Cybersecurity: Threats, Impacts, and State Regulator Response

Brad Robinson
Senior Director-Cyber Policy & Supervision, CSBS

CSBS

If measured as a country, cybercrime would be the third largest world economy behind the U.S. and China…

- *Cisco/Cybersecurity Ventures*

Top 3 Attack Types: 2021

- Ransomware
- Server Access Compromise
- Business Email Compromise

Source: *X-Force Threat Intelligence Index 2022, IBM Security*

Ransomware

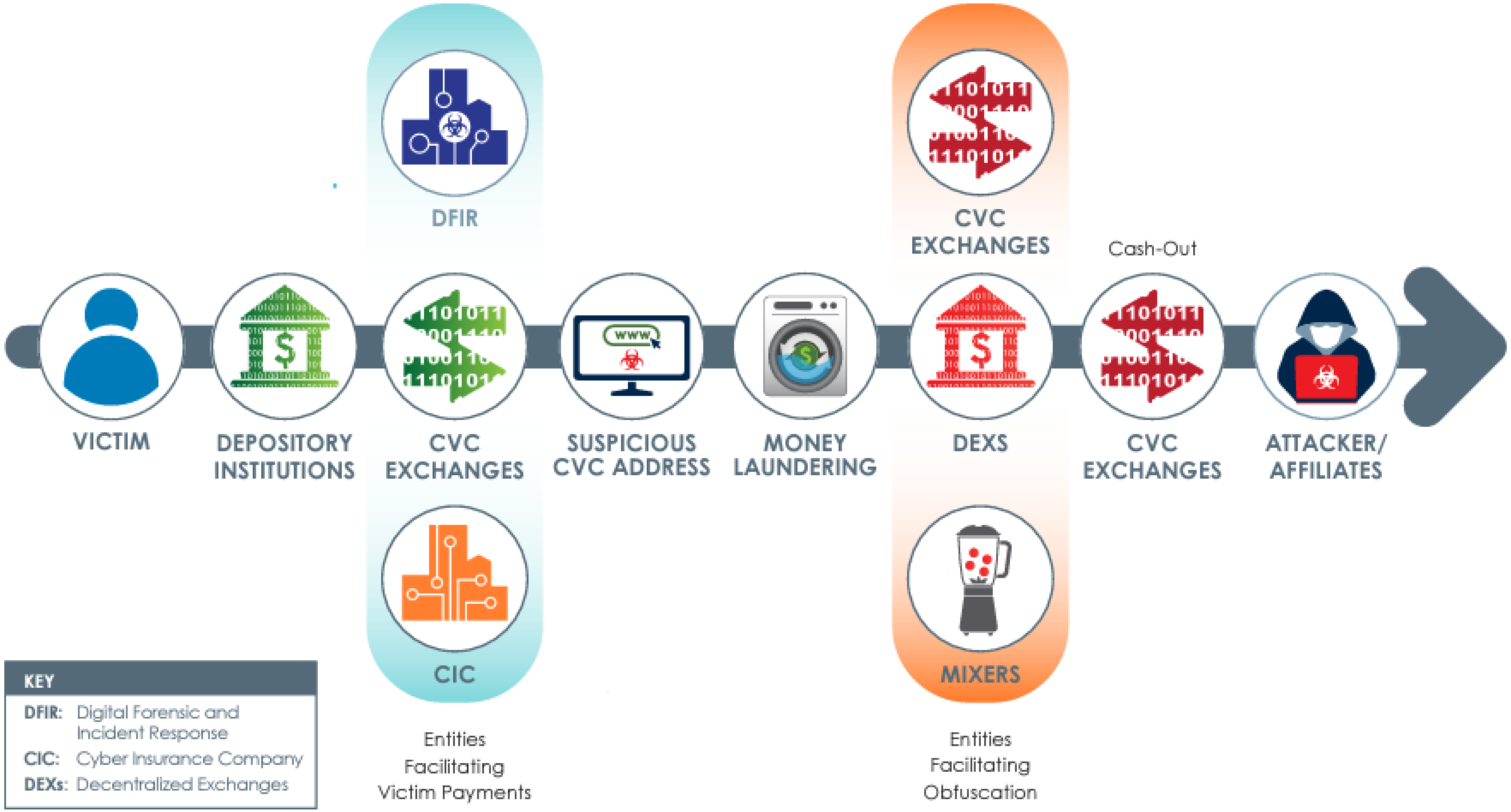
- Top attack type in 2020 and 2021 (21% of all observed attacks)
- Ransomware activity in 2021 appears to have been dominated by two groups:
    - REvil (37% of all observed activity…now appears to have been shut down)
    - Ryuk (13% of all observed activity)
- Ransomware groups remain prolific, but their lifespan is, on average, 17 months before rebranding or shutdown
    - Due largely to law enforcement actions
- Most common vectors for ransomware continue to be phishing, vulnerability exploitation, and remote services such as Remote Desktop Protocol (which is very susceptible to brute force attack)
- “Triple extortion” attacks have emerged as a concerning new trend
    - Exfiltration/Theft of data
    - Encryption of data
    - Distributed denial of service (DDoS) attack → Leak of data if ransom not paid

