White paper

The next ransomware attack is likely to be launched using an actual employee's credentials

How to accurately underwrite cybersecurity insurance

Executive Summary

With the increase in ransomware attacks over the past year, existing software tools to measure cyber risk have fallen short. As a result, insurers have begun to increase their utilization of third-party vendors to assess policyholders' external networked environments, which help inform premiums and scope of coverage. Insurance organizations can reduce their risk of cybersecurity claims by accurately predicting which companies are likely to become a victim of a ransomware or cybersecurity attack in the near future.

Problem

The $6 Trillion Cybercrime industry[1] exploited corporate vulnerabilities with new phishing methods to deliver ransomware, thus cyber rates have increased an average of 18% in 2021[2]. Most of the current tools analyze the cyber hygiene of a business based on a scan from outside the business — networks, open ports, software patching cadence, etc. All these aspects are essential parts of assessing cyber risk; however, this method does not consider the errors created by the employees of a business who are susceptible to phishing attacks in both their personal and work lives.

Solution

Experian's Cyber Risk Score predicts the likelihood of a cyber attack in the next 12 months by calculating each employee's cyber exposure in **both their personal and work lives** and then combines with risk data about the business. This prediction is calculated using many attributes, whether threat actors are able to construct employee credentials and gain network access to then implant malware inside the perimeter defenses.

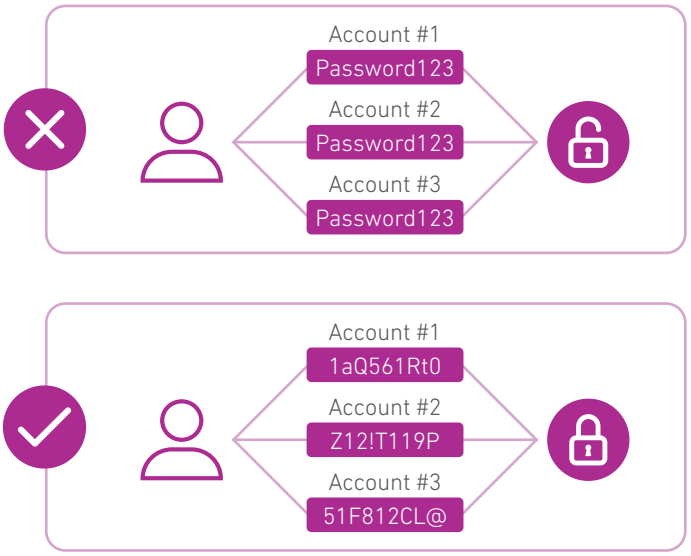
Data predicted the Colonial Pipeline attack

The May 7th, 2021 ransomware attack on Colonial Pipeline, which provides fuel to 45 percent of the US East Coast, seemed sudden to the organization and the outside world. The attack shut down the pipeline for six days[3] and caused significant disruption to travel and daily activities for people in the affected region. However, the company's cyber risk exposure had been increasing for over a year. According to Bloomberg[4], the hackers gained entry to the network through a virtual private network account using a single compromised password.

Security consultants found the account password available on the dark web, indicating that an employee may have used the same password on another account that was involved in a breach.

The Colonial Pipeline attack was predictable based on Experian's model score that put it in the riskiest decile 16 months before the May 2021 attack (at the time when an underwriter would have been assessing whether to extend cyber coverage to the business or not).

With a model that considers employee behavior and employee personal information available on the dark web, the devastating attack could have been predicted by an underwriter. Insurers considering underwriting Colonial could have made an informed decision to either decline writing the policy or, using Experian insights, ask direct questions about email/password policies before deciding on a premium amount.



[1] https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/
[2] https://www.insurancejournal.com/news/national/2021/05/27/616176.htm
[3] https://www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636
[4] https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password

Cybersecurity attacks on the rise

Since the COVID-19 pandemic began in March 2020, cybersecurity attacks have significantly increased. In 2020, the IC3 (the cybersecurity division of the FBI) received 2,474 complaints identified as ransomware with adjusted losses of over $29.1 million, which is an increase from 2,047 complaints identified as ransomware with adjusted losses of over $8.9 million in 2019[5]. Deloitte[6] found that before the pandemic, only 20 percent of cyberattacks used previously unseen malware or methods. However, the rate of novel attacks increased to 35 percent during the pandemic.

