
13TH ANNUAL LEADERSHIP EVENT
CYBER SECURITY SUMMIT
cybersecuritysummit.org
RESILIENCE UNLOCKED
TITLE SPONSOR
Island
#cybersecuritysummit #css13

STATE OF THE UNION: ANNUAL INFORMATION SECURITY REPORT

Oscar Minks, CTO

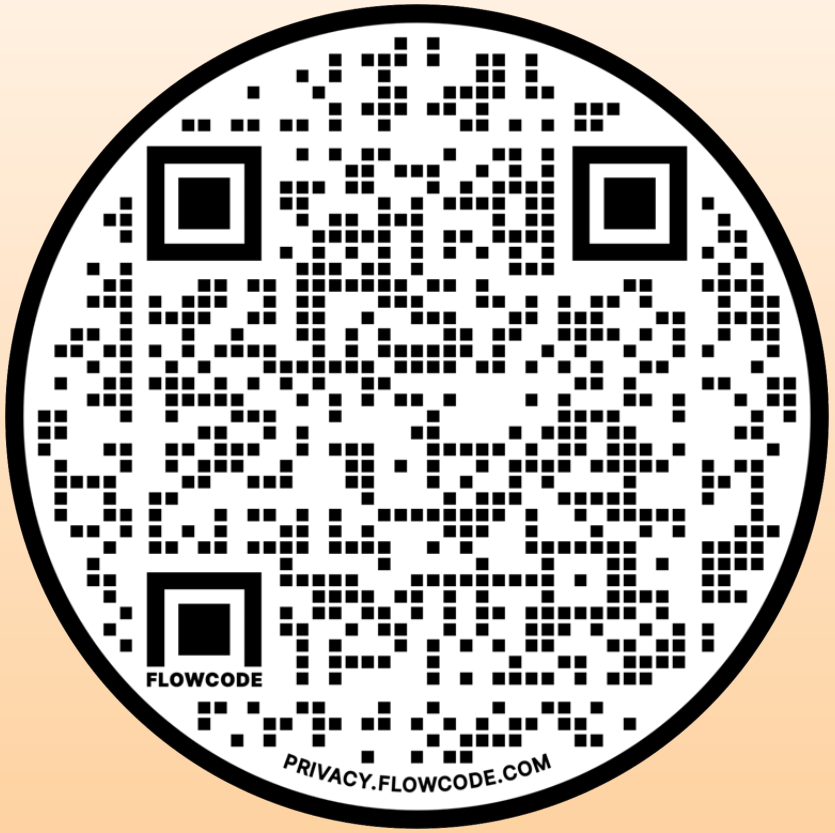
INTRO

Oscar Minks – CTO FRSecure

- Oversee FRSecure Security Operations – Red, Blue, Consulting
- Kentucky born and raised!
- I like helping people; hacking things; stopping hackers; fishing and playing music
- 19 Years in the industry/ MS in Info Sec/ GCFA, GREM
- Memes, anyone?
- Very happy to be here!

ABOUT THE DATA

- ~ 400 Validated Information Security Assessments
  - Healthcare, Technology, MFG, Consumer Services, Education.
  - All Sectors represented
- 55 Incident Response Engagements
  - Information has been anonymized
  - Data logged on controls, Root Cause, Exploits, etc..
- This is our Analysis, Interpretation, and a Proposed Path Forward