Source: *X-Force Threat Intelligence Index 2022, IBM Security*

Ransomware Statistics

- Globally, there were 304.7 million ransomware attacks in the first half of 2021, a 151% increase since 2020. *(SonicWall)*
- 80% of organizations were hit by a ransomware attack in 2021. *(Claroty x Forbes)*
- Approximately 32% of organizations reported losing C-level talent, and 29% reported being forced to eliminate jobs as a direct result of an attack. *(Cybereason)*
- Experts estimate that a ransomware attack took place every 11 seconds in 2021. *(Cybersecurity Ventures)*
- At least one employee downloaded a malicious mobile application in 46% of organizations in 2021. *(Check Point)*
- The total cost of a ransomware breach was an average of $4.62 million in 2021, excluding ransom payment. *(IBM)*
- The average ransom payment was $228,125 in Q2 of 2022. *(Coveware)*
- Of the 32% of ransomware victims who paid the ransom in 2021, only 65% of their data was ultimately recovered. *(Sophos)*

Ransomware Funds Movement



KEY

DFIR: Digital Forensic and Incident Response

CIC: Cyber Insurance Company

DEXs: Decentralized Exchanges

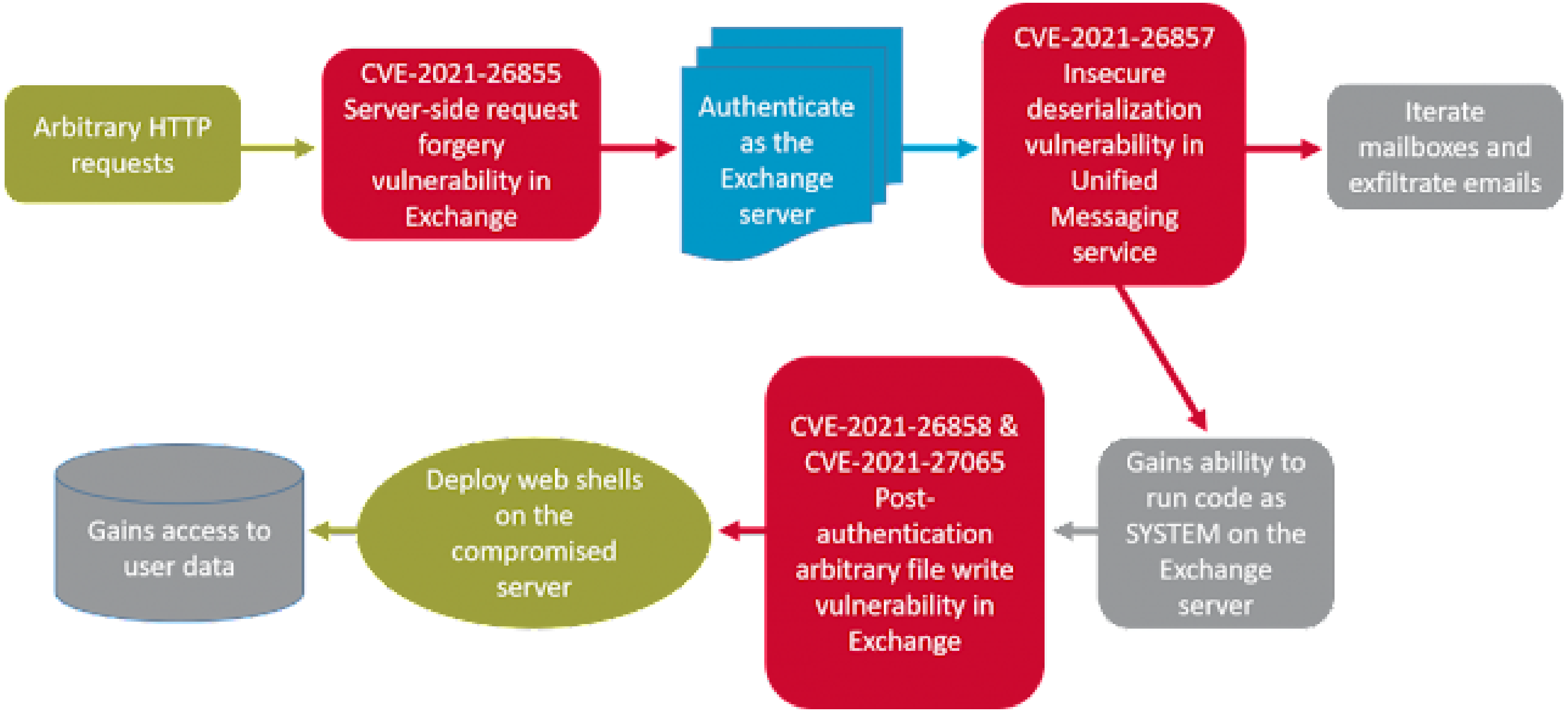
Source: *Fincen.gov*

Server Access Compromise

- Attacks involving bad actors gaining access to a server for unknown/undetermined purposes
- Second most common attack type in 2021 (14% of all observed attacks)
- Most server access attacks occurred in Asia
- Bad actors successful in deploying malware or penetration testing tools on servers
    - China Chopper Webshells
    - Back Orifice malware
    - Printspoofer
    - Mimikatz
- Some bad actors observed exploiting known vulnerabilities to allow remote code execution on a server
    - Microsoft Exchange Server
- Some server access attacks are believed to be failed attempts to steal data or deploy ransomware

Source: *X-Force Threat Intelligence Index 2022, IBM Security*

MS Exchange Server Attacks



Arbitrary HTTP requests

CVE-2021-26855 Server-side request forgery vulnerability in Exchange

Authenticate as the Exchange server

CVE-2021-26857 Insecure deserialization vulnerability in Unified Messaging service

Iterate mailboxes and exfiltrate emails

Gains ability to run code as SYSTEM on the Exchange server

CVE-2021-26858 & CVE-2021-27065 Post-authentication arbitrary file write vulnerability in Exchange

