**Big Security Data – Project Milestone 1**

Group #13: Kindell Holst, Denesha Record, William McGuire

April 14, 2025

**Introduction and Industry Background**

The main service of the insurance industry is insurance, which provides compensation in cases of sudden or unexpected loss to those willing to pay a premium. The topic of this loss can vary drastically. For example, one of the top advertisers in insurance is progressive, who offers vehicle insurance, property and protection insurance, health insurance, life insurance, business insurance, and a whole lot more. If there is something you have of value, whether that be your car or your life, you can get insurance to protect that value monetarily.

Insurance is a massive industry, with nearly 3 million employees in the US alone. There are over 5900 US insurance companies, and they have premiums that exceed 1 trillion dollars annually, making it one of the largest industries in the nation. If the largest insurance companies in the world are ranked by asset holding, many of the top ones will come out as holdings companies that happened to be classified as insurance. A fitting example of this would be Berkshire Hathaway, which is more known as a holdings company founded by Warren Buffet, than a typical insurance provider. Because of this, the top insurance companies should be looked at by market share for specific insurance types. For property/causality insurance, State Farm and Progressive hold the greatest market share. For life/annuity insurance, MetLife and Equitable Holdings are at the top. And for homeowner insurance, State Farm and Allstate. Other big players are Travellers, USAA, Liberty Mutual, and Farmers.

Like any industry of this size, technology has become incredibly important. The claims process can now be started by a simple picture on your phone, insurance packages can now be personalized to each customer through machine learning, and they have even implemented AI chatbots to guide customers on where to go and what to do. All of this has made information technology, and the data insurance companies hold more valuable. Some car insurance companies now offer personalized plans based off your driving habits. The customer puts a monitoring device in their car so that the insurance company has proof of or lack of proof of the customer's safe driving. This all adds up to more customer information being known due to the presence of more monitoring technology. A byproduct of this is more customer information being known than ever before, which can be taken advantage of in the wrong hands.

**Relevant Threat Trends in the Insurance Industry**

The most common data threat in the insurance industry is a personal info breach. This can involve hackers accessing customer or employee information including names, phone numbers, social security numbers, bank account info, even life insurance records and policies. These data breaches have cost the industry and customers countless dollars and hours. Companies are often legally required to provide costly services to customers in the wake of a data breach, but they still cost time and energy from the customer to clean up. Another area of concern is hackers targeting IT systems directly in ransomware attacks. A ransomware attack involves locking a company out of its computer systems and requiring them to pay a ransom to regain access. Companies often pay the ransom because it is cheaper than trying to get around the hacker’s systems. ([The insurance industry cyber crime report: recent attacks on insurance businesses | Insurance Business America)](https://www.insurancebusinessmag.com/us/guides/the-insurance-industry-cyber-crime-report-recent-attacks-on-insurance-businesses-448429.aspx)

One recent cyberattack that has affected many organizations is the MOVEit hack, perpetrated by the Cl0p ransomware group. MOVEit is a file transfer system. Cl0p exploited a vulnerability in the system and was able to gain access to many companies, compromising data of millions of people. ([What You Need to Know About the MOVEit Data Breach - Experian).](https://www.experian.com/blogs/ask-experian/moveit-data-breach/) Another common strategy is sim-swapping. This involves a hacker getting control of your phone number which allows them to use two-factor authentication to access your accounts and systems. The hacker needs to convince your mobile carrier to transfer your phone number to them. To do this, they need personal information which can often be found on social media. ([What is SIM swapping & how does the hijacking scam work? – Microsoft 365)](https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-sim-swapping) Hacker Noah Michael Urban is alleged to have 59 sim swapping victims as a part of the group Scattered Spider. ([What is SIM swapping & how does the hijacking scam work? – Microsoft 365)](https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-sim-swapping)

