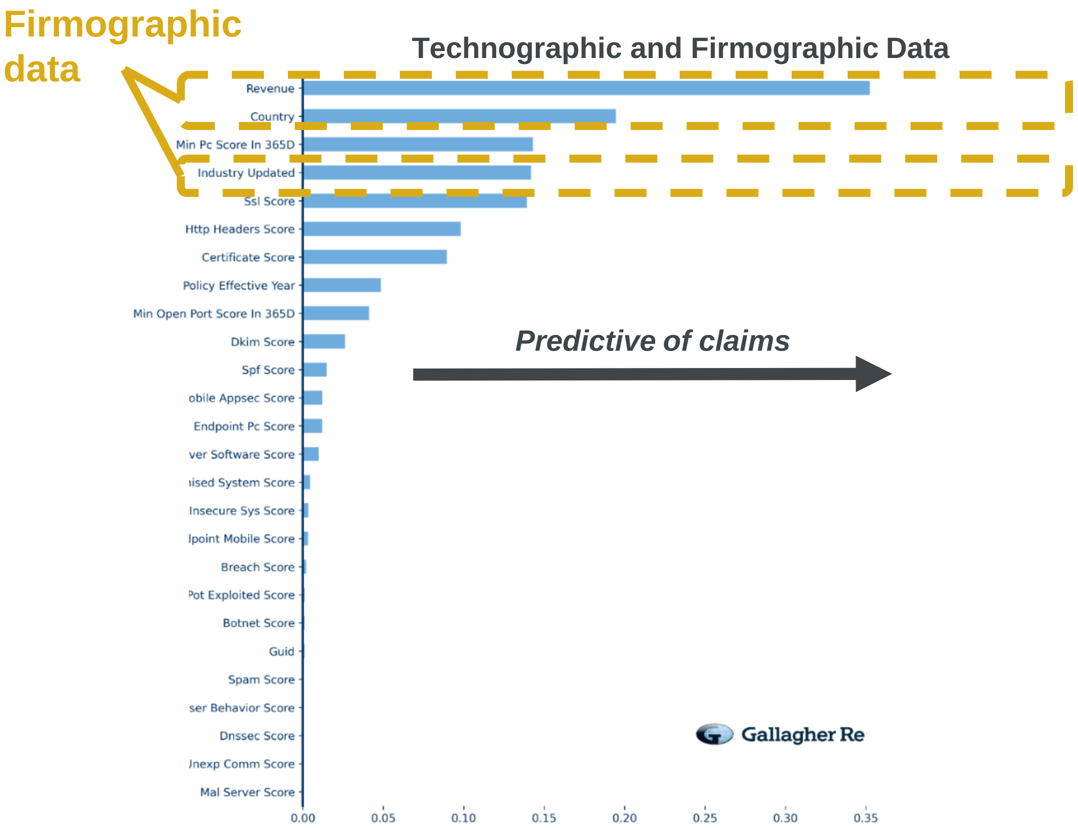
- When comparing technographic data in isolation, many hold some predictive value
- Gallagher Re engineered features were among the most predictive
- Industry seems to have low predictive value when considered in isolation