Deploy web shells on the compromised server

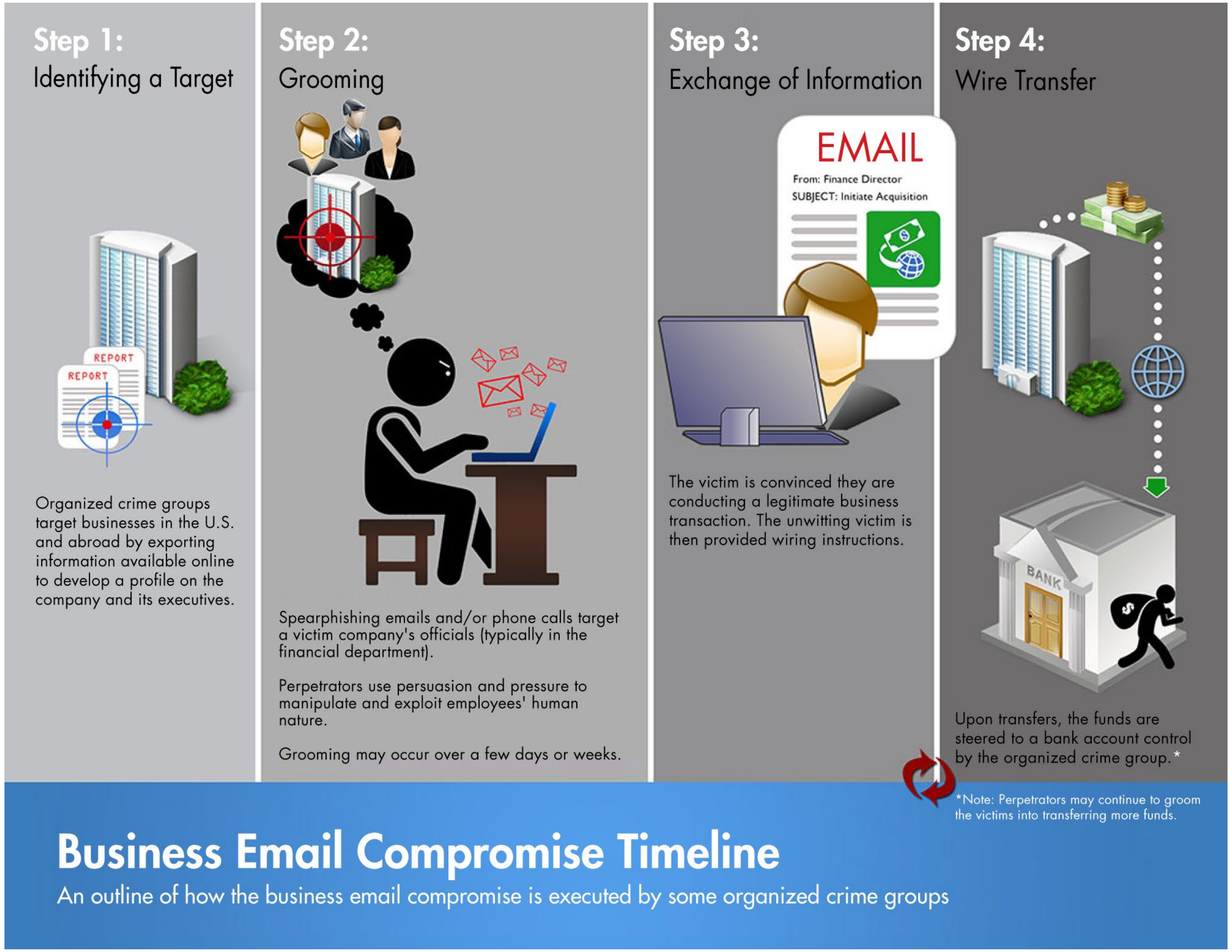
Gains access to user data

Source: *Symantec Enterprise Blogs*

Business Email Compromise (BEC)

- Third most common attack type in 2021 (8% of all observed attacks) *(IBM)*
- Over $43 billion stolen globally in BEC attacks since 2016 *(FBI)*
- 116,401 U.S. victims since 2013
- $14.8 billion lost domestically in the same time period
- BEC complaints tied to cryptocurrency are increasing *(FBI)*
    - "Direct transfer"… Bad actor sends altered wire info to BEC victim, who sends payment to prearranged crypto custodial account
    - "Second hop"… Bad actor establishes phony crypto account in separate fraud victim's name using stolen PII; bad actor then sends altered wire info to BEC victim, who transfers funds into account set up in fraud victim's name
    - Banks located in Thailand and Hong King were primary destinations of fraudulent funds
- Wider implementation of MFA is believed to be the reason for a decline in domestic BEC incidents, as bad actors shift BEC efforts to geographical regions (i.e., Latin America) where MFA use is not widespread *(IBM)*

Business Email Compromise (BEC)



Step 1: Identifying a Target

Organized crime groups target businesses in the U.S. and abroad by exporting information available online to develop a profile on the company and its executives.

Step 2: Grooming

Spearphishing emails and/or phone calls target a victim company's officials (typically in the financial department).

Perpetrators use persuasion and pressure to manipulate and exploit employees' human nature.

Grooming may occur over a few days or weeks.

Step 3: Exchange of Information

The victim is convinced they are conducting a legitimate business transaction. The unwitting victim is then provided wiring instructions.

Step 4: Wire Transfer

Upon transfers, the funds are steered to a bank account control by the organized crime group.*

*Note: Perpetrators may continue to groom the victims into transferring more funds.

Business Email Compromise Timeline

An outline of how the business email compromise is executed by some organized crime groups

Source: *FBI*

Attack Vectors

- Phishing
  - Average click rate of approximately 18%
  - Increased to 53% with concurrent use of vishing (voice phishing)
  - 222,127 phishing attacks recorded in June 2021 (a record high)
- Vulnerability exploitation
  - Bad actors leveraged multiple known vulnerabilities (including Log4j) and zero-day vulnerabilities (i.e., Kaseya, Microsoft Exchange Server) in 2021
  - Number of vulnerabilities continues to skyrocket, as well as number of tools used to exploit vulnerabilities
- Use of stolen credentials
- Brute force attacks (trial and error password guessing)
- Remote desktop protocol (RDP)
  - Brute force attacks against RDP are the most common methodology used by threat actors to gain access to Windows systems *(Zscaler)*

Source: *X-Force Threat Intelligence Index 2022, IBM Security*

Other Current Concerns

- Supply Chain & Third-Party Attacks/Disruptions
  - Reliance on third parties is significant in our institutions for infrastructure service and maintenance, core processing and platform OS, data storage, security, etc.
  - Attacks and incidents at relied-upon third parties can have a significant, simultaneous impact on multiple institutions across many geographies
    - Kaseya (2021)
    - Equifax (2017)
    - SolarWinds (2020)
- Critical Infrastructure Attacks
  - Recent concerns driven by geopolitical tensions (i.e., Russia/Ukraine conflict)
  - CISA issued multiple alerts regarding Russian activity/pro-Russian sympathizers
  - Urgent call to action delivered to regulators and industry in January 2022
  - Identify minimum service levels; alternate arrangements in the event of payment system disruptions; identify alternate access to critical bookkeeping records; preparations for extended power/telecom/financial market outages; alternate communications with critical service providers

Security Incident Costs

- Average domestic cost of a data breach: $9.44 million (and increasing annually)
- Estimated financial sector attack cost in 2022: $5.97 million
- An estimated 83% of all organizations have experienced multiple breaches
- Average cost savings for organizations having an IR team and regularly tested IR plan: $2.66 million
- Average time to identify and contain a data breach:
  - 207 days to identify
  - 70 days to contain
  - Shorter breach life cycle = lower costs
- Not all costs are immediately quantifiable
  - Reputation
  - Legal
  - Regulatory
  - Inability to service your customer

Source: *Cost of a Data Breach Report 2022, IBM Security*

Cyber Hygiene

Basic cyber hygiene practices can go a long way towards protecting your organization against cyber threats. Best practices include the following:

- Establish a consistent patching routine, particularly for critical- and high-severity patches
- Know your data and systems and manage who has access to them (including third-party access)
- Implement multi-factor authentication (MFA) throughout your company
- Encrypt sensitive customer and company data (in-transit and at-rest)
- Use anti-virus/anti-malware software and frequently update virus definitions
- Develop effective, event-specific incident response plans and test them frequently
- Build a strong ongoing vendor management program
- Implement a strong, repeatable employee training program, including frequent social engineering testing
- Ensure the isolation of data backups and test them frequently

Ransomware Self-Assessment Tool (R-SAT)

- Released in December 2020
  - Developed in conjunction with US Secret Service and Bankers Electronic Crimes Task Force (BECTF)
  - 16 questions, plus additional supporting narrative
- Goals: Evaluates entity preparedness towards:
  - Identifying, protecting, detecting, responding, and recovering from a ransomware attack
  - Can also assist third parties (auditors, consultants, regulators) that might review security practices
- Periodic internal reevaluation of security practices relative to ransomware preparedness
- **UPDATE COMING**: CSBS is currently working with BECTF to review and update

Bankers
Electronic Crimes Task Force

U.S. Department of
Homeland Security
United States
Secret Service

Resources

- *“Cybersecurity 101: A Resource Guide for Bank Executives”*… https://www.csbs.org/data-tools/cyber101
- Ransomware Self-Assessment Tool (R-SAT)… https://www.csbs.org/ransomware-self-assessment-tool
- Cybersecurity & Infrastructure Security Agency (CISA) Shields Up... https://www.cisa.gov/shields-up
- Stop Ransomware (U.S. Government website)… https://www.cisa.gov/stopransomware

FOR QUESTIONS OR ADDITIONAL INFORMATION, PLEASE CONTACT:

BRAD ROBINSON

SENIOR DIRECTOR, CYBERSECURITY POLICY AND SUPERVISION

brobinson@csbs.org

(205) 535-2220