Rate of novel attacks increased to **35%** during the pandemic

Organizations that are victims of an attack suffer financial losses in addition to reputational damage. Scripps Health, based in San Diego, California, reported that the May 1, 2021 ransomware attack they experienced cost almost $113 million, including $91 million in lost revenue. Additionally, the attack caused disruptions in hospital operations for nearly a month, including the healthcare organization's ability to treat patients. Months before the attack, Experian's Cyber Risk model detected an increase in corporate emails exposed on the dark web, which influenced the model to predict Scripps had the highest likelihood of an attack.

Hiscox research revealed that 63% of the small business workforce is now working remotely and 53% of small businesses in the US believe they are now more vulnerable to cyber-attacks[7].

Cyberattacks and data breaches are expensive and increasingly common. In fact, 60% of small businesses[8] go under within six months of a cyberattack.

Gaining access to employee accounts provides gateways for attacks

Many experts feel that by focusing on reducing the ransomware attacks started by malware, organizations can significantly reduce their overall cybersecurity risk. Because 92 percent of malware originates from phishing attacks[9] , reducing these kinds of attacks should be a high priority for companies.

An email address, either corporate or personal, is the gateway to a person's digital identity. Employees use their emails as their user names for logins for many different systems, both internally and externally. In addition, Google discovered that 65 percent of users use the same password[10] for multiple websites and applications, and 51 percent gravitate to a favorite password for most, if not all, of their accounts.

Once a hacker obtains a list of a person's previous passwords, they can attempt many versions until they gain access to the person's account. Since people often use the same password for home and work, if a perpetrator discovers someone's personal email or login password, they can often use that to access the work email and also gain access to the corporate network. With access to someone's account, perpetrators can even acquire the knowledge to answer or reset someone's security challenge questions.

Employees represent significant risk for organizations when it comes to ransomware attacks. When a perpetrator gains access to someone's email and password, they have access to many data points — such as sensitive company info, where they are traveling, their pet names and upcoming vacations. This information combined with access to their credentials, allows threat actors to engineer attacks that provide access to corporate networks, apps and data.

[5] https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

[6] https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html

[7] https://www.hiscoxgroup.com/cyber-readiness

[8] https://www.openpr.com/news/2392272/cyber-security-insurance-for-small-businesses-market-stunning

[9] https://purplesec.us/resources/cyber-security-statistics/

[10] https://www.forbes.com/sites/daveywinder/2019/02/05/google-reveals-a-big-problem-with-passwords-on-safer-internet-day/?sh=54fb99a35e0b

Accurate underwriting depends on evaluating many factors

To reduce losses and achieve profitability, cyber insurers must accurately underwrite policies to mitigate their own risk. A company's credit rating, financial stability and cash flow are good indicators of business health. Insurers need to incorporate cyber risk data to help them evaluate the exposure that is associated with a business. By using a cyber risk score, carriers can accurately price and set thresholds for exclusion.

Insurers today use technology to determine a company's risk of cyberattack by scanning from the outside to determine what ports are open and what software patches are needed. Outside-in scanning doesn't reveal the exposed employees inside the perimeter. Their credentials and behaviors in both their personal and work lives are analyzed alongside hundreds of business attributes.

Current cybersecurity underwriting strategies that utilize perimeter scanning services do not consider one of the most critical indicators of a potential cyberattack — employees credentials exposed on the dark web.

With the increase of remote work, employees are increasingly blending their work and personal lives more than ever, making more devices vulnerable to sharing information. A Malwarebytes study[11] found that more than half of remote workers reported using a work assigned device for personal tasks. Specific tasks included sending or receiving personal email (52 percent), reading the news (52 percent), shopping online (37 percent) and checking social media (25 percent). Each site or application where the employee uses their personal or work email as their username increases the risk of the company being a victim of a cyberattack.

