

Palmetto Cybersecurity Summit for Local Government

State of Cybersecurity in Government

Jeramy Kopacko

Sr Territory Solutions Engineer

February 2023

SOPHOS
Cybersecurity evolved.

Who am I?

- Originally from Pittsburgh, PA
- Reside in Raleigh, NC
- Final semester @ George Mason University
 - MS in Cybersecurity Engineering
- Entering 5th Year at Sophos
 - Commercial, Public Sector, Enterprise
 - Former K12 Technology Director (PA)
- Run a Blog “Query Corner” on Sophos Community
 - Focuses on DFIR queries using SQL
 - Based on osquery engine

Connect with me: <https://linktr.ee/jkopacko>

What's Happening with Cyber Insurance

The background of the slide features a complex pattern of overlapping light blue circles. Within these circles, there are numerous horizontal bars of varying lengths and shades of blue and grey, creating a layered, abstract effect.

The cyber insurance market is undergoing rapid change

It's getting harder and more expensive to get cyber insurance

Understand what insurers are expecting you to have in place

What Cyber Insurance Covers

- **Business interruption** costs
- **Forensic analysis** to identify the attack source
- **Ransom demands and specialists** to handle ransom negotiations
- **Costs to regain access or restore data** from backups or other sources
- **Legal** costs
- **Public relations** services
- **Notification** of clients and/or regulatory bodies
- **Credit monitoring** services for affected individuals

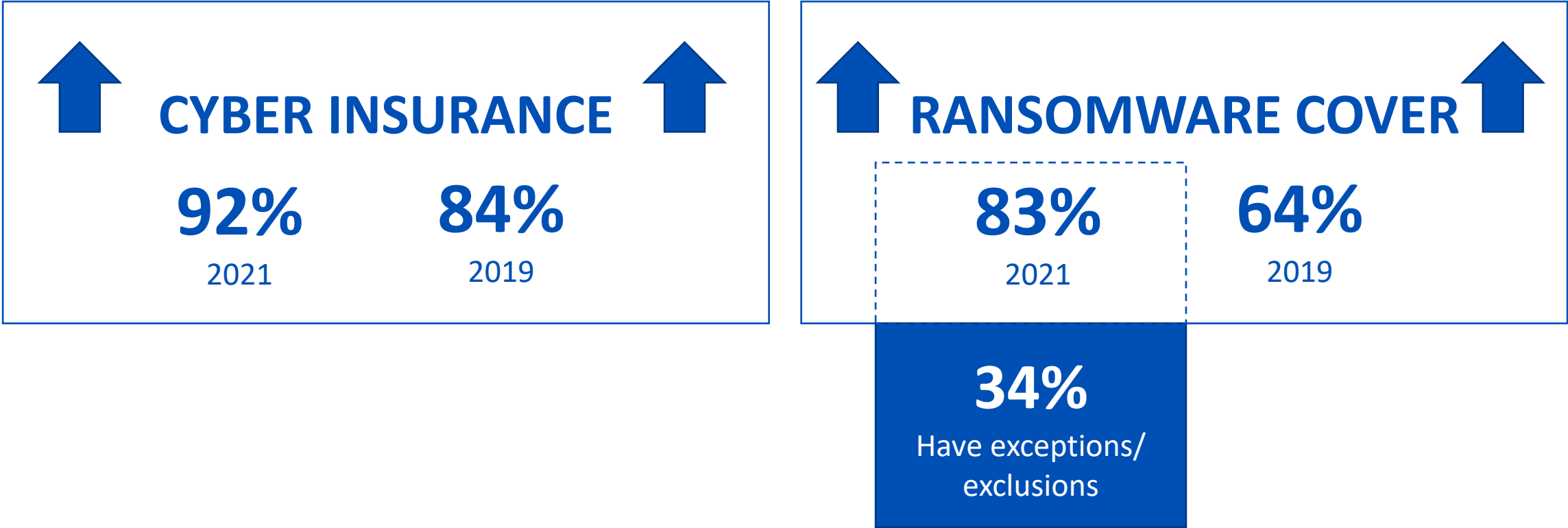
First party

Direct costs associated with the response to attack

Third party

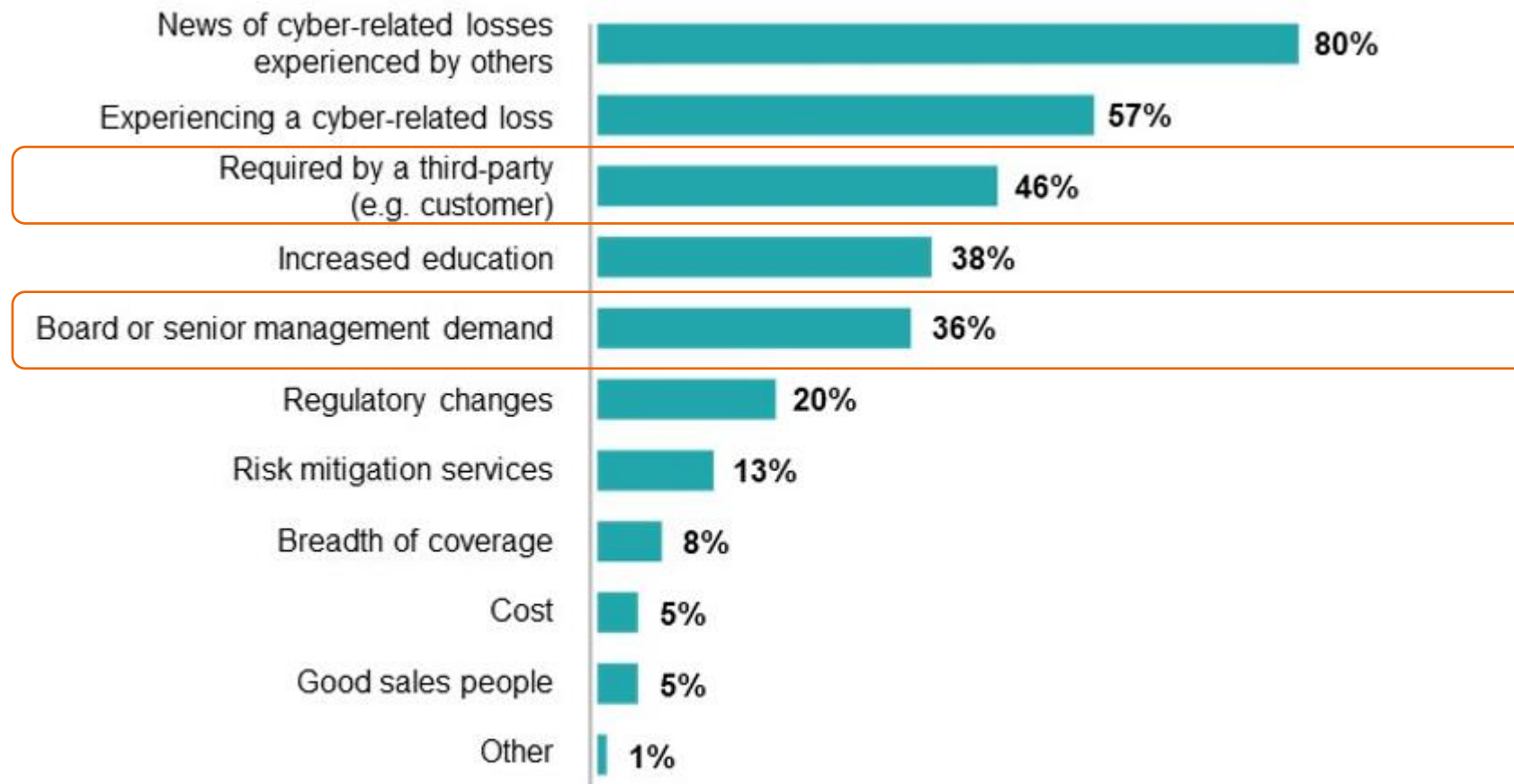
Primarily costs associated with lawsuits