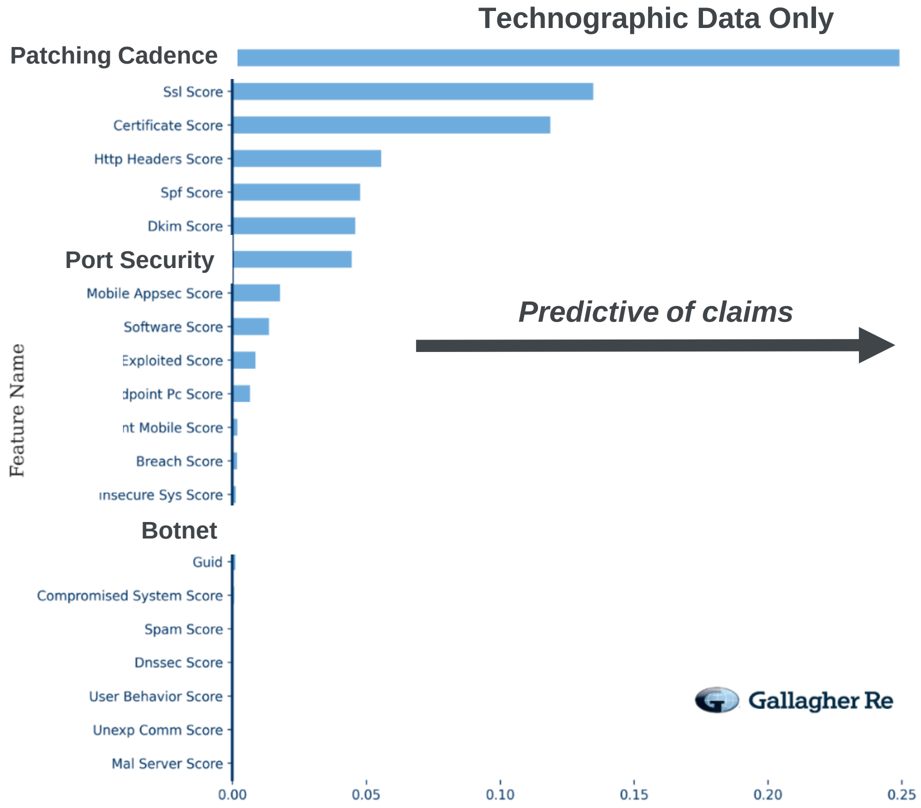


Institute and Faculty of Actuaries

All claims types feature importance

SHAP feature importance is based on the magnitude of SHAP feature attributions. SHAP values utilise game theory to compute the additive contribution of a feature to a prediction.





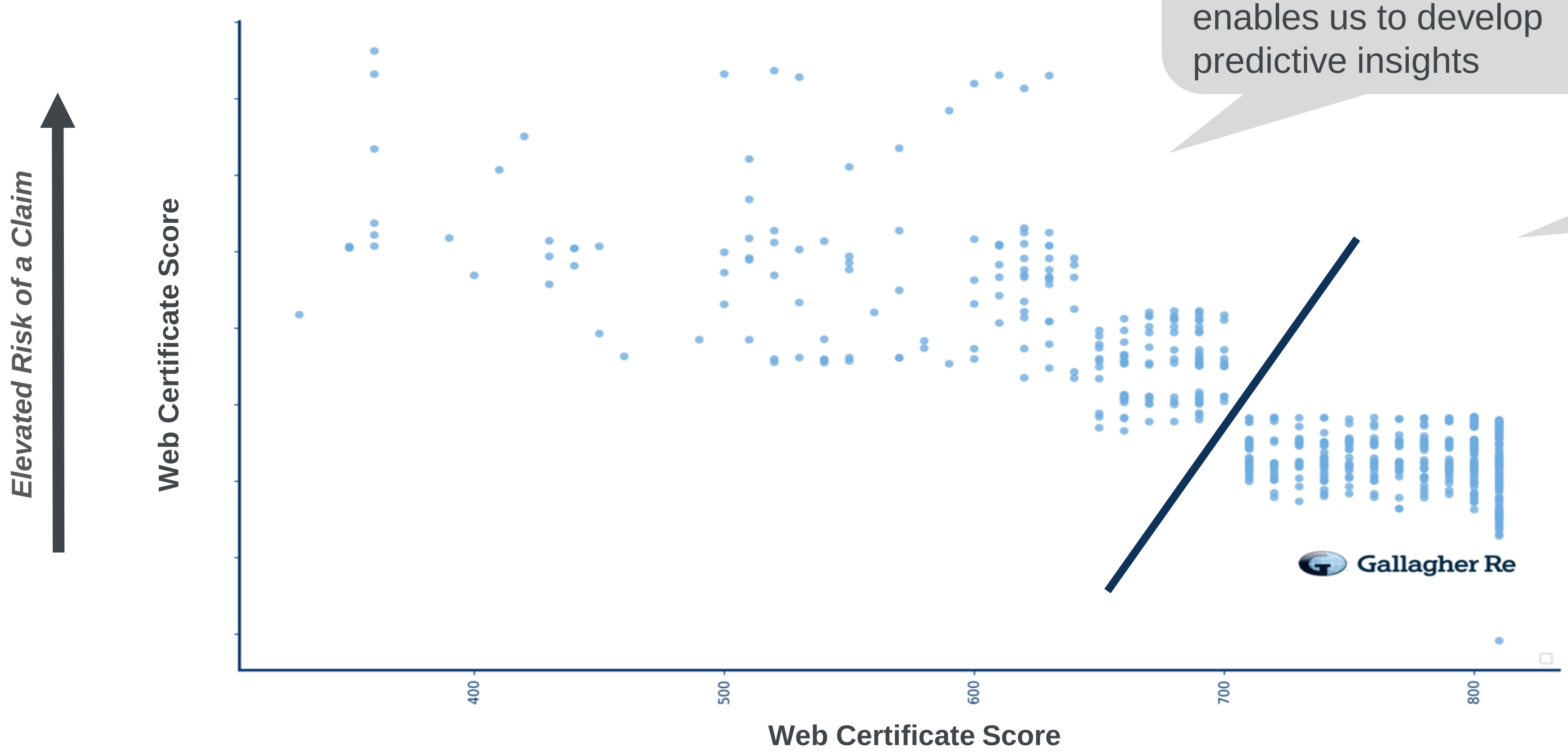
Institute and Faculty of Actuaries

All claims types prediction dependence

Interpreting charts to understand <u>when</u> a score matters.

