Why Cyber Insurance Should be Your SOC's New Best Friend

Speaker:
Catherine Lyle
HEAD OF CLAIMS, COALITION

Three things to know about me

I'm a lawyer

I  data

I'm not here to bullshit you

A few caveats

(I am a lawyer after all)

Claims data comes from **three sources**: our own policyholders, market data (NAIC), and insurance applications.

Our underwriting and risk engineering capabilities are **unique among cyber insurance providers**. As a result, we may see different types of claims than others.

Recently reported claims will continue **to develop and mature**. The report contains our current loss estimates through 2022, but these may fluctuate in overall severity in the coming months.

We have a shared mission

IT & Security teams

Insurer

The cyber crime market has shifted

Threat actors are increasingly sophisticated

If you're being hacked, you've been phished?

FTF and Ransomware are on fire

Threat actors are increasingly sophisticated

The professionalization of TAs

THEN

Wearehere <wearehere@protonmail.com> 5/20/16

to me

man i was waithing you to provide me a bitcoin address 4 hour.but you didnt if you can i really send you money. today i buy a samsung galaxy tab 2 to my child.and love moshcino mounted.and tommy hilfger jean and shirt.and goes to steak house for dinner.so today i lost 1000 usd :) so money goes.but what i can for you is i can send you another decryption key from your proccessor.there is 43 server infected and you r the 2 person contact me.there is 40 server infected i can give you more key if you want. i dont know u r from process managament team.answer me asap if you want another key.or i can provide u 2 key i am a little bit drunnk. :) LOL

NOW

At the initial stage, we will execute options A, B, and D at night. If you persist in wasting our time with futile tactics, we will be compelled to employ the remaining options with a well thought out strategy. You are fully aware of the consequences that await you if you continue to disregard our warnings and fail to adopt a serious approach. Prepare yourself for the forthcoming difficulties if you don't bring a substantial offer to the table today.

They study financials...

You

You are not well aware that we have been suffering financially. If this was the case you would never ask us for 18 million dollars because you know that would be impossible for us to pay. 8 million is also impossible as we do not have those funds available to us.

Support

We're still reviewing your financials and we see that you've 24 millions usd in WF investment account. Is that correct ? And Now, are you telling me that you're willing to pay just 1 million for everything ? Are you aware what's coming for you that you just don't find it worth more than your 1 million?

Support

You were trying to trick us with 1m and You're going to see what happens next!

...familiarize themselves with organizational relationships

Support

So, You won't need a decryptor. We offer an additional 20% discount when we complete the agreement without a decryptor. We will take care of data deletion and provide an additional security report.

We understand that data security is important to you, especially considering that your CCC-ONE XML reports already contain extensive information about insured customers' private details when you submit claims to insurance companies. If their information were to be leaked, it would cause significant problems for you, such as contacting companies like GEICO or any other and exposing them to the leak. We believe you have already obtained a favorable price by agreeing to work with us. Your price is rounded as 14,000.000 USD.

And apply pressure with depth and clarity.

Support

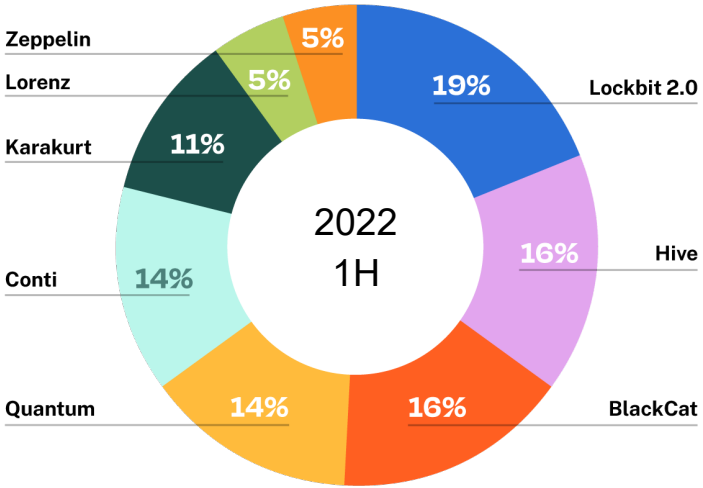
We have shown enough proof and provided insights to demonstrate that we possess complete data from you, as evidenced by the images and file reports you have browsed. You are well aware that we have all the necessary information ( ) . Our advice to you is: don't waste your time with meaningless questions and feigning ignorance. We have been polite in our efforts to resolve this matter confidentially. However, if you continue to prolong the process and miss the deadline, we will no longer maintain a friendly demeanor.