Level of Cyber Insurance Take-up



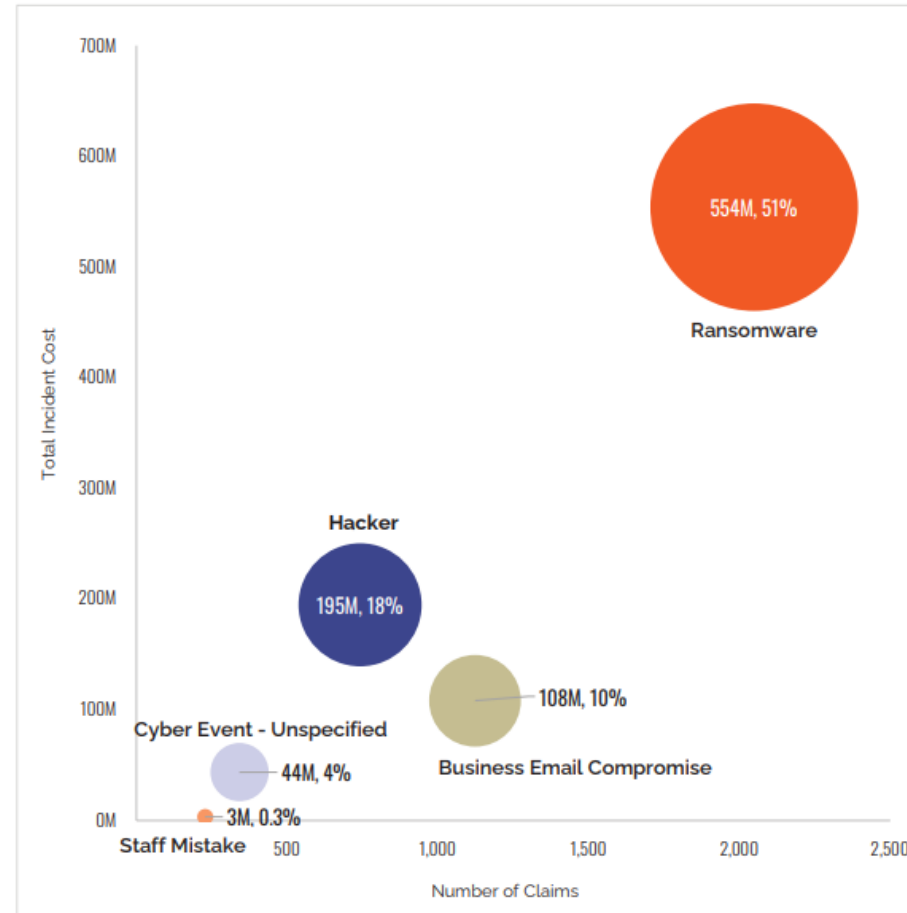
Does your organization have cyber insurance that covers it if it is hit by ransomware? (n=5,600/5,000). Yes; Yes, but there are exceptions/exclusions in our policy; No, our cyber insurance does not cover ransomware; I don't know if our cyber insurance covers ransomware.

Cyberattacks Are Fueling Cyber Insurance



What do you see as the current top drivers of new/increased cyber insurance sales? Please select the top three.
Cyber Insurance – The Market’s View; PartnerRe and Advisen, 2021

Top Five Causes of Cyber Insurance Claims, 2017-21



Top Causes of Loss – SMEs

Number of Claims, Total Incident Cost, % of Total Cyber Claims Incident Costs
NetDiligence Cyber Claims Study 2022

NetDiligence®

SOPHOS

Cyber Insurance Almost Always Pays Out Some Costs

98%

Cyber insurance payout rate



CLEAN-UP COSTS



77%

2021

67%

2019



RANSOM



40%

2021

44%

2019

Did the cyber insurance pay out to address the costs associated with the most significant ransomware attack that your organization suffered? (n=3,308 organizations that were hit by ransomware in the previous year and had cyber insurance cover against ransomware). Yes, it paid clean-up costs (e.g. cost to get the organization back up and running); Yes, it paid the ransom; Yes, it paid other costs (e.g. cost of downtime, lost opportunity etc.)

Examples of Exclusions

■ Third party providers

- Ex: a supplier or vendor suffer a breach

■ Lost portable devices

- Ex: lost/stolen phones, tablets, computers, etc
 - NOTE: encrypted devices vary

■ War/Invasion/Terrorism

- Ex: State-sponsored groups

■ Security Failures

- Ex: Investigation determine RPOC (RPOF) to be below minimum-security standards
 - Ex: EoL/EoS technology
 - Ex: Unpatched

■ Malicious insiders

Leading to Massive Changes in Offerings

Cyber insurers have two paths

Exit Market

“Lloyd's of London, which has around a fifth of the global cyber market, has discouraged members from taking on cyber business next year” Nov. 19, 2021

