Cyber Security:

Understanding the Risk and Career Landscape

Jenny Menna & James Binford

When we went to the moon in the 60s vs. now

Then, memory was small and computers were big.
Now, memory is large and computers are small.

Apollo Guidance Computer

- 2 MHz processor
- 4 kB RAM
- 75 kB storage
- Weight: 70 lbs

IBM System / 360 Model 75

- 6 MB (6,000 kB) program

Today's Apple iPhone

- 512 GB capacity
- **Nearly 1,000,000 times more capacity** than it took to put humans on the moon!
- And you can use it anywhere…

Source: *https://en.wikipedia.org/wiki/IPhone*
Source: *https://en.m.wikipedia.org/wiki/Apollo_Guidance_Computer*

Innovations in financial services in the past 10 years

Mobile payment apps

SAMSUNG pay Pay pay

Real-time payments

Zelle RTP

Geolocation-based banking

Aggregators

ENVESTNET
YODLEE

Digital $/Distributed Ledger

DTCC

Project Lithium

Voice-first banking

Hey Siri

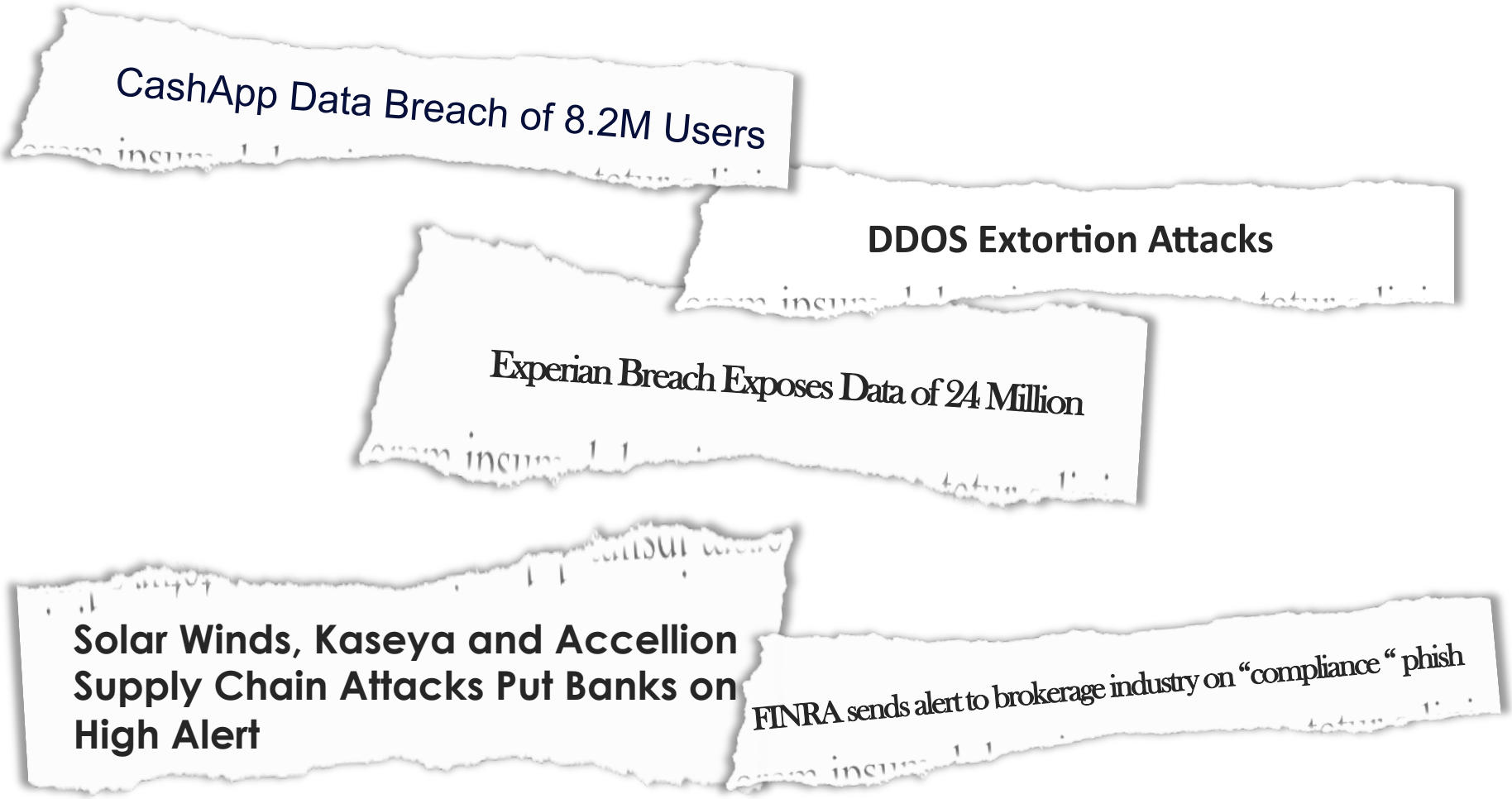
Sector Case Study:
Why Do I Rob Banks (In Cyberspace)?

