The Human Element of Cyber Breach and Why Humans and Their Organizations Continue to Struggle with Cyber Defense

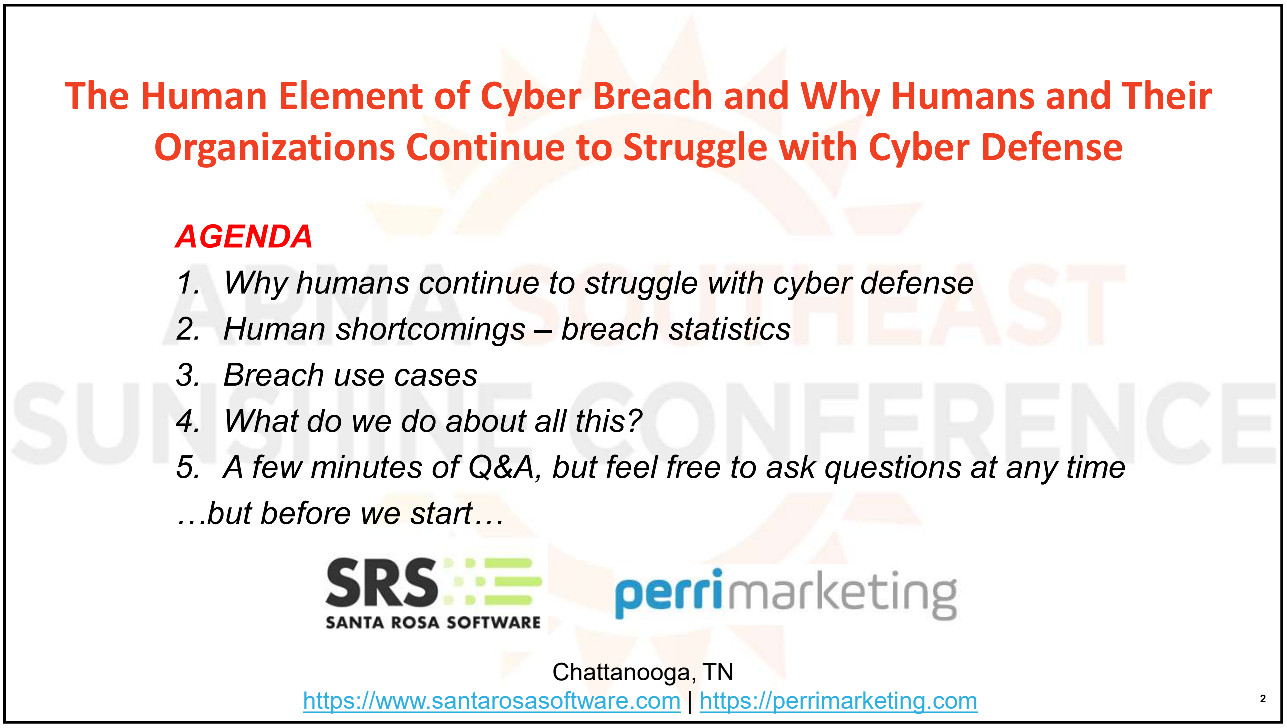
…and what to do about it.

SRS SANTA ROSA SOFTWARE perrimarketing

Chattanooga, TN
https://www.santarosasoftware.com | https://perrimarketing.com

1

1



The Human Element of Cyber Breach and Why Humans and Their Organizations Continue to Struggle with Cyber Defense

AGENDA

1. *Why humans continue to struggle with cyber defense*
2. *Human shortcomings – breach statistics*
3. *Breach use cases*
4. *What do we do about all this?*
5. *A few minutes of Q&A, but feel free to ask questions at any time*

…but before we start…

SRS SANTA ROSA SOFTWARE perrimarketing

Chattanooga, TN
https://www.santarosasoftware.com | https://perrimarketing.com

2

2

Who am I? Why am I speaking today?

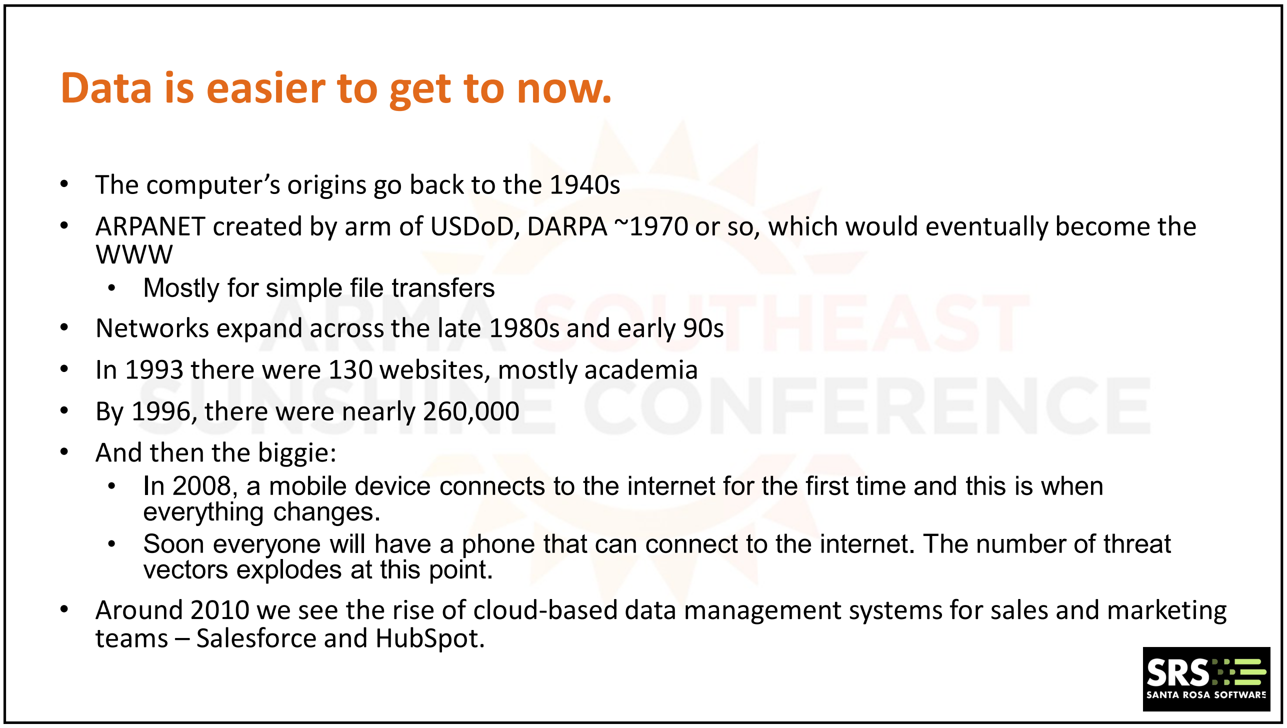
- Co-founder and CEO of Santa Rosa Software in 2019, a mainframe software vendor specializing in mobile applications for next gen mainframers.
  - Santa Rosa Software is a mobile apps vendor serving the next wave of mainframers…who sleep with their phones
- Founder and principal consultant of Perri Marketing in 2011, a tech marketing company serving ISVs
  - Over the years published many research/writing papers in InfoSec space
- Graduate of University of Georgia in early 1990s (ABJ)
- Started in the s/w biz in mid-1990s after a long stint in foodservice
- Started working in mainframe security space in 2008 at Allen Systems Group, now Rocket Software
- IBM Champion

3

ARMA SOUTHEAST SUNSHINE CONFERENCE

WHY WE HUMANS CONTINUE TO STRUGGLE WITH CYBER DEFENSE

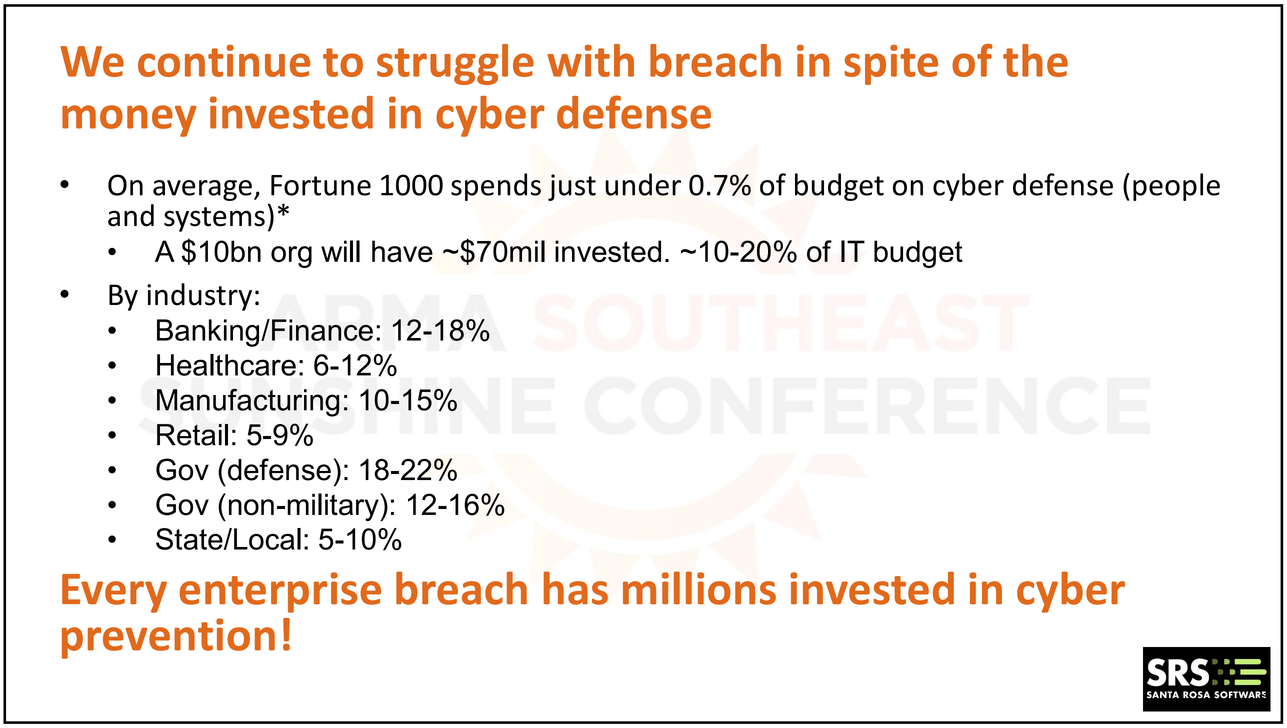
4



Data is easier to get to now.

- The computer's origins go back to the 1940s
- ARPANET created by arm of USDoD, DARPA ~1970 or so, which would eventually become the WWW
  - Mostly for simple file transfers
- Networks expand across the late 1980s and early 90s
- In 1993 there were 130 websites, mostly academia
- By 1996, there were nearly 260,000
- And then the biggie:
  - In 2008, a mobile device connects to the internet for the first time and this is when everything changes.
  - Soon everyone will have a phone that can connect to the internet. The number of threat vectors explodes at this point.
- Around 2010 we see the rise of cloud-based data management systems for sales and marketing teams – Salesforce and HubSpot.

5



We continue to struggle with breach in spite of the money invested in cyber defense

- On average, Fortune 1000 spends just under 0.7% of budget on cyber defense (people and systems)*
  - A $10bn org will have ~$70mil invested. ~10-20% of IT budget
- By industry:
  - Banking/Finance: 12-18%
  - Healthcare: 6-12%
  - Manufacturing: 10-15%
  - Retail: 5-9%
  - Gov (defense): 18-22%
  - Gov (non-military): 12-16%
  - State/Local: 5-10%

Every enterprise breach has millions invested in cyber prevention!

6

People, the problem since WWII

- Long-standing “cold war” between Business and IT
- Dates back to the 1940s – the first “modern” computer, the Mark 1
    - Thomas Watson Sr. (businessman and main financier) vs. Howard Aiken (a mathematician)
    - Aiken helped IBM rethink how they were processing “code” – think less a calculator and more a large-scale computer built for more dynamic processing
    - Aiken built the Mark 1 with help (a lot of it!) from IBM but the guys helping weren’t mathematicians, so they didn’t understand the big picture
    - Aiken issued a PR for his new revolutionary coding device, Watson was miffed.
    - IBM took over and said “we’ll take it from here”
- At the heart of the disagreement was the business leaders weren’t going to let a mathematician run the show and take the credit. Money trumps math.
    - Ironically, it was Aiken who brought mathematics to computing and allowed the expansion of programming so that computers could do more than simple calculation

SRS SANTA ROSA SOFTWARE

7

Today it persists: Business/Ops vs. IT…and the rest of us

Biz Priorities: Wall Street? BoD? FoD?

IT Priorities: Service Delivery, Security, Compliance, Avoiding Punitives

SRS SANTA ROSA SOFTWARE

8

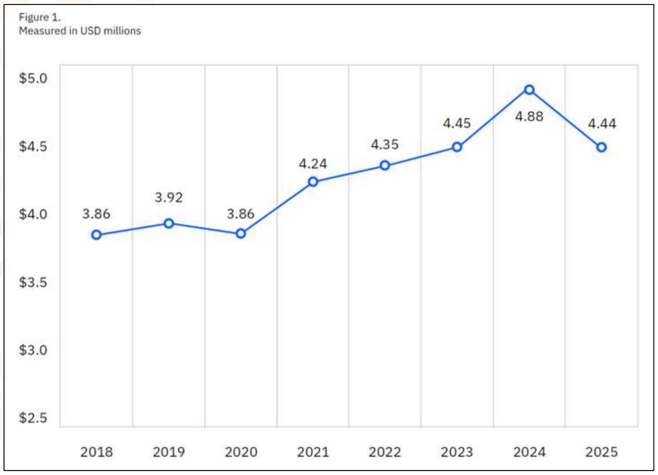
ARMA SOUTHEAST SUNSHINE CONFERENCE

HUMAN SHORTCOMINGS WITH BREACH STATISTICS

9

Cyber breach statistics globally

- There is a shortage of cyber crimefighters
  - AI is helping with the shortage of skilled crimefighters but the global average breach cost numbers keeps creeping up (from IBM 2025 breach report)



SRS SANTA ROSA SOFTWARE

10

Cyber breach statistics globally

- The top 8 countries breached and damages 2024-2025 (IBM 2025 breach report)

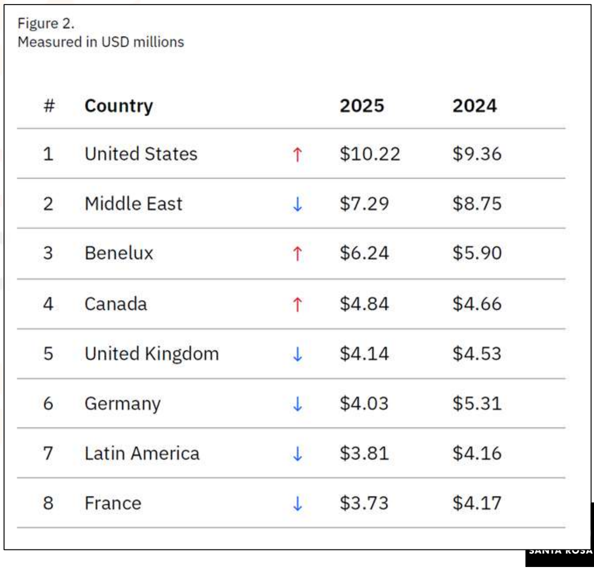


Figure 2.
Measured in USD millions

#	Country		2025	2024
1	United States	↑	$10.22	$9.36
2	Middle East	↓	$7.29	$8.75
3	Benelux	↑	$6.24	$5.90
4	Canada	↑	$4.84	$4.66
5	United Kingdom	↓	$4.14	$4.53
6	Germany	↓	$4.03	$5.31
7	Latin America	↓	$3.81	$4.16
8	France	↓	$3.73	$4.17

11

Cyber breach statistics US state, local, tribal territories

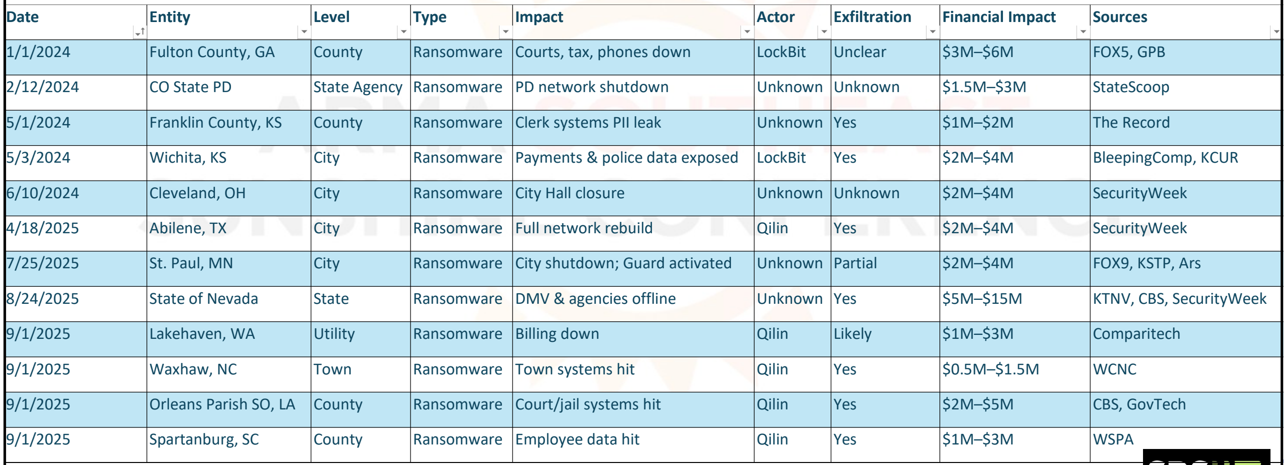
- 2018 and December 2024, 525 individual ransomware attacks were carried out against US government organizations, costing an estimated $1.09 billion in downtime.
- Ransomware attacks on SLTT are exponentially on the rise
  - Climbing from 41 in 2022 to 83 in 2023 and 88 in 2024.
  - Hit an all-time high in 2024 with 2.3 million records impacted, nearly three times the number of records affected in 2023 (almost 850,000).

For SLTT: Key infrastructure and services, such as 911 dispatch centers, sheriff's offices, city councils, and utilities. Government employees are often left stranded without their systems and have to resort to pen and paper. In some cases, organizations may be able to restore lost data using backups, but in many cases, they are forced to either pay extortionate ransom demands or make the costly decision to rebuild their systems from scratch.

12

Cyber breach statistics US state, local, tribal territories

- Security Today reports

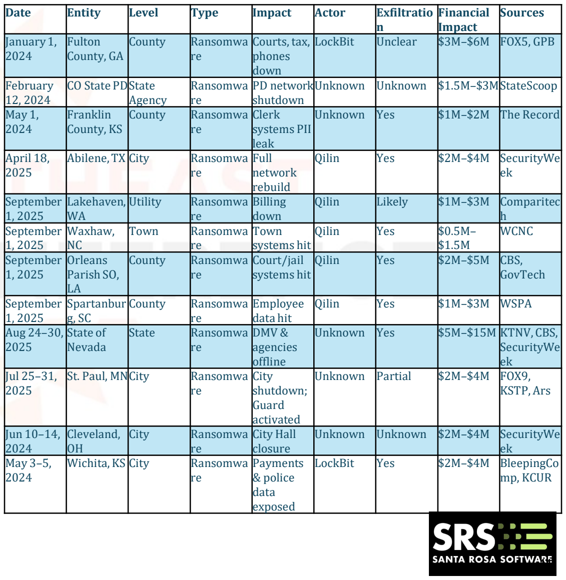


Date	Entity	Level	Type	Impact	Actor	Exfiltration	Financial Impact	Sources
1/1/2024	Fulton County, GA	County	Ransomware	Courts, tax, phones down	LockBit	Unclear	$3M–$6M	FOX5, GPB
2/12/2024	CO State PD	State Agency	Ransomware	PD network shutdown	Unknown	Unknown	$1.5M–$3M	StateScoop
5/1/2024	Franklin County, KS	County	Ransomware	Clerk systems PII leak	Unknown	Yes	$1M–$2M	The Record
5/3/2024	Wichita, KS	City	Ransomware	Payments & police data exposed	LockBit	Yes	$2M–$4M	BleepingComp, KCUR
6/10/2024	Cleveland, OH	City	Ransomware	City Hall closure	Unknown	Unknown	$2M–$4M	SecurityWeek
4/18/2025	Abilene, TX	City	Ransomware	Full network rebuild	Qilin	Yes	$2M–$4M	SecurityWeek
7/25/2025	St. Paul, MN	City	Ransomware	City shutdown; Guard activated	Unknown	Partial	$2M–$4M	FOX9, KSTP, Ars
8/24/2025	State of Nevada	State	Ransomware	DMV & agencies offline	Unknown	Yes	$5M–$15M	KTNV, CBS, SecurityWeek
9/1/2025	Lakehaven, WA	Utility	Ransomware	Billing down	Qilin	Likely	$1M–$3M	Comparitech
9/1/2025	Waxhaw, NC	Town	Ransomware	Town systems hit	Qilin	Yes	$0.5M–$1.5M	WCNC
9/1/2025	Orleans Parish SO, LA	County	Ransomware	Court/jail systems hit	Qilin	Yes	$2M–$5M	CBS, GovTech
9/1/2025	Spartanburg, SC	County	Ransomware	Employee data hit	Qilin	Yes	$1M–$3M	WSPA

SRS SANTA ROSA SOFTWARE

Cyber breach statistics US state, local, tribal territories

- By 2025, state and local governments were the third most-targeted sector for ransomware.
- A recorded 313% increase in attacks on SLTT governments (per MS-ISAC survey).
- Over 80% of these governments operate with fewer than five cybersecurity staff, making them highly vulnerable.
- Human error accounts for 70–90% of breaches.



Date	Entity	Level	Type	Impact	Actor	Exfiltration	Financial Impact	Sources
January 1, 2024	Fulton County, GA	County	Ransomware	Courts, tax, phones down	LockBit	Unclear	$3M–$6M	FOX5, GPB
February 12, 2024	CO State PD	State Agency	Ransomware	PD network shutdown	Unknown	Unknown	$1.5M–$3M	StateScoop
May 1, 2024	Franklin County, KS	County	Ransomware	Clerk systems PII leak	Unknown	Yes	$1M–$2M	The Record
April 18, 2025	Abilene, TX	City	Ransomware	Full network rebuild	Qilin	Yes	$2M–$4M	SecurityWeek
September 1, 2025	Lakehaven, WA	Utility	Ransomware	Billing down	Qilin	Likely	$1M–$3M	Comparitech
September 1, 2025	Waxhaw, NC	Town	Ransomware	Town systems hit	Qilin	Yes	$0.5M–$1.5M	WCNC
September 1, 2025	Orleans Parish SO, LA	County	Ransomware	Court/jail systems hit	Qilin	Yes	$2M–$5M	CBS, GovTech
September 1, 2025	Spartanburg, SC	County	Ransomware	Employee data hit	Qilin	Yes	$1M–$3M	WSPA
Aug 24–30, 2025	State of Nevada	State	Ransomware	DMV & agencies offline	Unknown	Yes	$5M–$15M	KTNV, CBS, SecurityWeek
Jul 25–31, 2025	St. Paul, MN	City	Ransomware	City shutdown; Guard activated	Unknown	Partial	$2M–$4M	FOX9, KSTP, Ars
Jun 10–14, 2024	Cleveland, OH	City	Ransomware	City Hall closure	Unknown	Unknown	$2M–$4M	SecurityWeek
May 3–5, 2024	Wichita, KS	City	Ransomware	Payments & police data exposed	LockBit	Yes	$2M–$4M	BleepingComp, KCUR

SRS SANTA ROSA SOFTWARE

Cyber breach statistics US state, local, tribal territories

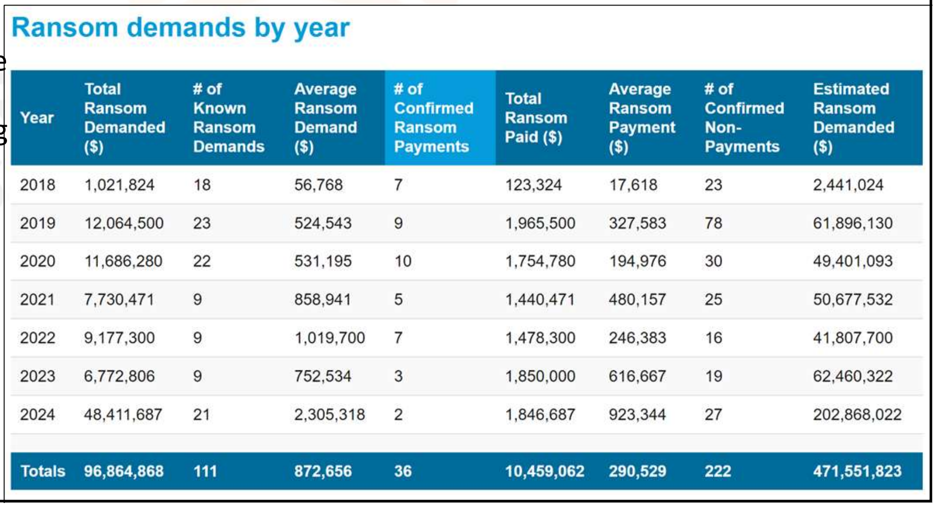
- On average, government organizations lost nearly 19.5 days to downtime, varying from seven days in 2021 to over 42 days in 2022
- The overall cost of these attacks is estimated to have been $1.09 billion
- Local governments have remained a key target for hackers over the years, as have emergency services, legal/judiciary entities, transport authorities, and libraries
- BlackSuit was the most prolific ransomware gang in 2024, with LockBit taking the top spot in 2023. LockBit was joined by ALPHV/BlackCat in 2022, while Dopplepaymer and Conti dominated in 2020/21, followed by Ryuk and Sodinokibi/REVIL in 2019, and SamSam in 2018

SRS SANTA ROSA SOFTWARE

15

Cyber breach statistics US state, local, tribal territories

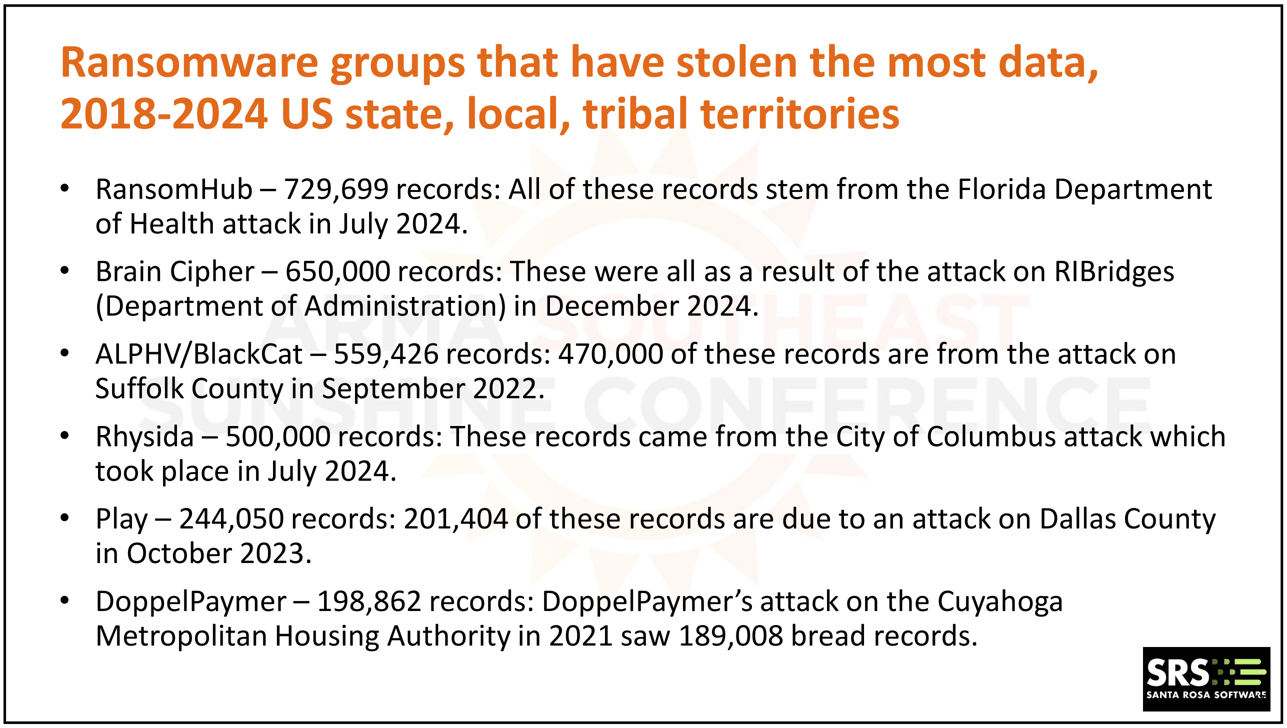
- In 2021, NC and FL introduced cybersecurity laws that ban government entities from paying ransom demands.
- Both states saw a dip in 2022 but the numbers rose again the following 2 years



Ransom demands by year

Year	Total Ransom Demanded ($)	# of Known Ransom Demands	Average Ransom Demand ($)	# of Confirmed Ransom Payments	Total Ransom Paid ($)	Average Ransom Payment ($)	# of Confirmed Non-Payments	Estimated Ransom Demanded ($)
2018	1,021,824	18	56,768	7	123,324	17,618	23	2,441,024
2019	12,064,500	23	524,543	9	1,965,500	327,583	78	61,896,130
2020	11,686,280	22	531,195	10	1,754,780	194,976	30	49,401,093
2021	7,730,471	9	858,941	5	1,440,471	480,157	25	50,677,532
2022	9,177,300	9	1,019,700	7	1,478,300	246,383	16	41,807,700
2023	6,772,806	9	752,534	3	1,850,000	616,667	19	62,460,322
2024	48,411,687	21	2,305,318	2	1,846,687	923,344	27	202,868,022
Totals	96,864,868	111	872,656	36	10,459,062	290,529	222	471,551,823

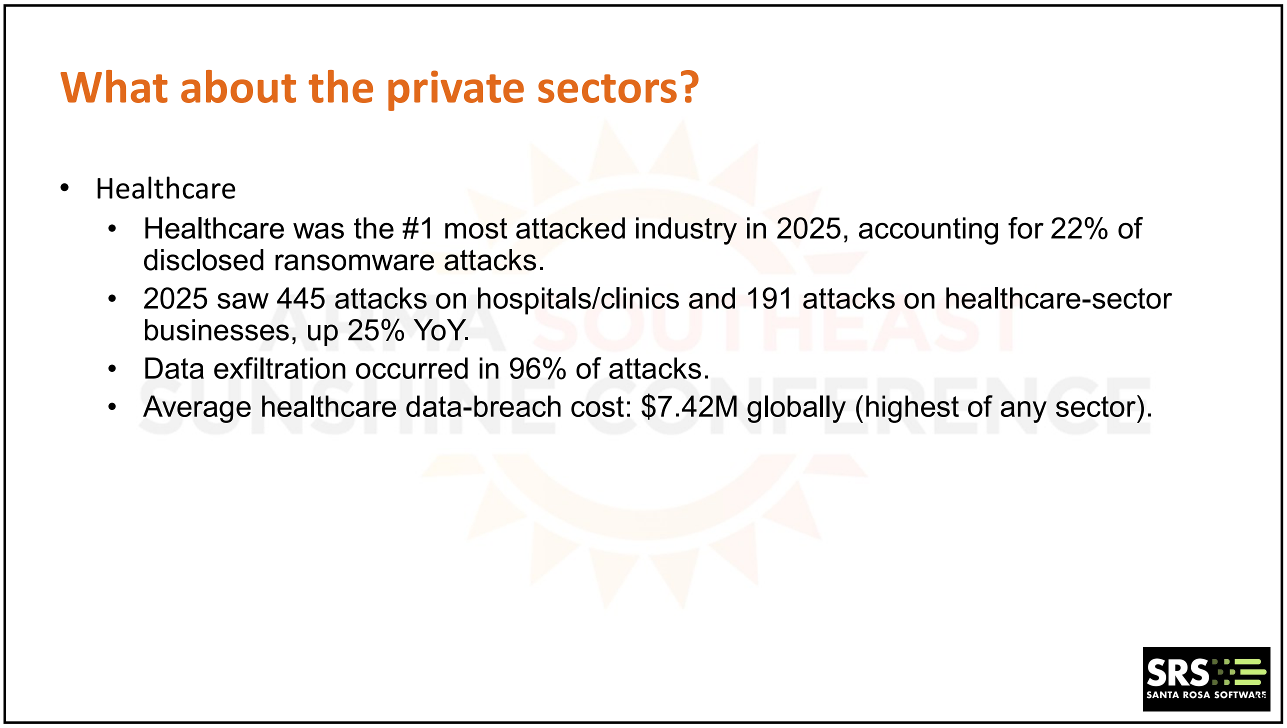
16



Ransomware groups that have stolen the most data, 2018-2024 US state, local, tribal territories

- RansomHub – 729,699 records: All of these records stem from the Florida Department of Health attack in July 2024.
- Brain Cipher – 650,000 records: These were all as a result of the attack on RIBridges (Department of Administration) in December 2024.
- ALPHV/BlackCat – 559,426 records: 470,000 of these records are from the attack on Suffolk County in September 2022.
- Rhysida – 500,000 records: These records came from the City of Columbus attack which took place in July 2024.
- Play – 244,050 records: 201,404 of these records are due to an attack on Dallas County in October 2023.
- DoppelPaymer – 198,862 records: DoppelPaymer's attack on the Cuyahoga Metropolitan Housing Authority in 2021 saw 189,008 bread records.

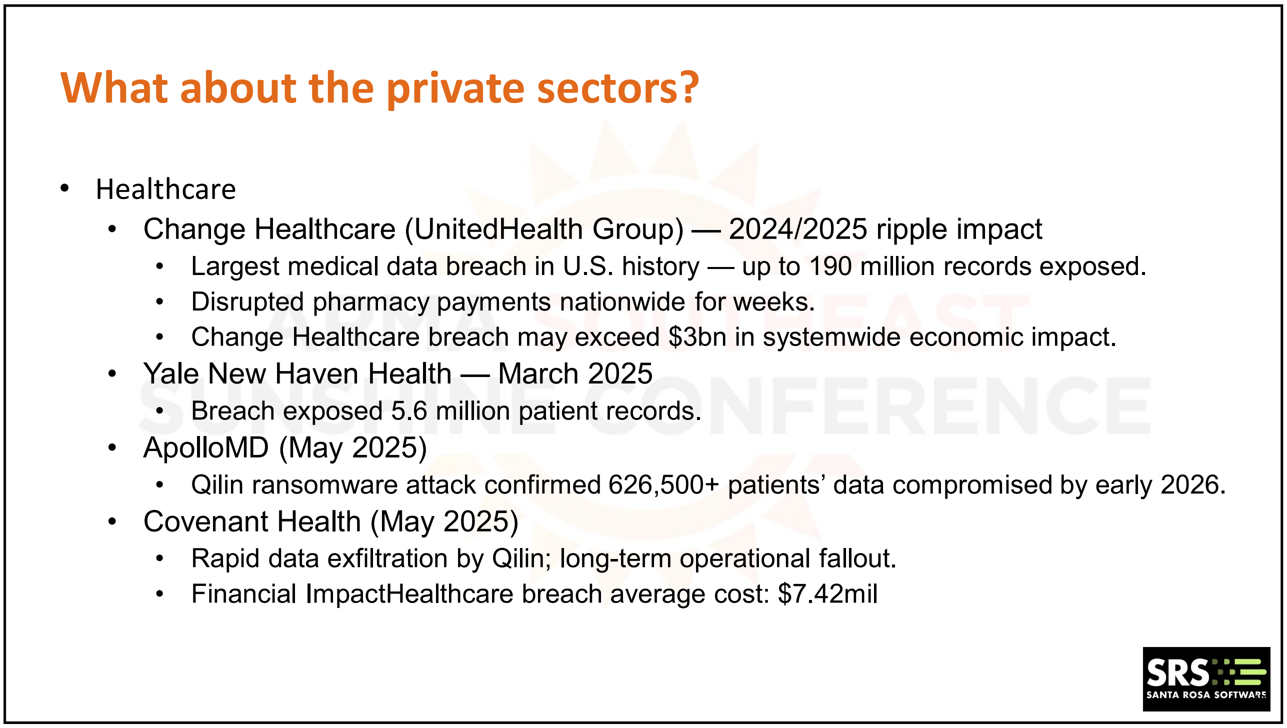
17



What about the private sectors?

- Healthcare
  - Healthcare was the #1 most attacked industry in 2025, accounting for 22% of disclosed ransomware attacks.
  - 2025 saw 445 attacks on hospitals/clinics and 191 attacks on healthcare-sector businesses, up 25% YoY.
  - Data exfiltration occurred in 96% of attacks.
  - Average healthcare data-breach cost: $7.42M globally (highest of any sector).

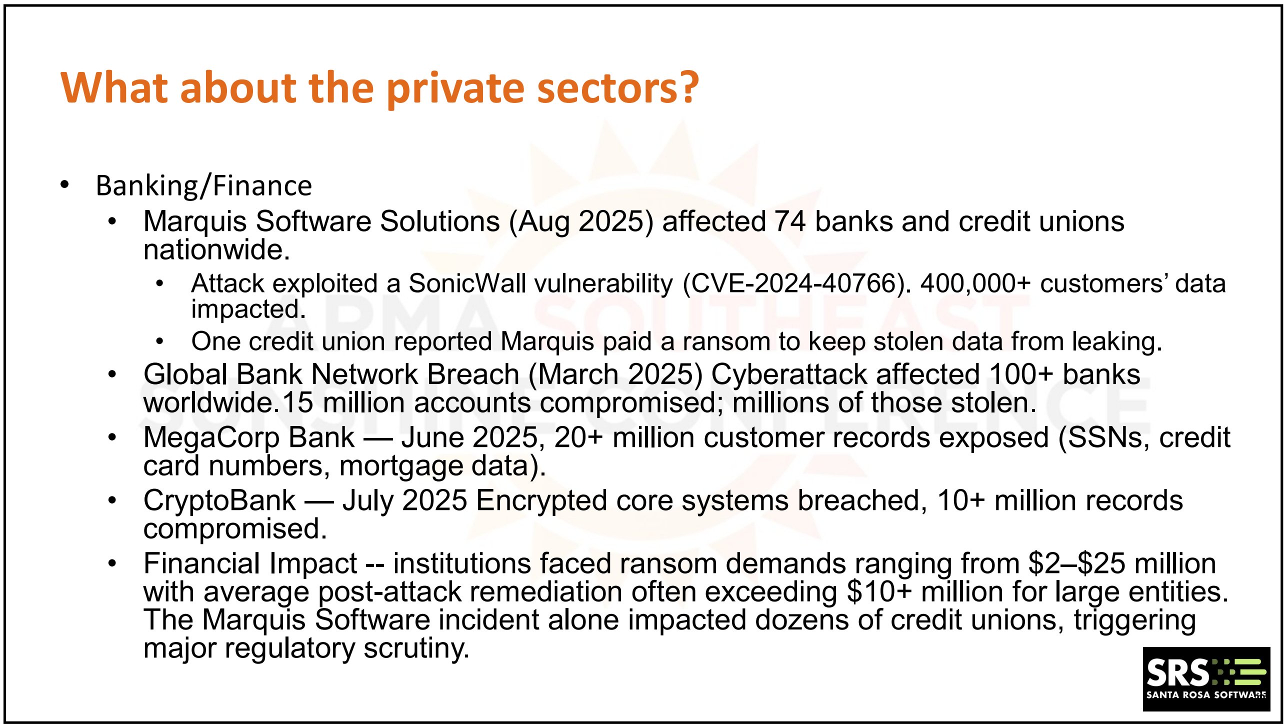
18



What about the private sectors?

- Healthcare
  - Change Healthcare (UnitedHealth Group) — 2024/2025 ripple impact
    - Largest medical data breach in U.S. history — up to 190 million records exposed.
    - Disrupted pharmacy payments nationwide for weeks.
    - Change Healthcare breach may exceed $3bn in systemwide economic impact.
  - Yale New Haven Health — March 2025
    - Breach exposed 5.6 million patient records.
  - ApolloMD (May 2025)
    - Qilin ransomware attack confirmed 626,500+ patients' data compromised by early 2026.
  - Covenant Health (May 2025)
    - Rapid data exfiltration by Qilin; long-term operational fallout.
    - Financial ImpactHealthcare breach average cost: $7.42mil

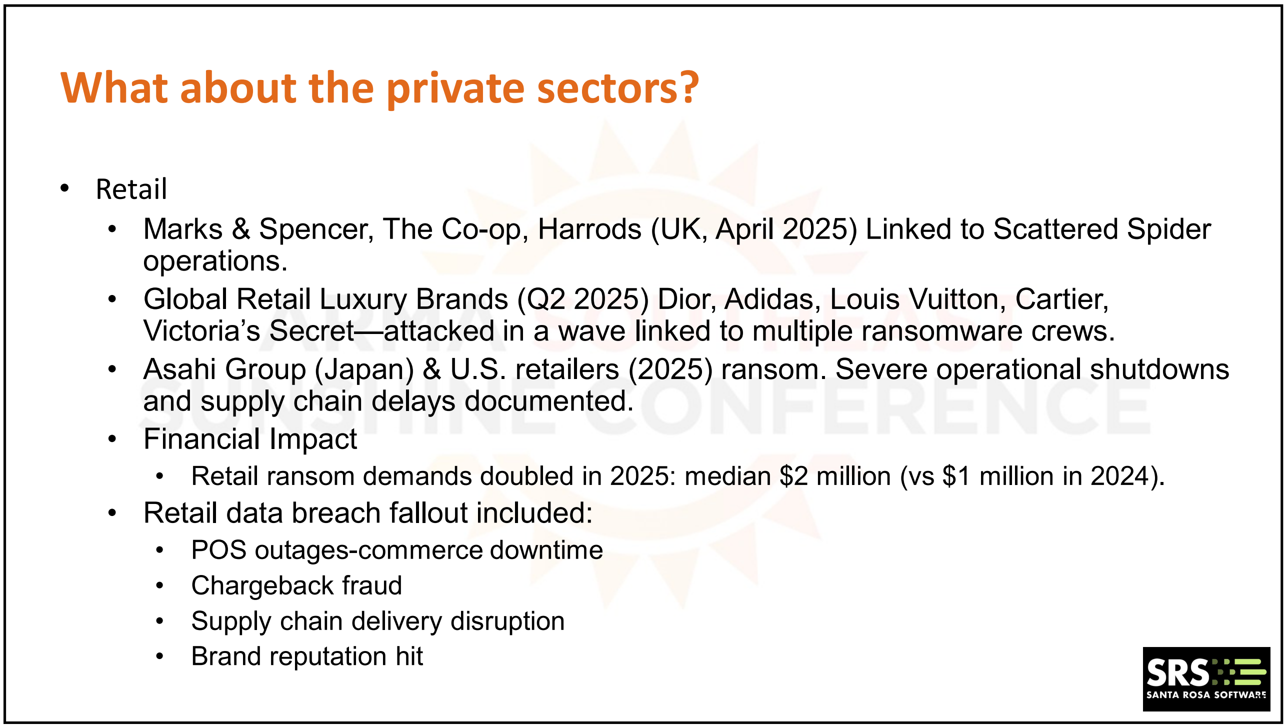
19



What about the private sectors?

- Banking/Finance
  - Marquis Software Solutions (Aug 2025) affected 74 banks and credit unions nationwide.
    - Attack exploited a SonicWall vulnerability (CVE-2024-40766). 400,000+ customers' data impacted.
    - One credit union reported Marquis paid a ransom to keep stolen data from leaking.
  - Global Bank Network Breach (March 2025) Cyberattack affected 100+ banks worldwide.15 million accounts compromised; millions of those stolen.
  - MegaCorp Bank — June 2025, 20+ million customer records exposed (SSNs, credit card numbers, mortgage data).
  - CryptoBank — July 2025 Encrypted core systems breached, 10+ million records compromised.
  - Financial Impact -- institutions faced ransom demands ranging from $2–$25 million with average post-attack remediation often exceeding $10+ million for large entities. The Marquis Software incident alone impacted dozens of credit unions, triggering major regulatory scrutiny.

20

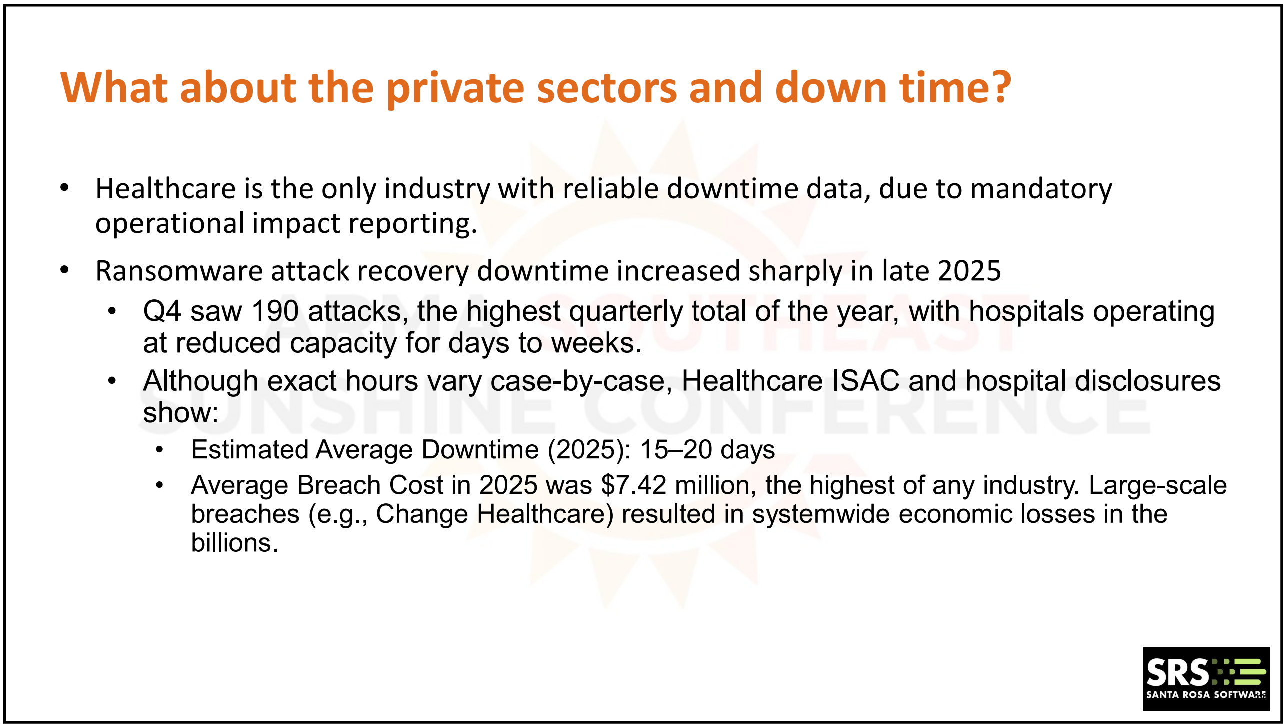


What about the private sectors?

- Retail
  - Marks & Spencer, The Co-op, Harrods (UK, April 2025) Linked to Scattered Spider operations.
  - Global Retail Luxury Brands (Q2 2025) Dior, Adidas, Louis Vuitton, Cartier, Victoria's Secret—attacked in a wave linked to multiple ransomware crews.
  - Asahi Group (Japan) & U.S. retailers (2025) ransom. Severe operational shutdowns and supply chain delays documented.
  - Financial Impact
    - Retail ransom demands doubled in 2025: median $2 million (vs $1 million in 2024).
  - Retail data breach fallout included:
    - POS outages-commerce downtime
    - Chargeback fraud
    - Supply chain delivery disruption
    - Brand reputation hit

SRS SANTA ROSA SOFTWARE

21

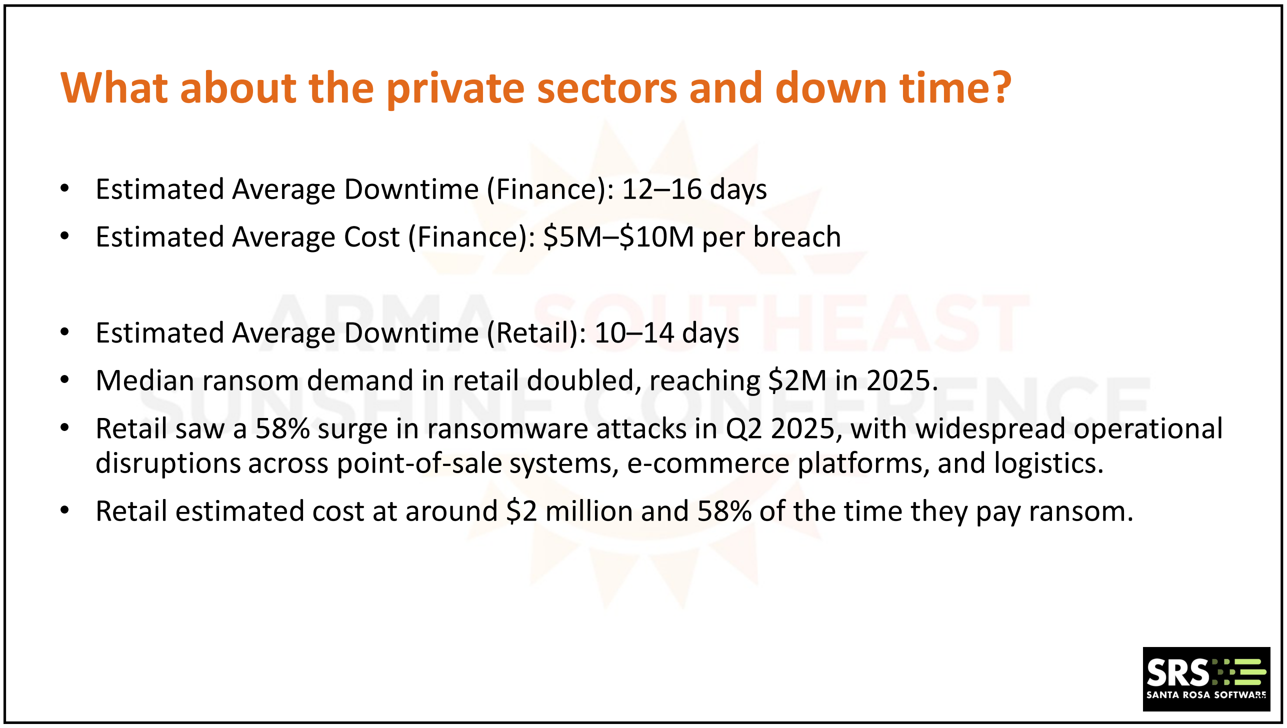


What about the private sectors and down time?

- Healthcare is the only industry with reliable downtime data, due to mandatory operational impact reporting.
- Ransomware attack recovery downtime increased sharply in late 2025
  - Q4 saw 190 attacks, the highest quarterly total of the year, with hospitals operating at reduced capacity for days to weeks.
  - Although exact hours vary case-by-case, Healthcare ISAC and hospital disclosures show:
    - Estimated Average Downtime (2025): 15–20 days
    - Average Breach Cost in 2025 was $7.42 million, the highest of any industry. Large-scale breaches (e.g., Change Healthcare) resulted in systemwide economic losses in the billions.

SRS SANTA ROSA SOFTWARE

22

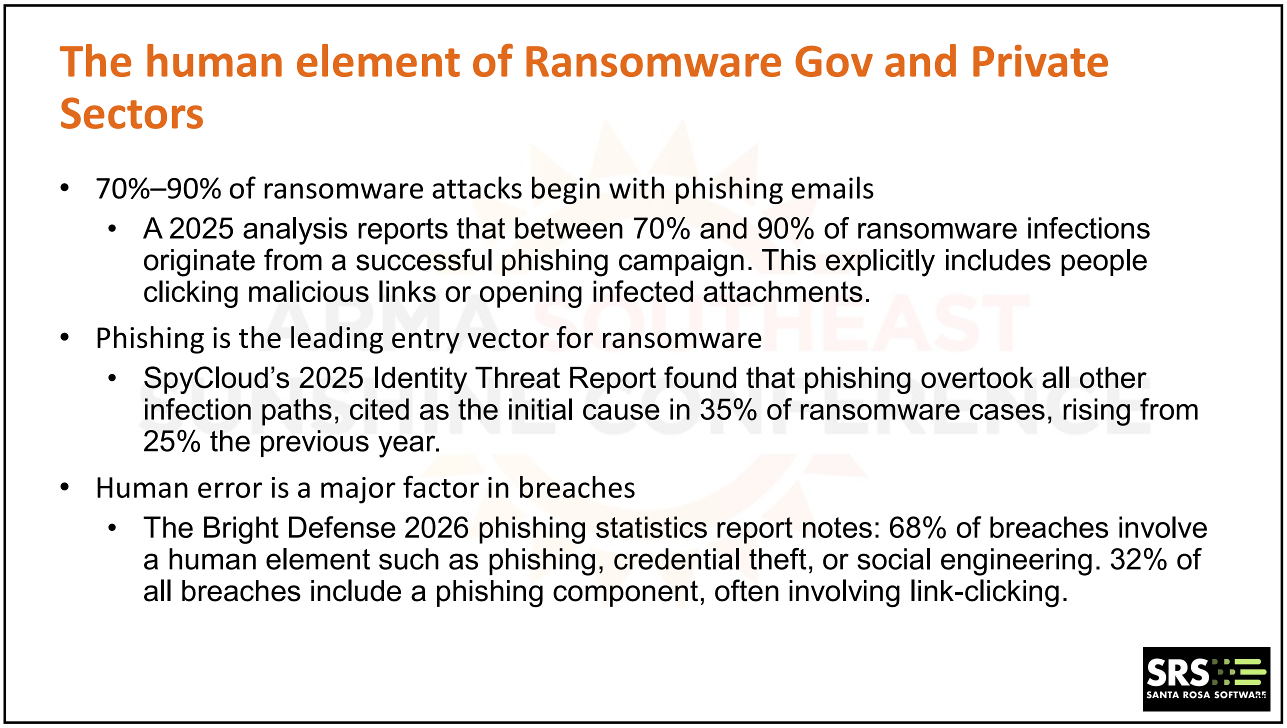


What about the private sectors and down time?

- Estimated Average Downtime (Finance): 12–16 days
- Estimated Average Cost (Finance): $5M–$10M per breach

- Estimated Average Downtime (Retail): 10–14 days
- Median ransom demand in retail doubled, reaching $2M in 2025.
- Retail saw a 58% surge in ransomware attacks in Q2 2025, with widespread operational disruptions across point-of-sale systems, e-commerce platforms, and logistics.
- Retail estimated cost at around $2 million and 58% of the time they pay ransom.

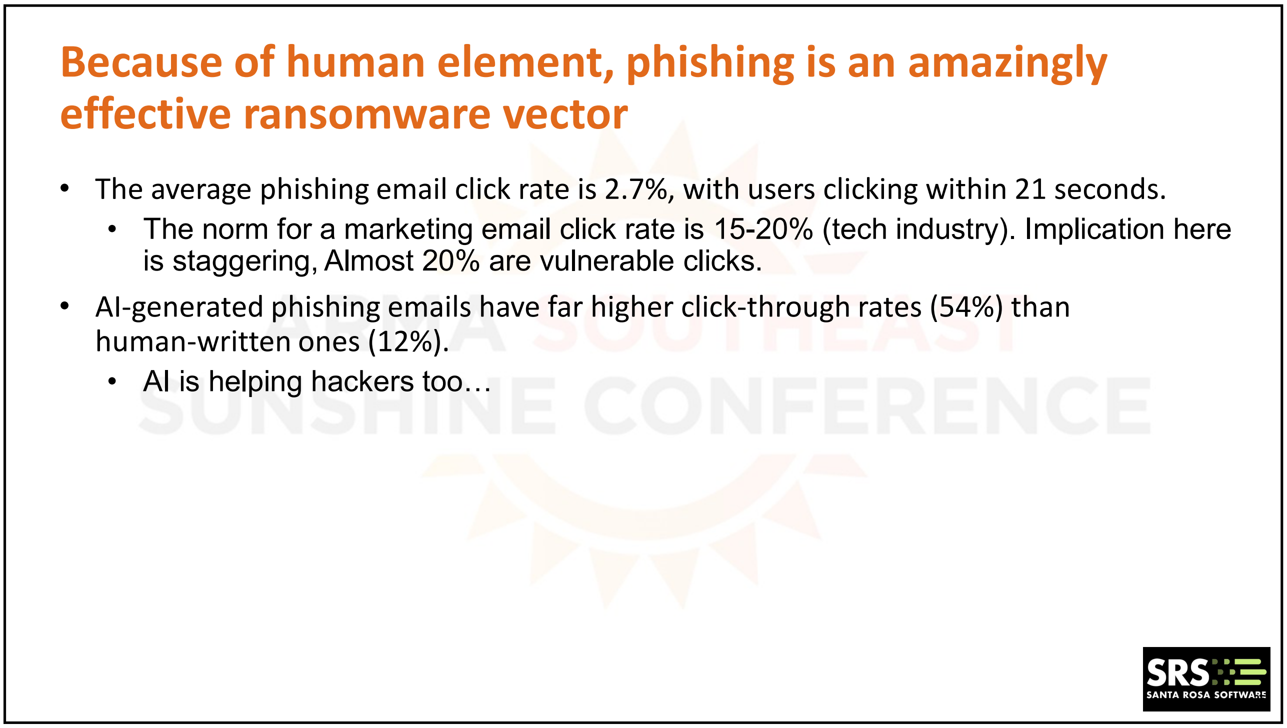
23



The human element of Ransomware Gov and Private Sectors

- 70%–90% of ransomware attacks begin with phishing emails
  - A 2025 analysis reports that between 70% and 90% of ransomware infections originate from a successful phishing campaign. This explicitly includes people clicking malicious links or opening infected attachments.
- Phishing is the leading entry vector for ransomware
  - SpyCloud’s 2025 Identity Threat Report found that phishing overtook all other infection paths, cited as the initial cause in 35% of ransomware cases, rising from 25% the previous year.
- Human error is a major factor in breaches
  - The Bright Defense 2026 phishing statistics report notes: 68% of breaches involve a human element such as phishing, credential theft, or social engineering. 32% of all breaches include a phishing component, often involving link-clicking.

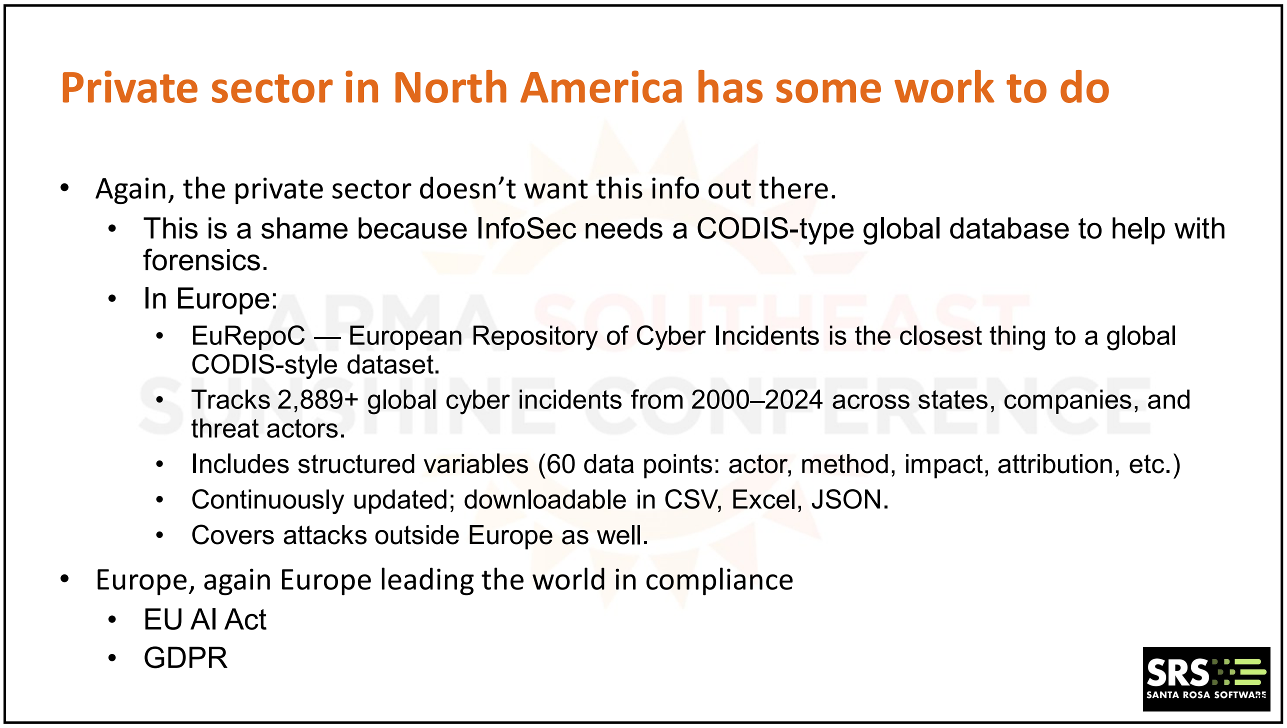
24



Because of human element, phishing is an amazingly effective ransomware vector

- The average phishing email click rate is 2.7%, with users clicking within 21 seconds.
  - The norm for a marketing email click rate is 15-20% (tech industry). Implication here is staggering, Almost 20% are vulnerable clicks.
- AI-generated phishing emails have far higher click-through rates (54%) than human-written ones (12%).
  - AI is helping hackers too…

25



Private sector in North America has some work to do

- Again, the private sector doesn't want this info out there.
  - This is a shame because InfoSec needs a CODIS-type global database to help with forensics.
  - In Europe:
    - EuRepoC — European Repository of Cyber Incidents is the closest thing to a global CODIS-style dataset.
    - Tracks 2,889+ global cyber incidents from 2000–2024 across states, companies, and threat actors.
    - Includes structured variables (60 data points: actor, method, impact, attribution, etc.)
    - Continuously updated; downloadable in CSV, Excel, JSON.
    - Covers attacks outside Europe as well.
- Europe, again Europe leading the world in compliance
  - EU AI Act
  - GDPR

26

ARMA SOUTHEAST
SUNSHINE CONFERENCE

USE CASES WITH HUMAN SHORTCOMINGS

27

A few historic hacks involving the human element

- The Earliest Recorded "Hacks"
  - The MIT Password Theft (1962): Student Allan Scherr used a punch card trick to bypass security and print all user passwords to gain more computer time.
    - From this hack was borne encryption.
  - The Morris Worm (1988): The first major internet-scale breach, which accidentally crashed 10% of the early web (He said he just wanted to measure how many computers were on the internet.)
    - From what I could research, it was the one of the first viruses because it replicated.
  - Was the first-ever conviction under the 1986 Computer Fraud and Abuse Act
- The First Modern Financial Heist: Citibank (1994), the Vladimir Levin hack
  - Method: Utilized dial-up wire transfer services to intercept customer PINS and passwords.
  - Impact: Attempted to steal $10.7 million; it was the first time a bank was robbed from a remote computer terminal across international borders.

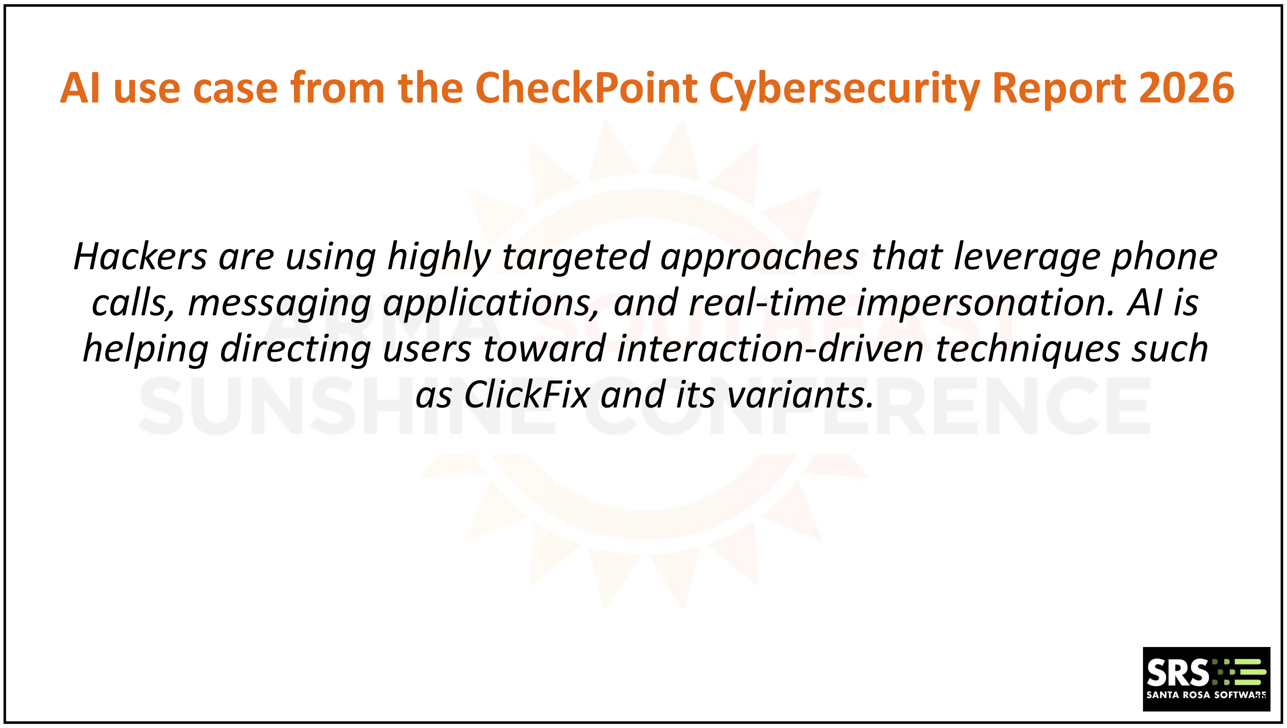
SRS SANTA ROSA SOFTWARE

28

AI is helping Gov and Industry fight cybercrime, but…

- 60 Minutes episode 2023 – "Surge in Digital Theft Targeting Seniors"
  - The episode highlights losses from digital theft have doubled in the past two years, according to the FBI.
  - Seniors are increasingly targeted because scammers view them as more trusting and financially stable.
  - Emotional Manipulation as a Key Strategy: AI-driven voice cloning and messaging tools help impersonate relatives convincingly saying they are in a hardship then asking for money.
  - Scammers targeting parents and grandparents, pretending to be children or grandchildren in distress.
- This is happening now. EVERYWHERE.

29



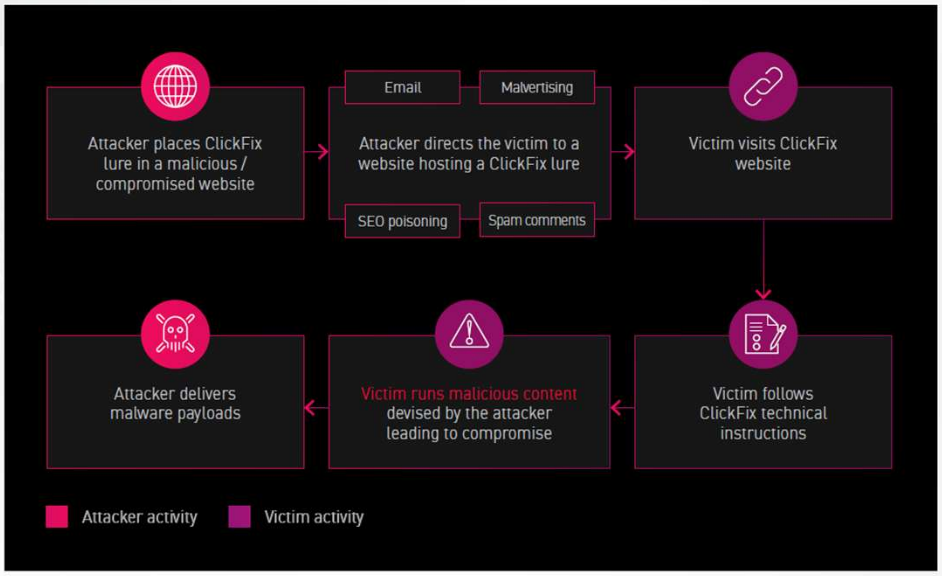
AI use case from the CheckPoint Cybersecurity Report 2026

Hackers are using highly targeted approaches that leverage phone calls, messaging applications, and real-time impersonation. AI is helping directing users toward interaction-driven techniques such as ClickFix and its variants.

30

AI use case from the CheckPoint Cybersecurity Report 2026

Here's what it looks like…



Attacker places ClickFix lure in a malicious / compromised website

Attacker directs the victim to a website hosting a ClickFix lure

Victim visits ClickFix website

Victim follows ClickFix technical instructions

Victim runs malicious content devised by the attacker leading to compromise

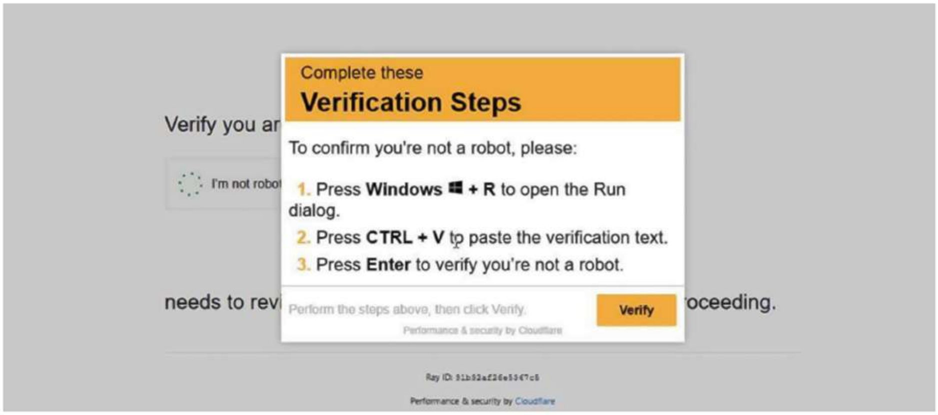
Attacker delivers malware payloads

🟥 Attacker activity 🟪 Victim activity

31

AI use case from the CheckPoint Cybersecurity Report 2026

Here's what it looks like…



Verify you ar

I'm not robot

needs to revi … oceeding.

Complete these
Verification Steps

To confirm you're not a robot, please:

1. Press **Windows** ⊞ **+ R** to open the Run dialog.
2. Press **CTRL + V** tp paste the verification text.
3. Press **Enter** to verify you're not a robot.

Perform the steps above, then click Verify.

Performance & security by Cloudflare

Ray ID: 91b32af26e5347c8

Performance & security by Cloudflare

32

AI use case from the CheckPoint Cybersecurity Report 2026

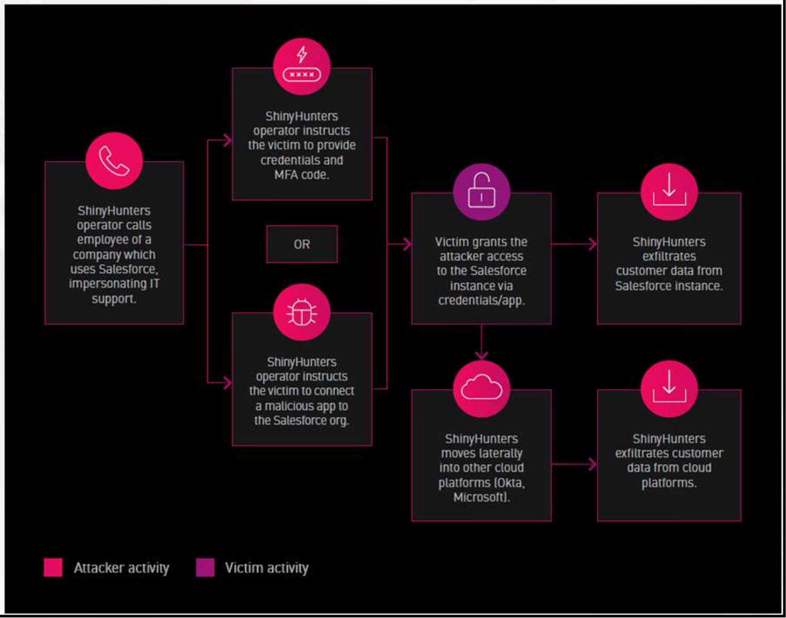
In 2025, ClickFix activity increased by nearly 500% compared to the previous year and was observed in nearly half of all documented malware incidents.

Voice-Based Social Engineering is the weapon of choice for major attacks and voice phishing, and impersonation will continue to grow in 2026 and beyond because of the human element of cyber crime.

33

AI use case from the CheckPoint Cybersecurity Report 2026

ClickFIx also compromised British auto manufacturer Jaguar Land Rover (JLR) in August of 2025…



ShinyHunters operator calls employee of a company which uses Salesforce, impersonating IT support.

ShinyHunters operator instructs the victim to provide credentials and MFA code.

OR

ShinyHunters operator instructs the victim to connect a malicious app to the Salesforce org.

Victim grants the attacker access to the Salesforce instance via credentials/app.

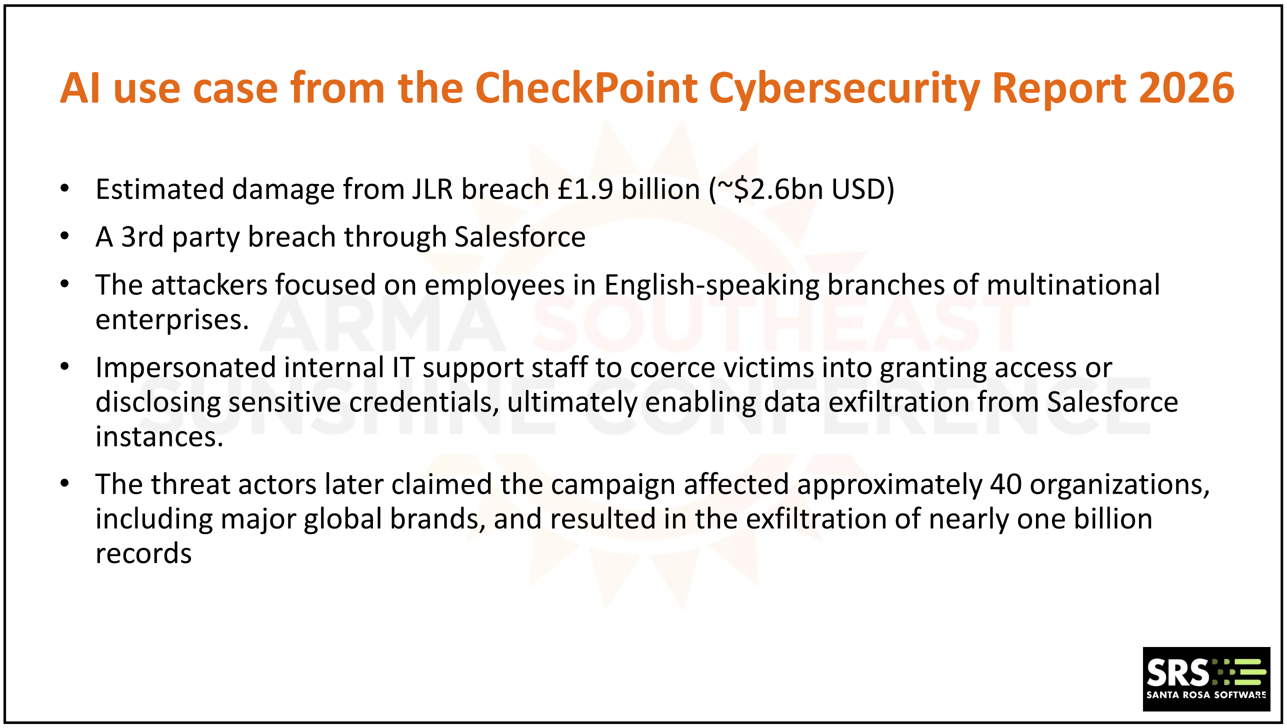
ShinyHunters exfiltrates customer data from Salesforce instance.

ShinyHunters moves laterally into other cloud platforms (Okta, Microsoft).

ShinyHunters exfiltrates customer data from cloud platforms.

🟥 Attacker activity 🟪 Victim activity

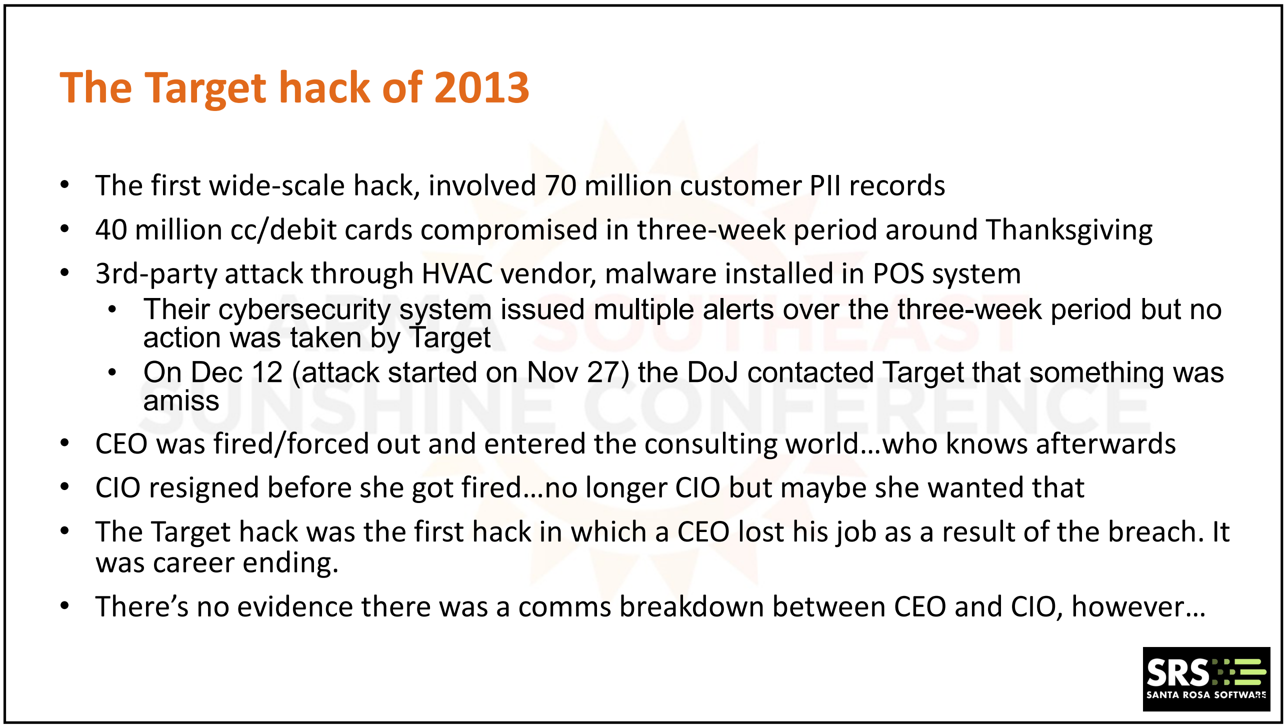
34



AI use case from the CheckPoint Cybersecurity Report 2026

- Estimated damage from JLR breach £1.9 billion (~$2.6bn USD)
- A 3rd party breach through Salesforce
- The attackers focused on employees in English-speaking branches of multinational enterprises.
- Impersonated internal IT support staff to coerce victims into granting access or disclosing sensitive credentials, ultimately enabling data exfiltration from Salesforce instances.
- The threat actors later claimed the campaign affected approximately 40 organizations, including major global brands, and resulted in the exfiltration of nearly one billion records

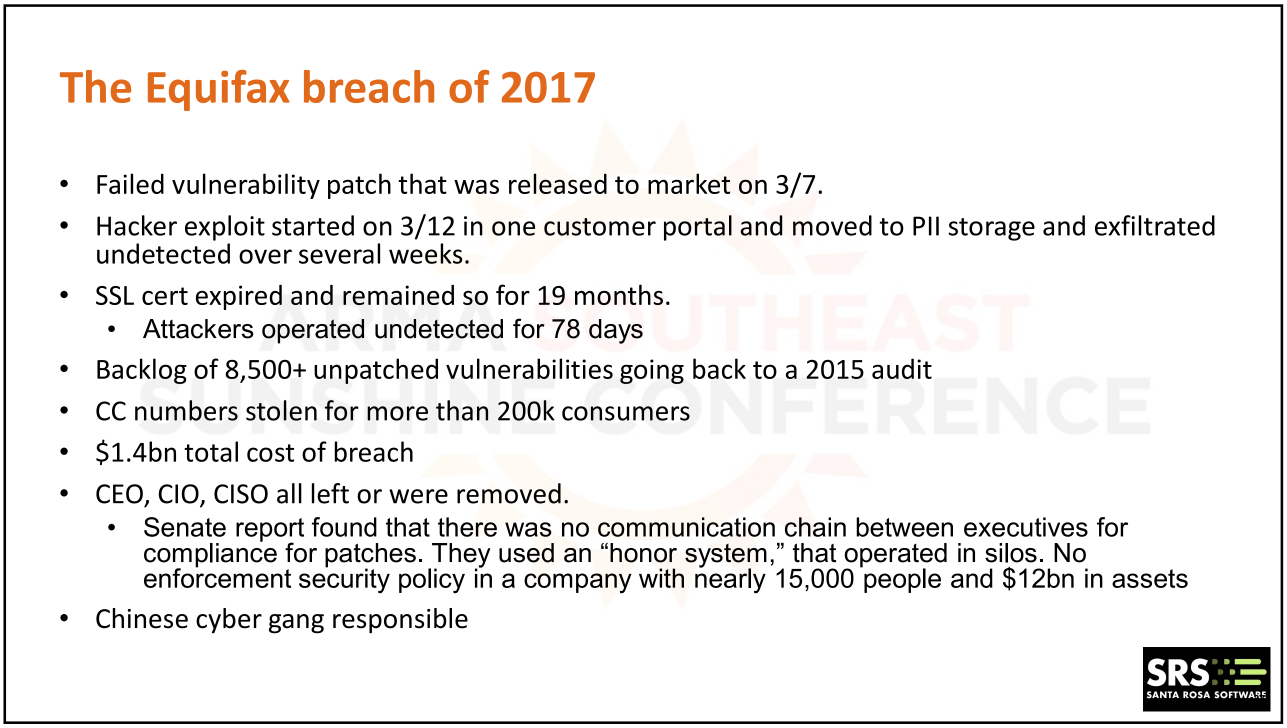
35



The Target hack of 2013

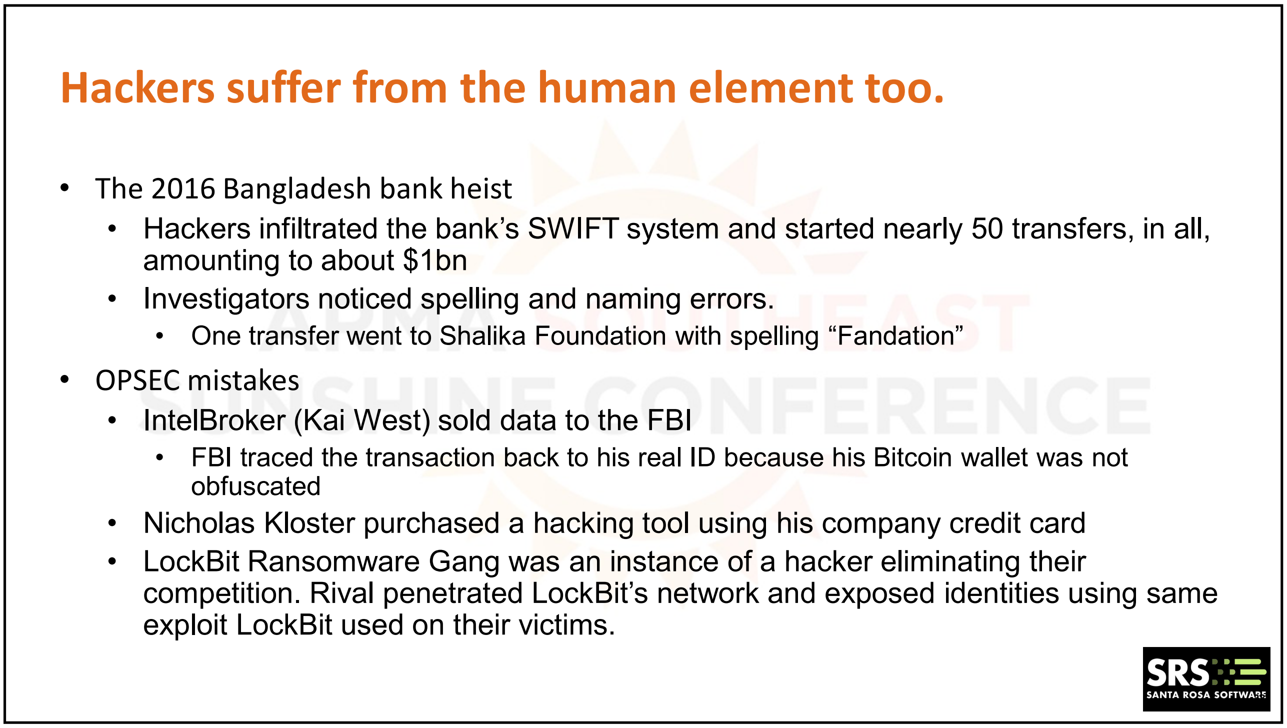
- The first wide-scale hack, involved 70 million customer PII records
- 40 million cc/debit cards compromised in three-week period around Thanksgiving
- 3rd-party attack through HVAC vendor, malware installed in POS system
  - Their cybersecurity system issued multiple alerts over the three-week period but no action was taken by Target
  - On Dec 12 (attack started on Nov 27) the DoJ contacted Target that something was amiss
- CEO was fired/forced out and entered the consulting world…who knows afterwards
- CIO resigned before she got fired…no longer CIO but maybe she wanted that
- The Target hack was the first hack in which a CEO lost his job as a result of the breach. It was career ending.
- There’s no evidence there was a comms breakdown between CEO and CIO, however…

36



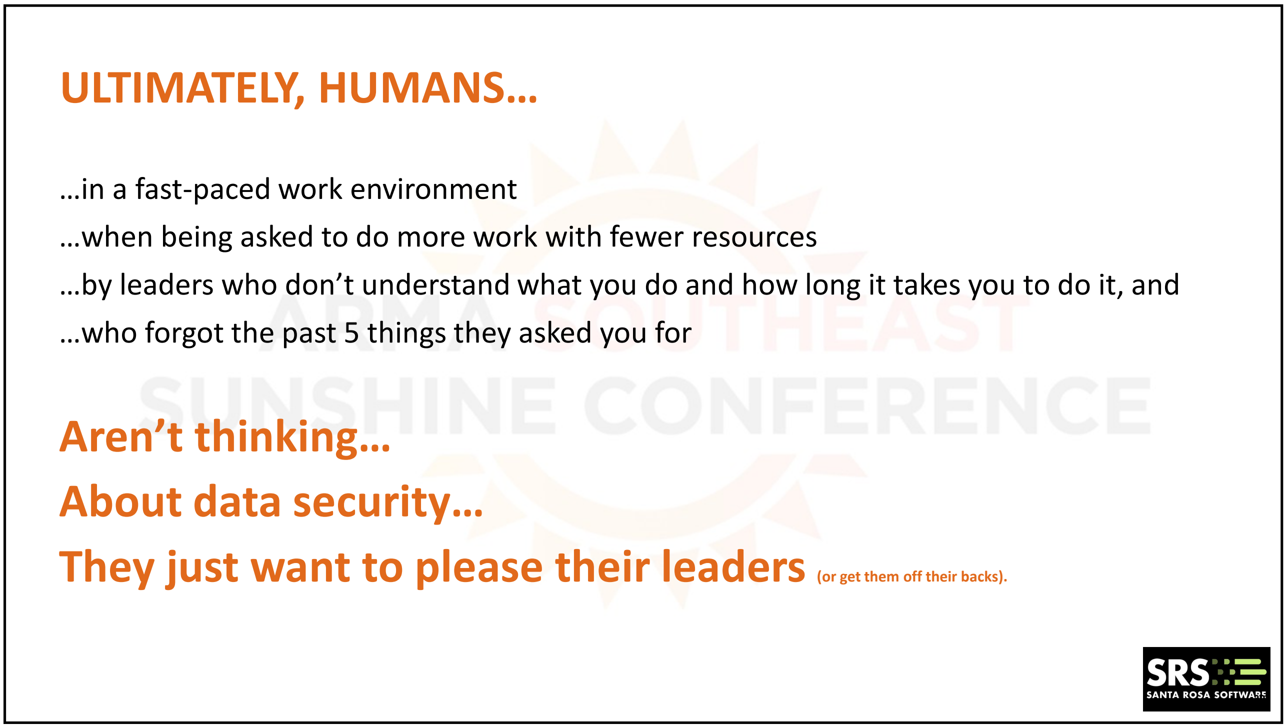
The Equifax breach of 2017

- Failed vulnerability patch that was released to market on 3/7.
- Hacker exploit started on 3/12 in one customer portal and moved to PII storage and exfiltrated undetected over several weeks.
- SSL cert expired and remained so for 19 months.
  - Attackers operated undetected for 78 days
- Backlog of 8,500+ unpatched vulnerabilities going back to a 2015 audit
- CC numbers stolen for more than 200k consumers
- $1.4bn total cost of breach
- CEO, CIO, CISO all left or were removed.
  - Senate report found that there was no communication chain between executives for compliance for patches. They used an “honor system,” that operated in silos. No enforcement security policy in a company with nearly 15,000 people and $12bn in assets
- Chinese cyber gang responsible



Hackers suffer from the human element too.

- The 2016 Bangladesh bank heist
  - Hackers infiltrated the bank’s SWIFT system and started nearly 50 transfers, in all, amounting to about $1bn
  - Investigators noticed spelling and naming errors.
    - One transfer went to Shalika Foundation with spelling “Fandation”
- OPSEC mistakes
  - IntelBroker (Kai West) sold data to the FBI
    - FBI traced the transaction back to his real ID because his Bitcoin wallet was not obfuscated
  - Nicholas Kloster purchased a hacking tool using his company credit card
  - LockBit Ransomware Gang was an instance of a hacker eliminating their competition. Rival penetrated LockBit’s network and exposed identities using same exploit LockBit used on their victims.



ULTIMATELY, HUMANS…

…in a fast-paced work environment

…when being asked to do more work with fewer resources

…by leaders who don't understand what you do and how long it takes you to do it, and

…who forgot the past 5 things they asked you for

Aren't thinking…

About data security…

They just want to please their leaders (or get them off their backs).

SRS SANTA ROSA SOFTWARE

39

ARMA SOUTHEAST
SUNSHINE CONFERENCE

SO, WHAT CAN YOU DO ABOUT IT?

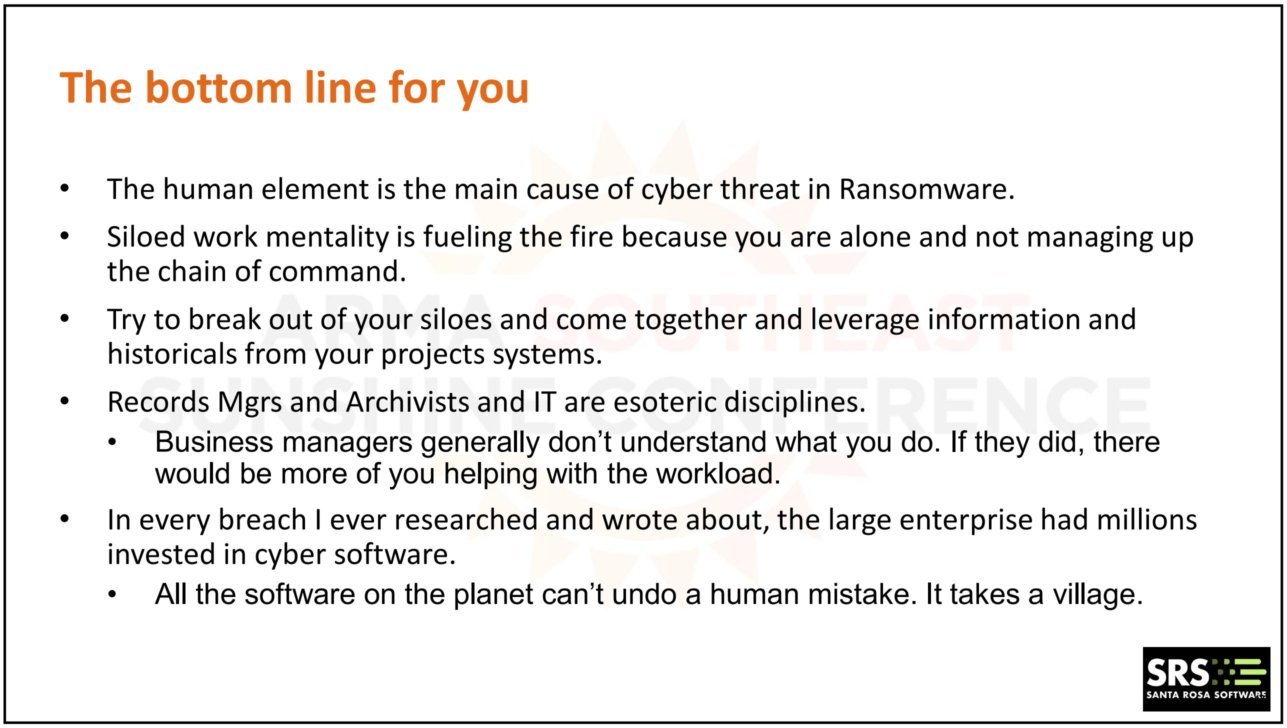
40

Unite!

THE WORKPLACE
"Come together, right now ... "
- The Beatles, Abbey Road album, 1969

What you need to do about it

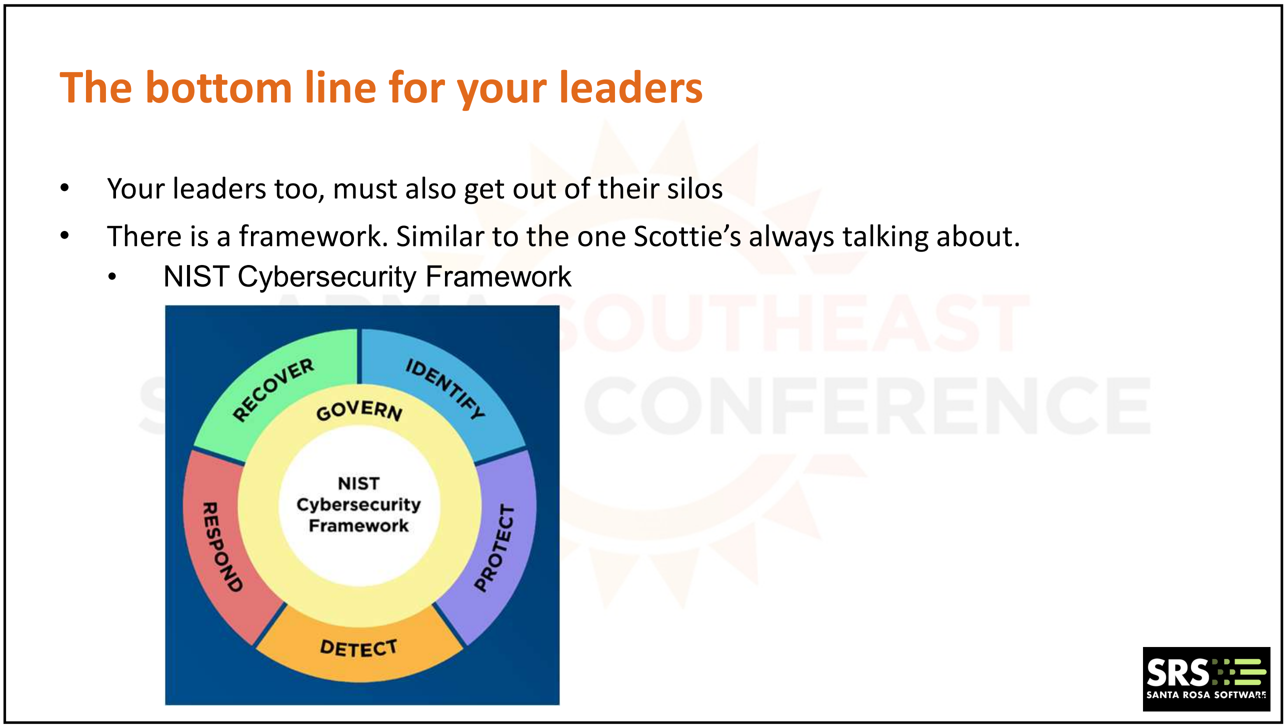
- There is strength in communication
  - RMs are more readily becoming single entity departments but there is strength in numbers. Find allies!
    - Find people like you – marketing, IT, other esoteric titles
  - Project management and PM systems are helpful.
    - How long will it take and what's the status?
    - More importantly:
      - What's in the work queue now?
      - What are the new requests?
      - What are the deadlines we're being asked?
- Do this math and communicate back up the chain of command. SET EXPECTATIONS up the chain.
  - Communicate together. You have a lot in common. Come together, right now.



The bottom line for you

- The human element is the main cause of cyber threat in Ransomware.
- Siloed work mentality is fueling the fire because you are alone and not managing up the chain of command.
- Try to break out of your siloes and come together and leverage information and historicals from your projects systems.
- Records Mgrs and Archivists and IT are esoteric disciplines.
  - Business managers generally don't understand what you do. If they did, there would be more of you helping with the workload.
- In every breach I ever researched and wrote about, the large enterprise had millions invested in cyber software.
  - All the software on the planet can't undo a human mistake. It takes a village.

43

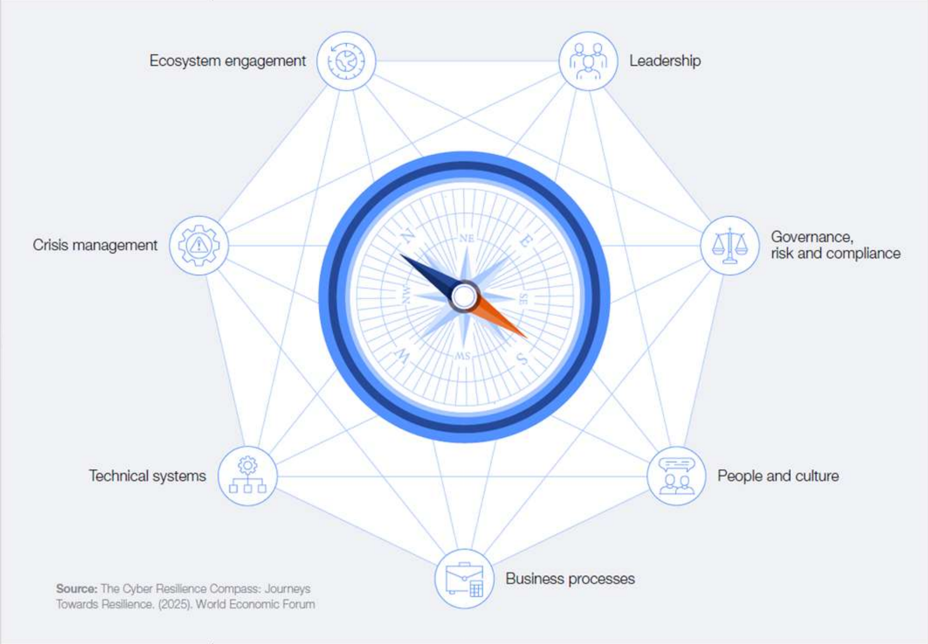


The bottom line for your leaders

- Your leaders too, must also get out of their silos
- There is a framework. Similar to the one Scottie's always talking about.
  - NIST Cybersecurity Framework

44

FIGURE 31 | Hallmarks of resilient organizations



Source: The Cyber Resilience Compass: Journeys Towards Resilience. (2025). World Economic Forum

SRS SANTA ROSA SOFTWARE

45

It takes a village to secure your data and IP

- Ecosystem engagement
- Leadership
- Governance, risk & compliance
- People and culture
- Business processes
- Technical systems
- Crisis management
- It must start at onboarding and be commandeered by your CHRO with periodic and recurring continuing education

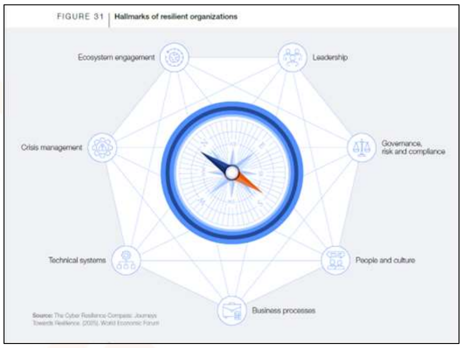


FIGURE 31 | Hallmarks of resilient organizations
Ecosystem engagement
Leadership
Crisis management
Governance, risk and compliance
Technical systems
People and culture
Business processes
Source: The Cyber Resilience Compass: Journeys Towards Resilience. (2025). World Economic Forum

SRS SANTA ROSA SOFTWARE

46

Few parting thoughts before Q&A

In every breach I ever researched and wrote about, the large enterprise had millions invested cyber tools and humans to prevent cybertheft.

HR-aided education at onboarding and continuous monitoring across all systems are a great start.

But it's better communication that will get you better InfoSec.

Give this presentation to your CHRO.

47

THANK YOU!

Tony Perri, CEO/Co-founder
Santa Rosa Software, LLC
Chattanooga, TN
tony.perri@santarosasoftware.com
https://santarosasoftware.com
https://www.linkedin.com/in/tonyperri/

IBM Champion

48

Presentation Sources

- https://www.nist.gov/cyberframework
- https://thebestvpn.com
- https://history.computer.org/pioneers/aiken.html
- https://securitytoday.com
- https://comparitech.com
- https://hipaajournal.com
- https://us.sciencehealth.com
- https://techradar.com
- https://cybersecurityinsiders.com
- https://infosecuritymagazine.com
- https://bluefin.com
- https://securityweek.com
- https://sophos.com
- https://govtech.com
- https://aeanet.org
- https://spycloud.com
- https://brightdefense.com
- https://secureframe.com
- https://www.weforum.org/publications/global-cybersecurity-outlook-2026/
- https://www.checkpoint.com/security-report/

SRS SANTA ROSA SOFTWARE

49