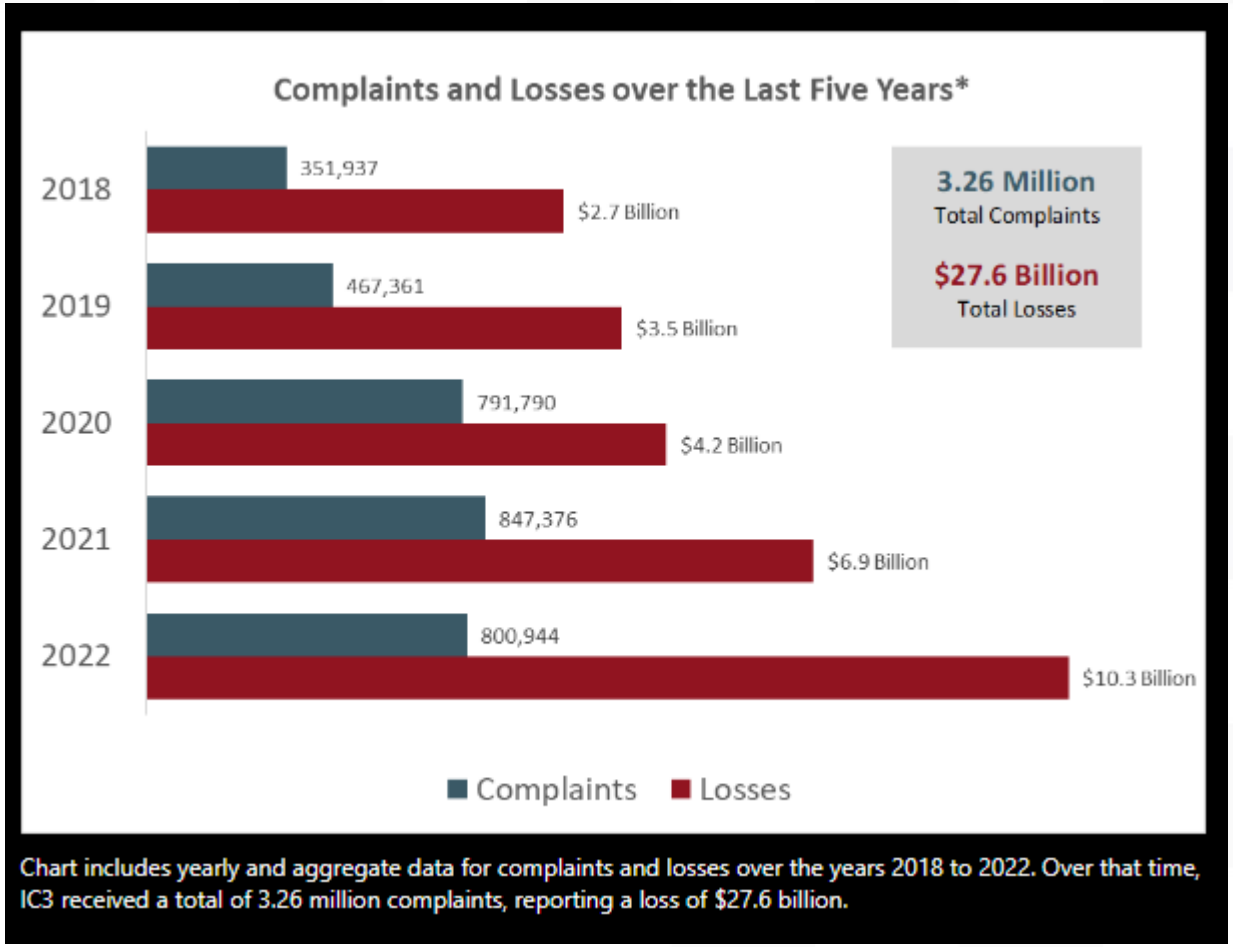
DOWNLOAD THE REPORT

KEY LEARNINGS – TL:DR (DPA)

1. You can’t secure what you don’t know exists.
2. Get a better handle on your vulnerability management program.
3. Logs, Logs, Logs, Logs, Logs…..
4. MFA Everything – but do it the right way.
5. IR Preparedness is key. Have a plan, test the plan. Insurance is not a plan.
6. Train, Train, Train. Develop a security focused culture. (Security as a life skill)
7. Security is not Easy!

IR OVERVIEW

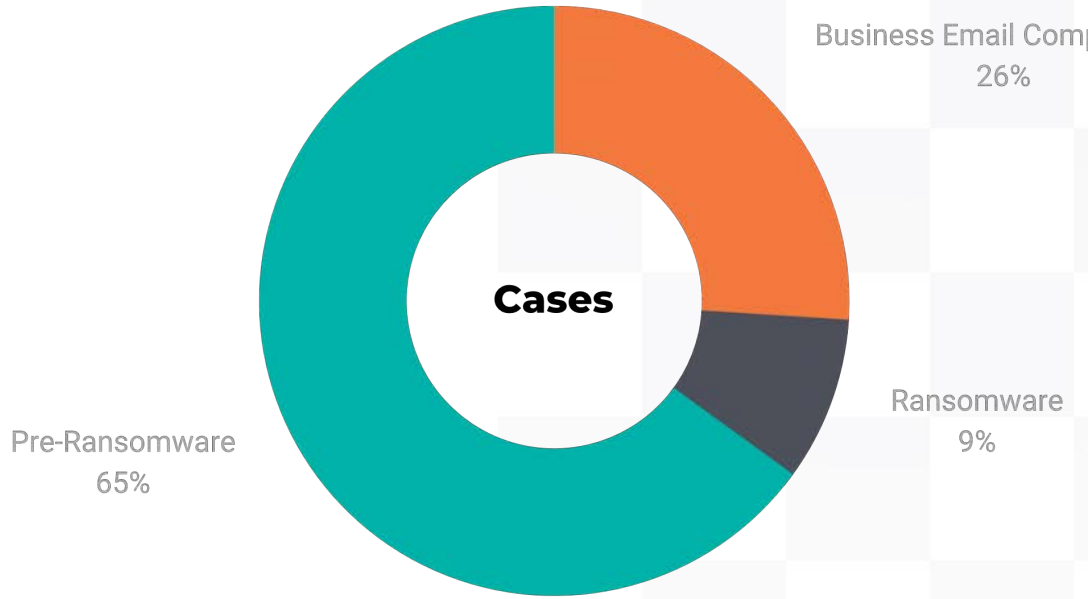
- Financial loss is on the rise
- This data can be used to Educate HOW attacks are happening
- Learn and implement
- Have fewer incidents



IR OVERVIEW

- 55 IR Engagements
  - Ransomware
  - Pre-Ransomware/Internal Compromise
  - Business Email Compromise