Companies using contractors add additional risk and complexity to cybersecurity. Contractors often use the same email for their work for many different organizations, which increases each organization's risk. Companies often use multiple contractors or freelancers throughout the year, including some for short-term projects. The fluidity these gig workers add to the equation makes it even more challenging to assess an organization's risk.

Experian Predictive Cyber Model more accurately predicts risk

Traditional cybersecurity underwriting tools evaluate future risk based on the risk of a company being attacked today. In the fast-moving world of cybersecurity, this assessment quickly becomes outdated and irrelevant. To more accurately predict the likelihood of an attack during the life of a policy, Experian's Cyber Risk Score uses a deep learning Identity Platform with data artifacts from across the Corporation to predict the likelihood of an attack over the next 12 months.

To underwrite a policy for 12 months, the insurer needs to predict how employee exposures will expand over time and what effect that will have on the risk of the business. Current scanning methods are not predictive, they are a snapshot of a company's defenses "today" with no modeling of how the past and current day exposures will change over the life of a cyber policy.

[11] https://blog.malwarebytes.com/malwarebytes-news/2020/10/work-devices-for-personal-use/

Experian's Cyber Risk Score looks at everyday actions of employees, such as the sites they visit, the strength of the passwords they use, and password repetition to determine the organization's cyber hygiene. For example, if an employee visits an unsafe website, it increases the risk that their digital identity could be compromised. It understands when employees access these websites using a personal email address versus using a business email address to login. The risk profile can't be fooled, using a personal email to access an unsafe website will not reduce the risk.

While each single action appears to be a negligible risk, when they're multiplied across the entire organization, the actions of employees can quickly add up to a significantly higher risk of the company becoming the victim of an attack.

> " By looking at the risk employees are creating from within, the Experian model accurately predicts cyber risk and attacks. Experian's Cyber Risk Score found that 44 percent of all cybersecurity claims were in the worst-scoring 20 percent of the companies, per the model. "

Experian's team of experts includes dark web "actors" who have been accepted into the dark web community with natural language speakers in Russian, Chinese, Korean and others. This allows Experian to participate in discussion groups and dark web forums about where attacks are being planned and where to gather harvested data from those attacks.

Once the data is gathered, Experian's model calculates the Cyber Risk Score using 500 different business and credit attributes and 140 cyber attributes.

Creating a more profitable cyber insurance business

The current approach to cyber insurance underwriting needs forward-looking models. The 2021 IBM Cost of a Data Breach Report[12] found that the average cost of a data breach increased 10 percent between 2020 and 2021 from $3.86 million to $4.24 million. Additionally, the report found that the cost difference in breaches where remote work was a factor was $1.07 million. With the rate of cyberattacks expected to rise and remote working remaining higher than pre-pandemic levels; cyber insurers should expect increased claims amounts.

By moving from an underwriting model that only focuses on a snapshot of today to one that predicts the future cyber risk of a company, based on employee exposure, insurers can more accurately price and balance their portfolios. With Experian's Cyber Risk Score, insurers can make a more accurate assessment of each policy submission and renewal, reducing claim losses.

[12] https://www.ibm.com/security/data-breach

Let Experian help you on your data journey

To learn more, contact an Experian representative at 1 800 520 1221 or visit www.experian.com/b2b.

About Experian's Business Information Services

Experian's Business Information Services team is a leader in providing data and predictive insights to organizations, helping them mitigate risk and improve profitability. The company's business database provides comprehensive, third party-verified information on 99.9 percent of all U.S. companies and millions of companies worldwide. We provide market-leading tools that assist clients of all sizes in making real-time decisions, processing new applications, managing customer relationships, and collecting on delinquent accounts.

Experian
475 Anton Blvd.
Costa Mesa, CA 92626

T: 1 800 520 1221
www.experian.com/b2b

010/21 • 1267-BIS