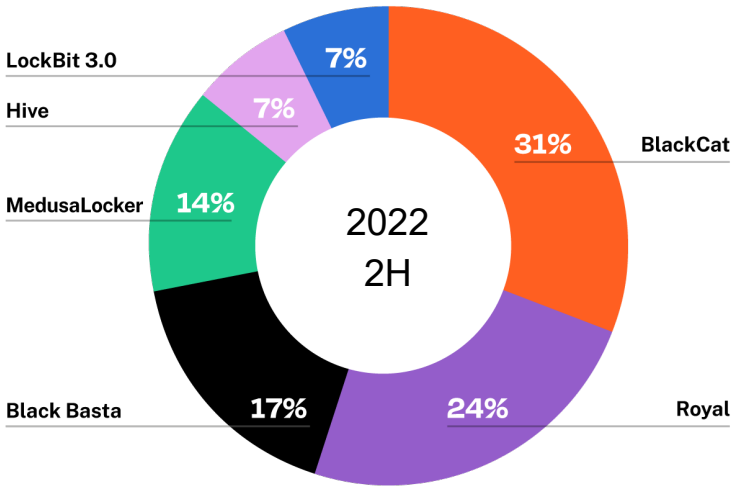
Furthermore, your contracted partners, such as and others, will not appreciate your inability to protect the confidential data and the resulting risk of a breach.

Make your decision today, or if you choose to prolong this negotiation, we will take immediate actions against your company and As a result, you will end up paying the non-discounted price to retrieve your data and decryptor. Your choice. Time is running out.

They continually adapt their attacks

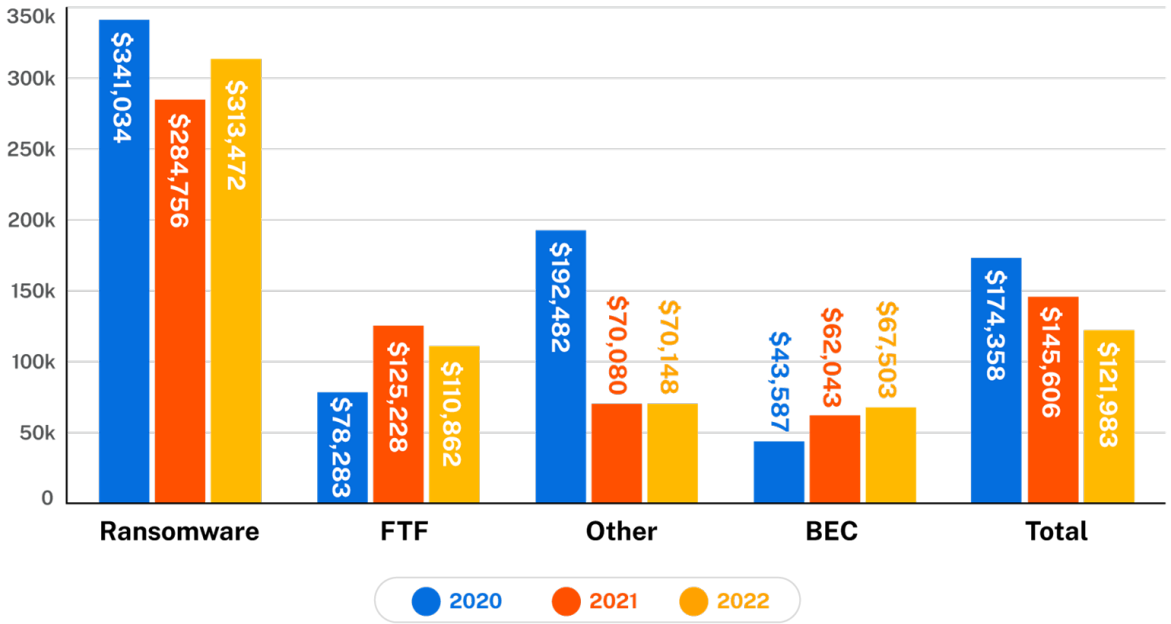
Top ransomware variants by number reported





Claims Severity by Event Type

Ransomware claims severity jumped 10% to an average loss of $313,472.



Ransomware is on fire

Ransomware returns

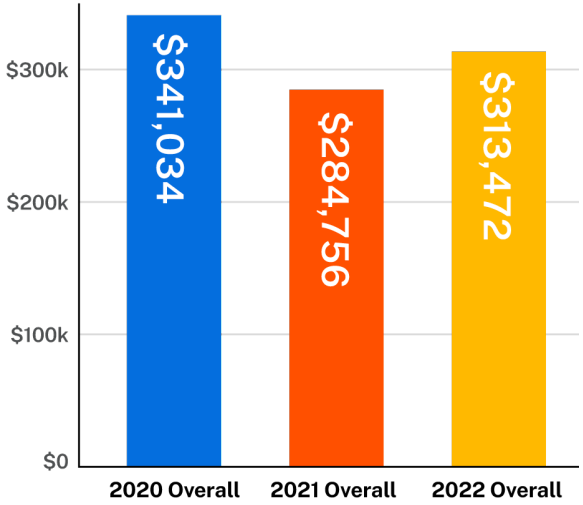
+27.3%

FREQUENCY

Between 2H 2022 and 1H 2023

...and is increasingly costly

RANSOMWARE SEVERITY



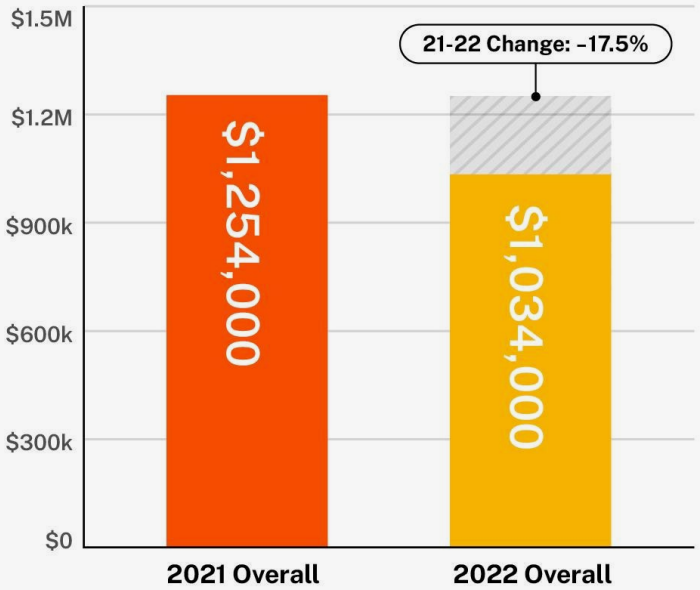
$478,863

SEVERITY in 1H 2023

Ransomware demands

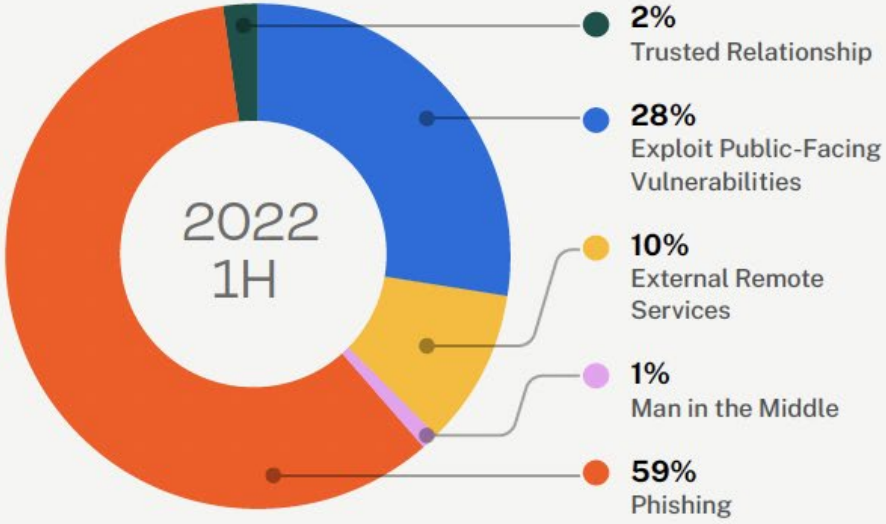
$1.4 million

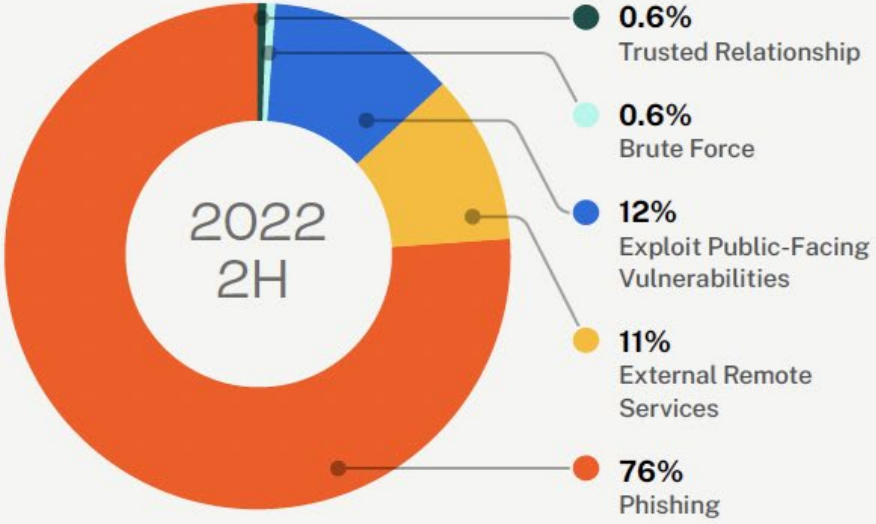
Average Ransom Demand in 1H 2023



If you're being hacked, you're being phished.

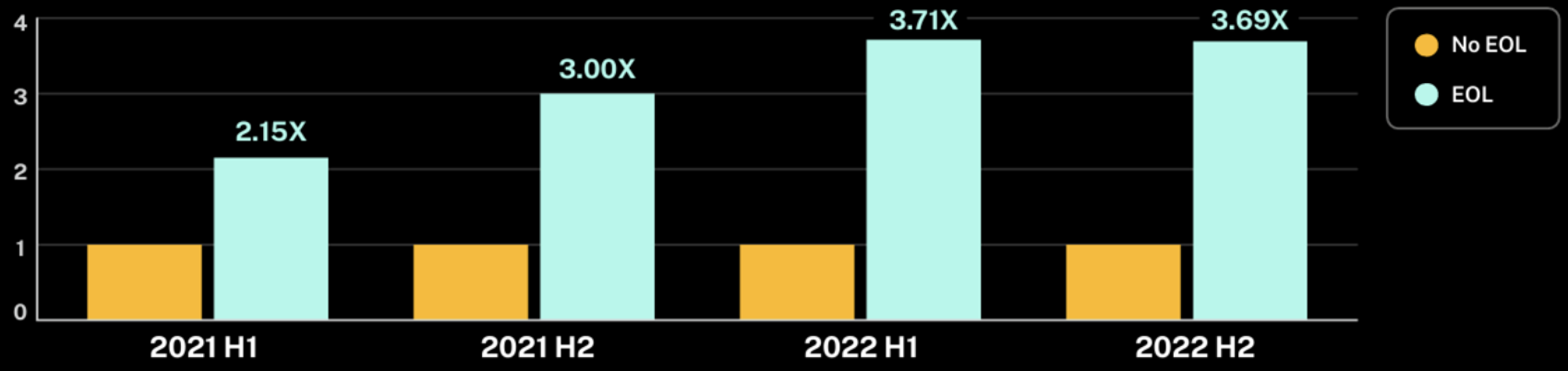
Percentage of reported claims by attack vector





Policyholders using EOL software were 3x more likely to experience a claim

Relative likelihood of a claim: End-of-life software



Typical process for FTF

1. Identification of victim(s)
2. Phishing emails sent to steal user credentials
3. Malicious logins are performed
4. Hacker searches for transactions to intercept
5. Mailbox rules created to avoid detection
6. Modification of payment instructions requested
7. Criminal voice or video verifies instructions
8. Criminal receives fraudulent funds transfer
9. Attack repeated on other contacts of the compromised mailbox user

Dwell time surged in FTF events

Average dwell time **increased 75%** to 42 days in 2022

*Attackers plan their attacks **longer***

FUNDS TRANSFER FRAUD | CASE STUDY

Insured faces $6.4M Loss after Funds Transfer Fraud

Industry: Union

Cybercrime Type: Social Engineering

Clawback Amount: $5.4M (all but $1M recovered)

How to protect your organization

Don’t make it easy. Patch and take EOL devices offline.

MFA all day.

Back ups – Don’t leave the keys in the door.

What to ask your insurance company

Pre-Claims Assistance

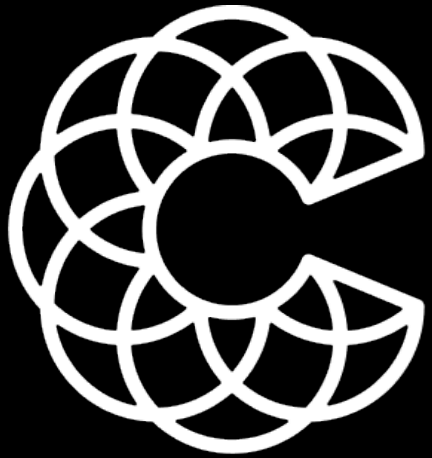
Incident Response Plans (IRP)

Ongoing Scanning & Alerting

Tabletop Exercises (TTX)

Security Resources

Data & Trend Sharing



Coalition®