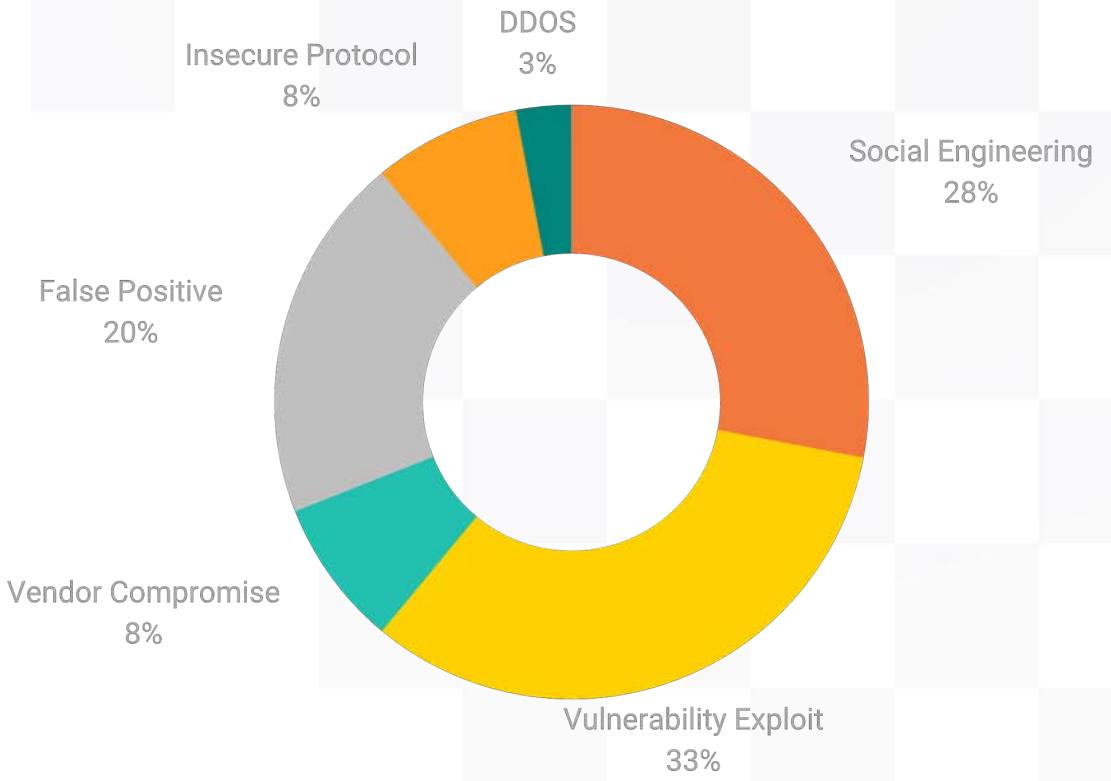
⚠ 2022 INCIDENT OVERVIEW



RANSOMWARE AND INTERNAL COMPROMISE

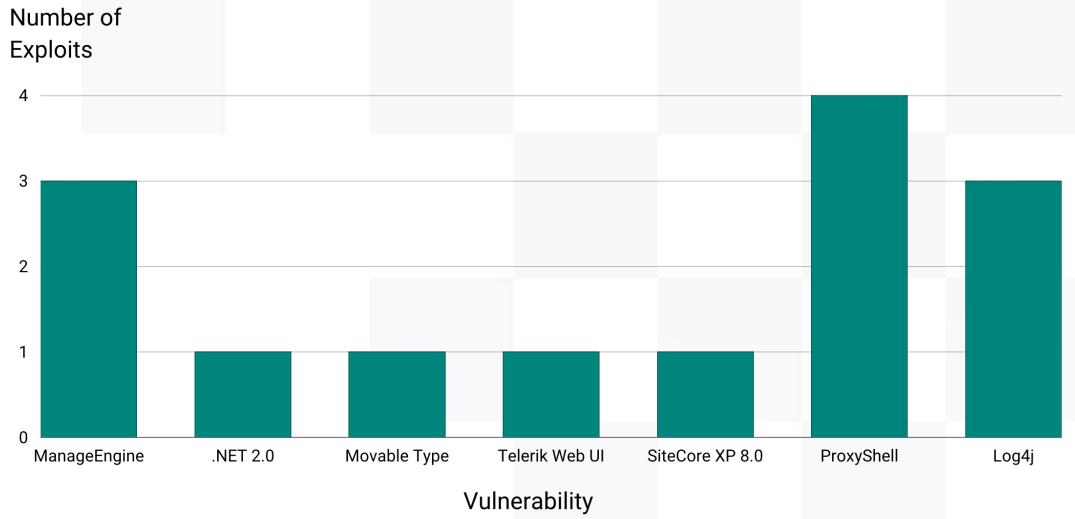
- < 10% of all cases resulted in encryption
  - FRSecure was notified post fact in all but 1
- Being prepared is pretty important…..

COMPROMISE ROOT CAUSE



VULNERABILITY EXPLOITS, OH MY!