Change Conditions

Taking on less risky clients

Increasing prices

Lowering limits

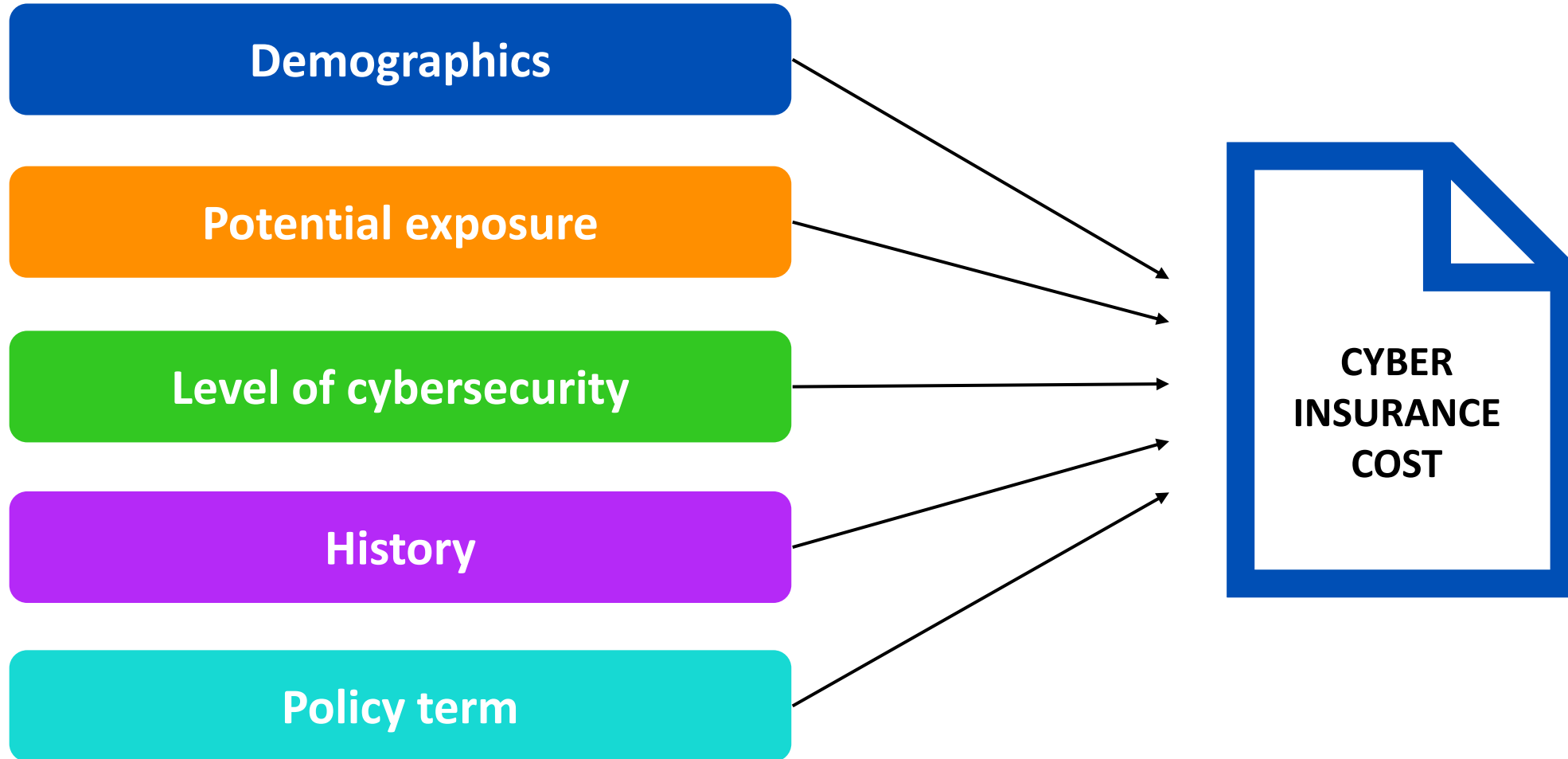
The Cyber Insurance Market Is Hardening

Cyber Risk Analysis

Insurers are hiring experts to help analyze risk associated with an organization to determine appropriate value during the underwriting process

Insurers have also started to create internal scoring models to assess risk based on proprietary factors and algorithms. Audits may increase or decrease this scoring.

Factors Insurers Consider



Why is **\$anyLevelOf** Government a Target?

- Valuable data
 - Government Entity
- Legacy Systems
 - Support older applications or technology
- Missing security controls
 - Budget constraints lead to sacrifices in protection
- Lacking necessary operators
 - Often can create constraints to hire and retain talent
- Foreign Adversaries
 - US government affiliation

New State & Local Requirements (announced Sept 22)

- “State and Local Government Cybersecurity Act” (S. 2520)
 - Designed to strengthen relationship between State, Local, Tribal, & Territorial (SLTT)
 - Directs DHS to share direct to governments to prevent and recover from attacks
- Codifies relationship between CISA and Multi-State Information Sharing and Analysis Center (MS-ISAC)
 - CISA = Cybersecurity and Infrastructure Agency
 - MS-ISAC = formed in 2022 to improve cybersec for SLTT
 - Includes all 56 states/territories, state capitals, 100s of govts, & 2500+ orgs
- Improve resources and operations relating to cybersecurity

1:30 – 2:20 PM (Salon C) Kyle Bryan – “No-Cost Resources with the MS-ISAC”