”Cause That’s Where the Money Is!”

- Also, the U.S financial industry represents the U.S. national power
- And banks have a lot of interesting information about their customers
- And banks represent and lend money to those who represent things some groups and individuals don’t like
- 10% of breaches in 2020 were in the financial industry (Verizon)
- 96% of breaches in 2022 were for financial or personal gain (Verizon)
- Nearly 2/3 of financial services companies have over 1,000 sensitive files open to every employee (Varonis)
- The average cost of a financial services data breach is $5.85M (Varonis)

This

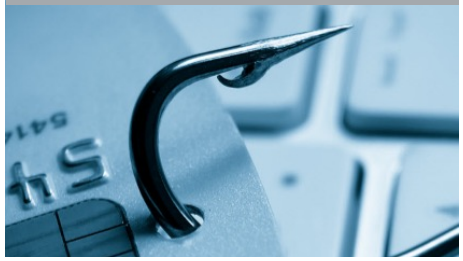
Financial Sector “Highlights” of 2020-2022



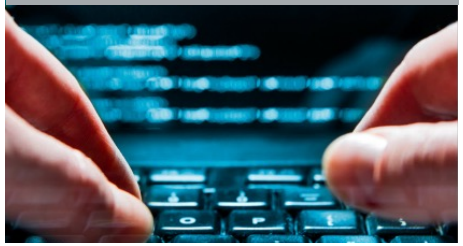
79 U.S. financial services companies reported data breaches affecting 1,000 or more consumers in 2022 according to Flashpoint