- Vulnerability Exploits, Oh My!
  - 33% of cases
  - Vulns we're old
    - Only 1 published within last 12 months
    - Most published in 2021
    - One from 2017



Application Exploits

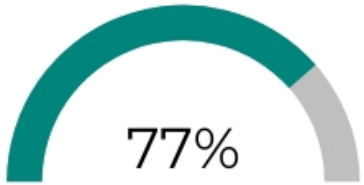
A PATCH IS NOT ENOUGH

- Remember ProxyShell and Log4j?
  - Exploit >> Persistent Web Shell
  - Patch Does NOT Remediate
  - Must Threat hunt!

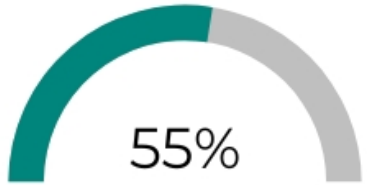
RANSOMWARE – EARLY DETECTION AND RESPONSE ARE IMPORTANT!

- Full Encryption – Ruh Roh
  - All reported POST fact
  - 100% - Vulnerability Exploitation
    - Dwell times ranges – 15 hours (smash and grab) to 9 months
    - 80% - Backup Destruction
  - We're backing up data – but we must evolve!
    - 91% of organizations have an effective backup strategy.
    - 85% of organizations store those backups in a remote facility to avoid physical disaster.
    - Backups were periodically tested and validated in 59% of organizations assessed
    - Air Gapped Bacups IS the BEST defense!

YOU CAN'T SECURE WHAT YOU DON'T KNOW EXISTS



Maintain an inventory of assets to allow for technical vulnerability management.

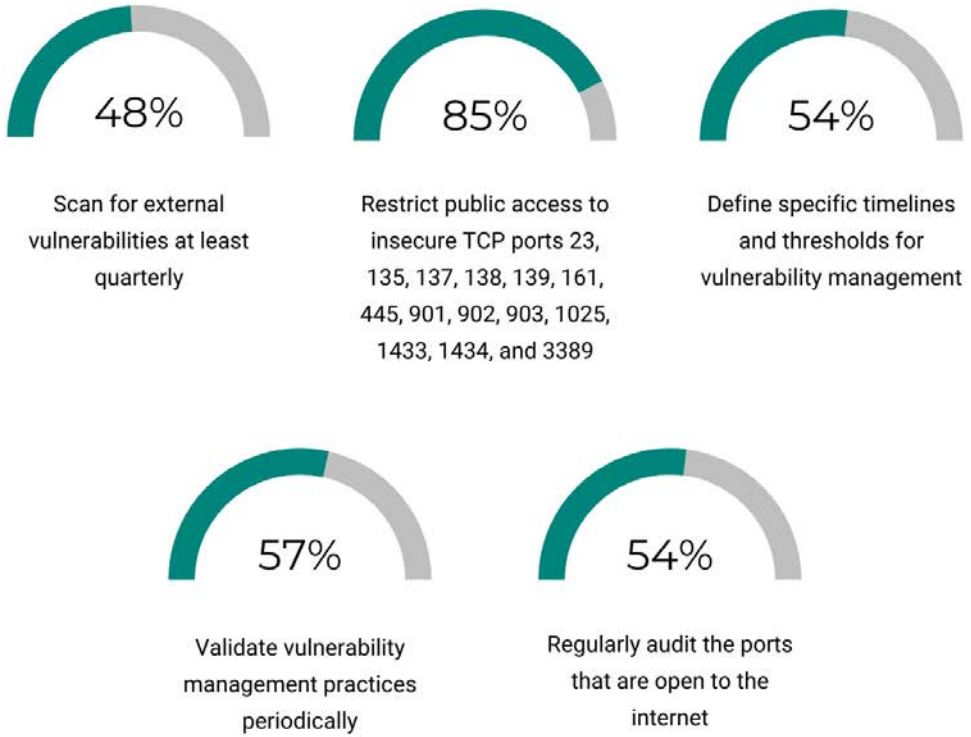


Critical business assets and their dependencies have been identified.

A complete, up to date, and detailed inventory of all cloud services is maintained.

YOU CAN'T SECURE WHAT YOU DON'T KNOW EXISTS

- Let's get better at identifying at attack surface!



YOU NEED TO TEST – NOT BECAUSE THE REGULATOR SAYS SO

- Room to Improve
  - 44% of organizations have conducted a penetration test against all externally facing systems in the past 12 months.
  - 43% of organizations have conducted a penetration test on their internal network in the past 12 months.
  - 51% of web applications are tested for security on a regular basis.
  - 34% of web applications are tested for security each time a change is made.

There is good news though!

- 86% of organizations had no critical-severity (CVSS 10) vulnerabilities on systems exposed to the internet.
- 82% had no high-severity (CVSS 7-9) vulnerabilities on systems exposed to the internet.