Cyber Insurance Survey

About the Survey



5,157

respondents



31

countries



100-5,000

employees



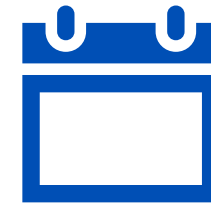
199

respondents
LOCAL/STATE



145

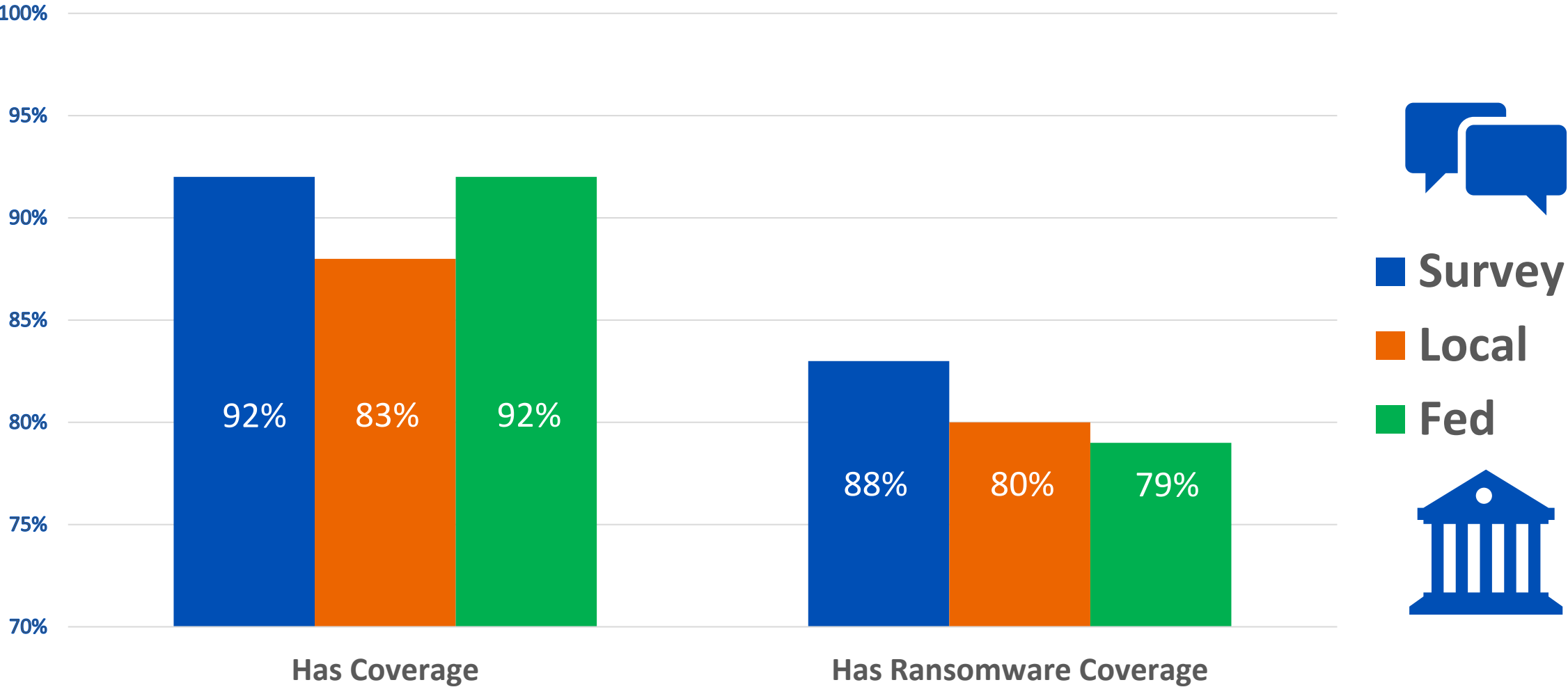
respondents
FEDERAL



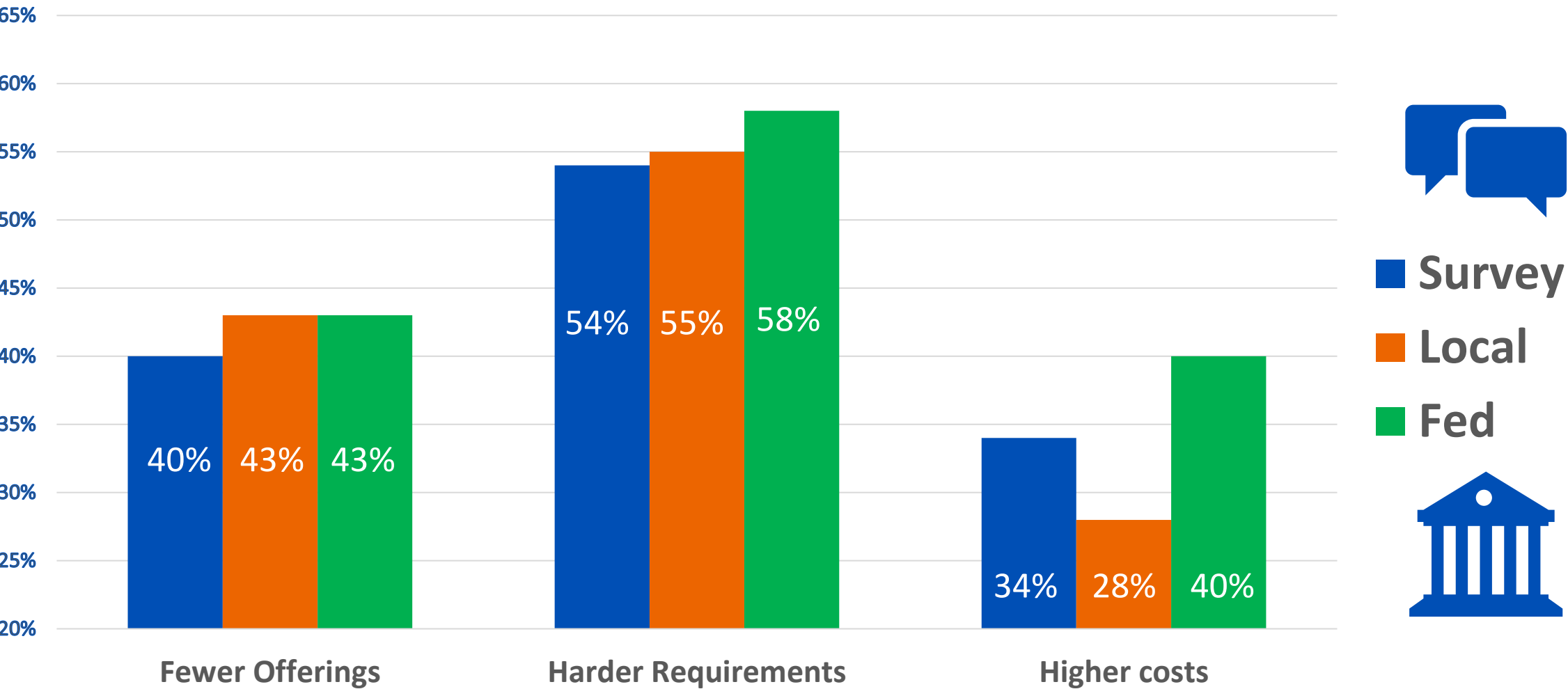
CY2022

research conducted

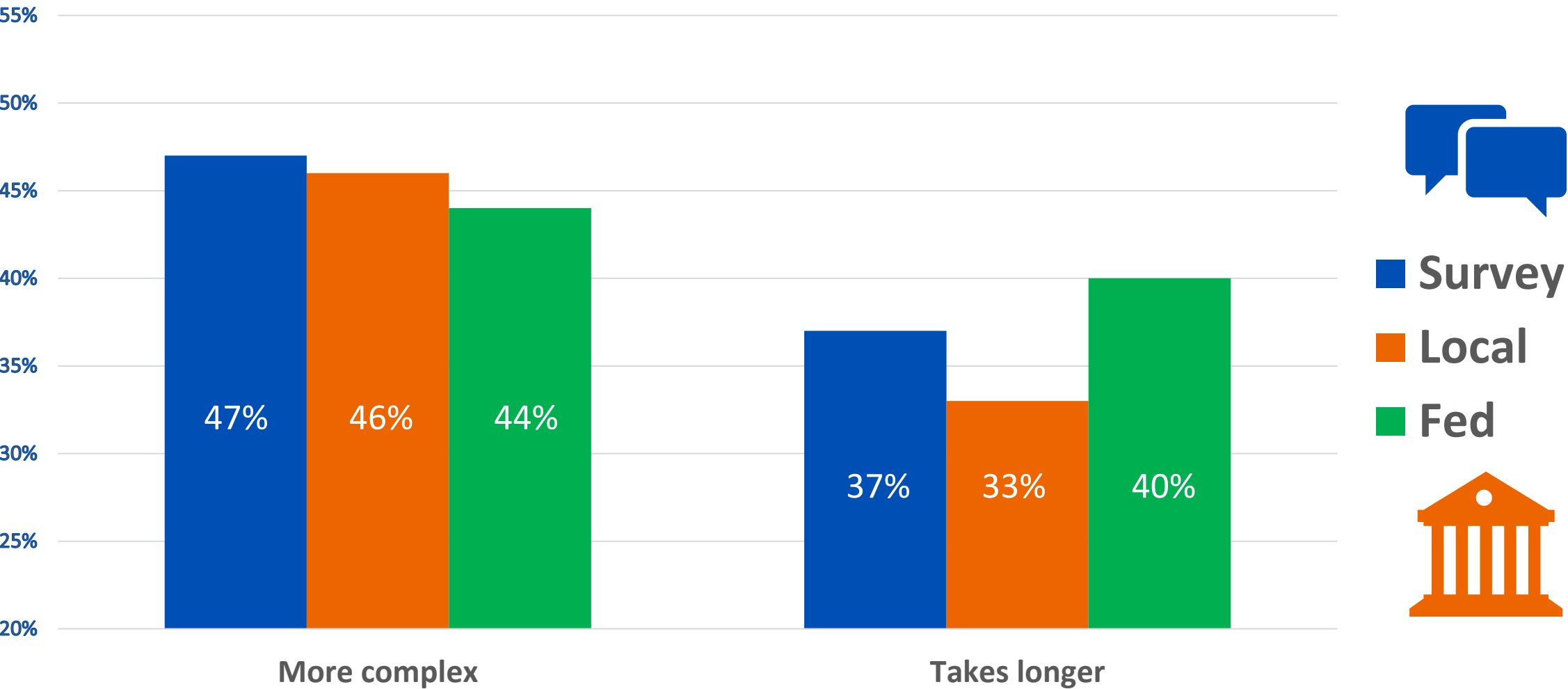
Do you have cyber insurance?