Sample Predictive Insights

Analysing the likelihood of different types of Cyber events against risk factors enables us to develop predictive insights



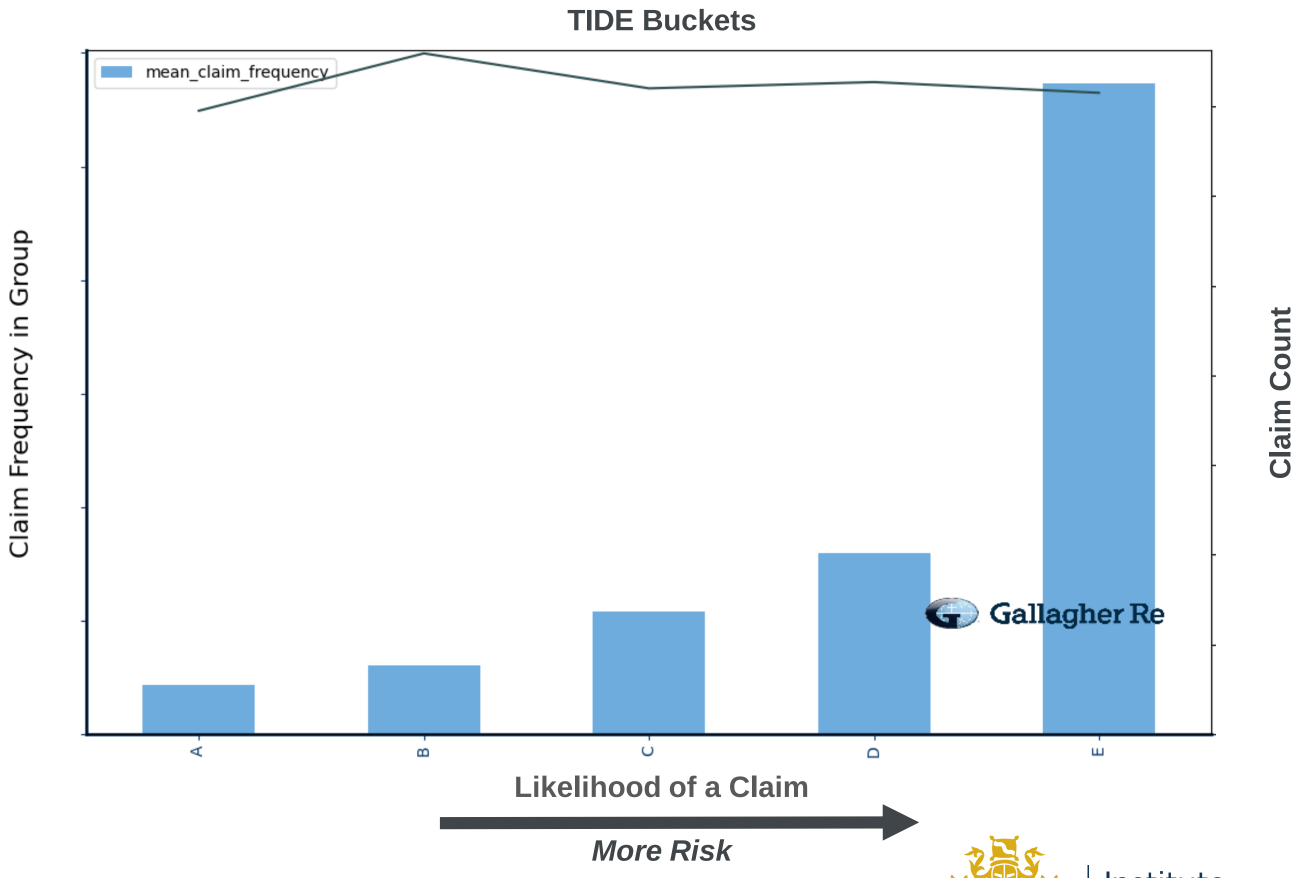
Risks with Website Certificate scores of 710 or over are statistically less likely to suffer a claim