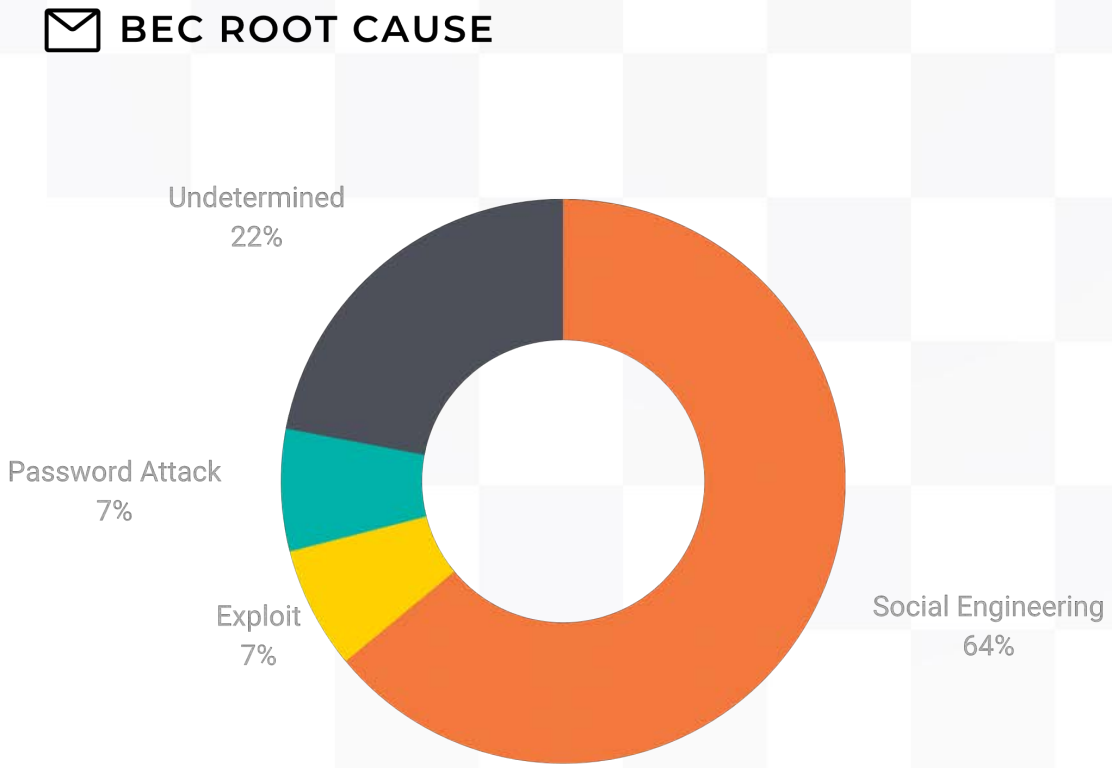
SOAPBOX WARNING – SECURITY IS NOT EASY!

- **Tighten up your egress!**
  - 44% of organizations configure egress filtering to only permit traffic that is specifically authorized for system functionality.

- **Remember Solarigate (Solarwinds)?**
  - Supply chain attack
  - Application update included malcode
  - For malcode to be weaponized – it required outbound connectivity to malicious IP (control server)
  - Attack would have been benign with proper egress filtering!

BUSINESS EMAIL COMPROMISE ROOT CAUSE

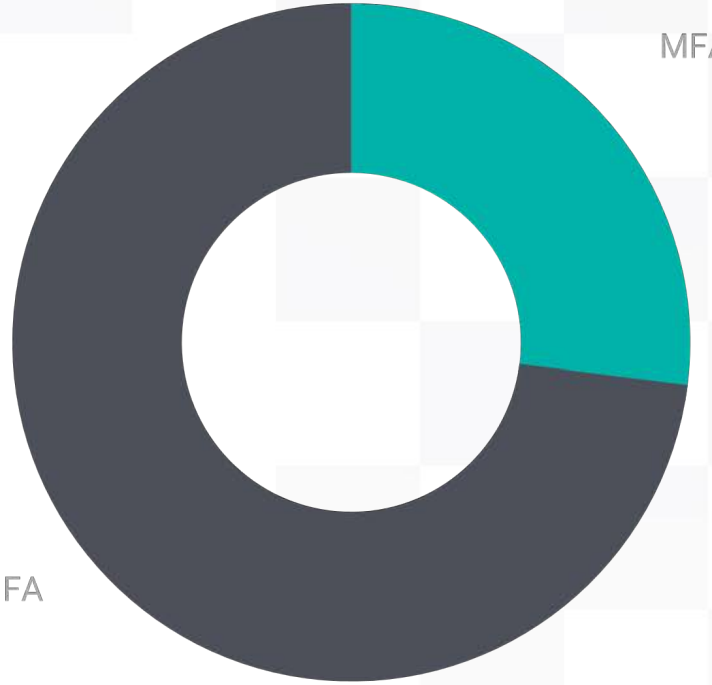
- Social Engineering Remains King
- Technology Evolves and Humans remain the weakest link
  - 80% of organizations test users periodically on their susceptibility to common attack vectors like downloading dangerous files and following malicious links in emails, documents, or web pages.
  - However, only 58% of organizations mandate security awareness training for all employees and contractors on a regular basis.
- Technology Improving but not Infallible
  - 68% of organizations have deployed proper malicious code protections for all applicable transmission methods