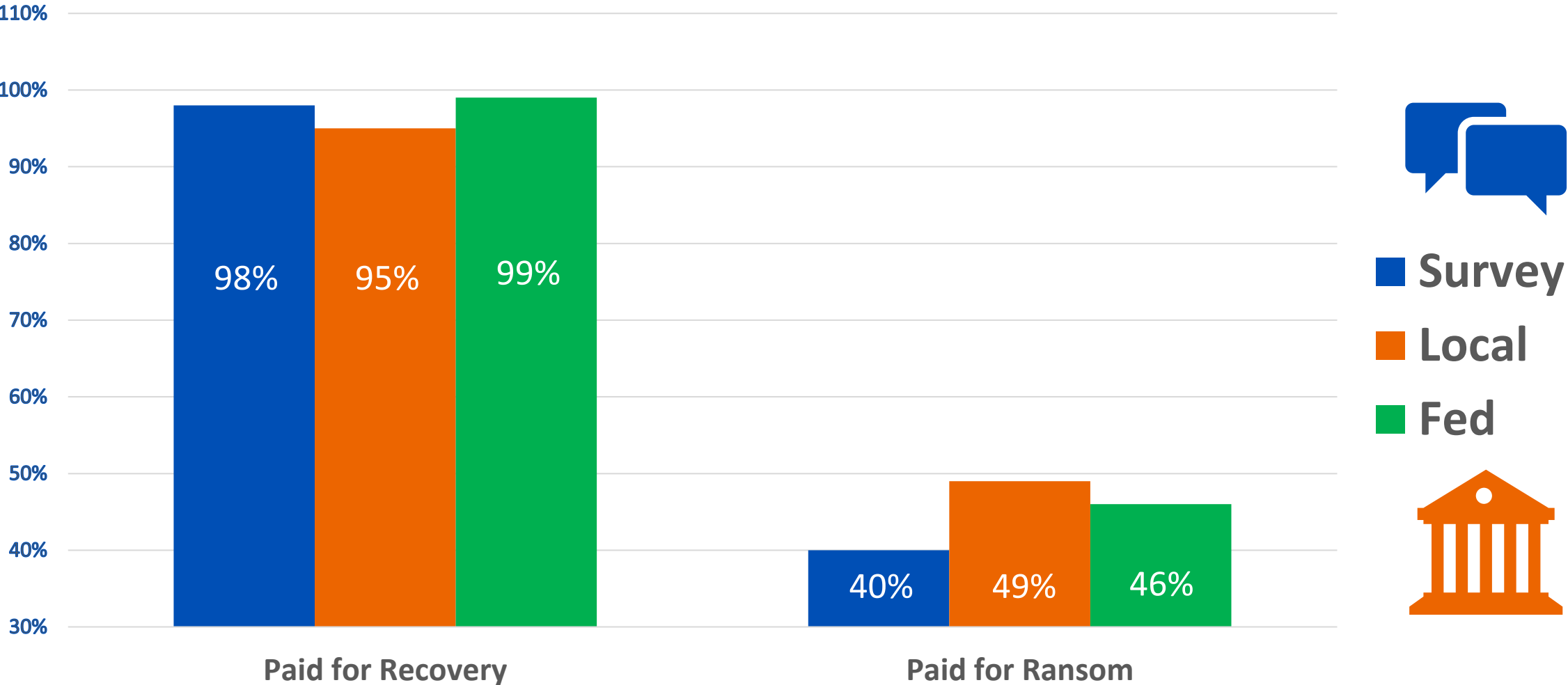
How is the experience buying insurance?



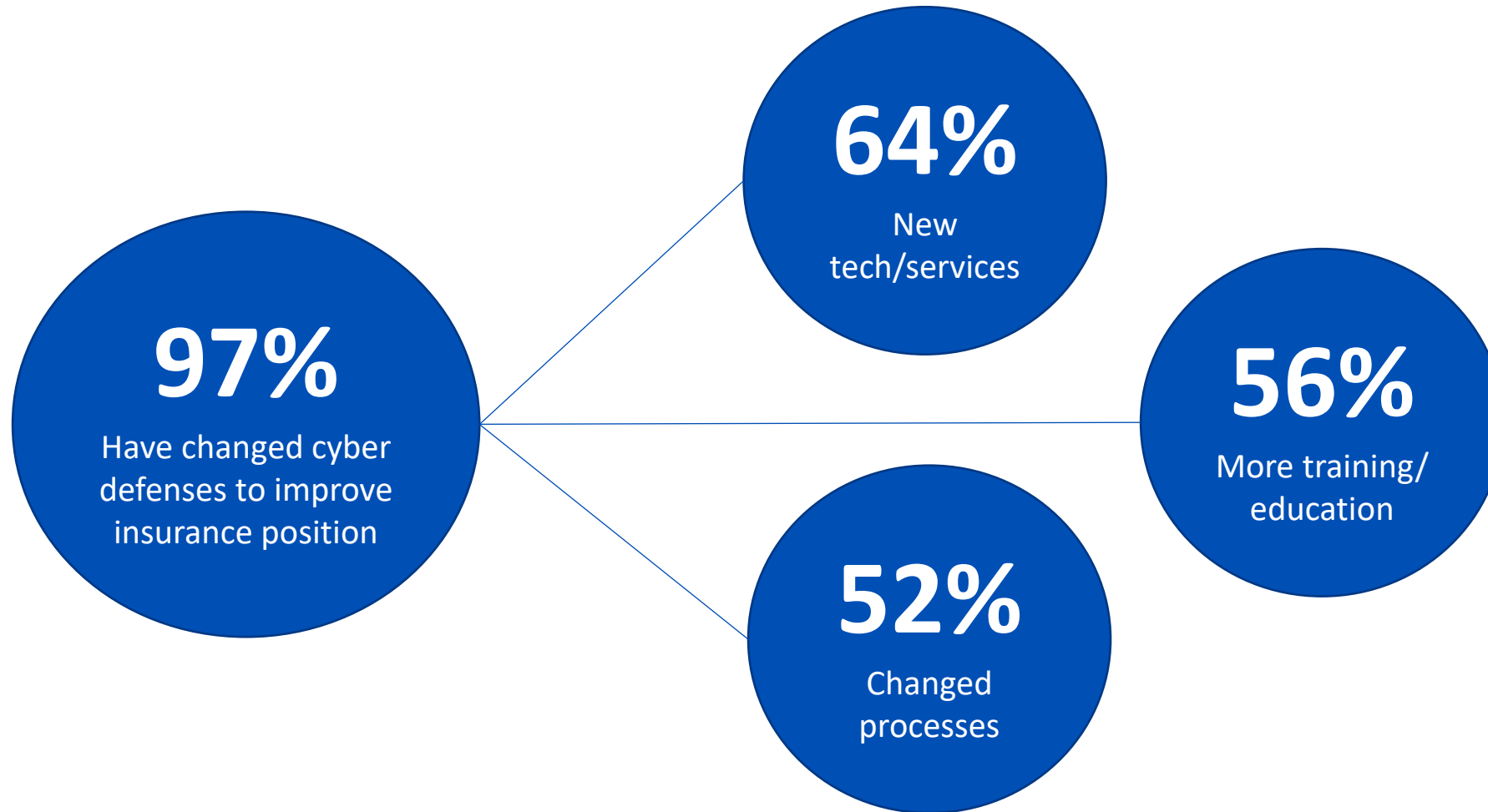
What about securing your policy?



Did your claim get paid?



Cyber Insurance Is Driving Improvements to Defenses



Over the last year has your organization made any changes to its cyber defenses to improve its insurance position? (n=5,157 respondents whose organization has cyber insurance. Excludes some answer options)

*Insurers are looking for the **use of security controls** that **they consider effective at preventing, detecting and remediating** malicious activity at various stages of the ransomware lifecycle. While cyber insurers ask a wide range of questions in their applications, certain central themes have emerged that point to their principal ransomware concerns and the security controls they believe best address them.*

Top Cybersecurity Controls



The key to insurability, mitigation, and resilience

Preparation for the underwriting process:

1. Start early!
2. Evaluate your cybersecurity maturity by reviewing required applications.
3. Expect more rigorous underwriting and more detailed questions.