Constantly evolving threats—motivational shifts

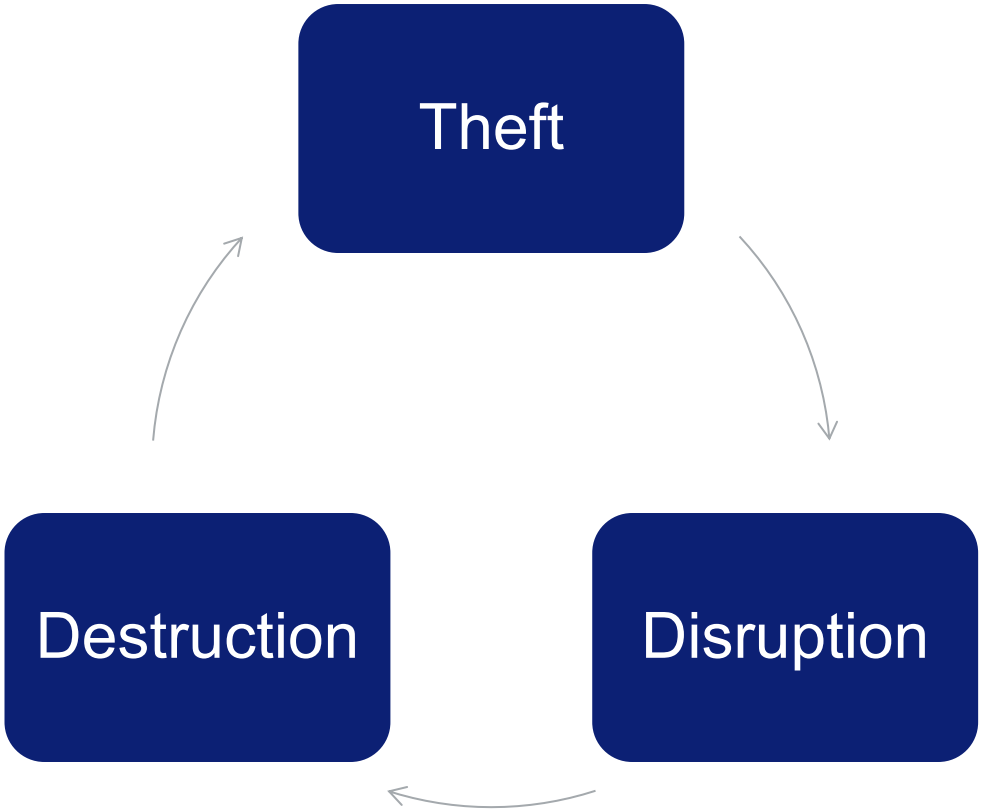
Criminals



Hacktivists



Nation-States



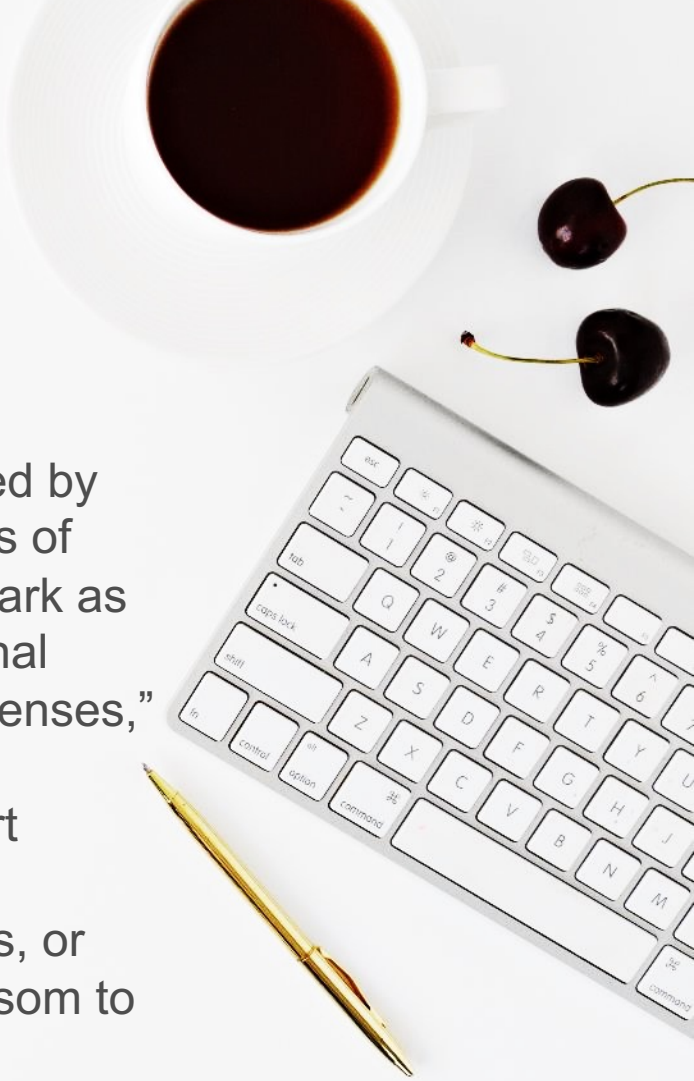
18% of Breaches involved an Insider, according to Verizon's 2022 Data Breach and Incident Response Report

Extremely organized crime

Organized Crime behind 79% of beaches per Verizon 2022 DBIR…

Cybersecurity alert: ransomware

Ransomware targeting consumers is declining; however, overall infection rates are growing particularly among large businesses



- “The average ransomware payment in cases worked by Unit 42 rose to $925,162 during the first five months of 2022, approaching the unprecedented $1 million mark as they rose 71% from last year. That’s before additional costs incurred by victims including remediation expenses,” downtime, reputational harm and other damages.
- Verizon Data Breach and Incident Response Report
- So what is ransomware really?
  - FBI defines as malicious software that encrypts, or locks, valuable digital files and demands a ransom to delete them.
  - But we have a malware protection/detection program…

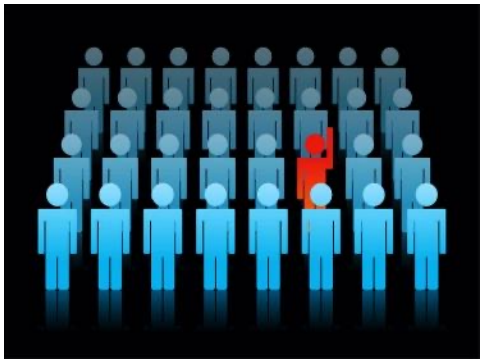
Varonis.com “134 Cybersecurity Statistics and Trends for 2021”
Unit 42 data provided by Palo Alto

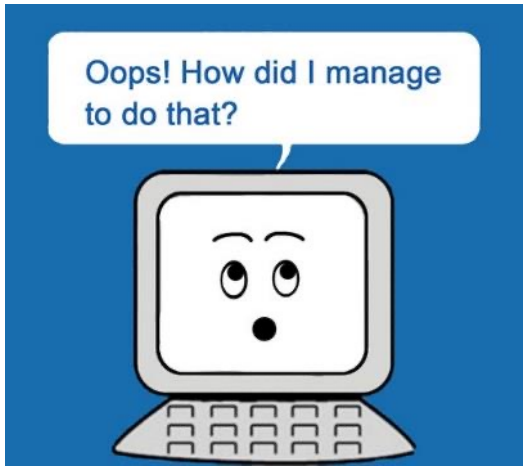
Ransomware, continued

Ransomware actors are continuously upping their game, like any smart business

- Targeting MSPs as a “force multiplier”
  - 1,500 Kaseya customers
- Created “Triple Extortion Ransomware”
  - Steal data
  - Threaten release
  - Target customers or partners
- What is your “Collateral Damage Strategy”?
  - Who is in your IT supply chain?
  - Non-IT? Did you think about Colonial Pipeline before it happened?
  - If I’m not even directly impacted why am I doing so much work?

So What Do I Worry About? A Case Study…

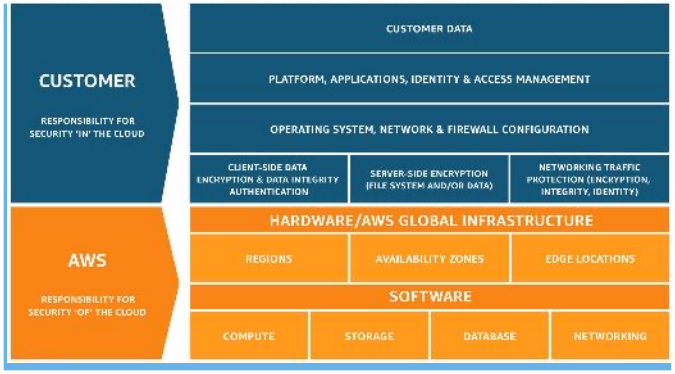




I Feel Like I'm Computing in a Cloud!

The global shift to Cloud Computing has unlocked tons of new business value – and tons of new risks!

What am I responsible for?



Where's my dang data?!

Who set up this Crypto miner?

NEWS › CRYPTOCURRENCY NEWS

Tesla's Cloud Was Hacked for Mining Cryptocurrency

By DANIEL LIBERTO Updated June 25, 2019

Do we even know what we're doing?

The cybersecurity talent shortage: The outlook for 2023

The available potential workforce isn't keeping pace with demand, and experts blame a lack of interest from young people entering the job market.

Published Jan. 13, 2023

(…and why do Millenials and GenZ want to ruin everything?)

Tips to help avoid being a victim

Avoid password reuse

- Remember to:
  - Use strong/multi factor authentication for high risk transactions
  - Make sure all passwords are complex

Update anti-virus (AV)

- AV has its limitations:
  - Most AV is reactive and struggles to find new or hidden malware strains
  - Only catches a fraction of malware

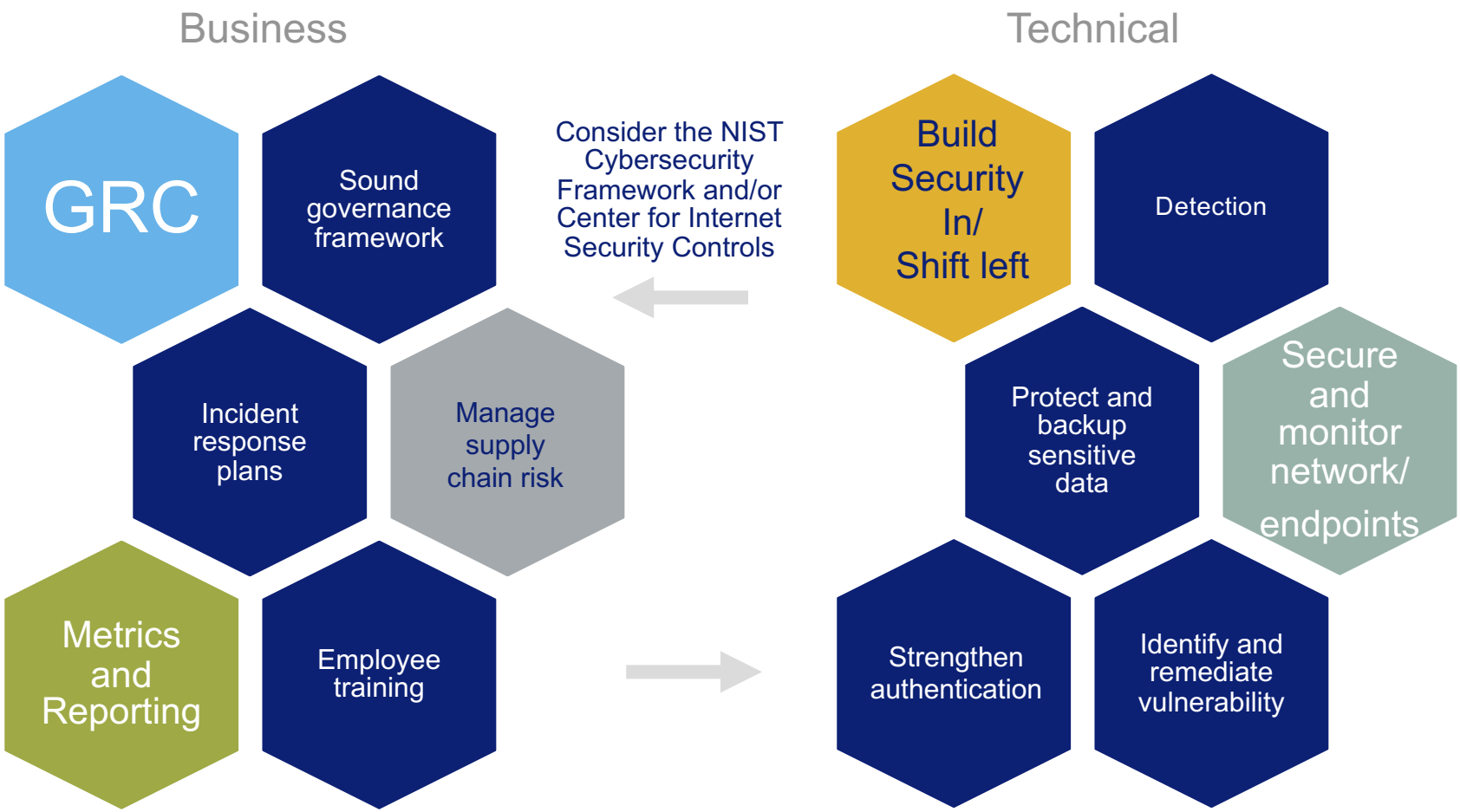
Email & browse smart

- Be careful of:
  - Email links
  - Downloading files
  - Plugins for your browser
  - Social media

Keep software current

- Remember:
  - Computers and phone do not “stay secure” over time
  - Regular updates or patches fix security issues

Industry cybersecurity best practices



Report on Cybersecurity Practices, FINRA, February 2015
https://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf

No, it's not just the CISO's problem…

What can "business" leaders do?

- Risk, security, IT and business leaders must come together to assess and treat the risks appropriately
- Discuss C-I-A. What should be focus on protecting?
- What's most important?
- Know "what's normal"
- Understand connections and third party risk. And M&A!
- Help balance operational resilience, speed to market and security
- Bring security in at the beginning
- Exercise and have crisis management and recovery plans in place

Cyber Employer Pros and Cons…

- Government
  - Less money, big access, big impact, great resume
  - Huge variety of roles
  - Can't be fired…
  - Can't smoke weed, loss of privacy, bureaucracy
- "In House" Private Sector
  - Money depends on company size, regulatory framework, CEO/Board but can be 2, 3, 4, etc. x more than government depending
  - Don't have to "sell" or hit billable hours
  - Depending on industry, may be rewarding
  - Depending on industry, may have access to cool stuff or not
- IT and Consulting
  - Can be big money/stock upside
  - Great resume builder, access to cutting edge
  - May have to sell/hit billable hours

Careers in Cyber – Our Journeys

James Binford ☁️🔓

Jenny Menna

Free resources

- **InfraGard -** a partnership between the FBI and members of the private sector providing a vehicle for the timely exchange of information and promotes learning opportunities to protect Critical Infrastructure**:** www.infragard.org
- **Global Cyber Alliance -** working together to eradicate systemic cyber risk: www.globalcyberalliance.org
- **National Council of Information Sharing and Analysis Centers (ISACs)** – www.nationalisacs.org
- **STOP. THINK. CONNECT.** - global online safety awareness campaign to help all digital citizens stay safer and more secure online: www.stopthinkconnect.org
- **Verizon DBIR** - 2022-data-breach-investigations-report-dbir.pdf (verizon.com)

Government

- **Scholarship for Service:** CyberCorps®: Scholarship for Service (opm.gov)
- **NIST NICE:** National Initiative for Cybersecurity Education (NICE) | NIST
- **NIST Cybersecurity Framework:** https://www.nist.gov/cyberframework
- **Federal Bureau of Investigation Cyber Division:** www.fbi.gov/investigate/cyber
- **Department of Homeland Security** http://www.cisa.gov
  - https://www.cisa.gov/stopransomware