The industry continues to see regular attacks from individual hackers, ransomware groups and organized cybercriminal groups. Another threat is from Advanced Persistent Threat (APT) groups sponsored by countries such as Iran and North Korea. These groups often target organizations for finanicial gain. For instance, North Korean group Lazarus completed a cyperheist against a Federal Reserve Bank of New York account that belongs to Bangladesh Bank. ([11 biggest financial sector cybersecurity threats | CSO Online)](https://www.csoonline.com/article/3609168/11-biggest-financial-sector-cybersecurity-threats.html)

**Critical Assets**

1. **Customer Information**

Customer information is one of the most valuable and vulnerable assets of an insurance company. Accurate customer information databases are critical to correct and competitive pricing and risk assessment. They allow the company to ensure premiums are competitive but high enough to offset claim costs while maintaining a reasonable profit. If customer information is compromised, the company is at risk of great financial harm. Additionally, the company has an ethical obligation to protect customer information. Customers entrust the company with their information and that should not be taken lightly. This asset is used by employees across the company as well as third party agents and vendors to set pricing and work claims, so it is essential that all employees and outside parties are properly trained on appropriate safeguards.

1. **Propriety data and models**

Proprietary data is used to develop models and risk assessment tools used to set pricing, assess risk and minimize claim cost, among other uses. If these models are not kept private, the company may lose competitive advantages which can lead to higher costs. These models are used by analysts to find ways to improve the company’s competitiveness and profitability.

1. **Investment Portfolio**

The company maintains a robust investment portfolio to offset financial risk and maintain solvency in the face of catastrophic events. These events ebb and flow but can happen many times a year with some degree of unpredictability, so the company needs to be able to finance fluctuating costs. The investment portfolio is accessed by the company finance department and the financial institutions holding the investments, leaving it vulnerable to the same threats banking institutions face, such as hackers.

1. **IT Infrastructure**

The IT infrastructure, including hardware as well as cloud services, is essential to company operations. Without it, there would be no company, no way to perform work, to service customers, to process claims. It is the backbone of the organization. It is accessed by every employee and third party vendor, from the CEO to the IT technicians to the janitor who must badge in and out of secure areas. The infrastructure is vulnerable to hackers at every level and any breach has the ability to cripple the company.

It is essential for the company to have a proactive cyber security threat operation to protect the infrastructure from hackers attempting to damage the company.

1. **Reputation**

The company’s reputation is everything. While not a tangible asset, it is a critical one. Customers make their decisions large based on how much they trust a company. It takes a long time to establish a good reputation, but it can be destroyed in an instant. If the company is victim to a data breach, many customers will leave the company and never consider returning. Every employee must be committed to protecting customer information and maintaining a good reputation for the company.

**Threat Scenarios for Our Insurance Company**

In today’s interconnected world, our company faces numerous cyber threats targeting our most sensitive and valuable assets. Below are five detailed threat scenarios, each outlining the adversaries involved, their capabilities, the infrastructure they are likely to exploit, and the victims within our organization.

1. **Customer Information**

**Adversary:** Organized cybercriminal groups that focus primarily on the insurance sector.

**Capabilities:** These attackers excel in social engineering and phishing techniques and are adept at exploiting vulnerabilities in third-party vendor systems which are often less tightly regulated, allowing them to bypass standard security measures.

**Infrastructure Exploited**: They target compromised IT systems at the broker or agency level, using malware and spyware to infiltrate and extract data from vulnerable vendor networks.

**Victim:** The direct victim is the customer data managed by our company and its third-party vendors. A successful breach here could lead to identity theft, fraudulent claims, and a significant loss of customer trust.

1. **Proprietary Data and Models**

Adversary: Nation-state sponsored groups or corporate espionage actors motivated by a desire for strategic advantage.

**Capabilities:** These groups are proficient in advanced persistent threat tactics. They can perform sophisticated network intrusions and lateral movements within secure environments to access highly guarded information.

**Infrastructure Exploited:** They exploit vulnerabilities in our internal networks, often through zero-day exploits, to breach secure data repositories and systems that process our proprietary actuarial, pricing, and historical claims models.

**Victim:** Our proprietary data and models critical for maintaining our competitive edge are at risk. A compromise can undermine our operational accuracy and strategic positioning in the market.

1. **Investment Portfolios**

**Adversary:** Financially motivated cyber thieves or fraudsters targeting high-value systems.

**Capabilities:** These attackers specialize in manipulating financial transactions and exploiting weak access controls. They are also skilled at social engineering, often securing access credentials from employees responsible for overseeing investment portfolios.

**Infrastructure Exploited:** They may infiltrate trading systems or online banking applications linked to our investment platforms, including potentially misusing electronic funds transfer (EFT) systems.

**Victim:** Our investment portfolios and the financial systems that safeguard our risk management efforts are the primary targets. A breach could lead to direct monetary losses and adversely impact investor confidence and overall risk management.

1. **IT Infrastructure**

**Adversary**: Hacktivists or nation-state actors employing ransomware and denial-of-service (DoS) tactics.

**Capabilities:** These adversaries are known for exploiting unpatched systems and misconfigured cloud environments. Their methods include launching large-scale distributed denial-of-service (DDoS) attacks and deploying ransomware, which can severely disrupt operations.

**Infrastructure Exploited:** They target our critical servers, network devices, and cloud infrastructure, particularly legacy systems that lack modern security standards.

**Victim:** Our overall IT operational environment becomes vulnerable, and disruptions here can lead to significant service outages, loss of data, and collateral damage to interconnected systems essential for day-to-day operations.

1. **Reputation**

**Adversary:** Disgruntled insiders or external activist hackers focused on damaging our public image.

**Capabilities:** These actors are skilled in launching digital smear campaigns and coordinating social media manipulation. They might leak sensitive information or deliberately falsify data, quickly spreading negative narratives online.

**Infrastructure Exploited:** They often leverage compromised customer data or internal communications to fabricate damaging stories using bot networks and fake accounts, they amplify misinformation across social media and news channels.

**Victim:** The company's reputation is the ultimate casualty. Damage to our brand can severely diminish customer confidence, lead to financial penalties, and cause long-term erosion of market trust.

**Intelligence Buy-In**

Cyber Threat Intelligence (CTI) is more than just another line item on our budget, it is a smart proactive investment for our insurance business. We deal with sensitive customer information, proprietary underwriting models, and sizable investment portfolios every day. In an era where cyber adversaries are constantly refining their tactics, our industry is in the crosshairs not only because of our own systems but also through our brokers and agencies, which often have less strict oversight. With nearly 60% of data breaches linked to third-party vendors, having a robust CTI strategy is not a luxury; it is a necessity.

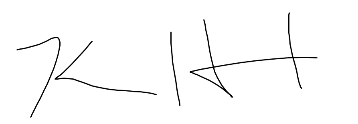
The digital landscape is evolving fast, with cybercriminals using ransomware, phishing, and advanced persistent threats to target not just our IT infrastructure but also the valuable data we hold. When attackers hit an insurance company, the damage is enormous due to lost customer trust, heavy financial penalties, and exposure of our critical actuarial and risk models. Past incidents in our sector have seen breaches costing millions, and these events drive up insurance premiums and operating costs, affecting our bottom line.

By integrating CTI into our security strategy, we are not waiting for an attack to happen. Instead, we are positioning ourselves to identify and counter threats before they escalate into full-blown breaches. This approach allows us to make smarter, more informed decisions, invest effectively in our most vulnerable areas, and fine-tune our incident response plans. In the competitive insurance market, this proactive stance not only shields our invaluable assets but also protects our reputation and ensures long-term profitability.

**Group Roles and Signatures**

Part 1 – William McGuire

Part 2 – Kindell Holst



Parts 3 and 4 – Denesha Record