MFA INSIGHTS

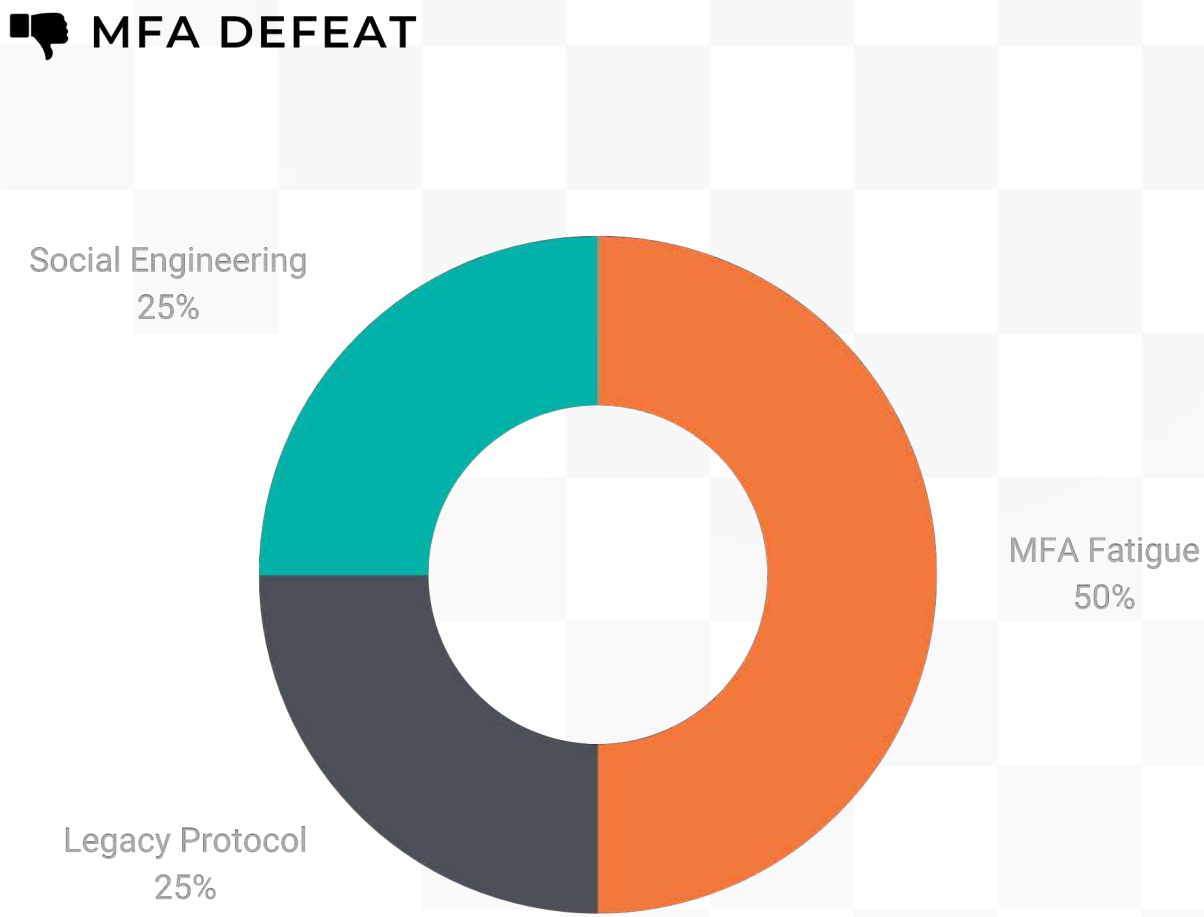
BEC MULTIFACTOR AUTHENTICATION

- MFA – We're still lagging!
  - 73% of BEC victims did not have MFA
  - 70% of organizations protect administrative login pages with multi-factor authentication.
  - 60% of organizations protect general-user login pages with multi-factor authentication.
- MFA – Not a silver bullet



MFA FATIGUE

- MFA Fatigue:
  - 50% of BEC w/ MFA
  - Utilized Push to Approve
  - Don’t use push – Train your users!



MFA FATIGUE

- MFA Fatigue:
  - Humans are creatures of habit
  - Attackers know this
  - Push to Approve (PTA) During common logon times
  - OR – Overload PTA
    - Victims respond to “annoyance”
  - Often unaware they are compromised!

VISHING MFA DEFEAT / LEGACY PROTOCOLS

- Vishing to defeat MFA
  - Helpdesk Vish
  - Compromised Creds
  - Updated OTP deliver phone number
  - Boom – access!
- Legacy Protocols
  - POP, SMTP, IMAP and MAP – no MFA
  - Review config – shut down if not required

MFA IMPLEMENTATION TIPS

- What to do?
  - Don’t use Push to Approve
  - Utilized Hardware Security Key or Authenticator Apps
  - Deploy to ALL accounts w/ Logon capabilities (Services)
  - Don’t stop w/ Email – ALL LOGONS

INGRESS UNKNOWN? LOGS NEEDED!