Institute and Faculty of Actuaries

Gallagher Re TIDE results

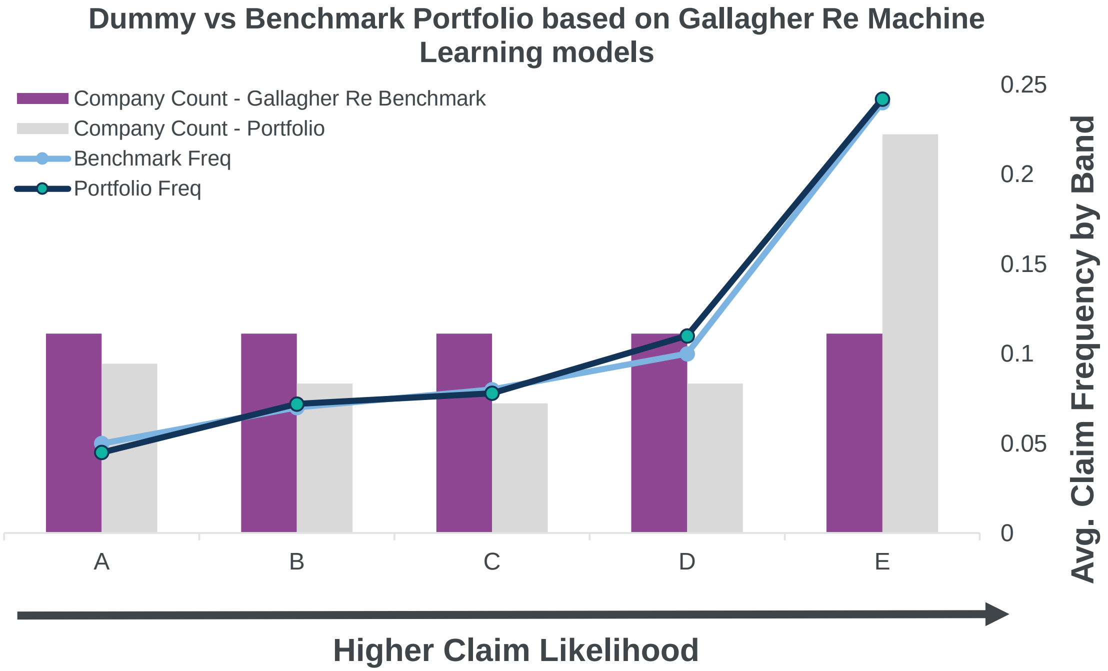
Non-Technical A-E Gallagher Re TIDE (Technographic Insight Detection Engine) Results:

- As individual scores have limited value in displaying portfolio risk, we've placed risks into 5 buckets depending on their likelihood of suffering a claim
- Risks in our modelled portfolio were placed equally into the five buckets with bucket E presenting materially more likelihood of a claim
- Other portfolios can be benchmarked against our modelled portfolio to show the % of risks falling into each bucket



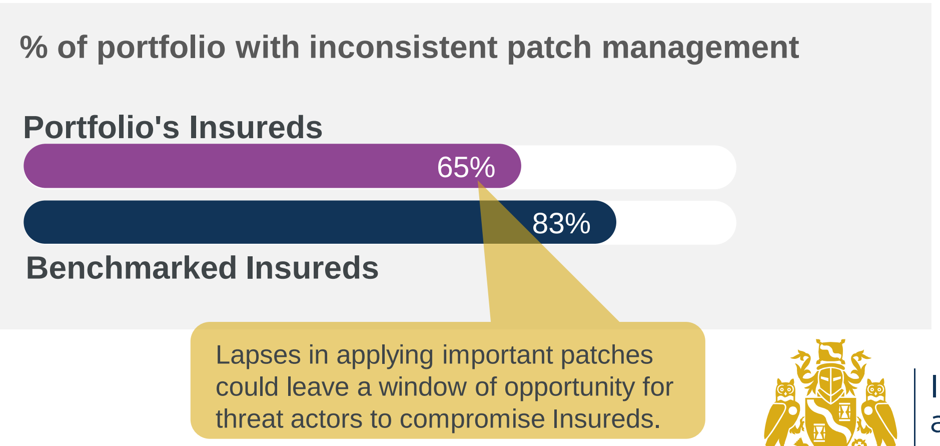
How can we use this technology to add value?

- Risks **placed in buckets between A-E depending on their likelihood of suffering a claim.** Bucket A represents those least likely to suffer a claim, with bucket E most likely.



Individual insights and benchmarking for:

- Portfolio performance against the **features we consider most predictive of claims** (below)
- Portfolio **exposure to aggregation risks through SPoF data** *e.g. cloud service providers, software solutions*
- Portfolio's **visible exposure to recent systemic events** *e.g. Log4J, Microsoft Exchange*
- Portfolio's **exposure to common attack vectors** *e.g. RDP, FTP*



Institute and Faculty of Actuaries

Next steps

Our study combined Cyber Security Ratings with firmographic, and claims data using Machine learning algorithms. The study concluded that some *“outside in”* technographic data holds the ability to predict claims.

Separate models for SME vs Large risks

Estimate financial impact of re-underwriting based on findings

Market engagement and feedback

Institute and Faculty of Actuaries

Questions?

Institute and Faculty of Actuaries

Institute
and Faculty
of Actuaries

Thank you

#GiroConf22