Multifactor authentication for remote access and admin/privileged controls



Endpoint Detection and Response (EDR)



Secured, encrypted, and tested backups



Privileged Access Management (PAM)



Email filtering and web security



Patch management and vulnerability management



Cyber incident response planning and testing



Cybersecurity awareness training and phishing testing



Hardening techniques, including Remote Desktop Protocol (RDP) mitigation



Logging and monitoring/network protections



End-of-life systems replaced or protected



Vendor/digital supply chain risk management

Note: Each insurance carrier has their own specific control requirements that may differ by company revenue size & industry class. For more on the Cyber hygiene see: [Cyber hygiene controls critical as cyber threats intensify \(marsh.com\)](https://www.marsh.com/cyber-hygiene-controls-critical-as-cyber-threats-intensify)

Keep the Attackers Out

- Multi-factor authentication
 - Can be required for access to network, privileged accounts, email, vendors, and backups
- Patch management
 - Do you have a control mechanism? How quickly can you deploy a fix?
- Employee training
 - Phishing training or periodic testing to achieve consistent, low failure rates
- Remote access controls
 - Secure access controls over VPN, firewall, etc.
- End of life technology
- Email and web filtering systems

Detect Intrusions and Behavior

- Endpoint Protection Products (EPP) + Endpoint Detection & Response (EDR)
- Conducting vulnerability scans
- Other endpoint protection
 - i.e. traditional A/V, such as signature based
- Intrusion detection systems
- Intrusion prevention systems
- Security Incident Event Management (SIEM)
- Next-generation Firewalls (NGFW)
- eXtended Detection & Response (XDR)
 - Sometimes referred to as a “Threat Focused SIEM”

Protect Users and Privileged Accounts

- Identity Access Management (IAM)
- Privileged Account Management (PAM)
- Network segmentation
- Configuration management practices
 - I.e. Microsoft Security baseline configurations, OS hardening, etc.
- Service account management

Everybody has a plan
until they get **hit with malware**

- Mike Tyson



Business Continuity Planning

- Backup practices
 - Encrypted copies, multiple on and off-site locations, etc.
- Incident response plans
 - Playbook for handling security events
 - Show that you exercise table-top exercises
 - Identify and document vendor response
- Disaster recovery planning
 - Business continuity plans
 - Recovery Time Objectives (RTO)

Samples of Questions

- Do you have firewalls in place to protect your data and devices?
- Do you have antivirus software in place to protect your data and devices?
- Do you encrypt your data at rest, in transit and/or on mobile devices?
- Do you have an intrusion detection/prevention system in place to protect your data and devices?
- Do you conduct vulnerability scanning and patching?
- Do you require the use of multi-factor authentication?
- Do you back up your electronic data?
- Do you have a business continuity plan, disaster recovery plan, and an incident response plan?
- Do you have vendor risk management protocols in place that address cyber risk controls, contractual liability, indemnification, etc.?
- Do you have an employee who is trained to address cyber risk issues?

Sophos 2023 Threat Report

Maturing criminal marketplaces present new challenges to defenders

What Is Sophos X-Ops?

Security Professionals
Sophos team sharing queries, tools, and techniques from CISO to frontline



MDR SecOps Analysts
Discovering new IOCs and hunting methods, in-the-wild impact



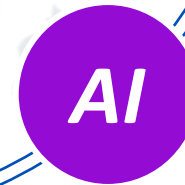
Sophos X-Ops

500+ experts across threat intel, analysis, data engineering, data science, threat hunting, adversary tracking, and incident response, staffing 6 global SOC's in every major theater

SophosLabs Researchers
Providing deep analysis of files, email, behaviors, URLs, IOCs, and DPI



Sophos AI Data Scientists
Development and insights on advanced ML models, automation and detection for MDR and Sophos products



Ransomware Remains One of the Greatest Cybercrime Threats to Organizations

Ransomware Operators Have Expanded Their Attack Surface

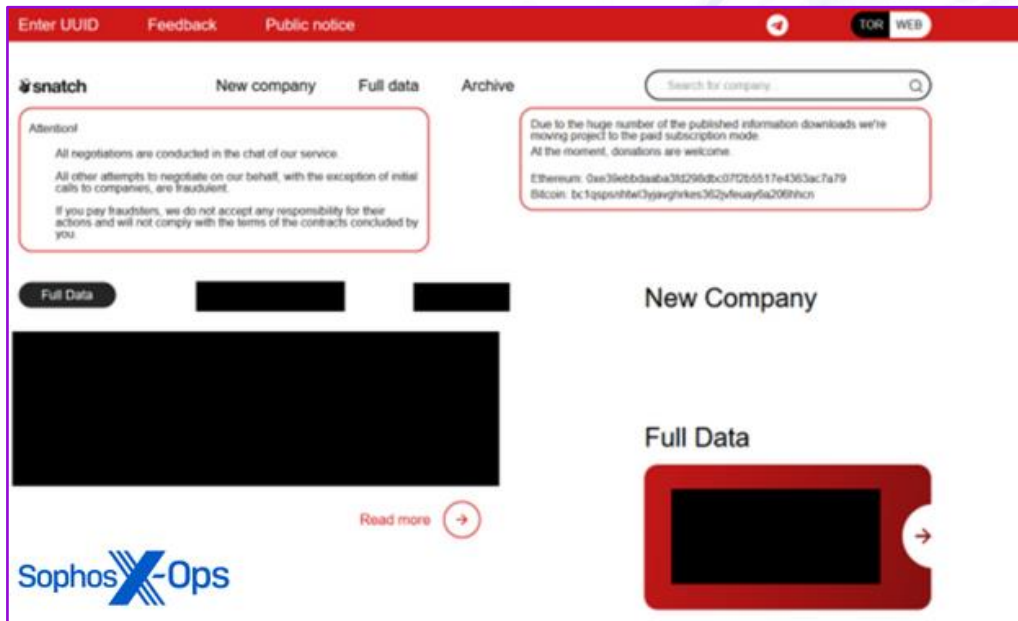
They're **not just targeting Windows** anymore, **but also Linux**

This complicates matters for defenders, since **many ransomware defenses focus on Windows**



They're also using **newer programming languages** like Rust and Go to better **evade detection** and **deliver payloads**

When it Comes to Delivering and Spreading Their Malware, Ransomware Operators Continue to Evolve



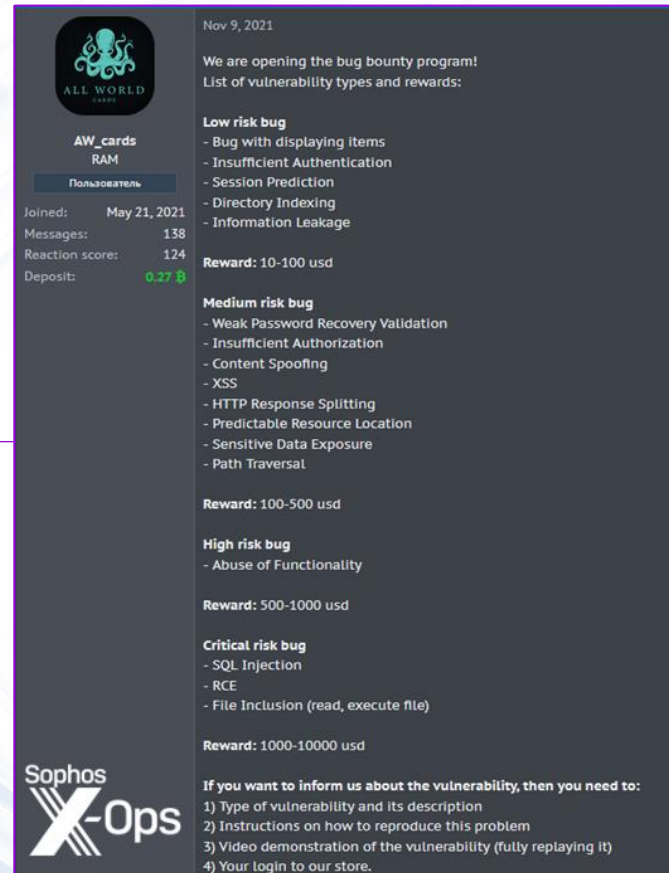
This includes **abusing benign applications** and **legitimate security tools**.

They have also been developing more **innovative extortion methods**:

- Selling stolen data through a subscription model
- Auctioning off stolen data to the highest criminal bidder
- Offering victims the chance to conceal the fact they've been breached

When it Comes to “Innovation,” LockBit Led the Pack

LockBit's new **bug bounty program** offers rewards between **\$1,000 to \$1 million** for a variety of activities, from **finding bugs in its malware** to ideas for **improving operations**



The screenshot shows a dark-themed announcement for the Sophos X-Ops bug bounty program. At the top left is the 'ALL WORLD CARD' logo. Below it, the user 'AW_cards' is listed with 'RAM' as their role. A sidebar on the left shows user statistics: 'Joined: May 21, 2021', 'Messages: 138', 'Reaction score: 124', and 'Deposit: 0.27 B'. The main content area, dated 'Nov 9, 2021', states 'We are opening the bug bounty program! List of vulnerability types and rewards:'. It lists four risk levels with their respective vulnerabilities and reward ranges: 'Low risk bug' (10-100 usd), 'Medium risk bug' (100-500 usd), 'High risk bug' (500-1000 usd), and 'Critical risk bug' (1000-10000 usd). At the bottom, it lists four requirements for reporting a vulnerability.

ALL WORLD CARD

AW_cards
RAM

Пользователь

Joined: May 21, 2021
Messages: 138
Reaction score: 124
Deposit: 0.27 B

Nov 9, 2021

We are opening the bug bounty program!
List of vulnerability types and rewards:

Low risk bug

- Bug with displaying items
- Insufficient Authentication
- Session Prediction
- Directory Indexing
- Information Leakage

Reward: 10-100 usd

Medium risk bug

- Weak Password Recovery Validation
- Insufficient Authorization
- Content Spoofing
- XSS
- HTTP Response Splitting
- Predictable Resource Location
- Sensitive Data Exposure
- Path Traversal

Reward: 100-500 usd

High risk bug

- Abuse of Functionality

Reward: 500-1000 usd

Critical risk bug

- SQL Injection
- RCE
- File Inclusion (read, execute file)

Reward: 1000-10000 usd

Sophos X-Ops

If you want to inform us about the vulnerability, then you need to:

- 1) Type of vulnerability and its description
- 2) Instructions on how to reproduce this problem
- 3) Video demonstration of the vulnerability (fully replaying it)
- 4) Your login to our store.


LockBit also offers its victims the chance to **purchase or destroy stolen data** or extend the time until **data is leaked**

Cybercrime Achieves a New Level of Commercialization and Commodification

Cybercriminals are Operating Like Mainstream Businesses

More and more cybercriminal gangs are taking a cue from the **software industry** and following an **“as-a-service” model** to scale their services to **industrial levels**

Phi4er
kilobyte
●●



Active arbitrage
● 0
27 posts
Joined
06/24/22 (ID: 132361)
Activity
кодинг / coder

Posted June 24 (edited)

Every Phisher Dream

Hello,
We offer our services for every phisher that want to success his campaigns. We decided to help you in creation and maintenance for your projects/campaigns with our long experience in phishing.


- We can create/clone any page
- Live panel can be done for the page
- Customizing the live panel for any feature needed
- Anti-bot system that protects the page for days and even weeks ^{best}

We can help you hosting your page on our personal servers with anti-bot and auto domain changer with extra fees. Just relax and see your campaigns running successfully,

Why us?

- Client's satisfaction is our priority
- Online 24/7 hours on TG
- We deliver your project/page ASAP
- Edits are done and delivered immediately
- Any features you dream of can be implemented in your page

Our mission?
Simply we are created to help in carrying out your fishing projects in a professional way.



Every Step of the Attack Chain—From the Initial Infection to Evading Detection—Is Now Available "As-a-Service"

OPSEC service i decide to publish it on XSS community since i recieved many request on setup hidden cobaltstrike with custom requiriments from teams to individual pentesters.

The service is not-documented at all, it as a **one-time** setup, or **monthly** subscribe.

- nmap scanner. (**blocked**) ✓
- BeaconEye scanner (**blocked**) ✓
- Cobalt parser . (**blocked**) ✓
- Hidden URI aka checksum8. (**hidden**) ✓
- Hide your Teamserver under CloudFlared Tunnel ✓
- Steal SSL for your target company. (**bypassed**) ✓
- Bypass most modern EDR's. (**bypassed**) ✓
- and / or Install TOR over Teamserver.
- and / or Install OpenVPN with redirector.
- and / or Install DNSCrypt (DoH) via CloudFlare.
- and / or Install Domains Randomizor.
- and / or Install JARM randomizor aka JA3's obfuscator.



The setup service will cost \$700 **one time** , for windows or linux teamserver without cost of vps, domains or modified version of cobaltstrike 4.x, or any extra services.

Cybercrime-as-a-Service Breaks Down Nearly all Barriers of Entry



dripper
HDD-drive
Пользователь

Joined: May 19, 2022
Messages: 44
Reaction score: 6

Jun 23, 2022

SophosX-Ops

I am looking for pentesting job.

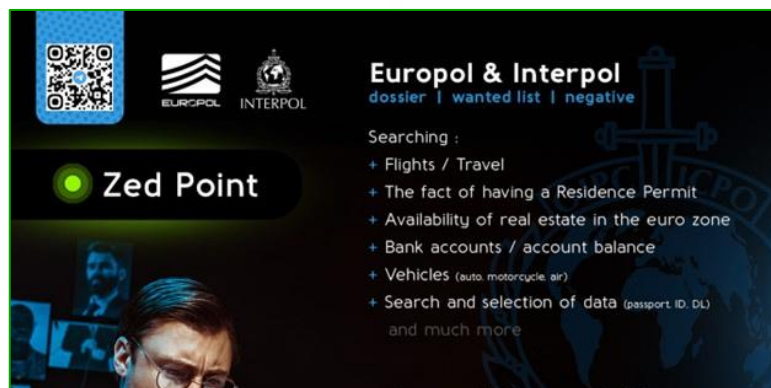
I have experience in AV Bypass on your docx/xlsx and bins
I can do lateral movement for you
I can code for you in C/Cpp python NIM
I have experience make crypts and loaders


More details in PM.


Make damage memorable. 😊

It's putting **tools and tactics** that once rested solely in the hands of the most sophisticated actors in the **hands of everyone**

Taking a Cue from RaaS, More Forums and Sub Areas of Cybercrime are Adding “Polish” to Their Marketing




**Hortage**
By Hortage, May 18 in [Job] - search, execution of work

**Hortage**
megabyte
●●●
Paid registration
4
59 posts
Joined
04/03/19 (ID: 91777)
Activity
вирусология / malware

Posted May 18 (edited)
We are looking for new people to join our team.
You should be able to access our targets.
Our targets are Tier 1 and specifically selected.
We do not work on mass .
Quality is our ultimate goal.
Sometimes we work on a target for several weeks and then we are successful.
You bring your own toolkit and experience.
We provide the infrastructure.
Payment is in %.
Leave your TOX ID in PM

Edited May 18 by Hortage



- More marketplaces are using **professionally designed graphics** and maintaining help wanted pages with dedicated recruiting staff
- Criminals can **pay to advertise** their services
- “Job seekers” can **post summaries** of their **qualifications and skills**

Demand for Infostealers and Stolen Credentials Grows

Thanks to the Adoption of Web Services, Demand for Credentials of All Kinds Has Grown



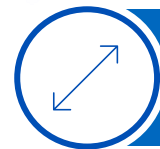
Stolen credentials now offer numerous ways to infiltrate targeted networks



Certain credentials can even be used to bypass MFA





Infostealers are also an easy way for would-be cybercriminals to get their "start" in cybercrime



They can pave the way for existing cybercriminals to expand their crime sprees

The Infostealer Ecosystem Has Even Started Trying to Profit off White Hat Efforts to Stop Credential Theft

Scraper group purchase :
\$2,000.00 for 1 year


(Choose a payment method)   Purchase

Are you a Security Intelligence company, Whitehat, OSINT researcher, data collector? Group Scraper is a purchase of the ability to collect data from our forum without blocking.

Capabilities:

- allowed to collect data from the forum;
- no bans and blocking of the account;
- there are no limits and restrictions on data collection (except for general web server restrictions);
- opening all hides (hidden text), regardless of the number of messages, likes and date of registration, except for administrative ones;

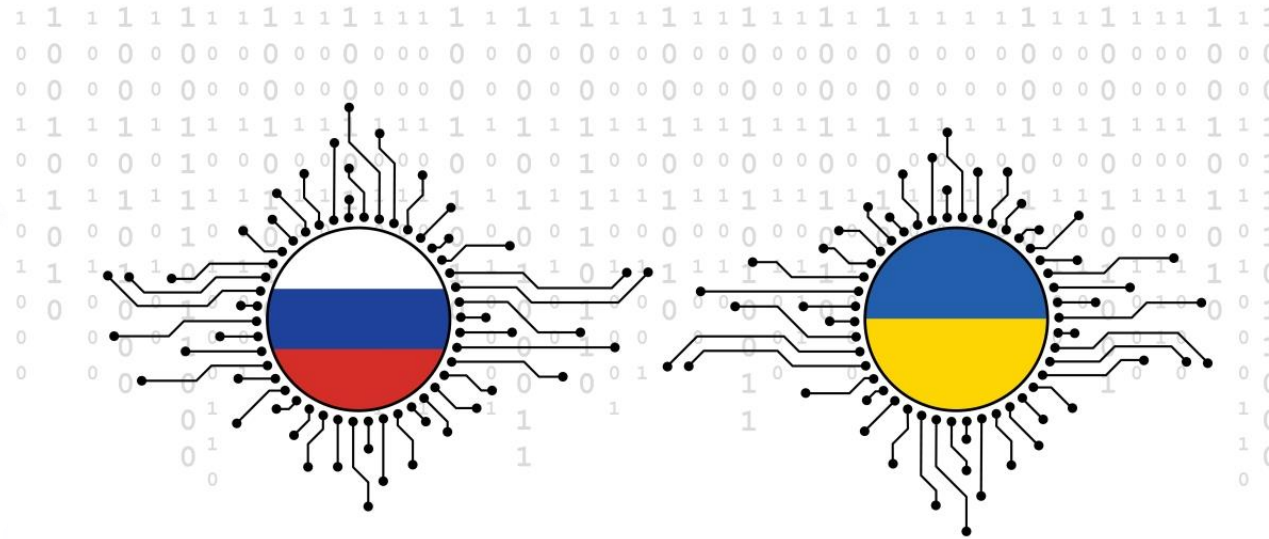
Attention! This group is intended exclusively for bot accounts, spiders and web scrapers. There is no possibility of communication, including personal correspondence, no API, no access to internal forum data, etc.



The underground forum XSS offered a **\$2,000 annual subscription** for **unimpeded data-collection access** to security professionals looking to scrape their forum

War in Ukraine Transforms the Threat Landscape

Inside Ukraine, the Cybercrime Landscape Has Shifted



Ukrainians and Russians have long been partners in (literal) crime

- Gangs **fell apart** thanks to **nationalism**
- This led to the **Conti Leaks**
- Another Twitter account also **doxed** alleged members of other ransomware groups

But these victories were short-lived

- Political events have made **international cooperation** to tackle ransomware **more difficult**
- Ransomware groups have **rearranged themselves**
- **A new REvil** may have even re-emerged

Attackers Turn to Legitimate Executables and LOLBins to Launch Attacks

Using Legitimate Security Tools for Bad Ends Remains Popular—especially Among Ransomware Groups



- These groups often utilize pirated copies of tools like **Metasploit Pro** purchased on underground forums
- **Cobalt Strike** played a role in **47%** of customer incidents
- This year, a new tool—**Brute Ratel**—was added to the mix

“Living of the Land Binaries” (LOLBins) Are on the Rise

With **LOLBins**, attackers take advantage of native Windows components to...



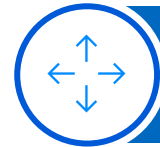
Execute system commands



Bypass preset security features



Download and execute remote malicious files



Move laterally across networks

<https://lolbas-project.github.io/>

Ransomware Groups Are Also Bringing Their Own Executables With Vulnerabilities



- This has led to a rise in "**Bring Your Own Driver**" (BYOD) attacks
- In many cases, the **goal is to disable EDR** to evade detection
- Both **AvosLocker** and **BlackByte** have used this technique

Threat Report Key Trends



1. **Ransomware** continues to be one of the **greatest cyber threats**
2. The "**cybercrime-as-a-service**" industry has reached a new level of **commercialization**
3. Demand for **infostealers** and **stolen credentials** grows
4. The **war in Ukraine** has led to a **shake-up of criminal alliances** and a **re-organization of the ransomware landscape**
5. Cybercriminals continue to **exploit legitimate executables** to launch attacks, including ransomware
6. **Cryptomining** has been on the **decline**
7. **Mobile devices** are at the center of **new types of cybercrime**

Sophos 2023 Threat Report



sophos.com/threatreport

Cybersecurity in 2023

Advice For Defenders

SOPHOS

Books to read

Putting off critical tasks until everyone forgets about them



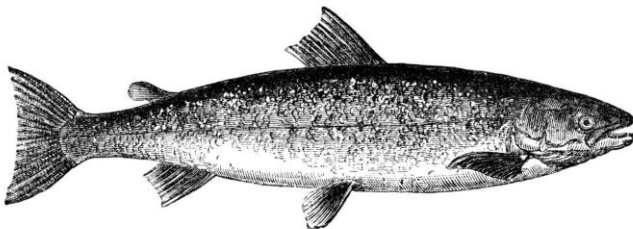
Getting Around to
Security Next Month

If there's time

O RLY?

@ThePracticalDev

Security by optimism and prayer



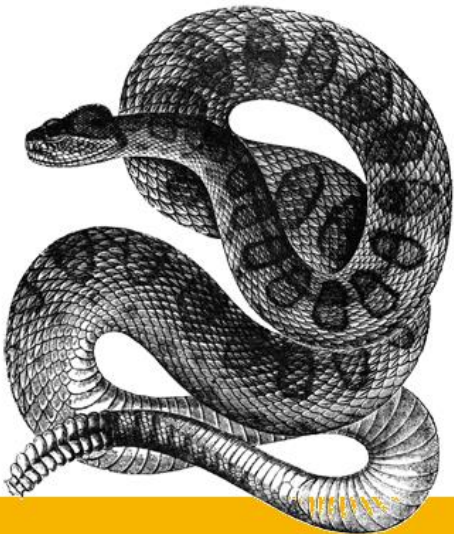
Expert

Hoping Nobody
Hacks You

O RLY?

@ThePracticalDev

A proven model to extend your career



Prepare Three
Envelopes

Handheld Guide

O RLY?

@jkopacko

Five Top Tips to Minimize Your Exposure

1

Implement defense-in-depth security controls

2

Proactively hunt for threats

3

Harden your environment

4

Have a cyber incident response plan

5

Make backups and practice restoring from them

Things to consider for 2023?

- DevSecOps
 - a platform to **Develop Security Operations**
 - Automate as much of the security process as possible
 - (Community Edition) Sophos Factory
 - <https://www.sophos.com/en-us/products/sophos-factory>
- APIs and how they're your best friend you never met before
 - Most platforms offer them in their software solution
 - Most are free!
 - Most want to be used!
 - Most will help you use them!
- Micro-segmentation of services and users ("ZTNA")
 - Parameter based access with conditional settings

SOPHOS
Cybersecurity delivered.