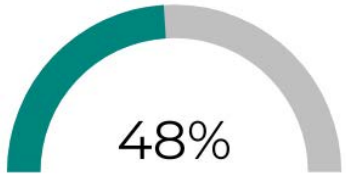
- Know Normal – Find Evil!
  - What does this mean?
- Creatures of habit
  - IP’s; Time; Fingerprint
- Time-Stamps are important – NTP
- M365 – Familiarize w/ Risky Users
- Monitor for new Devices or Authorized Apps (OAUTH)
  - 63% of organizations require access controls for mobile devices.
  - 69% of software applications within the organization are inventoried.

INGRESS UNKNOWN? LOGS NEEDED!

- Pro Tips!
  - Enable Script Block Logging across the domain
  - Don’t assume the identified compromised user – is the only compromised user
    - Most cases we find multiple accounts compromised.

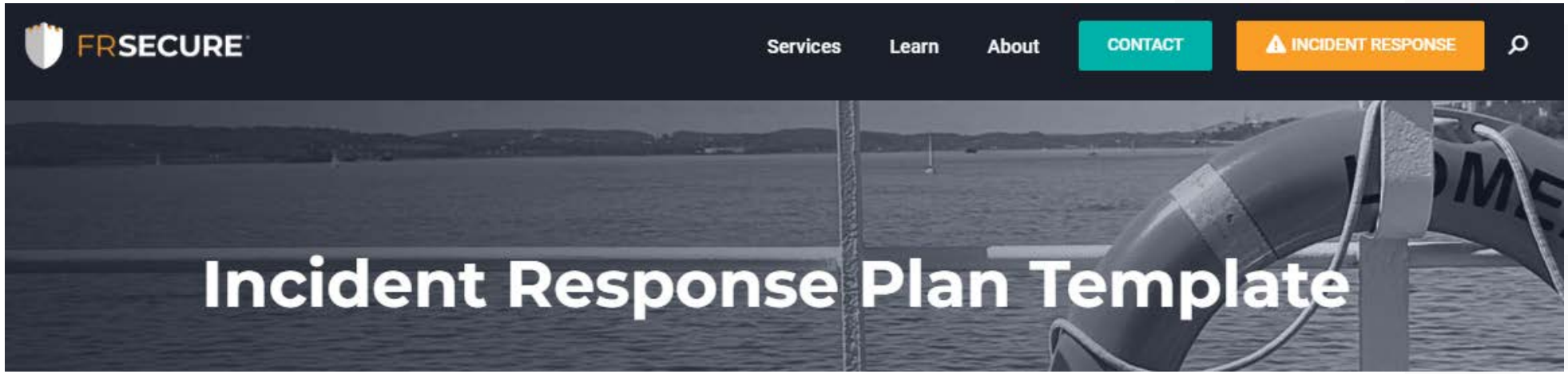
CYBER INSURANCE IS NOT YOUR IR PLAN

- Preparedness is key!!

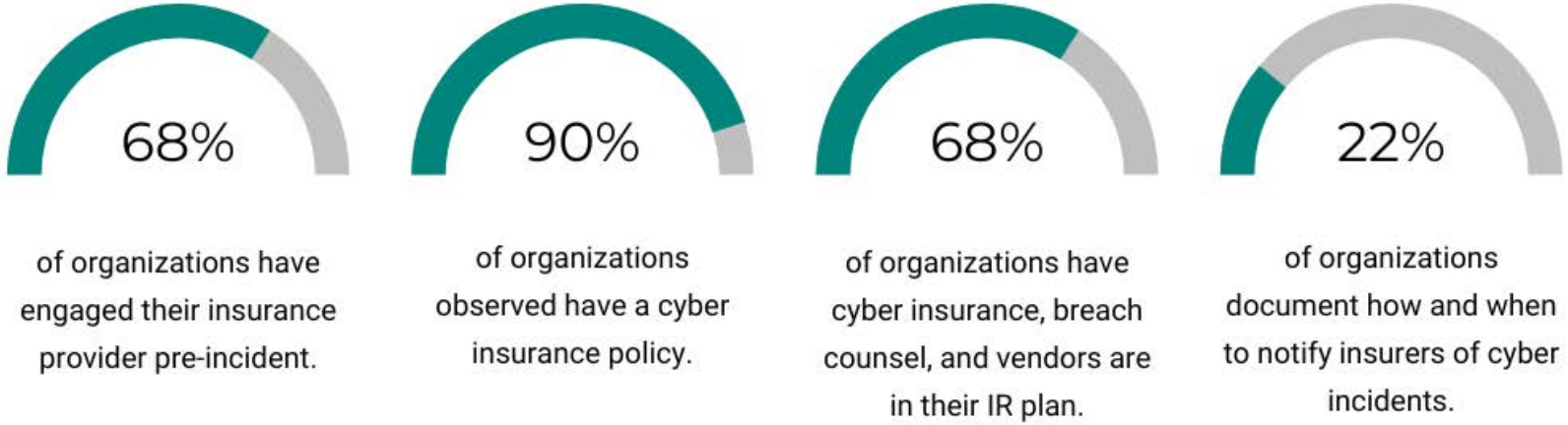


of organizations assessed have defined a formal incident response plan.

of organizations assessed are testing their incident response plan on a periodic basis.



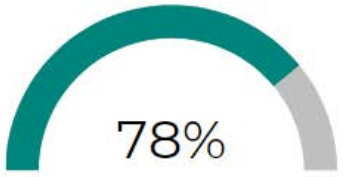
CYBER INSURANCE IS NOT YOUR IR PLAN



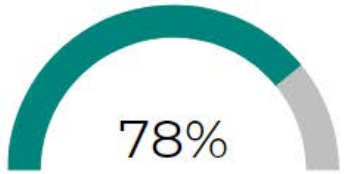
- You're doing it wrong!
  - Not an IR Plan
  - Engage Insurance BEFORE an incident
    - Know your breach coach
    - Agree upon a vendor (you CAN use yours)
    - Document in your IR plan HOW to engage

FOCUS ON SECURITY CULTURE

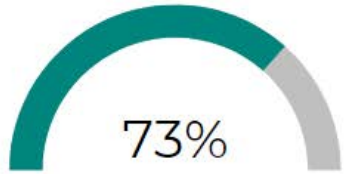
- Leaders set the tone!
- Security as a Life Skill!
- Home Life and Work Life habits co-exist!



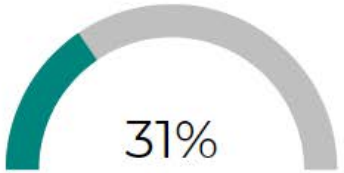
Train users on the dangers of malicious code and know how to deal with malicious code.



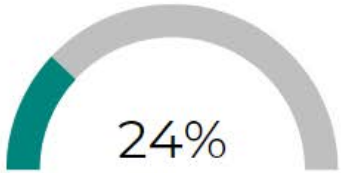
Train employees and relevant third parties on how to select and secure passwords.



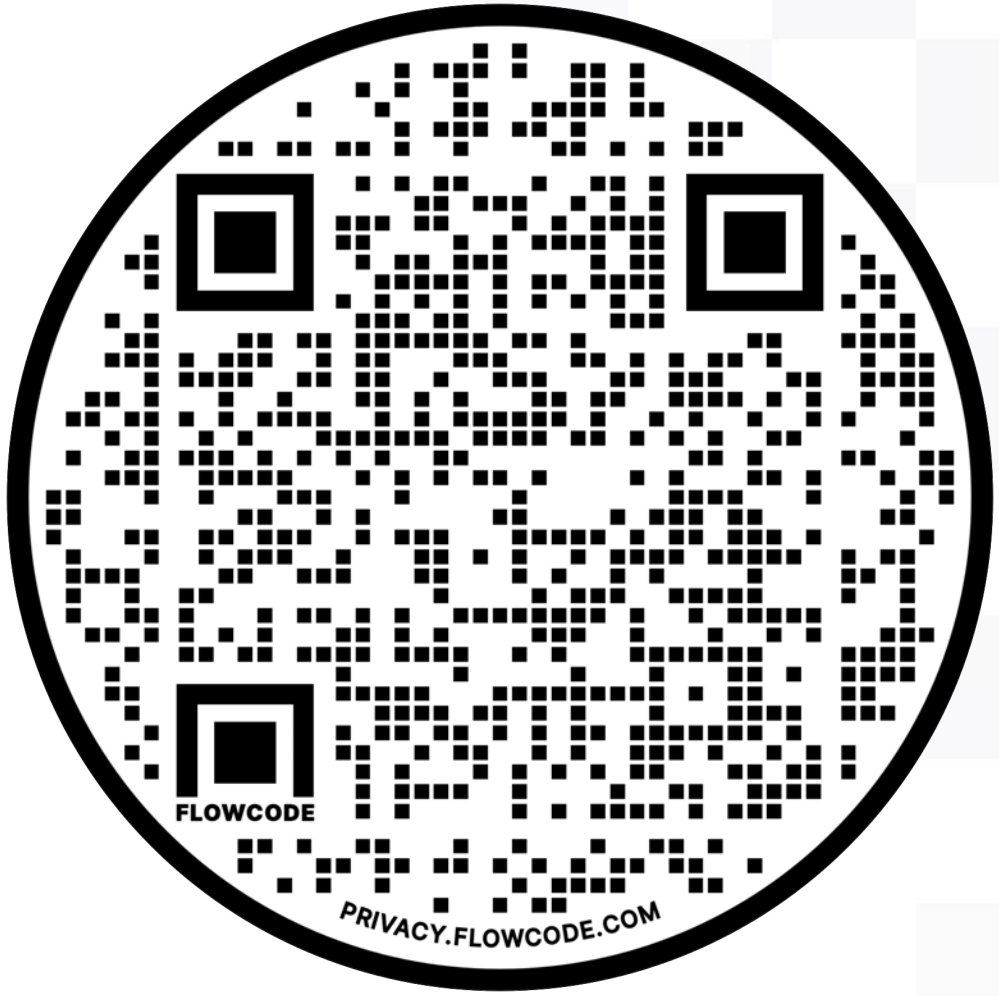
Developed a formal information security awareness, education, and training program.



Give privileged users specialized instruction and training.



Give executives training about their roles and responsibilities concerning InfoSec.



DOWNLOAD THE REPORT

QUESTIONS?

- Feel free to get in touch: